Scan A4119

Golomb

"Properties of ..."

add to 9 seqs

A185565

A2253

A4119

A39687

A259865

A199683

A56807

A259866

A259867

MATHEMATICS OF COMPUTATION, VOLUME 30, NUMBER 135
JULY 1976, PAGES 657–663

f91

Properties of the Sequence $3 \cdot 2^n + 1$

By Solomon W. Golomb*

Abstract. For applications to fast finite field transforms, one is interested in the arithmetic of $GF(p)$, where the order of the multiplicative group, $\varphi(p) = p - 1$, is divisible by a high power of 2, and where the multiplicative order of 2 modulo p is large. Primes of the form $3 \cdot 2^n + 1$ appear well-suited to these objectives. Results are obtained on the divisibility properties of the numbers $A_n = 3 \cdot 2^n + 1$, and on the exponent of 2 modulo A_n when A_n is prime. Generalizations to various related types of sequences are also considered.

1. Introduction. It is frequently of interest to study the divisibility properties of exponentially growing sequences of integers. Many such sequences $\{S_n\}$ have been studied extensively, including the Fibonacci sequence and the Mersenne sequence $(2^n - 1)$, which satisfy $S_0 = 0$, $S_1 = 1$, $S_{n+1} = aS_n + bS_{n-1}$ for $n \geqslant 1$, and $(S_m, S_n) = S_{(m,n)}$. A representative sequence which does not satisfy the $(S_m, S_n) = S_{(m,n)}$ condition is $\{A_n\} = \{3 \cdot 2^n + 1\}$. Its divisibility properties are treated here in some detail.

For applications to fast transforms of the type considered by Rader [1], and by Reed and Truong [2], we are interested in the arithmetic of $GF(p)$, where the order of the multiplicative group, $\varphi(p) = p - 1$, is divisible by a high power of 2, and where the multiplicative order of 2 modulo p is large. Primes of the form $3 \cdot 2^n + 1$ are well-suited to these objectives. We develop results on the factorization of the numbers $A_n = 3 \cdot 2^n + 1$, and on the index of 2 modulo A_n when A_n is prime. Generalizations to related types of sequences are also considered.

2. Factorization Results. Let $A_n = 3 \cdot 2^n + 1$, $n \geqslant 1$. We shall show that there are infinitely many primes q (Type I primes) which divide members of the sequence $\{A_n\}$, and infinitely many primes q (Type II primes) which do not.

THEOREM 1. *A prime q is of Type* I *if and only if* $-3 \equiv 2^k \pmod q$ *for some positive integer k.*

Proof. Clearly q is of Type I if and only if

$$A_n = 3 \cdot 2^n + 1 \equiv 0 \pmod q \quad \text{for some } n,$$

that is, if and only if $3 \cdot 2^n \equiv -1 \pmod q$. Since $2^{q-1} \equiv 1 \pmod q$, we have $-3 \equiv 2^k \pmod q$ with $k = q - n - 1$.

Remark. The Type I primes are all the prime factors of the numbers $2^k + 3$.

Received September 16, 1975; revised December 19, 1975.

AMS (MOS) subject classifications (1970). Primary 10A10, 10A15, 10A25, 10A40, 10L99.

* This research was supported in part by the Air Force Office of Scientific Research under Grant No. AFOSR 75–2798.

These include the primes of the form $2^k + 3$, namely $\{5, 7, 11, 19, 67, 131, \ldots\}$, as well as the prime factors of the composite numbers of this form yielding additionally $\{13, 29, 37, 53, 59, 61, \ldots\}$.

THEOREM 2. *If* $q \equiv 17, 23 \pmod{24}$, *then* q *is of Type* II.

Proof. It follows from $q \equiv 17, 23 \pmod{24}$ that $(2/q) = 1$ and $(-3/q) = -1$. If q were of Type I, then $2^k \equiv -3 \pmod{q}$, so $1 = (2/q)^k = (2^k/q) = (-3/q) = -1$, a contradiction.

