Primality Tests on Commutator Curves

Dissertation
der Mathematischen Fakultät
der Eberhard-Karls-Universität Tübingen
zur Erlangung des Grades eines
Doktors der Naturwissenschaften

vorgelegt von
Sebastian Wedeniwski

Tübingen
2001

Tag der mündlichen Qualifikation: 16. November 2001

Dekan:	Prof. Dr. C. Lubich
1. Berichterstatter:	Prof. Dr. W. Knapp
2. Berichterstatter:	Prof. Dr. P. Schmid

Vorwort

An dieser Stelle möchte ich mich bei all denen bedanken, die mir bei der Fertigstellung dieser Arbeit geholfen haben.

Zunächst gilt mein besonderer Dank meinem Betreuer Prof. Dr. W. Knapp für seine unermüdliche Diskussionsbereitschaft, die vielen wertvollen Anregungen und die Beweisvorschläge, welche in der gesamten Arbeit Eingang gefunden haben. Seine Genauigkeit bei der Korrektur und die hervorragenden Arbeitsbedingungen waren mir eine große Hilfe.
Desweiteren möchte ich mich bei Herrn Prof. Dr. P. Schmid für einen Beweisvorschlag bedanken, den er in Bezug auf die Bestimmung der Mächtigkeit der Menge $L_\epsilon(p)$ für eine ungerade Primzahl p und $\epsilon \in \{-1, 0, 1\}$ eingebracht hat. Ich habe diesen in Kapitel 4, Abschnitt 5 in veränderter Form übernommen.

Besonders gefreut habe ich mich, dass Prof. Dr. C. Pomerance, New Jersey, sich die Zeit genommen hat, diese Arbeit zu lesen und mit einigen Hinweisen und Vorschlägen zu verbessern – Herzlichen Dank dafür.

T. Rau war mir mit seinen zahlreichen sprachlichen Korrekturen die ganze Zeit über sehr hilfreich, wofür ich ihm danken möchte; und Th. Kaebel bin ich für Korrekturen einer früheren Manuskriptfassung dankbar.

Meinen letzten persönlichen Dank sage ich meiner Frau Esther für ihre zahlreichen Hilfen im Detail sowie ihre allgemeine Unterstützung dieser Arbeit.

Zusammenfassung

Das Thema dieser Arbeit sind effiziente Primzahltests.
Vor 25 Jahren formulierte G. L. Miller [**86**] einen Primzahltest, der gleichzeitig schnell und zuverlässig ist, dabei aber von der Annahme ausgeht, dass die Erweiterte Riemannsche Hypothese korrekt ist. Seither versuchten viele, einen Test ohne diese Annahme zu formulieren. Diese Versuche brachten jedoch nicht die gewünschten Ergebnisse und scheiterten darin, gleichzeitig schnell und zuverlässig zu sein.
Dieses Dilemma ist der Ausgangspunkt der vorliegenden Arbeit. In einem ersten Schritt habe ich versucht, einen Primzahltest zu formulieren, der sowohl die Bedingung der Schnelligkeit als auch die der Zuverlässigkeit erfüllt und nicht von der Korrektheit der Erweiterten Riemannschen Hypothese abhängt. Denn es existiert ein Bereich, für den die Riemannsche Hypothese bereits bewiesen ist. Mein Fokus lag nun darin, für den Primzahltest ebenfalls einen solchen gültigen Bereich zu finden. Folgende drei Ergebnisse, die für die Riemannsche Hypothese gelten, werden dabei berücksichtigt:

(1) Bereits 1979 zeigte H. W. Lenstra, Jr. in [**76**], dass Millers Primzahltest die Korrektheit der Erweiterten Riemannsche Hypothese nicht benötigt, wenn die zu testende Zahl nicht quadratfrei ist.
(2) J. van de Lune, H. J. J. te Riele und D. T. Winter zeigten in [**82**], dass die Riemannsche Zeta-Funktion genau 1 500 000 001 Nullstellen der Form $\sigma + it$ im Bereich $0 < t < 545\ 469\ 823,215$ besitzt. Diese Nullstellen haben alle den Realteil $\sigma = \frac{1}{2}$ und bestätigen damit die Riemannsche Hypothese in diesem Bereich.
(3) J. B. Conrey bewies in [**34**], dass mindestens 40% aller nichttrivialen Nullstellen der Riemannschen Zeta-Funktion auf der kritischen Geraden liegen.

Dieser Ansatz hat es ermöglicht, ihre Notwendigkeit innerhalb des Beweises des Primzahltests von G. L. Miller auf nur noch ein Schlüssellemma zu begrenzen. Zusätzlich konnte ich den Rechenaufwand für diesen Primzahltest verringern, indem nun weniger Basen für diesen Test notwendig sind. Leider konnte ich die Hypothese nicht völlig eliminieren, weshalb ich in einem zweiten Schritt einen neuen Ansatz für einen Primzahltest gewählt habe, dem die folgende These zugrundeliegt:

> Es ist von Vorteil, für einen Pseudoprimzahltest die *Kommutatorkurve* in der zweidimensionalen speziellen linearen Gruppe zu verwenden.

Dieser neue Pseudoprimzahltest benötigt im Gegensatz zum Pseudoprimzahltest von J. Grantham [**52**] nur einen skalaren Parameter; darüber hinaus ist die feste Anzahl von

Probedivisionen deutlich kleiner, weil nur all jene Primzahlen überprüft werden müssen, die kleiner als 80 sind, statt 50 000 wie es beim Pseudoprimzahltest von J. Grantham erforderlich ist. Außerdem ist er in mehrerlei Hinsicht ausbaufähig.

Die Arbeit ist insgesamt in sechs Kapitel und drei Appendizes gegliedert: Die theoretischen Grundlagen für das oben formulierte Ziel sind im Kapitel 2 zusammengetragen. Kapitel 3 liefert eine Übersicht aller entscheidenden Forschungsergebnisse, die während der 25 Jahre seit Miller erschienen sind und von denen ich einige auf ihre Vor- und Nachteile hin analysiere. Die eigentliche Forschungsarbeit beginnt mit Kapitel 4. Es werden Kommutatorkurven in der zweidimensionalen speziellen linearen Gruppe eingeführt und ihr Nutzen für einen Primzahltest ausgearbeitet. Aufgrund der erarbeiteten Ergebnisse werden die Kommutatorkurven für einen neuen Pseudoprimzahltest verwendet. Dies ist Thema des Kapitels 5 ist. Schließlich greife ich in Kapitel 6 den Miller-Test wieder auf und diskutiere für ihn die Notwendigkeit der Erweiterten Riemannschen Hypothese.

Als konkrete Ergebnisse dieser Arbeit erhalte ich folgendes:

(1) Ich führe in Kapitel 4 die *Kommutatorkurve* ein, welche durch einen skalaren Parameter in der zweidimensionalen speziellen linearen Gruppe bestimmt wird, und erarbeite für sie die theoretischen Grundlagen, die im weiteren Verlauf der Arbeit für einen Primzahltest eingesetzt werden. In den darauf folgenden Abschnitten werden alle möglichen Elementordnungen und deren Häufigkeit auf dieser Kurve ausgearbeitet. Die konkrete Verteilung der Elementordnungen auf dieser Kurve wird zuerst Modulo einer Primzahlpotenz in Theorem 4.32 und dann Modulo einer zusammengesetzen Zahl in Theorem 4.35 und Theorem 4.36 analysiert. Dabei stellt sich in Lemma 4.40 heraus, dass eine ordnungserhaltende Bijektion zwischen einem Bereich der Kommutatorkurve Modulo einer Primzahl p und einer Untergruppe von $\mathbb{F}_p^*$ existiert. Der verbleibende Bereich dieser Kurve kann bijektiv und ordnungserhaltend auf einer Teilmenge von $\mathbb{F}_{p^2}^*$ abgebildet werden, was in Lemma 4.42 gezeigt wird.

(2) In Abschnitt 7 des Kapitels 4 erarbeite ich rekursive Formeln und in Theorem 4.61 eine Beziehung zu den Lucas-Folgen, um Elementordnungen auf der Kommutatorkurve schnell ermitteln zu können. Im letzten Abschnitt 8 werden dann sieben Varianten zur Berechnung der Ordnung eines Elements auf dieser Kurve theoretisch nach dem „best-case“, „worst-case“ und „average-case“ Zeitverhalten bezüglich des Miller-Tests ausgewertet. Dabei stellt sich heraus, dass die schnellste Variante auf einer Lucas-Folge basiert und etwa dreimal soviel Laufzeit benötigt wie die Exponentiation Modulo einer natürlichen Zahl.

(3) Dann, in Theorem 4.53 des Kapitels 4 beweise ich ein Kriterium für die Kommutatorkurve über einer Primzahl p, welches analog zum Euler-Kriterium für $\mathbb{F}_p^*$ ist; dieses Kriterium ist das grundlegende Hilfsmittel für den später eingeführten und diskutierten Kommutatorkurventest.

(4) Es werden *LN-Zahlen* analog zu den Carmichael-Zahlen betrachtet. Diese Zahlen sind so definiert, dass sie analoge Eigenschaften zu den Carmichael-Zahlen

haben. Ich beweise dann schließlich in Corollary 4.48 des Kapitels 4, dass solche Zahlen nicht existieren können.

(5) Im Kapitel 5 erfolgt genau diese Einbindung der Kommutatorkurve in verschiedene Pseudoprimzahltests. Zuerst werden zwei einfache Tests aufgestellt, die analog zum Fermat- und Euler-Test sind (Algorithm 5.1 und Algorithm 5.2). Ich beweise darüber hinaus in Theorem 5.10, dass dieser Pseudoprimzahltest, der auf das Euler-Kriterium beruht, als zuverlässiger Primzahltest eingesetzt werden kann. Als wichtigster Pseudoprimzahltest ist der *Kommutatorkurventest* (*Commutator Curve Test*) zu nennen. In Theorem 5.28 beweise ich, dass dieser Test nach einer festen Anzahl von Probedivisionen (alle Primzahlen kleiner 80) das Ergebnis „wahr“ für eine zusammengesetzte Zahl mit einer Wahrscheinlichkeit ausgibt, die kleiner als $\frac{1}{16}$ ist; das heißt, dieser Test liefert das Ergebnis „wahr“ für eine zusammengesetzte Zahl mit einer Wahrscheinlichkeit kleiner als $\frac{1}{16^k}$, wenn k Basen in unabhängiger Weise zufällig gewählt werden.

(6) Zum Abschuss des Kapitels 5 wird, basierend auf dem Kommutatorkurventest, ein neuer *Hypothetical Commutator Curve Primality Test* aufgestellt, der schnell und – zumindest für alle Zahlen kleiner als 10^7 (Theorem 5.31) – zuverlässig ist.

(7) In Kapitel 6 führe ich einen neuen Beweis zur Korrektheit des Miller-Tests durch und überprüfe dabei jede Stelle, die die Korrektheit der Erweiterte Riemannsche Hypothese vorraussetzt. Außerdem diskutiere ich alternative Beweismöglichkeiten. Schließlich läßt sich die Notwendigkeit der Erweiterten Riemannschen Hypothese für den Beweis des Primzahltests von G. L. Miller auf nur noch ein Schlüssellemma 6.38 eingrenzen. Darüber hinaus zeige ich in Theorem 6.7 unter der Annahme, dass die Erweiterte Riemannsche Hypothese korrekt ist, dass der Miller-Test zur Überprüfung einer Zahl n nur noch für alle Primzahlbasen kleiner als $\frac{3}{2}\ln(n)^2$ durchgeführt werden muss.

Die drei Appendizes haben den folgenden Inhalt:

(1) Appendix A gibt eine obere Schranke für die kleinsten quadratischen Nichtreste an. Dies findet in Kapitel 6 Verwendung.

(2) Appendix B enthält Tabellen, die als Basis für Beobachtungen und Vermutungen in dieser Arbeit allgemein dienen.

(3) Appendix C bietet fünf unterschiedliche Implementierungen und Laufzeitvergleiche meines *Hypothetical Commutator Curve Primality Test* an.

Contents

CHAPTER 1

Introduction

This thesis is about efficient primality tests.
25 years ago, G. L. Miller [**86**] formulated a primality test that was both fast and reliable. But it depended on the assumption that the Extended Riemann Hypothesis is true. Since then, many attempts have been made to formulate a test that does not need this assumption. These attempts did not bring up the desired result, for they either lacked speed or reliability.
This dilemma is the starting point of my thesis. In a first step, I have tried to formulate a primality test that fulfills both requirements, speed and reliability, and that does not depend on the truth of the Extended Riemann Hypothesis. Nevertheless, the Riemann Hypothesis have been proved for a certain range. My main focus was to find such a valid range of numbers for Miller's primality test. The following three results, which are valid for Riemann's Hypothesis, are taken into account:

(1) As soon as 1979, H. W. Lenstra, Jr. proved in [**76**] that Miller's primality test does not depend on the Extended Riemann Hypothesis being true, if the tested number is not squarefree.
(2) J. van de Lune, H. J. J. te Riele and D. T. Winter shown in [**82**] the truth of the Riemann Hypothesis for the first 1 500 000 001 roots of the form $\sigma + it$ in the critical strip with $0 < t < 545\ 469\ 823.215$, i.e., all these roots have real part $\sigma = \frac{1}{2}$.
(3) J. B. Conrey proved in [**34**] that at least 40% of all non-trivial roots of Riemann's zeta function lie on the critical line.

As an effect, the necessity of the Extended Riemann Hypothesis in Miller's primality test could be reduced to one key lemma. In addition, by reducing the bases that are required for this test, I could reduce the run time. Nevertheless, I cannot remove the hypothesis completely. I therefore have chosen a second step for a new starting point to set up a primality test. One of its core elements, the following thesis, is a central element of this work:

> It is advantageous to use the *commutator curve* in the two-dimensional special linear group for a compositeness test.

This new compositeness test is constructed in a more simple way than that of J. Grantham [**52**]. It requires just one scalar parameter; furthermore, the fixed number of trial divisions has been reduced considerably. The reason for this is that only prime numbers up to 80 have to be tested, compared with up to $50,000$ which was the case beforehand. Additionally, it is in many ways expandable.

The thesis is overall organized in six chapters and three appendices. The theoretical basis of the work will be laid in Chapter 2. There, I will list the fundamental mathematical preliminaries. Chapter 3 will give a summary and survey of all important researches and results that have come up during the 25 years since Miller. I will comment each of them and show their pros and cons. After the known theoretical foundations are laid, Chapter 4 will start with my own research. I introduce commutator curves in the two-dimensional special linear group, and I will show their usefulness for a primality test. Having this results, the commutator curves will be used in a new compositeness test. This is subject of Chapter 5. Finally, in Chapter 6, I will go back to Miller's Test. Here, I will discuss the necessity of the Extended Riemann Hypothesis.

The main results of this work can be summarized in the following items:

(1) In Chapter 4, I will introduce the *commutator curve* which is described by one scalar parameter in the two-dimensional special linear group, and I will build the theoretical basis which will be used for a primality test in further working. In the sections following up to that, I will elaborate all possible orders of the elements, and their frequency on the curve. The definite distribution of the element's orders on this curve will first be analysed modulo a prime power in Theorem 4.32 and then modulo a composite number in Theorem 4.35 and Theorem 4.36. In Lemma 4.40, we will see that there exists an order-preserving bijection between a part of the cummutator curve modulo a prime number p and a subgroup of $\mathbb{F}_p^*$. The remaining part of this curve can be mapped bijectively and order-preserving onto a subset of $\mathbb{F}_{p^2}^*$. This will be shown in Lemma 4.42.
(2) In Section 7 of Chapter 4, I elaborate recursive formulas, and in Theorem 4.61 I will show a connection to Lucas' sequences. This will make possible a fast calculation of order of an element on the commutator curve. In the last Section 8, I will evaltuate seven variants of calculating the order of an element on this curve. They will theoretically be considered according to their best-case, worst-case and average-case running times with regard to Miller's test. We will see that the fastest variant is based on a Lucas sequence. It needs three times the running time of the exponentiation modulo a natural number.
(3) Then, in Theorem 4.53 of Chapter 4, I prove a criterion for a commutator curve over a prime number p, which is analogous to Euler's criterion for $\mathbb{F}_p^*$; this criterion is the basic aid for the later introduced and discussed commutator curve test.
(4) I will consider *LN-numbers* anologous to the Carmichael numbers. The numbers are defined in such a way that their properties are analogous to the Carmichael numbers. Finally, in Corollary 4.48 of Chapter 4, I prove that such numbers cannot exist.
(5) In Chapter 5, the commutator curve will be included into different composite tests. First, I will formulate two simple tests that are analogous to Fermat's and Euler's tests (Algorithm 5.1 und Algorithm 5.2). In addition, I will prove in Theorem 5.10 that this commutator test, that is based on Euler's criterion, can be used as reliable primality test. The most important commutator test is the *Commutator Curve Test*. In Theorem 5.28, I prove that this test, after a

fixed number of trial divisions (all prime numbers up to 80), returns the result "true" for a composite number with a probability less than $\frac{1}{16}$; this means that this test gives the result "true" for a composite number with a probability less than $\frac{1}{16^k}$, if k bases are chosen randomly and independently.

(6) At the end of Chapter 5, I will introduce a new *Hypothetical Commutator Curve Primality Test*, that is based on the commutatuor curve test. This test is fast and – at least for all numbers up to 10^7 (Theorem 5.31) – reliable.
(7) In Chapter 6, I will make a new proof for the correctness of Miller's test. I will check every part of this proof that depends on the Extended Riemann Hypothesis being true; in addition, I will discuss alternative ways of proof. Finally, I can reduce the necessity of the Extended Riemann Hypothesis for the proof of Miller's primality test to a single key Lemma 6.38. In addition, I show in Theorem 6.7 that Miller's test to check a number n, only has to be carried out for all prime bases less than $\frac{3}{2}\ln(n)^2$. This happens under the assumption that the Extended Riemann Hypothesis is true.

The three appendices have the following contents:

(1) Appendix A gives an upper bound for the least quadratic non-residue and is used in Chapter 6.
(2) Appendix B consists of tables which serve as a basis for observations and conjectures in this thesis.
(3) Appendix C offers five different implementations and comparisons of running times of my *Hypothetical Commutator Curve Primality Test*.

CHAPTER 2

Mathematical Preliminaries

1. Symbols and Notations

The following symbols are used in this thesis:

$\mathbb{N}$	the set of the natural numbers $\{0, 1, 2, \dots\}$
$\mathbb{N}_{>0}$	the set of the positive integers $\mathbb{N} - \{0\}$
$\mathbb{Z}$	the set of the integers
$\mathbb{Q}$	the set of the rational numbers
$\mathbb{P}$	the set of the prime numbers
$\mathbb{Z}/n\mathbb{Z}$	the commutative ring of integers modulo n, $\{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$
R^*	if R is a ring then R^* denotes the group of units of R
$\mathbb{F}_p$	the finite field of p elements, where p is a prime number
$\mathbb{R}$	the set of the real numbers
$\mathbb{R}_{>0}$	the set of the positive real numbers $\{x \in \mathbb{R} \mid x > 0\}$
$]a, b[$	an open interval $\{x \in \mathbb{R} \mid a < x < b\}$ with $a, b \in \mathbb{Q}$
$[a, b]$	a closed interval $\{x \in \mathbb{R} \mid a \leq x \leq b\}$ with $a, b \in \mathbb{Q}$
$\mathbb{C}$	the set of the complex numbers
$\mathrm{Re}(s)$	the real part of a complex number s
$\mathrm{Im}(s)$	the imaginary part of a complex number s
$\mathrm{Res}_a f$	the residue at $a \in \mathbb{C}$ of the meromorphic function f
$\gcd(a, b)$	the greatest common divisor of a, and b
$\mathrm{lcm}(a, b)$	the least common multiple of a, and b
δ_{mn}	Kronecker's symbol $\delta_{mn} := \begin{cases} 1\,, & \text{if } m = n \\ 0\,, & \text{else} \end{cases}$
I_m	the $m \times m$ identity matrix
$\det(A)$	the determinant of the matrix A
e^x	the exponential function of indeterminate x
$\ln(n)$	the natural logarithm
$\log(n)$	the logarithm to an unspecified base
γ	Euler's constant $\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \ln(n)\right)$
$\Gamma(s)$	the gamma function for complex numbers s, $\Gamma(s) := \lim_{n\to\infty} \frac{n!\, n^s}{\prod_{k=0}^{n}(s+k)}$

2. Number-Theoretic Functions

DEFINITION 2.1. We will use the following number-theoretic functions in this thesis:

ν_p : $\mathbb{N}_{>0} \to \mathbb{N} : n \mapsto \max\{k \in \mathbb{N} \mid p^k \mid n\}$
is the maximal power of $p \in \mathbb{P}$ in n.

φ : $\mathbb{N}_{>0} \to \mathbb{N} : n \mapsto |\{k \in \mathbb{N}_{>0} \mid k \leq n, \gcd(k,n) = 1\}|$
is the number of positive integers less than or equal to n relatively prime to n.

π : $\mathbb{N}_{>0} \to \mathbb{N} : n \mapsto |\{k \in \mathbb{P} \mid k < n\}|$
is the number of primes less than n.

THEOREM 2.2. *Let n be a positive integer with prime factorization $n = \prod_{k=1}^{r} p_k^{e_k}$. Then we have*

$$\varphi(n) = \prod_{k=1}^{r} p_k^{e_k-1}(p_k - 1) = n \prod_{k=1}^{r}(1 - p_k^{-1}).$$

PROOF. This theorem is well known in Number Theory; for a proof we refer for example to Satz 6.8 in [**43**] on page 51. □

THEOREM 2.3. *Let p be an odd prime number. Then*

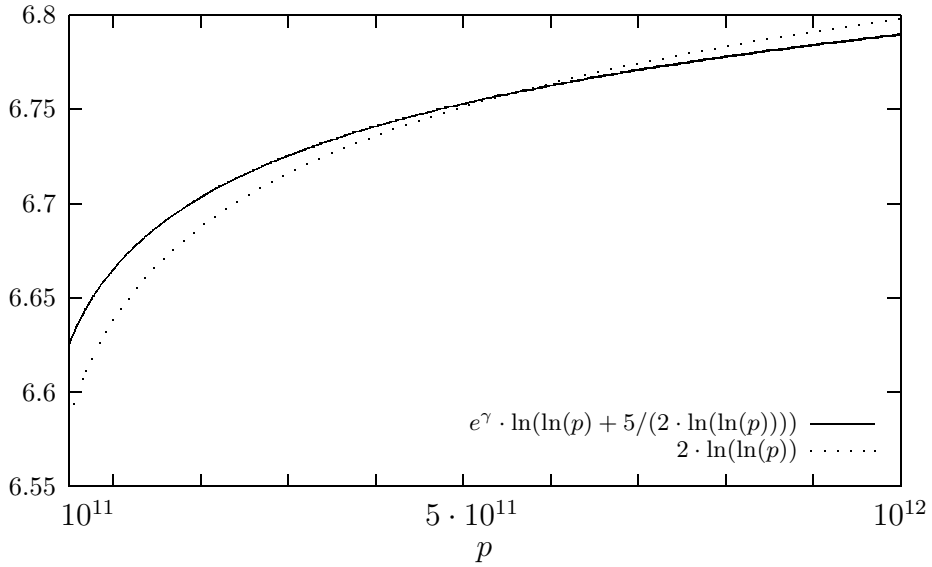
$$\frac{p-1}{\varphi(p-1)} < e^{\gamma} \ln(\ln(p)) + \frac{5}{2\ln(\ln(p))}.$$

PROOF. We refer to Theorem 15 in [**112**] on page 72 for a proof. □

COROLLARY 2.4. *Let p be a prime number greater than* 200 560 490 131. *Then*

$$\frac{p-1}{\varphi(p-1)} < 2\ln(\ln(p)).$$

PROOF. Consider the following diagram:



Then we see that the images of the function $p \mapsto 2\ln(\ln(p))$ are greater than the images of the function $p \mapsto e^{\gamma}\ln(\ln(p)) + \frac{5}{2\ln(\ln(p))}$ for $p > 6 \cdot 10^{11}$. Therefore, the assertion for $p > 6 \cdot 10^{11}$ follows by Theorem 2.3 and for $p < 6 \cdot 10^{11}$ by computation. □

3. The Chinese Remainder Theorem

THEOREM 2.5. *Let m be a natural number with coprime factorization $\prod_{k=1}^{r} m_k$ such that $\gcd(m_k, m_l) = 1$ for all $1 \leq k, l \leq r, k \neq l$, and let b_k be integers for $1 \leq k \leq r$. Then the system*

$$x \equiv b_k \pmod{m_k} \qquad \text{for all } 1 \leq k \leq r$$

is solvable and has a unique solution modulo m.

PROOF. This theorem is well known in Number Theory; for a proof we refer to Satz 6.6 in [**43**] on pages 47-48. □

4. The Legendre-Jacobi Symbol

First of all we define in this section a special symbol, called the *Legendre symbol*. This symbol is essentially a homomorphism from $(\mathbb{Z}/p\mathbb{Z})^*$ to $\{-1, 1\}$, where p is an odd prime number.

DEFINITION 2.6. Let p be an odd prime number, and let a be an integer. Then we denote by $\left(\frac{a}{p}\right)$ the *Legendre symbol*

$$\left(\frac{a}{p}\right) := \begin{cases} 0\,, & \text{if } a \mid p \\ 1\,, & \text{if } a \equiv x^2 \pmod{p} \text{ for some } x \in \mathbb{Z} \\ -1\,, & \text{else.} \end{cases}$$

C. G. J. Jacobi generalized the domain of the Legendre symbol to odd numbers, but not necessarily to odd prime numbers. This symbol, called the *Jacobi symbol*, is also written such as the Legendre symbol.

DEFINITION 2.7. Let n be an odd integer with prime factorization $\prod_{k=1}^{r} p_k$, and let a be an integer. We denote by $\left(\frac{a}{n}\right)$ the *Jacobi symbol*

$$\left(\frac{a}{n}\right) := \prod_{k=1}^{r} \left(\frac{a}{p_k}\right),$$

where $\left(\frac{a}{p_k}\right)$ denotes the corresponding Legendre symbol.

Jacobi's generalization has the virtue of being multiplicative and it is the same as the Legendre symbol if n is an odd prime number.

In the following theorem we collect some important properties of the Jacobi symbol, including the Law of Quadratic Reciprocity.

THEOREM 2.8. *Let a, b be integers, and let m, n be odd positive integers. Then the following equations are valid:*

$$\begin{aligned}\left(\frac{ab}{m}\right) &= \left(\frac{a}{m}\right)\left(\frac{b}{m}\right),\\ \left(\frac{a}{mn}\right) &= \left(\frac{a}{m}\right)\left(\frac{a}{n}\right),\\ \left(\frac{2}{m}\right) &= (-1)^{\frac{m^2-1}{8}},\\ \left(\frac{m}{n}\right) &= (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{m}\right).\end{aligned}$$

PROOF. We refer to [**61**] on pages 50-61 for a proof. □

5. Euler's Criterion for Quadratic Residues

THEOREM 2.9 (Euler). *Let p be an odd prime number. Then we have for every integer a*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

PROOF. This theorem is well known in Number Theory; for a proof we refer to Satz 11.1 in [**43**] on page 86. □

6. The Order of a Group Element

DEFINITION 2.10. Let a be an element of a multiplicatively written finite group $(G, \cdot)$. The *order* of a, denoted by $\mathrm{ord}(a)$, is the least positive integer b such that $a^b = 1$, where 1 is the neutral element of G:

$$\mathrm{ord} : G \to \mathbb{N}_{>0} : a \mapsto \min\{b \in \mathbb{N}_{>0} \mid a^b = 1\}.$$

If n is a natural number with $|G| = n$, and if $a \in G$ is an element of order n, then G is said to be *cyclic* and a is called a *generator* or a *primitive element* of G.
Let n be a natural number. Assume a can be considered modulo n. Then we define

$$\mathrm{ord}_n(a) := \mathrm{ord}(a \bmod n).$$

The following result is due to Lagrange and is the base for many useful theorems in number theory.

THEOREM 2.11 (Lagrange). *The order of an element divides the cardinality of the group.*

PROOF. This theorem is well known in Number Theory; for a proof we refer to Satz 7.1 in [**43**] on page 54. □

7. Irreducible Polynomials over $\mathbb{F}_p$

Let p be a prime number. Then a polynomial $f(x) \in \mathbb{F}_p[x]$ of degree $n \geq 1$ is said to be *irreducible over* $\mathbb{F}_p$ if it cannot be written as a product of two polynomials in $\mathbb{F}_p[x]$ each having a degree less than n. Such a polynomial $f(x)$ can be used to represent the elements of the finite field $\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$, the set $\{g(x) + f(x)\mathbb{Z} \mid g(x) \in \mathbb{F}_p[x]\}$, where the addition and multiplication of polynomials is performed modulo $f(x)$. In this thesis we will use the following polynomials:

DEFINITION 2.12. Let n be a natural number, and let p be a prime number. Let $\mathbb{F}_{p^n}$ be a finite field, and let $\alpha \in \mathbb{F}_{p^n}$. The *minimal polynomial* of α over $\mathbb{F}_p$ is the monic polynomial of least degree in $\mathbb{F}_p[x]$ having α as a root.

THEOREM 2.13. *Let n be a natural number, and let p be a prime number. Let $\mathbb{F}_{p^n}$ be a finite field, and let $\alpha \in \mathbb{F}_{p^n}$. Then*

1. *The minimal polynomial of α over $\mathbb{F}_p$, denoted by $m_\alpha(x)$, is unique.*
2. *The polynomial $m_\alpha(x)$ is irreducible over $\mathbb{F}_p$.*
3. *The leading coefficient of $m_\alpha(x)$ is 1.*
4. *The degree of $m_\alpha(x)$ is a divisor of n.*

PROOF. We refer to [**42**] on pages 128-130 for a proof. □

8. Commutators

DEFINITION 2.14. Let a, b be two elements of a group $(G, \cdot)$. Then the *commutator* of a, and b is defined by

$$a^{-1}b^{-1}ab.$$

The commutator is the element that commutes the two elements a, and b in group G by multiplication:

$$ab = ba(a^{-1}b^{-1}ab).$$

DEFINITION 2.15. Let G be a group. The *commutator group* G' is the group which is generated by all commutators:

$$G' := \langle a^{-1}b^{-1}ab \mid a, b \in G \rangle.$$

A group G is called *perfect*, if $G = G'$. G is commutative if and only if $G' = 1$, where 1 is the neutral element of G.

9. Linear Groups

In this thesis, we are especially interested in the following two linear groups:

DEFINITION 2.16. Let m be a positive integer, and p be a prime number. We denote by

$$GL_m(p) := \{A \in \mathbb{F}_p^{m\times m} \mid \det(A) \neq 0\}$$

the *general linear group* and by

$$SL_m(p) := \{A \in \mathbb{F}_p^{m\times m} \mid \det(A) = 1\}$$

the *special linear group.*
We define by I_m the $m \times m$ *identity matrix*:

$$I_m := (\delta_{kl})_{1\leq k,l\leq m},$$

where $\delta_{kl} := \begin{cases} 1\,, & \text{if } k = l \\ 0\,, & \text{else} \end{cases}$ is the Kronecker symbol.

The set $GL_m(p)$ of all invertible matrices of degree m over the finite field $\mathbb{F}_p$ is a group under the usual multiplication of matrices. It is called the general linear group of degree m over the finite field $\mathbb{F}_p$. Obviously, $GL_m(p)$ is just $M_m(p)^*$, where $M_m(p)$ is the ring of all matrices of degree m over the finite field $\mathbb{F}_p$. For $m \geq 2$, the group $GL_m(p)$ is non-commutative. Very important in this thesis is the normal subgroup $SL_m(p)$ of $GL_m(p)$ consisting of all matrices with determinant 1, which is called the special linear group. Especially we concentrate on the two-dimensional special linear group over finite fields which offers many useful properties for a primality test. An important work about these groups is [**37**] by L. E. Dickson.

We now introduce some fundamental theorems of groups of matrices over finite fields, which we will use later for the primality test.

THEOREM 2.17. *Let m be a positive integer, and p be a prime number. Then*

$$|GL_m(p)| = p^{\frac{m(m-1)}{2}} \prod_{k=1}^{m}(p^k - 1),$$

and

$$|SL_m(p)| = p^{\frac{m(m-1)}{2}} \prod_{k=2}^{m}(p^k - 1).$$

PROOF. We refer to (9.11) in [**124**] on page 81 for a proof. □

DEFINITION 2.18. Let m be a positive integer, p be a prime number, and $M \in \mathbb{F}_p^{m\times m}$ a $m \times m$ matrix over $\mathbb{F}_p$, then we define the *characteristic polynomial* as follows:

$$\chi_M(x) := det(xI_m - M),$$

with indeterminate x.

THEOREM 2.19. *Let m be a positive integer, p be a prime number, $M \in GL_m(p)$, and χ_M irreducible. Then*

$$\text{ord}(M) \mid p^m - 1,$$

and

$$\text{ord}(M) \nmid p^k - 1 \qquad \textit{for all } k,\ 1 \leq k < m.$$

PROOF. We refer to 7.3 in [**57**] on page 187 for a proof. □

Previously, we have seen many useful properties for the m-dimensional linear groups. But in this thesis we will reduce our focus on the two-dimensional special linear group in view of a primality testing algorithm where especially the following theorem of L. E. Dickson is fundamental:

THEOREM 2.20 (Dickson). *Let p be an odd prime number, and $a \in \mathbb{F}_p^*$ with $\langle a \rangle = \mathbb{F}_p^*$. Then we have*

$$\langle \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle = SL_2(p).$$

PROOF. We refer to Theorem 8.4 in [**48**] on page 44 for a proof. □

THEOREM 2.21. *Let p be an odd prime number. Then $SL_2(p)$ contains cyclic subgroups of order $p-1$ and $p+1$.*

PROOF. We refer to Theorem 8.3 in [**48**] on page 42 for a proof. □

We will discuss these two theorems more detailed in Chapter 4.

Moreover, we need an extended definition of the two-dimensional special linear group for the commutative ring $\mathbb{Z}/n\mathbb{Z}$, where n is a positive integer, to use this group for a primality test on n.

DEFINITION 2.22. Let m, and n be positive integers, and

$$A = (a_{kl})_{1 \leq k,l \leq m}, \quad \text{and} \quad B = (b_{kl})_{1 \leq k,l \leq m}$$

be $m \times m$ matrices over integers. Then we denote by

$$A \equiv B \pmod{n},$$

if $a_{kl} \equiv b_{kl} \pmod{n}$ for all $1 \leq k, l \leq m$.

Different from usual notation in group theory

$$SL_2(p^k) := \{A \in \mathbb{F}_{p^k}^{2\times 2} \mid \det(A) = 1\},$$

where p is a prime number, and k is a positive integer, the following definition is introduced for $SL_2(n)$, because in this thesis that group is only needed for the base of a primality test on n, where n is a positive integer.

DEFINITION 2.23. Let n be a positive integer. We denote by

$$GL_2(n) := \{A \in (\mathbb{Z}/n\mathbb{Z})^{2\times 2} \mid \det(A) \neq 0\}$$

the *two-dimensional general linear group* and by

$$SL_2(n) := \{A \in (\mathbb{Z}/n\mathbb{Z})^{2\times 2} \mid \det(A) = 1\}$$

the *two-dimensional special linear group*.

CHAPTER 3

Primality Testing

1. Introduction

One very important concern in number theory is to establish whether a given number n is prime or composite. At first sight the decision might seem to have the same order as factoring n. But factoring is not feasible in general if the length of n exceeds for example 200 decimal digits – in August 1999, the record in solving this task is the factorization of the 512-bit RSA-155 key using the Number Field Sieve by H. J. J. te Riele et al. [**109**], a number that can be written as the product of two 78 digit primes.
Until the work of É. Lucas in 1876, however, the problems of primality testing and factorizing were not considered separately. Although Fermat's theorem had been known since 1640, Lucas in 1876 (see [**138**], p. 53ff) seems to have been the first to recognize that this theorem could be useful in determining whether a number is composite. Several investigators, particularly M. Kraitchik and D. H. Lehmer in the 1920's, refound Lucas' work and tested the primality of many large numbers. Nevertheless, they are often applicable only to numbers n of a certain form, such as $n = 2^k \pm 1$. Indeed, particularly for *Mersenne numbers* $M_k = 2^k - 1$, an efficient method has been known since Lucas, and in June 1999 the largest prime is the 38th known Mersenne prime $M_{6972593}$, a number with more than 2 million decimal digits (see [**45**]).
In this chapter, we are not interested in primality tests for numbers of a certain form. A general-purpose primality test is of course not as fast as the special test designed for Mersenne primes, but we can test integers with many thousands of decimal digits.

2. Compositeness Tests

In this section, we shall discuss numerous tests which are mathematically simple and computationally fast. A primality test has generally the following form: If certain conditions on a number n are satisfied then n is a prime number, otherwise n is a composite number. Conversely, the following definition is possible:

DEFINITION 3.1. Let n be a natural number. We call a test a *compositeness test* which has the following form: If certain conditions on n are satisfied then n is a composite number, otherwise n is a prime number or in rare occasions a composite number. We denote such a rare occasion as a failure and call n in that case a *pseudoprime*, because n satisfies the conditions of the test like a prime.

These compositeness tests may have as a result that a composite number is being indicated as a prime (if the test fails), but never vice versa. Furthermore, they return the

correct result only with high probability and not with certainty. Briefly, if a compositeness test is performed on n, and the condition for being composite is not satisfied, then primality of n is not necessarily proved.

2.1. The Converse of Fermat's Theorem. Fermat's (little) theorem is the base for most efficient primality and compositeness tests.

THEOREM 3.2 (Fermat). *Let p be a prime number. Then we have for all $a \in \mathbb{F}_p^*$*

$$a^{p-1} \equiv 1 \pmod{p}.$$

PROOF. Let $a \in \mathbb{F}_p^*$. By Theorem 2.11, there exists a natural number b such that $b \cdot \operatorname{ord}(a) = |\mathbb{F}_p^*| = p - 1$. Then $a^{p-1} = (a^{\operatorname{ord}(a)})^b \equiv 1^b = 1 \pmod{p}$. □

Thus, if Theorem 3.2 is not satisfied for some integer n, and some a relatively prime to n, then n is successfully proved composite. Unfortunately, Fermat's theorem could not be used as a primality test, because there exist certain combinations of a and composite n for which $a^{n-1} \equiv 1 \pmod{n}$, and these values of n are thus not revealed as composite by this criterion. For example $n = 341 = 11 \cdot 31$ is the smallest composite number n with

$$2^{n-1} \equiv 1 \pmod{n}.$$

It can be observed that such numbers are rare; there are exactly 264 239 pseudoprimes for the base 2 up to 10^{13} (see [**99**]). This number is very small compared to the number of primes $\pi(10^{13}) = 346\,065\,536\,839$ (see [**14**] on page 300). Thus, if a randomly chosen number n satisfies the condtion $a^{n-1} \equiv 1 \pmod{n}$ for a base a then it is very likely that n is prime.

DEFINITION 3.3. Let n be a natural number greater than 2. We denote by $F(n)$ the set

$$F(n) := \{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a^{n-1} \equiv 1 \pmod{n}\}.$$

The algorithm for Fermat's test is very simple:

ALGORITHM 3.4 (Fermat Test).

Input: *$n \in \mathbb{N}$, and $a \in \mathbb{N}$ with $1 < a < n$.*
Output: *$R \in \{\text{true}, \text{false}\}$.*

(1) If $a^{n-1} \not\equiv 1 \pmod{n}$, then terminate with the result false*, otherwise terminate with the result* true*.*

The result of the Fermat test is always true for prime numbers, since $F(p) = \mathbb{F}_p^*$ for $p \in \mathbb{P}$.

THEOREM 3.5. *Let n be a natural number with prime factorization $n = \prod_{k=1}^{r} p_k^{e_k}$. Then we have*

$$|F(n)| = \prod_{k=1}^{r} \gcd(n-1, p_k - 1).$$

PROOF. We refer to Theorem 1 in [**16**] for a proof. □

2.2. Carmichael Numbers. Unfortunately, there exist composite numbers n such that $F(n)$ is equal to $(\mathbb{Z}/n\mathbb{Z})^*$; as a result, n is a pseudoprime to all bases relatively prime to it. Such a number can never be proved to be composite by using Fermat's Theorem 3.2 and is called a *Carmichael number* (see [**30**]). The following theorem gives a characterization of Carmichael numbers.

THEOREM 3.6 ([**30**]). *A composite number n is a Carmichael number if and only if $\lambda(n) \mid n-1$.*
The function $\lambda(n)$ is defined as follows:

(1) $\lambda(1) = 1$;
(2) $\lambda(p^e) = p^{e-1}(p-1)$, *if p is an odd prime;*
(3) $\lambda(2) = 1, \lambda(4) = 2, \lambda(2^e) = 2^{e-2}$ *for $e \geq 3$;*
(4) *if $n = \prod_{k=1}^{r} p_k^{e_k}$, then $\lambda(n) = \operatorname{lcm}(\lambda(p_k^{e_k}))_{k=1}^{r}$.*

The smallest Carmichael number is $561 = 3 \cdot 11 \cdot 17$, and there are only 246 683 Carmichael numbers smaller than 10^{16} (see [**100**], and [**101**]). This number is also very small compared to $\pi(10^{16}) = 279\ 238\ 341\ 033\ 925$ (see [**14**] on page 300). However, it is shown in [**5**] that there are infinitely many Carmichael numbers. Therefore, Fermat's test should not be used as a compositeness test.

2.3. The Solovay-Strassen Test. According to Euler's criterion for quadratic residues, we have

$$a^{\frac{n-1}{2}} \equiv \left(\tfrac{a}{n}\right) \pmod{n},$$

if n is an odd prime, and a is relatively prime to n. We refer to Theorem 82 in [**56**] on page 69 for a proof.

DEFINITION 3.7. Let n be a natural number greater than 2. We denote by $E(n)$ the set of bases a that satisfy Euler's criterion

$$E(n) := \{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a^{\frac{n-1}{2}} \equiv \left(\tfrac{a}{n}\right) \pmod{n}\}.$$

In 1974 R. Solovay and V. Strassen [**120**] have given a probabilistic algorithm based on this equation for compositeness proving that it has expected polynomial time.

ALGORITHM 3.8 (Solovay-Strassen Test).
Input: $n \in \mathbb{N}$, *and* $a \in \mathbb{N}$ *with* $1 < a < n$.
Output: $R \in \{\text{true}, \text{false}\}$.

(1) If $a^{\frac{n-1}{2}} \not\equiv \left(\tfrac{a}{n}\right) \pmod{n}$, *then terminate with the result* false, *otherwise terminate with the result* true.

Like for the Fermat test, compositeness of a number n can be proved with certainty, but a proof of primality cannot be obtained from the Solovay-Strassen test, because for example the Carmichael number $n = 561 = 3 \cdot 11 \cdot 17$ and the base $a = 2$ satisfy Euler's criterion.
Since the Jacobi symbol is only ± 1 for a base a relatively prime to n, we see that $E(n) \subseteq F(n)$. However, the Solovay-Strassen test can recognize composite numbers that

cannot be recognized as composite by the Fermat test, e.g. the Carmichael number 561 does not satisfy Euler's criterion for the base 5. Furthermore, the following theorem shows that no composite number can satisfy Euler's criterion for all bases.

THEOREM 3.9 ([**120**]). *Let n be an odd composite number greater than 2. Then $E(n)$ is a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$, and*

$$|E(n)| \leq \tfrac{1}{2}\varphi(n).$$

This Theorem 3.9 gives rise to the first compositeness test, which is probabilistic in nature: for 50 randomly chosen values of a, which are tested true by Algorithm 3.8. If it is not true for any value of a, then n is composite. If it is true for all 50 values, then we say that n is probably prime, with probability of error less than $2^{-50} \approx 10^{-15}$.

2.4. The Miller-Rabin Test. The idea of using Euler's criterion instead of Fermat's Theorem 3.2 to distinguish between primes and composites, can be carried a little further, if $n \equiv 1 \pmod 4$.

DEFINITION 3.10. Let n be a natural number greater than 2. We denote by $S(n)$ the set of bases a for which n is a *strong pseudoprime*

$$\begin{aligned} S(n) := \{a \in (\mathbb{Z}/n\mathbb{Z})^* \quad | \quad & b = \nu_2(n-1), a^{(n-1)\cdot 2^{-b}} \equiv 1 \pmod n \\ & \text{or } a^{(n-1)\cdot 2^{c-b}} \equiv -1 \pmod n \text{ for some } 0 \leq c < b\}. \end{aligned}$$

This concept was introduced by J. Selfridge using the following algorithm in 1974.

ALGORITHM 3.11 (Miller-Rabin Test).
Input: $n \in \mathbb{N}$, *and* $a \in \mathbb{N}$ *with* $1 < a < n$.
Output: $R \in \{\text{true}, \text{false}\}$.

(1) Set $b := \nu_2(n-1)$, *and* $m := \frac{n-1}{2^b}$.
(2) If $a^m \not\equiv 1 \pmod n$, *and there exists* $0 \leq c < b$ *with* $a^{m2^c} \not\equiv -1 \pmod n$, *then terminate with the result* false, *otherwise terminate with the result* true.

A variant of this test was first published by G. L. Miller in [**86**] as a non-probabilistic polynomial-time algorithm assuming the correctness of the Extended Riemann Hypothesis[1]. Four years later, a practical probabilistic variant of this test was independently shown by M. O. Rabin in [**106**] and L. Monier in [**87**], which has two advantages to the Solovay-Strassen test. Firstly, it does not require any computation of the Jacobi symbol. Secondly, we will show in Theorem 3.12 that $|S(n)|$ is smaller than $|E(n)|$, hence fewer trials have to be made to ensure a given probability. Rabin's original algorithm requires a small number of gcd computations. A simplification of his algorithm, which does not require any gcd computation and which is due to D. E. Knuth [**66**] on page 395, is now often called the Miller-Rabin test.

[1]For more details see Chapter 6.

THEOREM 3.12 ([**106**]). *Let n be an odd composite number greater than 9. Then $S(n)$ is a subset of $E(n)$, and*

$$|S(n)| \leq \tfrac{1}{4}\varphi(n).$$

By this Theorem 3.12, we see that if a base a satisfies the Miller-Rabin test, then it will also satisfy the Solovay-Strassen test, so the Miller-Rabin test completely supersedes the Solovay-Strassen test.
Likewise, for the Solovay-Strassen test, compositeness of a number n can be proved with certainty, but a proof of primality cannot be obtained from the Miller-Rabin test, e.g. $n = 2047 = 23 \cdot 89$ is the smallest number which is a strong pseudoprime to the base 2. There exists many numbers like

$$\begin{aligned} 8911 &= 7 \cdot 19 \cdot 67 && \text{(see [\textbf{108}] on page 123)} \\ 2000436751 &= 481 \cdot 1531 \cdot 2683 && \text{(see [\textbf{106}])} \\ \text{and}\quad 4987757503 &= 49939 \cdot 99877 && \text{(see [\textbf{66}] on page 662)} \end{aligned}$$

which show that the estimate of Theorem 3.12 cannot be improved in general. But the Algorithm 3.11 was carefully analysed by [**17**], [**35**], and [**65**].

2.5. Lucas-based Tests. In this section we briefly define a generalized version of the well-known Fibonacci sequence, and show a connection between these sequences and the compositeness tests. For more details we refer to H. C. Williams ([**138**], chapter 4). Let D, P, and Q be integers such that $D = P^2 - 4Q \neq 0$ and $P > 0$. The Lucas sequences $\{U_k(P,Q)\}_{k\in\mathbb{N}}$, and $\{V_k(P,Q)\}_{k\in\mathbb{N}}$ are defined recursively as follows

$$\begin{aligned} U_0(P,Q) &= 0, \\ V_0(P,Q) &= 2, \\ U_1(P,Q) &= 1, \\ V_1(P,Q) &= P, \\ U_{k+2}(P,Q) &= PU_{k+1}(P,Q) - QU_k(P,Q), \\ V_{k+2}(P,Q) &= PV_{k+1}(P,Q) - QV_k(P,Q) \quad \text{for } k \in \mathbb{N}. \end{aligned}$$

Fermat's Theorem 3.2 has an analogue for Lucas sequences:

THEOREM 3.13 ([**78**]). *If p is an odd prime number, where $p \nmid Q$, and $\left(\frac{D}{p}\right) = -1$, then*

$$p \mid U_{p+1}(P,Q).$$

Thus if Theorem 3.13 is not satisfied for some odd integer n such that $n \nmid Q$, and $\left(\frac{D}{n}\right) = -1$, then n is successfully proved composite. An odd composite number n, which satisfies $n \mid U_{n+1}(P,Q)$ with $n \nmid Q$, and $\left(\frac{D}{n}\right) = -1$, is called a *Lucas pseudoprime* with parameter P, and Q.
Like Euler's criterion and strong pseudoprimes, we can make the analogous definitions for Lucas' sequences. For more details we refer to [**16**]. More interesting for us is that P. Erdös, P. Kiss, A. Sárközy [**40**] and D. M. Gordon, C. Pomerance [**47**] have shown that the distribution of the Lucas pseudoprimes is hardly different from that of the ordinary pseudoprimes. This suggests that it is likely to be of little advantage for a compositeness

test using Lucas sequences on a number which is prime or a ordinary pseudoprime. In the next subsection we will give the first test which combine Fermat's test and Lucas sequences.

2.6. The Baillie - PSW Primality Test. In 1980, R. Baillie, C. Pomerance, J. L. Selfridge and S. S. Wagstaff, Jr., proposed a test, based on a combination of the Miller-Rabin test and a Lucas-based test, that seems very powerful ([**16**],[**104**]). Indeed, nobody has yet claimed the $620 that they offer for a counter-example that passes it, or a proof that no such number exists. It is known (see chapter 8 in [**23**]) that this algorithm is correct for all numbers n less than 10^{16}. But it is considered very likely that such a counter-example exist, which has shown by C. Pomerance in [**103**] using heuristic arguments.

Algorithm 3.14.
Input: $n \in \mathbb{N}$.
Output: $R \in \{\text{true}, \text{false}\}$.

(1) *If* $2^{n-1} \not\equiv 1 \pmod{n}$, *then terminate with the result* false.
(2) *Find the number* $D := (-1)^m(2m+5)$, *where* $m = \min\{k \in \mathbb{N} \mid \left(\frac{(-1)^k(2k+5)}{n}\right) = -1\}$.
(3) *If* $n \nmid U_{n+1}(1, \frac{1-D}{4})$, *then terminate with the result* false, *otherwise terminate with the result* true.

The success of this test suggests that it is possible to construct a test that is, in some sense, stronger than the Miller-Rabin test. R. Baillie prefers to find the number

$$D := \min\{4k+5 \mid k \in \mathbb{N}, \left(\tfrac{4k+5}{n}\right) = -1\}$$

in step (2) of Algorithm 3.14. References which discuss this primality test more detailed are for example [**90**], and [**91**]. Recently, A. O. L. Atkin [**9**] has even offered a prize of $2500 to the first person who can exhibit a composite number n which satisfies simultaneously a sequence of conditions involving three different compositeness criteria.

2.7. Grantham's Probable Primality Test. J. Grantham modified the "Baillie - PSW" primality test in such a way that he can give a concrete estimate of the probability that a composite number passes the test with the incorrect result true. Instead of Lucas' recurrence sequences, he computed in finite fields.

Algorithm 3.15.
Input: $n \in \mathbb{N}$, *where* $n > 2$ *and* $2 \nmid n$.
Output: $R \in \{\text{true}, \text{false}\}$.

(1) *If a prime number less than* 50 000 *divides* n, *then terminate with the result* false.
(2) *If* $\sqrt{n} \in \mathbb{Z}$, *then terminate with the result* false.
(3) *Choose* $a, b \in \mathbb{Z}/n\mathbb{Z}$ *such that*

$$\left(\tfrac{a^2-4b}{n}\right) = -1 \qquad \textit{and} \qquad \left(\tfrac{b}{n}\right) = 1.$$

(4) *Define the polynomial* $p(x) := x^2 - ax + b \in (\mathbb{Z}/n\mathbb{Z})[x]$ *and* $q(x) \equiv x^{\frac{n+1}{2}} \pmod{p(x)}$.
(5) *If* $q(x) \notin \mathbb{Z}/n\mathbb{Z}$ *or* $q(x)^2 \not\equiv b \pmod{p(x)}$, *then terminate with the result* false.

(6) *Let* $n^2-1=2^r s$, *where* s *is odd. If* $x^s \not\equiv 1 \pmod{p(x)}$ *and* $x^{2^k s} \not\equiv -1 \pmod{p(x)}$ *for all* $0 \le k \le r-2$, *then terminate with the result* false, *otherwise terminate with the result* true.

THEOREM 3.16 ([**52**]). *Let* p *be a prime number, and* n *be an odd composite number. The result of Algorithm 3.15 is always* true *for* p. *The probability that the Algorithm 3.15 returns the result* true *for* n *is less than* $\frac{1}{7710}$.

3. Primality Tests

The primality tests in this section are methods by which natural numbers n can be proved to be prime. The practical problem of rigorously proving that a number n is prime, is generally more computationally intensive than the compositeness tests of previous Section 2. Consequently, before applying one of these tests to a candidate prime n, the candidate should be subjected to a compositeness test such as the Miller-Rabin Algorithm 3.11.
Of course, Fermat's Theorem 3.2 can be used and simply extended to prove efficiently compositeness of a number n. Unfortunately, as already noted, all these approaches of previous Section 2 suffer from a serious defect: they cannot directly be used to prove the primality of n. In this section we will see that only Miller's compositeness method (Algorithm 3.11) could be used to establish primality in deterministic polynomial running time, but it requires the Extended Riemann Hypothesis which still seems very far from being proved. However, we want to see how successful we will be if we remove the Extended Riemann Hypothesis from Miller's test in Chapter 6.
Briefly, we describe all modern primality tests only as an overview. A few ideas of these tests are also important for Chapter 5.

3.1. Pocklington's Theorem. An appropriate modification of the Fermat Theorem 3.2 can be used to find the properties of all divisors of the number n that has to be tested. If a sufficient number of such properties are known, this can lead to the proof of the primality of n. A theorem towards this goal has been shown by H. C. Pocklington in [**102**] in 1914.

THEOREM 3.17 (Pocklington). *Let* n *be a natural number,* p *be a prime number dividing* $n-1$, *and* a *be relatively prime to* n. *If*

$$a^{n-1} \equiv 1 \pmod{n} \quad \text{and} \quad \gcd(a^{\frac{n-1}{p}} - 1, n) = 1, \tag{1}$$

then every prime divisor q *of* n *satisfies*

$$q \equiv 1 \pmod{p^{\nu_p(n-1)}}.$$

PROOF. Let $d := \operatorname{ord}_q(a)$. By Lagrange's Theorem 2.11, and (1), we have

$$d \mid n-1 \quad \text{and} \quad d \nmid \tfrac{n-1}{p} \quad \text{and} \quad d \mid q-1.$$

Hence,

$$p^{\nu_p(n-1)} \mid d \quad \text{and} \quad d \mid q-1.$$

Thus,

$$p^{\nu_p(n-1)} \mid q-1.$$

Therefore, the proof of the assertion follows by

$$q = m \cdot p^{\nu_p(n-1)} + 1,$$

for a natural number m. □

COROLLARY 3.18 (Pocklington). *Let n be a natural number, and $n = RF + 1$ with prime factorization $F = \prod_{k=1}^{r} p_k^{e_k} > \sqrt{n} - 1$, and $\gcd(F, R) = 1$. If there exists a base a relatively prime to n such that*

$$\begin{aligned} a^{n-1} &\equiv 1 \pmod{n} \\ \text{and} \quad \gcd(a^{\frac{n-1}{p_k}} - 1, n) &= 1 \quad \text{for all } k, 1 \le k \le r, \end{aligned}$$

then n is prime.

PROOF. Assuming n is composite, and let q be the smallest prime factor of n. Then clearly $q \le \sqrt{n}$. By Theorem 3.17, and the Chinese Remainder Theorem 2.5, it follows that $q \equiv 1 \pmod{F}$. But hence $q \ge F + 1 > \sqrt{n}$, we have a contradiction. □

A more elaborated version of Pocklington's Theorem 3.17 is presented in [**24**] by J. Brillhart, D. H. Lehmer and J. L. Selfridge, who show for example, that only a partial factorization $F > \sqrt[3]{n}$ of $n-1$ is needed to prove the primality of n with Pocklington's theorem.
We can also design primality proofs that depend on knowing the factorization of $n+1$, n^2+1, and $n^2 \pm n + 1$ (see [**134**], [**135**]), or also on higher degree finite fields and combine them. Since $|\mathbb{F}_{p^2}^*| = (p-1)(p+1)$, and $|SL_2(p)| = p(p-1)(p+1)$, it seems to be reasonable to carry out the proof using not only $\mathbb{F}_p$, but rather a finite ring or group which is isomorphic to $\mathbb{F}_{p^2}$ or $SL_2(p)$, respectively, if indeed p is prime. We will use a special linear group for a primality test in Chapter 5.

3.2. Modern Primality Tests Using Algebraic Number Theory. Previously, we saw various primality tests and recognized that they require the knowledge of the factorization of $n-1$ (or $n+1$, etc.). Even though only a partial factorization is needed, and combinations of calculating in different finite rings are used, the tests based only on Pocklington's Theorem 3.17 become impractical as soon as n has more than about 100 decimal digits.
A breakthrough with the Jacobi sum test was made in 1980 by L. M. Adleman, C. Pomerance and R. S. Rumely [**3**], who devised an algorithm for primality testing, which has a nearly polynomial running time of $O(\ln(n)^{C \ln(\ln(\ln(n)))})$ for a suitable constant C. The basic idea is to check a set of congruences which are analogous of Fermat's Theorem 3.2 in certain cyclotomic rings. If n is prime, these congruences always will be true. If n is composite, however, these identities are probably not satisfied like in a compositeness test. If, however, all these congruences are verified, then we get some information about the possible divisors of n, like Pocklington's Theorem 3.17. More precisely, the possible divisors of n must fall into a relatively small number of congruence classes, and these

can easily be checked. The following simple example roughly illustrates the flavor of the information obtained. Suppose for some integer a we have $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$. Then we will see by Lemma 5.4, that $\nu_2(p-1) \geq \nu_2(n-1)$ for every prime divisor p of n.
The version of the Jacobi sum primality test used in practice is a randomized algorithm, which terminates within $O(k \ln(n)^{C \ln(\ln(\ln(n)))})$ steps with probability at least $1 - 2^{-k}$, for every $k \in \mathbb{N}_{>0}$, and always gives a correct answer. The original Jacobi sum test was simplified, both theoretically and algorithmically by H. Cohen and H. W. Lenstra, Jr. [**31**], and H. Cohen and A. K. Lenstra have given in [**32**] an implementation report. We do not enter into all the details here, and refer for further improvements of the Jacobi sum test to W. Bosma, M. van der Hulst [**19**] and P. Mihăilescu [**85**]. This improved version of the Jacobi sum test is, indeed, practical in the sense that the primality of numbers with about 1000 decimal digits can be proved in a not too unreasonable amount of time. However, the test is not as easy to program as the probabilistic Miller-Rabin test (Algorithm 3.11), and the resulting code is not simple.

