18.781, Fall 2007 Problem Set 5

Solutions to Selected Problems

Problem 2.11.1 By the argument of from 122 page to 123 page, since $9 = 3^2$, the multiplicative group modulo 9 is a cyclic group of order $\phi(9) = 6$. It is clear that the additive group modulo 6 is a cyclic group of order 6. Hence, their isomorphic.

More precisely, define a function $f\colon R_9 \Rightarrow Z_6$ by

$$f(2) = 1, f(4) = 2, f(8) = 3, f(7) = 4, f(5) = 5, f(1) = 0.$$

(For each $a \in R_9$, there is an g such that $2^g \equiv a$ in modulo 9 because 2 is a primitive root of 9, and we define $f(a) = g$ where g lies in modulo 6. This is well defined since 6 is the order of 2 in modulo 9.
Then f is bijective, clearly. To show that f is an isomorphism, we need to show that f is a group homomorphism. For $a, b \in R_9$, there are g, h such that $2^g \equiv a$ and $2^h \equiv b$ in modulo 9. So we have

$$f(ab) \equiv f(2^g \cdot 2^h) == \equiv f(2^{g+h}) \equiv g + h \equiv f(2^g) + f(2^h) \equiv f(a) + f(b) \pmod 6.$$

Therefore f is a group homomorphism. □

Problem 2.11.6 By the argument from 122 page to 123 page, R_m is a cyclic group if and only if $m = 2, 4, p, p^\alpha$. For $2, 3, 4, 5, 6, 7$, each of them is one of the previous form, and 8 is not. Therefore, 8 is the smallest positive integer m such that the multiplicative group modulo m is not cyclic. □

Problem 2.11.11
Solution 1 If we proved that G is a group, it is clear that G is noncommutative because $a \oplus b = d \neq f = b \oplus a$. Looking at the table, we can easily find that e is an identity, and each element of a, b, c, d, f has an inverse element ($a \oplus a = b \oplus b = c \oplus c = e, d \oplus f = f \oplus d = e$).

It remains to prove the associativity. We need to show that $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ for $x, y, z \in \{e, a, b, c, d, f\}$. If one of x, y, z is e, the associativity clearly holds. For the other cases,

For $(x, y, z) = (a, a, a)$, we have $x \oplus (y \oplus z) = a = (x \oplus y) \oplus z$.
For $(x, y, z) = (a, a, b)$, we have $x \oplus (y \oplus z) = b = (x \oplus y) \oplus z$.
For $(x, y, z) = (a, a, c)$, we have $x \oplus (y \oplus z) = c = (x \oplus y) \oplus z$.
For $(x, y, z) = (a, a, d)$, we have $x \oplus (y \oplus z) = d = (x \oplus y) \oplus z$.

For $(x,y,z)=(a,a,f)$, we have $x\oplus(y\oplus z) = f = (x\oplus y)\oplus z$.
For $(x,y,z)=(a,b,a)$, we have $x\oplus(y\oplus z) = c = (x\oplus y)\oplus z$.
For $(x,y,z)=(a,b,b)$, we have $x\oplus(y\oplus z) = a = (x\oplus y)\oplus z$.
For $(x,y,z)=(a,b,c)$, we have $x\oplus(y\oplus z) = b = (x\oplus y)\oplus z$.
For $(x,y,z)=(a,b,d)$, we have $x\oplus(y\oplus z) = f = (x\oplus y)\oplus z$.
For $(x,y,z)=(a,b,f)$, we have $x\oplus(y\oplus z) = e = (x\oplus y)\oplus z$.

$$\vdots$$

For $(x,y,z)=(f,f,a)$, we have $x\oplus(y\oplus z) = c = (x\oplus y)\oplus z$.
For $(x,y,z)=(f,f,b)$, we have $x\oplus(y\oplus z) = a = (x\oplus y)\oplus z$.
For $(x,y,z)=(f,f,c)$, we have $x\oplus(y\oplus z) = b = (x\oplus y)\oplus z$.
For $(x,y,z)=(f,f,d)$, we have $x\oplus(y\oplus z) = f = (x\oplus y)\oplus z$.
For $(x,y,z)=(f,f,f)$, we have $x\oplus(y\oplus z) = e = (x\oplus y)\oplus z$.