(The relevant results of quadratic residue theory used here are:

(i) $(-1/q) = +1$ iff $q \equiv +1 \pmod{4}$,

(ii) $(2/q) = +1$ iff $q \equiv \pm 1 \pmod{8}$, and

(iii) $(3/q) = +1$ iff $q \equiv \pm 1 \pmod{12}$.)

Remark. By Dirichlet's Theorem, there are infinitely many primes $q \equiv 17 \pmod{24}$, including $\{17, 41, 89, 113, 137, \ldots\}$, and also infinitely many primes $q \equiv 23 \pmod{24}$, including $\{23, 47, 71, 167, \ldots\}$. Invoking also the density results on primes in arithmetic progressions, *at least one-fourth of all primes are of Type* II.

The next three results are similar to Theorem 2.

THEOREM 3. *If* $q \equiv 13, 19 \pmod{24}$, *then* q *does not divide* A_{2n+1}.

Proof. If $q \equiv 13, 19 \pmod{24}$, then $(-6/q) = (2/q)(-3/q) = (-1)(+1) = -1$. Also, if $3 \cdot 2^{2n+1} \equiv -1 \pmod{q}$, then $(3 \cdot 2^{n+1})^2 \equiv -6 \pmod{q}$, so

$$1 = \left(\frac{3 \cdot 2^{n+1}}{q}\right)^2 = \left(\frac{(3 \cdot 2^{n+1})^2}{q}\right) = \left(\frac{-6}{q}\right) = -1,$$

a contradiction.

THEOREM 4. *If* q *is a prime and* $q \mid A_{2n+1}$, *then* $q = 1, 5, 7,$ *or* $11 \pmod{24}$.

Note. Examination of Table I reveals that primes in all four of these residue classes modulo 24 are found among the factors of A_{2n+1}.

Proof. This merely combines the results of Theorem 2 and Theorem 3.

THEOREM 5. *If* $q \mid A_{2n}$, q *prime, then* $q \equiv 1 \pmod{6}$.

Note. It is seen in Table I that primes in all four of the residue classes 1, 7, 13, 19 modulo 24 are found among the factors of A_{2n}.

Proof. If $3 \cdot 2^{2n} \equiv -1 \pmod{q}$, then $(3 \cdot 2^n)^2 \equiv -3 \pmod{q}$, so $(-3/q) = 1$, which implies $q \equiv 1 \pmod{6}$.

Note. For even $n = 2m$, $A_n = 1 + 3 \cdot 2^{2m} = 1^2 + 3 \cdot (2^m)^2$ is of the form $a^2 + 3b^2$, and the theory of factorization in the ring $Z(\omega)$ of the Eisenstein integers can also be used to prove Theorem 5.

THEOREM 6. *Let* q *be a prime of Type* I, *and let* n_0 *be the smallest positive integer such that* q *divides* A_{n_0}. *Then* q *divides* A_n *if and only if* $n \equiv n_0 \pmod{e}$, *where* e *is the exponent of* 2 *modulo* q.

Proof. If $q \mid A_n$, then $3 \cdot 2^n \equiv -1 \equiv 3 \cdot 2^{n_0} \pmod{q}$, so $2^{n-n_0} \equiv 1 \pmod{q}$. Hence, $e \mid n - n_0$. If, on the other hand, $e \mid n - n_0$, then $2^{n-n_0} \equiv 1 \pmod{q}$, so $3 \cdot 2^n + 1 \equiv 3 \cdot 2^{n_0} + 1 \equiv 0 \pmod{q}$.

Remark. To determine whether q is of Type I or Type II, it suffices to test whether q divides any of $A_1, A_2, \ldots, A_e$, where e is the exponent of 2 modulo q.

Algorithm. To construct a table (see Table I) of the factors of the numbers A_n, we find for each prime q of Type I the smallest number A_{n_0} divisible by q, and then observe that q divides every eth term thereafter. Thus, when $q = 7$, $e = 3$, and every third term in the sequence $\{A_n\}$ is divisible by 7. Similarly, every fourth term is divisible by 5, etc.