In 1986, another primality testing algorithm was invented, first for theoretical purposes by S. Goldwasser and J. Kilian [**46**]: almost all primes could now be proved in probabilistic polynomial time. A. O. L. Atkin and F. Morain [**8**] considerably modified it to obtain a practical algorithm. This algorithm is based on an elliptic curve analogue to Pocklington's Theorem 3.17, by replacing the group $(\mathbb{Z}/n\mathbb{Z})^*$ by the group of points on an elliptic curve modulo n. The advantage of elliptic curves modulo n is the number of points m on an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ being inside the interval[2] $]n+1-2\sqrt{n}, n+1+2\sqrt{n}[$, if n is prime. Thus, it should be possible to construct an elliptic curve such that m can be partially factored. Fortunately, R. Schoof has developed a deterministic algorithm [**118**] for computing m if n is a prime number. With heuristic arguments the expected running time of this algorithm for proving the primality of n has been shown to be $O(\ln(n)^{6+\epsilon})$ for any $\epsilon > 0$, hence it is a polynomial time; but this is only an average, since for some numbers the running time could be much larger. Elliptic curve primality proving algorithms have been used to prove the primality of numbers of more than 1000 decimal digits. For more details we refer to [**8**].

L. M. Adleman and M.-D. Huang [**2**] later found an unpractical version, using a higher dimensional analogue of the elliptic curves test[3] that finds rigorous proofs of primality for all prime numbers n with a running time that is polynomial in $\log(n)$ with high probability. However, their method is purely of theoretical interest, even if it is the only known polynomial time primality proving algorithm, so we can formulate the following theorem, which is one of the major achievements of theoretical algorithmic number theory.

THEOREM 3.19 ([**2**]). *There exists a probabilistic polynomial time algorithm which can prove or disprove that a given number n is prime.*

[2]This was an important result of H. Hasse. A proof can be found on page 131 of [**119**], or an elementary proof in [**132**].

[3]Instead of using elliptic curves they use curves $y^2 = f(x)$, where $f(x)$ is a polynomial of degree 6.

4. Deterministic Versions

In Section 2 and also in Section 3, we have not specified how to choose the bases for the compositeness test or for Pocklington's Theorem 3.17. There are two fundamentally different approaches to solve this problem. The first approach is to select randomly a base among all possible bases; the second approach is to select a base or a set of bases by using a deterministic algorithm. The goal of this section is to describe methods to find "good" bases or, more precisely, to avoid combinations of "bad" bases. In other words, we are looking for the smallest set of bases which are neccessary for proving the primality of n.

4.1. Miller's Test and the Extended Riemann Hypothesis. A. Granville and C. Pomerance [**53**] have proved that there always exists a composite number that will pass the Algorithm 3.11 for every fixed set of bases. So we are interested in an algorithm which constructs a set of bases such that the number n is a proved prime. We will see in Chapter 5, that it might be possible to solve this problem with only two bases if we extend Miller's test a little.

Assuming the truth of the Extended Riemann Hypothesis, G. L. Miller has proved in [**86**] that consecutive Miller-Rabin tests can constitute a primality test working in polynomial time. He proved that if n is composite, there exists a base $a < C \cdot \ln(n)^2$ such that the Algorithm 3.11 returns the result false. In Chapter 6, we will prove that the constant C can be taken as $\frac{3}{2}$.
The Extended Riemann Hypothesis is required to prove the existence of a "small" quadratic non-residue for every divisor of the testing number n (see [**76**]).
This hypothesis is a generalization of the ordinary Riemann Hypothesis to the Dirichlet L-function. In the Extended Riemann Hypothesis, it is assumed that all L-functions have their non-trivial roots exactly on the line $s = \frac{1}{2}$.
We refer to Chapter 6 for more details about this test. Moreover, it is interesting and also useful to know the smallest strong pseudoprime to several bases simultaneously.

- If $n < 2\,047$ and the result of Algorithm 3.11 is true for the base 2, then n is a prime number.
- If $n < 1\,373\,653$ and the result of Algorithm 3.11 is true for the bases $\{2, 3\}$, then n is a prime number.
- If $n < 25\,326\,001$ and the result of Algorithm 3.11 is true for the bases $\{2, 3, 5\}$, then n is a prime number.
- If $n < 3\,215\,031\,751$ and the result of Algorithm 3.11 is true for the bases $\{2, 3, 5, 7\}$, then n is a prime number.
- If $n < 2\,152\,302\,898\,747$ and the result of Algorithm 3.11 is true for the bases $\{2, 3, 5, 7, 11\}$, then n is a prime number.
- If $n < 3\,474\,749\,660\,383$ and the result of Algorithm 3.11 is true for the bases $\{2, 3, 5, 7, 11, 13\}$, then n is a prime number.
- If $n < 341\,550\,071\,728\,321$ and the result of Algorithm 3.11 is true for the bases $\{2, 3, 5, 7, 11, 13, 17\}$, then n is a prime number.

The first three results are calculations of C. Pomerance, J. L. Selfridge and S. S. Wagstaff, Jr. [**104**]. The other extended results are provided by G. Jaeschke [**62**]. Additionally, in the same article, he has shown some other results:

- If $n < 9\ 080\ 191$ and the result of Algorithm 3.11 is true for the bases $\{31, 73\}$, then n is a prime number.
- If $n < 4\ 759\ 123\ 141$ and the result of Algorithm 3.11 is true for the bases $\{2, 7, 61\}$, then n is a prime number.
- If $n < 1\ 000\ 000\ 000\ 000$ and the result of Algorithm 3.11 is true for the bases $\{2, 13, 23, 1662803\}$, then n is a prime number.

4.2. Pocklington's Theorem. By Miller's test and assuming the Extended Riemann Hypothesis, we know that the prime recognition problem can be solved in polynomial time. But the problem is that the truth of the Extended Riemann Hypothesis is not yet proved.

It has been known since Lucas, that it is easy to find a proof of primality for a prime p if the complete factorization of $p-1$ is known. Indeed, we merely have to present a primitive root for p and prove that it is the primitive root by using the prime factorization of $p-1$. In fact, E. Bach [**13**] has recently shown that if the Extended Riemann Hypothesis is true, there exists a fast deterministic algorithm for finding a primitive root for a prime p. Another method that works very well in practice, is choosing random integers until a primitive root is found. The expected number of tries is $O(\ln(\ln(p)))$, which follows from Theorem 2.3.

But M. R. Fellows and N. Koblitz [**41**] have shown that they can determine whether a number n is prime or composite in deterministic polynomial time, if the complete factorization of $n-1$ is given. The advantage of it is, that this result does not rely on the truth of any unproved hypotheses. Their algorithm needs $O(\ln(n)^2)$ tries, and does not guarantee that it will find a primitive root or a set of generators; but it proves primality and is deterministic.

In 1997, a more elaborate version was given by S. Konyagin and C. Pomerance in [**68**]. They have shown how the prime or composite nature of p can be decided deterministically and in polynomial time $O(\ln(p)^{\frac{10}{7}})$. In addition, they only require a fully factorized divisor F of $p-1$, where $F > p^{\frac{1}{4}+\epsilon}$. In particular, they presented an algorithm which allows to decide whether n is prime or composite, if it is known that all prime divisors of n are congruent $1 \pmod F$ with $F \geq n^{\frac{3}{10}}$, which is a practical addition to [**24**].

Nevertheless, we have to know a large partial factorization of $n-1$ to prove the primality of n by this approach. Generally, this is not feasible for large numbers n, because it can be very time consuming.

CHAPTER 4

Commutator Curves

1. Introduction

DEFINITION 4.1. Let n be a positive integer. We define the *commutator flat* C_n by the set

$$C_n := \{c(x,y) \pmod n \mid x, y \in (\mathbb{Z}/n\mathbb{Z})^*\} \subseteq SL_2(n),$$

where the commutator c in the two-dimensional special linear group is defined by

$$\begin{aligned} c(x,y) &:= \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -y & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1+xy & -x \\ -y & 1 \end{pmatrix} \begin{pmatrix} 1+xy & x \\ y & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1+xy+x^2y^2 & x^2y \\ -xy^2 & 1-xy \end{pmatrix}. \end{aligned}$$

with $x, y \in (\mathbb{Z}/n\mathbb{Z})^*$.

Regarding the commutator flat, our main interest will be the distribution of the orders in $SL_2(n)$ of the points on this flat, where n is a positive integer. We consider this distribution of orders with regard to a compositeness test.
It is easy to see that the commutator flat is a subset of $SL_2(n)$, where n is a positive integer. But from the definition above it is not directly clear how many points are on the commutator flat C_n; or more precisely do there exist some points with the same image? This question will be answered in this section.

First, we will prove that the commutator flat can be represented by the disjoint union of sets which we will call *commutator curves*. In this context, we use the term *curve* for a set described by a single parameter.

THEOREM 4.2. *Let n be a positive integer. Then C_n is the disjoint union of C_n^x:*

$$C_n = \dot{\bigcup_{x \in (\mathbb{Z}/n\mathbb{Z})^*}} C_n^x,$$

where

$$C_n^x := \{c(x,y) \pmod n \mid y \in (\mathbb{Z}/n\mathbb{Z})^*\}$$

is a commutator curve *for $x \in (\mathbb{Z}/n\mathbb{Z})^*$.*

PROOF. Obviously, we have

$$C_n = \bigcup_{x \in (\mathbb{Z}/n\mathbb{Z})^*} C_n^x.$$

Therefore, we have to show that no different points have the same image under the map c to complete the proof of this theorem.
Let $x_1, x_2, y_1, y_2 \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $c(x_1, y_1) \equiv c(x_2, y_2) \pmod{n}$. Then from Definition 4.1, we have the following equations

$$\begin{aligned} x_1^2 y_1 &\equiv x_2^2 y_2 \pmod{n}, && (2)\\ x_1 y_1^2 &\equiv x_2 y_2^2 \pmod{n}, && (3)\\ x_1 y_1 &\equiv x_2 y_2 \pmod{n}. && (4) \end{aligned}$$

Since x_1, x_2, y_1, y_2 are invertible and from division (2) by (4), we have

$$x_1 \equiv x_2 \pmod{n}.$$

Similarly, divide (3) by (4), we have

$$y_1 \equiv y_2 \pmod{n}.$$

Thus, the points (x_1, y_1) and (x_2, y_2) are equal modulo n. □

The commutator has, above all, the following useful property

LEMMA 4.3. *Let G be a group, $x, y \in G$, m be a positive integer, and 1 be the unit element of G. Then we have*

$$(x^{-1}y^{-1}xy)^m = 1 \qquad \textit{if and only if} \qquad (x^{-1}yxy^{-1})^m = 1.$$

PROOF. The proof of the assertion follows directly by

$$\begin{aligned} & (x^{-1}y^{-1}xy)^m = \prod_{k=1}^{m}((yx)^{-1}(xy)) = 1 \\ \Leftrightarrow \quad & xy\prod_{k=2}^{m}((yx)^{-1}(xy)) = yx \\ \Leftrightarrow \quad & yx\prod_{k=2}^{m}((xy)^{-1}(yx)) = xy \\ \Leftrightarrow \quad & 1 = x^{-1}yx\prod_{k=2}^{m}(y^{-1}x^{-1}yx)y^{-1} = (x^{-1}yxy^{-1})^m. \quad \square \end{aligned}$$

COROLLARY 4.4. *Let n be a positive integer, and $x, y \in (\mathbb{Z}/n\mathbb{Z})^*$. Then*

$$\operatorname{ord}(c(x, y)) = \operatorname{ord}(c(x, -y)).$$

PROOF. It can be directly concluded from Lemma 4.3. □

By this corollary, we see that the orders on the commutator flat are symmetrical to the second argument. Before we collect more properties of the distribution of the orders on the commutator flat, we introduce the standard commutator curve over n, where n is a positive integer.

DEFINITION 4.5. Let n be a positive integer. We define the *standard commutator curve* C_n^1 by the set

$$C_n^1 := \{c(1,x) \pmod n \mid x \in (\mathbb{Z}/n\mathbb{Z})^*\},$$

where the commutator c in the two-dimensional special linear group is defined by

$$\begin{aligned} c(1,x) &:= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \\ &\underset{(4.1)}{=} \begin{pmatrix} 1+x+x^2 & x \\ -x^2 & 1-x \end{pmatrix} \end{aligned}$$

with $x \in (\mathbb{Z}/n\mathbb{Z})^*$.

Obviously, working with the standard commutator curve is more simple than with the commutator flat. But the main reason why we reduce the consideration from the commutator flat to the standard commutator curve, is because every commutator curve C_n^x is conjugate to the standard commutator curve C_n^1 via conjugation[1] by

$$\begin{pmatrix} 1 & 0 \\ 0 & x^{-1} \end{pmatrix} \in GL_2(n).$$

Hence both have the same distribution of orders and therefore they are equal under statistical considerations, where n is a positive integer. We will show this by the following theorem.

THEOREM 4.6. *Let n be a positive integer, and $x, y \in (\mathbb{Z}/n\mathbb{Z})^*$. Then we have*

$$c(x,y)^n \equiv I_2 \pmod n \qquad \textit{if and only if} \qquad c(1,xy)^n \equiv I_2 \pmod n.$$

PROOF. We have the following equation

$$\begin{aligned} c(x,y) &\underset{(4.1)}{=} \begin{pmatrix} 1+xy+x^2y^2 & x^2y \\ -xy^2 & 1-xy \end{pmatrix} \\ &= \begin{pmatrix} 1+xy & xy \\ -y & x^{-1}-y \end{pmatrix} \begin{pmatrix} 1 & 0 \\ xy & x \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -xy & 1-xy \end{pmatrix} \begin{pmatrix} 1 & 0 \\ xy & x \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -xy & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ xy & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & x^{-1} \end{pmatrix} c(1,xy) \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}. \end{aligned} \tag{5}$$

[1]The conjugation for a group G is defined by the map $\kappa : G \times G \to G : (a,x) \mapsto axa^{-1}$, e.g. see [**42**] on page 38.

Note that

$$\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} \notin SL_2(n) \qquad \text{if } x \not\equiv 1 \pmod{n}.$$

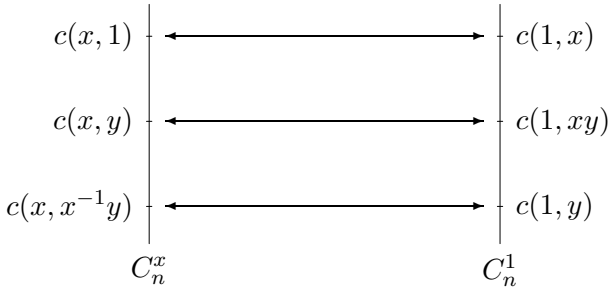
"⇒": We have $c(x,y)^n \equiv I_2 \pmod{n}$. Then from (5), we have

$$\begin{aligned} c(1,xy)^n &\underset{(5)}{=} \left(\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} c(x,y) \begin{pmatrix} 1 & 0 \\ 0 & x^{-1} \end{pmatrix} \right)^n \\ &= \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} c(x,y)^n \begin{pmatrix} 1 & 0 \\ 0 & x^{-1} \end{pmatrix} \\ &\equiv \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & x^{-1} \end{pmatrix} = I_2 \pmod{n}. \end{aligned}$$

"⇐": We have $c(1,xy)^n \equiv I_2 \pmod{n}$. Then from (5), we have

$$\begin{aligned} c(x,y)^n &\underset{(5)}{=} \left(\begin{pmatrix} 1 & 0 \\ 0 & x^{-1} \end{pmatrix} c(1,xy) \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} \right)^n \\ &= \begin{pmatrix} 1 & 0 \\ 0 & x^{-1} \end{pmatrix} c(1,xy)^n \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} \\ &\equiv \begin{pmatrix} 1 & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} = I_2 \pmod{n}. \quad \square \end{aligned}$$

In Theorem 4.6 we have shown that every point on the commutator flat can be transferred to a point on the standard commutator curve with the same order.



Therefore, we will concentrate our consideration of the distribution of orders on the standard commutator curve.

The Chinese Remainder Theorem 2.5 can be transferred on the standard commutator curve.

THEOREM 4.7. *Let m_1, m_2 be positive integers with $\gcd(m_1,m_2)=1$, and let*

$$c(1,x_1) \in C_{m_1}^1 \quad \text{and} \quad c(1,x_2) \in C_{m_2}^1,$$

then there exists a unique solution

$$c(1,x_3) \in C_{m_1m_2}^1$$

with $c(1,x_3) \equiv c(1,x_1) \pmod{m_1}$, and $c(1,x_3) \equiv c(1,x_2) \pmod{m_2}$.

PROOF. Let $k \in \{1, 2\}$. Then

$$c(1, x_3) = \begin{pmatrix} 1 + x_3 + x_3^2 & x_3 \\ -x_3^2 & 1 - x_3 \end{pmatrix} \equiv \begin{pmatrix} 1 + x_k + x_k^2 & x_k \\ -x_k^2 & 1 - x_k \end{pmatrix} = c(1, x_k) \pmod{m_k}$$

is in $C^1_{m_1 m_2}$ a unique solution since x_3 is a unique solution modulo $m_1 m_2$ with

$$x_3 \equiv x_k \pmod{m_k}$$

by Theorem 2.5. □

2. The Order of a Group Element in $SL_2(p)$

We know that the standard commutator curve over n is a subset of $SL_2(n)$, where n is a positive integer. So before considering the orders on the standard commutator curve, we will know which orders can be found in $SL_2(p)$, where p is an odd prime number.

THEOREM 4.8. *Let p be an odd prime number,*

$$A := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in SL_2(p),$$

and $\epsilon = \left(\frac{(a_{11}+a_{22})^2-4}{p}\right)$. Then we have exactly one of the following assertions

$$A^{p-\epsilon} \equiv I_2 \pmod{p} \qquad \text{if } \epsilon \neq 0,$$

and

$$A^{2p} \equiv I_2 \pmod{p} \qquad \text{if } \epsilon = 0.$$

PROOF. We have the characteristic polynomial

$$\begin{aligned} \chi_A(t) &= \det \begin{pmatrix} a_{11} - t & a_{12} \\ a_{21} & a_{22} - t \end{pmatrix} = (a_{11} - t)(a_{22} - t) - a_{12}a_{21} \\ &= t^2 - (a_{11} + a_{22})t + \underbrace{a_{11}a_{22} - a_{12}a_{21}}_{=1}. \end{aligned}$$

This polynomial $\chi_A(t)$ has the discriminant

$$D^2 = (a_{11} + a_{22})^2 - 4.$$

Let ξ_1, ξ_2 be the two roots of $\chi_A(t)$ in an algebraic closure of $\mathbb{F}_p$.
First of all, we assume that $(a_{11} + a_{22})^2 \not\equiv 4 \pmod{p}$. Then it is easy to show that

$$A = S \begin{pmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{pmatrix} S^{-1}$$

where

$$S = (2D)^{-1} \begin{pmatrix} 2a_{21} & a_{22} - a_{11} + D \\ -2a_{21} & a_{11} - a_{22} + D \end{pmatrix}.$$

The following two cases are possible

(1) If $\left(\frac{D^2}{p}\right) = 1$, the two eigenvalues ξ_1 and ξ_2 are distinct elements of $\mathbb{F}_p$, and we get

$$\begin{aligned} A^{p-1} &= (S\begin{pmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{pmatrix} S^{-1})^{p-1} \\ &= S\begin{pmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{pmatrix}^{p-1} S^{-1} \\ &= S\begin{pmatrix} \xi_1^{p-1} & 0 \\ 0 & \xi_2^{p-1} \end{pmatrix} S^{-1} \equiv I_2 \pmod{p}. \end{aligned}$$

(2) If $\left(\frac{D^2}{p}\right) = -1$, the two eigenvalues ξ_1 and ξ_2 are distinct elements of $\mathbb{F}_{p^2} - \mathbb{F}_p$, and we get

$$\begin{aligned} A^{p+1} &= (S\begin{pmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{pmatrix} S^{-1})^{p+1} \\ &= S\begin{pmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{pmatrix}^{p+1} S^{-1} \\ &= S\begin{pmatrix} \xi_1^{p+1} & 0 \\ 0 & \xi_2^{p+1} \end{pmatrix} S^{-1} \equiv I_2 \pmod{p}. \end{aligned}$$

Now we assume that $(a_{11} + a_{22})^2 \equiv 4 \pmod{p}$. Then the eigenspace corresponding to $\xi_1 = \xi_2$ has dimension two or one and since $\det(A) = 1$ we have $\xi_1 \in \{\pm 1\}$. So

$$A = \begin{pmatrix} \xi_1 & 0 \\ 0 & \xi_1 \end{pmatrix} = \pm I_2,$$

hence $A^{2p} = I_2^p = I_2$, or there exists a matrix $S \in GL_2(p)$ such that

$$A = S\begin{pmatrix} \xi_1 & 0 \\ 1 & \xi_1 \end{pmatrix} S^{-1}.$$

For $\xi_1 = \xi_2 = 1$ we have

$$A^p = S\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^p S^{-1} = S\begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix} S^{-1} \equiv I_2 \pmod{p}.$$

Similarly, for $\xi_1 = \xi_2 = -1$ we have $A^{2p} \equiv I_2 \pmod{p}$. □

COROLLARY 4.9. *Let p be an odd prime number, $x \in \mathbb{F}_p^*$, and $\epsilon = \left(\frac{x^2+4}{p}\right)$. Then we have exactly one of the following assertions*

$$c(1,x)^{p-\epsilon} \equiv I_2 \pmod{p} \qquad \text{if } \epsilon \neq 0,$$

and

$$\operatorname{ord}_p(c(1,x)) = 2p \qquad \text{if } \epsilon = 0.$$

PROOF. If $\epsilon \neq 0$, then this corollary follows directly by Theorem 4.8.
If $\epsilon = 0$, then, by Theorem 4.8, we have

$$c(1,x)^{2p} \equiv I_2 \pmod{p},$$

and there exists a matrix $S \in GL_2(p)$ and $\xi \in \pm 1$ such that

$$c(1,x) = S \begin{pmatrix} \xi & 0 \\ 1 & \xi \end{pmatrix} S^{-1}.$$

Suppose $\xi = 1$. Then the trace of the matrix

$$\operatorname{trace}(c(1,x)) = x^2 + 2 \equiv 2\xi = 2 \pmod{p}$$

contradicts $x \in \mathbb{F}_p^*$. Thus, $\xi = -1$. Therefore, $\operatorname{ord}_p(c(1,x)) = 2p$ as claimed. □

3. The Orders on the Standard Commutator Curve

First we consider a few examples of orders on the standard commutator curve over a prime number, before we collect some general properties about the distribution of the orders on the standard commutator curve.

EXAMPLE 4.10. *Let $p = 7$, and $x \in \mathbb{F}_p^*$, where $p \equiv 3 \pmod 4$. Then we have the following table for the orders on C_p^1:*

x	1	2	3	4	5	6
$\operatorname{ord}(c(1,x))$	8	3	8	8	3	8

Thus, we have the following frequencies of orders:

$\operatorname{ord}(c(1,x))$	2	3	4	6	7	8	14
frequency	0	2	0	0	0	4	0

EXAMPLE 4.11. *Let $p = 11$, and $x \in \mathbb{F}_p^*$, where $p \equiv 3 \pmod 4$. Then we have the following table for the orders on C_p^1:*

x	1	2	3	4	5	6	7	8	9	10
$\operatorname{ord}(c(1,x))$	5	12	4	5	12	12	5	4	12	5

Thus, we have the following frequencies of orders:

$\operatorname{ord}(c(1,x))$	2	3	4	5	6	10	11	12	22
frequency	0	0	2	4	0	0	0	4	0

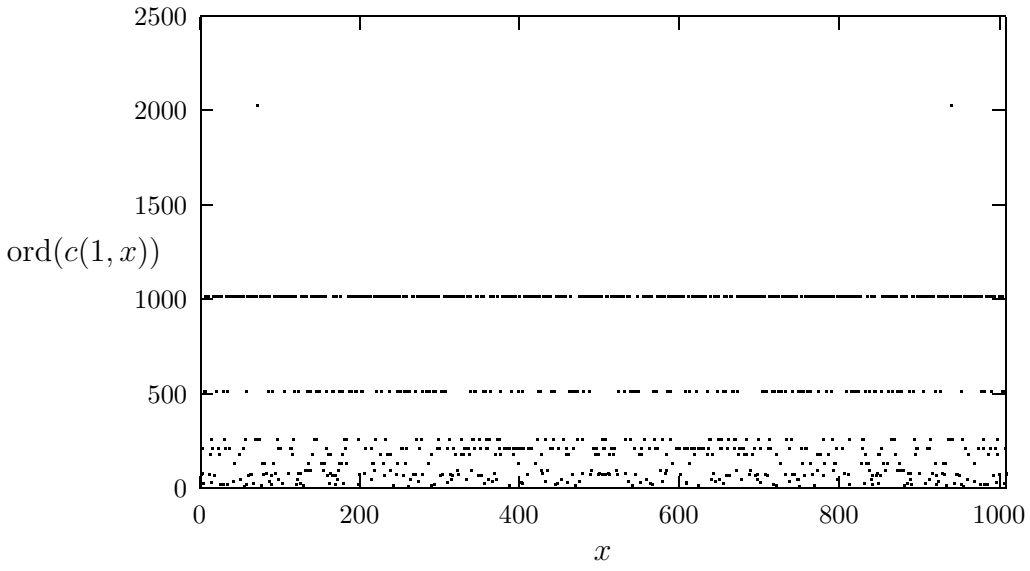
EXAMPLE 4.12. *Let $p = 13$, and $x \in \mathbb{F}_p^*$, where $p \equiv 1 \pmod 4$. Then we have the following table for the orders on C_p^1:*

x	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ord}(c(1,x))$	14	14	26	14	6	3	3	6	14	26	14	14

Thus, we have the following frequencies of orders:

$\operatorname{ord}(c(1,x))$	2	3	4	6	7	12	13	14	26
frequency	0	2	0	2	0	0	0	6	2

EXAMPLE 4.13. *Let $p = 1009$, and $x \in \mathbb{F}_p^*$, where $p \equiv 1 \pmod 4$. Then we have the following diagram for the orders on C_p^1:*



If we take all values of this diagram, we have the following frequencies of orders:

$\mathrm{ord}(c(1,x))$	3	4	6	7	8	9	10	12	14	18	21	24	28	36	42
frequency	2	2	2	6	4	6	4	4	6	6	12	8	12	12	12

$\mathrm{ord}(c(1,x))$	56	63	72	84	126	168	202	252	504	1010	2018
frequency	24	36	24	24	36	48	100	72	144	400	2

OBSERVATION 4.14. *These previous examples are a small selection of observations which are made on many numbers, e.g. in Appendix B. They give the following assertions:*

(1) *The frequency of an order on the standard commutator curve is even.*
(2) *Let n be a natural number greater than 2. Then we have $\mathrm{ord}(c(1,x)) \geq 3$ for every $x \in \mathbb{Z}$ with $x \not\equiv 0 \pmod{n}$.*
(3) *Let n be a squarefree odd natural number. Then we have exactly two numbers $x_1, x_2 \in (\mathbb{Z}/n\mathbb{Z})^*$ such that*
$$\mathrm{ord}(c(1,x_1)) = \mathrm{ord}(c(1,x_2)) = 2n$$
if and only if n is a prime number with $n \equiv 1 \pmod{4}$ and
$$x_1^2 \equiv x_2^2 \equiv -4 \pmod{n}$$
.
(4) *Let p be a prime number, and $x \in \mathbb{F}_p^*$ such that $\mathrm{ord}(c(1,x)) \nmid 2p$. Then*
$$|\{y \in \mathbb{F}_p^* \mid \mathrm{ord}(c(1,y)) = \mathrm{ord}(c(1,x))\}| = \varphi(\mathrm{ord}(c(1,x))).$$
(5) *Let p be a prime number, and $x \in \mathbb{F}_p^*$ such that $\mathrm{ord}(c(1,x)) \mid p+1$. Then*[2]
$$\nu_2(\mathrm{ord}(c(1,x))) = \nu_2(p+1).$$
(6) *Let p be a prime number, and $x \in \mathbb{F}_p^*$ such that $\mathrm{ord}(c(1,x)) \mid p-1$. Then*
$$\nu_2(\mathrm{ord}(c(1,x))) < \nu_2(p-1).$$

[2]The definition of the number-theoretic function ν_2 can be found in Definition 2.1 on page 6.

In this section, we will prove the first item of Observation 4.14, because it is easy. The proofs of the other five items of Observation 4.14 are more complex and they will be treated in the following three sections.

The first item of Observation 4.14 can easily be proved by Corollary 4.4.

THEOREM 4.15. *Let n be a natural number greater than 2, and $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Then*

$$|\{y \in (\mathbb{Z}/n\mathbb{Z})^* \mid \operatorname{ord}(c(1,y)) = \operatorname{ord}(c(1,x))\}| \text{ is even.}$$

PROOF. This can be concluded from Corollary 4.4. □

4. Recurrence Relations

In this section we are interested in points on the standard commutator curve which have a fixed order. These points can be characterized by the roots of the following polynomials.

DEFINITION 4.16. Let n be a natural number. Then we recursively define the polynomials $\theta_n(X), \omega_n(X) \in \mathbb{Z}[X]$ by

$$\begin{aligned}
\theta_0(X) &:= 0, \theta_1(X) := 1 + X, \\
\omega_0(X) &:= 0, \omega_1(X) := 1, \\
\theta_{m+2}(X) &:= (X^2+2)\theta_{m+1}(X) - \theta_m(X) + X, \\
\omega_{m+2}(X) &:= (X^2+2)\omega_{m+1}(X) - \omega_m(X) \qquad \text{for } m \in \mathbb{N}.
\end{aligned}$$

In addition, we define the polynomial

$$\psi_n(X) := \gcd(\theta_n(X), \omega_n(X)) \cdot \prod_{\substack{d \mid n \\ d < n}} \gcd(\theta_d(X), \omega_d(X))^{-1}.$$

Using these polynomials we will prove some further equations.

LEMMA 4.17. *Let n be a natural number. Then we have*

$$\begin{aligned}
X\theta_{n+1}(X) &= (X^2+X+1)\omega_{n+1}(X) - \omega_n(X) - 1, \\
\text{and} \quad X^2\omega_{n+1}(X) &= (X-1)\theta_{n+1}(X) + \theta_n(X) + 1.
\end{aligned}$$

PROOF. First, we have the following simple relations:

$$\begin{aligned}
X\theta_1(X) &\underset{(4.16)}{=} X^2 + X + 1 - 1 = X^2 + X, \quad \checkmark \\
X^2\omega_1(X) &\underset{(4.16)}{=} X^2 - 1 + 1 = X^2, \quad \checkmark \\
X\theta_2(X) &\underset{(4.16)}{=} (X^2+2)(X^2+X+1) - 1 - 1 = X^4 + X^3 + 3X^2 + 2, \quad \checkmark \\
\text{and} \quad X^2\omega_2(X) &\underset{(4.16)}{=} (X-1)(X^3+X^2+3X+2) + 1 + X + 1 = X^4 + 2X^2. \quad \checkmark
\end{aligned}$$

We proceed by induction on n. Let $n > 0$ and assume that we have the assertion for n by induction. Then, by the inductional assumption, we have

$$\begin{aligned} X\theta_{n+2}(X) &\underset{(4.16)}{=} (X^2+2)X\theta_{n+1}(X) - X\theta_n(X) + X^2 \\ &\underset{(IA)}{=} (X^2+2)((X^2+X+1)\omega_{n+1}(X) - \omega_n(X) - 1) - (X^2+X+1)\omega_n(X) \\ &\quad + \omega_{n-1}(X) + 1 + X^2 \\ &= (X^2+X+1)((X^2+2)\omega_{n+1}(X) - \omega_n(X)) - (X^2+2)\omega_n(X) \\ &\quad + \omega_{n-1}(X) - 1 \\ &\underset{(4.16)}{=} (X^2+X+1)\omega_{n+2}(X) - \omega_{n+1}(X) - 1, \end{aligned}$$

and

$$\begin{aligned} X^2\omega_{n+2}(X) &\underset{(4.16)}{=} X^2(X^2+2)\omega_{n+1}(X) - X^2\omega_n(X) \\ &\underset{(IA)}{=} (X^2+2)((X-1)\theta_{n+1}(X) + \theta_n(X) + 1) - (X-1)\theta_n(X) \\ &\quad - \theta_{n-1}(X) - 1 \\ &= (X-1)((X^2+2)\theta_{n+1}(X) - \theta_n(X) + X) + (X^2+2)\theta_n(X) \\ &\quad - \theta_{n-1}(X) + X + 1 \\ &\underset{(4.16)}{=} (X-1)\theta_{n+1}(X) + \theta_n(X) + 1. \quad \square \end{aligned}$$

THEOREM 4.18. *Let m be a natural number, n be a positive integer, and $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Then*

$$c(1,x)^m = \begin{pmatrix} 1 + x\theta_m(x) & x\omega_m(x) \\ -x^2\omega_m(x) & 1 + x\theta_m(x) - x(2+x)\omega_m(x) \end{pmatrix}.$$

PROOF. First, we have the following simple relations:

$$\begin{aligned} c(1,x)^0 &= \begin{pmatrix} 1 + x\theta_0(x) & x\omega_0(x) \\ -x^2\omega_0(x) & 1 + x\theta_0(x) - x(2+x)\omega_0(x) \end{pmatrix} \\ &\underset{(4.16)}{=} I_2, \end{aligned}$$

and

$$\begin{aligned} c(1,x)^1 &= \begin{pmatrix} 1 + x\theta_1(x) & x\omega_1(x) \\ -x^2\omega_1(x) & 1 + x\theta_1(x) - x(2+x)\omega_1(x) \end{pmatrix} \\ &\underset{(4.16)}{=} \begin{pmatrix} 1+x+x^2 & x \\ -x^2 & 1-x \end{pmatrix} \\ &\underset{(4.5)}{=} c(1,x). \end{aligned}$$

We proceed by induction on m. Let $m > 0$ and assume that we have the assertion for m by induction. We write θ_m instead of $\theta_m(x)$ and ω_m instead of $\omega_m(x)$ for better reading.

Then, by the inductional assumption, we have

$$\begin{aligned}
& c(1,x)^{m+1} \\
\underset{(IA)}{=} & \begin{pmatrix} 1+x\theta_m & x\omega_m \\ -x^2\omega_m & 1+x\theta_m-x(2+x)\omega_m \end{pmatrix}\begin{pmatrix} 1+x+x^2 & x \\ -x^2 & 1-x \end{pmatrix} \\
= & \begin{pmatrix} 1+x(1+x+(1+x+x^2)\theta_m-x^2\omega_m) & x(1+x\theta_m+\omega_m-x\omega_m) \\ -x^2((1+x+x^2)\omega_m+1+x\theta_m-x(2+x)\omega_m) & -x^3\omega_m+(1+x\theta_m-x(2+x)\omega_m)(1-x) \end{pmatrix} \\
\underset{(4.17)}{=} & \begin{pmatrix} 1+x(x+(2+x^2)\theta_m-\theta_{m-1}) & x((x^2+2)\omega_m-\omega_{m-1}) \\ -x^2((x^2+2)\omega_m-\omega_{m-1}) & 1+x((2+x^2)\theta_m-\theta_{m-1}-2-(x\theta_m-\omega_m+x\omega_m)(2+x)) \end{pmatrix} \\
\underset{(4.17)}{=} & \begin{pmatrix} 1+x\theta_{m+1} & x\omega_{m+1} \\ -x^2\omega_{m+1} & 1+x\theta_{m+1}-x(1+(x^2+x+1)\omega_m-\omega_{m-1}-1+(1-x)\omega_m)(2+x) \end{pmatrix} \\
\underset{(4.17)}{=} & \begin{pmatrix} 1+x\theta_{m+1} & x\omega_{m+1} \\ -x^2\omega_{m+1} & 1+x\theta_{m+1}-x(2+x)\omega_{m+1} \end{pmatrix}. \quad \square
\end{aligned}$$

COROLLARY 4.19. *Let m be a natural number, n be a positive integer, and $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Then we have*

$$\begin{aligned}
\theta_{2m}(x) &= x\theta_m(x)^2+2\theta_m(x)-x^2\omega_m(x)^2, \\
\textit{and} \quad \omega_{2m}(x) &= (\omega_{m+1}(x)-\omega_{m-1}(x))\omega_m(x).
\end{aligned}$$

PROOF. The proof of the assertion follows directly from Theorem 4.18 and the equation

$$\begin{aligned}
& c(1,x)^{2m} \\
\underset{(4.18)}{=} & \begin{pmatrix} 1+x\theta_m & x\omega_m \\ -x^2\omega_m & 1+x\theta_m-x(2+x)\omega_m \end{pmatrix}^2 \\
= & \begin{pmatrix} (1+x\theta_m)^2-x^3\omega_m^2 & x(2+2x\theta_m-x(2+x)\omega_m)\omega_m \\ -x^2(2+2x\theta_m-x(2+x)\omega_m)\omega_m & (1+x\theta_m-x(2+x)\omega_m)^2-x^3\omega_m \end{pmatrix} \\
\underset{(4.17)}{=} & \begin{pmatrix} 1+x(x\theta_m^2+2\theta_m-x^2\omega_m^2) & x(2((x^2+x+1)\omega_m-\omega_{m-1})-x(2+x)\omega_m)\omega_m \\ -x^2((x^2+2)\omega_m-2\omega_{m-1})\omega_m & (1+x\theta_m-x(2+x)\omega_m)^2-x^3\omega_m \end{pmatrix} \\
\underset{(4.16)}{=} & \begin{pmatrix} 1+x(x\theta_m^2+2\theta_m-x^2\omega_m^2) & x(\omega_{m+1}-\omega_{m-1})\omega_m \\ -x^2(\omega_{m+1}-\omega_{m-1})\omega_m & 1+x\theta_{2m}-x(2+x)\omega_{2m} \end{pmatrix},
\end{aligned}$$

where we write θ_m instead of $\theta_m(x)$ and ω_m instead of $\omega_m(x)$ for better reading. $\square$

Using this Theorem 4.18 it is easy to prove the second item of Observation 4.14.

THEOREM 4.20. *Let n be a natural number greater than 2, and $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Then*

$$\operatorname{ord}(c(1,x)) \geq 3.$$

PROOF. Since $x \not\equiv 0 \pmod{n}$, we have $c(1,x) \not\equiv I_2 \pmod{n}$. Thus $\operatorname{ord}(c(1,x)) \geq 2$. Suppose we have an integer x with $x \not\equiv 0 \pmod{n}$ such that $\operatorname{ord}(c(1,x)) = 2$. Then

$$\begin{aligned}
c(1,x)^2 & \underset{(4.18)}{=} \begin{pmatrix} 1+x\theta_2(x) & x\omega_2(x) \\ -x^2\omega_2(x) & 1+x\theta_2(x)-x(2+x)\omega_2(x) \end{pmatrix} \\
& \underset{(4.16)}{=} \begin{pmatrix} 1+x(2+x^2+x(3+x^2)) & x(2+x^2) \\ -x^2(2+x^2) & 1-x(2+x-x^2) \end{pmatrix} \\
& \equiv I_2 \pmod{n}.
\end{aligned}$$

Therefore,

$$2 + x^2 \equiv 0 \pmod{n} \quad \text{and} \quad 2 + x^2 + x(3 + x^2) \equiv 0 \pmod{n}.$$

Thus, we have $1 \equiv 0 \pmod{n}$, which contradicts $n \geq 3$. □

Moreover, by Theorem 4.18, we can determine all points point on the standard commutator curve with the order m by finding the roots of polynomial $\psi_m(X)$, where m is a positive integer.

THEOREM 4.21. *Let m, n be positive integers, and $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Then*

$$\psi_m(x) \equiv 0 \pmod{n} \qquad \Rightarrow \qquad \mathrm{ord}_n(c(1, x)) = m.$$

PROOF. We have $\theta_m(x) \equiv \omega_m(x) \equiv 0 \pmod{n}$. By Definition 4.16 of $\psi_m(x)$, and Theorem 4.18, we have

$$c(1, x)^m \equiv I_2 \pmod{n} \quad \text{and} \quad c(1, x)^d \not\equiv I_2 \pmod{n} \qquad \text{for all } d \mid m \text{ with } d < m.$$

Therefore, by Lagrange's Theorem 2.11, we get

$$\mathrm{ord}_n(c(1, x)) = m.$$

□

For example, we can characterize all points on the standard commutator curve, which have an order equal to six.

COROLLARY 4.22. *Let n be an odd positive integer, and $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Then we have*

$$x^2 \equiv -1 \pmod{n} \qquad \Rightarrow \qquad \mathrm{ord}(c(1, x)) = 6.$$

PROOF. We have the following equations

$$\begin{aligned}
\theta_2(X) &\underset{(4.16)}{=} (X^2 + 2)(1 + X) + X = X^3 + X^2 + 3X + 2 \\
\omega_2(X) &\underset{(4.16)}{=} X^2 + 2 \\
\theta_3(X) &\underset{(4.16)}{=} (X^2 + 2)(X^3 + X^2 + 3X + 2) - X - 1 + X \\
&= X^5 + X^4 + 5X^3 + 4X^2 + 6X + 3 \\
&= (X^2 + 3)(X^3 + X^2 + 2X + 1) \\
\omega_3(X) &\underset{(4.16)}{=} (X^2 + 2)^2 - 1 = X^4 + 4X^2 + 3 \\
&= (X^2 + 3)(X^2 + 1) \\
\theta_6(X) &\underset{(4.19)}{=} X(X^5 + X^4 + 5X^3 + 4X^2 + 6X + 3)^2 \\
&\quad + 2(X^5 + X^4 + 5X^3 + 4X^2 + 6X + 3) \\
&\quad - X^2(X^4 + 4X^2 + 3)^2 \\
&= X^{11} + X^{10} + 11X^9 + 10X^8 + 45X^7 + 36X^6 + 84X^5 + 56X^4 + 70X^3 \\
&\quad + 35X^2 + 21X + 6
\end{aligned}$$

$$\begin{aligned} &= (X^2+1)(X^2+3)(X^7+X^6+7X^5+6X^4+14X^3+9X^2+7X+2) \\ \omega_6(X) &\underset{(4.19)}{=} (X^6+6X^4+10X^2+4-X^2-2)(X^4+4X^2+3) \\ &= X^{10}+10X^8+36X^6+56X^4+35X^2+6 \\ &= (X^2+3)(X^2+2)(X^2+1)(X^4+4X^2+1). \end{aligned}$$

Therefore, we have

$$\begin{aligned} \psi_6(X) &\underset{(4.16)}{=} \gcd(\theta_6(X),\omega_6(X)) \cdot \gcd(\theta_2(X),\omega_2(X))^{-1} \cdot \gcd(\theta_3(X),\omega_3(X))^{-1} \\ &= (X^2+1)(X^2+3)\cdot 1^{-1}\cdot (X^2+3)^{-1} \\ &= X^2+1 \end{aligned}$$

and the proof of the assertion follows directly from Theorem 4.21. □

EXAMPLES 4.23. *Using (for example) the algebra package Maple from the University of Waterloo (Canada), we can calculate the following polynomials:*

$$\begin{aligned} \psi_3(X) &= X^2+3 \\ \psi_4(X) &= X^2+2 \\ \psi_5(X) &= X^4+5X^2+5 \\ \psi_6(X) &= X^2+1 \\ \psi_7(X) &= X^6+7X^4+14X^2+7 \\ \psi_8(X) &= X^4+4X^2+2 \\ \psi_9(X) &= X^6+6X^4+9X^2+3 \\ \psi_{10}(X) &= X^4+3X^2+1 \\ \psi_{11}(X) &= X^{10}+11X^8+44X^6+77X^4+55X^2+11 \\ \psi_{12}(X) &= X^4+4X^2+1 \\ \psi_{13}(X) &= X^{12}+13X^{10}+65X^8+156X^6+182X^4+91X^2+13 \\ \psi_{14}(X) &= X^6+5X^4+6X^2+1 \\ \psi_{15}(X) &= X^8+7X^6+14X^4+8X^2+1 \\ \psi_{16}(X) &= X^8+8X^6+20X^4+16X^2+2 \\ \psi_{17}(X) &= X^{16}+17X^{14}+119X^{12}+442X^{10}+935X^8+1122X^6+714X^4+204X^2+17 \\ \psi_{18}(X) &= X^6+6X^4+9X^2+1 \\ \psi_{19}(X) &= X^{18}+19X^{16}+152X^{14}+665X^{12}+1729X^{10}+2717X^8+2508X^6+1254X^4 \\ &\quad +285X^2+19. \end{aligned}$$

5. Distribution of Orders

In this section, we consider the set of orders on the standard commutator curve, split up into three sets.

DEFINITION 4.24. Let n be a natural number greater than 2. Considering the map

$$c : (\mathbb{Z}/n\mathbb{Z})^* \to SL_2(n) : x \mapsto \begin{pmatrix} 1+x+x^2 & x \\ -x^2 & 1-x \end{pmatrix} = c(1,x),$$

we define the set

$$N_{-1}(n) := \{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid c(1,x)^{n+1} \equiv I_2 \pmod{n}\},$$

which contains all elements $x \in (\mathbb{Z}/n\mathbb{Z})^*$, for which the order of the commutator $c(1,x)$ divides $n+1$. Hence,

$$N_1(n) := \{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid c(1,x)^{n-1} \equiv I_2 \pmod{n}\}$$

contains all elements $x \in (\mathbb{Z}/n\mathbb{Z})^*$, for which the order of the commutator $c(1,x)$ divides $n-1$. Finally,

$$N_0(n) := \{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid c(1,x)^{2n} \equiv I_2 \pmod{n}\}$$

is the set of all elements $x \in (\mathbb{Z}/n\mathbb{Z})^*$, for which the order of the commutator $c(1,x)$ divides $2n$.

The following theorem will show that the three sets $N_{-1}(n), N_0(n)$, and $N_1(n)$ are disjoint, if n is a natural number greater than 2.

THEOREM 4.25. *Let n be a natural number greater than 2. Then*

$$N_{-1}(n) \dot\cup N_0(n) \dot\cup N_1(n) \subseteq (\mathbb{Z}/n\mathbb{Z})^*.$$

PROOF. Let x be an integer such that $x \not\equiv 0 \pmod{n}$. We split up the proof of this theorem into three cases to prove that x is at most in one of the three sets $N_{-1}(n), N_0(n)$, and $N_1(n)$.

(1) If $c(1,x)^{n+1} \equiv c(1,x)^{n-1} \equiv I_2 \pmod{n}$, then we have
$$c(1,x)^2 = c(1,x)^{n+1-(n-1)} = c(1,x)^{n+1} \cdot c(1,x)^{n-1} \equiv I_2 \pmod{n}.$$
But this equation contradicts Theorem 4.20.

(2) If $c(1,x)^{n+1} \equiv c(1,x)^{2n} \equiv I_2 \pmod{n}$, then we have
$$c(1,x)^{n-1} = c(1,x)^{2n-(n+1)} = c(1,x)^{2n} \cdot c(1,x)^{n+1} \equiv I_2 \pmod{n}.$$
Hence, we get a contradiction by considering the first case.

(3) If $c(1,x)^{n-1} \equiv c(1,x)^{2n} \equiv I_2 \pmod{n}$, then we have
$$c(1,x)^{n+1} = c(1,x)^{2n-(n-1)} = c(1,x)^{2n} \cdot (c(1,x)^{n-1})^{-1} \equiv I_2 \pmod{n}.$$
Hence, we get a contradiction by considering the second case.

Therefore, the three sets are disjoint. □

Before we consider more details about these three sets, we will define in this section other three sets, which are also disjoint and whose size is easier to estimate.

DEFINITION 4.26. Let n be a natural number greater than 2. Then we define the following three sets

$$L_\epsilon(n) = \{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{n}\right) = \epsilon\},$$

where $\epsilon \in \{-1, 0, 1\}$.
It is immediate that $(\mathbb{Z}/n\mathbb{Z})^* = L_{-1}(n) \dot\cup L_0(n) \dot\cup L_1(n)$ holds.

5.1. The Standard Commutator Curve with Prime Power Modulus. First, we consider the six sets defined above only for prime numbers. In this case we will easily see by the following theorem that $N_\epsilon(p)$ is equal to $L_\epsilon(p)$, where $\epsilon \in \{-1, 0, 1\}$, and p is an odd prime number.

THEOREM 4.27. *Let p be an odd prime number. Then*

$$N_\epsilon(p) = L_\epsilon(p),$$

where $\epsilon \in \{-1, 0, 1\}$.

PROOF. This theorem follows directly from Corollary 4.9. □

In this subsection, we will determine the size of $L_\epsilon(p^k)$ for an odd prime number p, and a positive integer k, hence also for $N_\epsilon(p^k)$. Doing this, we need a theorem which considers the sum over Legendre's symbol of a quadratic polynomial, and two lemmata which have been already proved by K. F. Gauß.

LEMMA 4.28. *Let p be an odd prime number, and let a and k be positive integers. Then*

$$\sum_{x=0}^{p^k-1} \left(\tfrac{x(a-x)}{p^k}\right) = \begin{cases} p^{k-1}(p-1)\left(\tfrac{-1}{p}\right)^k, & \text{if } a \equiv 0 \pmod p \\ -p^{k-1}\left(\tfrac{-1}{p}\right), & \text{if } a \not\equiv 0 \pmod p, \text{ and } k \text{ is odd} \\ p^{k-1}(p-2), & \text{else.} \end{cases}$$

PROOF. If $a \equiv 0 \pmod p$, then

$$\left(\tfrac{x(a-x)}{p^k}\right) = \left(\tfrac{-x^2}{p^k}\right) = \begin{cases} \left(\tfrac{-1}{p^k}\right), & \text{if } x \not\equiv 0 \pmod p \\ 0, & \text{else.} \end{cases}$$

Therefore, we have

$$\sum_{x=0}^{p^k-1} \left(\tfrac{x(a-x)}{p^k}\right) = \varphi(p^k) \cdot \left(\tfrac{-1}{p}\right)^k = p^{k-1}(p-1)\left(\tfrac{-1}{p}\right)^k. \tag{6}$$

If $a \not\equiv 0 \pmod p$, then we have for all $b \in \mathbb{F}_{p^k}^*$ the following identity

$$\sum_{x=0}^{p^k-1} \left(\tfrac{x(a-x)}{p^k}\right) = \sum_{x=0}^{p^k-1} \left(\tfrac{x(b-x)}{p^k}\right), \tag{7}$$

since there exists $c \in \mathbb{F}_{p^k}^*$ with $bc \equiv a \pmod{p^k}$ such that

$$\sum_{x=0}^{p^k-1} \left(\tfrac{x(a-x)}{p^k}\right) = \sum_{d=0}^{p^k-1} \left(\tfrac{cd(a-cd)}{p^k}\right) = \sum_{d=0}^{p^k-1} \left(\tfrac{c^2d(b-d)}{p^k}\right) = \sum_{x=0}^{p^k-1} \left(\tfrac{x(b-x)}{p^k}\right).$$

If k is odd, then

$$0 = \sum_{y=0}^{p^k-1} \sum_{x=0}^{p^k-1} \left(\tfrac{xy}{p^k}\right)$$

$$= \sum_{b=0}^{p^k-1}\sum_{x=0}^{p^k-1}\left(\tfrac{x(b-x)}{p^k}\right)$$

$$\underset{(6),(7)}{=} p^{2(k-1)}(p-1)\left(\tfrac{-1}{p}\right)^k + p^{k-1}(p-1)\sum_{x=0}^{p^k-1}\left(\tfrac{x(a-x)}{p^k}\right).$$

If k is even, then we have the identity

$$\sum_{y=0}^{p^k-1}\sum_{x=0}^{p^k-1}\left(\tfrac{xy}{p^k}\right) = (p^{k-1}(p-1))^2.$$

Combining these two cases, we finally get

$$\sum_{x=0}^{p^k-1}\left(\tfrac{x(a-x)}{p^k}\right) = \begin{cases} -p^{k-1}\left(\tfrac{-1}{p}\right), & \text{if } k \text{ is odd} \\ p^{k-1}(p-2), & \text{else.} \end{cases}$$

□

LEMMA 4.29. *Let p be an odd prime number, and let a, b, and k be positive integers. Then*

$$\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+a}{p^k}\right) = \sum_{x=0}^{p^k-1}\left(\tfrac{x^2+ab^2}{p^k}\right).$$

PROOF. The proof of the assertion follows directly by the following calculation

$$\begin{aligned}
\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+a}{p^k}\right) &= p^{k-1}\left(\tfrac{a}{p^k}\right) + \sum_{x\in\mathbb{F}_{p^k}^*}\left(\tfrac{x^2+a}{p^k}\right) \\
&= p^{k-1}\left(\tfrac{a}{p^k}\right) + \sum_{y\in\mathbb{F}_{p^k}^*}\left(\tfrac{y^{-2}+a}{p^k}\right) \\
&= p^{k-1}\left(\tfrac{a}{p^k}\right) + \sum_{y\in\mathbb{F}_{p^k}^*}\left(\tfrac{y^2}{p^k}\right)\left(\tfrac{y^{-2}+a}{p^k}\right) \\
&= p^{k-1}\left(\tfrac{a}{p^k}\right) + \sum_{y\in\mathbb{F}_{p^k}^*}\left(\tfrac{1+ay^2}{p^k}\right) \\
&= p^{k-1}\left(\tfrac{ab^2}{p^k}\right) + \sum_{x\in\mathbb{F}_{p^k}^*}\left(\tfrac{x^2}{p^k}\right)\left(\tfrac{1+a(\frac{b}{x})^2}{p^k}\right) \\
&= \sum_{x=0}^{p^k-1}\left(\tfrac{x^2+ab^2}{p^k}\right). \quad \square
\end{aligned}$$

THEOREM 4.30. *Let p be an odd prime number, and let a and k be positive integers. Then*

$$\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+a}{p^k}\right)=\begin{cases} p^{k-1}(p-1)\,, & \text{if } a\equiv 0 \pmod p \\ -p^{k-1}\,, & \text{if } a\not\equiv 0 \pmod p \text{ and } k \text{ is odd} \\ p^{k-1}(p-1-(-1)^{\frac{p-1}{2}}\left(\tfrac{a}{p}\right))\,, & \text{else.}\end{cases}$$

PROOF. If $a\equiv 0 \pmod p$, then

$$\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+a}{p^k}\right)=\sum_{x=0}^{p^k-1}\left(\tfrac{x^2}{p^k}\right)=\varphi(p^k)=p^{k-1}(p-1). \tag{8}$$

Let $a\not\equiv 0 \pmod p$. If $\left(\frac{a}{p}\right)=1$, then $\left(\frac{a^{-1}}{p}\right)=1$, and there exists $b\in\mathbb{F}_{p^k}^*$ such that

$$a^{-1}\equiv b^2 \pmod{p^k}.$$

Therefore,

$$\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+a}{p^k}\right)=\left(\tfrac{a^{-1}}{p^k}\right)\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+a}{p^k}\right)=\sum_{x=0}^{p^k-1}\left(\tfrac{(bx)^2+1}{p^k}\right)=\sum_{y=0}^{p^k-1}\left(\tfrac{y^2+1}{p^k}\right). \tag{9}$$

Let $u\in\mathbb{F}_{p^k}^*$ with $\left(\frac{u}{p}\right)=-1$. If $\left(\frac{a}{p}\right)=-1$, then there exists $b\in\mathbb{F}_{p^k}^*$ such that

$$u\equiv ab^2 \pmod{p^k}.$$

Hence, by Lemma 4.29, we have

$$\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+a}{p^k}\right)\underset{(4.29)}{=}\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+u}{p^k}\right). \tag{10}$$

If k is odd, then

$$\begin{aligned} 0 &= \sum_{x=0}^{p^k-1}\sum_{a=0}^{p^k-1}\left(\tfrac{x^2+a}{p^k}\right) \\ &= \sum_{a=0}^{p^k-1}\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+a}{p^k}\right) \\ &\underset{(8),(9),(10)}{=} p^{2(k-1)}(p-1)+\tfrac{p-1}{2}\cdot p^{k-1}\left(\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+1}{p^k}\right)+\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+u}{p^k}\right)\right). \end{aligned}$$

If k is even, then we have the identity

$$\sum_{x=0}^{p^k-1}\sum_{a=0}^{p^k-1}\left(\tfrac{x^2+a}{p^k}\right)=(p^{k-1}(p-1))^2.$$

Therefore,

$$\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+1}{p^k}\right)+\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+u}{p^k}\right)=\begin{cases}-2p^{k-1}\,, & \text{if } k \text{ is odd}\\ 2p^{k-1}(p-1)\,, & \text{else.}\end{cases} \tag{11}$$

The proof of the assertion will be completed by equations (9), (10), (11), and the following two case considerations:

(1) If $\left(\frac{-1}{p}\right)=1$, then there exists $b\in\mathbb{F}_p^*$ such that $b^2\equiv -1 \pmod{p^k}$. By Lemma 4.28, we have

$$\begin{aligned}\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+1}{p^k}\right) &= \sum_{x=0}^{p^k-1}\left(\tfrac{x^2-b^2}{p^k}\right)=\sum_{x=0}^{p^k-1}\left(\tfrac{(x-b)(x+b)}{p^k}\right)=\sum_{y=0}^{p^k-1}\left(\tfrac{y(y-2b)}{p^k}\right)=\sum_{y=0}^{p^k-1}\left(\tfrac{y(2b-y)}{p^k}\right)\\ &\underset{(4.28)}{=}\begin{cases}-p^{k-1}\,, & \text{if } k \text{ is odd}\\ p^{k-1}(p-2)\,, & \text{else.}\end{cases}\end{aligned}$$

(2) If $\left(\frac{-1}{p}\right)=-1$, then from (10), and Lemma 4.28, we have

$$\begin{aligned}\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+u}{p^k}\right) &\underset{(10)}{=} \sum_{x=0}^{p^k-1}\left(\tfrac{x^2-1}{p^k}\right)=\left(\tfrac{-1}{p}\right)^k\sum_{x=0}^{p^k-1}\left(\tfrac{(x+1)(1-x)}{p^k}\right)=\left(\tfrac{-1}{p}\right)^k\sum_{y=0}^{p^k-1}\left(\tfrac{y(2-y)}{p^k}\right)\\ &\underset{(4.28)}{=}\begin{cases}-p^{k-1}\,, & \text{if } k \text{ is odd}\\ p^{k-1}(p-2)\,, & \text{else.}\end{cases}\end{aligned}$$

□

This Theorem 4.30 can easily be extended to all quadratic polynomials.