Solution 2 As above, it is enough to show that $x\oplus(y\oplus z) = (x\oplus y)\oplus z$ for $x,y,z\in\{e,a,b,c,d,f\}$.
Consider the set of bijective function from the set $\{1,2,3\}$ to itself. This set is composed by 6 elements, namely

e, which is defined by $e(1)=1, e(2)=2, e(3)=3$.
a, which is defined by $a(1)=2, a(2)=1, a(3)=3$.
b, which is defined by $b(1)=1, b(2)=3, b(3)=2$.
c, which is defined by $c(1)=3, c(2)=2, c(3)=1$.
d, which is defined by $d(1)=2, d(2)=3, d(3)=1$.
f, which is defined by $f(1)=3, f(2)=1, f(3)=2$.

If we define the composition of functions as a operation $\oplus$, it can be verified that these satisfy the given table. Since the composition of functions is associative generally, (that is, $f\circ(g\circ h)=(f\circ g)\circ h$.) the operation $\oplus$ which is given by table is clearly associative. $\square$

Problem 3.1.7 (a) Note that for $p = 8k+t$, $\frac{p^2-1}{8} = \frac{(8k+t)^2-1}{8} = 2(4k^2+kt)+\frac{t^2-1}{8}$, and $(-1)^{2(4k^2+kt)}=1$ surely. Then, since $61\equiv 5 \pmod 8$, we can compute that

$$\left(\frac{2}{61}\right) = (-1)^{\frac{61^2-1}{8}} = (-1)^{\frac{5^2-1}{8}} = -1.$$

Therefore, there is no solution for $x^2\equiv 2 \pmod{61}$.

(b) Since $59\equiv 3 \pmod 8$, we can compute that

$$\left(\frac{2}{59}\right) = (-1)^{\frac{59^2-1}{8}} = (-1)^{\frac{3^2-1}{8}} = -1.$$

Therefore, there is no solution for $x^2\equiv 2 \pmod{61}$.

(c) We can compute that

$$\left(\frac{-2}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right) = (-1)^{\frac{61^2-1}{2}}(-1) = (1)\cdot(-1) = -1.$$

Therefore, there is no solution for $x^2 \equiv -2 \pmod{61}$.

(d) We can compute that

$$\left(\frac{-2}{59}\right) = \left(\frac{-1}{59}\right)\left(\frac{2}{59}\right) = (-1)^{\frac{59-1}{2}}(-1) = (-1)\cdot(-1) = 1.$$

Therefore, there are solutions for $x^2 \equiv -2 \pmod{59}$, and by the remark followed by theorem 3.1, the number of solutions is 2.

(e) Since $x^2 \equiv 2 \pmod{122}$ implies that $x^2 \equiv 2 \pmod{61}$, there is no solution by (a).

(f) Since $x^2 \equiv 2 \pmod{118}$ implies that $x^2 \equiv 2 \pmod{59}$, there is no solution by (b).

(g) Since $x^2 \equiv -2 \pmod{122}$ implies that $x^2 \equiv -2 \pmod{61}$, there is no solution by (c).

(h) $x^2 \equiv -2 \pmod{118}$ if and only if $x^2 \equiv -2 \pmod{59}$ and $x^2 \equiv -2 \equiv 0 \pmod{2}$. By (d), there are two solutions of $x^2 \equiv -2 \pmod{59}$, and $x^2 \equiv 0 \pmod{2} \Leftrightarrow x \equiv 0 \pmod{2}$. Therefore, by Chinese remainder theorem, there are two solutions for $x^2 \equiv -2 \pmod{118}$). $\square$.

Problem 3.1.10 By theorem 3.3, $x^2 \equiv 2 \pmod{p}$ has a solution if and only if $\frac{p^2-1}{8}$ is even. Since p is odd, $p \equiv 1,3,5,7 \pmod{8}$. Note again that for $p = 8k+t$, $\frac{p^2-1}{8} = \frac{(8k+t)^2-1}{8} = 2(4k^2+kt) + \frac{t^2-1}{8}$. Therefore, for each $t = 1,3,5,7$, we have $\frac{p^2-1}{8} \equiv 0,1,1,0 \pmod{2}$. In conclusion, $x^2 \equiv 2 \pmod{p}$ has a solution if and only if $p \equiv 1,7 \pmod{8}$. $\square$

Problem 3.1.12

$$\left(\frac{r_1r_2}{p}\right) = \left(\frac{r_1}{p}\right)\left(\frac{r_2}{p}\right) = 1\cdot 1 = 1$$
$$\left(\frac{n_1n_2}{p}\right) = \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right) = (-1)\cdot(-1) = 1$$
$$\left(\frac{rn}{p}\right) = \left(\frac{r}{p}\right)\left(\frac{n}{p}\right) = (1)\cdot(-1) = -1$$

implies that r_1r_2, n_1n_2 are residues and rn is a nonresidue for any odd prime p.