THEOREM 7. *Numbers in the sequence* $\{A_{6n}\}$ *have no prime factors less than* 61. (*Note, however, that* 61 *divides* A_{24} *and* 67 *divides* A_{60}.)

Proof. For each of the primes q of Type I which satisfy Theorem 5, there is an n_0 and an e, depending only on q, such that q divides A_n if and only if $n \equiv n_0 \pmod{e}$. For each such prime < 61, e has a factor in common with 6, and $n_0 + ej$ can never be a multiple of 6, $j = 0, 1, 2, \ldots$. (The direct verification required for this is readily found in Table I.)

THEOREM 8. *There are infinitely many primes of Type* I, *and infinitely many of Type* II.

Proof. By the corollary to Theorem 2, there are infinitely many primes of Type II. To show that there are infinitely many primes of Type I, we use the following proof by contradiction, suggested by L. R. Welch.

Suppose there were only finitely many primes, $q_1, q_2, \ldots, q_k$, which divide the terms of $\{A_n\}$, $n \geqslant 1$. Then $3 \cdot 2^n + 1 = \Pi_{i=1}^k q_i^{e_{in}}$, and modulo the product of those q_i for which $e_{in} > 0$, we have

$$3 \cdot 2^n + 1 = \prod_{i=1}^{k} q_i^{e_{in}} \equiv 0 \quad \left(\mathrm{mod} \prod_{e_{in}>0} q_i\right)$$

for all n. Let $N = \text{L.C.M.}\, \{\varphi(q_1), \varphi(q_2), \ldots, \varphi(q_k)\} > 1$, where φ is Euler's phi-function. Then clearly $2^N \equiv 1 \pmod{\Pi_{e_{iN}>0}\, q_i}$, from which $3 \cdot 2^N + 1 \equiv 4 \pmod{\Pi_{e_{iN}>0}\, q_i}$, which contradicts $3 \cdot 2^N + 1 \equiv 0 \pmod{\Pi_{e_{iN}>0}\, q_i}$, since all the q_i are odd.

3. The Exponent of 2 Modulo p. In this section we will assume that p is a prime of the form $3 \cdot 2^n + 1$. Since $\varphi(p) = 3 \cdot 2^n$, the order of any element in the multiplicative group modulo p is of the form $3^j \cdot 2^k$, where $0 \leqslant j \leqslant 1$ and $0 \leqslant k \leqslant n$. We will specifically be concerned with the order of 2 in this group, i.e. the exponent $e_2(p)$ of 2 modulo p.

THEOREM 9. *If* $p = 3 \cdot 2^n + 1$ *is prime, then* 2 *is not primitive modulo* p *except in the case* $p = 13$. *In fact,* $e_2(p)$ *divides* $3 \cdot 2^{n-1}$ *in all cases except* $p = 13$.

Proof. For 2 to be primitive modulo p, it must be a quadratic nonresidue of p. Hence, $p \equiv \pm 3 \pmod{8}$. But if $n \geqslant 3$, then $p \equiv 1 \pmod{8}$. Also, for $n = 1$, $p = 7 \not\equiv \pm 3 \pmod{8}$. Finally, if $n = 2$, then $p = 13$, for which 2 is primitive.

THEOREM 10. *The exponent of* 2 *modulo a prime* $p = 3 \cdot 2^n + 1$ *fails to be divisible by* 3 *if and only if* p *divides a Fermat number.*

Proof. Suppose $e_2(p) = 2^k$, $0 \leqslant k \leqslant n$. Then $2^{2^k} \equiv 1 \pmod{p}$, and p divides $2^{2^k} - 1 = F_0 F_1 F_2 \cdots F_{k-1}$ where $F_i = 2^{2^i} + 1$. Then in fact p divides F_{k-1}, or else $e_2(p)$ would be less than 2^k. Conversely, if p divides $F_r = 2^{2^r} + 1$, then $2^{2^r} \equiv -1 \pmod{p}$, $2^{2^{r+1}} \equiv 1 \pmod{p}$, and $e_2(p)$ is a divisor of 2^{r+1}, and thus of the form 2^k.

new seq. Please enter (space)

Name: 3·2**N + 1.