COROLLARY 4.31. *Let p be an odd prime number, and let a, b, and k be positive integers. Then we have*

$$\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+ax+b}{p^k}\right)=\begin{cases}p^{k-1}(p-1)\,, & \text{if } a^2-4b\equiv 0 \pmod{p}\\ -p^{k-1}\,, & \text{if } a^2-4b\not\equiv 0 \pmod{p} \text{ and } k \text{ is odd}\\ p^{k-1}\left(p-1-(-1)^{\frac{p-1}{2}}\left(\tfrac{a^2-4b}{p}\right)\right)\,, & \text{else.}\end{cases}$$

PROOF. Let $c=\frac{a}{2}$, and $d=c^2$. Then the proof of the assertion follows directly from Theorem 4.30, and the equations

$$\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+ax+b}{p^k}\right)=\sum_{x=0}^{p^k-1}\left(\tfrac{x^2+ax+d+b-d}{p^k}\right)=\sum_{x=0}^{p^k-1}\left(\tfrac{(x+c)^2+(b-d)}{p^k}\right)=\sum_{y=0}^{p^k-1}\left(\tfrac{y^2+(b-d)}{p^k}\right).$$

□

Now we know the exact value of the sum over Jacobi's symbol of a quadratic polynomial. In the following theorem we give an exact value of the size of the three sets $L_{-1}(p^k), L_0(p^k)$, and $L_1(p^k)$ for an odd prime number p, and a positive integer k.

THEOREM 4.32. *Let p be an odd prime number, and let k be a positive integer. Then*

$$|L_1(p^k)| = \begin{cases} \frac{p-3}{2}\cdot p^{k-1}, & \text{if } p\equiv 3 \pmod 4, \text{ and } k \text{ is odd} \\ \frac{p-5}{2}\cdot p^{k-1}, & \text{if } p\equiv 1 \pmod 4, \text{ and } k \text{ is odd} \\ p^{k-1}(p-1), & \text{if } p\equiv 3 \pmod 4, \text{ and } k \text{ is even} \\ p^{k-1}(p-3), & \text{if } p\equiv 1 \pmod 4, \text{ and } k \text{ is even,} \end{cases}$$

$$|L_{-1}(p^k)| = \begin{cases} \frac{p+1}{2}\cdot p^{k-1}, & \text{if } p\equiv 3 \pmod 4, \text{ and } k \text{ is odd} \\ \frac{p-1}{2}\cdot p^{k-1}, & \text{if } p\equiv 1 \pmod 4, \text{ and } k \text{ is odd} \\ 0, & \text{if } p\equiv \pm 1 \pmod 4, \text{ and } k \text{ is even,} \end{cases}$$

$$\text{and} \qquad |L_0(p^k)| = \begin{cases} 0, & \text{if } p\equiv 3 \pmod 4 \\ 2p^{k-1}, & \text{if } p\equiv 1 \pmod 4. \end{cases}$$

Note that $|L_\epsilon(p^k)| \equiv 0 \pmod{p^{k-1}}$ in all cases $\epsilon \in \{-1,0,1\}$.

PROOF. We split up the proof of this theorem into the following five steps:

(1) The equation $x^2 \equiv -4 \pmod{p^k}$ has no solution, if -1 is a quadratic non-residue modulo p. Otherwise, the equation $x^2 \equiv -4 \pmod{p^k}$ has $2p^{k-1}$ solutions, if -1 is a quadratic residue modulo p. Moreover, we have

$$\left(\tfrac{-1}{p}\right) = \begin{cases} -1, & \text{if } p\equiv 3 \pmod 4 \\ 1, & \text{if } p\equiv 1 \pmod 4. \end{cases}$$

Therefore,

$$|L_0(p^k)| = \begin{cases} 0, & \text{if } p\equiv 3 \pmod 4 \\ 2p^{k-1}, & \text{if } p\equiv 1 \pmod 4. \end{cases}$$

(2) We have

$$|L_1(p^k)| + |L_0(p^k)| + |L_{-1}(p^k)| = |\mathbb{F}_{p^k}^*| = \varphi(p^k) = p^{k-1}(p-1).$$

(3) Let $p \equiv 3 \pmod 4$. Then from the first step we have $\left(\frac{x^2+4}{p^k}\right) \neq 0$ for all integers x. By Theorem 4.30, we have

$$\begin{aligned} |L_1(p^k)| &= |\{x \in \mathbb{F}_{p^k}^* \mid \left(\tfrac{x^2+4}{p^k}\right) = 1\}| \\ &= \tfrac{1}{2}\sum_{x\in\mathbb{F}_{p^k}^*} \left(\left(\tfrac{x^2+4}{p^k}\right)+1\right) \\ &= \tfrac{p-1}{2}\cdot p^{k-1} + \tfrac{1}{2}\sum_{x\in\mathbb{F}_{p^k}^*} \left(\tfrac{x^2+4}{p^k}\right) \\ &= \tfrac{p-2}{2}\cdot p^{k-1} + \tfrac{1}{2}\sum_{x=0}^{p^k-1} \left(\tfrac{x^2+4}{p^k}\right) \\ &\underset{(4.30)}{=} \begin{cases} \frac{p-3}{2}\cdot p^{k-1}, & \text{if } k \text{ is odd} \\ p^{k-1}(p-1), & \text{else.} \end{cases} \end{aligned}$$

(4) Let $p \equiv 1 \pmod 4$. Then from the first step we have $\pm a \in \mathbb{F}_{p^k}^*$ such that

$$a^2 \equiv -4 \pmod{p^k}. \tag{12}$$

By Theorem 4.30, we have the following equation analogous to the third step:

$$\begin{aligned}
|L_1(p^k)| &= |\{x \in \mathbb{F}_{p^k}^* \mid \left(\tfrac{x^2+4}{p^k}\right) = 1\}| \\
&\underset{(12)}{=} \frac{1}{2}\left(\sum_{x \in \mathbb{F}_{p^k}^*} \left(\left(\tfrac{x^2+4}{p^k}\right) + 1\right) - \underbrace{|L_0(p^k)|}_{=2p^{k-1}}\right) \\
&= \tfrac{p-1}{2} \cdot p^{k-1} + \frac{1}{2} \sum_{x \in \mathbb{F}_{p^k}^*} \left(\tfrac{x^2+4}{p^k}\right) - p^{k-1} \\
&= \tfrac{p-4}{2} \cdot p^{k-1} + \frac{1}{2} \sum_{x=0}^{p^k-1} \left(\tfrac{x^2+4}{p^k}\right) \\
&\underset{(4.30)}{=} \begin{cases} \frac{p-5}{2} \cdot p^{k-1}, & \text{if } k \text{ is odd} \\ p^{k-1}(p-3), & \text{else.} \end{cases}
\end{aligned}$$

(5) Combining them all, we finally get the proof of the assertion. □

5.2. The Standard Commutator Curve with Composite Modulus. Considering the sets $N_\epsilon(n)$ and $L_\epsilon(n)$ for a composite number n, where $\epsilon \in \{-1, 0, 1\}$, is more difficult than for a prime power as the previous subsection. In this subsection we will give a lower and an upper bound for the two sets $L_1(n)$ and $L_{-1}(n)$, where n is a natural number.
Based on this subsection we will discuss in the next subsection the equality of $N_\epsilon(n)$ and $L_\epsilon(n)$ for a composite number n, where $\epsilon \in \{-1, 0, 1\}$. That consideration is similar to the question about the existence of numbers analogous to the Carmichael Numbers.
From Corollary 4.4 we can directly conclude that the number of elements in each of the three sets of Definition 4.24 is even, which is valid not only for prime numbers.

Corollary 4.33. *Let n be a natural number greater than 2. Then*

$$2 \mid N_{-1}(n), \quad 2 \mid N_0(n), \quad 2 \mid N_1(n).$$

Proof. This can be concluded from Corollary 4.4. □

The same property is also valid for the three sets of Definition 4.26 by the following lemma.

Lemma 4.34. *Let n be a natural number greater than 2. Then*

$$2 \mid L_{-1}(n), \quad 2 \mid L_0(n), \quad 2 \mid L_1(n).$$

Proof. Let $x \in (\mathbb{Z}/n\mathbb{Z})^*$, and $\epsilon \in \{-1, 0, 1\}$ such that $\left(\frac{x^2+4}{n}\right) = \epsilon$. Then

$$\pm x \in L_\epsilon(n). \quad \square$$

In the following two theorems we give an upper and a lower bound for the size of the two sets $L_{-1}(n)$, and $L_1(n)$, where n is an odd squarefree and composite number.

THEOREM 4.35. *Let n be an odd squarefree and composite number. Then*

$$|L_1(n)| \leq \tfrac{\varphi(n)+4}{2}, \quad \textit{and} \quad |L_{-1}(n)| \leq \tfrac{\varphi(n)-4}{2}.$$

PROOF. Let $\prod_{k=1}^{r} p_k$ be the factorization of n.
If $r = 2$ and $n = p_1p_2$, then we have by Theorem 4.32, the Chinese Remainder Theorem 2.5 and the multiplicativity of the Jacobi symbol

$$\begin{aligned}
|L_1(p_1p_2)| &= |L_1(p_1)| \cdot |L_1(p_2)| + |L_{-1}(p_1)| \cdot |L_{-1}(p_2)| \\
&\underset{(4.32)}{\leq} \tfrac{p_1-3}{2} \cdot \tfrac{p_2-3}{2} + \tfrac{p_1+1}{2} \cdot \tfrac{p_2+1}{2} \\
&= \tfrac{p_1p_2-3p_1-3p_2+9}{4} + \tfrac{p_1p_2+p_1+p_2+1}{4} \\
&= \tfrac{p_1p_2-p_1-p_2+5}{2} \\
&= \tfrac{\varphi(p_1p_2)+4}{2},
\end{aligned}$$

and

$$\begin{aligned}
|L_{-1}(p_1p_2)| &= |L_{-1}(p_1)| \cdot |L_1(p_2)| + |L_1(p_1)| \cdot |L_{-1}(p_2)| \\
&\underset{(4.32)}{\leq} \tfrac{p_1+1}{2} \cdot \tfrac{p_2-3}{2} + \tfrac{p_1-3}{2} \cdot \tfrac{p_2+1}{2} \\
&= \tfrac{p_1p_2-3p_1-p_2-3}{4} + \tfrac{p_1p_2+p_1-3p_2-3}{4} \\
&= \tfrac{p_1p_2-p_1-p_2-3}{2} \\
&= \tfrac{\varphi(p_1p_2)-4}{2}.
\end{aligned}$$

We proceed by induction on r. Let $n = mp$, where p is prime, and assume that we have by induction

$$|L_1(m)| \leq \tfrac{\varphi(m)+4}{2}, \quad \text{and} \quad |L_{-1}(m)| \leq \tfrac{\varphi(m)-4}{2}. \tag{13}$$

Then, from the Chinese Remainder Theorem 2.5 and the multiplicativity of the Jacobi symbol, we have by the inductional assumption

$$\begin{aligned}
|L_1(mp)| &= |L_1(m)| \cdot |L_1(p)| + |L_{-1}(m)| \cdot |L_{-1}(p)| \\
&\underset{(13),(4.32)}{\leq} \tfrac{\varphi(m)+4}{2} \cdot \tfrac{\varphi(p)-2}{2} + \tfrac{\varphi(m)-4}{2} \cdot \tfrac{\varphi(p)+2}{2} \\
&= \tfrac{\varphi(mp)-2\varphi(m)+4\varphi(p)-8}{4} + \tfrac{\varphi(mp)-4\varphi(p)+2\varphi(m)-8}{4} \\
&= \tfrac{\varphi(mp)-8}{2} \\
&< \tfrac{\varphi(mp)+4}{2}.
\end{aligned}$$

Obviously, the proof of the estimate $|L_{-1}(mp)| < \frac{\varphi(mp)-4}{2}$ is analogous. □

THEOREM 4.36. *Let n be a squarefree odd composite number with prime factorization $\prod_{k=1}^{r} p_k$. Then*

$$|L_\epsilon(n)| \geq \begin{cases} \frac{1}{2}\prod_{k=1}^{r}(p_k-3) - \epsilon\cdot(-2)^{r-1}\,, & p_1 \equiv 1 \pmod 4 \\ \frac{p_1-1}{2}\prod_{k=2}^{r}(p_k-3) - \epsilon\cdot(-2)^{r-1}\,, & p_1 \equiv 3 \pmod 4, \end{cases}$$

where $\epsilon \in \{\pm 1\}$.

PROOF. If $r=2$, $p_1 \equiv 1 \pmod 4$, and $n = p_1p_2$, then we have by Theorem 4.32, the Chinese Remainder Theorem 2.5, and the multiplicativity of the Jacobi symbol

$$\begin{aligned} |L_1(p_1p_2)| &= |L_1(p_1)|\cdot|L_1(p_2)| + |L_{-1}(p_1)|\cdot|L_{-1}(p_2)| \\ &\underset{(4.32)}{\geq} \tfrac{p_1-5}{2}\cdot\tfrac{p_2-5}{2} + \tfrac{p_1-1}{2}\cdot\tfrac{p_2-1}{2} \\ &= \tfrac{p_1p_2-5p_1-5p_2+25}{4} + \tfrac{p_1p_2-p_1-p_2+1}{4} \\ &= \tfrac{p_1p_2-3p_1-3p_2+13}{2} \\ &= \tfrac{(p_1-3)(p_2-3)}{2} + 2, \end{aligned}$$

and

$$\begin{aligned} |L_{-1}(p_1p_2)| &= |L_{-1}(p_1)|\cdot|L_1(p_2)| + |L_1(p_1)|\cdot|L_{-1}(p_2)| \\ &\underset{(4.32)}{\geq} \tfrac{p_1-1}{2}\cdot\tfrac{p_2-5}{2} + \tfrac{p_1-5}{2}\cdot\tfrac{p_2-1}{2} \\ &= \tfrac{p_1p_2-5p_1-p_2+5}{4} + \tfrac{p_1p_2-p_1-5p_2+5}{4} \\ &= \tfrac{p_1p_2-3p_1-3p_2+5}{2} \\ &= \tfrac{(p_1-3)(p_2-3)}{2} - 2. \end{aligned}$$

If $r=2$, $p_1 \equiv 3 \pmod 4$, and $n = p_1p_2$, then similar to the previous case we get

$$\begin{aligned} |L_1(p_1p_2)| &= |L_1(p_1)|\cdot|L_1(p_2)| + |L_{-1}(p_1)|\cdot|L_{-1}(p_2)| \\ &\underset{(4.32)}{\geq} \tfrac{p_1-3}{2}\cdot\tfrac{p_2-5}{2} + \tfrac{p_1+1}{2}\cdot\tfrac{p_2-1}{2} \\ &= \tfrac{p_1p_2-5p_1-3p_2+15}{4} + \tfrac{p_1p_2-p_1+p_2-1}{4} \\ &= \tfrac{p_1p_2-3p_1-p_2+7}{2} \\ &= \tfrac{(p_1-1)(p_2-3)}{2} + 2, \end{aligned}$$

and

$$\begin{aligned} |L_{-1}(p_1p_2)| &= |L_{-1}(p_1)|\cdot|L_1(p_2)| + |L_1(p_1)|\cdot|L_{-1}(p_2)| \\ &\underset{(4.32)}{\geq} \tfrac{p_1+1}{2}\cdot\tfrac{p_2-5}{2} + \tfrac{p_1-3}{2}\cdot\tfrac{p_2-1}{2} \\ &= \tfrac{p_1p_2-5p_1+p_2-5}{4} + \tfrac{p_1p_2-p_1-3p_2+3}{4} \\ &= \tfrac{p_1p_2-3p_1-p_2-1}{2} \\ &= \tfrac{(p_1-1)(p_2-3)}{2} - 2. \end{aligned}$$

We proceed by induction on r. Let $mp_{r+1} = \prod_{k=1}^{r+1} p_r$ be the prime factorization of n, and assume that we have by induction

$$|L_\epsilon(m)| \geq \begin{cases} \frac{1}{2}\prod_{k=1}^{r}(p_k-3) - \epsilon\cdot(-2)^{r-1}\,, & p_1 \equiv 1 \pmod 4 \\ \frac{p_1-1}{2}\prod_{k=2}^{r}(p_k-3) - \epsilon\cdot(-2)^{r-1}\,, & p_1 \equiv 3 \pmod 4, \end{cases} \tag{14}$$

where $\epsilon \in \{\pm 1\}$. If $p_1 \equiv 1 \pmod 4$, then from the Chinese Remainder Theorem 2.5, and the multiplicativity of the Jacobi symbol, we have by the inductional assumption

$$\begin{aligned} |L_1(mp_{r+1})| &= |L_1(m)|\cdot|L_1(p_{r+1})| + |L_{-1}(m)|\cdot|L_{-1}(p_{r+1})| \\ &\underset{(14),(4.32)}{\geq} \tfrac{p_{r+1}-5}{2}\cdot\tfrac{1}{2}\Big(\prod_{k=1}^{r}(p_k-3) - (-2)^{r-1}\Big) \\ &\quad + \tfrac{p_{r+1}-1}{2}\cdot\tfrac{1}{2}\Big(\prod_{k=1}^{r}(p_k-3) + (-2)^{r-1}\Big) \\ &= \tfrac{p_{r+1}-3}{2}\prod_{k=1}^{r}(p_k-3) + 2\cdot(-2)^{r-1} \\ &> \tfrac{1}{2}\prod_{k=1}^{r+1}(p_k-3) - (-2)^r. \end{aligned}$$

Obviously, the proof of the estimate $|L_{-1}(mp_{r+1})| \geq \frac{1}{2}\prod_{k=1}^{r+1}(p_k-3) + (-2)^r$ is analogous to the estimate given above.
If $p_1 \equiv 3 \pmod 4$, then the proof is similar to the previous case. □

COROLLARY 4.37. *Let $n > 15$ be a squarefree odd natural number. Then*

$$|L_\epsilon(n)| > 0,$$

where $\epsilon \in \{\pm 1\}$.

PROOF. If n is composite, then this corollary follows directly from Theorem 4.36. Otherwise, if n is prime, then this corollary follows directly from Theorem 4.32. □

THEOREM 4.38. *Let n be an odd composite number with prime factorization $\prod_{k=1}^{r} p_k^{a_k}$ such that a_1 is odd. Then*

$$|L_0(n) \cup L_\epsilon(n)| \geq \tfrac{\varphi(n)}{2} - \epsilon\cdot(-2)^{r-1}\prod_{k=1}^{r} p_k^{a_k-1}\big(1 - \delta_k\cdot\tfrac{p_k+1}{2}\big),$$

where $\epsilon \in \{\pm 1\}$, and $\delta_k = \begin{cases} 0\,, & \text{if } a_k \text{ is odd} \\ 1\,, & \text{else.} \end{cases}$

PROOF. Assume $r = 2$ and $n = p_1^{a_1}p_2^{a_2}$.
If a_2 is odd, then we have by Theorem 4.32, the Chinese Remainder Theorem 2.5, and

the multiplicativity of the Jacobi symbol

$$\begin{aligned}
|L_0(p_1^{a_1}p_2^{a_2}) \cup L_1(p_1^{a_1}p_2^{a_2})| &= |L_0(p_1^{a_1}) \cup L_1(p_1^{a_1})| \cdot |L_0(p_2^{a_2}) \cup L_1(p_2^{a_2})| \\
&\quad + |L_0(p_1^{a_1}) \cup L_{-1}(p_1^{a_1})| \cdot |L_0(p_2^{a_2}) \cup L_{-1}(p_2^{a_2})| \\
&\quad - |L_0(p_1^{a_1})| \cdot |L_0(p_2^{a_2})| \\
&\underset{(4.32)}{\geq} (\tfrac{p_1-3}{2} \cdot \tfrac{p_2-3}{2} + \tfrac{p_1+1}{2} \cdot \tfrac{p_2+1}{2}) \cdot p_1^{a_1-1}p_2^{a_2-1} \\
&= (\tfrac{p_1p_2-3p_1-3p_2+9}{4} + \tfrac{p_1p_2+p_1+p_2+1}{4}) \cdot p_1^{a_1-1}p_2^{a_2-1} \\
&= \tfrac{p_1p_2-p_1-p_2+5}{2} \cdot p_1^{a_1-1}p_2^{a_2-1} \\
&= \tfrac{\varphi(p_1p_2)}{2} + 2p_1^{a_1-1}p_2^{a_2-1},
\end{aligned}$$

and

$$\begin{aligned}
|L_0(p_1^{a_1}p_2^{a_2}) \cup L_{-1}(p_1^{a_1}p_2^{a_2})| &= |L_0(p_1^{a_1}) \cup L_{-1}(p_1^{a_1})| \cdot |L_0(p_2^{a_2}) \cup L_1(p_2^{a_2})| \\
&\quad + |L_0(p_1^{a_1}) \cup L_1(p_1^{a_1})| \cdot |L_0(p_2^{a_2}) \cup L_{-1}(p_2^{a_2})| \\
&\quad - |L_0(p_1^{a_1})| \cdot |L_0(p_2^{a_2})| \\
&\underset{(4.32)}{\geq} (\tfrac{p_1+1}{2} \cdot \tfrac{p_2-3}{2} + \tfrac{p_1-3}{2} \cdot \tfrac{p_2+1}{2}) \cdot p_1^{a_1-1}p_2^{a_2-1} \\
&= (\tfrac{p_1p_2-3p_1+p_2-3}{4} + \tfrac{p_1p_2+p_1-3p_2-3}{4}) \cdot p_1^{a_1-1}p_2^{a_2-1} \\
&= \tfrac{p_1p_2-p_1-p_2-3}{2} \cdot p_1^{a_1-1}p_2^{a_2-1} \\
&= \tfrac{\varphi(p_1p_2)}{2} - 2p_1^{a_1-1}p_2^{a_2-1}.
\end{aligned}$$

If a_2 is even, then similar to the previous case we get

$$\begin{aligned}
|L_0(p_1^{a_1}p_2^{a_2}) \cup L_1(p_1^{a_1}p_2^{a_2})| &\underset{(4.32)}{\geq} \tfrac{p_1-3}{2} \cdot (p_2-1) \cdot p_1^{a_1-1}p_2^{a_2-1} \\
&= \tfrac{p_1p_2-p_1-3p_2+3}{2} \cdot p_1^{a_1-1}p_2^{a_2-1} \\
&= \tfrac{\varphi(p_1p_2)}{2} - (p_2-1)p_1^{a_1-1}p_2^{a_2-1},
\end{aligned}$$

and

$$\begin{aligned}
|L_0(p_1^{a_1}p_2^{a_2}) \cup L_{-1}(p_1^{a_1}p_2^{a_2})| &\underset{(4.32)}{\geq} \tfrac{p_1+1}{2} \cdot (p_2-1) \cdot p_1^{a_1-1}p_2^{a_2-1} \\
&= \tfrac{p_1p_2-p_1+p_2+1}{2} \cdot p_1^{a_1-1}p_2^{a_2-1} \\
&= \tfrac{\varphi(p_1p_2)}{2} + p_1^{a_1-1}p_2^{a_2} \\
&> \tfrac{\varphi(p_1p_2)}{2} + (p_2-1)p_1^{a_1-1}p_2^{a_2-1}.
\end{aligned}$$

We proceed by induction on r. Let $mp_{r+1} = \prod_{k=1}^{r+1} p_r$ be the prime factorization of n, and assume that we have by induction

$$|L_0(m) \cup L_\epsilon(m)| \geq \tfrac{\varphi(m)}{2} - \epsilon \cdot (-2)^{r-1} \prod_{k=1}^{r-1} p_k^{a_k-1}(1 - \delta_k \cdot \tfrac{p_k+1}{2}), \tag{15}$$

where $\epsilon \in \{\pm 1\}$.
If a_{r+1} is odd, then, from the Chinese Remainder Theorem 2.5, and the multiplicativity

of the Jacobi symbol, we have by the inductional assumption

$$\begin{aligned}
& |L_0(mp_{r+1}) \cup L_1(mp_{r+1})| \\
= \quad & |L_0(p_{r+1}) \cup L_1(p_{r+1})| \cdot |L_0(m) \cup L_1(m)| \\
& + |L_0(p_{r+1}) \cup L_{-1}(p_{r+1})| \cdot |L_0(m) \cup L_{-1}(m)| - |L_0(p_{r+1})| \cdot |L_0(m)| \\
\underset{(15),(4.32)}{\geq} \quad & \tfrac{p_{r+1}-3}{2} \cdot p_{r+1}^{a_{r+1}-1}(\tfrac{\varphi(m)}{2} - (-2)^{r-1} \prod_{k=1}^{r-1} p_k^{a_k-1}(1 - \delta_k \cdot \tfrac{p_k+1}{2})) \\
& + \tfrac{p_{r+1}+1}{2} \cdot p_{r+1}^{a_{r+1}-1}(\tfrac{\varphi(m)}{2} + (-2)^{r-1} \prod_{k=1}^{r-1} p_k^{a_k-1}(1 - \delta_k \cdot \tfrac{p_k+1}{2})) \\
\underset{(\delta_{r+1}=0)}{=} \quad & \tfrac{\varphi(mp_{r+1})}{2} - (-2)^r \prod_{k=1}^{r} p_k^{a_k-1}(1 - \delta_k \cdot \tfrac{p_k+1}{2}).
\end{aligned}$$

Similarly, if a_{r+1} is even, then we have by the inductional assumption

$$\begin{aligned}
& |L_0(mp_{r+1}) \cup L_1(mp_{r+1})| \\
= \quad & |L_0(p_{r+1}) \cup L_1(p_{r+1})| \cdot |L_0(m) \cup L_1(m)| \\
& + |L_0(p_{r+1}) \cup L_{-1}(p_{r+1})| \cdot |L_0(m) \cup L_{-1}(m)| - |L_0(p_{r+1})| \cdot |L_0(m)| \\
\underset{(15),(4.32)}{\geq} \quad & (p_{r+1}-1)p_{r+1}^{a_{r+1}-1}(\tfrac{\varphi(m)}{2} - (-2)^{r-1} \prod_{k=1}^{r-1} p_k^{a_k-1}(1 - \delta_k \cdot \tfrac{p_k+1}{2})) \\
\underset{(\delta_{r+1}=1)}{=} \quad & \tfrac{\varphi(mp_{r+1})}{2} - (-2)^r \prod_{k=1}^{r} p_k^{a_k-1}(1 - \delta_k \cdot \tfrac{p_k+1}{2}).
\end{aligned}$$

Obviously, the proof of the estimate

$$|L_0(mp_{r+1}) \cup L_{-1}(mp_{r+1})| \geq \tfrac{\varphi(mp_{r+1})}{2} + (-2)^r \prod_{k=1}^{r} p_k^{a_k-1}(1 - \delta_k \cdot \tfrac{p_k+1}{2})$$

is analogous to the one given above. □

By the results of this subsection, we can now prove the third item of Observation 4.14.

THEOREM 4.39. *Let n be a squarefree odd natural number. Then we have exactly two numbers $x_1, x_2 \in (\mathbb{Z}/n\mathbb{Z})^*$ such that*

$$\operatorname{ord}(c(1, x_1)) = \operatorname{ord}(c(1, x_2)) = 2n$$

if and only if n is a prime number with $n \equiv 1 \pmod 4$, and $x_1^2 \equiv x_2^2 \equiv -4 \pmod n$.

PROOF. "⇒": Let p be a prime divisor of n. Then we have

$$c(1, x_1)^{2n} \equiv c(1, x_2)^{2n} \equiv I_2 \pmod p.$$

By Lagrange's Theorem 2.11, and Theorem 2.17, we get

$$c(1, x_1)^{2p} \equiv c(1, x_2)^{2p} \equiv I_2 \pmod p.$$

Therefore, by Corollary 4.9, we have

$$\left(\tfrac{x_1^2+4}{p}\right) = \left(\tfrac{x_2^2+4}{p}\right) = 0.$$

Thus,

$$\left(\tfrac{x_1^2+4}{n}\right) = \left(\tfrac{x_2^2+4}{n}\right) = 0.$$

Suppose n is a natural number with r distinct prime divisors. Then every prime divisor of n must be congruent 1 modulo 4. Otherwise, we do not have a solution for the congruence $x^2 \equiv -4 \pmod{n}$ in $(\mathbb{Z}/n\mathbb{Z})^*$. This gives us 2^r solutions. But since we have only two solutions x_1, x_2 for the congruence above, we get $r = 1$. Therefore, n is a prime number.
"$\Leftarrow$": The proof of this direction follows from Corollary 4.9, Theorem 4.27, and Theorem 4.32. □

5.3. How Frequent does an Order of a Point on the Standard Commutator Curve Occur? In this subsection, we will prove the fourth item of Observation 4.14. Therefore, we start with proving one lemma which considers the frequency of an order of a point on the standard commutator curve which divides $p-1$, and then another lemma in which we consider $p+1$ instead.

LEMMA 4.40. *Let p be an odd prime number, and $a \in \mathbb{F}_p^*$ such that $\operatorname{ord}(a) = p-1$. Then the map*

$$\alpha : A \to B : a^{2k} \mapsto \begin{cases} c(1, a^k - a^{-k}), & \text{if } 1 \le k < \frac{p-1}{4} \\ c(1, a^{-k} - a^k), & \text{if } \frac{p-1}{4} < k \le \frac{p-3}{2} \end{cases}$$

with

$$A := \{a^{2k} \mid k \in \mathbb{N}_{>0}, k \le \tfrac{p-3}{2}, k \ne \tfrac{p-1}{4}\},$$

and

$$B := \{M \in C_p^1 \mid \operatorname{ord}(M) \mid \tfrac{p-1}{2}\}$$

is bijective and order-preserving, i.e.

$$\operatorname{ord}(\alpha(a^{2k})) = \operatorname{ord}(a^{2k}) = \tfrac{p-1}{\gcd(p-1,2k)}$$

for positive integers $k \le \frac{p-3}{2}$ with $k \ne \frac{p-1}{4}$.

PROOF. We prove this lemma in three steps that the map α is injective and surjective, hence bijective, and order-preserving.

Injective: Let $a^{2k}, a^{2l} \in A$ with $1 \le k, l < \frac{p-1}{4}$ such that

$$c(1, a^k - a^{-k}) = \alpha(a^{2k}) \equiv \alpha(a^{2l}) = c(1, a^l - a^{-l}) \pmod{p}.$$

Then, by Definition 4.5, we have

$$a^{-k} - a^{-l} \equiv a^k - a^l = a^{k+l}(a^{-l} - a^{-k}) \pmod{p}.$$

Thus,

$$a^{k+l} \equiv -1 \equiv a^{\frac{p-1}{2}} \pmod{p} \qquad \text{or} \qquad a^k \equiv a^l \pmod{p}.$$

By $1 \leq k, l < \frac{p-1}{4}$, we have

$$a^{k+l} \not\equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Therefore,

$$a^{2k} \equiv a^{2l} \pmod{p}.$$

Similarly, we get $a^{2k} \equiv a^{2l} \pmod{p}$ for $\frac{p-1}{4} < k, l \leq \frac{p-3}{2}$.

Suppose $1 \leq k < \frac{p-1}{4}$ and $\frac{p-1}{4} < l \leq \frac{p-3}{2}$. Then, by Definition 4.5, we have

$$a^{-k} + a^{-l} \equiv a^k + a^l = a^{k+l}(a^{-l} + a^{-k}) \pmod{p}.$$

Thus,

$$a^{k+l} \equiv 1 \equiv a^{p-1} \pmod{p} \qquad \text{or} \qquad a^k \equiv -a^l \equiv a^{\frac{p-1}{2}+l} \pmod{p}.$$

Therefore,

$$k + l \equiv 0 \pmod{p-1} \qquad \text{or} \qquad k - l \equiv 0 \pmod{\tfrac{p-1}{2}},$$

which contradict $1 \leq k < \frac{p-1}{4}$ and $\frac{p-1}{4} < l \leq \frac{p-3}{2}$.

Similarly, we get a contradiction for $\frac{p-1}{4} < k \leq \frac{p-3}{2}$ and $1 \leq l < \frac{p-1}{4}$.

Surjective: We have $\operatorname{ord}(a) = p - 1$. Therefore,

$$\begin{aligned} |A| &= |\{k \in \mathbb{N}_{>0} \mid k \leq \tfrac{p-3}{2}, k \neq \tfrac{p-1}{4}\}| \\ &= \begin{cases} \frac{p-3}{2}, & \text{if } p \equiv 3 \pmod 4 \\ \frac{p-5}{2}, & \text{if } p \equiv 1 \pmod 4. \end{cases} \end{aligned}$$

Thus, it follows by a forward reference on Theorem 4.53 (which is not critical)

$$\begin{aligned} |A| &\underset{(4.32)}{=} |L_1(p)| \\ &\underset{(4.27)}{=} |N_1(p)| \\ &\underset{(4.24)}{=} |\{x \in \mathbb{F}_p^* \mid c(1,x)^{p-1} \equiv I_2 \pmod p\}| \\ &\underset{(4.53)}{=} |\{x \in \mathbb{F}_p^* \mid c(1,x)^{\frac{p-1}{2}} \equiv I_2 \pmod p\}| \\ &= |B|. \end{aligned}$$

Order-preserving: Let k be a positive integer with $k \leq \frac{p-3}{2}$ and $k \neq \frac{p-1}{4}$. By $\operatorname{ord}(a) = p - 1$, we have $\operatorname{ord}(a^{2k}) = \frac{p-1}{\gcd(p-1,2k)}$. Therefore, we have to show that

$$\operatorname{ord}(c(1, \epsilon(a^k - a^{-k}))) = \operatorname{ord}(\alpha(a^{2k})) = \operatorname{ord}(a^{2k})$$

where $\epsilon \in \{\pm 1\}$. By the matrix

$$\begin{aligned} M &:= c(1, \epsilon(a^k - a^{-k})) \\ &\underset{(4.5)}{=} \begin{pmatrix} \epsilon(a^k - a^{-k}) + a^{2k} + a^{-2k} - 1 & \epsilon(a^k - a^{-k}) \\ 2 - a^{2k} - a^{-2k} & 1 - \epsilon(a^k - a^{-k}) \end{pmatrix}, \end{aligned}$$

we get the characteristic polynomial

$$\chi_M(t) = t^2 - (a^{2k} + a^{-2k})t + 1 = (t - a^{2k})(t - a^{-2k}).$$

Hence,

$$\operatorname{ord}(\alpha(a^{2k})) = \operatorname{ord}(c(1, \epsilon(a^k - a^{-k}))) = \operatorname{ord}(a^{2k}). \quad \square$$

EXAMPLE 4.41. *Let $p = 13$, and $a = 2$. Then, by the table of Example 4.12, we get the following sets*

$$A = \{3, 4, 9, 10\} \equiv \{2^4, 2^2, 2^8, 2^{10}\} \pmod{13},$$

and

$$\begin{aligned} B = \{ \quad & c(1, 2^2 - 2^{-2}) \equiv c(1, 4 - 10) \equiv c(1, 7) \pmod{13}, \\ & c(1, 2^1 - 2^{-1}) \equiv c(1, 2 - 7) \equiv c(1, 8) \pmod{13}, \\ & c(1, 2^{-4} - 2^4) \equiv c(1, 9 - 3) = c(1, 6) \pmod{13}, \\ & c(1, 2^{-5} - 2^5) \equiv c(1, 11 - 6) = c(1, 5) \pmod{13}\}, \end{aligned}$$

which are an example for the previous Lemma 4.40.

LEMMA 4.42. *Let p be an odd prime number, and $a \in \mathbb{F}_{p^2}^*$ such that $\operatorname{ord}(a) = 2(p+1)$. Then the map*

$$\alpha : A \to B : a^{2k} \mapsto \begin{cases} c(1, a^k - a^{-k}), & \text{if } 1 \le k < \frac{p+1}{2} \\ c(1, a^{-k} - a^k), & \text{if } \frac{p+1}{2} < k \le p+1 \end{cases}$$

with

$$A := \{a^{2k} \mid k \in \mathbb{N}_{>0}, 2 \nmid k, k \le p+1, k \ne \tfrac{p+1}{2}\},$$

and

$$B := \{M \in C_p^1 \mid \operatorname{ord}(M) \mid p+1\}$$

is bijective and order-preserving, i.e.

$$\operatorname{ord}(\alpha(a^{2k})) = \operatorname{ord}(a^{2k}) = \tfrac{p+1}{\gcd(p+1,k)}$$

for odd positive integers $k \le p+1$ with $k \ne \frac{p+1}{2}$.

PROOF. We prove this lemma in three steps that the map α is injective and surjective, hence bijective, and order-preserving.

Injective: Let $a^{2k}, a^{2l} \in A$ with k, l odd and $1 \le k, l < \frac{p+1}{2}$ such that

$$c(1, a^k - a^{-k}) = \alpha(a^{2k}) \equiv \alpha(a^{2l}) = c(1, a^l - a^{-l}) \pmod{p}.$$

Then, by Definition 4.5, we have

$$a^{-k} - a^{-l} \equiv a^k - a^l = a^{k+l}(a^{-l} - a^{-k}) \pmod{p}.$$

Thus,

$$a^{k+l} \equiv -1 \equiv a^{p+1} \pmod{p} \qquad \text{or} \qquad a^k \equiv a^l \pmod{p}.$$

By $1 \le k, l < \frac{p+1}{2}$, we have

$$a^{k+l} \not\equiv a^{p+1} \pmod{p}.$$

Therefore,

$$a^{2k} \equiv a^{2l} \pmod{p}.$$

Similarly, we get $a^{2k} \equiv a^{2l} \pmod{p}$ for k, l odd and $\frac{p+1}{2} < k, l \leq p+1$.
Suppose k, l is odd, $1 \leq k < \frac{p+1}{2}$ and $\frac{p+1}{2} < l \leq p+1$. Then, by Definition 4.5, we have

$$a^{-k} + a^{-l} \equiv a^k + a^l = a^{k+l}(a^{-l} + a^{-k}) \pmod{p}.$$

Thus,

$$a^{k+l} \equiv 1 \equiv a^{2(p+1)} \pmod{p} \qquad \text{or} \qquad a^k \equiv -a^l \equiv a^{p+1+l} \pmod{p}.$$

Therefore,

$$k + l \equiv 0 \pmod{2(p+1)} \qquad \text{or} \qquad k - l \equiv 0 \pmod{p+1},$$

which contradict $1 \leq k < \frac{p+1}{2}$ and $\frac{p+1}{2} < l \leq p+1$.
Similarly, we get a contradiction for $\frac{p+1}{2} < k \leq p+1$ and $1 \leq l < \frac{p+1}{2}$.

Surjective: We have $\operatorname{ord}(a) = 2(p+1)$. Therefore,

$$\begin{aligned} |A| &= |\{k \in \mathbb{N}_{>0} \mid 2 \nmid k, k \leq p+1, k \neq \tfrac{p+1}{2}\}| \\ &= \begin{cases} \frac{p+1}{2}, & \text{if } p \equiv 3 \pmod{4} \\ \frac{p-1}{2}, & \text{if } p \equiv 1 \pmod{4}. \end{cases} \end{aligned}$$

Thus,

$$\begin{aligned} |A| &\underset{(4.32)}{=} |L_1(p)| \\ &\underset{(4.27)}{=} |N_1(p)| \\ &\underset{(4.24)}{=} |\{x \in \mathbb{F}_p^* \mid c(1,x)^{p+1} \equiv I_2 \pmod{p}\}| \\ &= |B|. \end{aligned}$$

Order-preserving: Let k be an odd positive integer with $k \leq p+1$ and $k \neq \frac{p+1}{2}$. By $\operatorname{ord}(a) = 2(p+1)$, we have $\operatorname{ord}(a^{2k}) = \frac{p+1}{\gcd(p+1,k)}$. Therefore, we have to show that

$$\operatorname{ord}(c(1, \epsilon(a^k - a^{-k}))) = \operatorname{ord}(\alpha(a^{2k})) = \operatorname{ord}(a^{2k})$$

where $\epsilon \in \{\pm 1\}$. By the matrix

$$\begin{aligned} M &:= c(1, \epsilon(a^k - a^{-k})) \\ &\underset{(4.5)}{=} \begin{pmatrix} \epsilon(a^k - a^{-k}) + a^{2k} + a^{-2k} - 1 & \epsilon(a^k - a^{-k}) \\ 2 - a^{2k} - a^{-2k} & 1 - \epsilon(a^k - a^{-k}) \end{pmatrix}, \end{aligned}$$

we get the characteristic polynomial

$$\chi_M(t) = t^2 - (a^{2k} + a^{-2k})t + 1 = (t - a^{2k})(t - a^{-2k}).$$

Hence,

$$\operatorname{ord}(\alpha(a^{2k})) = \operatorname{ord}(c(1, \epsilon(a^k - a^{-k}))) = \operatorname{ord}(a^{2k}). \quad \square$$

By the previous lemmata, we know which orders on the standard commutator curve occur, and from the following theorem we get the frequency of an occuring order on the curve.

THEOREM 4.43. *Let p be a prime number, and $x \in \mathbb{F}_p^*$ such that* $\operatorname{ord}(c(1,x)) \nmid 2p$. *Then*

$$|\{y \in \mathbb{F}_p^* \mid \operatorname{ord}(c(1,y)) = \operatorname{ord}(c(1,x))\}| = \varphi(\operatorname{ord}(c(1,x))).$$

PROOF. Let d be a positive integer such that $d \mid p-1$. Then we have $\varphi(d)$ elements with the order equal to d in $\mathbb{F}_p^*$. If $\operatorname{ord}(c(1,x)) \mid p-1$, then the proof of the assertion is complete by Lemma 4.40. Otherwise, if $\operatorname{ord}(c(1,x)) \mid p+1$, then the proof of the assertion follows from Lemma 4.42. □

An interesting result is given by the following theorem that the group G, which is generated by all points on the standard commutator curve, is equal to $SL_2(p)$ if p is a prime number greater than 3; hence G is perfect.

THEOREM 4.44. *Let p be a prime number greater than* 3. *Then*

$$\langle c(1,x) \mid x \in \mathbb{F}_p^* \rangle = SL_2(p).$$

PROOF. By Lemma 4.40, and Lemma 4.42, we have $x_1, x_2 \in \mathbb{F}_p^*$ with

$$\operatorname{ord}(c(1,x_1)) = \tfrac{p-1}{2} \quad \text{and} \quad \operatorname{ord}(c(1,x_2)) = p+1.$$

If $p \equiv 1 \pmod 4$, then by Theorem 4.39, we have a $x_3 \in \mathbb{F}_p^*$ with $\operatorname{ord}(c(1,x_3)) = 2p$. Therefore,

$$\begin{aligned} |\langle c(1,x_1), c(1,x_2), c(1,x_3)\rangle| &\geq \operatorname{lcm}(\operatorname{ord}(c(1,x_1)), \operatorname{ord}(c(1,x_2), \operatorname{ord}(c(1,x_3)))) \\ &= \tfrac{p-1}{4} \cdot (p+1)p \\ &\underset{(2.17)}{=} \tfrac{|SL_2(p)|}{4}. \end{aligned}$$

By 8.27 in [**57**] on page 213 and easy calculations, the index

$$|SL_2(p) : \langle c(1,x_1), c(1,x_2), c(1,x_3)\rangle| \leq 4$$

must be equal to 1. Therefore,

$$\langle c(1,x_1), c(1,x_2), c(1,x_3)\rangle = SL_2(p).$$

If $p \equiv 3 \pmod 4$, then

$$|\langle c(1,x_1), c(1,x_2)\rangle| \geq \operatorname{lcm}(\operatorname{ord}(c(1,x_1)), \operatorname{ord}(c(1,x_2))) = \tfrac{p-1}{2} \cdot (p+1).$$

By 8.27 in [**57**] on page 213 and easy calculations, the index

$$|SL_2(p) : \langle c(1,x_1), c(1,x_2)\rangle| \leq 2p$$

must be equal to 1 for $p > 11$. Therefore,

$$\langle c(1,x_1), c(1,x_2)\rangle = SL_2(p).$$

If $p \in \{5, 7, 11\}$, then we can easily verify the results of the following table by calculating:

p	$\lvert SL_2(p)\rvert$	$\lvert\langle c(1,x) \mid x \in \mathbb{F}_p^*\rangle\rvert$
5	120	120
7	336	336
11	1320	1320

□

Theorem 4.44 is not correct for the prime numbers 2 and 3:

p	$\lvert SL_2(p)\rvert$	$\lvert\langle c(1,x) \mid x \in \mathbb{F}_p^*\rangle\rvert$
2	6	3
3	24	8

Comment: In all cases $\langle c(1,x) \mid x \in \mathbb{F}_p^*\rangle$ is the commutator subgroup of $SL_2(p)$. Recall that $SL_2(p)$ is solvable for $p \in \{2,3\}$.

5.4. Numbers Analogous to the Carmichael Numbers. In this subsection we will see that $N_\epsilon(n)$ is not equal to $L_\epsilon(n)$ for a composite number n, where $\epsilon \in \{\pm 1\}$.

(1) In the first theorem, we will prove that if such an LN-number exists, this number must be squarefree.
(2) In the second theorem, we will prove that an LN-number cannot exist.
(3) In two lemmata and another theorem, we consider specific divisibility relations.

Before we prove the theorems of this section, we state a well known fact which is fundamental for this subsection.

LEMMA 4.45. *Let n be an odd natural number. Then*

$$\gcd(n-1, n+1) = 2.$$

PROOF. Since $n-1$ and $n+1$ are even, the lemma follows directly from the equation $(n+1)-(n-1) = 2$. □

THEOREM 4.46. *Let n be an odd composite number. If we have for every integer x with $\epsilon(n) = \left(\frac{x^2+4}{n}\right) \neq 0$ the relation*

$$c(1,x)^{n-\epsilon(n)} \equiv I_2 \pmod{n},$$

then n is squarefree.

PROOF. Suppose n is not squarefree. Then we have $n = p^e \cdot m$ for a prime number p, an exponent $e \geq 2$, and a number m coprime to p. First, we consider the case that $p \in \{3,5\}$.
Let $p = 3$. Then we have $\operatorname{ord}_9(c(1,x)) = 12$ for $x \equiv 2 \pmod 9$ and $\left(\frac{x^2+4}{n}\right) = \left(\frac{8}{n}\right) \neq 0$ since n is odd. Therefore, we have $12 \mid \operatorname{ord}_n(c(1,2))$. Hence, $12 \mid n - \left(\frac{8}{n}\right)$. It follows that $n \equiv \pm 1 \pmod{12}$, which contradicts $n \equiv 0 \pmod 3$.
Let $p = 5$. Then we have $\operatorname{ord}_{25}(c(1,x)) = 30$ for $x \equiv 2 \pmod{25}$ and $\left(\frac{x^2+4}{n}\right) = \left(\frac{8}{n}\right) \neq 0$ since n is odd. Therefore, we have $30 \mid \operatorname{ord}_n(c(1,2))$. Hence, $30 \mid n - \left(\frac{8}{n}\right)$. It follows that $n \equiv \pm 1 \pmod{30}$, which contradicts $n \equiv 0 \pmod 5$.
Now let $p > 5$. Since $(\mathbb{Z}/p^e\mathbb{Z})^*$ is a cyclic group of order $\varphi(p^e) = p^e - p^{e-1}$, we have an element $a \in (\mathbb{Z}/p^e\mathbb{Z})^*$ with

$$\operatorname{ord}_{p^e}(a) = p^e - p^{e-1} = p^{e-1}(p-1).$$

Since $n \not\equiv 0 \pmod 3$, we have $a^2 \not\equiv 1 \pmod p$. Set $x := a - a^{-1}$. Then $x \in (\mathbb{Z}/p^e\mathbb{Z})^*$ since $a^2 - 1 \not\equiv 0 \pmod p$. By $n \not\equiv 0 \pmod 5$, we have also $a^2 + 1 \not\equiv 0 \pmod p$. Let

$$S := \begin{pmatrix} 1 & (a+1)^{-1} \\ 1 & a(a-1)^{-1} \end{pmatrix},$$

then we have

$$S^{-1} = (a^2+1)^{-1} \begin{pmatrix} a(a+1) & 1-a \\ 1-a^2 & a^2-1 \end{pmatrix}$$

and

$$\begin{aligned} S \cdot c(1,x) \cdot S^{-1} &= S \cdot c(1, a - a^{-1}) \cdot S^{-1} \\ &= \begin{pmatrix} 1 & (a+1)^{-1} \\ 1 & a(a-1)^{-1} \end{pmatrix} \begin{pmatrix} a - a^{-1} + a^2 + a^{-2} - 1 & a - a^{-1} \\ 2 - a^2 - a^{-2} & 1 - a + a^{-1} \end{pmatrix} S^{-1} \\ &= \begin{pmatrix} a^2 & a^2(a+1)^{-1} \\ a^{-2} & a^{-1}(a-1)^{-1} \end{pmatrix} \begin{pmatrix} a(a+1) & 1-a \\ 1-a^2 & a^2-1 \end{pmatrix} (a^2+1)^{-1} \\ &\equiv \begin{pmatrix} a^2 & 0 \\ 0 & a^{-2} \end{pmatrix} \pmod{p^e}. \end{aligned}$$

Hence,

$$\operatorname{ord}_{p^e}(c(1,x)) = \operatorname{ord}_{p^e}(a^2) = p^{e-1} \cdot \tfrac{p-1}{2}.$$

By the divisibility relation

$$\operatorname{ord}_{p^e}(c(1,x)) \mid n - \epsilon(n),$$

it follows that $p^{e-1} \cdot \frac{p-1}{2} \mid n - \epsilon(n)$, in particular $p \mid n - \epsilon(n)$, which contradicts $p \mid n$. □

THEOREM 4.47. *Let n be a squarefree odd composite number. Then there exists at least one integer x with $\epsilon = \left(\frac{x^2+4}{n}\right) \in \{\pm 1\}$ such that*

$$c(1,x)^{n-\epsilon} \not\equiv I_2 \pmod n.$$

PROOF. If $n = 15$, then the assertion follows by $c(1,2)^{14} \not\equiv I_2 \pmod{15}$.
Assume $n \neq 15$ and $c(1,x)^{n-\epsilon} \equiv I_2 \pmod n$ for all integers x with $\epsilon = \left(\frac{x^2+4}{n}\right) \in \{\pm 1\}$.
If $3 \mid n$, then, by Corollary 4.37, there exist two integers x_1 and x_2 such that

$$\left(\tfrac{x_1^2+4}{n}\right) = -\left(\tfrac{x_2^2+4}{n}\right) = 1.$$

Since $\operatorname{ord}_3(c(1,x_1)) = \operatorname{ord}_3(c(1,x_2)) = 4$, we have $4 \mid n-1$ and $4 \mid n+1$, which contradicts Lemma 4.45. Thus, $3 \nmid n$.
If $5 \mid n$, then, by Corollary 4.37, there exist two integers x_1 and x_2 such that

$$\left(\tfrac{x_1^2+4}{n}\right) = -\left(\tfrac{x_2^2+4}{n}\right) = 1.$$

Since $\operatorname{ord}_5(c(1,x_1)) = \operatorname{ord}_5(c(1,x_2)) = 6$, we have $6 \mid n-1$ and $6 \mid n+1$, which contradicts Lemma 4.45. Thus, $5 \nmid n$.
Let $\prod_{k=1}^{r} p_k$ be the prime factorization of n. Then, by Theorem 4.36, Lemma 4.40, and Lemma 4.42, we have $x_1, x_2 \in \mathbb{F}_{p_1}^*$ such that

$$\operatorname{ord}_{p_1}(c(1,x_1)) = \tfrac{p_1-1}{2} \qquad \text{and} \qquad \operatorname{ord}_{p_1}(c(1,x_2)) = p_1 + 1. \tag{16}$$

By Corollary 4.37, there exist $x_{2k-1}, x_{2k} \in \mathbb{F}_{p_k}^*$ for $2 \le k \le r$ such that

$$\left(\tfrac{x_{2k-1}^2+4}{p_k}\right) = 1 \quad \text{and} \quad \left(\tfrac{x_{2k}^2+4}{p_k}\right) = \begin{cases} -1\,, & \text{if } k = 2 \\ 1\,, & \text{else.} \end{cases}$$

Then, by Chinese Remainder Theorem 2.5, there exist $y_1, y_2 \in (\mathbb{Z}/n\mathbb{Z})^*$ such that

$$y_1 \equiv x_{2k-1} \pmod{p_k} \quad \text{and} \quad y_2 \equiv x_{2k} \pmod{p_k} \quad \text{for } 1 \le k \le r.$$

Therefore, we have $\left(\tfrac{y_1^2+4}{n}\right) = \left(\tfrac{y_2^2+4}{n}\right) = 1$. Hence, by the assumption and equations (16), we get

$$c(1, y_1)^{n-1} \equiv c(1, y_2)^{n-1} \equiv I_2 \pmod{n}$$

and

$$\tfrac{p_1-1}{2} \mid n-1 \quad \text{and} \quad p_1 + 1 \mid n-1. \tag{17}$$

By Corollary 4.37, there exists an integer z such that $\left(\tfrac{z^2+4}{n}\right) = -1$. Let $d := \operatorname{ord}_{p_1}(c(1, z))$. Then $d \mid n+1$, and either $d \mid \tfrac{p_1-1}{2}$ or $d \mid p_1+1$. Hence, by divisibility relation (17), we get $d \mid n-1$. Therefore, by Lemma 4.45, we get $d \le 2$, which contradicts Theorem 4.20. □

COROLLARY 4.48. *Let n be an odd composite number. Then there exists at least one integer x with $\epsilon = \left(\tfrac{x^2+4}{n}\right) \in \{\pm 1\}$ such that*

$$c(1, x)^{n-\epsilon} \not\equiv I_2 \pmod{n}.$$

PROOF. It can be directly concluded from Theorem 4.46 and Theorem 4.47. □

LEMMA 4.49. *Let n be an odd natural number with prime factorization $n = \prod_{k=1}^r p_k$, $\prod_{k=2}^r p_k < p_1^2$, $\tfrac{p_1-1}{2} \mid n-1$ and $p_1 + 1 \mid n+1$. Then*

$$n = p_1 \cdot \tfrac{p_1^2+1}{2}.$$

PROOF. We have

$$\begin{aligned} n \equiv 1 \pmod{\tfrac{p_1-1}{2}} \quad &\text{and} \quad n \equiv -1 \pmod{p_1+1} \\ \text{and} \quad p_1 \equiv 1 \pmod{\tfrac{p_1-1}{2}} \quad &\text{and} \quad p_1 \equiv -1 \pmod{p_1+1}. \end{aligned}$$

Thus,

$$n \equiv p_1 \pmod{\tfrac{p_1-1}{2}} \quad \text{and} \quad n \equiv p_1 \pmod{p_1+1}.$$

Therefore,

$$\begin{aligned} & n - p_1 = p_1\Big(1 - \prod_{k=2}^r p_k\Big) \equiv 0 \pmod{\tfrac{p_1-1}{2}(p_1+1)} \\ \underset{(\gcd(p_1, p_1^2-1)=1)}{\Rightarrow} \quad & 1 - \prod_{k=2}^r p_k \equiv 0 \pmod{\tfrac{p_1^2-1}{2}}. \end{aligned}$$

By

$$1 < \prod_{k=2}^r p_k < p_1^2,$$

we have

$$\prod_{k=2}^{r} p_k = \tfrac{p_1^2+1}{2},$$

hence

$$n = p_1 \cdot \tfrac{p_1^2+1}{2}. \quad \square$$

LEMMA 4.50. *Let n be a squarefree odd composite number with the prime factorization $n = p_1p_2p_3$ with $p_2p_3 = \frac{p_1^2+1}{2}$. Assume $p_3 < p_2 < p_1$. Then*

$$p_1 < \sqrt{2}\, p_2 \quad \text{and} \quad p_1 < 2\, p_3 - 1.$$

PROOF. Suppose $p_3 \leq \frac{p_1+1}{2}$. Then

$$p_1 > p_2 = \tfrac{p_1^2+1}{2\, p_3} \geq \tfrac{p_1^2+1}{p_1+1} > p_1 - 1$$

is a contradiction since p_2 is an integer. Thus, $p_3 > \frac{p_1+1}{2} > \frac{p_1}{2}$.
Suppose $p_2 \leq \frac{p_1}{\sqrt{2}}$. Then

$$p_3 = \tfrac{p_1^2+1}{2\, p_2} \geq \tfrac{p_1^2+1}{\sqrt{2}\, p_1} = \tfrac{p_1}{\sqrt{2}} + \tfrac{1}{\sqrt{2}\, p_1} > \tfrac{p_1}{\sqrt{2}} \geq p_2$$

is a contradiction to $p_2 > p_3$. Thus, $p_1 < \sqrt{2}\, p_2$. $\square$

THEOREM 4.51. *Let n be a squarefree odd composite number with the prime factorization $n = p_1p_2p_3$ with $p_3 < p_2 < p_1$. Then at least one of the following four divisibility relations fails:*

$$\tfrac{p_1-1}{2} \mid n-1, p_1+1 \mid n+1, \tfrac{p_2-1}{2} \mid n-1 \text{ and } p_2+1 \mid n+1.$$

PROOF. Suppose we have

$$\tfrac{p_1-1}{2} \mid n-1, p_1+1 \mid n+1, \tfrac{p_2-1}{2} \mid n-1 \text{ and } p_2+1 \mid n+1.$$

Then from Lemma 4.49, and Lemma 4.50, we have

$$p_2p_3 = \tfrac{p_1^2+1}{2} \quad \text{and} \quad p_1 < \sqrt{2}\, p_2. \tag{18}$$

Moreover, we have

$$\begin{aligned} n \equiv 1 \pmod{\tfrac{p_2-1}{2}} \quad &\text{and} \quad n \equiv -1 \pmod{p_2+1} \\ \text{and} \quad p_2 \equiv 1 \pmod{\tfrac{p_2-1}{2}} \quad &\text{and} \quad p_2 \equiv -1 \pmod{p_2+1}. \end{aligned}$$

Thus,

$$n \equiv p_2 \pmod{\tfrac{p_2-1}{2}} \quad \text{and} \quad n \equiv p_2 \pmod{p_2+1}.$$

Therefore,

$$\begin{aligned} & n - p_2 = p_2(1 - p_1p_3) \equiv 0 \pmod{\tfrac{p_2^2-1}{2}} \\ \underset{(\gcd(p_2, p_2^2-1)=1)}{\Rightarrow} \quad & p_1p_3 \equiv 1 \pmod{\tfrac{p_2^2-1}{2}}. \end{aligned}$$

From $p_1 \underset{(18)}{<} \sqrt{2}\, p_2$, we have $p_1p_3 < \sqrt{2}\, p_2^2 < \frac{3p_2^2-1}{2} = \frac{p_2^2+1}{2} + 2 \cdot \frac{p_2^2-1}{2}$. Thus,

$$p_1p_3 = \tfrac{p_2^2+1}{2}. \tag{19}$$

Therefore from (18), and (19), we have

$$\frac{p_2^2+1}{2p_1} \underset{(19)}{=} p_3 \underset{(18)}{=} \frac{p_1^2+1}{2p_2}.$$

Hence,

$$2p_2(p_2^2+1) = 2p_1(p_1^2+1).$$

Since the map $t \mapsto 2t(t^2+1)$ is strictly monotonic increasing, we have

$$p_1 = p_2,$$

which contradicts $p_1 > p_2$. □

6. Euler's Criterion on the Standard Commutator Curve

In this section, we will see that we can prove a theorem on the standard commutator curve, which is similar to Euler's criterion for the quadratic residues. By this theorem, we can give – in Subsection 3.1 of Chapter 5 on pages 154–164 – a precise estimate for the exponent of 2 in $p \pm 1$ for every prime divisor p of a natural number n, and we can prove the fifth and sixth item of Observation 4.14. But first of all, we need the following lemma.