The reduced residue system of 12 is $\{1,5,7,11\}$ and it is easy to verify that the square of each of them is 1 modulo 12. Therefore, 5,7 are nonresidues, and their product is 11, which is also a nonresidue. $\square$

Problem 3.1.17 Denote the first given product $1\cdot 3\cdots(p-2)$ by P, and the second given product $2\cdot 4\cdots(p-1)$ by R. Also denote $(2k+1)!$ by Q. Then

$$1) \text{ By Wilson's theorem, } PR \equiv (-1) \pmod p.$$
$$2) \; Q \equiv 1 \cdot 2 \cdots \cdot (2k+1)$$
$$\equiv 1 \cdot (-2) \cdot 3 \cdot (-4) \cdots (-2k) \cdot (2k+1) \cdot (-1)^k$$
$$\equiv (-1)^k \cdot 1 \cdot (p-2) \cdot 3 \cdot (p-4) \cdots (p-2k) \cdot (2k+1)$$
$$\equiv (-1)^k P \pmod p.$$

For any $a, b \in \{1, 2, \cdots, 2k+1\}$, we have $0 < a + b < p$. This implies that $a \not\equiv -b \pmod p$. Also, since $p = 4k+3$, -1 is a nonresidue. Then by exercise 12, if n is any nonresidue, $-n$ is the quadratic residue. This induces that, since the number of quadratic residue is $2k+1$, by replacing any nonresidue n in Q by the quadratic residue $-n$, we could have all the quadratic residues modulo p. Thus, we can find that

$$3) \; Q \equiv (-1)^{2k+1-m} A \equiv (-1)^{m+1} A \pmod p$$

where A is the product of all quadratic residue modulo p.
Suppose $\{a_1, \cdots, a_{2k+1}\}$ are all quadratic residues, then since $p = 4k+3$, $\{-a_1, \cdots - a_{2k+1}\}$ are all nonresidues, and the union of them is just the reduced residue class modulo p. This implies that $A \cdot (-1)^{2k+1} A \equiv (p-1)! \equiv -1 \pmod p$ by Wilson's theorem. Therefore, $A^2 \equiv 1 \pmod p$, and we have $A \equiv 1 \pmod p$ or $A \equiv -1 \pmod p$. But since A is a product of quadratic residue, A is also a quadratic residue. This implies that $A \neq -1 \pmod p$ since -1 is a nonresidue modulo $p = 4k+3$. Thus $A \equiv 1 \pmod p$.

By 2),3), we have $P \equiv (-1)^k Q \equiv (-1)^{k+m+1} \pmod p$. By 1), we have $R \equiv (-1)^{k+m} \pmod p$, as desired. □

Problem 3.1.18 Recall the theorem 2.37.

If p is a prime and $(a, p) = 1$, then the congruence $x^n \equiv a \pmod p$ has $(n, p-1)$ solutions or no solution according as $a^{\frac{p-1}{(n,p-1)}} \equiv 1 \pmod p$ or not.

Suppose that $p = 3k+2$. Applying the above theorem with $n = 3$, then $(n, p-1) = 1$, hence for any a such that $(a, p) = 1$, $a^{\frac{p-1}{(n,p-1)}} \equiv a^{p-1} \equiv 1 \pmod p$. This implies that all integers in a reduced residue system modulo p are cubic residues.

Now suppose that $p = 3k+1$. Then $(3, p-1) = 3$. By above theorem, $x^3 \equiv a \pmod p$ has 3 solutions or no solution. Consider the set $A = \{1^3, 2^3, \cdots, (p-1)^3\}$. Then A can be divided to $\frac{p-1}{3}$ sets such that the elements of each set are same in modulus p. Those elements give us cubic residues clearly, and there are no other cubic residues because the definition of A. Hence, only one-third of the members of a reduced residue system are cubic residues. □

Problem 3.1.20 If there is an integer x such that $p \mid (x^2+1)$, then $x^2 \equiv -1 \pmod p$. Hence -1 is a quadratic residue modulus p, and this implies that $p \equiv 1 \pmod 4$.