A4119 Ref. MTAC 30 660 76. A4119

A181565

A2253

0 4

SSC

Primes are A39687

TABLE I

Factorization of the Numbers $A_n = 3 \cdot 2^n + 1$

n	$3 \cdot 2^n + 1$	Factorization	n	$3 \cdot 2^n + 1$	Factorization
1	7	PRIME	22	12582913	$7 \cdot 313 \cdot 5743$
2	13	PRIME	23	25165825	$5^2 \cdot 1006633$
3	25	5^2	24	50331649	$61 \cdot 825109$
4	49	7^2	25	100663297	$7^3 \cdot 269 \cdot 1091$
5	97	PRIME	26	201326593	$13 \cdot 1567 \cdot 9883$
6	193	PRIME	27	402653185	$5 \cdot 11 \cdot 1399 \cdot 5233$
7	385	$5 \cdot 7 \cdot 11$	28	805306369	$7 \cdot 37 \cdot 139 \cdot 22369$
8	769	PRIME	29	1610612737	$79 \cdot 20387503$
9	1537	$29 \cdot 53$	30	3221225473	PRIME
10	3073	$7 \cdot 439$	31	6442450945	$5 \cdot 7 \cdot 184070027$
11	6145	$5 \cdot 1229$	32	12884901889	$19^2 \cdot 35692249$
12	12289	PRIME	33	25769803777	$13613 \cdot 1893029$
13	24577	$7 \cdot 3511$	34	51539607553	$7 \cdot 181 \cdot 40678459$
14	49153	$13 \cdot 19 \cdot 199$	35	103079215105	$5 \cdot 823 \cdot 25049627$
15	98305	$5 \cdot 19661$	36	206158430209	PRIME
16	196609	$7 \cdot 28087$	37	412316860417	$7 \cdot 11 \cdot 29 \cdot 59 \cdot 3129611$
17	393217	$11 \cdot 35747$	38	824633720833	$13 \cdot 829 \cdot 1063 \cdot 71983$
18	786433	PRIME	39	1649267441665	$5 \cdot 316133 \cdot 1043401$
19	1572865	$5 \cdot 7 \cdot 44939$	40	3298534883329	$7 \cdot 10243 \cdot 46004029$
20	3145729	$727 \cdot 4327$	41	6597069766657	PRIME
21	6291457	$347 \cdot 18131$	42	13194139533313	$103 \cdot 128098442071$

The additional cases known [3] where $3 \cdot 2^n + 1$ is prime occur for $n = 66$, 189, 201, 209, 276, 353, 408, 438, and 534.

COROLLARY. *The exponent of* 2 *modulo a prime* $p = 3 \cdot 2^n + 1$ *fails to be divisible by* 3 *if and only if* p *divides a Fermat number* F_j *with* $j \leqslant n - 1$.

(This is in fact shown in the proof of Theorem 10.)

Note. Two cases where a Fermat number has a prime factor $p = 3 \cdot 2^n + 1$ are known [3], namely $3 \cdot 2^{41} + 1$ divides F_{38}, and $3 \cdot 2^{209} + 1$ divides F_{207}. That n must be odd for p to divide a Fermat number is established in the following theorem of Morehead [4].

THEOREM 11. *If* $p = 3 \cdot 2^{2m} + 1$ *is a prime, then* $e_2(p)$ *must be divisible by* 3. (*Hence, by Theorem* 10, *such a prime cannot divide any Fermat number.*)

A39687

A259865

TABLE II

Exponents of 2 *modulo primes* $p = 3 \cdot 2^n + 1$ ✓

n	$3 \cdot 2^n + 1$ (prime)	Exponent of 2 mod p
1	7	$3 = 3 \cdot 2^{n-1}$
2	13	$12 = 3 \cdot 2^n$
5	97	$48 = 3 \cdot 2^{n-1}$
6	193	$96 = 3 \circ 2^{n-1}$
8	769	$384 = 3 \cdot 2^{n-1}$
12	12289	$6144 = 3 \cdot 2^{n-1}$
18	786433	$393216 = 3 \cdot 2^{n-1}$
30	3221225473	$805306368 = 3 \cdot 2^{n-2}$
36	206158430209	$103079215104 = 3 \cdot 2^{n-1}$
41	6597069766657	$1649267441664 = 3 \cdot 2^{n-2}$