LEMMA 4.52. *Let p be an odd prime number, $x \in \mathbb{F}_p^*$, and $\epsilon = \left(\frac{x^2+4}{p}\right) \in \{\pm 1\}$. Then there exists a matrix $A \in SL_2(p)$ with $A^2 = c(1,x)$ if and only if $\epsilon = 1$.*

PROOF. "⇐": We have $\epsilon = 1$. Hence, there exists $\alpha \in \mathbb{F}_p$ such that $\alpha^{-2} = x^2+4$. Let

$$A = \begin{pmatrix} -\alpha(x^2+x+2) & -\alpha x \\ \alpha x^2 & \alpha(x-2) \end{pmatrix}.$$

It is easy to see that $\det(A) = \alpha^2(x^2+4) = 1$ and from $\alpha \in \mathbb{F}_p$, we have $A \in SL_2(p)$. Thus, the proof of this direction will be complete by the following calculation:

$$\begin{aligned}
A^2 &= \alpha^2 \begin{pmatrix} -(x^2+x+2) & -x \\ x^2 & x-2 \end{pmatrix}^2 \\
&= \alpha^2 \begin{pmatrix} (x^2+x+2)^2 - x^3 & x(x^2+x+2) - x^2 + 2x \\ -x^2(x^2+x+2) + (x-2)x^2 & -x^3 + (x-2)^2 \end{pmatrix} \\
&= \alpha^2 \begin{pmatrix} x^4+x^2+4+x^3+4x^2+4x & x^3+4x \\ -x^4-4x^2 & -x^3+x^2-4x+4 \end{pmatrix} \\
&= \tfrac{1}{x^2+4} \begin{pmatrix} (x^2+x+1)(x^2+4) & x(x^2+4) \\ -x^2(x^2+4) & (1-x)(x^2+4) \end{pmatrix} \\
&= c(1,x).
\end{aligned}$$

"⇒": Let

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in SL_2(p)$$

such that

$$\begin{aligned} A^2 &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}^2 \\ &= \begin{pmatrix} a_{11}^2 + a_{12}a_{21} & a_{12}(a_{11} + a_{22}) \\ a_{21}(a_{11} + a_{22}) & a_{22}^2 + a_{12}a_{21} \end{pmatrix} \\ &= c(1, x) = \begin{pmatrix} 1 + x + x^2 & x \\ -x^2 & 1 - x \end{pmatrix}. \end{aligned}$$

Therefore, we get the following equations:

$$a_{11}^2 + a_{12}a_{21} = 1 + x + x^2 \tag{20}$$
$$a_{22}^2 + a_{12}a_{21} = 1 - x \tag{21}$$
$$a_{12}(a_{11} + a_{22}) = x \tag{22}$$
$$a_{21}(a_{11} + a_{22}) = -x^2 \tag{23}$$
$$a_{11}a_{22} - a_{12}a_{21} = 1. \tag{24}$$

Firstly, we generate five simple relations.

(1) Since $x \neq 0$, we have
$$a_{11} + a_{22} \neq 0. \tag{25}$$
(2) Subtract (21) from (20). Then we have
$$a_{11}^2 - a_{22}^2 = (a_{11} - a_{22})(a_{11} + a_{22}) = x(x + 2). \tag{26}$$
(3) Substitute one x of (23) by (22), and divide the resulting equation by
$$a_{11} + a_{22} \underset{(25)}{\neq} 0,$$
then we have
$$a_{21} = -xa_{12}. \tag{27}$$
(4) Add (21) to (24). Then we have
$$a_{22}(a_{22} + a_{11}) = 2 - x. \tag{28}$$
(5) Multiply both sides of (22), and (28), and divide the resulting equation by
$$a_{11} + a_{22} \underset{(25)}{\neq} 0,$$
then we have
$$a_{22}x = (2 - x)a_{12}. \tag{29}$$

Secondly, we consider the case $x = 2$. By (27), and (28), we have $a_{21} = -2a_{12}$ and $a_{22} = 0$. Thus, we have the following matrix equation

$$A^2 = \begin{pmatrix} a_{11}^2 - 2a_{12}^2 & a_{12}a_{11} \\ -2a_{12}a_{11} & -2a_{12}^2 \end{pmatrix} = c(1, 2) = \begin{pmatrix} 7 & 2 \\ -4 & -1 \end{pmatrix}.$$

Therefore, we have, by addition of $a_{11}^2 - 2a_{12}^2 = 7$ and $2a_{12}^2 = 1$, the equation $a_{11}^2 = 8$. Hence

$$\epsilon = \left(\tfrac{x^2+4}{p}\right) = \left(\tfrac{4+4}{p}\right) = \left(\tfrac{8}{p}\right) = 1.$$

Thirdly, we consider the case $x^2+x+2=0$. By addition of (20), and (24), we have $a_{11}(a_{11}+a_{22})=0$. Thus, by (25), we get the equation $a_{11}=0$ and $a_{12}a_{21}=-1$ from (24). By $x\neq 0$, (22), and (23), we have $a_{21}=-xa_{12}$. Therefore, we get $a_{21}^2=x$ from the equation $a_{12}a_{21}=-1$ and so we have $\left(\frac{x}{p}\right)=1$. Hence

$$\begin{aligned}\epsilon &= \left(\tfrac{x^2+4}{p}\right)=\left(\tfrac{x^2+(-2)^2}{p}\right)=\left(\tfrac{x^2+(x^2+x)^2}{p}\right)\\ &= \left(\tfrac{x^2+x^4+2x^3+x^2}{p}\right)=\left(\tfrac{x^2(2+x^2+x+x)}{p}\right)=\left(\tfrac{x^3}{p}\right)=\left(\tfrac{x}{p}\right)\\ &= 1.\end{aligned}$$

Now we can assume that $x\neq 2$ and $x^2+x+2\neq 0$. In the following six steps, we evaluate exact equations for the four coefficients of matrix A.

(1) Divide (26) by (28). Then we have

$$\begin{aligned}& a_{11}-a_{22}=a_{22}\frac{x(x+2)}{2-x}\\ \Rightarrow\quad & a_{11}=a_{22}\left(1+\frac{x(x+2)}{2-x}\right)=a_{22}\frac{x^2+x+2}{2-x}.\end{aligned}\tag{30}$$

(2) Substitute (27) and (29) in (23). Then we have

$$\begin{aligned}& -xa_{12}(a_{11}+(2x^{-1}-1)a_{12})=-x^2\\ \Rightarrow\quad & -x(2x^{-1}-1)a_{12}^2-xa_{11}a_{12}=-x^2\\ \Rightarrow\quad & a_{12}^2-\frac{xa_{11}}{x-2}a_{12}+\frac{x^2}{x-2}=0\\ \Rightarrow\quad & a_{12}=\frac{xa_{11}}{2(x-2)}\pm\sqrt{\frac{x^2a_{11}^2}{4(x-2)^2}-\frac{x^2}{x-2}}\\ & \qquad =\frac{xa_{11}\pm\sqrt{x^2(a_{11}^2-4x+8)}}{2(x-2)}.\end{aligned}\tag{31}$$

(3) Substitute (31) in (29) and substitute the resulting equation in (30), then we have

$$\begin{aligned}a_{11} &= \frac{2-x}{x}\cdot\frac{x^2+x+2}{2-x}\cdot\frac{xa_{11}\pm\sqrt{x^2(a_{11}^2-4x+8)}}{2(x-2)}\\ &= \frac{(x^2+x+2)(a_{11}\pm\sqrt{a_{11}^2-4x+8})}{2(x-2)}\\ \Rightarrow\quad \left(\frac{2(x-2)}{x^2+x+2}-1\right)^2a_{11}^2 &= \left(\frac{-x^2+x-6}{x^2+x+2}\right)^2a_{11}^2\\ &= a_{11}^2-4x+8\\ \Rightarrow\quad a_{11}^2\left(\frac{x^4+x^2+36-2x^3+12x^2-12x}{x^4+x^2+4+2x^3+4x^2+4x}-1\right) &= -4x+8\\ \Rightarrow\quad a_{11}^2\frac{32-4x^3+8x^2-16x}{(x^2+x+2)^2} &= a_{11}^2\frac{(x^2+4)(8-4x)}{(x^2+x+2)^2}=8-4x\end{aligned}$$

$$\Rightarrow \quad a_{11}^2 = \frac{(x^2+x+2)^2}{x^2+4}. \tag{32}$$

(4) Substitute (32) in the square of (30). Then we have

$$a_{22}^2 = \frac{(2-x)^2}{x^2+4} \tag{33}$$

(5) Substitute (33) in the square of (29). Then we have

$$a_{12}^2 = \frac{x^2}{x^2+4} \tag{34}$$

(6) Substitute (34) in the square of (27). Then we have

$$a_{21}^2 = \frac{x^4}{x^2+4}. \tag{35}$$

By equation (34), we have $x^2+4 = x^2 \cdot a_{12}^{-2}$, hence $\epsilon = 1$. □

Now we can formulate Euler's criterion on the standard commutator curve as follows.

THEOREM 4.53. *Let p be an odd prime number, $x \in \mathbb{F}_p^*$, and $\epsilon := \left(\frac{x^2+4}{p}\right)$. Then*

$$c(1,x)^{\frac{p-\epsilon}{2}} = \epsilon \cdot I_2, \qquad \text{if } \epsilon \neq 0,$$

and

$$c(1,x)^{2p} = I_2, \qquad \text{if } \epsilon = 0.$$

PROOF.

(1) If $\epsilon = 1$. By Corollary 4.9, and Lemma 4.52, there exists a cyclic subgroup G of order $p-1$ such that $A \in G$ with $A^2 = c(1,x)$. Then

$$c(1,x)^{\frac{p-1}{2}} = A^{p-1} \equiv I_2 \pmod{p}.$$

(2) If $\epsilon = -1$. Let G be a cyclic subgroup of $SL_2(p)$ with $|G| = p+1$ and $c(1,x) \in G$. The group G exists by virtue of Corollary 4.9. By Lemma 4.52, $c(1,x)$ is not a square, and so there exists a generator $g \in G$ with $c(1,x) = g^a$, where a is an odd integer. Since g is a generator, we have

$$g^{\frac{p+1}{2}} \equiv -1 \pmod{p}.$$

Hence, it follows

$$c(1,x)^{\frac{p+1}{2}} = (g^a)^{\frac{p+1}{2}} = (g^{\frac{p+1}{2}})^a \equiv (-I_2)^a = -I_2 \pmod{p}.$$

(3) If $\epsilon = 0$. The assertion follows directly from Theorem 4.39. □

REMARK 4.54. This theorem can also be proved by using Lemma 4.40 and Lemma 4.42.

By Euler's criterion on the standard commutator curve, the fifth and sixth item of Observation 4.14 are simple corollaries.

COROLLARY 4.55. *Let p be a prime number, and $x \in \mathbb{F}_p^*$ such that $\mathrm{ord}_p(c(1,x)) \mid p+1$. Then*

$$\nu_2(\mathrm{ord}_p(c(1,x))) = \nu_2(p+1).$$

PROOF. Let $a = \mathrm{ord}_p(c(1,x))$. Then we have, by Theorem 4.53, the following two divisibility relations

$$a \mid p+1 \quad \text{and} \quad a \nmid \tfrac{p+1}{2}.$$

By the relation $a \mid p+1$, we have $\nu_2(a) \leq \nu_2(p+1)$. Additionally, by $a \nmid \frac{p+1}{2}$, we get the assertion $\nu_2(a) = \nu_2(p+1)$. □

COROLLARY 4.56. *Let p be a prime number, and $x \in \mathbb{F}_p^*$ such that $\mathrm{ord}_p(c(1,x)) \mid p-1$. Then*

$$\nu_2(\mathrm{ord}_p(c(1,x))) < \nu_2(p-1).$$

PROOF. Let $a = \mathrm{ord}_p(c(1,x))$. Then we have, by Theorem 4.53, the divisibility relation $a \mid \frac{p-1}{2}$. Then $\nu_2(a) \leq \nu_2(\frac{p-1}{2}) < \nu_2(p-1)$. □

7. Correlation to a Lucas Sequence

In this section we will see that we can define another curve which has the same distribution of orders as the standard commutator curve. Furthermore, we will see that the recurrence relation of this new curve is better to handle in practice as that of the standard commutator curve (see Section 4 on page 60). This recurrence relation is the Lucas sequence $\{U_k(x,-1)\}_{k\in\mathbb{N}}$ (see Subsection 2.5 of Chapter 3 on page 29).

DEFINITION 4.57. We define a new curve C'_n for a positive integer n by the set

$$C'_n := \{c(x) \pmod n \mid x \in (\mathbb{Z}/n\mathbb{Z})^*\},$$

where c in the two-dimensional special linear group is defined by

$$c(x) := \begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix}^2 = \begin{pmatrix} 1 & x \\ x & 1+x^2 \end{pmatrix}$$

with $x \in (\mathbb{Z}/n\mathbb{Z})^*$.

In the following theorem we will see that the curve C'_n has the same distribution of orders as the standard commutator curve C^1_n.

THEOREM 4.58. *Let n be a positive integer, and $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Then*

$$c(x) = S^{-1}c(1,x)S$$

with $S = \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}$.

PROOF. The proof of the assertion follows directly by

$$\begin{aligned} S^{-1}c(1,x)S &\underset{(4.5)}{=} \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1+x+x^2 & x \\ -x^2 & 1-x \end{pmatrix} \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -x & -1-x^2 \\ x-1 & 1-x+x^2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & x \\ x & 1+x^2 \end{pmatrix} \\ &= c(x). \quad \square \end{aligned}$$

COROLLARY 4.59. *Let n be a positive integer, and $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Then*

$$\operatorname{ord}(c(x)) = \operatorname{ord}(c(1,x)).$$

PROOF. This corollary follows directly from Theorem 4.58. $\square$

After that consideration we can define the *square root curve* D_n for a positive integer n by the set

$$D_n := \{d(x) \pmod n \mid x \in (\mathbb{Z}/n\mathbb{Z})^*\},$$

where d in the two-dimensional general linear group is defined by

$$d(x) := \begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix}$$

with $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Obviously, we have $d(x)^2 = c(x)$.

COROLLARY 4.60. *Let p be an odd prime number, $x \in \mathbb{F}_p^*$, and $\epsilon := \left(\frac{x^2+4}{p}\right)$. Then*

$$d(x)^{p-\epsilon} \equiv \epsilon \cdot I_2 \pmod p, \qquad \text{if } \epsilon \neq 0,$$

and

$$d(x)^{4p} \equiv I_2 \pmod p, \qquad \text{if } \epsilon = 0.$$

PROOF. This corollary follows directly from Theorem 4.53, and Theorem 4.58. $\square$

In the next theorem we will see that the power of $d(x)$ can be determined by a Lucas sequence.

THEOREM 4.61. *Let n, m be positive integers, and $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Then*

$$\begin{aligned} d(x)^m &= U_{m-1}(x,-1) \cdot I_2 + U_m(x,-1) \cdot d(x) \\ &= \begin{pmatrix} U_{m-1}(x,-1) & U_m(x,-1) \\ U_m(x,-1) & xU_m(x,-1) + U_{m-1}(x,-1) \end{pmatrix} \\ &= \begin{pmatrix} U_{m-1}(x,-1) & U_m(x,-1) \\ U_m(x,-1) & U_{m+1}(x,-1) \end{pmatrix}, \end{aligned}$$

with the Lucas sequence

$$\begin{aligned} U_0(x,-1) &:= 0, \\ U_1(x,-1) &:= 1, \\ U_{k+2}(x,-1) &:= xU_{k+1}(x,-1) + U_k(x,-1) \quad \text{for } k \in \mathbb{N}. \end{aligned}$$

PROOF. If $m \in \{1, 2\}$, then the assertion follows directly by

$$\begin{aligned} d(x)^1 &= U_0(x,-1)\cdot I_2 + U_1(x,-1)\cdot d(x), \quad \checkmark \\ d(x)^2 &= I_2 + x\cdot d(x) \\ &= U_1(x,-1)\cdot I_2 + (xU_1(x,-1) + U_0(x,-1))\cdot d(x) \\ &= U_1(x,-1)\cdot I_2 + U_2(x,-1)\cdot d(x). \quad \checkmark \end{aligned}$$

We proceed by induction on m. Assume that we have the assertion for m by induction. Then

$$\begin{aligned} d(x)^{m+1} &= d(x)\cdot d(x)^m \\ &\underset{(IA)}{=} d(x)(U_{m-1}(x,-1)\cdot I_2 + U_m(x,-1)\cdot d(x)) \\ &= U_{m-1}(x,-1)\cdot d(x) + U_m(x,-1)\cdot d(x)^2 \\ &= U_{m-1}(x,-1)\cdot d(x) + U_m(x,-1)\cdot (I_2 + x\cdot d(x)) \\ &= U_m(x,-1)\cdot I_2 + (xU_m(x,-1) + U_{m-1}(x,-1))\cdot d(x)) \\ &= U_m(x,-1)\cdot I_2 + U_{m+1}(x,-1)\cdot d(x). \quad \square \end{aligned}$$

8. Curves in Practice

In this section we are interested in the running time of calculating the power of a point on the standard commutator curve, i.e. we are interested in calculating $c(1,x)^m$ where m, n are positive integers, and $x \in (\mathbb{Z}/n\mathbb{Z})^*$.

It is well known that the power algorithm needs $O(\log(m))$ modular multiplications modulo n using the binary representation of the exponent $m \in \mathbb{N}_{>0}$. Most important for the running time of the power algorithm is the number of modular multiplications modulo n per iteration to square a point on the standard commutator curve. It is useful to differ between multiplications and squarings if we count the number of multiplications since squaring in $(\mathbb{Z}/n\mathbb{Z})^*$ is about 33% faster than a normal multiplication[3]. For more details about these differences we refer to [**117**], [**130**], and [**131**].

In the analysis of algorithms we concentrate on precisely characterizing the number of units by determining their best-case, worst-case, and average-case performance. We use one modular multiplication of the Miller-Rabin test (Algorithm 3.11) as a unit[4] for theoretical comparisons of the different methods to implement the power of a point on the standard commutator curve. The best-case performance for the power algorithm will be achieved if the exponent is a power of two; the worst-case performance will be achieved if the binary representation of the exponent contains only digit 1; the average-case performance will be achieved if the count of digit 1 and digit 0 is equal in the binary representation of the exponent.

First, we consider the Miller-Rabin test. In the best-case we have only 1 squaring which takes 75% running time of one modular multiplication. In the worst-case we have 1

[3]This difference is also correct for Karatsuba's multiplication and the multiplication based on FFT.
[4]This unit was also suggested by A. O. L. Atkin in [**9**].

squaring and 1 multiplication per iteration. In the average-case we have 1 squaring and $\frac{1}{2}$ multiplication per iteration.

Algorithm	best-case	worst-case	average-case
Miller-Rabin test	0.75	1.75	1.25

Since $c(1,x)$ is a matrix, the obvious answer to the performance are 8 multiplications to multiply two different matrices and 3 multiplications and 2 squarings to square a matrix in a commutative group. By Strassen's fast matrix computation [**123**], we can reduce to 7 multiplications to multiply two different matrices.

Algorithm	best-case	worst-case	average-case
Matrix multiplication of $c(1,x)$	4.5	12.5	8.5
Strassen's fast matrix computation of $c(1,x)$	4.5	11.5	8

Using the recurrence relations for the standard commutator curve of Section 4 we need 5 multplications and 2 squaring to calculate $\theta_{2m}(x)$ and $\omega_{2m}(x)$ and 4 multplications to calculate $\theta_{2m+1}(x)$ and $\omega_{2m+1}(x)$ if $\theta_m(x), \theta_{m-1}(x), \omega_m(x)$ and $\omega_{m-1}(x)$ are given and if we use local variables.

Algorithm	best-case	worst-case	average-case
Recurrence relation using $\theta_m(x)$ and $\omega_m(x)$	6.5	10.5	8.5

We can use the square root curve of the previous section instead of the standard commutator curve if we are only interested in specific information of the order of a point. Since $d(x)$ is a symmetric matrix, the obvious answer to the performance are 8 multiplications to multiply two different matrices and 1 multiplication and 3 squarings to square a matrix in a commutative group. By Strassen's fast matrix computation [**123**], we can reduce to 7 multiplications to multiply two different matrices.

Algorithm	best-case	worst-case	average-case
Matrix multiplication of $d(x)$	3.25	11.25	7.25
Strassen's fast matrix computation of $d(x)$	3.25	10.25	6.75

Now we state a well known theorem (see for example [**138**]) which gives two identity properties of the Lucas sequences.

THEOREM 4.62. *Let m, n be positive integers, and $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Then*

$$\begin{aligned} U_{2m-1}(x,-1) &= U_m(x,-1)^2 + U_{m-1}(x,-1)^2, \\ \text{and} \quad U_{2m}(x,-1) &= xU_m(x,-1)^2 + 2U_m(x,-1)U_{m-1}(x,-1) \end{aligned}$$

PROOF. We write U_m instead of $U_m(x,-1)$ for better reading. Then by Theorem 4.61, we have

$$\begin{aligned} d(x)^{2m} &\underset{(4.61)}{=} \begin{pmatrix} U_{2m-1} & U_{2m} \\ U_{2m} & U_{2m+1} \end{pmatrix} \\ &= \begin{pmatrix} U_{m-1} & U_m \\ U_m & U_{m+1} \end{pmatrix}^2 \end{aligned}$$

$$= \begin{pmatrix} U_{m-1}^2 + U_m^2 & U_m(U_{m-1} + U_{m+1}) \\ U_m(U_{m-1} + U_{m+1}) & U_m^2 + U_{m+1}^2 \end{pmatrix}.$$

Therefore,

$$\begin{aligned} U_{2m-1} &= U_m^2 + U_{m-1}^2 \\ U_{2m} &= U_m(U_{m-1} + U_{m+1}) \\ &= U_m(U_{m-1} + xU_m + U_{m-1}) \\ &= xU_m^2 + 2U_mU_{m-1}. \quad \square \end{aligned}$$

Using the Lucas sequence above to calculate a power of a point on the square root curve we need 2 multplications and 1 squaring to calculate $U_{2m}(x,-1)$ and 1 squaring and 1 reusable squaring to calculate $U_{2m+1}(x,-1)$ if $U_m(x,-1)$ and $U_{m-1}(x,-1)$ are given.

Algorithm	best-case	worst-case	average-case
Lucas sequence using $U_m(x,-1)$	2.75	3.5	3.25

The following theorem gives an improvement to calculate this Lucas sequence for the square root curve if we consider only a fixed x, e.g. $x \in \{\pm 1\}$.

THEOREM 4.63. *Let m, n be positive integers, and $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Then*

$$U_m(x,-1)U_{m-1}(x,-1) = x^{-1}(U_m(x,-1)^2 - U_{m-1}(x,-1)^2 + (-1)^m).$$

PROOF. If $m \in \{1,2\}$, then the assertion follows directly by

$$\begin{aligned} U_1(x,-1)U_0(x,-1) &= 0 = x^{-1}(1^2 - 0^2 - 1), \quad \checkmark \\ U_2(x,-1)U_1(x,-1) &= x = x^{-1}(x^2 - 1^2 + 1). \quad \checkmark \end{aligned}$$

We proceed by induction on m. Assume that we have the assertion for m by induction. We write U_m instead of $U_m(x,-1)$ for better reading. Then, by the inductional assumption, we have

$$\begin{aligned} U_{m+1}U_m &= (xU_m + U_{m-1})(xU_{m-1} + U_{m-2}) \\ &= ((x^2+1)U_{m-1} + xU_{m-2})(xU_{m-1} + U_{m-2}) \\ &= x(x^2+1)U_{m-1}^2 + (2x^2+1)U_{m-1}U_{m-2} + xU_{m-2}^2 \\ &\underset{(IA)}{=} x(x^2+1)U_{m-1}^2 + x^{-1}(U_{m-1}^2 - U_{m-2}^2 + (-1)^m) \\ &\quad + xU_{m-2}^2 + 2x^2U_{m-1}U_{m-2} \\ &= x^{-1}((x^4+3x^2+1)U_{m-1}^2 - U_{m-2}^2 + (-1)^m) + 2x^2U_{m-1}U_{m-2} \\ &= x^{-1}((x^2+1)^2U_{m-1}^2 + 2x(x^2+1)U_{m-1}U_{m-2} + x^2U_{m-2}^2 \\ &\quad - (x^2U_{m-1} + 2xU_{m-1}U_{m-2} + U_{m-2}^2) + (-1)^m) \\ &= x^{-1}((x^2+1)U_{m-1} + xU_{m-2})^2 - (xU_{m-1} + U_{m-2})^2 + (-1)^m) \\ &= x^{-1}(U_{m+1}^2 - U_m^2 + (-1)^m). \quad \square \end{aligned}$$

Using this theorem we can replace the multiplication by 2 reusable squarings, e.g. for $x = 1$ we have the Fibonacci sequence and the iteration can be calculated by squarings.

Finally, we get the following list which is ordered by the average-case performance of each algorithm:

Algorithm	best-case	worst-case	average-case
Miller-Rabin test	0.75	1.75	1.25
Lucas sequence using $U_m(1,-1)$	1.5	1.5	1.5
Lucas sequence using $U_m(x,-1)$	2.75	3.5	3.25
Strassen's fast matrix computation of $d(x)$	3.25	10.25	6.75
Matrix multiplication of $d(x)$	3.25	11.25	7.25
Strassen's fast matrix computation of $c(1,x)$	4.5	11.5	8
Recurrence relation using $\theta_m(x)$ and $\omega_m(x)$	6.5	10.5	8.5
Matrix multiplication of $c(1,x)$	4.5	12.5	8.5

By this table we get the following conclusion:
Let m, n be positive integers, $x \in (\mathbb{Z}/n\mathbb{Z})^*$, and $\epsilon \in \{\pm 1\}$. Then the running time of the test $c(1,x)^m \equiv \epsilon I_2 \pmod{n}$ is about 3 times that of the Miller-Rabin test.

CHAPTER 5

Compositeness Tests on the Standard Commutator Curve

1. Introduction

In this chapter, we use the results of the commutator curve to construct three compositeness tests on the standard commutator curve.
First, we describe a simple compositeness test similar to Fermat's test[1]. The second compositeness test is based on Euler's criterion of the commutator curve[2]. The following subsection shows that if a composite number n passes this compositeness test with the result true, the exponent of 2 in $p \pm 1$ can be specified where p is any prime divisor of n. Additionally, in the next subsection it will be shown that this test based on Euler's criterion can recognize every composite number.

By collecting observations of the described compositeness test from the previous chapter, we construct a commutator curve test, along with a fixed number of trial divisions, which returns for a composite number n the result true with probability less than $\frac{1}{16}$. Thus, if k different bases x are chosen at random, this test returns the result true for a composite number n with probability at most $\frac{1}{16^k}$.

The final section will be a conclusion and further discussion of this chapter.

It should be noted that the idea of primality testing in finite fields, or using Lucas' recurrence sequences, is not new. Lenstra's Galois Theory Test [**77**] is an example of such a method of proving primality using finite fields. The combination of finite fields and pseudoprimes also exists in some other works, such as [**52**]. The goal here, however, is different, because the algorithms of this chapter are not only a direct combination of an ordinary pseudoprime and a Lucas-based pseudoprime. They are rather a result of concentrating on a curve in the non-commutative group $SL_2(n)$ where $n > 1$ is an odd natural number. This is different from the open problems, where no number is known which is both a pseudoprime to the base 2 and a Fibonacci pseudoprime[3]; or many other problems by combining different pseudoprimes that can be found for example in [**104**], [**16**], [**103**], [**9**] and [**51**].
Up to now, all these powerful tests have depended on one condition: They have to use the smallest integer as a base, such that the Jacobi symbol is negative. Under this precondition, no number has been found for which the tests fail. But as soon as not the

[1]See Algorithm 3.4 on page 23.
[2]See Section 6 of previous Chapter 4.
[3]Fibonacci pseudoprimes are Lucas-based pseudoprime with parameter $P = 1$ and $Q = 1$

smallest integer is used, there are many counter-examples. The commutator curve test does not depend on this condition.

2. Compositeness Test Analogous to Fermat's Test

First, the following simple compositeness test is introduced. In this test the output false means that the input number n is composite; otherwise, if the output is true, then n is a pseudoprime[4].

ALGORITHM 5.1.
Input: $n \in \mathbb{N}$, *where* $2 \nmid n$, *and* $x \in (\mathbb{Z}/n\mathbb{Z})^*$, *where* $\left(\frac{x^2+4}{n}\right) \neq 0$.
Output: $R \in \{\text{true}, \text{false}\}$.

(1) If $c(1,x)^{n-\epsilon} \not\equiv I_2 \pmod{n}$ *with* $\epsilon = \left(\frac{x^2+4}{n}\right)$, *then terminate with the result* false, *otherwise terminate with the result* true.

By Corollary 4.9, it is easy to see that the result of Algorithm 5.1 is always true for prime numbers n and arbitrary "bases" $x \in (\mathbb{Z}/n\mathbb{Z})^*$.

Like Fermat's Algorithm 3.4, compositeness of a number n can be proved with certainty. A proof of primality, however, cannot be obtained from this test. The composite number $n = 323 = 17 \cdot 19$, for example, and the base $x = 1$ will pass Algorithm 5.1 with the result true.

But the main difference between Algorithm 5.1 and Fermat's test is that this algorithm can recognize every odd composite number which will not pass the test for all possible bases $x \in (\mathbb{Z}/n\mathbb{Z})^*$; see Corollary 4.48.

3. Compositeness Test Based on Euler's Criterion

In this section, the following compositeness test is introduced. For the results true and false of this test see the notes on Algorithm 5.1.

ALGORITHM 5.2.
Input: $n \in \mathbb{N}$, *where* n *is odd, and* $x \in (\mathbb{Z}/n\mathbb{Z})^*$ *with* $\left(\frac{x^2+4}{n}\right) = -1$.
Output: $R \in \{\text{true}, \text{false}\}$.

(1) If $(x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ *and* $c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod{n}$, *then terminate with the result* true, *otherwise terminate with the result* false.

It is easy to see that Algorithm 5.2 always returns the result true for prime numbers.

THEOREM 5.3. *Let* p *be an odd prime number, and let* $x \in \mathbb{F}_p^*$ *with* $\left(\frac{x^2+4}{p}\right) = -1$. *Then Algorithm 5.2 returns the result* true.

PROOF. This can be concluded from Theorem 2.9, and Theorem 4.53. □

[4]See Definition 3.1 on page 21.

We can easily construct composite numbers which pass the Algorithm 5.2 with the incorrect result true, e.g. the smallest number is $n = 3281 = 17 \cdot 193$ with respect to the bases $x \in \{81, 1432\}$ (see tables in Appendix B).

3.1. The Exponent of 2 in $n \pm 1$. In the end of the previous chapter we have proved the fifth and sixth item of Observation 4.14 as simple consequences of Euler's criterion on the standard commutator curve. This gives us some information about the exponent 2 in $p \pm 1$ where p is a prime number. But what can we say about the exponent of 2 in $n \pm 1$ if n is a composite number?
This topic was discussed by H. Cohen and H. W. Lenstra, Jr. in [**31**] on page 311 for the exponent of 2 in $n - 1$. The properties which they have found (see for example Lemma 5.7) are used as a part of their primality test (see Section 3.2 of Chapter 3 on page 36). In this section, it will be shown that similar results can be obtained for the exponent of 2 in $n + 1$, since Euler's criterion was the main key in [**31**], which we have analyzed in the previous section.

The following four lemmata connect the exponent of 2 in $n \pm 1$ with Legendre's symbol which will be combined in the main theorem of this section.

LEMMA 5.4. *Let n be an odd natural number, and let x and m be integers with*

$$\gcd(n, m) = 1 \quad \text{and} \quad c(1, x)^m \equiv -I_2 \pmod{n}.$$

Then

$$\nu_2(2m) = \nu_2(\operatorname{ord}_p(c(1, x))) \leq \nu_2(p - \epsilon(p))$$

for all prime divisors p of n, where $\epsilon(p) := \left(\frac{x^2+4}{p}\right)$.

PROOF. Let p be a prime divisor of n. Since

$$c(1, x)^m \equiv -I_2 \pmod{p},$$

then, by Lagrange's Theorem 2.11, we have

$$\operatorname{ord}_p(c(1, x)) \mid 2m \qquad \text{and} \qquad \operatorname{ord}_p(c(1, x)) \nmid m.$$

Hence,

$$\nu_2(2m) = \nu_2(\operatorname{ord}_p(c(1, x))).$$

By Corollary 4.9, we have $\operatorname{ord}_p(c(1, x)) \mid p - \epsilon(p)$. Thus,

$$2^{\nu_2(2m)} \mid p - \epsilon(p).$$

Therefore, we have proved the assertion

$$\nu_2(2m) \leq \nu_2(p - \epsilon(p)) \quad \text{and} \quad \nu_2(2m) \leq \nu_2(\operatorname{ord}_p(c(1, x))). \quad \square$$

LEMMA 5.5. *Let n be an odd natural number, and let x, and m be integers with*

$$\gcd(n, m) = 1 \quad \text{and} \quad c(1, x)^m \equiv -I_2 \pmod{n}.$$

Let p be a prime divisor of n with $\left(\frac{x^2+4}{p}\right) = -1$. Then

$$\nu_2(2m) = \nu_2(\operatorname{ord}_p(c(1, x))) = \nu_2(p + 1).$$

PROOF. Let $d := \mathrm{ord}_p(c(1,x))$. By Lemma 5.4, we know that

$$\nu_2(p+1) \geq \nu_2(2m) \quad \text{and} \quad \nu_2(d) \geq \nu_2(2m). \tag{36}$$

By Theorem 4.53, we see

$$d \mid p+1 \qquad \text{and} \qquad d \nmid \tfrac{p+1}{2} \qquad \text{and} \qquad d \mid 2m.$$

Hence,

$$\nu_2(d) \leq \nu_2(2m) \qquad \text{and} \qquad 2^{\nu_2(p+1)} \mid d \qquad \text{and} \qquad d \mid 2m.$$

Thus,

$$\nu_2(d) \leq \nu_2(2m) \quad \text{and} \quad \nu_2(p+1) \leq \nu_2(2m).$$

Therefore, the proof of the assertion follows by (36). □

LEMMA 5.6. *Let n be an odd natural number, and let x, and m be integers with*

$$\gcd(n,m) = 1 \quad \textit{and} \quad c(1,x)^m \equiv -I_2 \pmod{n}.$$

Let p be a prime divisor of n with $\left(\frac{x^2+4}{p}\right) = 1$. Then

$$\nu_2(2m) = \nu_2(\mathrm{ord}_p(c(1,x))) < \nu_2(p-1).$$

PROOF. Let $d := \mathrm{ord}_p(c(1,x))$. By Lemma 5.4, we know that

$$\nu_2(p-1) \geq \nu_2(2m) \quad \text{and} \quad \nu_2(d) \geq \nu_2(2m). \tag{37}$$

By Theorem 4.53, we have

$$c(1,x)^{\frac{p-1}{2}} \equiv I_2 \pmod{p} \qquad \text{and} \qquad c(1,x)^m \equiv -I_2 \pmod{p},$$

hence

$$d \mid \tfrac{p-1}{2} \qquad \text{and} \qquad d \mid 2m. \tag{38}$$

Therefore, we have

$$\nu_2(d) \leq \nu_2(2m).$$

Suppose that $\nu_2(p-1) = \nu_2(2m)$. Then, by (38), we get $d \mid m$. But this contradicts

$$c(1,x)^m \equiv -I_2 \pmod{p}.$$

Then the proof of the assertion follows by (37). □

LEMMA 5.7. *Let n be an odd natural number, and x, and m be integers such that*

$$\gcd(n,m) = 1 \quad \textit{and} \quad x^m \equiv -1 \pmod{n}.$$

Then for every prime divisor p of n we have $\nu_2(p-1) \geq \nu_2(2m)$; and $\nu_2(p-1) = \nu_2(2m)$ if and only if $\left(\frac{x}{p}\right) = -1$.

PROOF. The proof of this lemma is similar to the proofs of the previous three lemmata, so we refer to lemma (7.23) in [**31**] on page 311. □

THEOREM 5.8. *Let n be an odd natural number, and x be an integer with*

$$(x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod{n},$$

and

$$c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod{n}.$$

Let p be a prime divisor of n, and define $\epsilon(p) := \left(\frac{x^2+4}{p}\right)$. Then the following assertions hold:

(1) *If $n \equiv 3 \pmod 4$,*

$$\begin{aligned} \nu_2(p+\epsilon(p)) &= \nu_2(n-1) = 1 \\ \nu_2(p-1) &> \nu_2(n+1), \qquad \text{if } \epsilon(p) = 1 \\ \nu_2(p+1) &= \nu_2(n+1), \qquad \text{if } \epsilon(p) = -1. \end{aligned}$$

(2) *If $n \equiv 1 \pmod 4$,*

$$\begin{aligned} \nu_2(p+1) &= \nu_2(n+1) = 1 \\ \nu_2(p-1) &> \nu_2(n-1), \qquad \text{if } \epsilon(p) = 1 \\ \nu_2(p-1) &= \nu_2(n-1), \qquad \text{if } \epsilon(p) = -1. \end{aligned}$$

PROOF. We consider the following two cases:

(1) If $n \equiv 3 \pmod 4$:
Let p be a prime divisor of n with $\epsilon(p) = \left(\frac{x^2+4}{p}\right) = -1$. By Lemma 5.7 (applied to x^2+4 instead of x), and Lemma 5.5, we have

$$\begin{aligned} \nu_2(p+\epsilon(p)) &= \nu_2(p-1) \underset{(5.7)}{=} \nu_2(n-1) = 1 \\ \nu_2(p+1) &\underset{(5.5)}{=} \nu_2(n+1). \end{aligned}$$

Assume that there exists a prime divisor q of n with $\epsilon(q) = \left(\frac{x^2+4}{q}\right) = 1$. By Lemma 5.6, we have

$$\nu_2(q-1) \underset{(5.6)}{>} \nu_2(n+1), \tag{39}$$

and by Lemma 4.45, and (39),

$$\nu_2(q+\epsilon(q)) = \nu_2(q+1) \underset{(\nu_2(q-1)>1)}{=} 1.$$

(2) If $n \equiv 1 \pmod 4$:
Let p be a prime divisor of n with $\epsilon(p) = \left(\frac{x^2+4}{p}\right) = -1$. By Lemma 5.7, and Lemma 5.5, we have

$$\begin{aligned} \nu_2(p-1) &\underset{(5.7)}{=} \nu_2(n-1) \\ \nu_2(p+1) &\underset{(5.5)}{=} \nu_2(n+1) = 1. \end{aligned}$$

Assume that there exists a prime divisor q of n with $\epsilon(q) = \left(\frac{x^2+4}{q}\right) = 1$. By Lemma 5.7, we have

$$\nu_2(q-1) \underset{(5.7)}{>} \nu_2(n-1) > 1,$$

thus by Lemma 4.45

$$\nu_2(q+1) \underset{(4.45)}{=} 1 = \nu_2(n+1). \quad \square$$

COROLLARY 5.9. *Let n be an odd natural number, and x be an integer with*

$$(x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod{n},$$

and

$$c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod{n}.$$

Let p be a prime divisor of n such that $\left(\frac{x^2+4}{p}\right) = 1$. Then

$$\nu_2(p-1) \geq 3.$$

PROOF. If $n \equiv 3 \pmod 4$, then from Theorem 5.8 we have

$$\nu_2(p-1) > \nu_2(n+1) \geq 2.$$

If $n \equiv 1 \pmod 4$, then from Theorem 5.8 we have

$$\nu_2(p-1) > \nu_2(n-1) \geq 2. \quad \square$$

3.2. Recognition of Composite Numbers. In the following theorem we will see that Algorithm 5.2 returns the result false for at least one base if n is composite

THEOREM 5.10. *Let $n \neq 15$ be a squarefree odd natural number with prime factorization $\prod_{k=1}^{r} p_k$. If we have*

$$c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod{n}$$

for all $x \in (\mathbb{Z}/n\mathbb{Z})^*$ with $\left(\frac{x^2+4}{n}\right) = -1$, then n is prime.

PROOF. Assume n is composite. Choose p_1 such that $p_1 \notin \{3,5\}$. By Lemma 4.40, there exists $x_1 \in \mathbb{F}_{p_1}^*$ such that

$$\nu_2(\mathrm{ord}_{p_1}(c(1,x_1))) = 0. \tag{40}$$

Thus, we have $\left(\frac{x_1^2+4}{p_1}\right) = 1$. Moreover, by Theorem 4.32, there exist $x_k \in \mathbb{F}_{p_k}^*$ such that

$$\prod_{k=2}^{r} \left(\frac{x_k^2+4}{p_k}\right) = -1.$$

Then, by Chinese Remainder Theorem 2.5, there exists $x \in (\mathbb{Z}/n\mathbb{Z})^*$ such that

$$x \equiv x_k \pmod{p_k} \quad \text{for } 1 \leq k \leq n.$$

Therefore, we have $\left(\frac{x^2+4}{n}\right) = -1$. Hence, by the assertion of this theorem, we get

$$c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod{n}.$$

But by Lemma 5.6, we get

$$\nu_2(\mathrm{ord}_{p_1}(c(1,x_1))) \underset{(5.6)}{=} \nu_2(n+1) > 0$$

which contradicts (40). □

4. Commutator Curve Test

In this section an improved compositeness test which is based on the standard commutator curve is presented.

Algorithm 5.11 (Commutator Curve Test).
Input: $n, B \in \mathbb{N}$, *where* $B \geq 7$.
Output: $R \in \{\text{true}, \text{false}\}$.

(1) *If* $n \in \{p \in \mathbb{P} \mid p \leq B, p \leq n\}$, *terminate with the result* true.
(2) *If* $q \mid n$, *where* $q \in \{p \in \mathbb{P} \mid p \leq B, p < \sqrt{n}\}$, *terminate with the result* false.
(3) *If* n *is a perfect square, terminate with the result* false.
(4) *Choose* $x \in (\mathbb{Z}/n\mathbb{Z})^*$ *such that* $\left(\frac{x^2+4}{n}\right) \in \{0, -1\}$.
(5) *If* $\left(\frac{x^2+4}{n}\right) = 0$ *and* $c(1,x)^n \not\equiv -I_2 \pmod{n}$ *or if* $\left(\frac{x^2+4}{n}\right) = -1$ *and Algorithm 5.2 returns the result* false *for* x, *then terminate with the result* false, *otherwise terminate with the result* true.

This algorithm is an extension of Algorithm 5.2, and can also be formulated with polynomials or recurrence sequences which are discussed in the previous chapter. More details about different implementations and comparisons of running times can be found in Appendix C.
A little disadvantage of this algorithm is the requirement of a list which contains all prime numbers less than or equal to B. A fast algorithm to generate such a set is the sieve of Eratosthenes. But it is known today that this algorithm is only efficient for about $B \leq 10^7$ (see for example [**130**]).

This compositeness test, along with a fixed number of trial divisions for $B \geq 79$, returns for a composite number n the result true with a probability less than $\frac{1}{16}$, which will be proved in the next subsection. Thus, if k different bases x are chosen at random, this test returns the result true for a composite number n with a probability at most $(\frac{1}{16})^k$. We call that probability the *probability of error* of Algorithm 5.11.
Of course, if more than one iteration of Algorithm 5.11 is performed, steps 1, 2, and 3 can be omitted in subsequent iterations.

4.1. Probability of Error.

We define the following two sets to carry out the proofs in this subsection.

Definition 5.12. Let n be an odd integer greater than 2. We denote by $K(n)$ and $K'(n)$ the sets

$$K(n) := \{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid (x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod{n}\}$$

and

$$K'(n) := \{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{n}\right) = -1, c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod{n}\}.$$

By Theorem 3 of [**104**] it is known that

$$K(n) \subseteq \{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid (x^2+4)^{\frac{n-1}{2}} \equiv \left(\tfrac{x^2+4}{n}\right) \pmod{n}\}.$$

Therefore, we have

$$K(n) = \{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{n}\right) = -1, (x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod{n}\}.$$

But in general

$$\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod{n}\} \not\subseteq K'(n),$$

e.g. we have $c(1,12)^{\frac{377+1}{2}} \equiv -I_2 \pmod{377}$ and $\left(\frac{12^2+4}{377}\right) = 1$.

In many proofs in this subsection we observe the following correlation: the size of $|K'(n)|$ decreases if the size of $|K(n)|$ increases. By that property, an upper bound for the size of $|K(n) \cap K'(n)|$ can easily be estimated by the minimum of $\{|K(n)|, |K'(n)|\}$.

$K(n) = K'(n)$ may be possible, for example $K(343) = K'(343)$ with $|K(343)| = 1$ or $K(8911) = K'(8911)$ with $|K(8911)| = 445$.

The proof of main Theorem 5.28, which gives for $B \geq 79$ that Algorithm 5.11 returns the result true for a composite number n with a probability less than $\frac{1}{16}$, is split as follows:

(1) First, two lemmata give the exact number of elements in special subsets of cyclic groups which are the fundament of all further estimates of $|K(n)|$ and $|K'(n)|$.
(2) In the next lemma we will prove that the probability of error is very small in the case that n is not squarefree.
(3) After that, we formulate two lemmata, which give in general the base for upper bounds of $|K(n)|$.
(4) In addition, we consider ten lemmata for estimating upper bounds of the size of $K(n) \cap K'(n)$ in the cases of n being a product of two, three or four distinct odd prime numbers.
(5) Using the lemmata of this subsection, there follows a theorem with the assertion that the probability of error is less than $\frac{1}{16}$ for $B \geq 79$.

First, we state a well known lemma[5] which gives the exact number of elements in special subsets of cyclic groups.

LEMMA 5.13. *Let m, and n be positive integers with $n \geq 2$, and let G be a multiplicatively written cyclic group $(G, \cdot)$ with $|G| = n$. Then*

$$|\{x \in G \mid x^m = 1\}| = \gcd(n, m).$$

[5]See Theorem 1 in [**16**].

PROOF. Let $d := \gcd(n, m)$ and $g \in G$ be a generator and $1 \leq k \leq n$. Then an element g^k satisfies $g^{km} = 1$ if and only if $n \mid km$. This is equivalent to

$$\tfrac{n}{d} \mid k \cdot \tfrac{m}{d}.$$

By $\gcd(\frac{n}{d}, \frac{m}{d}) = 1$, we have $\frac{n}{d} \mid k$. Thus,

$$|\{x \in G \mid x^m = 1\}| = |\{1 \leq j \leq n \mid \tfrac{n}{d} \mid j\}| = |\{1 \leq j \leq d \mid j \cdot \tfrac{n}{d} \leq n\}| = d. \quad \square$$

LEMMA 5.14. *Let n be a natural number greater than 1, and write $n = q^s t$ where q is a prime number and $q \nmid t$. Let G be a multiplicatively written cyclic group $(G, \cdot)$ with $|G| = n$. Let $\xi \in G - \{1\}$ such that $\xi^q = 1$, and let r, and u be natural numbers with $r < s$ and $q \nmid u$. Then*

$$|\{x \in G \mid x^{q^r u} = \xi\}| = q^r \cdot \gcd(u, t).$$

PROOF. Let $x \in G$. Then there exists a generator $g \in G$, and natural number k less than n such that $x = g^k$ and $g^{\frac{n}{q}} = \xi$. From $g^{\frac{n}{q}} = \xi$, and $n = q^s t$, we get

$$\begin{aligned} |\{x \in G \mid x^{q^r u} = \xi\}| &= |\{x \in G \mid x^{q^r u} = g^{\frac{n}{q}}\}| \\ &= |\{x \in G \mid x^{q^r u} = g^{q^{s-1}t}\}| \\ &= |\{k \in \mathbb{N} \mid k < n, q^r u k \equiv q^{s-1} t \pmod{q^s t}\}|. \end{aligned}$$

Let $d := \gcd(q^r u, q^s t) = q^r \cdot \gcd(u, t)$. Then the congruence

$$k \cdot \tfrac{q^r u}{d} \equiv \tfrac{q^{s-1} t}{d} \pmod{\tfrac{q^s t}{d}}$$

has a unique solution. Therefore, the congruence

$$k \cdot \tfrac{q^r u}{d} \equiv \tfrac{q^{s-1} t}{d} \pmod{q^s t}$$

has d solutions as claimed. $\square$

LEMMA 5.15. *Let n be an odd composite number. If p is a prime divisor of n, and k a positive integer such that $p^k \mid n$, then*

$$|\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid x^{n-1} \equiv 1 \pmod{n}\}| \leq \tfrac{\varphi(n)}{p^{k-1}}.$$

PROOF. Let $x \in \{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid x^{n-1} \equiv 1 \pmod{n}\}$. By Lemma 5.13, there can be at most

$$\gcd(n-1, p^k - p^{k-1}) \underset{(p \mid n)}{=} \gcd(n-1, p-1) \leq p - 1$$

solutions to the congruence

$$x^{n-1} \equiv 1 \pmod{p^k}.$$

Therefore, by the Chinese Remainder Theorem 2.5, we have at most

$$\tfrac{\varphi(n)}{p^{k-1}}$$

solutions x to the congruence modulo n. $\square$

LEMMA 5.16. *Let n be a squarefree odd composite number, and let p be a prime divisor of n. Then*

$$|\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x^2+4}{p}\right) = 1, (x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod p\}| \leq \gcd(\prod_{\substack{\mathbb{P} \ni q \mid n \\ q \neq p}} q-1, p-1)$$

and

$$|\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x^2+4}{p}\right) = -1, (x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod p\}| \leq \gcd(\prod_{\substack{\mathbb{P} \ni q \mid n \\ q \neq p}} q-1, p-1).$$

PROOF. Let a, b be integers. If $\nu_2(a) > \nu_2(b)$, then

$$\nu_2(b) = \nu_2(a-b). \tag{41}$$

If $a \neq b$ and $\nu_2(a) = \nu_2(b)$, then

$$\nu_2(b) < \nu_2(a-b). \tag{42}$$

Assume there exists a prime divisor r of n, and $y \in \mathbb{F}_r^*$ such that

$$\left(\tfrac{y}{r}\right) = -\left(\tfrac{y}{n}\right) = 1 \quad \text{and} \quad y^{\frac{n-1}{2}} \equiv -1 \pmod r.$$

Then, by Lemma 5.7, we have

$$\nu_2(r-1) \underset{(5.7)}{>} \nu_2(n-1) \underset{(41)}{=} \nu_2((n-1)-(r-1)) = \nu_2(n-r). \tag{43}$$

Assume there exists a prime divisor r of n, and $y \in \mathbb{F}_r^*$ such that

$$\left(\tfrac{y}{r}\right) = \left(\tfrac{y}{n}\right) = -1 \quad \text{and} \quad y^{\frac{n-1}{2}} \equiv -1 \pmod r.$$

Then, by Lemma 5.7, we have

$$\nu_2(r-1) \underset{(5.7)}{=} \nu_2(n-1) \underset{(42)}{<} \nu_2((n-1)-(r-1)) = \nu_2(n-r). \tag{44}$$

Let $t := \nu_2(n-p)$. Then

$$\begin{aligned}
& |\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x^2+4}{p}\right) = 1, (x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod p\}| \\
\leq\ & 2 \cdot |\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x}{p}\right) = 1, x^{\frac{n-1}{2}} \equiv -1 \pmod p\}| \\
=\ & 2 \cdot |\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x}{p}\right) = 1, x^{\frac{n-1-(p-1)}{2}} \equiv -1 \pmod p\}| \\
=\ & 2 \cdot |\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x}{p}\right) = 1, x^{\frac{n-p}{2}} \equiv -1 \pmod p\}| \\
\underset{(5.14)}{=}\ & 2^t \cdot \gcd\left(\frac{n-p}{2^t}, \frac{p-1}{2^{\nu_2(p-1)}}\right) \\
\underset{(43)}{=}\ & \gcd(n-p, p-1) \\
\underset{(p \mid n)}{=}\ & \gcd(\prod_{\substack{\mathbb{P} \ni q \mid n \\ q \neq p}} q-1, p-1),
\end{aligned}$$

and

$$\begin{aligned}
& |\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x^2+4}{p}\right) = -1, (x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod p\}| \\
\leq\ & 2 \cdot |\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x}{p}\right) = -1, x^{\frac{n-1}{2}} \equiv -1 \pmod p\}| \\
=\ & 2 \cdot |\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x}{p}\right) = -1, x^{\frac{n-1-(p-1)}{2}} \equiv 1 \pmod p\}| \\
=\ & 2 \cdot |\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x}{p}\right) = -1, x^{\frac{n-p}{2}} \equiv 1 \pmod p\}| \\
=\ & 2 \cdot (|\{x \in \mathbb{F}_p^* \mid x^{\frac{n-p}{2}} \equiv 1 \pmod p\}| - |\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x}{p}\right) = 1, x^{\frac{n-p}{2}} \equiv 1 \pmod p\}|) \\
\underset{(5.13)}{=}\ & 2 \cdot (\gcd(\tfrac{n-p}{2}, p-1) - \gcd(\tfrac{n-p}{2}, \tfrac{p-1}{2})) \\
=\ & 2 \cdot \gcd(\tfrac{n-p}{2}, p-1) - \gcd(n-p, p-1) \\
\underset{(44)}{=}\ & 2 \cdot \gcd(n-p, p-1) - \gcd(n-p, p-1) \\
=\ & \gcd(n-p, p-1) \\
\underset{(p|n)}{=}\ & \gcd(\prod_{\substack{\mathbb{P} \ni q \mid n \\ q \neq p}} q-1, p-1). \quad \square
\end{aligned}$$

LEMMA 5.17. *Let n be an odd squarefree number with prime factorization $n = \prod_{k=1}^r p_k$. Then*

$$|K(n)| \leq \prod_{k=1}^r \gcd(p_k - 1, \prod_{\substack{l=1 \\ l \neq k}}^r p_l - 1).$$

PROOF. Let $n-1 = 2^t m$, and $p_k - 1 = 2^{t_k} m_k$ for all $1 \leq k \leq r$. Let $y \in K(n)$, and $\epsilon_k := \left(\frac{y}{p_k}\right)$. Then, by Lemma 5.7, we have $t_k \geq t$ for all $1 \leq k \leq r$, and $t_k = t$ if and only if $\epsilon_k = -1$. Therefore, the Legendre symbol is always equal for all elements of $K(n)$ over a prime divisor of n, i.e.

$$x_1, x_2 \in K(n) \qquad \Rightarrow \qquad \left(\tfrac{x_1^2+4}{p_k}\right) = \left(\tfrac{x_2^2+4}{p_k}\right) \quad \text{for all } 1 \leq k \leq r. \tag{45}$$

Thus, by the Chinese Remainder Theorem 2.5, and Lemma 5.16, we get the proof of the assertion as follows

$$\begin{aligned}
|K(n)| \quad &= \quad |\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid (x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod n\}| \\
&= \quad |\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{n}\right) = -1, (x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod n\}| \\
&\underset{(2.5),(45)}{=} \quad \prod_{k=1}^r |\{x \in \mathbb{F}_{p_k}^* \mid \left(\tfrac{x^2+4}{p_k}\right) = \epsilon_k, (x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod{p_k}\}| \\
&\underset{(5.16)}{\leq} \quad \prod_{k=1}^r \gcd(p_k - 1, \prod_{\substack{l=1 \\ l \neq k}}^r p_l - 1). \quad \square
\end{aligned}$$

EXAMPLE 5.18. *There exist many numbers like*

$$\begin{aligned}
87 &= 3 \cdot 29 \\
3653 &= 13 \cdot 281
\end{aligned}$$

$$51223 \;=\; 181 \cdot 283$$

which show that the upper bound of Lemma 5.17 cannot be improved in general.