If there is an integer x such that $p \mid (x^2 - 2)$, then $x^2 \equiv 2 \pmod{p}$. Hence 2 is a quadratic residue modulus p, and this implies that $p \equiv 1$ or $7 \pmod 8$ by the exercise 10.

If there is an integer x such that $p \mid (x^2 + 2)$, then $x^2 \equiv -2 \pmod{p}$. Hence -2 is a quadratic residue modulus p. Since $-2 = (-1) \cdot 2$, it implies that (-1) and 2 are both quadratic residues or both nonresidues. So, it is easy to verify that $p \equiv 1$ or $3 \pmod 8$ using previous two observations.

If there is an integer x such that $p \mid (x^4 + 1)$, then $x^4 \equiv -1 \pmod{p}$ has a solution. By theorem 2.37, this implies that $(-1)^{\frac{p-1}{(4,p-1)}} \equiv 1 \pmod{p}$. Therefore, $\frac{p-1}{(4,p-1)}$ should be even number. When we think of $p = 8k+1, 8k+3, 8k+5, 8k+7$, we can easily find that only $p = 8k+1$ make it even.

Suppose that there are only finitely many primes of the form $8n+1$. Let $p_1, \cdots, p_a$ are all the such prime numbers. Consider the number $P = 16(p_1 \cdots p_a)^4 + 1$. Since $P > 2$ (17 is a prime of the form $8n+1$), there exist an prime number p which divides $P = (2p_1 \cdots p_a)^4 + 1$. By above observation, $p = 8k+1$, but p cannot be any of p_i since $(p_i, P) = 1$. This is a contradiction. Thus there are infinitely many primes of the form $8n+1$.

Remark *I added an coefficient 16 to make P an odd number. If you want to let $P = (p_1 \cdots p_a)^4 + 1$, you should explain that P is not of the form 2^t, (which is also easy to prove), to make sure that P has an odd prime factor.*

Suppose that there are only finitely many primes of the form $8n+3$. Let $q_1, \cdots, q_b$ are all the such prime numbers. Consider the number $Q = (q_1 \cdots q_b)^2 + 2$. Note that $Q > 1$. By above observation, any prime factor of Q have the form $q = 8k+1$ or $q = 8k+3$. If all the prime factors of Q have the form $8k+1$, then their product should be of the form $8k+1$, too. But $Q \equiv 3 \pmod 8$ (Note that the square of odd number is 1 in modulo 8), so it is impossible. This implies that there exist an prime number $q = 8k+3$ which divides Q. But q cannot be any of q_i since $(q_i, Q) = (q_i, 2) = 1$. This is a contradiction. Thus there are infinitely many primes of the form $8n+3$.

Suppose that there are only finitely many primes of the form $8n+5$. Let $r_1, \cdots, r_c$ are all the such prime numbers. Consider the number $R = 4(r_1 \cdots r_c)^2 + 1$. By above observation, any prime factor of $R = (2r_1 \cdots r_c)^2 + 1$ have the form $r = 8k+1$ or $r = 8k+5$. If all the prime factors of R have the form $8k+1$, then their product should be of the form $8k+1$, too. But $R \equiv 5 \pmod 8$, so it is impossible. This implies that there exist an prime number $r = 8k+5$ which divides R. But r cannot be any of r_i since $(r_i, R) = 1$. This is a contradiction. Thus there are infinitely many primes of the form $8n+5$.

Suppose that there are only finitely many primes of the form $8n+7$. Let $s_1, \cdots, s_d$ are all the such prime numbers. Consider the number $S = (s_1 \cdots s_d)^2 - 2$. Note that $S > 1$ (7 is a prime of the form $8n+7$). By above observation, any prime factor of S have the form $s = 8k+1$ or $s = 8k+7$. If all the prime factors of S have the form $8k+1$, then their product should be of the form $8k+1$, too. But $S \equiv 7 \pmod 8$, so it is impossible. This implies that there exist an prime number $s = 8k + 7$ which divides S. But s cannot be any of s_i since $(s_i, S) = (s_i, 2) = 1$. This is a contradiction. Thus there are infinitely many primes of the form $8n + 7$. $\square$

If you have any question, please contact me : Yoonsuk Hyun (yshyun@math.mit.edu)