Proof. If and only if 2 is a cubic residue modulo p, $e_2(p)$ will fail to be divisible by 3. The condition for 2 to be a cubic residue modulo a prime p is known [5], and can be stated as follows:

2 is a cubic residue modulo a prime p, $p \equiv 1 \pmod 6$, if and only if there are positive integers a and b such that $p = a^2 + 27b^2$, $a \not\equiv 0 \pmod 3$.

Suppose then that $p = 3 \cdot 2^{2m} + 1 = a^2 + 27b^2$ is prime. Then, factoring over the ring $Z(\omega)$ of the Eisenstein integers, $p = (1 + 2^m\sqrt{-3})(1 - 2^m\sqrt{-3}) = (a + 3b\sqrt{-3})(a - 3b\sqrt{-3})$. However, if $p \equiv 1 \pmod 6$ is prime, it has a unique factorization as a product of two complex conjugate primes in the Eisenstein ring. Since $2^m \neq 3b$, the two factorizations obtained appear distinct. However, to complete the proof, we must verify that the two factorizations do not differ merely by unit factors. The only units in $Z(\omega)$ are the sixth roots of unity, ± 1 and $\pm(1 \pm \sqrt{-3})/2$. Clearly, the two factorizations differ by more than ± 1. Consider then

$$\frac{\pm(1 \pm \sqrt{-3})}{2} \cdot (1 + 2^m\sqrt{-3}) = \pm\left(\frac{1 \pm 3 \cdot 2^m}{2} + \frac{2^m \pm 1}{2}\sqrt{-3}\right).$$

Since $m \geqslant 1$, both coefficients $(1 \pm 3 \cdot 2^m)/2$ and $(2^m \pm 1)/2$ are half-integers, and therefore cannot coincide with those of $a \pm 3b\sqrt{-3}$.

The exponent of 2 modulo p for each prime $p = 3 \cdot 2^n + 1$ of Table I is shown in Table II. When this exponent is divisible by 2^{n-1}, it indicates that 2 is not a quartic residue modulo p. The condition for 2 to be a quartic residue modulo p is known [5], and may be stated as: 2 is a quartic residue modulo p, where $p \equiv 1 \pmod 8$, if and only if there exist positive integers a and b such that $p = a^2 + 64b^2$, $a \not\equiv 0 \pmod 2$.

A199683, A56807,

A259866

TABLE III

Properties of the sequence $3 \cdot 10^n + 1$

A259867

n	Prime factors of $3 \cdot 10^n + 1$	Exponent of 2
1	31	5
2	7 × 43	
3	3001	1500
4	19 × 1579	
5	13 × 47 × 491	
6	853 × 3517	
7	30000001	234375
8	7^2 × 6122449	
9	7589 × 395309	
10	30000000001	300000000
11	13^2 × 1775147929	
12	67 × 44776119403	
13	17 × 23 × 62191 × 1233721	
14	7 × 95773 × 447486691	
15	29 × 103448275862069	
16	31 × 379 × 15901 × 160581649	
17	13 × 2281 × 23911 × 423111547	
18	16921 × 5188801 × 34168681	
19	163 × 184049079754601227	
20	7 × 428571428571428571143	

From Table II, it is seen that 2 is sometimes a quartic residue modulo $p = 3 \cdot 2^n + 1$ and sometimes not. No provable pattern has yet been discerned.

4. Analogous Cases. The factorization properties of the sequence $\{2^n + 3\}$ are very similar to those of the sequence $\{3 \cdot 2^n + 1\}$. The corollary to Theorem 1 states that both of these sequences have the same set of prime factors. As numbers in binary notation, the two sequences are mirror images of each other. Most of the theorems proved for $\{3 \cdot 2^n + 1\}$ have obvious analogues for the sequence $\{2^n + 3\}$. For example, when n is even, $2^n + 3 \equiv 1 \pmod 6$, and when this number is prime, the analogue of Theorem 11 holds, using essentially the same proof.