LEMMA 5.19. *Let n be a squarefree odd composite number, and let p be a prime divisor of n. Then*

$$|\{M \in C_p^1 \mid \mathrm{ord}(M) \mid \tfrac{p-1}{2}, M^{\frac{n+1}{2}} \equiv -I_2 \pmod p\}| \leq \tfrac{1}{2} \cdot \gcd(\prod_{\substack{\mathbb{P} \ni q \mid n \\ q \neq p}} q+1, p-1)$$

and

$$|\{M \in C_p^1 \mid \mathrm{ord}(M) \mid p+1, M^{\frac{n+1}{2}} \equiv -I_2 \pmod p\}| \leq \tfrac{1}{2} \cdot \gcd(\prod_{\substack{\mathbb{P} \ni q \mid n \\ q \neq p}} q-1, p+1).$$

PROOF. Let a, b be integers. If $\nu_2(a) > \nu_2(b)$. Then

$$\nu_2(b) = \nu_2(a+b). \tag{46}$$

If $a \neq b$ and $\nu_2(a) = \nu_2(b)$, then

$$\nu_2(b) < \nu_2(a-b). \tag{47}$$

Assume there exists a prime divisor q of n, and $y \in K'(n)$ such that

$$\left(\tfrac{y^2+4}{n}\right) = -\left(\tfrac{y^2+4}{q}\right) = -1.$$

Then, by Lemma 5.6, we have

$$\nu_2(q-1) \underset{(5.6)}{>} \nu_2(n+1) \underset{(46)}{=} \nu_2((n+1)+(q_2-1)) = \nu_2(n+q). \tag{48}$$

Assume there exists a prime divisor q of n, and $y \in K'(n)$ such that

$$\left(\tfrac{y^2+4}{n}\right) = \left(\tfrac{y^2+4}{q}\right) = -1.$$

Then, by Lemma 5.5, we have

$$\nu_2(q+1) \underset{(5.5)}{=} \nu_2(n+1) \underset{(47)}{<} \nu_2((n+1)-(q+1)) = \nu_2(n-q). \tag{49}$$

Let $t := \nu_2(n+p)$, and let $G \subseteq \mathbb{F}_{p^2}^*$ be a cyclic group of order $p+1$. Then

$$\begin{aligned}
& |\{M \in C_p^1 \mid \mathrm{ord}(M) \mid \tfrac{p-1}{2}, M^{\frac{n+1}{2}} \equiv -I_2 \pmod p\}| \\
\underset{(4.40)}{\leq} \; & |\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x}{p}\right) = 1, x^{\frac{n+1}{2}} \equiv -1 \pmod p\}| \\
= \; & |\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x}{p}\right) = 1, x^{\frac{n+1+(p-1)}{2}} \equiv -1 \pmod p\}| \\
= \; & |\{x \in \mathbb{F}_p^* \mid \left(\tfrac{x}{p}\right) = 1, x^{\frac{n+p}{2}} \equiv -1 \pmod p\}| \\
\underset{(5.14)}{=} \; & 2^{t-1} \cdot \gcd\left(\frac{n+p}{2^t}, \frac{p-1}{2^{\nu_2(p-1)}}\right) \\
\underset{(48)}{=} \; & \tfrac{1}{2} \cdot \gcd(n+p, p-1) \\
\underset{(p \mid n)}{=} \; & \tfrac{1}{2} \cdot \gcd(\prod_{\substack{\mathbb{P} \ni q \mid n \\ q \neq p}} q+1, p-1),
\end{aligned}$$

and

$$\begin{aligned}
& |\{M \in C_p^1 \mid \mathrm{ord}(M) \mid p+1, M^{\frac{n+1}{2}} \equiv -I_2 \pmod p\}| \\
\underset{(4.42)}{\leq} & |\{x \in G \mid \mathrm{ord}(x) \nmid \tfrac{p+1}{2}, x^{\frac{n+1}{2}} = -1\}| \\
= & |\{x \in G \mid \mathrm{ord}(x) \nmid \tfrac{p+1}{2}, x^{\frac{n+1-(p+1)}{2}} = 1\}| \\
= & |\{x \in G \mid \mathrm{ord}(x) \nmid \tfrac{p+1}{2}, x^{\frac{n-p}{2}} = 1\}| \\
= & |\{x \in G \mid x^{\frac{n-p}{2}} = 1\}| - |\{x \in G \mid \mathrm{ord}(x) \mid \tfrac{p+1}{2}, x^{\frac{n-p}{2}} = 1\}| \\
\underset{(5.13)}{=} & \gcd(\tfrac{n-p}{2}, p+1) - \gcd(\tfrac{n-p}{2}, \tfrac{p+1}{2}) \\
= & \gcd(\tfrac{n-p}{2}, p+1) - \tfrac{1}{2} \cdot \gcd(n-p, p+1) \\
\underset{(49)}{=} & \gcd(n-p, p+1) - \tfrac{1}{2} \cdot \gcd(n-p, p+1) \\
= & \tfrac{1}{2} \cdot \gcd(n-p, p+1) \\
\underset{(p|n)}{=} & \tfrac{1}{2} \cdot \gcd(\prod_{\substack{\mathbb{P} \ni q \mid n \\ q \neq p}} q-1, p+1). \quad \square
\end{aligned}$$

LEMMA 5.20. *Let $n \equiv 3 \pmod 4$ be a product of two distinct odd prime numbers*

$$p_1 = 2^{s_1} t_1 + 1 \quad \text{and} \quad p_2 = 2^{s_2} t_2 + 1,$$

where t_1 and t_2 are odd. Then

$$|K'(n)| \leq \begin{cases} \frac{1}{4} \cdot \gcd(p_1+1, p_2-1)^2, & \text{if } s_1 < s_2 \\ \frac{1}{4} \cdot \gcd(p_1-1, p_2+1)^2, & \text{if } s_1 > s_2. \end{cases}$$

PROOF. Let $k \in \{1,2\}$. By Lemma 5.19, we have

$$\begin{aligned}
d_k := & |\{M \in C_{p_k}^1 \mid \mathrm{ord}(M) \mid \tfrac{p_k-1}{2}, M^{\frac{n+1}{2}} \equiv -I_2 \pmod{p_k}\}| \\
\underset{(5.19)}{=} & \begin{cases} \frac{1}{2} \cdot \gcd(p_2+1, p_1-1), & \text{if } k=1 \\ \frac{1}{2} \cdot \gcd(p_1+1, p_2-1), & \text{if } k=2 \end{cases}
\end{aligned}$$

and

$$\begin{aligned}
d'_k := & |\{M \in C_{p_k}^1 \mid \mathrm{ord}(M) \mid p_k+1, M^{\frac{n+1}{2}} \equiv -I_2 \pmod{p_k}\}| \\
\underset{(5.19)}{=} & \begin{cases} \frac{1}{2} \cdot \gcd(p_2-1, p_1+1), & \text{if } k=1 \\ \frac{1}{2} \cdot \gcd(p_1-1, p_2+1), & \text{if } k=2. \end{cases}
\end{aligned}$$

If $s_1 > s_2$, then, by Lemma 5.5, and Lemma 5.6, we have $\left(\frac{x^2+4}{p_1}\right) = -\left(\frac{x^2+4}{p_2}\right) = 1$. Therefore,

$$\begin{aligned}
|K'(n)| = & |\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{n}\right) = -1, c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod n\}| \\
= & |\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{p_1}\right) = -\left(\tfrac{x^2+4}{p_2}\right) = 1, c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod n\}| \\
\underset{(4.7)}{\leq} & d_1 \cdot d'_2 \\
= & \tfrac{1}{4} \cdot \gcd(p_2+1, p_1-1)^2.
\end{aligned}$$

If $s_1 < s_2$, then, by Lemma 5.5, and Lemma 5.6, we have $-\left(\frac{x^2+4}{p_1}\right) = \left(\frac{x^2+4}{p_2}\right) = 1$. Therefore,

$$\begin{aligned} |K'(n)| &= |\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{n}\right) = -1, c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod n\}| \\ &= |\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{p_1}\right) = -\left(\tfrac{x^2+4}{p_2}\right) = -1, c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod n\}| \\ &\underset{(4.7)}{\leq} d_1' \cdot d_2 \\ &= \tfrac{1}{4} \cdot \gcd(p_1+1, p_2-1)^2. \quad \square \end{aligned}$$

Example 5.21. *There exist many numbers like*

$$\begin{aligned} 51 &= 3 \cdot 17 \\ 4559 &= 47 \cdot 97 \\ 27971 &= 83 \cdot 337 \end{aligned}$$

which show that the upper bound of Lemma 5.20 cannot be improved in general.

Lemma 5.22. *Let $n \equiv 1 \pmod 4$ be a product of two distinct odd prime numbers p_1 and p_2. Then*

$$|K'(n)| \leq \tfrac{1}{4} \cdot (\gcd(p_2+1, p_1-1)^2 + \gcd(p_1+1, p_2-1)^2).$$

Proof. Let $k \in \{1,2\}$. By Lemma 5.19, we have

$$\begin{aligned} d_k &:= |\{M \in C^1_{p_k} \mid \operatorname{ord}(M) \mid \tfrac{p_k-1}{2}, M^{\frac{n+1}{2}} \equiv -I_2 \pmod{p_k}\}| \\ &\underset{(5.19)}{=} \begin{cases} \frac{1}{2} \cdot \gcd(p_2+1, p_1-1), & \text{if } k=1 \\ \frac{1}{2} \cdot \gcd(p_1+1, p_2-1), & \text{if } k=2 \end{cases} \end{aligned}$$

and

$$\begin{aligned} d_k' &:= |\{M \in C^1_{p_k} \mid \operatorname{ord}(M) \mid p_k+1, M^{\frac{n+1}{2}} \equiv -I_2 \pmod{p_k}\}| \\ &\underset{(5.19)}{=} \begin{cases} \frac{1}{2} \cdot \gcd(p_2-1, p_1+1), & \text{if } k=1 \\ \frac{1}{2} \cdot \gcd(p_1-1, p_2+1), & \text{if } k=2. \end{cases} \end{aligned}$$

Then we have

$$\begin{aligned} |K'(n)| &= |\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{n}\right) = -1, c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod n\}| \\ &= |\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{p_1}\right) = -\left(\tfrac{x^2+4}{p_2}\right) = 1, c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod n\}| \\ &\quad + |\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{p_1}\right) = -\left(\tfrac{x^2+4}{p_2}\right) = -1, c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod n\}| \\ &\underset{(4.7)}{\leq} d_1 \cdot d_2' + d_1' \cdot d_2 \\ &= \tfrac{1}{4} \cdot (\gcd(p_2+1, p_1-1)^2 + \gcd(p_1+1, p_2-1)^2). \quad \square \end{aligned}$$

Lemma 5.23. *Let n be a product of two distinct odd prime numbers*

$$p_1 = 2^{s_1}t_1 + 1 \quad \text{and} \quad p_2 = 2^{s_2}t_2 + 1,$$

where t_1 and t_2 are odd. Then

$$|K(n)\cap K'(n)| \leq \begin{cases} \frac{p_1-1}{2}\,, & \text{if } s_1 > s_2 \\ \frac{p_2-1}{2}\,, & \text{if } s_1 < s_2 \\ 0\,, & \text{else.} \end{cases}$$

PROOF. Let $d_1 := \gcd(p_1-1, p_2-1)$, and $d_2 := \gcd(p_1-1, p_2+1)$.
If $K(n)\cap K'(n) \neq \emptyset$, then, by Theorem 5.8, we have $s_1 \neq s_2$. If $s_1 > s_2$, then

$$d_1 d_2 \mid p_1 - 1. \tag{50}$$

By Theorem 5.8, Lemma 5.17, Lemma 5.19, and Lemma 5.20, we have

$$\begin{array}{lll} & |K(n)\cap K'(n)| & \\ = & \min\{|K(n)|, |K(n)\cap K'(n)|\} & \\ \underset{(5.8)}{=} & \min\{|K(n)|, |\{x\in(\mathbb{Z}/n\mathbb{Z})^* \mid \left(\frac{x^2+4}{p_1}\right) = -\left(\frac{x^2+4}{p_2}\right) = 1\}\cap K'(n)|\} & \\ \underset{(5.17),(5.19),(5.20)}{\leq} & \min\{d_1^2, \tfrac{1}{4}\cdot d_2^2\} & \\ \underset{(50)}{\leq} & \min\{d_1^2, (\tfrac{p_1-1}{2d_1})^2\} & \\ \leq & \frac{p_1-1}{2}. & \end{array}$$

If $s_1 < s_2$, then the proof of the assertion is similar. □

LEMMA 5.24. *Let m_0 be a positive integer, and let m_1, m_2, m_3 be distinct positive integers. Then*

$$\begin{array}{rcl} (m_0m_1m_2-1)(m_0m_1m_3-1)(m_0m_2m_3-1) & > & m_0^3((m_1^2-1)(m_2^2-1)(m_3^2-1)+1) \\ & & + m_0^2(m_1+m_2+m_3). \end{array}$$

PROOF. Let a, b be positive integers. Then we have the following relation

$$\begin{array}{lll} & m_0^3a^2b^2 + m_0ab - m_0^3a^2 - m_0^2a^2b^2 - m_0^2ab + m_0^2a^2 & \\ = & m_0a((ab^2-a)m_0^2 - (ab^2-a+b)m_0 + b) & \\ = & m_0a(m_0-1)(m_0 - \frac{b}{a(b^2-1)}) & \\ \underset{(a,b,m_0\geq 1)}{\geq} & 0. & \end{array} \tag{51}$$

Assume $m_1 > m_2 > m_3$. Then the proof of the assertion follows by

$$\begin{array}{ll} & (m_0m_1m_2-1)(m_0m_1m_3-1)(m_0m_2m_3-1) - m_0^3(m_1^2-1)(m_2^2-1)(m_3^2-1) - m_0^3 \\ = & (m_0^2m_1^2m_2m_3 - m_0m_1m_2 - m_0m_1m_3 + 1)(m_0m_2m_3-1) \\ & - m_0^3(m_1^2m_2^2 - m_1^2 - m_2^2 + 1)(m_3^2-1) - m_0^3 \\ = & m_0^3m_1^2m_2^2m_3^2 - m_0^2m_1^2m_2m_3 - m_0^2m_1m_2^2m_3 - m_0^2m_1m_2m_3^2 + m_0m_1m_2 + m_0m_1m_3 \\ & + m_0m_2m_3 - m_0^3(m_1^2m_2^2m_3^2 - m_1^2m_3^2 - m_2^2m_3^2 - m_1^2m_2^2 + m_1^2 + m_2^2 + m_3^2) - 1 \\ = & m_0^3m_1^2m_3^2 + m_0^3m_2^2m_3^2 + m_0^3m_1^2m_2^2 + m_0m_1m_2 + m_0m_1m_3 + m_0m_2m_3 \\ & - m_0^2m_1^2m_2m_3 - m_0^2m_1m_2^2m_3 - m_0^2m_1m_2m_3^2 - m_0^3m_1^2 - m_0^3m_2^2 - m_0^3m_3^2 - 1 \end{array}$$

$$
\begin{aligned}
&\underset{(51)}{\geq} && m_0^2m_1^2m_3^2 + m_0^2m_2^2m_3^2 + m_0^2m_1^2m_2^2 + m_0^2m_1m_2 + m_0^2m_1m_3 + m_0^2m_2m_3 \\
&&& - m_0^2m_1^2m_2m_3 - m_0^2m_1m_2^2m_3 - m_0^2m_1m_2m_3^2 - m_0^2m_1^2 - m_0^2m_2^2 - m_0^2m_3^2 - 1 \\
&> && m_0^2m_1^2m_3^2 + m_0^2m_2^2m_3^2 + m_0^2m_1^2m_2^2 + m_0^2m_1m_3 \\
&&& - m_0^2m_1^2m_2m_3 - m_0^2m_1m_2^2m_3 - m_0^2m_1m_2m_3^2 - m_0^2m_1^2 \\
&= && m_0^2(m_1^2m_3^2 + m_2^2m_3^2 + m_1^2m_2^2 - m_1^2m_2m_3 - m_1^2) \\
&&& - m_0^2m_1m_2^2m_3 - m_0^2m_1m_2m_3^2 + m_0^2m_1m_3 \\
&= && m_0^2(m_1^2(m_3 - m_2)^2 + m_1^2m_2m_3 + m_2^2m_3^2 - m_1^2) \\
&&& - m_0^2m_1m_2^2m_3 - m_0^2m_1m_2m_3^2 + m_0^2m_1m_3 \\
&\geq && m_0^2(m_1^2m_2m_3 + m_2^2m_3^2) - m_0^2m_1m_2^2m_3 - m_0^2m_1m_2m_3^2 + m_0^2m_1m_3 \\
&= && m_0^2m_2m_3(m_1^2 + m_2m_3) - m_0^2m_1m_2^2m_3 - m_0^2m_1m_2m_3^2 + m_0^2m_1m_3 \\
&= && m_0^2m_2m_3(m_1^2 + (m_1 - (m_1 - m_2))(m_1 - (m_1 - m_3))) \\
&&& - m_0^2m_1m_2^2m_3 - m_0^2m_1m_2m_3^2 + m_0^2m_1m_3 \\
&= && m_0^2m_2m_3(2m_1^2 - m_1(m_1 - m_2) - m_1(m_1 - m_3) + (m_1 - m_2)(m_1 - m_3)) \\
&&& - m_0^2m_1m_2^2m_3 - m_0^2m_1m_2m_3^2 + m_0^2m_1m_3 \\
&\geq && m_0^2m_2m_3(2m_1^2 - m_1(m_1 - m_2) - m_1(m_1 - m_3) + 2) \\
&&& - m_0^2m_1m_2^2m_3 - m_0^2m_1m_2m_3^2 + m_0^2m_1m_3 \\
&= && m_0^2m_2m_3(m_1m_2 + m_1m_3) - m_0^2m_1m_2^2m_3 - m_0^2m_1m_2m_3^2 + m_0^2m_3(m_1 + 2m_2) \\
&> && m_0^2m_3(m_1 + m_2 + m_3). \quad \square
\end{aligned}
$$

LEMMA 5.25. *Let $B \geq 2$ be a positive integer, and let m_1, m_2, m_3 be distinct positive integers which are greater than B. Let*

$$
\begin{aligned}
d_1 &:= \gcd(m_2m_3 - 1, m_1 - 1), \\
d_2 &:= \gcd(m_1m_3 - 1, m_2 - 1), \\
d_3 &:= \gcd(m_1m_2 - 1, m_3 - 1), \\
d_1' &:= \gcd(m_2m_3 - 1, m_1 + 1), \\
d_2' &:= \gcd(m_1m_3 - 1, m_2 + 1), \\
\textit{and} \quad d_3' &:= \gcd(m_1m_2 - 1, m_3 + 1).
\end{aligned}
$$

Then

$$d_1d_2d_3d_1'd_2'd_3' < \tfrac{3(B+1)^3}{(B^2-3)(B-1)^3} \cdot (m_1 - 1)^2(m_2 - 1)^2(m_3 - 1)^2.$$

PROOF. Let

$$A := \frac{(m_1^2 - 1)(m_2^2 - 1)(m_3^2 - 1)}{d_1d_2d_3d_1'd_2'd_3'} \quad \text{and} \quad A' := \frac{(m_1m_2 - 1)(m_1m_3 - 1)(m_2m_3 - 1)}{d_1d_2d_3d_1'd_2'd_3'},$$

then, by Lemma 5.24, we have $A' > A$. Therefore,

$$
\begin{aligned}
1 + \frac{1}{A} &= \frac{A + 1}{A} \\
&\leq \frac{A'}{A} < \frac{(m_1m_2 - 1)(m_1m_3 - 1)(m_2m_3 - 1)}{(m_1^2 - 1)(m_2^2 - 1)(m_3^2 - 1)}
\end{aligned}
$$

$$\begin{aligned}
&= \frac{(m_1^2m_2m_3 - m_1m_2 - m_1m_3 + 1)(m_2m_3 - 1)}{(m_1^2m_2^2 - m_1^2 - m_2^2 + 1)(m_3^2 - 1)} \\
&= \frac{m_1^2m_2^2m_3^2 - m_1^2m_2m_3 - m_1m_2^2m_3 - m_1m_2m_3^2}{m_1^2m_2^2m_3^2 - m_1^2m_3^2 - m_2^2m_3^2 - m_1^2m_2^2 + m_1^2 + m_2^2 + m_3^2 - 1} \\
&\quad + \frac{m_1m_2 + m_1m_3 + m_2m_3 - 1}{m_1^2m_2^2m_3^2 - m_1^2m_3^2 - m_2^2m_3^2 - m_1^2m_2^2 + m_1^2 + m_2^2 + m_3^2 - 1} \\
&< \frac{m_1^2m_2^2m_3^2}{m_1^2m_2^2m_3^2 - m_1^2m_3^2 - m_2^2m_3^2 - m_1^2m_2^2} \\
&= \frac{1}{1 - (m_1^2m_3^2 + m_2^2m_3^2 + m_1^2m_2^2)/(m_1m_2m_3)^2} \\
&< \frac{1}{1 - \frac{3}{B^2}} \\
&= \frac{B^2}{B^2 - 3} \\
&= 1 + \frac{3}{B^2 - 3}.
\end{aligned}$$

Thus,

$$A > \frac{B^2 - 3}{3}.$$

Therefore,

$$\begin{aligned}
d_1d_2d_3d_1'd_2'd_3' &< \tfrac{3}{B^2-3} \cdot (m_1^2 - 1)(m_2^2 - 1)(m_3^2 - 1) \\
&< \tfrac{3(B+1)^3}{(B^2-3)(B-1)^3} \cdot (m_1 - 1)^2(m_2 - 1)^2(m_3 - 1)^2. \quad \square
\end{aligned}$$

LEMMA 5.26. *Let B be a positive integer with $B \geq 3$, and let n be a product of three distinct odd prime numbers p_1, p_2, and p_3 such that all prime divisors of n are greater than B. Then*

$$|K(n) \cap K'(n)| < \tfrac{\sqrt{6}(B+1)^2}{4B(B-1)^2} \cdot \varphi(n).$$

PROOF. Let

$$\begin{aligned}
d_1 &:= \gcd(p_2p_3 - 1, p_1 - 1), d_2 := \gcd(p_1p_3 - 1, p_2 - 1), d_3 := \gcd(p_1p_2 - 1, p_3 - 1), \\
d_4 &:= \gcd(p_2p_3 - 1, p_1 + 1), d_5 := \gcd(p_1p_3 - 1, p_2 + 1), d_6 := \gcd(p_1p_2 - 1, p_3 + 1), \\
d_7 &:= \gcd(p_2p_3 + 1, p_1 - 1), d_8 := \gcd(p_1p_3 + 1, p_2 - 1).
\end{aligned}$$

By

$$B^3 - B^2 \underset{(B \geq 3)}{<} B^3 - 3B + B^2 - 3,$$

we have

$$\tfrac{1}{B^2-3} < \tfrac{B+1}{(B-1)B^2}. \tag{52}$$

Assume $\nu_2(p_1-1)=\nu_2(p_2-1)=\nu_2(p_3-1)$. Then, by Theorem 5.8, Lemma 5.17, Lemma 5.19, and Lemma 5.25, we have

$$\begin{aligned}
& |K(n)\cap K'(n)| \\
\leq\ & \min\{|K(n)|, |K(n)\cap K'(n)|\} \\
\underset{(5.8)}{\leq}\ & \min\{|K(n)|, |\{x\in(\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{p_1}\right)=\left(\tfrac{x^2+4}{p_2}\right)=\left(\tfrac{x^2+4}{p_3}\right)=-1\}\cap K'(n)|\} \\
\underset{(5.17),(5.19)}{\leq}\ & \min\{d_1d_2d_3, \tfrac{1}{8}\cdot d_4d_5d_6\} \\
\underset{(5.25)}{<}\ & \min\{d_1d_2d_3, \tfrac{3(B+1)^3\varphi(n)^2}{8(B^2-3)(B-1)^3d_1d_2d_3}\} \\
\underset{(52)}{<}\ & \min\{d_1d_2d_3, \tfrac{3(B+1)^4\varphi(n)^2}{8B^2(B-1)^4d_1d_2d_3}\} \\
\leq\ & \tfrac{\sqrt{6}(B+1)^2}{4B(B-1)^2}\cdot\varphi(n).
\end{aligned}$$

Assume $\nu_2(p_1-1)>\nu_2(p_3-1)$ and $\nu_2(p_2-1)>\nu_2(p_3-1)$. Then

$$d_1d_7 \mid p_1-1, \quad \text{and} \quad d_2d_8 \mid p_2-1. \tag{53}$$

By Theorem 5.8, Lemma 5.17, and Lemma 5.19, we have

$$\begin{aligned}
& |K(n)\cap K'(n)| \\
\leq\ & \min\{|K(n)|, |K(n)\cap K'(n)|\} \\
\underset{(5.8)}{\leq}\ & \min\{|K(n)|, |\{x\in(\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{p_1}\right)=\left(\tfrac{x^2+4}{p_2}\right)=-\left(\tfrac{x^2+4}{p_3}\right)=1\}\cap K'(n)|\} \\
\underset{(5.17),(5.19)}{\leq}\ & \min\{d_1d_2d_3, \tfrac{1}{8}\cdot d_6d_7d_8\} \\
\underset{(53)}{\leq}\ & \min\{d_1d_2d_3, \tfrac{(p_1-1)(p_2-1)(p_3^2-1)}{8d_1d_2d_3}\} \\
<\ & \min\{d_1d_2d_3, \tfrac{\varphi(n)^2}{8B^2d_1d_2d_3}\} \\
\leq\ & \tfrac{\sqrt{2}}{4B}\cdot\varphi(n).
\end{aligned}$$

Combination of these two cases completes the proof of the assertion. □

LEMMA 5.27. *Let B be a positive integer with $B\geq 17$, and let n be a product of four distinct odd prime numbers p_1, p_2, p_3, and p_4 such that all prime divisors of n are greater than B. Then*

$$|K(n)\cap K'(n)| < \tfrac{\sqrt{5}}{8\sqrt{B}}\cdot\varphi(n).$$

PROOF. Let

$$\begin{aligned}
d_1 &:= \gcd(p_2p_3p_4-1, p_1-1), d_2 := \gcd(p_1p_3p_4-1, p_2-1), \\
d_3 &:= \gcd(p_1p_2p_4-1, p_3-1), d_4 := \gcd(p_1p_2p_3-1, p_4-1), \\
d_5 &:= \gcd(p_1p_3p_4-1, p_2+1), d_6 := \gcd(p_1p_2p_4-1, p_3+1), \\
d_7 &:= \gcd(p_1p_2p_3-1, p_4+1), d_8 := \gcd(p_2p_3p_4+1, p_1-1), \\
d_9 &:= \gcd(p_1p_3p_4+1, p_2-1), d_{10} := \gcd(p_1p_2p_4+1, p_3-1).
\end{aligned}$$

We have

$$4B(p_2+1)(p_3+1)(p_4+1) \underset{(B\geq 17)}{<} 5(p_1-1)(p_2-1)(p_3-1)(p_4-1). \tag{54}$$

Assume $\nu_2(p_1-1) > \nu_2(p_2-1) = \nu_2(p_3-1) = \nu_2(p_4-1)$. Then

$$d_1 d_9 \mid p_1 - 1. \tag{55}$$

By Theorem 5.8, Lemma 5.17, and Lemma 5.19, we have

$$\begin{aligned}
& |K(n) \cap K'(n)| \\
\leq\ & \min\{|K(n)|, |K(n) \cap K'(n)|\} \\
\underset{(5.8)}{\leq}\ & \min\{|K(n)|, \\
& \quad |\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid -\left(\tfrac{x^2+4}{p_1}\right) = \left(\tfrac{x^2+4}{p_2}\right) = \left(\tfrac{x^2+4}{p_3}\right) = \left(\tfrac{x^2+4}{p_4}\right) = -1\} \cap K'(n)|\} \\
\underset{(5.17),(5.19)}{\leq}\ & \min\{d_1d_2d_3d_4, \tfrac{1}{16} \cdot d_5d_6d_7d_8\} \\
\underset{(55)}{\leq}\ & \min\{d_1d_2d_3d_4, \tfrac{(p_1-1)(p_2^2-1)(p_3^2-1)(p_4^2-1)}{16d_1d_2d_3d_4}\} \\
\underset{(54)}{<}\ & \min\{d_1d_2d_3d_4, \tfrac{5\varphi(n)^2}{64Bd_1d_2d_3d_4}\} \\
\leq\ & \tfrac{\sqrt{5}}{8\sqrt{B}} \cdot \varphi(n).
\end{aligned}$$

Assume $\nu_2(p_1-1), \nu_2(p_2-1)$, and $\nu_2(p_3-1)$ are greater than $\nu_2(p_4-1)$. Then

$$d_1 d_8 \mid p_1 - 1, d_2 d_9 \mid p_2 - 1, \text{ and } d_3 d_{10} \mid p_3 - 1. \tag{56}$$

By Theorem 5.8, Lemma 5.17, and Lemma 5.19, we have

$$\begin{aligned}
& |K(n) \cap K'(n)| \\
\leq\ & \min\{|K(n)|, |K(n) \cap K'(n)|\} \\
\underset{(5.8)}{\leq}\ & \min\{|K(n)|, \\
& \quad |\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\tfrac{x^2+4}{p_1}\right) = \left(\tfrac{x^2+4}{p_2}\right) = \left(\tfrac{x^2+4}{p_3}\right) = -\left(\tfrac{x^2+4}{p_4}\right) = 1\} \cap K'(n)|\} \\
\underset{(5.17),(5.19)}{\leq}\ & \min\{d_1d_2d_3d_4, \tfrac{1}{16} \cdot d_7d_8d_9d_{10}\} \\
\underset{(56)}{\leq}\ & \min\{d_1d_2d_3d_4, \tfrac{(p_1-1)(p_2-1)(p_3-1)(p_4^2-1)}{16d_1d_2d_3d_4}\} \\
<\ & \min\{d_1d_2d_3d_4, \tfrac{\varphi(n)^2}{16B^3d_1d_2d_3d_4}\} \\
\leq\ & \tfrac{1}{4\sqrt{B^3}} \cdot \varphi(n).
\end{aligned}$$

Combination of these two cases completes the proof of the assertion. □

THEOREM 5.28. *Let n be a composite number. Then Algorithm 5.11 returns for n and $B \geq 79$ the result* true *with probability less than $\frac{1}{16}$.*

PROOF. By the first step of Algorithm 5.11, we know that the least prime divisor of n is greater than 82. Let r be the number of prime divisors of n.
First, we assume that n is not squarefree. Let $\prod_{k=1}^{r} p_k^{a_k}$ be the prime factorization of n. Then, by the third step of Algorithm 5.11, we know that n is not a perfect square.

Hence, we can choose p_1 such that a_1 is odd. Then by Lemma 5.15, Algorithm 5.11 returns the result true with the probability

$$\begin{aligned}
\frac{|K(n)\cap K'(n)|}{|L_{-1}(n)\cup L_0(n)|} &\underset{(4.38),(5.15)}{\leq} \frac{2\cdot\varphi(n)}{83\cdot(\varphi(n)-2\cdot(-2)^{r-1}\prod_{k=1}^{r}p_k^{a_k-1}(1-\delta_k\cdot\frac{p_k+1}{2}))}\\
&\leq \frac{2\cdot\varphi(n)}{83\cdot(\varphi(n)-2^r p_1^{a_1-1}\prod_{k=2}^{r}p_k^{a_k-1}\cdot\frac{p_k-1}{2})}\\
&= \frac{2\cdot\varphi(n)}{83\cdot(\varphi(n)-2p_1^{a_1-1}\cdot\varphi(\frac{n}{p_1}))}\\
&= \frac{2}{83\cdot(1-\frac{2}{p_1-1})}\\
&\leq \frac{2}{83\cdot(1-\frac{1}{41})}\\
&< \frac{1}{40}\,,
\end{aligned}$$

as claimed.

Now we may assume that n is squarefree. If $r=2$, then by Theorem 4.38, and Lemma 5.23, Algorithm 5.11 returns the result true with the probability

$$\frac{|K(n)\cap K'(n)|}{|L_{-1}(n)\cup L_0(n)|} \underset{(4.38),(5.23)}{\leq} \frac{2}{\varphi(n)-4}\cdot\frac{\varphi(n)}{2\cdot 83} < \frac{1}{82}\,.$$

If $r=3$, then by Theorem 4.38, and Lemma 5.26, Algorithm 5.11 returns the result true with the probability

$$\frac{|K(n)\cap K'(n)|}{|L_{-1}(n)\cup L_0(n)|} \underset{(4.38),(5.26)}{\leq} \frac{2}{\varphi(n)+8}\cdot\frac{\sqrt{6}\cdot\varphi(n)}{4\cdot 83}\cdot\left(\frac{83+1}{83-1}\right)^2 < \frac{1}{64}\,.$$

If $r=4$, then by Theorem 4.38, and Lemma 5.27, Algorithm 5.11 returns the result true with the probability

$$\frac{|K(n)\cap K'(n)|}{|L_{-1}(n)\cup L_0(n)|} \underset{(4.38),(5.27)}{<} \frac{2}{\varphi(n)-16}\cdot\frac{\sqrt{5}\cdot\varphi(n)}{8\cdot\sqrt{83}} < \frac{1}{16}\,.$$

If $r\geq 5$, then, by Theorem 5.8, we have

$$\left(\tfrac{x_1^2+4}{p_k}\right)=\left(\tfrac{x_2^2+4}{p_k}\right) \quad \text{for all } x_1,x_2\in K(n)\cap K'(n) \text{ and } 1\leq k\leq r.$$

Therefore, by Lemma 5.19, we have

$$|K(n)\cap K'(n)| \underset{(5.8),(5.19)}{\leq} \frac{\varphi(n)}{2^r}\,. \tag{57}$$

By Theorem 4.38, Algorithm 5.11 returns the result true with the probability

$$\frac{|K(n)\cap K'(n)|}{|L_{-1}(n)\cup L_0(n)|} \underset{(4.38),(57)}{\leq} \frac{1}{2^{r-1}+\frac{2\cdot(-1)^{r-1}}{\varphi(n)}} < \frac{1}{16}\,,$$

as claimed. □

5. Discussion

If we analyse the numerical values of Appendix B, it seems to be possible to improve Lemma 5.23 by the following conjecture.

CONJECTURE 5.29. *Let n be a product of two distinct odd prime numbers p_1 and p_2. Then*

$$|K(n) \cap K'(n)| \leq \min\{p_1 - 1, p_2 - 1\}.$$

Unfortunatelly, this conjecture cannot be proved by the techniques described in this dissertation. I can only verify that this upper bound is correct for all odd composite numbers less than 10^7 (see Appendix B). Moreover, the following table shows that this upper bound cannot be improved.

n	$\lvert K(n)\rvert$	$\lvert K'(n)\rvert$	$\lvert K(n) \cap K'(n)\rvert$
$1102121 = 41 \cdot 26881$	$400 = 40^2/4$	400	40
$2589949 = 109 \cdot 23761$	$2916 = 108^2/4$	2916	108
$5142569 = 137 \cdot 37537$	$4624 = 136^2/4$	4624	136
$5188709 = 29 \cdot 178921$	$196 = 28^2/4$	196	28
$5639129 = 89 \cdot 63361$	$1936 = 88^2/4$	1936	88
$6548309 = 53 \cdot 123553$	$676 = 52^2/4$	676	52
$7214033 = 113 \cdot 63841$	$3136 = 112^2/4$	3136	112
$7739629 = 157 \cdot 49297$	$6084 = 156^2/4$	6084	156

Why may a proof of Conjecture 5.29 be important?

Clearly, we do not get a better probability of error for Algorithm 5.2 if this conjecture is true and can be proved. More interesting is that we will get

$$|K(n) \cap K'(n)| < \sqrt{n},$$

if n is a product of two prime numbers. And that would be a base to prove, analogous to [**24**], that only a partial factorization $F > \sqrt[4]{n}$ of $n - 1$ would be sufficient to prove the primality of n with Pocklington's Theorem 3.17. This would be an improvement to [**68**].
With Theorem 6.7 in the following chapter, it would also give an improvement of Miller's test.

How important is it to require $\left(\frac{a^2+4}{n}\right) = -1$ for the base a of the commutator test?

If we try to make this commutator test deterministic like Miller's test, we will get many counter-examples. The following table gives the number of commutator pseudoprimes for the base 1 below a natural number x like Table 1 of [**104**]:

x	$CP_1(x)$	$ECP_1(x)$	$SCP_1(x)$
10	0	0	0
10^2	0	0	0
10^3	2	1	0
10^4	9	4	2
10^5	50	30	14
10^6	155	92	41
10^7	511	301	142
10^8	1460	894	399
10^9	4152	2567	1165
10^{10}	11072	6928	3107

For the base 1, let $CP_1(x)$, $ECP_1(x)$, and $SCP_1(x)$ denote the number of commutator pseudoprimes, Euler's variant, and the strong variant, respectively, not exceeding $x \in \mathbb{N}$. A comparison with Table 1 of [**104**] shows that commutator pseudoprimes are only a bit rarer than the ordinary pseudoprimes. Also, like Miller's test, it can be shown that, for all odd composite numbers n below 10^{10}, the equation

$$\begin{aligned} & c(1,a)^{(n-\epsilon)\cdot 2^{-b}} \equiv I_2 \pmod{n} \\ \text{or} \quad & \exists_{0\le d<b} : c(1,a)^{(n-\epsilon)\cdot 2^{d-b}} \equiv -I_2 \pmod{n}, \text{ where } \epsilon = \left(\tfrac{a^2+4}{n}\right), b = \nu_2(n-\epsilon) \end{aligned}$$

is not satisfied for any base $a \in \{1,2,3,4,5,6\}$.
Nevertheless, if we choose the bases in that way, we cannot use all properties and heuristic arguments of Algorithm 5.11 which are collected in this chapter.
Moreover, the probability of error less than $\frac{1}{16}$ cannot be proven, for example not for $n = 119 = 7 \cdot 17$ or $n = 779 = 19 \cdot 41$ etc.

Why did I choose the commutator curve in SL_2, and not another family of matrices?

The answer is quite simple if we regard the subject from the group theory. The commutators have a significant place here. Moreover, I analysed many different products of matrices such as

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$$

or

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$$

for positive integers x, y. Or for example a curve like

$$r(x) := \begin{pmatrix} 0 & 1 \\ -1 & x \end{pmatrix}$$

with $x \in (\mathbb{Z}/n\mathbb{Z})^*$, where n is a natural number greater than 2. By Corollary 4.31, the curve $r(x)$ has the order distribution

$$\begin{aligned} & (|x \in \mathbb{F}_p^* \mid \left(\tfrac{x^2-4}{p}\right) = 1\}|, |x \in \mathbb{F}_p^* \mid \left(\tfrac{x^2-4}{p}\right) = 0\}|, |x \in \mathbb{F}_p^* \mid \left(\tfrac{x^2-4}{p}\right) = -1\}|) \\ & \underset{(4.31)}{=} (\tfrac{p-3}{2}, 2, \tfrac{p-3}{2}), \end{aligned}$$

where p is a prime number greater than 3. Since that distribution is symmetric, it would be better than the distribution of the commutator (see Theorem 4.32). Unfortunatelly, the most important Theorem 4.53 for the correctness of the tests based on the commutator curves in this chapter, is not correct for the curve $r(x)$, e.g.

$$r(4)^3 \equiv I_2 \pmod 5 \quad \text{or} \quad r(7)^{27} \equiv I_2 \pmod{53},$$

etc.

Why do I concentrate on such a compositeness test, although there are well-known good and modern primality tests?

Indeed, we have good primality proving algorithms. However, the running time between the answer "is pseudoprime" and "is prime" is still very large. Of course, before an algorithm rigorously proves that a number n is prime, n must successfully pass a compositeness test, so that it is certain that n is really a pseudoprime. But the most important argument is that, for example in the Jacobi sum test, there exists a part, where many kinds of compositeness tests followed by a step in which a limited amount of trial divisions is performed. No one has ever encountered an example of a number, for which the trial division was really needed – that means, every number that has passed the compositeness tests, actually was prime. Moreover, every improvement of Pocklinton's theorem, such as Conjecture 5.29, is an improvement of every modern primality proving algorithm, e.g. the Jacobi sum test and the elliptic curve test. In the same sense, a speedup of Maurer's algorithm for generating provable primes [**83**] can be achieved. And such improvements can be realized by the commutator curve test.

Finally, the following test is formulated

ALGORITHM 5.30 (Hypothetical Commutator Curve Primality Test).
Input: $n \in \mathbb{N}$, *where* n *is odd,* $n \geq 5$, *and* $n \not\equiv 7 \pmod 8$.
Output: $R \in \{\text{true}, \text{false}\}$.

(1) If n is a perfect square, terminate with the result false.
(2) Set $M := \emptyset$.
(3) Choose $x \in (\mathbb{Z}/n\mathbb{Z})^*$ *with* $\pm x \notin M$ *and*

$$\left(\tfrac{x^2+4}{n}\right) = -1.$$

(4) Terminate with the result false, *if*

$$(x^2+2)^{n-1} \not\equiv 1 \pmod n \quad \text{or} \quad (x^2+4)^{\frac{n-1}{2}} \not\equiv -1 \pmod n$$
$$\text{or} \quad c(1,x)^{\frac{n+1}{2}} \not\equiv -I_2 \pmod n.$$

(5) Set $M := M \cup \{x\}$ *and go to step (3), if* $|M| < 2$.
(6) Let $y, z \in M$ *with* $y \neq z$ *and terminate with the result* false, *if*

$$gcd(y \pm z, n) > 1,$$

otherwise terminate with the result true.

THEOREM 5.31. *Let $n \geq 5$ be an odd natural number with $n \not\equiv 7 \pmod 8$ and $n < 10^7$. Then Algorithm 5.30 returns the result* true *if and only if n is a prime number.*

PROOF. The assertion follows directly from computations and the tables of Appendix B. □

The theorem given above is also correct for $n \equiv 7 \pmod 8$ if we extend step (4) of Algorithm 5.30 by the test $x^2(x^2+4) \not\equiv -2 \pmod n$. Then by Example 4.23, we exclude all elements on the standard commutator curve which have an order equal to eight, which are no good bases for the test. If we do not extend step (4), there exist specific bases for a composite number n, for which Algorithm 5.30 returns the result true. These specific bases are given in the following table

n	M
$198982759 = 3527 \cdot 56417$	$\{9895300, 75626759\}$
198982759	$\{9895300, 81832629\}$
198982759	$\{20168848, 45562611\}$
198982759	$\{20168848, 51768481\}$
198982759	$\{45562611, 61692219\}$
198982759	$\{51768481, 61692219\}$
198982759	$\{75626759, 91756367\}$
198982759	$\{81832629, 91756367\}$
$921858631 = 7591 \cdot 121441$	$\{6492010, 22514888\}$
921858631	$\{6492010, 390966882\}$
921858631	$\{22514888, 273186613\}$
921858631	$\{114349119, 143356017\}$
921858631	$\{114349119, 410050620\}$
921858631	$\{143356017, 394027742\}$
921858631	$\{273186613, 390966882\}$
921858631	$\{394027742, 410050620\}$

The most interesting fact is that if we reach step (6) of Algorithm 5.30 for a composite number n, the order of $c(1,y)$ and $c(1,z)$ is always six and this is only possible for $y^2 \equiv z^2 \equiv -1 \pmod n$ by Corollary 4.22. Otherwise, if we do not require the condition $(x^2+2)^{n-1} \equiv 1 \pmod n$, then experiments show that Algorithm 5.30 returns the result true for $n \in \{3866257, 4216601, 79786523, 97676723\}$ for specific bases y and z, and the order of $c(1,y)$ and $c(1,z)$ is not always six.

CHAPTER 6

Miller's Test and the Extended Riemann Hypothesis

1. Introduction

In this chapter, we will give an upper bound for the least quadratic non-residue, which is important for the correctness of Miller's primality test. First, I will mention that Miller's idea to combine the primality test with the least non-residue[1], was already presented 43 years before by M. Hall in [**55**]. But at Hall's time, there was no polynomial upper bound for the least quadratic non-residue known.
In 1918, J. M. Vinogradov has proved in [**128**] that the least quadratic non-residue modulo an odd natural number $m \geq 2$ is less than $m^{\frac{1}{2\sqrt{e}}} \ln(m)^2$. This upper bound was improved many times to the bound $O(m^{\frac{1}{4\sqrt{e}}})$ by D. A. Burgess in [**27**] at 1957; it was extended to the least non-residue of kth power by both authors (see [**129**], and [**28**]). In the following theorem we will give an elementary proof for a simple upper bound and we will see that the least quadratic non-residue can only be a prime number.

THEOREM 6.1. *Let $m \geq 3$ be a squarefree natural number, and*

$$x = \min\{k \in \mathbb{N}_{>0} \mid \left(\tfrac{k}{m}\right) = -1\},$$

then x is a prime number, and

$$x \leq 1 + \sqrt{m-1}.$$

PROOF. Suppose x is composite. Then there exist two natural numbers $a, b > 1$ such that $x = ab$. By

$$-1 = \left(\tfrac{x}{m}\right) = \left(\tfrac{ab}{m}\right) = \left(\tfrac{a}{m}\right) \cdot \left(\tfrac{b}{m}\right),$$

we have $\left(\frac{a}{m}\right)$ or $\left(\frac{b}{m}\right)$ equal to -1, which contradict the definition of x. Hence, x is a prime number.
Let $t \equiv -m \pmod{x}$ with $t \geq 0$ and $s = \frac{t+m}{x}$. Then $t > 0$ since from $x \mid m$ it follows $\left(\frac{x}{m}\right) \in \{0, 1\}$ which contradicts the definition of x.
From $1 \leq t < x$, we have $\left(\frac{t}{m}\right) = 1$. Therefore, we get

$$1 = \left(\tfrac{t}{m}\right) = \left(\tfrac{t+m}{m}\right) = \left(\tfrac{s \cdot x}{m}\right) = \left(\tfrac{s}{m}\right) \cdot \left(\tfrac{x}{m}\right) = -\left(\tfrac{s}{m}\right).$$

Thus, $\frac{x+m}{x} > s \geq x$. Hence, $x^2 - x - m < 0$. Therefore, $(x-1)^2 < (x - \frac{1}{2})^2 < m + \frac{1}{4}$. Since x and m are integers, we get $(x-1)^2 \leq m$. Finally, since m is squarefree, we have $(x-1)^2 \leq m - 1$. □

[1] G. L. Miller used in [**86**] the least non-residue of kth powers, but H. W. Lenstra, Jr. has proved in [**76**], that the quadratic non-residue is sufficient.

More interesting is the improvement by N. C. Ankeny [**6**] in 1952, who has given the very impressive bound $O(\log(m)^2)$. Since this publication of N. C. Ankeny, many other improvements of the bound and explicit constants for Ankeny's theorem have been developed, see e.g. [**88**], [**10**], [**11**], [**49**], and [**89**]. Today, the best known explicit upper bound for the least quadratic non-residue is $\frac{3}{2}\ln(m)^2 - \frac{44}{5}\ln(m) + 13$ which will be proved in this chapter.
However, the disadvantage of the proof of N. C. Ankeny, and all the other theorems based on it, is that he used the *Extended Riemann Hypothesis* in his proof.

1.1. Riemann Hypothesis. The *Riemann Hypothesis*, which was first published in [**110**][2] on page 148, states that the non-trivial roots of $\zeta(s)$, where s is a complex number, all lie on the *citical line* $\frac{1}{2} + it$, where t is a real number.

DEFINITION 6.2. Let s be a complex number with $\mathrm{Re}(s) > 0$. Then, the *Riemann zeta function* $\zeta(s)$ is an analytic function of s, which is defined by

$$\zeta(s) := \sum_{k=1}^{\infty} \frac{1}{k^s}$$

for $\mathrm{Re}(s) > 1$, and by analytic continuation for $\mathrm{Re}(s) \leq 1, s \neq 1$. Hence, we have[3]

$$\pi^{-\frac{s}{2}}\Gamma(\tfrac{s}{2})\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma(\tfrac{1-s}{2})\zeta(1-s).$$

DEFINITION 6.3. Let s be a complex number. Then we define the *analytic continuation of the zeta function* by

$$\xi(s) := \tfrac{s}{2}(s-1)\pi^{-\frac{s}{2}}\Gamma(\tfrac{s}{2})\zeta(s).$$

In 1859 B. Riemann has noted in [**110**], that he will work with the function $\xi(\frac{1}{2} + it)$, where t is a real number, instead of ξ:

> „...es ist sehr wahrscheinlich, dass alle Wurzeln reell sind. Hiervon wäre allerdings ein strenger Beweis zu wünschen; ich habe indess die Aufsuchung desselben nach einigen flüchtigen vergeblichen Versuchen vorläufig bei Seite gelassen, da er für den nächsten Zweck meiner Untersuchung entbehrlich schien."

In our terminology, B. Riemann has assumed that all non-trivial roots of ξ, and consequently of ζ, lie on the line $\frac{1}{2} + it$, where t is a real number. In this form, his note has entered the history of mathematics as the Riemann Hypothesis.
Unfortunately, nobody knows if the assertion of this hypothesis is correct or wrong, i.e. no counter-example was found. But for that, there exist many computational records especially for Riemann's zeta function to generate roots, which confirm Riemann's Hypothesis. Before we give an overview of the main records, we need a definition which order the roots of an analytic function by increasing absolute value of their imaginary part; roots with the same imaginary part are not ordered inside these roots.

[2] In: *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse*, Monatsberichte der Berliner Akademie, November 1859.

[3] See E. Landau in [**71**] on pages 63-69, especially Satz 418.

DEFINITION 6.4. Let $f : \mathbb{C} \to \mathbb{C}$ be an analytic function with $f(\bar{s}) = \overline{f(s)}$ for all complex numbers s. Then we define the following set of roots

$$N(f) := \{s \neq 0 \mid 0 < \mathrm{Re}(s) < 1, f(s) = 0\}.$$

Since $f(\bar{s}) = \overline{f(s)}$, in many cases we need only consider roots with a positive imaginary part. We assume that the roots $z(f,n) \in N(f)$ with a positive imaginary part are counted according to their multiplicities and ordered so that

$$\begin{aligned} & 0 < \mathrm{Im}(z(f,k)) \leq \mathrm{Im}(z(f,k+1)) \\ \text{and} \quad & \mathrm{Re}(z(f,k)) \leq \mathrm{Re}(z(f,k+1)) \qquad \text{if} \quad \mathrm{Im}(z(f,k)) = \mathrm{Im}(z(f,k+1)) \end{aligned}$$

for positive integer k.
All roots $\rho(f,n) \in N(f)$ are counted according to their multiplicities and ordered so that

$$\begin{aligned} & |\mathrm{Im}(\rho(f,k))| \leq |\mathrm{Im}(\rho(f,k+1))| \\ \text{and} \quad & \mathrm{Im}(\rho(f,k)) > \mathrm{Im}(\rho(f,k+1)) \qquad \text{if} \quad \mathrm{Im}(\rho(f,k)) = -\mathrm{Im}(\rho(f,k+1)) \\ \text{and} \quad & \mathrm{Re}(\rho(f,k)) \leq \mathrm{Re}(\rho(f,k+1)) \qquad \text{if} \quad |\mathrm{Im}(\rho(f,k))| = |\mathrm{Im}(\rho(f,k+1))| \end{aligned}$$

for positive integer k.

An overview of the main records gives the following table[4] [**94**]:

Year	Author	Source	n	H(n)
1903	J. P. Gram	[**50**]	15	65.801
1914	R. J. Backlund	[**15**]	79	199.649
1925	J. I. Hutchinson	[**58**]	138	300.468
1935	E. C. Titchmarsh	[**125**]	1 041	1 467.477
1953	A. M. Turing	[**127**]	1 104	1 539.742
1955	D. H. Lehmer	[**73**]	10 000	9 878.056
1956	D. H. Lehmer	[**73**]	15 000	14 041.137
1956	D. H. Lehmer	[**74**]	25 000	21 942.593
1958	N. A. Meller	[**84**]	35 337	29 750.168
1966	R. S. Lehman	[**72**]	250 000	170 570.745
1968	J. B. Rosser, J. M. Yohe, L. Schoenfeld	[**114**]	3 500 000	1 893 193.452
1977	R. P. Brent	[**20**]	40 000 000	18 114 537.803
1979	R. P. Brent	[**21**]	75 000 000	32 585 736.400
1979	R. P. Brent	[**21**]	81 000 001	35 018 261.243
1982	R. P. Brent, J. van de Lune, H. J. J. te Riele, D. T. Winter	[**22**]	200 000 001	81 702 130.190
1983	J. van de Lune, H. J. J. te Riele	[**81**]	300 000 001	119 590 809.282
1986	J. van de Lune, H. J. J. te Riele, D. T. Winter	[**82**]	1 500 000 001	545 439 823.215

[4]The four values $H(n)$ for $n \in \{15000, 25000, 35337, 250000\}$ are not in the cited literature, but H. J. J. te Riele communicated me these values personally.

Where the function H gives the positive upper bound for which Riemann's Hypothesis was known to be true

$$H : \mathbb{N} \to \mathbb{R} : n \mapsto \begin{cases} t\,, & \text{if } \forall_{1\leq k\leq n} : \mathrm{Re}(z(\zeta,k)) = \frac{1}{2} \wedge |\mathrm{Im}(z(\zeta,k))| \leq t \\ 0\,, & \text{if } \exists_{1\leq k\leq n} : \mathrm{Re}(z(\zeta,k)) \neq \frac{1}{2} \vee |\mathrm{Im}(z(\zeta,k))| > t. \end{cases}$$

Of course, we can choose $H(n)$ everywhere in the open interval

$$]\,\mathrm{Im}(z(\zeta,n)), \mathrm{Im}(z(\zeta,n+1))[\,.$$

Often, the *Gram points*[5] separate the imaginary part of two consecutive non-trivial roots of the zeta function and, then we can take $H(n)$ equal to the $(n-1)$th Gram point.

In 1988, a faster method for simultaneous computation of large sets of roots of the zeta function was invented by A. M. Odlyzko and A. Schönhage [**96**]. It has been implemented and used to compute $175 \cdot 10^6$ roots near root number 10^{20} and 10 billion roots near root number 10^{22} (see [**93**], and [**95**]). But till now, the table above is up-to-date[6].

1.2. Extended Riemann Hypothesis. The *Extended Riemann Hypothesis* says that all the non-trivial zeros of the Dirichlet L-function $L(s,\chi)$ for a real character χ modulo a natural number $m \geq 2$, where s is a complex number, are on the critical line.

Definition 6.5. The function $\chi : \mathbb{N} \to \mathbb{R}$ is called a *real character* modulo a natural number $m \geq 2$, if the function χ satisfies the following four properties

(1) $\chi(1) \neq 0$,
(2) $\chi(k) = 0$ for all $k \in \mathbb{N}$ with $\gcd(k,m) > 1$,
(3) $\chi(k_1 \cdot k_2) = \chi(k_1) \cdot \chi(k_2)$ for all $k_1, k_2 \in \mathbb{N}$,
(4) $\chi(k_1) = \chi(k_2)$ for all $k_1, k_2 \in \mathbb{N}$ with $k_1 \equiv k_2 \pmod{m}$.

Let s be a complex number with $\mathrm{Re}(s) > 0$, and let χ be a character. Then, we define the *L-function* by

$$L(s,\chi) := \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s}.$$

By the functional equation of the L-function, $L(s,\chi)$ can also – like the zeta function – be analytically continued to the complex numbers[7].

There also exist computational records[8] for some special L-functions, see e.g. [**121**], [**115**].

[5]The nth Gram point for $n \in \mathbb{N} \cup \{-1\}$ is defined as the unique solution of the equation $\theta(t) = n \cdot \pi$, where $\theta(t) = \arg(\pi^{-\frac{it}{2}}\Gamma(\frac{1+2it}{4}))$ (see for example [**21**]).

[6]By the end of the year 2000, J. van de Lune had checked that the first 5 300 000 000 roots of the zeta function lie on the critical line (unpublished).

[7]See H. Davenport in [**36**] on pages 65-72, especially page 71.

[8]A different study of the zeta function is to evaluate one value of $\zeta(s)$ for an integer s to high precision in order, for example, to resolve some other constant or ascertain some conjecture. Since L. Euler it is known that $\zeta(2) = \frac{\pi^2}{6}$ and $\zeta(4) = \frac{\pi^4}{90}$. But what do we know about $\zeta(3)$? R. Apéry [**7**] has proved that $\zeta(3)$ is irrational, although it is not known whether it is transcendental, but it seems to be [**133**].

By these computational proceedings, we get further informations of the Extended Riemann Hypothesis, but they are not enough to prove the hypothesis.

In this chapter, our intention is to use all empirical informations about the Extended Riemann Hypothesis with regard to Miller's primality test. We concentrate on two questions. First, is it possible to remove the Extended Riemann Hypothesis from Miller's primality test? And second, is it at least possible to find an upper bound for composite numbers n, for which Miller's test is reliable?
All proofs in this chapter are based primarily on methods taken from the dissertation of E. Bach [**11**]. However, we concentrate on Miller's test, and not on the least quadratic non-residue in general like he did.

2. Miller's Primality Test

In this chapter, we will prove the correctness of the following primality algorithm assuming the Extended Riemann Hypothesis is true.

ALGORITHM 6.6 (ERH – Miller-Selfridge-Weinberger Test [**137**]).
Input: $n \in \mathbb{N}$ *where* $n > 8$.
Output: $R \in \{\text{true}, \text{false}\}$.

(1) If $a^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$ *for some* $a \in \mathbb{P}$ *with* $a < \frac{3}{2}\ln(n)^2 - \frac{44}{5}\ln(n) + 13$, *then terminate with the result* false, *otherwise terminate with the result* true.

THEOREM 6.7 (ERH). *Assume the Extended Riemann Hypothesis is correct. Let n be a composite number with r prime divisors. Then there exists a prime number*

$$a < \tfrac{6}{r^2}\ln(n)^2 - \tfrac{88}{5\cdot r}\ln(n) + 13$$

such that Miller's Algorithm 3.11 returns the result false for the base a.

PROOF. By Theorem 2 of [**76**][9], we know that n may be assumed to be squarefree. Suppose $a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$ for all prime numbers less than $\frac{6}{r^2}\ln(n)^2 - \frac{88}{5\cdot r}\ln(n) + 13$. Let p, q be different prime divisors of n such that $pq < \sqrt[r]{n^2}$. Then from Theorem 6.35 there exists a base

$$a_1 < \tfrac{3}{2}\ln(pq)^2 - \tfrac{44}{5}\ln(pq) + 13 < \tfrac{6}{r^2}\ln(n)^2 - \tfrac{88}{5\cdot r}\ln(n) + 13$$

such that a_1 is the least quadratic non-residue modulo pq. Therefore, by Theorem 6.1, the base a_1 is prime.
Suppose without loss of generality that $\left(\frac{a_1}{p}\right) = -1$ and $\left(\frac{a_1}{q}\right) = 1$. By Lemma 5.7, we have

$$\nu_2(q-1) > \nu_2(n-1). \tag{58}$$

Similarly, also by Theorem 6.35, there exists a base

$$a_2 < \tfrac{3}{2}\ln(q)^2 - \tfrac{44}{5}\ln(q) + 13 < \tfrac{6}{r^2}\ln(n)^2 - \tfrac{88}{5\cdot r}\ln(n) + 13$$

such that $a_2 \in \mathbb{P}$ is the least quadratic non-residue modulo q. But by Lemma 5.7, we get $\nu_2(q-1) = \nu_2(n-1)$ which contradicts equation (58). □

[9] S. Pajunen has shown in [**98**] an improvement of this theorem.

COROLLARY 6.8 (ERH). *Let $n > 8$ be a natural number and assume that the Extended Riemann Hypothesis is true. Then the Algorithm 6.6 is correct.*

PROOF. This can be concluded from Theorem 6.7. □

THEOREM 6.9. *Let n be a natural number less than $6 \cdot 10^{19}$. Then the Algorithm 6.6 is correct without the requirement of the Extended Riemann Hypothesis.*

PROOF. The proof of the assertion is analogous to Theorem 6.7. Instead of Theorem 6.35, we use the table of pseudosquares (Appendix A) to get an upper bound for the least quadratic non-residue.

□

H. Cohen and H. W. Lenstra, Jr. have said in [**31**] that "for a typical 100-digit number this method is approximately 500 times as slow as the algorithm described in this paper, although it is faster."
In fact, their Jacobi sum algorithm was a great improvement. However, for a comparison with Miller's test, they have used all bases less than $70\ln(n)^2$. If we use, like in Algorithm 6.6, the constant $\frac{3}{2}$ instead of 70, then this Miller's algorithm runs 46 times faster than Miller's test which was described in [**31**]. And so, the improvement of H. Cohen and H. W. Lenstra, Jr. ([**31**]) is now not more than about 11 times, which implies that prejudices against Miller's test are no longer valid[10].

3. Hierarchy of the Proof

The proof of Theorem 6.35, that gives the upper bound

$$x < \tfrac{3}{2}\ln(m)^2 - \tfrac{44}{5}\ln(m) + 13.$$

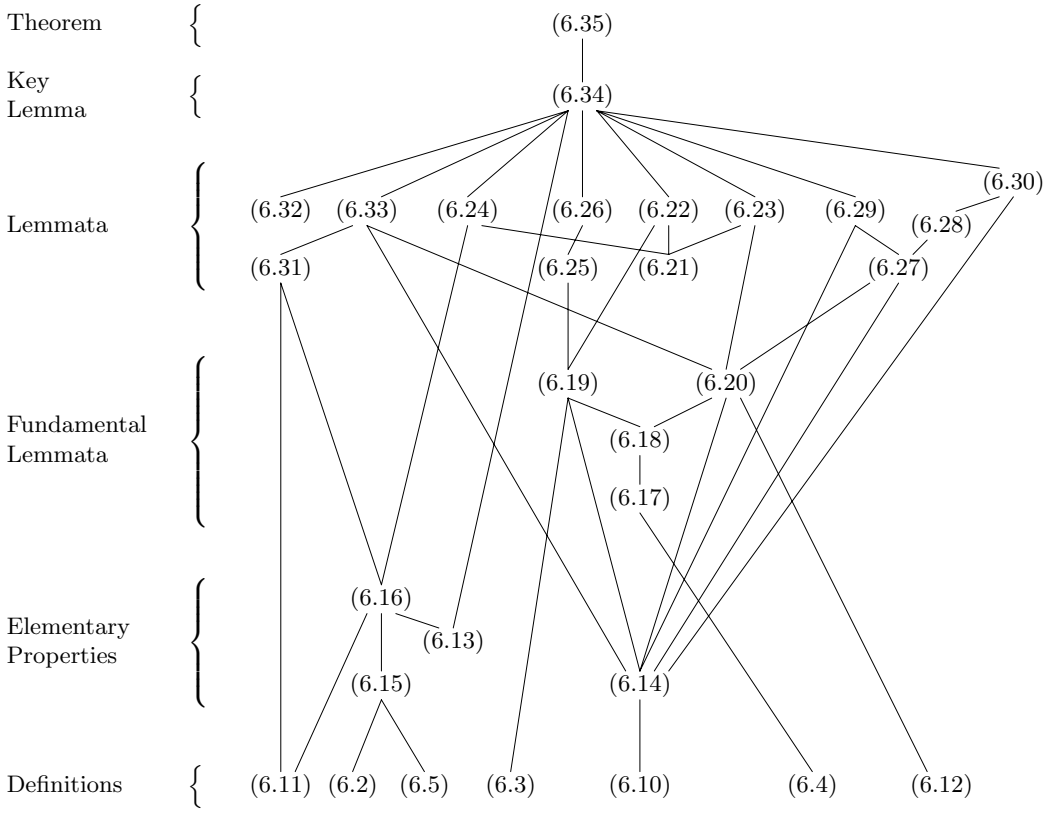
for the least quadratic non-residue modulo a natural number m which is greater than 1, is split in the following six steps:

(1) First, in Section 4, we will define some necessary basic functions for the proof of the theorem.
(2) In addition, in Section 5, we will collect some required elementary properties of the defined functions. To complete the picture, we will prove the properties which are not well known.
(3) Section 6 contains some fundamental lemmata about the roots of the zeta function and L-function. Since the proof of the first lemma are too extensive for this thesis, we will just refer to the corresponding literature; the main idea of these proofs are based essentially on Hadamards' theory of entire functions and the Weierstrassian product theorem.
(4) The real work of the proof is in Section 7. This more technical section is based partly on the dissertation of E. Bach [**11**], with concentration on Miller's test and the possibility of removing the Extended Riemann Hypothesis.

[10]Certainly, since 1984, the Jacobi sum test (see for example [**85**]) has been improved.

(5) Section 8 combines all lemmata of Section 7 in one key lemma. In our discussion in Section 10, we will see that it is possible to prove all lemmata, inclusive the key lemma, without the necessity of the Extended Riemann Hypothesis.
(6) Finally, Section 9 contains the proof of the theorem about an upper bound for the least quadratic non-residue.

The following diagram gives an overview of the structure of the proof.



This hierarchical diagram is read from bottom to up in such a way, that one item is dependent on the items beneath. The direct dependencies are marked with lines.

4. Definitions

Additionally to the previous definitions of this chapter, we will use the following definitions throughout this chapter.

DEFINITION 6.10. Let s be a complex number. Then we define the *gamma function*[11] by the equation

$$\frac{1}{\Gamma(s)} := se^{s\gamma} \prod_{k=1}^{\infty} \left(1 + \frac{s}{k}\right) e^{-\frac{s}{k}}.$$

[11]See for example [**36**] on page 73.

DEFINITION 6.11. The Λ-*function*[12] introduced by von Mangoldt is defined by

$$\Lambda : \mathbb{N} \to \mathbb{R} : n \mapsto \begin{cases} \ln(p)\,, & \text{if } n = p^k,\ p \in \mathbb{P},\ k \in \mathbb{N}_{>0} \\ 0\,, & \text{else.} \end{cases}$$

Additionally, we will need the following function

$$\psi : \mathbb{N}_{\geq 0} \to \mathbb{R} : n \mapsto \sum_{k=1}^{n} \Lambda(k).$$

DEFINITION 6.12. Let s be a complex number, $m \geq 2$ be a natural number, χ a character modulo m, and

$$\delta = \begin{cases} 0\,, & \text{if } \chi(-1) = 1 \\ 1\,, & \text{if } \chi(-1) = -1. \end{cases}$$

Then we define the *analytic continuation of the L-function* by

$$\xi(s, \chi) := (\tfrac{\pi}{m})^{-\frac{s+\delta}{2}} \Gamma(\tfrac{s+\delta}{2}) L(s, \chi).$$

5. Elementary Properties

THEOREM 6.13. *Let s be a complex number with $|s| < 1$. Then*

$$\sum_{k=1}^{\infty} (-1)^{k+1} \frac{s^k}{k} = \ln(1+s).$$

PROOF. This theorem is a well known Taylor serie in Analysis; for a proof we refer for example to [**107**] on page 149.

□

LEMMA 6.14. *Let s be a complex number. Then*

$$\tfrac{\Gamma'}{\Gamma}(s) = -\gamma - \frac{1}{s} + \sum_{k=1}^{\infty} \left(\frac{1}{k} - \frac{1}{k+s} \right).$$

PROOF. By Definition 6.10, it follows for the first derivative of the gamma function

$$\begin{aligned} \Gamma'(s) \underset{(6.10)}{=} & -\frac{e^{-s\gamma}}{s^2} \prod_{k=1}^{\infty} \left(1 + \frac{s}{k}\right)^{-1} e^{\frac{s}{k}} + s^{-1}(-\gamma) e^{-s\gamma} \prod_{k=1}^{\infty} \left(1 + \frac{s}{k}\right)^{-1} e^{\frac{s}{k}} \\ & + s^{-1} e^{-s\gamma} \frac{d\left(\prod_{k=1}^{\infty} \left(1 + \frac{s}{k}\right)^{-1} e^{\frac{s}{k}}\right)}{ds} \\ = & \frac{1}{s e^{s\gamma}} \left(\sum_{k=1}^{\infty} \left(\prod_{\substack{l=1 \\ l \neq k}}^{\infty} \left(1 + \frac{s}{l}\right)^{-1} e^{\frac{s}{l}} \right) \frac{d\left((1 + \frac{s}{k})^{-1} e^{\frac{s}{k}}\right)}{ds} \right. \\ & \left. - \prod_{k=1}^{\infty} \left(1 + \frac{s}{k}\right)^{-1} e^{\frac{s}{k}} \left(\gamma + \frac{1}{s}\right) \right) \end{aligned}$$

[12] See for example [**36**] on pages 55-60.

$$
\begin{aligned}
&= \frac{1}{se^{s\gamma}}\left(\sum_{k=1}^{\infty}\prod_{l=1}^{\infty}\left(1+\frac{s}{l}\right)^{-1}e^{\frac{s}{l}}\frac{1}{k}\left(1-\left(1+\frac{s}{k}\right)^{-1}\right)\right.\\
&\quad\left.-\prod_{k=1}^{\infty}\left(1+\frac{s}{k}\right)^{-1}e^{\frac{s}{k}}\left(\gamma+\frac{1}{s}\right)\right)\\
&= \underbrace{\frac{1}{se^{s\gamma}}\prod_{l=1}^{\infty}\left(1+\frac{s}{l}\right)^{-1}e^{\frac{s}{l}}}_{\underset{(6.10)}{=}\Gamma(s)}\left(-\gamma-\frac{1}{s}+\sum_{k=1}^{\infty}\left(\frac{1}{k}-\frac{1}{k+s}\right)\right).
\end{aligned}
$$

The proof of the assertion is complete by the multiplication with the inverse of the gamma function (Definition 6.10). □

THEOREM 6.15. *Let s be a complex number with $\mathrm{Re}(s) > 1$, and let χ be a character. Then Euler's identity is*

$$\zeta(s) = \prod_{p\in\mathbb{P}}\frac{1}{1-p^{-s}}, \tag{59}$$

and we have the analog of Euler's identity

$$L(s,\chi) = \prod_{p\in\mathbb{P}}\frac{1}{1-\chi(p)p^{-s}}. \tag{60}$$

PROOF. This theorem is well known in Multiplicative Number Theory; for a proof we refer for example to [**36**] on pages 1-3. □

THEOREM 6.16. *Let s be a complex number with $\mathrm{Re}(s) > 1$, and let χ be a character. Then we have*

$$\frac{\zeta'}{\zeta}(s) = -\sum_{k=1}^{\infty}\frac{\Lambda(k)}{k^s}, \tag{61}$$

$$\frac{L'}{L}(s,\chi) = -\sum_{k=1}^{\infty}\frac{\Lambda(k)\chi(k)}{k^s}. \tag{62}$$

PROOF. We will give only a proof of equation (62), because the proof of the other equation is analogous. Equation (62) follows by Theorem 6.15, Theorem 6.13, and Definition 6.11

$$
\begin{aligned}
\frac{L'}{L}(s,\chi) &= \frac{d\ln(L(s,\chi))}{ds}\\
&\underset{(60)}{=} \frac{d\left(\sum_{p\in\mathbb{P}}\ln(\frac{1}{1-\chi(p)p^{-s}})\right)}{ds}\\
&\underset{(6.13)}{=} \frac{d\left(\sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}(\frac{\chi(p)^k}{k\cdot p^{ks}})\right)}{ds}
\end{aligned}
$$

$$\begin{aligned} &= \sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}\frac{d(\frac{1}{k}e^{-k\ln(p)s})}{ds}\,\chi(p^k)\\ &= -\sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}\frac{\ln(p)\chi(p^k)}{p^{ks}}\\ &\underset{(6.11)}{=} -\sum_{k=1}^{\infty}\frac{\Lambda(k)\chi(k)}{k^s}. \quad \square \end{aligned}$$

6. Fundamental Lemmata

LEMMA 6.17. *Let s be a complex number, and let χ be a primitive character. Moreover, define $A := -\frac{\gamma}{2} - 1 + \frac{1}{2}\ln(4\pi)$, and $B(\chi) := \frac{\xi'}{\xi}(0,\chi)$. Then we have the following relation between the non-trivial roots of the zeta/L-function and the function ξ*

$$\xi(s) = \tfrac{1}{2}\,e^{As}\prod_{k=1}^{\infty}\left(1-\frac{s}{\rho(\zeta,k)}\right)e^{s\rho(\zeta,k)^{-1}}, \tag{63}$$

$$\xi(s,\chi) = \xi(0,\chi)\,e^{B(\chi)s}\prod_{k=1}^{\infty}\left(1-\frac{s}{\rho(L,k)}\right)e^{s\rho(L,k)^{-1}}. \tag{64}$$

PROOF. We refer to [**36**] on pages 79-83 for a proof. $\square$

LEMMA 6.18. *Let s be a complex number, and let χ be a primitive character. Moreover define $B(\chi) := \frac{\xi'}{\xi}(0,\chi)$. Then we have*

$$\frac{\xi'}{\xi}(s) = -\frac{\gamma}{2} - 1 + \frac{1}{2}\ln(4\pi) + \sum_{k=1}^{\infty}\left(\frac{1}{s-\rho(\zeta,k)} + \frac{1}{\rho(\zeta,k)}\right), \tag{65}$$

$$\frac{\xi'}{\xi}(s,\chi) = B(\chi) + \sum_{k=1}^{\infty}\left(\frac{1}{s-\rho(L,k)} + \frac{1}{\rho(L,k)}\right). \tag{66}$$

PROOF. We have the elementary equation

$$-\frac{s}{x^2} = \frac{x-s}{x}\cdot\frac{x+s-x}{(s-x)x} = \left(1-\frac{s}{x}\right)\left(\frac{1}{s-x}+\frac{1}{x}\right). \tag{67}$$

Let $A := -\frac{\gamma}{2} - 1 + \frac{1}{2}\ln(4\pi)$. Then, by Lemma 6.17, we have for the first derivative of the function ξ the following equation

$$\begin{aligned} &\xi'(s)\\ \underset{(63)}{=}\ &\tfrac{1}{2}\,Ae^{As}\prod_{k=1}^{\infty}\left(1-\frac{s}{\rho(\zeta,k)}\right)e^{s\rho(\zeta,k)^{-1}}\\ &+\tfrac{1}{2}\,e^{As}\sum_{n=1}^{\infty}\left(\prod_{\substack{k=1\\k\neq n}}^{\infty}\left(1-\frac{s}{\rho(\zeta,k)}\right)e^{s\rho(\zeta,k)^{-1}}\right)\underbrace{\left(\frac{1}{\rho(\zeta,n)}\left(1-\frac{s}{\rho(\zeta,n)}\right)-\frac{1}{\rho(\zeta,n)}\right)}_{\underset{(65)}{=}-\frac{s}{\rho(\zeta,n)^2}}e^{s\rho(\zeta,n)^{-1}} \end{aligned}$$

$$\underset{(67)}{=} \underbrace{\tfrac{1}{2}\, e^{As} \prod_{k=1}^{\infty} \left(1 - \frac{s}{\rho(\zeta,k)}\right) e^{s\rho(\zeta,k)^{-1}}}_{\underset{(65)}{=} \xi(s)} \left(A + \sum_{k=1}^{\infty} \left(\frac{1}{s-\rho(\zeta,k)} + \frac{1}{\rho(\zeta,k)}\right)\right).$$

The proof of equation (65) is complete by the multiplication with the inverse of the function ξ, and Lemma 6.17.
Using Lemma 6.17, the proof of second equation (66) is analogous. □

LEMMA 6.19. *Let s be a complex number. Then we have*

$$\tfrac{\zeta'}{\zeta}(s) = \tfrac{1}{1-s} - 1 + \ln(2\pi) - \tfrac{1}{2}\sum_{k=1}^{\infty}\left(\tfrac{1}{k} - \tfrac{2}{2k+s}\right) + \sum_{k=1}^{\infty}\left(\tfrac{1}{s-\rho(\zeta,k)} + \tfrac{1}{\rho(\zeta,k)}\right).$$

PROOF. By Definition 6.3, we have the following equation for the first derivative of the function ξ

$$\begin{aligned}\xi'(s) \underset{(6.3)}{=}\ & \tfrac{s-1}{2}\,\pi^{-\frac{s}{2}}\,\Gamma(\tfrac{s}{2})\zeta(s) + \tfrac{s}{2}\,\pi^{-\frac{s}{2}}\,\Gamma(\tfrac{s}{2})\zeta(s) \\ & + \tfrac{s}{2}(s-1)(-\tfrac{1}{2}\ln(\pi)\pi^{-\frac{s}{2}})\Gamma(\tfrac{s}{2})\zeta(s) \\ & + \tfrac{s}{2}(s-1)\pi^{-\frac{s}{2}}\,\Gamma'(\tfrac{s}{2})\zeta(s) + \tfrac{s}{2}(s-1)\pi^{-\frac{s}{2}}\,\Gamma(\tfrac{s}{2})\zeta'(s). \qquad (68)\end{aligned}$$

Transforming equation (68) to $\zeta'(s)$, and Definition 6.3 to $\zeta(s)$, and from Lemma 6.18, and Lemma 6.14, we get

$$\begin{aligned}\tfrac{\zeta'}{\zeta}(s) \underset{(6.3),(68)}{=}\ & \frac{\xi'(s) - \frac{s-1}{2}\pi^{-\frac{s}{2}}\,\Gamma(\frac{s}{2})\zeta(s) - \frac{s}{2}\pi^{-\frac{s}{2}}\,\Gamma(\frac{s}{2})\zeta(s)}{\xi(s)} \\ & + \frac{\frac{s}{4}(s-1)\ln(\pi)\pi^{-\frac{s}{2}}\,\Gamma(\frac{s}{2})\zeta(s) - \frac{s}{2}(s-1)\pi^{-\frac{s}{2}}\,\Gamma'(\frac{s}{2})\zeta(s)}{\xi(s)} \\ \underset{(6.3),(65)}{=}\ & -\frac{\gamma}{2} - 1 + \tfrac{1}{2}\ln(4\pi) + \sum_{k=1}^{\infty}\left(\frac{1}{s-\rho(\zeta,k)} + \frac{1}{\rho(\zeta,k)}\right) - \frac{1}{s} - \frac{1}{s-1} \\ & + \tfrac{1}{2}\ln(\pi) - \tfrac{1}{2}\,\tfrac{\Gamma'}{\Gamma}(\tfrac{s}{2}) \\ \underset{(6.14)}{=}\ & \frac{1}{1-s} - 1 + \ln(2\pi) - \frac{1}{2}\sum_{k=1}^{\infty}\left(\frac{1}{k} - \frac{2}{2k+s}\right) \\ & + \sum_{k=1}^{\infty}\left(\frac{1}{s-\rho(\zeta,k)} + \frac{1}{\rho(\zeta,k)}\right). \quad \square\end{aligned}$$

LEMMA 6.20. *Let s be a complex number, m a natural number greater than 1, χ a primitive character modulo m, and $\delta = \begin{cases} 0\,, & \text{if } \chi(-1)=1 \\ 1\,, & \text{if } \chi(-1)=-1 \end{cases}$. Then*

$$\begin{aligned} \tfrac{L'}{L}(s,\chi) &= B(\chi) + \tfrac{1}{s+\delta} + \tfrac{1}{2}\ln(\tfrac{\pi}{m}) + \tfrac{\gamma}{2} - \tfrac{1}{2}\sum_{k=1}^{\infty}\left(\tfrac{1}{k} - \tfrac{2}{2k+\delta+s}\right) \\ &\quad + \sum_{k=1}^{\infty}\left(\tfrac{1}{s-\rho(L,k)} + \tfrac{1}{\rho(L,k)}\right), \end{aligned}$$

where $B(\chi) := \frac{\xi'}{\xi}(0,\chi)$.

PROOF. By Definition 6.12, we have

$$\begin{aligned} \xi'(s,\chi) &\underset{(6.12)}{=} -\tfrac{1}{2}\ln(\tfrac{\pi}{m})\cdot(\tfrac{\pi}{m})^{-\frac{s+\delta}{2}}\,\Gamma(\tfrac{s+\delta}{2})L(s,\chi) + (\tfrac{\pi}{m})^{-\frac{s+\delta}{2}}\,\Gamma'(\tfrac{s+\delta}{2})\tfrac{1}{2}L(s,\chi) \\ &\quad + (\tfrac{\pi}{m})^{-\frac{s+\delta}{2}}\,\Gamma(\tfrac{s+\delta}{2})L'(s,\chi). \end{aligned} \tag{69}$$

Transforming equation (69) to $L(s,\chi)$ and using Lemma 6.18, and Lemma 6.14, we have

$$\begin{aligned} \tfrac{L'}{L}(s,\chi) &\underset{(6.12),(69)}{=} \frac{\xi'(s,\chi) + \frac{1}{2}\ln(\frac{\pi}{m})\cdot(\frac{\pi}{m})^{-\frac{s+\delta}{2}}\,\Gamma(\frac{s+\delta}{2})L(s,\chi)}{\xi(s,\chi)} \\ &\quad - \frac{(\frac{\pi}{m})^{-\frac{s+\delta}{2}}\,\Gamma'(\frac{s+\delta}{2})\frac{1}{2}L(s,\chi)}{\xi(s,\chi)} \\ &\underset{(6.12),(66)}{=} B(\chi) + \sum_{k=1}^{\infty}\left(\frac{1}{s-\rho(L,k)} + \frac{1}{\rho(L,k)}\right) + \tfrac{1}{2}\ln(\tfrac{\pi}{m}) - \tfrac{1}{2}\,\tfrac{\Gamma'}{\Gamma}(\tfrac{s+\delta}{2}) \\ &\underset{(6.14)}{=} B(\chi) + \tfrac{1}{2}\ln(\pi) - \frac{1}{2}\left(-\gamma - \frac{2}{s+\delta} + \sum_{k=1}^{\infty}\left(\frac{1}{k} - \frac{2}{2k+\delta+s}\right)\right) \\ &\quad + \sum_{k=1}^{\infty}\left(\frac{1}{s-\rho(L,k)} + \frac{1}{\rho(L,k)}\right). \quad \square \end{aligned}$$

7. Lemmata

LEMMA 6.21. *Let s be a complex number with $\mathrm{Re}(s) > 0$, k a natural number, $\delta \in \{0,1\}$, ρ a complex number with $0 < \mathrm{Re}(\rho) < 1$, x a positive real number, and $a \in \,]0,1[$. Then*

1. $$\tfrac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \tfrac{x^s}{(s+a)^2}\,ds = \begin{cases} 0\,, & \text{if } 0 < x \le 1 \\ \frac{\ln(x)}{x^a}\,, & \text{if } x > 1 \end{cases}$$

2. $$\tfrac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \tfrac{x^s}{(s+a)^2(1-s)}\,ds = \begin{cases} 0\,, & \text{if } 0 < x \le 1 \\ -\frac{x}{(a+1)^2} + \frac{1}{x^a(a+1)^2} + \frac{\ln(x)}{x^a(a+1)}\,, & \text{if } x > 1 \end{cases}$$

3. $$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2(2k+\delta+s)}\,ds = \begin{cases} 0\,, & \text{if } 0<x\leq 1 \\ \frac{\ln(x)}{x^a(2k+\delta-a)} - \frac{1}{x^a(2k+\delta-a)^2} + \frac{1}{x^{2k+\delta}(2k+\delta-a)^2}\,, & \text{if } x>1 \end{cases}$$

4. $$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2(s-\rho)}\,ds = \begin{cases} 0\,, & \text{if } 0<x\leq 1 \\ \frac{x^\rho}{(a+\rho)^2} - \frac{\ln(x)}{x^a(a+\rho)^2} - \frac{1}{x^a(a+\rho)^2}\,, & \text{if } x>1. \end{cases}$$

PROOF. The proof of the first integral formula is split in the following three steps:

(1) residue calculation,
(2) consideration of the convergence, and
(3) using Cauchy's integral theorem.

(1) **Residue calculation.**
Let w be a real number. Then the rational function

$$f_1(s) := \frac{e^{sw}}{(s+a)^2}$$

has a pole of second order at $s=-a$, and is else regular, since the analytic continuation of $(s+a)^2 f_1(s)$ is

$$g_1(s) := e^{sw}.$$

By residue calculation[13], we have

$$\operatorname{Res}_{-a} f_1 = \frac{1}{(2-1)!} g_1^{(2-1)}(-a) = we^{-aw}. \tag{70}$$

(2) **Consideration of the convergence.**
We have the following equation

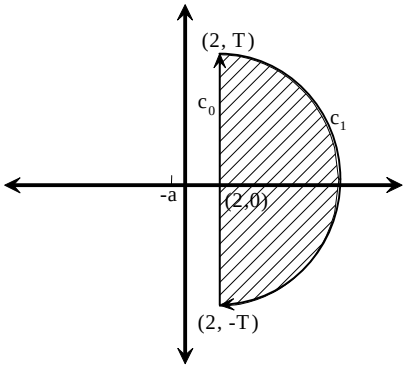
$$\int \frac{dt}{a^2+t^2} = \tfrac{1}{a}\cdot\arctan(\tfrac{t}{a}), \tag{71}$$

then the convergence of the first integral follows by

$$\begin{aligned}
\left|\lim_{T\to\infty}\int_{2-iT}^{2+iT}\frac{e^{sw}}{(s+a)^2}\,ds\right| &\underset{\left(\substack{t:=\frac{s-2}{i}\\ ds=idt}\right)}{\leq} |i|\lim_{T\to\infty}\int_{-T}^{T}\left|\frac{e^{(2+it)w}}{(2+it+a)^2}\right|dt \\
&= \lim_{T\to\infty}\int_{-T}^{T}\frac{e^{2w}}{(2+a+it)(2+a-it)}\,dt \\
&= e^{2w}\lim_{T\to\infty}\int_{-T}^{T}\frac{dt}{(2+a)^2+t^2} \\
&\underset{(71)}{=} \frac{e^{2w}}{2+a}\lim_{T\to\infty}\left(\arctan(\tfrac{T}{2+a}) - \arctan(\tfrac{-T}{2+a})\right) \\
&= \frac{2e^{2w}}{2+a}\lim_{T\to\infty}\arctan(\tfrac{T}{2+a}) \\
&= \frac{\pi e^{2w}}{2+a}.
\end{aligned}$$

[13]See for example [**107**] on page 304.

(3) **Cauchy's integral theorem.**
We split the integral up into the following two regions to calculate the integral:
(a) Let $w \leq 0$ for the first region. Therefore, we use a closed curve consisting of a line segment c_0 and a semicircle c_1,
(i) $c_0 : [-T, T] \to \mathbb{C} : y \mapsto 2 + iy$
(ii) and $c_1 : [\frac{\pi}{2}, 3\frac{\pi}{2}] \to \mathbb{C} : \varphi \mapsto 2 - Te^{-i\varphi}$.



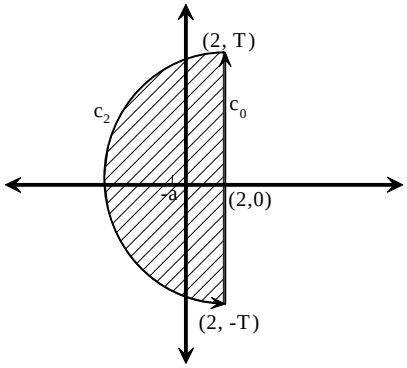
The arc length of c_1 is

$$|c_1| = \int_{\frac{\pi}{2}}^{3\frac{\pi}{2}} T \underbrace{\sqrt{|ie^{i\varphi}|^2}}_{=1} d\varphi = \pi T. \tag{72}$$

Hence

$$\begin{aligned} 0 \leq \left| \lim_{T\to\infty} \int_{2-iT}^{2+iT} \frac{e^{sw}}{(s+a)^2}\, ds \right| &= \left| \lim_{T\to\infty} \int_{c_1} \frac{e^{sw}}{(s+a)^2}\, ds \right| \\ &\leq \lim_{T\to\infty} \int_{c_1} \left| \frac{e^{sw}}{(s+a)^2} \right| ds \\ &\underset{(|s|=\sqrt{4+T^2}\geq T)}{\leq} \lim_{T\to\infty} |c_1| \frac{e^{2w}}{(T+a)^2} \\ &\underset{(72)}{=} \lim_{T\to\infty} \frac{\pi T e^{2w}}{(T+a)^2} \\ &= 0. \end{aligned} \tag{73}$$

(b) Let $w > 0$ for the second region. Therefore, we use a closed curve consisting a line segment c_0 and a semicircle c_2,
(i) $c_0 : [-T, T] \to \mathbb{C} : y \mapsto 2 + iy$
(ii) and $c_2 : [\frac{\pi}{2}, \frac{3\pi}{2}] \to \mathbb{C} : \varphi \mapsto 2 + Te^{i\varphi}$.



The arc length of c_2 is calculated analogous to (72) and is

$$|c_2| = \pi T. \tag{74}$$

In this region, there is the pole $s = -a$ with the residue we^{-aw} by (70). Thus, we have by the theorem of residues

$$\begin{aligned} 0 \leq \left| \lim_{T\to\infty} \int_{2-iT}^{2+iT} \frac{e^{sw}}{(s+a)^2} ds - 2\pi i \cdot we^{-aw} \right| &= \left| \lim_{T\to\infty} \int_{c_2} \frac{e^{sw}}{(s+a)^2}\, ds \right| \\ &\leq \lim_{T\to\infty} \int_{c_2} \left| \frac{e^{sw}}{(s+a)^2} \right| ds \\ &\underset{(|s|\geq T)}{\leq} \lim_{T\to\infty} |c_2| \frac{e^{2w}}{(T+a)^2} \\ &\underset{(74)}{=} \lim_{T\to\infty} \frac{\pi T e^{2w}}{(T+a)^2} \\ &= 0. \end{aligned} \tag{75}$$

By (73), (75), and the definition $x := e^w$, it follows that the value of the first integral is

$$\frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2}\, ds = \begin{cases} 0\,, & \text{if } 0 < x \leq 1 \\ \frac{\ln(x)}{x^a}\,, & \text{if } x > 1. \end{cases}$$

We will only do the residue calculation for the other three integrals since the consideration of the convergence and using Cauchy's integral theorem is analogous to the calculation of the first integral. Then we consider the following three functions

$$\begin{aligned} f_2(s) &:= \frac{e^{sw}}{(s+a)^2(1-s)},\ \tilde{f}_2(s) := \frac{e^{sw}}{1-s},\ \tilde{f}_2'(s) = \frac{we^{sw}}{1-s} + \frac{e^{sw}}{(1-s)^2}, \\ f_3(s) &:= \frac{e^{sw}}{(s+a)^2(2k+\delta+s)}, \\ \tilde{f}_3(s) &:= \frac{e^{sw}}{2k+\delta+s},\ \tilde{f}_3'(s) = \frac{we^{sw}}{2k+\delta+s} - \frac{e^{sw}}{(2k+\delta+s)^2}, \\ f_4(s) &:= \frac{e^{sw}}{(s+a)^2(s-\rho)},\ \tilde{f}_4(s) := \frac{e^{sw}}{s-\rho},\ \tilde{f}_4'(s) = \frac{we^{sw}}{s-\rho} - \frac{e^{sw}}{(s-\rho)^2}. \end{aligned}$$

These three functions f_2, f_3 and f_4 have the following residues

$$\begin{aligned}
\operatorname{Res}_{-a} f_2 &= \frac{1}{(2-1)!}\tilde{f}_2^{(2-1)}(-a) = \frac{we^{-aw}}{1+a} + \frac{e^{-aw}}{(1+a)^2},\\
\operatorname{Res}_{1} f_2 &= \lim_{s\to 1}(s-1)f_2(s) = \lim_{s\to 1} -\frac{e^{sw}}{(s+a)^2} = -\frac{e^{w}}{(a+1)^2},\\
\operatorname{Res}_{-a} f_3 &= \frac{1}{(2-1)!}\tilde{f}_3^{(2-1)}(-a) = \frac{we^{-aw}}{2k+\delta-a} - \frac{e^{-aw}}{(2k+\delta-a)^2},\\
\operatorname{Res}_{-2k-\delta} f_3 &= \lim_{s\to 1}(2k+\delta+s)f_3(s) = \lim_{s\to -2k-\delta} \frac{e^{sw}}{(s+a)^2} = \frac{e^{-w(2k+\delta)}}{(2k+\delta-a)^2},\\
\operatorname{Res}_{-a} f_4 &= \frac{1}{(2-1)!}\tilde{f}_4^{(2-1)}(-a) = -\frac{we^{-aw}}{a+\rho} - \frac{e^{-aw}}{(a+\rho)^2},\\
\operatorname{Res}_{\rho} f_4 &= \lim_{s\to \rho}(s-\rho)f_4(s) = \lim_{s\to \rho} \frac{e^{sw}}{(s+a)^2} = \frac{e^{\rho w}}{(a+\rho)^2}.
\end{aligned}$$

By these residue calculations, we get the value of the following three integrals

$$\begin{aligned}
\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} f_2(s)\,ds &= \begin{cases} 0\,, & \text{if } w \le 0 \\ -\frac{e^{w}}{(a+1)^2} + \frac{e^{-aw}}{(a+1)^2} + \frac{we^{-aw}}{a+1}\,, & \text{else} \end{cases}\\
\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} f_3(s)\,ds &= \begin{cases} 0\,, & \text{if } w \le 0 \\ \frac{e^{-w(2k+\delta)}}{(2k+\delta-a)^2} + \frac{we^{-aw}}{2k+\delta-a} - \frac{e^{-aw}}{(2k+\delta-a)^2}\,, & \text{else} \end{cases}\\
\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} f_4(s)\,ds &= \begin{cases} 0\,, & \text{if } w \le 0 \\ \frac{e^{\rho w}}{(a+\rho)^2} - \frac{we^{-aw}}{a+\rho} - \frac{e^{-aw}}{(a+\rho)^2}\,, & \text{else.} \end{cases}
\end{aligned}$$

By the substitution of $x = e^w$, the proof of the assertion is complete. □

LEMMA 6.22. *Let x be a positive real number, and $a \in \,]0,1[$. Then*

$$\begin{aligned}
&\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2}\,\frac{\zeta'}{\zeta}(s)\,ds\\
&= -\frac{x}{(a+1)^2} + \sum_{k=1}^{\infty} \frac{x^{\rho(\zeta,k)}}{(\rho(\zeta,k)+a)^2} + \frac{\zeta'}{\zeta}(-a)\frac{\ln(x)}{x^a} + \frac{1}{x^a}\left(\frac{\zeta'}{\zeta}\right)'(-a) + \sum_{k=1}^{\infty}\frac{x^{-2k}}{(2k-a)^2}.
\end{aligned}$$

PROOF. By Lemma 6.19, we have

$$\left(\frac{\zeta'}{\zeta}\right)'(-a) \underset{(6.19)}{=} \frac{1}{(1+a)^2} - \sum_{k=1}^{\infty}\frac{1}{(2k-a)^2} - \sum_{k=1}^{\infty}\frac{1}{(\rho(\zeta,k)+a)^2}. \tag{76}$$

Using Lemma 6.19, Lemma 6.21, and equation (76), we complete the proof of the assertion as follows

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2}\,\frac{\zeta'}{\zeta}(s)\,ds$$

$$
\begin{aligned}
&\underset{(6.19)}{=} \left(\ln(2\pi) - 1 - \tfrac{1}{2}\sum_{k=1}^{\infty}\tfrac{1}{k} + \sum_{k=1}^{\infty}\tfrac{1}{\rho(\zeta,k)}\right)\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2}ds \\
&\quad + \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2}\left(\tfrac{1}{1-s} + \sum_{k=1}^{\infty}\tfrac{1}{2k+s} + \sum_{k=1}^{\infty}\tfrac{1}{s-\rho(\zeta,k)}\right)ds \\
&\underset{(6.21)}{=} \left(\ln(2\pi) - 1 - \tfrac{1}{2}\sum_{k=1}^{\infty}\tfrac{1}{k} + \sum_{k=1}^{\infty}\tfrac{1}{\rho(\zeta,k)}\right)\frac{\ln(x)}{x^a} \\
&\quad - \frac{x}{(a+1)^2} + \frac{1}{x^a(a+1)^2} + \frac{\ln(x)}{x^a(a+1)} \\
&\quad + \sum_{k=1}^{\infty}\left(\frac{\ln(x)}{x^a(2k-a)} - \frac{1}{x^a(2k-a)^2} + \frac{1}{x^{2k}(2k-a)^2}\right) \\
&\quad + \sum_{k=1}^{\infty}\left(\frac{x^{\rho(\zeta,k)}}{(a+\rho(\zeta,k))^2} - \frac{\ln(x)}{x^a(a+\rho(\zeta,k))^2} - \frac{1}{x^a(a+\rho(\zeta,k))^2}\right) \\
&\underset{(76),(6.19)}{=} \tfrac{\zeta'}{\zeta}(-a)\frac{\ln(x)}{x^a} - \frac{\ln(x)}{x^a}\sum_{k=1}^{\infty}\frac{1}{2k-a} + \frac{\ln(x)}{x^a}\sum_{k=1}^{\infty}\frac{1}{\rho(\zeta,k)+a} - \frac{x}{(1+a)^2} \\
&\quad + \frac{1}{x^a}\left(\tfrac{\zeta'}{\zeta}\right)'(-a) + \sum_{k=1}^{\infty}\left(\frac{\ln(x)}{x^a(2k-a)} + \frac{1}{x^{2k}(2k-a)^2}\right) \\
&\quad + \sum_{k=1}^{\infty}\left(\frac{x^{\rho(\zeta,k)}}{(a+\rho(\zeta,k))^2} - \frac{\ln(x)}{x^a(a+\rho(\zeta,k))}\right) \\
&= -\frac{x}{(a+1)^2} + \sum_{k=1}^{\infty}\frac{x^{\rho(\zeta,k)}}{(\rho(\zeta,k)+a)^2} + \tfrac{\zeta'}{\zeta}(-a)\frac{\ln(x)}{x^a} + \frac{1}{x^a}\left(\tfrac{\zeta'}{\zeta}\right)'(-a) \\
&\quad + \sum_{k=1}^{\infty}\frac{x^{-2k}}{(2k-a)^2}. \quad \square
\end{aligned}
$$

LEMMA 6.23. *Let x be a positive real number, $a \in \,]0,1[\,$, and let χ a character. Let* $\delta = \begin{cases} 0\,, & \text{if } \chi(-1) = 1 \\ 1\,, & \text{if } \chi(-1) = -1 \end{cases}$. *Then*

$$
\begin{aligned}
&\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2}\,\tfrac{L'}{L}(s,\chi)\,ds \\
&= \sum_{k=1}^{\infty}\frac{x^{\rho(L,k)}}{(\rho(L,k)+a)^2} + \tfrac{L'}{L}(-a,\chi)\frac{\ln(x)}{x^a} + \frac{1}{x^a}\left(\tfrac{L'}{L}\right)'(-a,\chi) + \sum_{k=0}^{\infty}\frac{x^{-2k-\delta}}{(2k+\delta-a)^2}.
\end{aligned}
$$

PROOF. By Lemma 6.20, we have

$$
\left(\tfrac{L'}{L}\right)'(-a,\chi) \underset{(6.20)}{=} -\frac{1}{(\delta-a)^2} - \sum_{k=1}^{\infty}\frac{1}{(2k+\delta-a)^2} - \sum_{k=1}^{\infty}\frac{1}{(\rho(L,k)+a)^2}. \tag{77}
$$

Define $B(\chi) := \frac{\xi'}{\xi}(0,\chi)$. Using Lemma 6.20, Lemma 6.21, and equation (77), we complete the proof of the assertion as follows

$$
\begin{aligned}
& \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2}\,\tfrac{L'}{L}(s,\chi)\,ds \\
\underset{(6.20)}{=}\quad & \left(B(\chi)+\tfrac{1}{2}\ln(\tfrac{\pi}{m})+\tfrac{\gamma}{2}-\tfrac{1}{2}\sum_{k=1}^{\infty}\frac{1}{k}+\sum_{k=1}^{\infty}\frac{1}{\rho(L,k)}\right)\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2}\,ds \\
& +\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2}\left(\frac{1}{s+\delta}+\sum_{k=1}^{\infty}\frac{1}{2k+\delta+s}+\sum_{k=1}^{\infty}\frac{1}{s-\rho(L,k)}\right)ds \\
\underset{(6.21)}{=}\quad & \left(B(\chi)+\tfrac{1}{2}\ln(\tfrac{\pi}{m})+\tfrac{\gamma}{2}-\tfrac{1}{2}\sum_{k=1}^{\infty}\frac{1}{k}+\sum_{k=1}^{\infty}\frac{1}{\rho(L,k)}\right)\frac{\ln(x)}{x^a} \\
& +\frac{\ln(x)}{x^a(\delta-a)}-\frac{1}{x^a(\delta-a)^2}+\frac{1}{x^\delta(\delta-a)^2} \\
& +\sum_{k=1}^{\infty}\left(\frac{\ln(x)}{x^a(2k+\delta-a)}-\frac{1}{x^a(2k+\delta-a)^2}+\frac{1}{x^{2k+\delta}(2k+\delta-a)^2}\right) \\
& +\sum_{k=1}^{\infty}\left(\frac{x^{\rho(L,k)}}{(a+\rho(L,k))^2}-\frac{\ln(x)}{x^a(a+\rho(L,k))^2}-\frac{1}{x^a(a+\rho(L,k))^2}\right) \\
\underset{(77),(6.20)}{=}\quad & \tfrac{L'}{L}(-a,\chi)\frac{\ln(x)}{x^a}-\frac{\ln(x)}{x^a}\sum_{k=1}^{\infty}\frac{1}{2k+\delta-a}+\frac{\ln(x)}{x^a}\sum_{k=1}^{\infty}\frac{1}{\rho(L,k)+a} \\
& +\frac{1}{x^\delta(\delta-a)^2}+\frac{1}{x^a}\left(\tfrac{L'}{L}\right)'(-a,\chi) \\
& +\sum_{k=1}^{\infty}\left(\frac{\ln(x)}{x^a(2k+\delta-a)}+\frac{1}{x^{2k+\delta}(2k+\delta-a)^2}\right) \\
& +\sum_{k=1}^{\infty}\left(\frac{x^{\rho(L,k)}}{(a+\rho(L,k))^2}-\frac{\ln(x)}{x^a(a+\rho(L,k))}\right) \\
=\quad & \sum_{k=1}^{\infty}\frac{x^{\rho(L,k)}}{(\rho(L,k)+a)^2}+\tfrac{L'}{L}(-a,\chi)\frac{\ln(x)}{x^a}+\frac{1}{x^a}\left(\tfrac{L'}{L}\right)'(-a,\chi) \\
& +\sum_{k=0}^{\infty}\frac{x^{-2k-\delta}}{(2k+\delta-a)^2}. \quad \square
\end{aligned}
$$

LEMMA 6.24. *Let x be a positive real number, $a \in]0,1[$, and χ a character. Then*

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2}\,\frac{\zeta'}{\zeta}(s)\,ds = -\sum_{k=1}^{x-1}\Lambda(k)(\tfrac{k}{x})^a\ln(\tfrac{x}{k}). \tag{78}$$

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2}\,\tfrac{L'}{L}(s,\chi)\,ds=-\sum_{k=1}^{x-1}\Lambda(k)\chi(k)(\tfrac{k}{x})^a\ln(\tfrac{x}{k}). \tag{79}$$

PROOF. We will give only a proof of equation (79) since the proof of equation (78) is analogous. Using Theorem 6.16, and Lemma 6.21, equation (79) is proved as follows

$$\begin{aligned}\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2}\,\tfrac{L'}{L}(s,\chi)\,ds &\underset{(62)}{=} \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2}\left(-\sum_{k=1}^{\infty}\frac{\Lambda(k)\chi(k)}{k^s}\right)ds\\ &= -\frac{1}{2\pi i}\sum_{k=1}^{\infty}\Lambda(k)\chi(k)\int_{2-i\infty}^{2+i\infty}\frac{(\frac{x}{k})^s}{(s+a)^2}\,ds\\ &\underset{(6.21)}{=} -\sum_{k=1}^{x-1}\Lambda(k)\chi(k)(\tfrac{k}{x})^a\ln(\tfrac{x}{k}).\quad\square\end{aligned}$$

LEMMA 6.25. *Let α be a positive integer such that $\mathrm{Re}(\rho(\zeta,k))=\frac{1}{2}$ for all positive integers k with $|\mathrm{Im}(\rho(\zeta,k))|\le\alpha$. Let β be a positive real number such that*

$$\beta\le\frac{|\{k\in\mathbb{N}_{>0}\mid \mathrm{Re}(\rho(\zeta,k))=\frac{1}{2}\}|}{|\{k\in\mathbb{N}_{>0}\mid 0<\mathrm{Re}(\rho(\zeta,k))<1\}|}.$$

Let $x\ge 1$ be a real number, $a\in\,]0,1[$, and $C(\alpha):=\sum_{k=1}^{\alpha}\left(\frac{1}{\rho(\zeta,k)}+\frac{1}{\bar\rho(\zeta,k)}\right)$. Then

$$\left|\sum_{k=1}^{\infty}\frac{x^{\rho(\zeta,k)}}{(\rho(\zeta,k)+a)^2}\right|<\sqrt{x}(\gamma+2-\ln(4\pi))+(1-\beta)(\tfrac{x}{2}-\sqrt{x})(\gamma+2-\ln(4\pi)-C(\alpha)).$$

PROOF. By Lemma 6.19, we have the following three equations

$$\begin{aligned}\mathrm{Re}(\tfrac{\zeta'}{\zeta}(0)) &\underset{(6.19)}{=} 1+\tfrac{1}{2}\ln(\pi)+\tfrac{\gamma}{2}-\sum_{k=1}^{\infty}\frac{1}{\rho(\zeta,k)}\\ &\underset{(6.19)}{=} 1+\tfrac{1}{2}\ln(\pi)+\tfrac{\gamma}{2}-\sum_{k=1}^{\infty}\frac{1}{\bar\rho(\zeta,k)}\\ &\underset{(6.19)}{=} \ln(2\pi).\end{aligned}$$

Therefore, we have

$$\begin{aligned}\sum_{k=1}^{\infty}\left(\frac{1}{\rho(\zeta,k)}+\frac{1}{\bar\rho(\zeta,k)}\right) &= \gamma+2+\ln(\pi)-2\ln(2\pi)\\ &= \gamma+2+\ln(\tfrac{\pi}{4\pi^2})\\ &= \gamma+2-\ln(4\pi).\end{aligned} \tag{80}$$

Let σ, and t be real numbers with $\sigma>0$. Then we have the following estimate

$$\frac{1}{\sigma+it}+\frac{1}{\sigma-it}=\frac{2\sigma}{\sigma^2+t^2}>0. \tag{81}$$

Thus, we have

$$C(\alpha) \underset{(80),(81)}{<} \gamma + 2 - \ln(4\pi). \tag{82}$$

Hence, the proof of the assertion follows by

$$\begin{aligned}
\left|\sum_{k=1}^{\infty} \frac{x^{\rho(\zeta,k)}}{(\rho(\zeta,k)+a)^2}\right| &\leq \sum_{k=1}^{\infty} \frac{x^{\mathrm{Re}(\rho(\zeta,k))}}{|\rho(\zeta,k)+a|^2} \\
&< \sum_{k=1}^{\infty} \frac{x^{\mathrm{Re}(\rho(\zeta,k))}}{|\rho(\zeta,k)|^2} \\
&= \sum_{k=1}^{\infty} \frac{x^{\mathrm{Re}(\rho(\zeta,k))}}{\rho(\zeta,k)\bar{\rho}(\zeta,k)} \\
&= \sum_{k=1}^{\infty} \frac{x^{\mathrm{Re}(\rho(\zeta,k))}}{2\mathrm{Re}(\rho(\zeta,k))} \left(\frac{1}{\rho(\zeta,k)} + \frac{1}{\bar{\rho}(\zeta,k)}\right) \\
&\underset{(82)}{\leq} \sqrt{x}(\gamma + 2 - \ln(4\pi)) \\
&\quad + \sum_{k=\alpha+1}^{\infty} \left(\frac{x^{\mathrm{Re}(\rho(\zeta,k))}}{2\mathrm{Re}(\rho(\zeta,k))} - \sqrt{x}\right) \left(\frac{1}{\rho(\zeta,k)} + \frac{1}{\bar{\rho}(\zeta,k)}\right) \\
&< \sqrt{x}(\gamma + 2 - \ln(4\pi)) \\
&\quad + \sum_{k=\alpha+1}^{\infty} (\beta\sqrt{x} + (1-\beta)\tfrac{x}{2} - \sqrt{x}) \left(\frac{1}{\rho(\zeta,k)} + \frac{1}{\bar{\rho}(\zeta,k)}\right) \\
&= \sqrt{x}(\gamma + 2 - \ln(4\pi)) \\
&\quad + (1-\beta)(\tfrac{x}{2} - \sqrt{x})(\gamma + 2 - \ln(4\pi) - C(\alpha)). \quad \square
\end{aligned}$$

COROLLARY 6.26. *Let $x \geq 1$ be a real number, and $a \in]0,1[$. Then*

$$\left|\sum_{k=1}^{\infty} \frac{x^{\rho(\zeta,k)}}{(\rho(\zeta,k)+a)^2}\right| < \frac{\sqrt{x}}{21} + 18 \cdot 10^{-10} x.$$

PROOF. This corollary is an easy conclusion of an easy estimate; see for example articles [**82**], and [**34**], and Lemma 6.25.

(1) First, we have the following upper bound

$$\gamma + 2 - \ln(4\pi) < \tfrac{1}{21}. \tag{83}$$

(2) J. van de Lune et al. have shown, by extensive computations [**82**], that Riemann's Hypothesis is true for all non-trivial roots of the zeta function with an absolute value less than 545 439 823. A simple summation of the evaluated roots shows

$$\gamma + 2 - \ln(4\pi) - C(3 \cdot 10^9) < 6 \cdot 10^{-9}. \tag{84}$$

(3) Moreover, J. B. Conrey has proved in [**34**], that at least 40% of all non-trivial roots of the zeta function lie on the critical line $\frac{1}{2} + it$ where t is a real number.