Let B be any positive even integer which is not a multiple of 3. The general sequence $\{3B^n + 1\}$ has many similarities to the special case $\{3 \cdot 2^n + 1\}$ already considered, and the numbers look particularly simple in base B notation. Moreover, Theorem 11 still holds: When n is even, 3 must divide the exponent of 2 modulo any prime p of the form $3B^n + 1$. (The basic proof technique of Theorem 11 still applies.) However, it is easy, in this more general context, to produce numerous counterexamples when n is odd. Thus, with $B = 10$ and $n = 1$, we get $p = 31 = 2^2 + 27 \cdot 1^2$, and 2 *is* a cubic residue modulo 31. Similarly, with $B = 14$ and $n = 1$, we get $p = 43 = 4^2 + 27 \cdot 1^2$, and 2 *is* a cubic residue modulo 43. In Table III, we see factorizations of numbers of the form $3 \cdot 10^n + 1$, and the exponent of 2 when $3 \cdot 10^n + 1$ is prime.

If one wishes to generalize from the sequence $\{3 \cdot 2^n + 1\}$ to the sequences $\{k \cdot 2^n + 1\}$ for other odd values of k, there are extensive tables available [3], indicating when $k \cdot 2^n + 1$ is prime for all $k < 100$ and all $n < 512$. The basic test for primeness used in [3] was the following theorem of Proth (1878):

THEOREM 12. *Let $N = k \cdot 2^n + 1$ with $0 < k < 2^n$. Choose any a such that $(a/N) = -1$. Then N is prime if and only if $a^{(N-1)/2} \equiv -1 \pmod N$.*

For a proof of this theorem, and a discussion of this and related results, see [6].

The method used in the proof of Theorem 8 can be extended to obtain the following very general result on prime divisors of exponentially growing sequences of integers. The details are left to the reader.

THEOREM 13. *Let $a_1, a_2, \ldots, a_k$ be distinct positive integers such that none is a perfect power of another, with $k > 1$. Let $c_1, c_2, \ldots, c_k$ be nonzero integers. Let $f_1(x), f_2(x), \ldots, f_k(x)$ be polynomials in x with integer coefficients, and positive leading coefficients. Then among the integer terms of the sequence $\{S_n\} = \{c_1a_1^{f_1(n)} + c_2a_2^{f_2(n)} + \cdots + c_ka_k^{f_k(n)}\}$ there are infinitely many distinct prime factors. (The terms S_n will be integers for all sufficiently large values of n, since each of the polynomials $f_i(x)$ takes on only positive values for sufficiently large x.)*

Acknowledgment. Many helpful suggestions by the referee have been incorporated, resulting in the streamlining of wording, format, and proofs.

Departments of Electrical Engineering and Mathematics
University of Southern California
Los Angeles, California 90007

1. C. M. RADER, "Discrete convolutions via Mersenne transforms," *IEEE Trans. Computers*, v. C-21, 1972, pp. 1269–1273.

2. I. S. REED & T. K. TRUONG, "The use of finite fields to compute convolutions," *IEEE Trans. Information Theory*, v. IT-21, 1975, pp. 208–213.

3. R. M. ROBINSON, "A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers," *Proc. Amer. Math. Soc.*, v. 9, 1958, pp. 673–681. MR 20 #3097.

4. J. C. MOREHEAD, "Note on the factors of Fermat's numbers," *Bull. Amer. Math. Soc.*, v. 12, 1906, pp. 449–451.

5. E. LEHMER, "Criteria for cubic and quartic residuacity," *Mathematika*, v. 5, 1958, pp. 20–29. MR 20 #1668.

6. R. M. ROBINSON, "The converse of Fermat's theorem," *Amer. Math. Monthly*, v. 64, 1957, pp. 703–710. MR 20 #4520.