By these three items, and Lemma 6.25, we get

$$\begin{aligned}\left|\sum_{k=1}^{\infty}\frac{x^{\rho(\zeta,k)}}{(\rho(\zeta,k)+a)^2}\right| &\underset{(6.25),(83),(84)}{<} \frac{\sqrt{x}}{21}+\frac{3}{5}(\frac{x}{2}-\sqrt{x})\cdot 6\cdot 10^{-9}\\ &< \frac{\sqrt{x}}{21}+18\cdot 10^{-10}x. \quad \square\end{aligned}$$

LEMMA 6.27. *Let s,t be complex numbers, χ a character, and* $\delta=\begin{cases}0\,, & \text{if } \chi(-1)=1\\ 1\,, & \text{if } \chi(-1)=-1.\end{cases}$ *Then*

$$\frac{L'}{L}(s,\chi)-\frac{L'}{L}(t,\chi)=\frac{1}{s+\delta}-\frac{1}{2}\frac{\Gamma'}{\Gamma}(\frac{s+\delta+2}{2})+\frac{1}{2}\frac{\Gamma'}{\Gamma}(\frac{t+\delta}{2})+\sum_{k=1}^{\infty}\left(\frac{1}{s-\rho(L,k)}-\frac{1}{t-\rho(L,k)}\right).$$

PROOF. By Lemma 6.20, and Lemma 6.14, the proof of the assertion follows by

$$\begin{aligned}\frac{L'}{L}(s,\chi)-\frac{L'}{L}(t,\chi) &\underset{(6.20)}{=} \frac{1}{s+\delta}+\frac{\gamma}{2}-\frac{1}{2}\sum_{k=1}^{\infty}\left(\frac{1}{k}-\frac{2}{2k+\delta+s}\right)-\frac{1}{t+\delta}-\frac{\gamma}{2}+\frac{1}{2}\sum_{k=1}^{\infty}\left(\frac{1}{k}-\frac{2}{2k+\delta+t}\right)\\ &\quad+\sum_{k=1}^{\infty}\left(\frac{1}{s-\rho(L,k)}-\frac{1}{t-\rho(L,k)}\right)\\ &= \frac{1}{s+\delta}-\frac{1}{2}\left(-\gamma-\frac{2}{s+\delta+2}+\sum_{k=1}^{\infty}\left(\frac{1}{k}-\frac{2}{2k+s+\delta+2}\right)\right)\\ &\quad+\frac{1}{2}\left(-\gamma-\frac{2}{t+\delta}+\sum_{k=1}^{\infty}\left(\frac{1}{k}-\frac{2}{2k+t+\delta}\right)\right)\\ &\quad+\sum_{k=1}^{\infty}\left(\frac{1}{s-\rho(L,k)}-\frac{1}{t-\rho(L,k)}\right)\\ &\underset{(6.14)}{=} \frac{1}{s+\delta}-\frac{1}{2}\frac{\Gamma'}{\Gamma}(\frac{s+\delta+2}{2})+\frac{1}{2}\frac{\Gamma'}{\Gamma}(\frac{t+\delta}{2})+\sum_{k=1}^{\infty}\left(\frac{1}{s-\rho(L,k)}-\frac{1}{t-\rho(L,k)}\right). \quad \square\end{aligned}$$

LEMMA 6.28. *Let s be a complex number, χ a character, and* $\delta=\begin{cases}0\,, & \text{if } \chi(-1)=1\\ 1\,, & \text{if } \chi(-1)=-1.\end{cases}$ *Then*

$$\left(\frac{L'}{L}\right)'(s,\chi)=-\frac{1}{(s+\delta)^2}-\frac{1}{4}\left(\frac{\Gamma'}{\Gamma}\right)'(\frac{s+\delta+2}{2})-\sum_{k=1}^{\infty}\frac{1}{(\rho(L,k)-s)^2}.$$

PROOF. By Lemma 6.27, it follows

$$\frac{L'}{L}(s,\chi)\underset{(6.27)}{=}\frac{L'}{L}(2,\chi)+\frac{1}{s+\delta}-\frac{1}{2}\frac{\Gamma'}{\Gamma}(\frac{s+\delta+2}{2})+\frac{1}{2}\frac{\Gamma'}{\Gamma}(\frac{2+\delta}{2})-\sum_{k=1}^{\infty}\left(\frac{1}{\rho(L,k)-s}-\frac{1}{\rho(L,k)-2}\right).$$

Taking derivatives, we get

$$\left(\frac{L'}{L}\right)'(s,\chi)=-\frac{1}{(s+\delta)^2}-\frac{1}{2}\left(\frac{\Gamma'}{\Gamma}\right)'(\frac{s+\delta+2}{2})\frac{1}{2}-\sum_{k=1}^{\infty}\frac{1}{(\rho(L,k)-s)^2}. \quad \square$$

LEMMA 6.29 (ERH). *Assume the Extended Riemann Hypothesis is correct. Let m be a natural number greater than 1, $a \in]0,1[$, χ a quadratic character modulo m, and* $\delta = \begin{cases} 0\,, & \text{if } \chi(-1)=1 \\ 1\,, & \text{if } \chi(-1)=-1 \end{cases}$. *Then*

$$\tfrac{L'}{L}(-a,\chi) > \tfrac{\zeta'}{\zeta}(a+1) + \frac{1}{\delta-a} - \ln(2) - (2a+1)\sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+a|^2}\,.$$

PROOF. Let t be a real number, and $\sigma = \frac{1}{2}$. Then we have

$$(a+\sigma)(a+1-\sigma) = (a+1-\sigma)^2. \tag{85}$$

Therefore, we have

$$\begin{aligned} & \frac{1}{(a+\sigma+it)(a+1-\sigma-it)} + \frac{1}{(a+\sigma-it)(a+1-\sigma+it)} \\ = \;& \frac{2(a+\sigma)(a+1-\sigma)+2t^2}{|a+\sigma+it|^2\cdot|a+1-\sigma-it|^2} \\ \underset{(85)}{=} \;& \frac{2((a+1-\sigma)^2+t^2)}{|a+\sigma+it|^2\cdot((a+1-\sigma)^2+t^2)} \\ = \;& \frac{1}{|a+\sigma+it|^2} + \frac{1}{|a+\sigma-it|^2}\,. \end{aligned} \tag{86}$$

Let n be a positive integer. Then, by the relation $4n^2+8n+4 > 4n^2+8n+3$, we get

$$\frac{1}{2n+1}+\frac{1}{2n+3} = \frac{4n+4}{(2n+1)(2n+3)} > \frac{1}{n+1} = \frac{1}{2n+2}+\frac{1}{2n+2}\,.$$

Hence,

$$\frac{1}{2n+3}-\frac{1}{2n+2} > \frac{1}{2n+2}-\frac{1}{2n+1}\,. \tag{87}$$

By Lemma 6.14, and Lemma 6.27, we complete the proof of the assertion as follows

$$\begin{aligned} & \tfrac{L'}{L}(-a,\chi) \\ \underset{(6.27)}{=} \;& \tfrac{L'}{L}(a+1,\chi) + \frac{1}{\delta-a} - \tfrac{1}{2}\tfrac{\Gamma'}{\Gamma}\left(\tfrac{\delta+2-a}{2}\right) + \tfrac{1}{2}\tfrac{\Gamma'}{\Gamma}\left(\tfrac{\delta+a+1}{2}\right) \\ & -\sum_{k=1}^{\infty}\left(\frac{1}{a+\rho(L,k)}+\frac{1}{a+1-\rho(L,k)}\right) \end{aligned}$$

$$
\begin{aligned}
\underset{(6.14)}{=} \quad & \tfrac{L'}{L}(a+1,\chi) + \frac{1}{\delta - a} \\
& - \tfrac{1}{2}\left(-\gamma - \frac{2}{\delta+2-a} + \sum_{k=1}^{\infty}\left(\frac{1}{k} - \frac{2}{2k+\delta+2-a}\right)\right) \\
& + \tfrac{1}{2}\left(-\gamma - \frac{2}{\delta+a+1} + \sum_{k=1}^{\infty}\left(\frac{1}{k} - \frac{2}{2k+\delta+a+1}\right)\right) \\
& - \sum_{k=1}^{\infty}\left(\frac{1}{a+\rho(L,k)} + \frac{1}{a+1-\rho(L,k)}\right) \\
= \quad & \tfrac{L'}{L}(a+1,\chi) + \frac{1}{\delta-a} + \sum_{k=0}^{\infty}\left(\frac{1}{2k+\delta+2-a} - \frac{1}{2k+\delta+a+1}\right) \\
& - (2a+1)\sum_{k=1}^{\infty}\frac{1}{(a+\rho(L,k))\,(a+1-\rho(L,k))} \\
\underset{(ERH),(86),(87)}{>} \quad & \tfrac{L'}{L}(a+1,\chi) + \frac{1}{\delta-a} - \sum_{k=0}^{\infty}\left(\frac{1}{2k+1} - \frac{1}{2k+2}\right) \\
& -(2a+1)\sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+a|^2} \\
\underset{(6.16)}{=} \quad & -\sum_{k=1}^{\infty}\frac{\Lambda(k)\chi(k)}{k^{a+1}} + \frac{1}{\delta-a} - \sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k} - (2a+1)\sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+a|^2} \\
\underset{(6.13)}{>} \quad & -\sum_{k=1}^{\infty}\frac{\Lambda(k)}{k^{a+1}} + \frac{1}{\delta-a} - \ln(2) - (2a+1)\sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+a|^2} \\
\underset{(6.16)}{=} \quad & \tfrac{\zeta'}{\zeta}(a+1) + \frac{1}{\delta-a} - \ln(2) - (2a+1)\sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+a|^2}\,. \quad \square
\end{aligned}
$$

LEMMA 6.30. *Let m be a natural number greater than 1, $a \in \,]0,1[$, χ a quadratic character modulo m, and $\delta = \begin{cases} 0\,, & \text{if } \chi(-1)=1 \\ 1\,, & \text{if } \chi(-1)=-1 \end{cases}$. Then*

$$\left(\tfrac{L'}{L}\right)'(-a,\chi) + \frac{1}{(\delta-a)^2} + \sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+a|^2} > -\tfrac{5}{4}\,.$$

PROOF. By Lemma 6.28, and Lemma 6.14, we have

$$
\begin{aligned}
& \left(\tfrac{L'}{L}\right)'(-a,\chi) + \frac{1}{(\delta-a)^2} + \sum_{k=1}^{\infty}\frac{1}{(\rho(L,k)+a)^2} \\
\underset{(6.28)}{=} \quad & -\tfrac{1}{4}\left(\tfrac{\Gamma'}{\Gamma}\right)'\left(\tfrac{\delta+2-a}{2}\right)
\end{aligned}
$$

$$\begin{aligned}
&\underset{(6.14)}{=} -\tfrac{1}{4}\left(\frac{4}{(\delta+2-a)^2}+\sum_{k=1}^{\infty}\frac{4}{(2k+\delta+2-a)^2}\right)\\
&= -\sum_{k=1}^{\infty}\frac{1}{(2k+\delta-a)^2}\\
&> -\sum_{k=1}^{\infty}\frac{1}{(2k-1)^2}\\
&= -\tfrac{\pi^2}{8} > -\tfrac{5}{4}\,.
\end{aligned}$$

Therefore, we complete the proof of the assertion by the estimate

$$-\left(\tfrac{L'}{L}\right)'(-a,\chi)-\frac{1}{(\delta-a)^2}-\tfrac{5}{4}<\left|\sum_{k=1}^{\infty}\frac{1}{(\rho(L,k)+a)^2}\right|\le\sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+a|^2}\,.\quad\square$$

LEMMA 6.31. *Let x be a positive integer, $a\in\,]0,1[$, and χ a real character with $\chi(k)=1$ for $k\in\{l\in\mathbb{N}\mid 1\le l<x\}$ and $\chi(x)\neq 1$. Then*

$$\tfrac{L'}{L}(a+1,\chi)<\tfrac{\zeta'}{\zeta}(a+1)-\frac{2\ln(x)}{x^{a+1}}+\frac{52(a+1)}{25\cdot ax^a}\,.$$

PROOF. By a result due to J. B. Rosser and L. Schoenfeld[14] ([**112**] on page 71), we get an upper bound for the function ψ (see Definition 6.11)

$$\psi(x)<1.03883x\qquad\text{for positive integers } x. \tag{88}$$

By this estimate (88), and Theorem 6.16, we get

$$\begin{aligned}
\tfrac{L'}{L}(a+1,\chi) &\underset{(62)}{=} -\sum_{k=1}^{x-1}\frac{\Lambda(k)}{k^{a+1}}-\sum_{k=x}^{\infty}\frac{\Lambda(k)\chi(k)}{k^{a+1}}\\
&\underset{(61)}{=} \tfrac{\zeta'}{\zeta}(a+1)+\sum_{k=x}^{\infty}\frac{\Lambda(k)}{k^{a+1}}-\sum_{k=x}^{\infty}\frac{\Lambda(k)\chi(k)}{k^{a+1}}\\
&< \tfrac{\zeta'}{\zeta}(a+1)+2\sum_{k=x}^{\infty}\frac{\Lambda(k)}{k^{a+1}}\\
&\underset{(6.11)}{=} \tfrac{\zeta'}{\zeta}(a+1)+2\sum_{k=x}^{\infty}\frac{\psi(k)-\psi(k-1)}{k^{a+1}}\\
&\underset{(6.1)}{=} \tfrac{\zeta'}{\zeta}(a+1)+2\sum_{k=x+1}^{\infty}\frac{\psi(k)-\psi(k-1)}{k^{a+1}}\\
&= \tfrac{\zeta'}{\zeta}(a+1)+2\left(\sum_{k=x}^{\infty}\frac{\psi(k)}{k^{a+1}}-\frac{\psi(x)}{x^{a+1}}-\sum_{k=x}^{\infty}\frac{\psi(k)}{(k+1)^{a+1}}\right)
\end{aligned}$$

[14] L. Schoenfeld has shown in [**116**] a sharper upper bound $\psi(x)<1.001102x+1.001102\sqrt{x}+3\sqrt[3]{x}$ for positive integers x, but this bound is only useful for larger values ($x\ge 2339$).

$$\begin{aligned}
&\underset{(6.1)}{\leq} && \tfrac{\zeta'}{\zeta}(a+1) - \frac{2\ln(x)}{x^{a+1}} + 2\sum_{k=x}^{\infty}\psi(k)\left(\frac{1}{k^{a+1}} - \frac{1}{(k+1)^{a+1}}\right)\\
&= && \tfrac{\zeta'}{\zeta}(a+1) - \frac{2\ln(x)}{x^{a+1}} + 2\sum_{k=x}^{\infty}\psi(k)(a+1)\int_k^{k+1}\frac{dt}{t^{a+2}}\\
&\leq && \tfrac{\zeta'}{\zeta}(a+1) - \frac{2\ln(x)}{x^{a+1}} + 2(a+1)\sum_{k=x}^{\infty}\int_k^{k+1}\frac{\psi(t)}{t^{a+2}}\,dt\\
&\underset{(88)}{\leq} && \tfrac{\zeta'}{\zeta}(a+1) - \frac{2\ln(x)}{x^{a+1}} + 2(a+1)\cdot 1.03883\cdot\int_x^{\infty}\frac{dt}{t^{a+1}}\\
&= && \tfrac{\zeta'}{\zeta}(a+1) - \frac{2\ln(x)}{x^{a+1}} + 2(a+1)\cdot 1.03883\cdot(0+\tfrac{1}{ax^a})\\
&< && \tfrac{\zeta'}{\zeta}(a+1) - \frac{2\ln(x)}{x^{a+1}} + \frac{52(a+1)}{25\cdot ax^a}\,. \quad \square
\end{aligned}$$

LEMMA 6.32. *Let $x \geq 1$ be a real number, $a \in \left]0,1\right[$, $m \geq 2$ be a positive integer, and let χ be a quadratic character modulo m. Let σ' be a real number such that $\mathrm{Re}(\rho(L,k)) \leq \sigma'$ for all positive integers k. Let $d \leq a+\sigma$ be a real non-negative number such that there do not exists a non-trivial root of the L-function which imaginary part is inside the interval $\left]\, a+\sigma-d\sqrt{2}, a+\sigma+d\sqrt{2}\,\right[$. Then*

$$x^{\sigma'}\left(\sum_{k=1}^{\infty}\frac{2d^2}{|\rho(L,k)+a|^4} - \sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+a|^2}\right) \leq \sum_{k=1}^{\infty}\frac{x^{\rho(L,k)}}{(\rho(L,k)+a)^2}\,.$$

PROOF. Let ρ be a non-trivial root of the L-function and define $\rho := \sigma + it$. Then we have

$$((a+\sigma)-t)^2 \geq 2d^2 \quad \text{and} \quad (a+\sigma)^2+t^2 \geq t^2-(a+\sigma)^2+2d^2.$$

Hence, by $\sigma \leq \sigma'$, we get the two estimates

$$\begin{aligned}
x^{\sigma'-\sigma}((a+\sigma)^2+t^2) &\geq 2(a+\sigma)t+2d^2\\
\text{and}\quad x^{\sigma'-\sigma}((a+\sigma)^2+t^2) &\geq t^2-(a+\sigma)^2+2d^2. \qquad (89)
\end{aligned}$$

Therefore,

$$\begin{aligned}
& -x^{\sigma'}|\bar{\rho}+a|^2 - x^{\sigma'}|\rho+a|^2\\
= \;& -2x^{\sigma'}((a+\sigma)^2+t^2)\\
\underset{(89)}{\leq} \;& 2x^{\sigma}(((a+\sigma)^2-t^2)\cos(t\ln(x)) + 2(a+\sigma)t\sin(t\ln(x)) - 2d^2)\\
= \;& x^{\sigma}(\cos(t\ln(x)) + i\sin(t\ln(x))((a+\sigma)^2-t^2-2i(a+\sigma)t)\\
& + x^{\sigma}(\cos(t\ln(x)) - i\sin(t\ln(x)))((a+\sigma)^2-t^2+2i(a+\sigma)t) - 4d^2x^{\sigma}\\
= \;& x^{\sigma+it}((a+\sigma)^2-t^2-2i(a+\sigma)t) + x^{\sigma-it}((a+\sigma)^2-t^2+2i(a+\sigma)t) - 4d^2x^{\sigma}\\
= \;& x^{\rho}(a+\sigma-it)^2 + x^{\bar{\rho}}(a+\sigma+it)^2 - 4d^2x^{\sigma}\\
\leq \;& x^{\rho}(\bar{\rho}+a)^2 + x^{\bar{\rho}}(\rho+a)^2 - 4d^2x^{\sigma'}.
\end{aligned}$$

Thus,

$$\begin{aligned} -\frac{x^{\sigma'}}{|\rho+a|^2} - \frac{x^{\sigma'}}{|\bar{\rho}+a|^2} &\leq \frac{x^{\rho}(\bar{\rho}+a)^2 + x^{\bar{\rho}}(\rho+a)^2 - 4d^2x^{\sigma'}}{((a+\sigma)^2+t^2)^2} \\ &= \frac{x^{\rho}}{(\rho+a)^2} + \frac{x^{\bar{\rho}}}{(\bar{\rho}+a)^2} - \frac{2d^2x^{\sigma'}}{|\rho+a|^4} - \frac{2d^2x^{\sigma'}}{|\bar{\rho}+a|^4} \end{aligned}$$

The proof of the assertion is complete by adding the summands of the right sum and of the left sum of the assertion since χ is a quadratic character and we have two important properties for the non-trivial roots of the L-function

(1) $\bar{\chi} = \chi^{-1} = \chi$,
(2) $L(\rho,\chi) = L(\bar{\rho},\bar{\chi}) = L(\bar{\rho},\chi)$ for $\rho \in \mathbb{C}$ with $0 < \mathrm{Re}(\rho) < 1$ and $L(\rho,\chi) = 0$.

□

Lemma 6.33 (ERH). *Assume the Extended Riemann Hypothesis is correct. Let x, and $m \geq 2$ be positive integers, $a \in]0,1[$, χ a primitive quadratic character modulo m with $\chi(k) = 1$ for $k \in \{l \in \mathbb{N} \mid 1 \leq l < x\}$ and $\chi(x) \neq 1$, and $\delta = \begin{cases} 0\,, & \text{if } \chi(-1) = 1 \\ 1\,, & \text{if } \chi(-1) = -1. \end{cases}$ Then*

$$\sum_{k=1}^{\infty} \frac{1}{|a+\rho(L,k)|^2} < \tfrac{1}{2a+1}\left(\ln(\tfrac{m}{\pi}) + 2\cdot\tfrac{\zeta'}{\zeta}(a+1) - \tfrac{4\ln(x)}{x^{a+1}} + \tfrac{104(a+1)}{25a\cdot x^a} + \tfrac{\Gamma'}{\Gamma}(\tfrac{a+1+\delta}{2})\right).$$

Proof. We define the functions σ and t as follows

$$\sigma(L,k) + it(L,k) := \rho(L,k) \qquad \text{for positive integers } k.$$

By Lemma 6.20, Lemma 6.31, and Lemma 6.14, we complete the proof of the assertion as follows

$$\begin{aligned} & \sum_{k=1}^{\infty} \frac{1}{|a+\rho(L,k)|^2} \\ \underset{(ERH)}{=} & \sum_{k=1}^{\infty} \frac{1}{(a+\frac{1}{2})^2 + t(L,k)^2} \\ = & \sum_{k=1}^{\infty} \frac{1}{2(a+\frac{1}{2})} \left(\frac{1}{a+1-\frac{1}{2}-it(L,k)} + \frac{1}{a+1-\frac{1}{2}+it(L,k)} \right) \\ \underset{(ERH)}{=} & \frac{1}{2a+1} \sum_{k=1}^{\infty} \left(\frac{1}{a+1-\rho(L,k)} + \frac{1}{a+1-\bar{\rho}(L,k)} \right) \\ = & \frac{1}{2a+1} \left(\sum_{k=1}^{\infty} \frac{1}{a+1-\rho(L,k)} + \sum_{k=1}^{\infty} \frac{1}{a+1-\bar{\rho}(L,k)} \right) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2a+1}\left(\ln(\tfrac{m}{\pi}) + \tfrac{L'}{L}(a+1,\chi) + \tfrac{L'}{L}(a+1,\bar{\chi})\right) \\
&\quad - \frac{1}{2a+1}\left(\frac{2}{a+1+\delta} + \gamma - \sum_{k=1}^{\infty}\left(\frac{1}{k} - \frac{2}{2k+\delta+a+1}\right)\right) \\
&\underset{(6.14),(6.31)}{<} \frac{1}{2a+1}\left(\ln(\tfrac{m}{\pi}) + 2\cdot\tfrac{\zeta'}{\zeta}(a+1) - \tfrac{4\ln(x)}{x^{a+1}} + \tfrac{104(a+1)}{25a\cdot x^a} + \tfrac{\Gamma'}{\Gamma}(\tfrac{a+1+\delta}{2})\right). \quad \square
\end{aligned}$$

8. Key Lemma

LEMMA 6.34 (ERH). *Assume the Extended Riemann Hypothesis is correct. Let x, and $m \geq 2$ be positive integers, let $a \geq 2$ be a real number, χ a quadratic character modulo m with $\chi(k) = 1$ for $k \in \{l \in \mathbb{N} \mid 1 \leq l < x\}$, and $\delta = \begin{cases} 0\,, & \text{if } \chi(-1) = 1 \\ 1\,, & \text{if } \chi(-1) = -1. \end{cases}$ Let σ be a real number such that $\mathrm{Re}(\rho(L,k)) \leq \sigma$ for all positive integers k. Then*

$$\tfrac{a^2}{(a+1)^2}\, x < \tfrac{a}{2+a}(\ln(m) + t(x))(x^\sigma + r(x)) + s(x),$$

where

$$\begin{aligned}
r(x) &:= \tfrac{(2a+1)\ln(x)+1}{\sqrt[a]{x}}, \\
s(x) &:= \tfrac{\ln(x)}{\sqrt[a]{x}}\left(\tfrac{\zeta'}{\zeta}(-\tfrac{1}{a}) + \tfrac{\zeta'}{\zeta}(\tfrac{a+1}{a}) + \ln(2) - \tfrac{a}{a\delta-1}\right) \\
&\quad + \tfrac{1}{\sqrt[a]{x}}\left(\left(\tfrac{\zeta'}{\zeta}\right)'(-\tfrac{1}{a}) + \tfrac{a^2}{(a\delta-1)^2} + \tfrac{5}{4}\right) \\
&\quad + \tfrac{\sqrt{x}}{21} + 18\cdot 10^{-10}x + \begin{cases} -a^2\,, & \text{if } \delta = 0 \\ \tfrac{4}{9x^2} - \ln(1+\tfrac{1}{x})\,, & \text{if } \delta = 1, \end{cases} \\
\textit{and} \quad t(x) &:= 2\cdot\tfrac{\zeta'}{\zeta}(\tfrac{a+1}{a}) - \tfrac{4\ln(x)}{x^{a+1}} + \tfrac{104(a+1)}{25\sqrt[a]{x}} + \tfrac{\Gamma'}{\Gamma}(\tfrac{a+1+a\delta}{2a}) - \ln(\pi).
\end{aligned}$$

PROOF. Let n be a positive integer. Then we have

$$(2n-\tfrac{1}{2})^2 \underset{(a\geq 2)}{\leq} (2n-\tfrac{1}{a})^2. \tag{90}$$

By the estimate

$$\begin{aligned}
& (2n)^2(2n+\tfrac{5}{2})^2((2n+1)^2 + x^{-1}(2n+\tfrac{3}{2})^2) \\
= \;& (16n^4+40n^3+25n^2)(4n^2+4n+1+x^{-1}(4n^2+6n+\tfrac{9}{4})) \\
< \;& (16n^4+40n^3+37n^2+15n+\tfrac{9}{4})(4n^2+10n+\tfrac{25}{4}+4n^2x^{-1}) \\
= \;& (4n^2+6n+\tfrac{9}{4})(4n^2+4n+1)(4n^2+10n+\tfrac{25}{4}+4n^2x^{-1}) \\
= \;& (2n+\tfrac{3}{2})^2(2n+1)^2((2n+\tfrac{5}{2})^2 + x^{-1}(2n)^2),
\end{aligned}$$

we get

$$\frac{1}{(2n+\frac{3}{2})^2} - \frac{x^{-1}}{(2n+\frac{5}{2})^2} < \frac{1}{(2n)^2} - \frac{x^{-1}}{(2n+1)^2}\,. \tag{91}$$

Therefore, we have an upper bound for the following sum

$$\begin{aligned}
& \sum_{k=1}^{\infty} \frac{x^{-2k}}{(2k-\frac{1}{a})^2} - \sum_{k=0}^{\infty} \frac{x^{-2k-1}}{(2k+\frac{a-1}{a})^2} && (92)\\
\underset{(90)}{\leq} & \sum_{k=1}^{\infty} \frac{x^{-2k}}{(2k-\frac{1}{2})^2} - \sum_{k=0}^{\infty} \frac{x^{-2k-1}}{(2k+1)^2} \\
= & \frac{4}{9x^2} - \frac{1}{x} + \sum_{k=1}^{\infty} \left(\frac{1}{(2k+\frac{3}{2})^2} - \frac{x^{-1}}{(2k+1)^2} \right) x^{-2k} \\
\underset{(91)}{<} & \frac{1}{3x^2} + \sum_{k=1}^{\infty} x^{-2k} \left(\frac{1}{(2k)^2} - \frac{x^{-1}}{(2k+1)^2} \right) \\
= & \frac{4}{9x^2} - \frac{1}{x} + \sum_{k=1}^{\infty} \frac{4k^2+4k+1-x^{-1}4k^2}{(2k)^2(2k+1)^2} \cdot x^{-2k} \\
\underset{(x^{-1}\leq 1)}{<} & \frac{4}{9x^2} - \frac{1}{x} + \sum_{k=1}^{\infty} \frac{8k^3-x^{-1}8k^3+4k^2+4k^2+2k-x^{-1}4k^2}{(2k)^2(2k+1)^2} \cdot x^{-2k} \\
= & \frac{4}{9x^2} - \frac{1}{x} + \sum_{k=1}^{\infty} \frac{(2k+1-x^{-1}2k)(4k^2+2k)}{(2k)^2(2k+1)^2} \cdot x^{-2k} \\
= & \frac{4}{9x^2} - \frac{1}{x} + \sum_{k=1}^{\infty} \frac{2k+1-x^{-1}2k}{2k(2k+1)} \cdot x^{-2k} \\
= & \frac{4}{9x^2} - \frac{1}{x} + \sum_{k=1}^{\infty} \left(\frac{1}{2k} - \frac{x^{-1}}{2k+1} \right) \cdot x^{-2k} \\
= & \frac{4}{9x^2} + \sum_{k=1}^{\infty} (-1)^k \cdot \frac{x^{-k}}{k} \\
\underset{(6.13)}{=} & \frac{4}{9x^2} - \ln(1+\tfrac{1}{x}). && (93)
\end{aligned}$$

Using Lemma 6.22, Lemma 6.23, Lemma 6.24, Lemma 6.29, and Lemma 6.30 of the previous section, we conclude

$$\begin{aligned}
& -\frac{x}{(\frac{1}{a}+1)^2} + \sum_{k=1}^{\infty} \frac{x^{\rho(\zeta,k)}}{(\rho(\zeta,k)+\frac{1}{a})^2} + \frac{\zeta'}{\zeta}(-\tfrac{1}{a}) \frac{\ln(x)}{\sqrt[a]{x}} \\
& + \frac{1}{\sqrt[a]{x}} \left(\frac{\zeta'}{\zeta} \right)' (-\tfrac{1}{a}) + \sum_{k=1}^{\infty} \frac{x^{-2k}}{(2k-\frac{1}{a})^2} \\
\underset{(6.22)}{=} & \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+\frac{1}{a})^2} \frac{\zeta'}{\zeta}(s)\, ds
\end{aligned}$$

$$
\begin{aligned}
\underset{(78)}{=} \quad & -\sum_{k=1}^{x-1} \Lambda(k)(\tfrac{k}{x})^{\frac{1}{a}} \ln(\tfrac{x}{k}) \\
= \quad & -\sum_{k=1}^{x-1} \Lambda(k)\chi(k)(\tfrac{k}{x})^{\frac{1}{a}} \ln(\tfrac{x}{k}) \\
\underset{(79)}{=} \quad & \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+\frac{1}{a})^2}\, \tfrac{L'}{L}(s,\chi)\, ds \\
\underset{(6.23)}{=} \quad & \sum_{k=1}^{\infty} \frac{x^{\rho(L,k)}}{(\rho(L,k)+\frac{1}{a})^2} + \tfrac{L'}{L}(-\tfrac{1}{a},\chi)\frac{\ln(x)}{\sqrt[a]{x}} + \frac{1}{\sqrt[a]{x}}\left(\tfrac{L'}{L}\right)'(-\tfrac{1}{a},\chi) \\
& + \sum_{k=0}^{\infty} \frac{x^{-2k-\delta}}{(2k+\delta-\frac{1}{a})^2} \\
\underset{(6.29),(6.30)}{>} \quad & \sum_{k=1}^{\infty} \frac{x^{\rho(L,k)}}{(\rho(L,k)+\frac{1}{a})^2} + \sum_{k=0}^{\infty} \frac{x^{-2k-\delta}}{(2k+\delta-\frac{1}{a})^2} \\
& + \frac{\ln(x)}{\sqrt[a]{x}}\left(\tfrac{\zeta'}{\zeta}(\tfrac{1}{a}+1) + \frac{1}{\delta-\frac{1}{a}} - \ln(2) - (2a+1)\sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+\frac{1}{a}|^2}\right) \\
& - \frac{1}{\sqrt[a]{x}}\left(\frac{1}{(\delta-\frac{1}{a})^2} + \sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+\frac{1}{a}|^2} + \tfrac{5}{4}\right).
\end{aligned}
$$

Therefore, by Lemma 6.32, we have

$$
\begin{aligned}
& \frac{a^2}{(a+1)^2}\, x - \sum_{k=1}^{\infty}\frac{x^{\sigma}}{|\rho(L,k)+\frac{1}{a}|^2} - \sum_{k=1}^{\infty}\frac{x^{-2k}}{(2k-\frac{1}{a})^2} + \sum_{k=0}^{\infty}\frac{x^{-2k-\delta}}{(2k+\delta-\frac{1}{a})^2} \\
\underset{(6.32)}{\leq} \quad & \frac{x}{(\frac{1}{a}+1)^2} + \sum_{k=1}^{\infty}\frac{x^{\rho(L,k)}}{(\rho(L,k)+\frac{1}{a})^2} - \sum_{k=1}^{\infty}\frac{x^{-2k}}{(2k-\frac{1}{a})^2} + \sum_{k=0}^{\infty}\frac{x^{-2k-\delta}}{(2k+\delta-\frac{1}{a})^2} \\
\underset{(y\leq|y|)}{<} \quad & \left|\sum_{k=1}^{\infty}\frac{x^{\rho(\zeta,k)}}{(\rho(\zeta,k)+\frac{1}{a})^2}\right| + \frac{\ln(x)}{\sqrt[a]{x}}\cdot\tfrac{\zeta'}{\zeta}(-\tfrac{1}{a}) + \frac{1}{\sqrt[a]{x}}\cdot\left(\tfrac{\zeta'}{\zeta}\right)'(-\tfrac{1}{a}) \\
& - \frac{\ln(x)}{\sqrt[a]{x}}\left(\tfrac{\zeta'}{\zeta}(\tfrac{1}{a}+1) + \frac{1}{\delta-\frac{1}{a}} - \ln(2) - (2a+1)\sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+\frac{1}{a}|^2}\right) \\
& + \frac{1}{\sqrt[a]{x}}\left(\frac{1}{(\delta-\frac{1}{a})^2} + \sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+\frac{1}{a}|^2} + \tfrac{5}{4}\right)
\end{aligned}
$$

$$
\begin{aligned}
\leq \quad & \left| \sum_{k=1}^{\infty} \frac{x^{\rho(\zeta,k)}}{(\rho(\zeta,k)+\frac{1}{a})^2} \right| + \frac{\ln(x)}{\sqrt[a]{x}} \left(\tfrac{\zeta'}{\zeta}(-\tfrac{1}{a}) + \tfrac{\zeta'}{\zeta}(\tfrac{1}{a}+1) \right) \\
& - \frac{\ln(x)}{\sqrt[a]{x}} \left(\frac{a}{a\delta-1} - \ln(2) - (2a+1) \sum_{k=1}^{\infty} \frac{1}{|\rho(L,k)+\frac{1}{a}|^2} \right) \\
& + \frac{1}{\sqrt[a]{x}} \left(\left(\tfrac{\zeta'}{\zeta} \right)'(-\tfrac{1}{a}) + \frac{a^2}{(a\delta-1)^2} + \sum_{k=1}^{\infty} \frac{1}{|\rho(L,k)+\frac{1}{a}|^2} + \tfrac{5}{4} \right).
\end{aligned}
$$

Using Corollary 6.26, and Lemma 6.33, we can complete the proof of the assertion as follows

$$
\begin{aligned}
& \frac{a^2}{(a+1)^2}\, x \\
\underset{(6.26)}{<} \quad & \tfrac{\sqrt{x}}{21} + 18 \cdot 10^{-10} x + \sum_{k=1}^{\infty} \frac{1}{|\rho(L,k)+\frac{1}{a}|^2} \left(x^{\sigma} + \frac{(2a+1)\ln(x)+1}{\sqrt[a]{x}} \right) \\
& - \frac{\ln(x)}{\sqrt[a]{x}} \left(\tfrac{\zeta'}{\zeta}(-\tfrac{1}{a}) + \tfrac{\zeta'}{\zeta}(\tfrac{a+1}{a}) + \ln(2) - \frac{a}{a\delta-1} \right) \\
& + \frac{1}{\sqrt[a]{x}} \left(\left(\tfrac{\zeta'}{\zeta} \right)'(-\tfrac{1}{a}) - \frac{a^2}{(a\delta-1)^2} + \tfrac{5}{4} \right) + \sum_{k=1}^{\infty} \frac{x^{-2k}}{(2k-\frac{1}{a})^2} - \sum_{k=0}^{\infty} \frac{x^{-2k-\delta}}{(2k+\delta-\frac{1}{a})^2} \\
\underset{(6.33)}{<} \quad & \tfrac{\sqrt{x}}{21} + 18 \cdot 10^{-10} x \\
& + \tfrac{a}{2+a} \left(\ln(\tfrac{m}{\pi}) + 2 \cdot \tfrac{\zeta'}{\zeta}(\tfrac{a+1}{a}) - \tfrac{4\ln(x)}{x^{a+1}} + \tfrac{104(a+1)}{25\sqrt[a]{x}} + \tfrac{\Gamma'}{\Gamma}(\tfrac{a+1+a\delta}{2a}) \right) \left(x^{\sigma} + \tfrac{(2a+1)\ln(x)+1}{\sqrt[a]{x}} \right) \\
& + \frac{\ln(x)}{\sqrt[a]{x}} \left(\tfrac{\zeta'}{\zeta}(-\tfrac{1}{a}) + \tfrac{\zeta'}{\zeta}(\tfrac{a+1}{a}) + \ln(2) - \frac{a}{a\delta-1} \right) \\
& + \frac{1}{\sqrt[a]{x}} \left(\left(\tfrac{\zeta'}{\zeta} \right)'(-\tfrac{1}{a}) + \frac{a^2}{(a\delta-1)^2} + \tfrac{5}{4} \right) + \sum_{k=1}^{\infty} \frac{x^{-2k}}{(2k-\frac{1}{a})^2} - \sum_{k=0}^{\infty} \frac{x^{-2k-\delta}}{(2k+\delta-\frac{1}{a})^2} \\
\underset{(93)}{<} \quad & \tfrac{a}{2+a}(\ln(m)+t(x))(x^{\sigma}+r(x)) + s(x). \quad \square
\end{aligned}
$$

9. The Least Quadratic Non-Residue

THEOREM 6.35 (ERH). *Assume the Extended Riemann Hypothesis is correct. Let m be an odd positive integer greater than 1 such that m is not a perfect square, and*

$$x = \min\{k \in \mathbb{N}_{>0} \mid \left(\tfrac{k}{m}\right) \neq 1\}.$$

Then

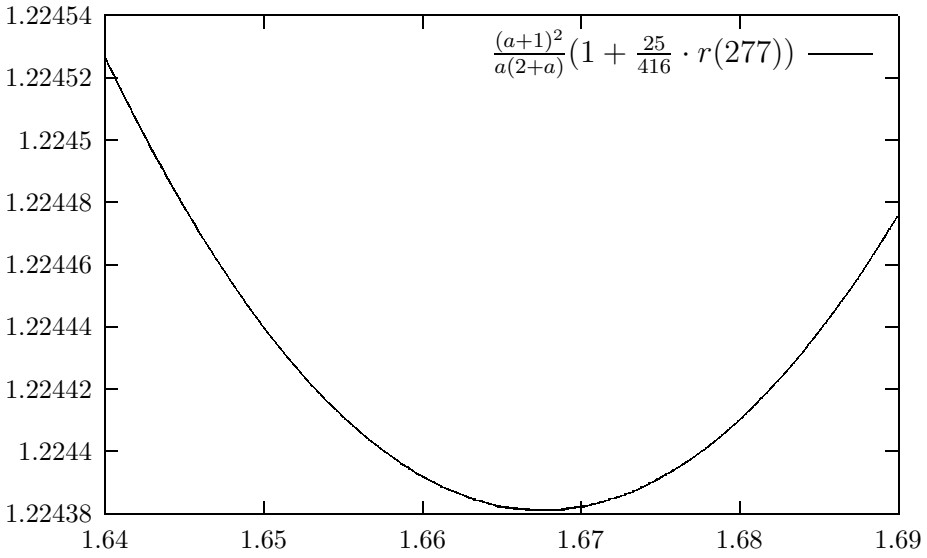
$$x < \tfrac{3}{2}\ln(m)^2 - \tfrac{44}{5}\ln(m) + 13.$$

PROOF. First, we define the following three functions

$$r(x) \;:=\; \tfrac{(2a+1)\ln(x)+1}{\sqrt[a]{x}},$$

$$\begin{aligned} s(x) &:= \tfrac{\ln(x)}{\sqrt[a]{x}}\left(\tfrac{\zeta'}{\zeta}(-\tfrac{1}{a})+\tfrac{\zeta'}{\zeta}(\tfrac{a+1}{a})+\ln(2)-\tfrac{a}{a\delta-1}\right) \\ &\quad + \tfrac{1}{\sqrt[a]{x}}\left(\left(\tfrac{\zeta'}{\zeta}\right)'(-\tfrac{1}{a})+\tfrac{a^2}{(a\delta-1)^2}+\tfrac{5}{4}\right) \\ &\quad + \tfrac{\sqrt{x}}{21}+18\cdot 10^{-10}x+\begin{cases} -a^2, & \text{if } \delta=0 \\ \frac{4}{9x^2}-\ln(1+\frac{1}{x}), & \text{if } \delta=1, \end{cases} \\ \text{and}\quad t(x) &:= 2\cdot\tfrac{\zeta'}{\zeta}(\tfrac{a+1}{a})-\tfrac{4\ln(x)}{x^{a+1}}+\tfrac{104(a+1)}{25\sqrt[a]{x}}+\tfrac{\Gamma'}{\Gamma}(\tfrac{a+1+a\delta}{2a})-\ln(\pi). \end{aligned}$$

By the table of pseudosquares (Appendix A), we can assume that $m > 6\cdot 10^{19}$ and $x > 277$. We consider the following diagram to decide a value for a:



Let $a = \frac{167}{100}$. Then we have the following three estimates

$$\begin{aligned} r(x) &< 0.876, \\ s(x) &< \max\{\tfrac{\ln(x)}{x^{1.67}}(1.757-1.189+0.7+1.67)+\tfrac{1}{x^{1.67}}(-0.27+2.79+\tfrac{5}{4})+\tfrac{\sqrt{x}}{21} \\ &\qquad + 18\cdot 10^{-10}x-2.788, \\ &\qquad \tfrac{\ln(x)}{x^{1.67}}(1.757-1.189+0.7-2.49)+\tfrac{1}{x^{1.67}}(-0.27+6.22+\tfrac{5}{4})+\tfrac{\sqrt{x}}{21} \\ &\qquad + 18\cdot 10^{-10}x+0.01\} \\ &< \tfrac{\sqrt{x}}{21}+18\cdot 10^{-10}x, \\ t(x) &< -2.378+0.383-0.169-1.1447<-3.3. \end{aligned}$$

Assume the Extended Riemann Hypothesis is correct. Then, by Lemma 6.34, we get

$$\begin{aligned} \tfrac{27889}{71289}\,x &= \tfrac{a^2}{(a+1)^2}\,x \\ &\underset{(6.34)}{<} \tfrac{a}{2+a}(\ln(m)+t(x))(x^{\sigma}+r(x))+s(x) \\ &\underset{(ERH)}{<} \tfrac{167}{367}(\ln(m)-3.3)(\sqrt{x}+0.876)+\tfrac{\sqrt{x}}{21}+18\cdot 10^{-10}x \end{aligned}$$

$$< \quad \tfrac{167}{367}\sqrt{x}\ln(m) + 0.3987\ln(m) - 1.45\sqrt{x} + 18\cdot 10^{-10}x - 1.31.$$

Therefore,

$$\begin{aligned}\sqrt{x}(1-47\cdot 10^{-10}) &< \tfrac{71289}{61289}\ln(m) + \tfrac{1.0192}{\sqrt{x}}\ln(m) - 3.7 - \tfrac{3.34}{\sqrt{x}} \\ &\underset{(\sqrt{x}>\frac{416}{25})}{<} \tfrac{306103}{250000}\ln(m) - \tfrac{37}{10}.\end{aligned}$$

Thus, we get

$$x < \tfrac{3}{2}\ln(m)^2 - \tfrac{44}{5}\ln(m) + 13. \quad \square$$

10. Necessity of the Extended Riemann Hypothesis

Our intention in this chapter was to use all empirical information about the Extended Riemann Hypothesis, with regard to Miller's primality test. We have seen that only Lemma 6.29, and Lemma 6.33 require the Extended Riemann Hypothesis. However, we can replace these lemmata by the following weaker estimates.

LEMMA 6.36. *Let m be a natural number greater than 1, $a \in]0,1[$, χ a quadratic character modulo m, and $\delta = \begin{cases} 0\,, & \text{if } \chi(-1)=1 \\ 1\,, & \text{if } \chi(-1)=-1 \end{cases}$. Then*

$$\tfrac{L'}{L}(-a,\chi) > \tfrac{\zeta'}{\zeta}(a+2) + \frac{1}{\delta - a} - 2a\ln(2) - 2(a+1)\sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+a|^2}.$$

PROOF. The proof of this lemma is analogous to the proof of Lemma 6.29 using $\frac{L'}{L}(a+2,\chi)$ instead of $\frac{L'}{L}(a+1,\chi)$. $\square$

LEMMA 6.37. *Let x, and $m \geq 2$ be positive integers, $a \in]0,1[$, χ a primitive real character modulo m with $\chi(k) = 1$ for $k \in \{l \in \mathbb{N} \mid 1 \leq l < x\}$, $\chi(x) \neq 1$, and let $\delta = \begin{cases} 0\,, & \text{if } \chi(-1)=1 \\ 1\,, & \text{if } \chi(-1)=-1 \end{cases}$. Then*

$$\sum_{k=1}^{\infty}\frac{1}{|\rho(L,k)+a|^2} < \ln(\tfrac{m}{\pi}) + 2\cdot\tfrac{\zeta'}{\zeta}(a+1) - \tfrac{4\ln(x)}{x^{a+1}} + \tfrac{104(a+1)}{25a\cdot x^a} + \tfrac{\Gamma'}{\Gamma}(\tfrac{a+1+\delta}{2}).$$

PROOF. The proof of this lemma is analogous to the proof of Lemma 6.33 using the estimate

$$\begin{aligned}&\sum_{k=1}^{\infty}\frac{1}{|a+\rho(L,k)|^2} \\ =\ &\sum_{k=1}^{\infty}\frac{1}{(a+\sigma(L,k))^2 + t(L,k)^2} \\ <\ &\sum_{k=1}^{\infty}\frac{1}{(a+1-\sigma(L,k))^2 + t(L,k)^2} \\ =\ &\sum_{k=1}^{\infty}\frac{1}{2(a+1-\sigma(L,k))}\left(\frac{1}{a+1-\sigma(L,k)-it(L,k)} + \frac{1}{a+1-\sigma(L,k)+it(L,k)}\right).\end{aligned}$$

□

And with these two lemmata it is also possible and easy to replace the key Lemma 6.34 by the following lemma, which does not require the validity of the Extended Riemann Hypothesis.

LEMMA 6.38. *Let x, and $m \geq 2$ be positive integers, $a \geq 2$ be a real number, χ a quadratic character modulo m with $\chi(k) = 1$ for $k \in \{l \in \mathbb{N} \mid 1 \leq l < x\}$, and let* $\delta = \begin{cases} 0\,, & \text{if } \chi(-1) = 1 \\ 1\,, & \text{if } \chi(-1) = -1 \end{cases}$. *Let σ be a real number such that $\mathrm{Re}(\rho(L,k)) \leq \sigma$ for all positive integers k. Then*

$$\tfrac{a^2}{(a+1)^2}\, x < (\ln(m) + t(x))(x^\sigma + r(x)) + s(x)$$

with the same definitions as in Lemma 6.34.

PROOF. The proof of this lemma is analogous to the proof of Lemma 6.34 using Lemma 6.36 instead of Lemma 6.29, and using Lemma 6.37 instead of Lemma 6.33. □

Hence, Theorem 6.35 is the only one where the Extended Riemann Hypothesis is required for Miller's test. Thus, the result of this chapter is – beside the improvement of the constant $\frac{3}{2}$ for the upper bound for the least quadratic non-residue – that we need the Extended Riemann Hypothesis only in the last step of the proof instead generally in the whole one.

Last, if we want to formulate Theorem 6.35 without the Extended Riemann Hypothesis, we can do it in the following way:

We will consider the real number σ of Lemma 6.38. By Definition 6.4, σ is less than 1. However, let σ equal to 1, then the estimate in Lemma 6.38 is always true and we cannot derive an estimate for the modulus m. The sharpest known estimate for σ is given by A. A. Karatsuba and S. M. Voronin in [**64**]:

$$\sigma \leq 1 - \tfrac{C}{\log(T)}$$

for a suitable constant C and $T \to \infty$. But this estimate is not useful, if also the modulus m is very large.

Finally, we can say that a sharp estimate of the real number σ of Lemma 6.38, for example using empirical results, gives a good estimate for the least quadratic non-residue, so that a fast Miller test (Theorem 6.7) will be the result.

THEOREM 6.39. *If there exists a constant C such that $\sigma \leq 1 - C$, then Miller's primality test can be performed in deterministic polynomial running time by testing $O(\ln(n)^{\frac{1}{C}})$ bases.*

PROOF. This can be concluded from Lemma 6.37. □

11. Discussion

Do we have a similar improvement for other than quadratic characters?

The proof uses the properties of quadratic characters, e.g. in Lemma 6.32. Therefore, it is not possible to transfer this result for other characters. It may be possible to formulate this proof without that restriction, but that is not the subject of this thesis.

Can be the estimate of Theorem 6.35 further improved?

Using the table of pseudosquares (Appendix A) for a comparison of Theorem 6.35 with empirical results, we can see that the least quadratic non-residue modulo m is for large m not much greater than $\frac{1}{7}\ln(m)^2$. Moreover, if we are only interested in Miller's test, we can see by Chapter 3.2 ([**104**], [**62**]) that the bound is not much greater than $\frac{1}{65}\ln(m)^2$. Now we recapitulate the proof and consider every estimate which could be the reason for the factor between the estimate of Theorem 6.35 and empirical results. It is easy to see that Corollary 6.26, Lemma 6.29, and Lemma 6.30 cannot be the reasons. The difference to empirical results in Lemma 6.31 is a little bit larger and so it grows in Lemma 6.33. But we have seen in the proof of Lemma 6.34 that this difference changes only the addition part 13 in the proof of Theorem 6.35 and this plays definitely a minor role in the estimate. Thus, Lemma 6.32 remains, and this affects the factor in front of $\ln(m)^2$. If we know more about the position of the non-trivial roots of the L-function, then we can choose $d > 0$ in Lemma 6.32 to achieve a better approximation. But we cannot suppose in general for example that all non-trivial roots have an absolute value of the imaginary part that is greater than 1. On the other hand, we nearly have a factor 10 between empirical results of the least quadratic non-residue and Miller's test. In Theorem 6.7, we have obtained a factor of $\frac{r^2}{4}$ where r is the number of prime divisors of n, and this factor is at least 1. Thus, the difference between the prime divisors cannot be too large, at least if $r = 2$, because the estimate in the proof of Theorem 6.7 can be constructed using the largest prime divisor of n, if r is even.

Does there exist another way to prove the correctness of Miller's test without using the Extended Riemann Hypothesis?

For example, we can find two bases $a_1, a_2 \in (\mathbb{Z}/n\mathbb{Z})^*$ such that

$$a_1^{\frac{n-1}{2}} \equiv a_2^{\frac{n-1}{2}} \equiv -1 \pmod{n},\ a_1 \not\equiv a_2 \pmod{n} \quad \text{and} \quad \left(\tfrac{a_1}{p}\right) = -\left(\tfrac{a_2}{p}\right) = -1$$

for a prime divisor p of the composite number n. Then it is easy to see by Lemma 5.7 that Algorithm 3.11 returns for these two bases the result false. But a strategy without using the least quadratic non-residue, appears hopeless.

APPENDIX A

Pseudosquares

DEFINITION A.1. Let p be a prime number. We denote by M_p the smallest number such that the Jacobi symbol over p is always equal to 1 for all prime numbers less than or equal to p

$$M_p := \min\{m \in \mathbb{N} \mid \left(\tfrac{q}{m}\right) = 1 \quad \text{for all } 2 \leq q \leq p\}.$$

In the literature, this definition is split in the definition of pseudosquares and negative pseudosquares if $M_p \equiv 1 \pmod 8$ or $M_p \equiv -1 \pmod 8$, respectively, see [**75**]. Thus, the pseudosquares behave locally like a perfect square modulo all primes less than or equal to p, but are nevertheless not a perfect square.

$p \in \mathbb{P}$	M_p	$\lfloor \frac{10^4}{\Delta(p)} \ln(M_p)^2 \rfloor / 10^4$	Source
2	7	1.2621	[**75**] (1970)
3	23	1.9662	
5	71	2.5957	
7	311	2.9950	
11	479	2.9299	
13	1 559	3.1793	
17	5 771	3.9381	
19	10 559	3.7319	
23	18 191	3.3175	
29	31 391	3.4584	
31	118 271	3.6875	
37,41	366 791	3.8177	
43,47,53	2 155 919	3.6048	
59,61	6 077 111	3.6415	
67	98 538 359	4.7715	
71	120 293 879	4.7419	
73,79	131 486 759	4.2106	
83	508 095 719	4.5151	
89,97,101, 103,107,109	2 570 169 839	4.1545	
113,127	196 265 095 099	5.1613	
131	513 928 659 191	5.3075	
137	844 276 851 239	5.4255	[**122**] (1989)
139	1 043 702 750 999	5.1398	
149	4 306 732 833 311	5.6046	
151	8 402 847 753 431	5.6409	
157	47 375 970 146 951	6.0832	
163	52 717 232 543 951	5.9778	
167	100 535 431 791 791	6.0087	
173,179	178 936 222 537 081	5.9504	
181,191	493 092 541 684 679	5.9304	
193,197, 199,211	1 088 144 332 169 831	5.3756	
223	11 641 399 247 947 921	6.0286	
227	88 163 809 868 323 439	6.6480	[**25**] (1991)
229	196 640 248 121 928 601	6.8053	[**80**] (1991)
233	423 414 931 359 807 911	6.8925	[**80**] (1994)
239	695 681 268 077 667 119	7.0036	
241,251	1 116 971 853 972 029 831	6.7198	
257,263,269	3 546 374 752 298 322 551	6.7319	
271	10 198 100 582 046 287 689	6.9158	
277	69 848 288 320 900 186 969	7.4300	[**138**] (1998)

where

$$\Delta : \mathbb{P} \to \mathbb{P} : p \mapsto \min\{q \in \mathbb{P} \mid q > p\}.$$

APPENDIX B

Counter-Examples for Algorithm 5.2

DEFINITION B.1. Let n be a natural number. We denote by $K(n)$ the set of bases a for which n is a *commutator pseudoprime*

$$K(n) := \{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid (x^2+4)^{\frac{n-1}{2}} \equiv -1 \pmod{n},\ c(1,x)^{\frac{n+1}{2}} \equiv -I_2 \pmod{n}\}.$$

Furthermore, in the following tables[1] we will list only the smallest set $K'(n) \subset K(n)$ such that $K(n) = \{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid \pm a \in K'(n)\}$. Additionally, we will consider the set

$$K''(n) = \{a \in K'(n) \mid (a^2+2)^{n-1} \equiv 1 \pmod{n}\}.$$

REMARK B.2. All computations till $n = 12\ 671\ 501$ are complete. Additionally, all ordinary pseudoprimes for the base 2 (see [**99**]) less than 2 449 977 757 are tested.

n	$K''(n)$
3281	$\{81, 1432\}$
432821	$\{195212, 203820\}$
973241	$\{7897, 37136, 83997, 195862, 208393, 367119, 396358, 484989\}$
1551941	$\{203808, 767873\}$
2202257	$\{1484, 1089900\}$
2545181	$\{177437, 823394\}$
3020093	$\{1326902, 1392871\}$
3028133	$\{495849, 540877\}$
4561481	$\{475513, 1458782\}$
4923521	$\{1362920, 1577988\}$
5173601	$\{310891, 1658589\}$
5193161	$\{322254, 2024833\}$
5774801	$\{57724, 2433649\}$
6710177	$\{1433138, 3048903\}$
9846401	$\{188300, 1301717\}$
11107121	$\{889347, 3770584\}$
16070429	$\{5490182, 7463399\}$
46256489	$\{3885213, 5151145\}$
54029741	$\{16143305, 23669724\}$
76923461	$\{3856373, 30040645\}$
102690677	$\{202926, 27699608\}$
198982759	$\{9895300, 20168848, 45562611, 51768481, 61692219, 75626759, 81832629, 91756367\}$
242131889	$\{30673676, 93384139\}$
390612221	$\{181985494, 183405638\}$
545220869	$\{93330047, 188574250\}$
717653129	$\{21996305, 356154466\}$
741470549	$\{83047998, 254905701\}$

[1]The computations have been done by using the arithmetic of [**130**]; the program is only a few hundred lines long.

n	$K''(n)$
921858631	{6492010, 22514888, 114349119, 143356017, 273186613, 390966882, 394027742, 410050620}
1536112001	{703276597, 728044855}
1860373241	{169168150, 266845273}

n	$K'(n)$
3281	{81, 1432}
5983	{395, 1728}
27403	{1560, 4575, 11376, 13012}
41369	{7740, 8749, 10422, 10767, 11431, 11776}
43289	{8118, 13455, 15234, 20571}
47783	{1381, 4073, 11476, 14168}
60551	{18380, 22390}
70531	{12885, 16901}
100127	{37443, 43729}
137461	{7233, 7738, 24926, 25431}
161027	{9513, 56491}
231703	{49472, 109380}
334109	{53205, 85047, 94231, 101626}
345421	{6701, 34496}
369271	{11493, 16694, 88812, 94013, 116999, 122200, 141565, 146766}
430127	{12751, 144669}
432821	{195212, 203820}
476971	{83999, 122064, 132806, 138102}
501227	{25796, 41533, 48239, 56495, 86419, 115568, 116343, 130530, 160454, 190378, 191153, 198634, 228558, 236039}
509233	{70641, 72754}
528019	{35507, 159434}
624293	{227805, 237312}
626459	{81971, 114630, 125859, 158518, 227452, 271340}
635627	{14150, 42300}
754291	{321046, 355306}
824261	{263243, 271404, 283544, 291705, 344853, 353014, 365154, 369336, 373315, 377497, 389637, 397798}
851927	{169897, 401600}
864499	{79229, 190998}
877099	{10637, 95072, 343631, 427759}
879829	{15829, 368769}
893173	{102099, 444045}
913891	{112615, 136628, 271164, 393484}
973241	{7897, 37136, 83997, 195862, 208393, 367119, 396358, 484989}
1054747	{26461, 207201, 292416, 526078}
1056551	{17173, 30113, 61761, 76050, 107698, 109047, 167924, 199572, 200921, 212512, 213861, 245509, 246858, 304386, 305735, 337383, 338732, 384669, 396260, 397609, 429257, 442197, 476543, 522480}
1102121	{46970, 60554, 73851, 100732, 114316, 127613, 141197, 181375, 208256, 248721, 302483, 342661, 369542, 410007, 423304, 436888, 450185, 477066, 490650, 503947}
1102759	{23080, 33263, 50634, 60817, 96720, 106903, 124274, 134457, 180617, 190800, 218354, 254257, 264440, 291994, 348337, 421977}
1106327	{56073, 289375}
1209911	{121561, 185177}
1250731	{268115, 613183}
1253311	{142843, 431093}
1300399	{366530, 395210}

n	$K'(n)$
1302451	{22422, 255084}
1325843	{113206, 540983}
1388903	{84714, 533599}
1397419	{89358, 131072}
1441091	{120932, 253828, 427264, 493712, 572619, 639067}
1447513	{385266, 566724}
1474511	{67941, 171463, 193084, 296606}
1507963	{516751, 567243}
1509709	{90497, 126839, 483891, 701227}
1530787	{449682, 606289}
1551941	{203808, 767873}
1643533	{113061, 672867}
1697183	{632566, 773293}
1708901	{238830, 268868}
1728619	{471115, 605281}
1729331	{94333, 108455, 115962, 318750, 485590, 688378, 710007, 816536}
1766927	{182685, 485798}
1803013	{324888, 459239}
1840409	{291896, 440215}
1860839	{3085, 337632, 521095, 579683, 756976, 920400}
1893943	{158251, 271032, 409543, 522324}
1895791	{30793, 919380}
1897811	{146808, 193437, 601731, 941976}
1907851	{55129, 355325, 638635, 858762}
1911059	{35202, 293190, 514107, 842499}
2004403	{485873, 963565}
2085245	{64107, 115838, 117032, 162412, 186163, 197478, 254637, 300017, 335083, 352942, 366108, 381193, 388008, 419033, 532887, 556638, 561138, 567953, 603212, 614063, 614527, 751668, 752132, 783157, 798242, 805057, 836082, 916528, 973687, 978187, 985002, 1031112}
2149519	{147021, 176306, 239541, 321539, 380109, 562868, 644866, 703436}
2164427	{74383, 419981}
2172059	{84780, 117272, 236319, 268811, 387858, 420350, 571889, 773941, 925480, 1077019}
2176217	{310929, 335991, 336506, 386115, 411177, 1058612}
2202257	{1484, 1089900}
2236387	{544733, 908796}
2236811	{86098, 253134, 412149, 658552, 751381, 912976}
2263127	{191723, 402494}
2435423	{4935, 223458}
2545181	{177437, 823394}
2589949	{6598, 30359, 64685, 77881, 88446, 101642, 135968, 149164, 172925, 207251, 231012, 244208, 267969, 315491, 326056, 349817, 373578, 386774, 397339, 410535, 444861, 492383, 505579, 529340, 553101, 563666, 576862, 624384, 671906, 682471, 729993, 743189, 825037, 848798, 861994, 872559, 909516, 920081, 991364, 1004560, 1015125, 1028321, 1038886, 1052082, 1062647, 1099604, 1133930, 1157691, 1170887, 1194648, 1218409, 1242170, 1252735, 1276496}
2687719	{254173, 357689, 435326, 481724, 585240, 662877, 886360, 963997, 1067513, 1113911, 1191548, 1295064}
2740561	{624247, 1146158}
2799653	{171623, 396567, 408713, 441507, 478188, 858115, 870261, 1009697, 1021843, 1091318, 1316262, 1328408}
2895017	{293105, 1441015}

n	$K'(n)$
2944369	{94176, 137861, 316463, 377622, 604784, 630995, 714503, 858157, 919316, 994087, 1329955, 1373640}
3011479	{1098655, 1159246}
3020093	{1326902, 1392871}
3028133	{495849, 540877}
3090091	{333170, 1505474}
3116107	{49490, 148302}
3132949	{449913, 956110, 1123402, 1503350}
3175883	{574185, 1228541}
3307079	{124873, 169041, 1476217, 1520385}
3337849	{1069986, 1184240, 1518841, 1633095}
3387547	{492001, 788568}
3391249	{245162, 1626533}
3399527	{1521853, 1610559}
3422959	{246109, 253502, 264008, 719261, 726654, 1121596, 1236771, 1328600}
3452147	{373762, 1655183}
3538417	{1216954, 1304777}
3546629	{865666, 1180901}
3574999	{199497, 421317}
3767233	{1184690, 1472613}
3866257	{98695, 232630, 276225, 339876, 410160, 455855, 473811, 517406, 571932, 633385, 651341, 697036, 749462, 813113, 874566, 990643}
3871979	{134265, 244616, 393013, 568592, 827340, 928450, 1206221, 1890055}
3884165	{60602, 186413, 1367253, 1614268}
3999137	{1075879, 1109866, 1303211, 1337198, 1404420, 1631752}
4060519	{1050951, 1060346}
4095439	{169652, 480698, 584380, 895426, 1128159, 1439205, 1542887, 1853933}
4109363	{856991, 1215082}
4109741	{993438, 1504620}
4216601	{14100, 22094, 50294, 64713, 80063, 86488, 104585, 209489, 224839, 279130, 347840, 376040, 384034, 474519, 480944, 496294, 499041, 520816, 535235, 550585, 565004, 571429, 607623, 665592, 695361, 810368, 836459, 840137, 864659, 926944, 933369, 963138, 969563, 984913, 1060048, 1081823, 1089817, 1107914, 1136114, 1150533, 1162205, 1180302, 1256368, 1274465, 1280890, 1306981, 1310659, 1343175, 1346853, 1383047, 1421988, 1425666, 1433660, 1512473, 1548667, 1570442, 1675346, 1693443, 1705115, 1708793, 1744987, 1747734, 1765831, 1795600, 1835472, 1841897, 1859994, 1886085, 1892510, 1896188, 1922279, 1925957, 1928704, 1932382, 1968576, 2019189}
4366459	{633977, 1485969, 1544136, 1970331}
4403027	{886570, 1409114}
4561481	{475513, 1458782}
4593653	{135385, 539574, 1529077, 2204036}
4615207	{1257937, 1510249, 2169301, 2193594}
4839217	{1279361, 1941480}
4870847	{681995, 1860498}
4923521	{1362920, 1577988}
5073799	{364256, 1341733, 1352775, 2015035}
5141239	{626140, 683424, 791639, 848923, 855276, 955523, 984165, 1020775, 1121022, 1149664, 1743178, 1757499, 1908677, 1922998, 2172808, 2258734, 2338307, 2373302, 2424233, 2538801}

n	$K'(n)$
5142569	{35876, 73413, 76735, 226883, 264420, 301957, 336172, 373709, 377031, 414568, 448783, 452105, 486320, 489642, 523857, 527179, 598931, 602253, 677327, 711542, 749079, 752401, 789938, 827475, 861690, 865012, 899227, 902549, 936764, 977623, 1015160, 1049375, 1052697, 1124449, 1161986, 1202845, 1315456, 1352993, 1387208, 1499819, 1537356, 1612430, 1615752, 1649967, 1653289, 1687504, 1728363, 1762578, 1765900, 1803437, 1837652, 1878511, 1991122, 2025337, 2028659, 2100411, 2141270, 2175485, 2178807, 2213022, 2216344, 2250559, 2325633, 2328955, 2363170, 2404029, 2441566, 2475781}
5173601	{310891, 1658589}
5188709	{51721, 127200, 485042, 663963, 946326, 1021805, 1200726, 1304168, 1558568, 1662010, 1737489, 2019852, 2095331, 2274252}
5193161	{322254, 2024833}
5256091	{304340, 2301022}
5340581	{536124, 2388153}
5344373	{834195, 939534, 1379066, 2191578}
5639129	{13073, 50288, 76434, 139795, 203156, 240371, 266517, 303732, 393239, 430454, 456600, 557176, 583322, 683898, 747259, 773405, 836766, 1064064, 1153571, 1190786, 1254147, 1280293, 1317508, 1380869, 1507591, 1787181, 1824396, 1887757, 1913903, 2014479, 2141201, 2230708, 2267923, 2294069, 2331284, 2484152, 2521367, 2584728, 2610874, 2648089, 2674235, 2711450, 2774811, 2800957}
5730859	{156980, 583949, 765401, 1022458, 1260813, 1608596, 1838992, 2096049, 2277501, 2712429}
5754739	{31614, 356248, 637376, 687456, 811659, 859634, 962010, 1142867, 1149441, 1293218, 1417421, 1465396, 1748629, 1755203, 1894659, 2136491, 2184466, 2500421, 2742253, 2790228}
5774801	{57724, 2433649}
5828549	{1956745, 2226293, 2660544, 2898457}
5888251	{1202969, 1462946}
5919187	{1837345, 2127142}
5934499	{1227901, 1514765}
5942627	{563152, 799203}
5989213	{366963, 980193, 1206994, 1820224, 1920479, 2760510}
6003923	{1992859, 2688614}
6060647	{228026, 746133, 938917, 1457024, 1651618, 2109480, 2133578, 2145627, 2229970, 2242019, 2266117, 2723979}
6063991	{74215, 120329, 143386, 189500, 327842, 443127, 479153, 525267, 604526, 617495, 801951, 950381, 1032521, 1101692, 1193920, 1204008, 1216977, 1227065, 1240034, 1273179, 1447547, 1549863, 1585889, 1595977, 1619034, 1655060, 1793402, 1872661, 2000915, 2023972, 2047029, 2139257, 2208428, 2218516, 2379915, 2438998, 2495200, 2623454, 2633542, 2679656, 2702713, 2715682, 2748827, 2761796}
6209113	{182314, 2268075}
6385861	{1490990, 2408296, 2584701, 2601606, 2690544, 2866949}
6537529	{184802, 639460, 1825245, 2279903}
6548309	{51132, 72421, 195974, 319527, 566633, 668897, 690186, 813739, 916003, 937292, 1039556, 1163109, 1410215, 1533768, 1555057, 1657321, 1780874, 1802163, 1925716, 2049269, 2151533, 2296375, 2419928, 2543481, 2667034, 3037693}
6577771	{832713, 1524448}
6591551	{1424075, 2374047}
6698249	{345437, 521321, 1838456, 2014340}
6710177	{1433138, 3048903}

n	$K'(n)$
6776909	{118843, 644952, 2178326, 2704435}
6871633	{1416867, 1719563}
6897089	{149742, 649030}
6967199	{2186113, 3463476}
7037869	{105102, 1260843, 1429960, 1640164, 3006109, 3175226}
7099861	{1130508, 1610870, 2069969, 2550331}
7166039	{466457, 1849938}
7207261	{909390, 1401266}
7214033	{30445, 94286, 97237, 161078, 288760, 349650, 352601, 416442, 477332, 480283, 541173, 544124, 605014, 668855, 732696, 735647, 860378, 924219, 927170, 988060, 991011, 1051901, 1115742, 1182534, 1243424, 1246375, 1437898, 1498788, 1562629, 1690311, 1693262, 1754152, 1757103, 1820944, 1881834, 1945675, 2009516, 2073357, 2076308, 2137198, 2140149, 2203990, 2328721, 2520244, 2584085, 2714718, 2775608, 2839449, 2906241, 3030972, 3286336, 3350177, 3414018, 3416969, 3480810, 3544651}
7227599	{30063, 484034, 604998, 1149336, 1270300, 1814638, 1935602, 2449699}
7361351	{1659616, 2800107}
7433243	{520397, 2864447}
7537771	{23555, 539168, 565717, 846937, 1081330, 1362550, 1559257, 1951822, 2467435, 2664142, 2945362, 3487524}
7612721	{732364, 1989551}
7739629	{86426, 135723, 160059, 185020, 209356, 234317, 258653, 283614, 307950, 332911, 357247, 406544, 431505, 505138, 530099, 603732, 677990, 751623, 776584, 825881, 850217, 875178, 899514, 948811, 1170960, 1244593, 1368148, 1417445, 1441781, 1491078, 1516039, 1565336, 1589672, 1638969, 1762524, 1836157, 1861118, 1910415, 1934751, 1984048, 2156900, 2206197, 2230533, 2279830, 2304791, 2354088, 2378424, 2403385, 2427721, 2477018, 2699167, 2772800, 2797761, 2871394, 2994949, 3044246, 3068582, 3093543, 3117879, 3142840, 3167176, 3216473, 3290731, 3340028, 3364364, 3389325, 3413661, 3462958, 3487919, 3561552, 3586513, 3635810, 3660146, 3709443, 3734404, 3783701, 3808037, 3857334}
7743539	{718770, 792694, 811175, 1110849, 1905532, 3735151, 3809075, 3827556}
7827203	{1091834, 3278717}
7883731	{1196010, 2050804}
8286151	{594619, 3284997}
8510347	{49660, 188265, 259648, 398253, 627424, 837412, 849192, 932355, 1059180, 1075337, 1142343, 1237286, 1285325, 1297105, 1375891, 1380268, 1447274, 1507093, 1585879, 1590256, 1685199, 1823804, 1895187, 2033792}
8518127	{199875, 3688880}
8683849	{280640, 1077566, 1768887, 2043418, 2274602, 2565813, 2840344, 3071528}
8759599	{209333, 899477, 3535763, 4225907}
8881361	{169231, 310365, 734501, 875635, 902772, 1043906, 1256934, 1398068, 1779367, 1920501, 1947638, 2088772, 2470071, 2611205, 2613125, 2754259, 2824233, 2965367, 2992504, 3133638, 3346666, 3487800, 3657991, 3799125, 3826262, 3869099, 3967396, 4010233, 4037370, 4178504, 4180424, 4321558}
8896271	{214795, 256077, 276718, 404435, 445717, 466358, 535908, 785116, 845523, 969369, 1299625, 1464753, 1535819, 1650522, 1691804, 1725459, 2001419, 2044217, 2063342, 2064858, 2106140, 2372957, 2414239, 2600008, 2725370, 2765136, 2766652, 2787293, 2856843, 3046483, 3095392, 3166458, 3219238, 3290304, 3356098, 3479944, 3528853, 3620560, 3785688, 3810200, 3971457, 3975328, 4012739, 4046394, 4161097, 4202379, 4322354, 4384277}
8944981	{1203900, 1590859, 1606906, 1993865, 2474245, 2861204}
8993239	{107813, 1114569, 2598890, 3821272}

n	$K'(n)$
9033781	{437229, 584599, 1375422, 1552266, 3364917, 3512287}
9348709	{512341, 4180387}
9366751	{1045693, 3673690}
9371251	{1611977, 2189164}
9693949	{787781, 4483727}
9713027	{673425, 2710383}
9752227	{1916244, 2045953, 2722307, 2852016, 2926661, 3056370}
9846401	{188300, 1301717}
9880751	{680679, 2202747, 3347584, 3649741}
9980983	{202232, 243419, 2035595, 2481246, 4465628, 4726479, 4808853, 4911279}
10054043	{1226604, 2863906}
10137509	{253903, 1048223, 3737555, 4531875}
10610063	{1129452, 4207318}
10621799	{643542, 2006153, 2416578, 2574190, 3936801, 4347226}
10727261	{3451203, 4051982}
10824919	{316961, 321899, 704035, 708973, 837444, 1224518, 1229456, 1863378, 2250452, 2255390, 2383861, 2770935, 3409795, 3796869, 4317352, 5343286}
10829647	{1511635, 4054167}
10931029	{294167, 983229, 1296439, 1985501}
10961017	{81725, 2628842, 2909034, 5456151}
11107121	{889347, 3770584}
11150939	{1189488, 1771687, 2340116, 5301291}
11293981	{1741695, 4484891}
11012021	{231108, 5002291}
11081459	{2830024, 2832748, 2878841, 2881565, 5368508, 5371232}
11541307	{680180, 4387398}
11559211	{36549, 1383634, 1744364, 2157835, 2858938, 2912869, 3091449, 3504920, 4206023, 4259954, 4386983, 4530799, 5681327, 5734068}
11637583	{2211694, 3777569}
11703119	{4588913, 5121209}
11797127	{1387489, 4339164}
12042727	{1168724, 5632350}
12123113	{1045817, 2915804}
12263131	{113661, 552170, 1912553, 2578384, 2955902, 3621733}
12411827	{111343, 263502, 345134, 584241, 1105929, 1806829, 1915514, 2698046, 2741520, 2893679, 2937153, 3170944, 3192681, 3583947, 3605684, 3719685, 3828370, 5371697, 5523856, 5670699, 5980333, 6192387}
12511589	{403642, 1431824, 2268523, 3666834, 4103989, 4337124, 5502300, 6172590}
12580409	{81056, 3376882, 3497461, 4180742, 4301321, 4983262}
13057787	{396142, 619830, 1197635, 3611657, 3835345, 5429122}
13338371	{4972804, 6005969}
14970499	{2400614, 3092727, 3210641, 3902754}
15976747	{2349318, 4192645}
16070429	{5490182, 7463399}
17134043	{4719826, 6297345}
18740971	{957041, 3816949}
19404139	{2764236, 5398413}
20261251	{463279, 8852756}
21623659	{1171693, 1784594}
22075579	{4396943, 8604625}
24214051	{262144, 5338971}
30894307	{8340098, 15395384}
31166803	{11765444, 12666383}
31436123	{7461514, 8441009, 8859538, 9839033, 13830290, 14809785}

n	$K'(n)$
37109467	{145311, 2828162}
38010307	{13000875, 13457159}
38118763	{2072878, 3113712}
38210323	{6850614, 14425413}
39465091	{15388, 9460884}
44314129	{3286365, 14595545, 14927367, 18077582}
46256489	{3885213, 5151145}
54029741	{16143305, 23669724}
59631211	{596056, 17870782}
61219789	{11458684, 17327901, 21097909, 26967126}
68512867	{11973934, 32681737}
70593931	{302706, 1978350}
72543547	{1458764, 22080842}
74411131	{6852398, 28841210}
76725091	{12302248, 35790166}
76923461	{3856373, 30040645}
77533123	{618693, 19891071}
77817979	{529434, 1235066}
79786523	{78003, 4007133, 4948468, 8553420, 12638556, 13118740, 13579891, 14060075, 17587024, 18145211, 21672160, 21750163, 22613495, 22691498, 26776634, 30783767, 31725102, 35810238}
80375707	{8149930, 32981595}
87499651	{13205712, 40700657}
89308771	{218995, 27764454}
91659283	{11205234, 17291447, 41534660, 44038410}
97676723	{4345461, 16120790, 16394586, 18538374, 18812170, 19609588, 22394128, 22667924, 39278421, 40075839, 40349635, 43134175}
100463443	{594838, 2132882}
101270251	{5512840, 19014340}
101276579	{4058637, 50514728}
102690677	{202926, 27699608}
105305443	{20687394, 40458901}
110139499	{40106497, 50582507}
119558011	{8492203, 53706142}
122166307	{47801130, 58991068}
127050067	{10424892, 43547726}
140197051	{23711218, 38081795}
154287451	{35577203, 57427501}
180703451	{48946570, 85920666}
194556451	{9130428, 90586146}
198982759	{9895300, 20168848, 45562611, 51768481, 61692219, 75626759, 81832629, 91756367}
208969223	{30346704, 39658701, 41145402, 47253271, 49070827, 52274955, 53661527, 55779470, 58983598, 59769396, 68395724, 77707721}
215878531	{1703732, 9610510, 35035613, 51776750, 63090992, 65975176, 88516095, 96422873}
217875571	{8664075, 16998416}
223625851	{11117273, 50710831}
226359547	{16305671, 83103251}
235426913	{15645107, 18964646, 44674801, 68302108, 83029817, 86349356, 99740095, 112059511}
242131889	{30673676, 93384139}
258172333	{22248217, 30882408, 36019675, 44653866, 64072645, 72706836}
259765747	{78709311, 102078236}
271763467	{31077534, 118799540}
282769771	{104322155, 116496614}
284736091	{119364604, 121503637}

n	$K'(n)$
284834299	{42841740, 139333186}
287449091	{61475550, 93914639}
305897131	{7053490, 55768977, 87552735, 136268222}
307694323	{2214016, 5326231, 36033419, 42186918, 53183411, 60308696, 60516177, 80849315, 81056796, 105332073, 113145420, 124141913, 136039261, 139151476}
310978027	{114261304, 152859348}
313748611	{31793468, 34385860, 88838670, 91431062}
317641171	{33996423, 75044576, 100353317, 108246855}
320326003	{18908403, 102314887}
326266051	{42178784, 47393034}
330198331	{17828327, 52256589}
341994131	{80156938, 146092541}
352802803	{4589448, 156575145}
356836819	{55795101, 111328135}
357872971	{89390964, 94066436}
360787771	{52942421, 99211202}
390612221	{181985494, 183405638}
418044563	{81552584, 87832578}
426783811	{9008398, 119849779}
435016187	{12743789, 196199762}
442181291	{66810496, 126153260}
453967739	{10689805, 86410067, 94902059, 123412902, 199133164, 207625156}
455198563	{44715303, 112257698}
461272267	{101933411, 221987046}
478614067	{6555623, 98786947}
480668347	{59116847, 165038571}
488169289	{168260976, 183690401, 206117653, 221547078, 231906481, 240833383}
498706651	{16489129, 119275996, 120495007, 223281874}
508606771	{80920580, 142142971}
535252867	{125374337, 131202519}
536342419	{17049582, 46640433, 78150572, 99277016, 103315895, 113437278, 177127293, 238228283, 259354727, 263393606}
545220869	{93330047, 188574250}
554599051	{5576561, 5950364, 7943980, 19966644, 20340447, 22334063, 41960053, 46819492, 56350136, 61209575, 111362810, 125752893, 269481479, 270727489}
576724219	{269177218, 281423423}
592467451	{35100481, 44543537}
628868467	{94494918, 128398346}
635155291	{48893951, 56640037}
640650931	{42076743, 267420659}
673778827	{105443043, 162443517}
696998251	{125131920, 249975121}
714663139	{9729153, 175929883, 261387513, 287074896}
717653129	{21996305, 356154466}
717831211	{253234022, 317675793}
724160251	{35555792, 35826658}
741470549	{83047998, 254905701}
750616739	{8520438, 58673186}
758581651	{97138116, 373923615}
764240611	{211144230, 320823068}
770909107	{2042964, 82115782}
770937931	{47037196, 368751142}
771337891	{62703575, 265008679}

n	$K'(n)$
791118043	{181008148, 185764347}
796072003	{132112592, 220613597}
801093011	{166359289, 229693775, 238255918, 301263705, 301590404, 373160334}
811730923	{59555792, 330941941}
818391211	{83478937, 142818481, 232277339, 291616883}
826004467	{80290494, 270373053}
830664451	{260209573, 395341520}
839268139	{34884674, 127698947}
839280691	{123105999, 224798503}
867022747	{61869130, 182944914}
893692819	{251018376, 349967711}
900736411	{87601732, 163565682}
903390643	{36468356, 209376662}
914906539	{37025884, 125587533}
921858631	{6492010, 22514888, 114349119, 143356017, 273186613, 390966882, 394027742, 410050620}
967266451	{274858977, 292213704}
974471243	{10995878, 47990028, 420887735, 450380688, 457881885, 487096405}
980056507	{23198842, 263786958}
1005833971	{274176142, 492593571}
1022336611	{30504234, 282811570}
1057426651	{21751812, 396162386}
1070941987	{284095346, 388851272}
1087190371	{114776100, 135386344, 471417584, 492027828}
1098743563	{34450014, 334496181}
1110582947	{35245918, 96496025, 238490923, 273621190, 405363133, 501974809}
1112671603	{328536961, 535364714}
1117890019	{30136535, 218429669}
1163227759	{37998117, 216431553, 244930741, 244942706, 251627139, 280138292, 421727173, 458571728}
1181566219	{105460468, 194468208, 438731932, 527739672}
1192903531	{142399930, 585752945}
1205772499	{426679602, 478030692}
1229751667	{307505257, 602843599}
1267154071	{201190472, 289302030, 552347761, 626694752}
1272558739	{2417615, 12749621, 60841167, 128454461, 143621697, 163018963, 293891039, 304223045, 352314591, 367481827, 435095121, 613603488}
1312573123	{632802142, 650906671}
1318717531	{401939115, 418541973}
1378646179	{431566434, 584113973}
1397357851	{229569505, 370910847}
1409372779	{165165665, 490769046}
1414154827	{16019042, 431548767}
1426319563	{264499272, 320820726}
1440922891	{574021197, 614388673}
1441678411	{354604860, 720806323}
1446818651	{590028629, 607422676}
1468824787	{51677347, 706917806}
1470650851	{155358394, 318834311}
1495190699	{31099815, 71633234, 174597816, 255664654, 461362285, 501895704}
1510474841	{75621394, 120422115, 209175004, 247050723, 452987092, 579615700, 601262022, 734815632}
1517039371	{456909809, 562794459}
1518290707	{75617868, 710841600}
1526732803	{257443804, 623983641}
1529819971	{31351824, 251549938}

n	$K'(n)$
1532419099	{473655069, 680943729}
1536112001	{703276597, 728044855}
1537433899	{61052985, 673956349}
1537641691	{371945158, 400992498}
1589307919	{1977949, 122079597, 163986261, 180919230, 567442998, 626282631, 676959430, 750340177}
1609916491	{283262983, 658732434}
1614508267	{86733609, 645916386}
1617921667	{511188341, 562365339}
1644637051	{327648032, 353114845}
1671603667	{222718019, 238786217}
1672125131	{348568153, 553739162}
1725675451	{93482600, 331393634, 518410289, 782388928}
1734059291	{3523879, 18689158, 132350672, 544013059, 657674573, 679887610}
1785843547	{440071674, 573905143}
1791426787	{439415097, 875526745}
1803768091	{73921458, 840574009}
1860373241	{169168150, 266845273}
1905958891	{439345202, 741694959}
1911197947	{383295232, 884373755}
1922687293	{139767381, 186657177, 500489759, 562392516, 564243429, 719103150, 720954063, 779108095, 782856820, 825997891}
1928903971	{338280613, 737615354}
2058874201	{54084184, 243867206, 468808442, 493788205, 654802340, 658591464, 683571227, 778497311, 844585362, 968280333}
2116483027	{155982888, 577420851}
2139155051	{12190301, 14242754, 38884478, 106561837, 132994892, 155584163, 180225887, 182278340, 206658942, 208711395, 307017169, 350052804, 376746981, 403180036, 427821760, 470857395, 495499119, 521932174, 544521445, 569163169, 595596224, 644879672, 671312727, 689967760, 695954451, 716400815, 765684263, 792117318, 859794677, 884436401, 890423092, 910869456, 933458727, 1033816954, 1054263318, 1060250009}
2155416251	{30853345, 67318400, 170698959, 470423008, 506888063, 708440367}
2172155819	{542359256, 723042015}
2222229767	{48595615, 65252382, 226440824, 249272916, 432429492, 471918351, 706743265, 794295235, 833784094, 907420566, 1021268563}
2246762899	{17568027, 856976238}
2269307587	{417213141, 1125066183}
2302024969	{85249937, 294308472, 323059646, 702618055}
2321591371	{63395819, 147657942, 485539590, 696593351, 716190010, 761150068, 927243771, 972203829}
2352371251	{921151697}
2372976563	{86080207, 712599344}
2437907779	{185666660, 921089378}

APPENDIX C

The Commutator Curve Primality Test in C++

I give in this appendix an implementation of Algorithm 5.30 in C++ using the arithmetic PIOLOGIE V 1.3 [**130**] and Strassen's fast matrix computation [**123**], [**131**].

ALGORITHM C.1 (Hypothetical Commutator Curve Primality Test).
Input: $n \in \mathbb{N}$, *where* n *is odd,* $n \geq 5$, *and* $n \not\equiv 7 \pmod 8$.
Output: $R \in \{\text{true}, \text{false}\}$.

(1) If $\sqrt{n} \in \mathbb{Z}$, *terminate with the result* false.
(2) Set $M := \emptyset$.
(3) Choose $x \in (\mathbb{Z}/n\mathbb{Z})^*$ *with* $\pm x \notin M$ *and*

$$\left(\tfrac{x^2+4}{n}\right) = -1.$$

(4) Terminate with the result false, *if*

$$(x^2+2)^{n-1} \not\equiv 1 \pmod n \quad or \quad (x^2+4)^{\frac{n-1}{2}} \not\equiv -1 \pmod n$$
$$or \quad c(1,x)^{\frac{n+1}{2}} \not\equiv -I_2 \pmod n.$$

(5) Set $M := M \cup \{x\}$ *and go to step (4), if* $|M| < 2$.
(6) Let $y, z \in M$ *with* $y \neq z$ *and terminate with the result* false, *if*

$$gcd(y \pm z, n) > 1,$$

otherwise terminate with the result true.

1. Running Times

There exist four ways to implement step (4) of Algorithm 5.30:

(1) By matrix in $SL_2(n)$

$$(x^2+2)^{n-1} \not\equiv 1 \pmod n \quad \text{or} \quad (x^2+4)^{\frac{n-1}{2}} \not\equiv -1 \pmod n$$
$$\text{or} \quad c(1,x)^{\frac{n+1}{2}} \not\equiv -I_2 \pmod n.$$

(2) By minimal polynomial in $(\mathbb{Z}/n\mathbb{Z})[t]$

$$(x^2+2)^{n-1} \not\equiv 1 \pmod n \quad \text{or} \quad (x^2+4)^{\frac{n-1}{2}} \not\equiv -1 \pmod n$$
$$\text{or} \quad x^{\frac{n+1}{2}} \not\equiv -1 \pmod{(n, t^2-(x^2+2)t+1)}.$$

(3) By recurrence relation

$$\begin{aligned}(x^2+2)^{n-1} &\not\equiv 1 \pmod n \quad \text{or} \quad (x^2+4)^{\frac{n-1}{2}} \not\equiv -1 \pmod n \\ \text{or} \quad \omega_{\frac{n+1}{2}}(x) &\not\equiv 0 \pmod n \quad \text{or} \quad x\theta_{\frac{n+1}{2}}(x) \not\equiv -2 \pmod n,\end{aligned}$$

where $\omega_n(x)$ and $\theta_n(x)$ are defined in Section 4 of Chapter 4 on page 60.

(4) By Lucas sequence $U_n(x,-1)$

$$\begin{aligned}(x^2+2)^{n-1} &\not\equiv 1 \pmod n \quad \text{or} \quad (x^2+4)^{\frac{n-1}{2}} \not\equiv -1 \pmod n \\ \text{or} \quad U_{n+1}(x,-1) &\not\equiv 0 \pmod n \quad \text{or} \quad U_n(x,-1) \not\equiv -1 \pmod n.\end{aligned}$$

In the following table we give running times to certify large prime numbers for the different implementations using the arithmetic PIOLOGIE V 1.3 on a Pentium II with 300 MHz, Microsoft Windows NT 4.0 and Microsoft Visual C++ 6.0.

$p \in \mathbb{P}$	Algorithm 1 in $SL_2(p)$	Algorithm 1 in $SL_2(p)$ using Strassen's matrix comp.	Algorithm 2 in $\mathbb{F}_p[t]/f(t)\mathbb{F}_p$	Algorithm 3 using recurrence relation	Algorithm 4 using Lucas sequence
$2^{1279}-1$	5.39 s	5.39 s	5.18 s	4.12 s	4.07 s
$2^{2203}-1$	21.66 s	21.67 s	20.87 s	16.57 s	16.45 s
$2^{2281}-1$	25.67 s	25.68 s	24.54 s	19.50 s	19.34 s
$2^{3217}-1$	63.74 s	63.96 s	61.28 s	48.15 s	48.16 s
$3\cdot 2^{2208}+1$	18.83 s	18.86 s	18.01 s	12.96 s	12.82 s
$3\cdot 2^{3912}+1$	91.71 s	91.91 s	87.60 s	62.54 s	62.25 s
$320!+1$	27.21 s	26.96 s	25.44 s	16.53 s	15.07 s
$324!-1$	26.31 s	26.10 s	24.55 s	16.40 s	15.04 s
$469!-1$	101.13 s	99.87 s	94.34 s	61.58 s	56.68 s

From this table it is easy to see that Algorithm 4 is the fastest implementation of the Hypothetical Commutator Curve Primality Test. This was also the theoretical result of Section 8 of Chapter 4 on page 143.

2. Commutator Curve Primality Test Based on Polynomials

```
bool isprime(const Natural& n)
{
  if ((n&1) == 0) return (n == 2);

  Natural x,x2;
  sqrt(n, x, x2);
  if (x2 == 0) return false;

  Natural m = n-1;
  Natural l = n >> 1;
  Natural k = 1;
  polynomial<Natural> a,b;
  x = 4; x2 = 0;
  a.m = n;
```

```
  while (true) {
    while (true) {
      x += k; k += 2;
      if (x >= n) x -= n;
      const int i = jacobi(x, n);
      if (i == -1) break;
      if (i == 0) return false;
    }
    if (pow(x, l, n) != m) return false;
    x -= 2; ++l;
    if (pow(x, m, n) != 1) return false;
    a.p[1] = n-x; a.p[0] = 1;
    b.p[1] = 1; b.p[0] = 0;
    if (pow(b, l, a) != m) return false;
    if (x2 != 0) break;
    x += 2; --l; x2 = k >> 1;
  }
  k >>= 1;
  return (gcd(x2+k, n) == 1 && gcd(abs(x2, k), n) == 1);
}
```

3. Commutator Curve Primality Test Based on Matrices

```
void commutator(const Natural& y, matrix<Integer>& a)
{
  a.p[2] = y*y; a.p[2] %= a.m;
  a.p[0] = y+1; a.p[0] += a.p[2];
  if (a.p[0] >= a.m) a.p[0] -= a.m;
  a.p[1] = y; a.p[3] = y-1;
  if (a.p[2] != 0) a.p[2] = a.m-a.p[2];
  if (a.p[3] != 0) a.p[3] = a.m-a.p[3];
}

bool isprime(const Natural& n)
{
  if ((n&1) == 0) return (n == 2);

  Natural x,x2;
  sqrt(n, x, x2);
  if (x2 == 0) return false;

  Integer m = n-1;
  Integer l = n >> 1;
  Natural k = 1;
  matrix<Integer> a(n);
  x = 4; x2 = 0;
  while (true) {
    while (true) {
```

```
      x += k; k += 2;
      if (x >= n) x -= n;
      const int i = jacobi(x, n);
      if (i == -1) break;
      if (i == 0) return false;
    }
    if (pow(x, abs(l), n) != abs(m)) return false;
    x -= 2; ++l;
    if (pow(x, abs(m), n) != 1) return false;
    commutator(k >> 1, a);
    if (pow(a, l) != m) return false;
    if (x2 != 0) break;
    x += 2; --l; x2 = k >> 1;
  }
  k >>= 1;
  return (gcd(x2+k, n) == 1 && gcd(abs(x2, k), n) == 1);
}
```

4. Commutator Curve Primality Test Based on Recurrence Relations

```
bool isprime(const Natural& n)
{
  if ((n&1) == 0) return (n == 2);

  Natural x,x2;
  sqrt(n, x, x2);
  if (x2 == 0) return false;

  Natural m = n-1;
  Natural l = n >> 1;
  Natural k = 1;
  x2 = 4;
  Natural x3 = Digit(0);
  while (true) {
    while (true) {
      x2 += k; k += 2;
      if (x2 >= n) x2 -= n;
      const int i = jacobi(x2, n);
      if (i == -1) break;
      if (i == 0) return false;
    }
    if (pow(x2, abs(l), n) != abs(m)) return false;
    x2 -= 2;
    if (pow(x2, abs(m), n) != 1) return false;
    x2 += 2;                // x2 == x*x+4
    x = k >> 1;
    Natural z1 = x*x;       // z1 == x*x (mod n)
    z1 %= n;
```

```
Natural z2 = x+2;
z2 *= x; z2 %= n;       // z2 == x(x+2) (mod n)
Natural z3 = x-1;
if (z3 != 0) z3 = n-z3; // z3 == 1-x (mod n)
Natural z4 = z1+x;
++z4;
if (z4 >= n) z4 -= n;   // z4 == x*x+x+1 (mod n)
Natural w = 1;          // w_1 := 1
Natural t = x+1;        // t_1 := x+1
if (t >= n) t -= n;
Digit m2 = log2(++l)-1;
do {
  Natural h1 = w*w;
  // w_{2m} = (2 + 2xt_m - (x^2+2x)w_m)w_m
  Natural h2 = x*t;
  ++h2; h2 <<= 1;
  Natural h3 = z2*w;
  if (h2 < h3) {
    h3 -= h2; w *= h3; w %= n;
    if (w != 0) w = n-w;
  } else { h2 -= h3; w *= h2; w %= n; }
  // t_{2m} = xt_m^2 + 2t_m - x^2w_m^2
  h1 *= z1; h2 = t*t;
  h2 *= x; t <<= 1; t += h2;
  if (t < h1) {
    h1 -= t; h1 %= n;
    if (h1 != 0) t = n-h1;
    else t = 0;
  } else { t -= h1; t %= n; }
  if (l.testbit(m2)) {
    // w_{2m+1} = 1 + xt_{2m} + (1-x)w_{2m}
    h1 = z3*w; h2 = x*t; ++h1; h1 += h2;
    // t_{2m+1} = 1 + x + (1+x+x^2)t_{2m} - x^2w_{2m}
    h2 = w*z1; t *= z4; ++t; t += x;
    if (t < h2) {
      h2 -= t; h2 %= n;
      if (h2 != 0) t = n-h2;
      else t = 0;
    } else { t -= h2; t %= n; }
    w = h1%n;
  }
} while (m2-- > 0);
if (w != 0) return false;
t *= x; t += 2; t %= n;
if (t != 0) return false;

if (x3 != 0) break;
x3 = x; --l;
```

```
  }
  k >>= 1;
  return (gcd(x3+k, n) == 1 && gcd(abs(x3, k), n) == 1);
}
```

5. Commutator Curve Primality Test Based on Lucas Sequence $U_n(x, -1)$

```
bool isprime(const Natural& n)
{
  if ((n&1) == 0) return (n == 2);

  Natural x,x2;
  sqrt(n, x, x2);
  if (x2 == 0) return false;

  Natural m = n-1;
  Natural l = n >> 1;
  Natural l2 = n+1;
  Natural k = 1;
  x2 = 4;
  Natural x3 = Digit(0);
  while (true) {
    while (true) {
      x2 += k; k += 2;
      if (x2 >= n) x2 -= n;
      const int i = jacobi(x2, n);
      if (i == -1) break;
      if (i == 0) return false;
    }
    if (pow(x2, abs(l), n) != abs(m)) return false;
    x2 -= 2;
    if (pow(x2, abs(m), n) != 1) return false;
    x2 += 2;
    x = k >> 1;
    Natural u0 = 0;          // U_0(x, -1) := 0
    Natural u1 = 1;          // U_1(x, -1) := 1
    Digit m2 = log2(l2)-1;
    do {
      // U_{2m-1}(x, -1) = U_m(x, -1)^2 + U_{m-1}(x, -1)^2
      // U_{2m}(x, -1)   = xU_m(x, -1)^2 + 2U_m(x, -1)U_{m-1}(x, -1)
      Natural h0 = u0*u0;
      Natural h1 = u1*u1;
      Natural h3 = u0*u1;
      h3 <<= 1;
      u0 = h0+h1; u0 %= n;
      h1 *= x;
      u1 = h1+h3; u1 %= n;
      if (l2.testbit(m2)) {
```

```
        // U_{m+2}(x, -1) = xU_{m+1}(x, -1) + U_m(x, -1)
        h0 = x*u1; h0 += u0;
        u0 = u1;
        u1 = h0%n;
      }
    } while (m2-- > 0);
    if (u1 != 0 || u0 != m) return false;

    if (x3 != 0) break;
    x3 = x;
  }
  k >>= 1;
  return (gcd(x3+k, n) == 1 && gcd(abs(x3, k), n) == 1);
}
```

6. Simple Polynomial Class

```
template<class T>
struct polynomial {
  // p[1]*x + p[0], where p[1],p[0] in Z/mZ.
  T p[2];
  static T m;

  polynomial() {}
  polynomial(const T& a) { p[0] = a%m; }
  polynomial(const polynomial& a) { *this = a; }

  polynomial& operator=(const polynomial& a) {
    p[0] = a.p[0]; p[1] = a.p[1];
    return *this;
  }

  void mulmod(const polynomial& a, const polynomial& b);
};


template<class T>
T polynomial<T>::m = T();

template<class T>
inline bool operator!=(const polynomial<T>& a, const T& b)
{
  return (a.p[1] != 0 || a.p[0] != b);
}

template<class T>
void polynomial<T>::mulmod(const polynomial<T>& a, const polynomial<T>& b)
// Algorithm:  c.mulmod(a, b)
```

```
// Input:      a,b,c in polynomial<T> where b = x^2 + b.p[1]*x + b.p[0].
// Output:     c in polynomial<T> such that c := c*a (mod b) ||
{
  if (this == &b) { p[0] = p[1] = 0; return; }
  T x[3];
  if (this == &a) {
    // p[1]^2*x^2 + 2*p[0]*p[1]*x + p[0]^2
    x[1] = p[0]*p[1]; x[1] <<= 1;
  } else {
    // p[1]*a.p[1]*x^2 + (p[0]*a.p[1]+p[1]*a.p[0])*x + p[0]*a.p[0]
    x[1] = p[0]*a.p[1]; x[1] += p[1]*a.p[0];
  }
  x[0] = p[0]*a.p[0]; x[2] = p[1]*a.p[1];
  p[0] = x[0]%m; p[1] = x[1]%m; x[2] %= m;
  x[0] = b.p[0]*x[2]; x[0] %= m;
  x[1] = b.p[1]*x[2]; x[1] %= m;
  if (p[0] < x[0]) p[0] += m; p[0] -= x[0];
  if (p[1] < x[1]) p[1] += m; p[1] -= x[1];
}

template<class T>
polynomial<T> pow(polynomial<T> a, T b, const polynomial<T>& c)
// Algorithm:  d := pow(a, b, c)
// Input:      a,c in polynomial<T> and b in T.
// Output:     d in polynomial<T> such that d = a^b (mod c) ||
{
  if (b == 1) return a;
  else if (b == 0) return T(1);

  while ((b&1) == 0) { a.mulmod(a, c); b >>= 1; }

  polynomial<T> z = a;
  while (--b != 0) {
    while ((b&1) == 0) { a.mulmod(a, c); b >>= 1; }
    z.mulmod(a, c);
  }
  return z;
}
```

7. Simple Matrix Class

```
template<class T>
struct matrix {
  T p[4];
  T m;

  matrix& mod() { p[0] %= m; p[1] %= m; p[2] %= m; p[3] %= m; return *this; }
```

```
  matrix(const T& a) { p[0] = p[1] = p[2] = p[3] = 0; m = a; }
  matrix(const matrix& a) { *this = a; }

  matrix& operator=(const matrix& a) {
    p[0] = a.p[0]; p[1] = a.p[1]; p[2] = a.p[2]; p[3] = a.p[3]; m = a.m;
    mod();
    return *this;
  }

  matrix& operator*=(const matrix& a);
};

template <class T>
matrix<T>& matrix<T>::operator*=(const matrix<T>& a)
{
  if (this == &a) {
    // T commutative:
    const T t = p[0]+p[3];
    p[0] *= p[0];
    const T s = p[1]*p[2];
    p[0] += s;
    p[1] *= t; p[2] *= t;
    p[3] *= p[3];
    p[3] += s;
  } else {
#ifdef STRASSEN_MUL
    p[2] = p[0] - p[2];
    T h4 = a.p[3] - a.p[1];
    T h5 = p[2] * h4;
    p[2] = p[3] - p[2];
    h4 += a.p[0];
    T h = p[2] + p[0];
    T h2 = a.p[3] - h4;
    T h3 = h * h2;
    h2 = p[2] * h4;
    h4 -= a.p[2];
    h = p[3] * h4;
    p[2] = p[1] - p[2];
    p[3] = p[2] * a.p[3];
    p[2] = p[0] * a.p[0];
    p[0] = p[1] * a.p[2];
    p[0] += p[2];
    p[2] += h2;
    h3 += p[2];
    p[2] += h5;
    p[1] = p[3] + h3;
    p[3] = h5 + h3;
    p[2] -= h;
```

```
#else
    T u = p[0];
    T s = p[0]*a.p[0];
    T t = p[1]*a.p[2];
    p[0] = s+t;
    s = u*a.p[1];
    t = p[1]*a.p[3];
    p[1] = s+t;
    u = p[2];
    s = p[2]*a.p[0];
    t = p[3]*a.p[2];
    p[2] = s+t;
    s = u*a.p[1];
    t = p[3]*a.p[3];
    p[3] = s+t;
#endif
  }
  mod();
  return *this;
}

template <class T>
inline bool operator!=(const matrix<T>& a, const T& b)
{
  return (a.p[0] != b || a.p[1] != 0 || a.p[2] != 0 || a.p[3] != b);
}

template<class T>
matrix<T> pow(matrix<T> a, T b)
// Algorithm:  d := pow(a, b)
// Input:      a,b in T.
// Output:     d in T such that d = a^b ||
{
  if (b == 1) return a;
  else if (b == 0) return T(1);

  while ((b&1) == 0) { a *= a; b >>= 1; }

  matrix<T> z = a;
  while (--b != 0) {
    while ((b&1) == 0) { a *= a; b >>= 1; }
    z *= a;
  }
  return z;
}
```

Bibliography

[1] W. W. Adams, D. Shanks, *Strong primality tests that are not sufficient*, Mathematics of Computation **39** (1982), 255–300.

[2] L. M. Adleman, M.-D. Huang, *Primality Testing and Abelian Varieties Over Finite Fields*, 1992.

[3] L. M. Adleman, C. Pomerance, R. S. Rumely, *On Distinguishing Prime Numbers from Composite Numbers*, Annals of Mathematics **117** (1983), 173–206.

[4] L. A. Ahlfors, *Complex Analysis*, Third Edition, 1979.

[5] W. R. Alford, A. Granville, C. Pomerance, *There are Infinitely many Carmichael Numbers*, Annals of Mathematics **140** (1994), 703–722.

[6] N. C. Ankeny, *The Least Quadratic Non Residue*, Annals of Mathematics **55** (1952), 65–72.

[7] R. Apéry, *Irrationalité de $\zeta(2)$ et $\zeta(3)$*, Astérisque **61** (1979), 11–13.

[8] A. O. L. Atkin, F. Morain, *Elliptic Curves and Primality Proving*, Mathematics of Computation **61** (1993), 29–68.

[9] A. O. L. Atkin, *Intelligent Primality Test Offer*, Computational Perspectives on Number Theory, Proceedings of a Conference in Honor of A. O. L. Atkin (1995), 1–11.

[10] E. Bach, *Fast Algorithms under the Extended Riemann Hypothesis – A Concrete Estimate*, Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing (1982), 290–295.

[11] E. Bach, *Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms*, 1985.

[12] E. Bach, *Explicit Bounds for Primality Testing and Related Problems*, Mathematics of Computation **55** (1990), 355–380.

[13] E. Bach, *Comments on Search Procedures for Primitive Roots*, Mathematics of Computation **66** (1997), 1719–1727.

[14] E. Bach, J. Shallit, *Algorithmic Number Theory – Volume 1: Efficient Algorithms*, 1996.

[15] R. J. Backlund, *Über die Nullstellen der Riemannschen Zetafunktion*, Dissertation, Helsingfors, 1916.

[16] R. Baillie, S. S. Wagstaff, Jr., *Lucas Pseudoprimes*, Mathematics of Computation **35** (1980), 1391–1417.

[17] P. Beauchemin, G. Brassard, C. Crépeau, C. Goutier, C. Pomerance, *The Generation of Random Numbers that are Probably Prime*, Journal of Cryptology **1** (1988), 53–64.

[18] D. Bleichenbacher, *Efficiency and Security of Cryptosystems based on Number Theory*, Dissertation, ETH Zürich, 1996.

[19] W. Bosma, M. van der Hulst, *Primality Proving with Cyclotomy*, Dissertation, University of Amsterdam, 1990.

[20] R. P. Brent, *The First 40,000,000 Zeros of $\zeta(s)$ Lie on the Critical Line*, Notices of the American Mathematical Society **24** (1977), A-417.

[21] R. P. Brent, *On the Zeros of the Riemann Zeta Function in the Critical Strip*, Mathematics of Computation **33** (1979), 1361–1372.

[22] R. P. Brent, J. van de Lune, H. J. J. te Riele, D. T. Winter, *On the Zeros of the Riemann Zeta Function in the Critical Strip II*, Mathematics of Computation **39** (1982), 681–688.

[23] D. Bressoud, S. Wagon, *A Course in Computational Number Theory*, 2000.

[24] J. Brillhart, D. H. Lehmer, J. L. Selfridge, *New Primality Criteria and Factorizations of $2^m \pm 1$*, Mathematics of Computation **29** (1975), 620–647.

[25] N. D. Bronson, D. A. Buell, *Congruential Sieves on FPGA Computers*, Proceedings of Symposia in Applied Mathematics **48** (1994), 547–551.
[26] J. Brüdern, *Einführung in die analytische Zahlentheorie*, 1995.
[27] D. A. Burgess, *The Distribution of Quadratic Residues and Non-Residues*, Mathematika **4** (1957), 106–112.
[28] D. A. Burgess, *On Character Sums and Primitive Roots*, Proceedings of the London Mathematical Society, No. 3, **12** (1962), 179–192.
[29] D. A. Burgess, *On the Quadratic Character of a Polynomial*, Jounal of the London Mathematical Society **42** (1967), 73–80.
[30] R. D. Carmichael, *On Composite Numbers P which Satisfy the Fermat Congruence* $a^{P-1} \equiv 1 \bmod P$, American Mathematical Monthly **19** (1912), 22–27.
[31] H. Cohen, H. W. Lenstra, Jr., *Primality Testing and Jacobi Sums*, Mathematics of Computation **42** (1984), 297–330.
[32] H. Cohen, A. K. Lenstra, *Implementation of a New Primality Test*, Mathematics of Computation **48** (1987), 103–121.
[33] H. Cohen, *A Course in Computational Algebraic Number Theory*, Second Corrected Printing, 1995.
[34] J. B. Conrey, *More than Two Fifths of the Zeros of the Riemann Zeta Function are on the Critical Line*, Journal für die reine und angewandte Mathematik **399** (1989), 1–26.
[35] I. Damgård, P. Landrock, C. Pomerance, *Average Case Error Estimates for the Strong Probable Prime Test*, Mathematics of Computation **61** (1993), 177–194.
[36] H. Davenport, *Multiplicative Number Theory*, Third Edition, 2000.
[37] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, 1901.
[38] L. E. Dickson, *History of the Theory of Numbers – Divisibility and Primality*, Volume I, 1952.
[39] H. M. Edwards, *Riemann's Zeta Function*, 1974.
[40] P. Erdös, P. Kiss, A. Sárközy, *A Lower Bound for the Counting Function of Lucas Pseudoprimes*, Mathematics of Computation **41** (1988), 315–323.
[41] M. R. Fellows, N. Koblitz, *Self-Witnessing Polynomial-Time Complexity and Prime Factorization*, Designs, Codes and Cryptography **2** (1992), 231–235.
[42] G. Fischer, R. Sacher, *Einführung in die Algebra*, 1983.
[43] O. Forster, *Algorithmische Zahlentheorie*, 1996.
[44] J. von zur Gathen, J. Gerhard, *Modern Computer Algebra*, 1999.
[45] The Great Internet Mersenne Prime Search (GIMPS), availabe at `www.mersenne.org/prime.htm`.
[46] S. Goldwasser, J. Kilian, *Almost all primes can be quickly certified*, in Proceedings of the 18$^{\text{th}}$ Annual ACM Symposium on Theory of Computation (1986), 316–329.
[47] D. M. Gordon, C. Pomerance, *The Distribution of Lucas and Elliptic Pseudoprimes*, Mathematics of Computation **57** (1991), 825–838. Corrigendum in **60** (1993), 877.
[48] D. Gorenstein, *Finite Groups*, 1980.
[49] S. Graham, R. J. Ringrose, *Lower Bounds for Least Quadratic Non-Residues*, Analytic Number Theory, Proceedings of a Conference in Honor of Paul T. Bateman, 1990.
[50] J. P. Gram, *Note sur les zéros de la fonction* $\zeta(s)$ *de Riemann*, Acta Mathematica **27** (1903), 289–304.
[51] J. Grantham, *Frobenius Pseudoprimes*, Dissertation, University of Georgia, 1997.
[52] J. Grantham, *A Probable Prime Test with High Confidence*, Journal of Number Theory **72** (1998), 32–47.
[53] A. Granville, *Primality Testing and Carmichael Numbers*, Notices of the American Mathematical Society **39** (1992), 696-700.
[54] S. Gurak, *Pseudoprimes for Higher-Order Linear Recurrence Sequences*, Mathematics of Computation **55** (1990), 783–813.
[55] M. Hall, *Quadratic Residues in Factorization*, Bulletin of the American Mathematical Society **39** (1933), 758–763.
[56] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Fifth Edition, 1979.

[57] B. Huppert, *Endliche Gruppen I*, 1967.
[58] J. I. Hutchinson, *On the Roots of the Riemann Zeta Function*, Transactions of the American Mathematical Society **27** (1925), 49–60.
[59] A. E. Ingham, *The Distribution of Prime Numbers*, 1932.
[60] A. Ivić, *The Riemann Zeta-Function – The Theory of the Riemann Zeta-Function with Applications*, 1985.
[61] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Second Edition, 1990.
[62] G. Jaeschke, *On Strong Pseudoprimes to Several Bases*, Mathematics of Computation **61** (1993), 915–926.
[63] A. A. Karatsuba, *Basic Analytic Number Theory*, 1993.
[64] A. A. Karatsuba, S. M. Voronin, *The Riemann Zeta-Function*, 1992.
[65] S. H. Kim, C. Pomerance, *The Probability that a Random Probable Prime is Composite*, Mathematics of Computation **53** (1989), 721–741.
[66] D. E. Knuth, *The Art of Computer Programming – Volume 2: Seminumerical Algorithms*, Third Edition, 1998.
[67] N. Koblitz, *A Course in Number Theory and Cryptography*, Second Edition, 1994.
[68] S. Konyagin, C. Pomerance, *On Primes Recognizable in Deterministic Polynomial Time*, in R. L. Graham, J. Nešetřil (Eds.): The Mathematics of Paul Erdös I, 1997.
[69] H. Kurzweil, B. Stellmacher, *Theorie der endlichen Gruppen – Eine Einführung*, 1998.
[70] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, First Volume, 1909.
[71] E. Landau, *Vorlesungen über Zahlentheorie*, Second Volume, 1927.
[72] R. S. Lehman, *Separation of Zeros of the Riemann Zeta-Function*, Mathematics of Computation **20** (1966), 523–541.
[73] D. H. Lehmer, *On the Roots of the Riemann Zeta-Function*, Acta Mathematica **95** (1956), 291–298.
[74] D. H. Lehmer, *Extended Computation of the Riemann Zeta-Function*, Mathematika **3** (1956), 102–108.
[75] D. H. Lehmer, E. Lehmer, D. Shanks, *Integer Sequences Having Prescribed Quadratic Character*, Mathematics of Computation **24** (1970), 433–451.
[76] H. W. Lenstra, Jr., *Miller's Primality Test*, Information Processing Letters **8** (1979), 86–88.
[77] H. W. Lenstra, Jr., *Primality Testing*, in H. W. Lenstra, Jr., R. Tijdeman (Eds.): Computational Methods in Number Theory Part I, Second Edition, 1994.
[78] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, American Journal of Mathematics **1** (1878), 184–240, 289–321.
[79] R. F. Lukes, *A Very Fast Electronic Number Sieve*, Dissertation, Unversity of Manitoba, 1996.
[80] R. F. Lukes, C. D. Patterson, H. C. Williams, *Some Results on Pseudosquares*, Mathematics of Computation **65** (1996), 361–372.
[81] J. van de Lune, H. J. J. te Riele, *On the Zeros of the Riemann Zeta Function in the Critical Strip III*, Mathematics of Computation **41** (1983), 759–767.
[82] J. van de Lune, H. J. J. te Riele, D. T. Winter, *On the Zeros of the Riemann Zeta Function in the Critical Strip IV*, Mathematics of Computation **46** (1986), 667–681.
[83] U. M. Maurer, *Fast Generation of Prime Numbers and Secure Public-Key Crypotographic Parameters*, to appear in Journal of Cryptology.
[84] N. A. Meller, *Computations Connected with the Check of Riemann's Hypothesis*, Doklady Akademii Nauk SSSR **123** (1958), 246–248.
[85] P. Mihăilescu, *Cyclotomy of Rings & Primality Testing*, Dissertation, ETH Zürich, 1998.
[86] G. L. Miller, *Riemann's Hypothesis and Tests for Primality*, Journal of Computer and System Sciences **13** (1976), 300–317.
[87] L. Monier, *Evaluation and Comparison of Two Efficient Probabilistic Primality Testing Algorithms*, Theoretical Computer Science **12** (1980), 97–108.
[88] H. L. Montgomery, *Topics in Multiplicative Number Theory*, 1971.

[89] H. L. Montgomery, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, 1994.
[90] W. More, *Probable Prime Tests Using Lucas Sequences*, G.E. Bergum et.al. (eds.), Applications of Fibonacci Numbers **7** (1998), 283–289.
[91] W. More, *The LD Probable Prime Test*, R.C. Mullin, G.L. Mullen (eds.), Countemporary Mathematics **225** (1999), 185–191.
[92] P. M. Neumann, Ch. E. Praeger, *A Recognition Algorithm for Special Linear Groups*, Proceedings of the London Mathematical Society, No. 3, **65** (1992), 555–603.
[93] A. M. Odlyzko, *The* 10^{20}*-th Zero of the Riemann Zeta Function and 175 Million of it Neighbors*, preprint, 1990.
[94] A. M. Odlyzko, *Analytic Computations in Number Theory*, Proceedings of Symposia in Applied Mathematics **48** (1994), 451–463,
[95] A. M. Odlyzko, *The* 10^{22}*-nd zero of the Riemann zeta function*, preprint, 2001.
[96] A. M. Odlyzko, A. Schönhage, *Fast Algorithms for Multiple Evaluations of the Riemann Zeta Function*, Transactions of the American Mathematical Society **309** (1988), 797–809.
[97] S. J. Patterson, *An Introduction to the Theory of the Riemann Zeta-Function*, 1988.
[98] S. Pajunen, *On Two Theorems of Lenstra*, Information Processing Letters **11** (1980), 224–228.
[99] R. G. E. Pinch, *The Pseudoprimes up to* 10^{13}, preprint, 1993.
[100] R. G. E. Pinch, *The Carmichael Numbers up to* 10^{15}, Mathematics of Computation **61** (1993), 381–391.
[101] R. G. E. Pinch, *The Carmichael Numbers up to* 10^{16}, preprint, 1998.
[102] H. C. Pocklington, *The Determination of the Prime or Composite Nature of Large Numbers by Fermat's Theorem*, Proceedings of the Cambridge Philosophical Society **18** (1914-1916), 29–30.
[103] C. Pomerance, *Are there Counter-Examples to the Baillie – PSW Primality Test?*, Dopo Le Parole aangeboden aan Dr. A. K. Lenstra, privately published, 1984.
[104] C. Pomerance, J. L. Selfridge, S. S. Wagstaff, Jr., *The Pseudoprimes to* $25 \cdot 10^9$, Mathematics of Computation **35** (1980), 1003–1026.
[105] K. Prachar, *Primzahlverteilung*, 1957.
[106] M. O. Rabin, *Probabilistic Algorithm for Testing Primality*, Journal of Number Theory **12** (1980), 128–138.
[107] R. Remmert, *Funktionentheorie I*, Second Edition, 1989.
[108] P. Ribenboim, *The New Book of Prime Number Records*, 1996.
[109] H. te Riele, et al., *New Factorization Record*, available at Number Theory Listserver and Archives (NMBRTHRY) `http://listserv.nodak.edu/archives/nmbthry.html`, August 1999.
[110] B. Riemann, *Gesammelte Mathematische Werke und Wissenschaftlicher Nachlaß*, Second Edition, 1892.
[111] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Second Edition, 1994.
[112] J. B. Rosser, L. Schoenfeld, *Approximate Formulas for Some Functions of Prime Numbers*, Illinois Journal of Mathematics **6** (1962), 64–94.
[113] J. B. Rosser, L. Schoenfeld, *Sharper Bounds for the Chebyschev Functions* $\theta(x)$ *and* $\psi(x)$, Mathematics of Computation **29** (1975), 243–269.
[114] J. B. Rosser, Y. M. Yohe, L. Schoenfeld, *Rigorous Computation and the Zeros of the Riemann Zeta-Function*, Information Processing **68**, Proceedings of IFIP Congress (1968), 70–76.
[115] R. Rumely, *Numerical Computations Concerning the ERH*, Mathematics of Computation **61** (1993), 415–440.
[116] L. Schoenfeld, *Sharper Bounds for the Chebyschev Functions* $\theta(x)$ *and* $\psi(x)$ *II*, Mathematics of Computation **30** (1976), 337–360.
[117] A. Schönhage, A. F. W. Grotefeld, E. Vetter, *Fast Algorithms – A Multitape Turning Machine Implementation*, 1994.
[118] R. Schoof, *Elliptic Curves Over Finite Fields and the Computation of Square Roots mod* p, Mathematics of Computation **44** (1985), 483-494.
[119] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 1986.

[120] R. Solovay, V. Strassen, *A Fast Monte-Carlo Test for Primality*, SIAM Journal on Computing **6** (1977), 84–85.
[121] R. Spira, *Calculation of Dirichlet L-Functions*, Mathematics of Computation **23** (1969), 489–497.
[122] A. J. Stephens, H. C. Williams, *An Open Architecture Number Sieve*, London Mathematical Society Lecture Note Series **154** (1990), 38–75.
[123] V. Strassen, *Gaussian elimination is not optimal*, Numerische Mathematik **13** (1969), 354–356.
[124] M. Suzuki, *Group Theory I*, 1982.
[125] E. C. Titchmarsh, *The Zeros of the Riemann Zeta-Function*, Proceedings of the Royal Society of London **151** (1935), 234–255.
[126] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, 1951.
[127] A. M. Turing, *Some Calculations of the Riemann Zeta-Function*, Proceedings of the London Mathematical Society **3** (1953), 99–117.
[128] J. M. Vinogradov, *Sur la distribution des résidus et des non-résidus des puissances*, Journal of the Physico-Mathematical Society of Perm **1** (1918), 94–96.
[129] J. M. Vinogradov, *On the Bound of the Least Non-Residue of n-th Powers*, Transactions of the American Mathematical Society **29** (1927), 218–227.
[130] S. Wedeniwski, *Piologie – Eine exakte arithmetische Bibliothek in C++*, Edition 1.0, Technical Report WSI 96-35, available at `www.hipilib.de`, December 1996.
[131] S. Wedeniwski, *Generische Matrizen und die Implementation schneller Matrixoperationen*, Diploma thesis, Universität Tübingen, 1996.
[132] S. Wedeniwski, *Elliptische Kurven in der Kryptologie*, Diploma thesis, Universität Tübingen, 1997.
[133] S. Wedeniwski, $128,000,026$ *Digits of Zeta(3)*, at `http://lacim.uqam.ca/piDATA/Zeta3.txt`, December 1998.
[134] H. C. Williams, J. S. Judd, *Determination of the Primality of N by Using Factors of* $N^2 \pm 1$, Mathematics of Computation **30** (1976), 157–172.
[135] H. C. Williams, J. S. Judd, *Some Algorithms for Prime Testing Using Generalized Lehmer Functions*, Mathematics of Computation **30** (1976), 867–886.
[136] H. C. Williams, *On Numbers Analogous to the Carmichael Numbers*, Canadian Mathematical Bulletin **20** (1977), 133–143.
[137] H. C. Williams, *Primality Testing on a Computer*, Ars Combinatoria **5** (1978), 127–185.
[138] H. C. Williams, *Édouard Lucas and Primality Testing*, 1998.

Lebenslauf

Persönliche Daten:

Name	Sebastian Wedeniwski
Geburtstag	17.10.1971
Geburtsort	Aiud Alba (Rumänien)
Familienstand	verheiratet

Ausbildung und beruflicher Werdegang:

1978 bis 1992	Schulische Ausbildung, Abitur
1992 bis 1993	Zivildienst in der Behindertenanstalt Stetten
1993	Bundessieger des 12. Bundeswettbewerbes Informatik
1993 bis 1997	Doppelstudium der Informatik und Mathematik an der Universität Tübingen
Februar 1997	Diplom in Informatik Diplomarbeit „Generic Matrices and the Implementation of Fast Matrix Operations“
August 1997	Diplom in Mathematik Diplomarbeit „Elliptische Kurven in der Kryptologie“
1996 bis 1998	Wissenschaftlicher Mitarbeiter im Fachbereich Praktische Informatik
1997	Forschungsaufenthalt am Rensselaer Polytechnic Institute, USA
1985 bis 2000	Selbständige Informatiktätigkeiten und Projekte in den Bereichen/Branchen Werkzeugmaschinenbau, Baugewerbe, Automobilindustrie, Arithmetik und Kryptologie
seit 1998	Angestellter der IBM im Bereich ADS Banking Projects
Dezember 1998	Weltrekord bei der Berechnung der Riemannschen Zetafunktion $\zeta(3)$
July 1999	Weltrekord bei der Berechnung der Eulerschen Zahl e
1999	Patentanmeldung „Anzeige von Meldungen mehrerer parallel ablaufender Prozesse“
1998 bis 2001	Promotion an der Mathematischen Fakultät der Universität Tübingen über das Thema „Primality Tests on Commutator Curves“
2001	Patentanmeldung „Delayed Frame in Java for a Waiting Information“