18.781, Fall 2007 Problem Set 4

Solutions to Selected Problems

Problem 2.7.2 You may want to solve this problem by taking x as 0 through 6 and find the value of x which makes the given equation true. It might be easier, but here we will use the Theorem 2.29.

Since $(4,7) = 1$, by multiplying 4, the given equation has same solution with

$$x^3 + 6x^2 + 3x + 4 \equiv 0 \pmod 7.$$

Since degree of this equation is 3, if we show that x^3+6x^2+3x+4 is a factor of x^7-x modulo 7, we can conclude that $x^3 + 6x^2 + 3x + 4 \equiv 0 \pmod 7$ has three solutions by Theorem 2.29. Keeping the fact that every coefficient is in modulo 7 in your mind, divide $x^7 - x$ by $x^3 + 6x^2 + 3x + 4$. Then we can calculate like following :

$$\begin{gathered}
(x^7 - x) - (x^3 + 6x^2 + 3x + 4)(x^4) \equiv (x^6 + 4x^5 + 3x^4 - x) \\
(x^6 + 4x^5 + 3x^4 - x) - (x^3 + 6x^2 + 3x + 4)(x^3) \equiv (5x^5 + 3x^3 - x) \\
(5x^5 + 3x^3 - x) - (x^3 + 6x^2 + 3x + 4)(5x^2) \equiv 5x^4 + 2x^3 + x^2 - x \\
(5x^4 + 2x^3 + x^2 - x) - (x^3 + 6x^2 + 3x + 4)(5x) \equiv 0
\end{gathered}$$

This implies that $x^3 + 6x^2 + 3x + 4$ is a factor of $x^7 - x$ modulo 7, so we've done. □

Problem 2.7.3 We can find that

$$x^{14} + 12x^2 \equiv x^{14} - x^2 \equiv x(x^{13} - x) \pmod{13}.$$

Since $(x^{13} - x) \equiv 0 \pmod{13}$ for all integer x by Fermat's theorem, $x^{14} + 12x^2 \equiv 0 \pmod{13}$ has 13 solutions. □

Problem 2.7.4 First of all, if the degree of f is strictly less than 1, $f(x) \equiv 0 \pmod{p}$ has a solution if and only if $f(x)$ is identically zero. Then if we let $q(x) = 0$, we get a desired conclusion. Now assume that degree of $f > 0$.
We will use an induction on j. Before proceeding, we prove the following claim :

Suppose that $f(x) \equiv 0 \pmod{p}$ has a solution $x \equiv a \pmod{p}$. Then there is a polynomial $q(x)$ such that $f(x) \equiv (x - a)q(x) \pmod{p}$.

Dividing $f(x)$ by $(x-a)$, we have $f(x) \equiv (x-a)q(x) + r(x) \pmod{p}$ where $\deg(r) < 1$, that is, $r(x)$ is constant in modulo p. Since $f(a) \equiv 0 \pmod{p}$, $r(a) \equiv 0 \pmod{p}$. Hence $r(x) \equiv 0$ in modulo p, so we can find that $f(x) \equiv (x-a)q(x) \pmod{p}$.

Now we prove the statement of problem by induction. The case of $j = 1$ is just proved by the claim. Suppose that the statement is true for $j = k$, and consider the case of $j = k+1$. Because that $f(x) \equiv 0 \pmod{p}$ has k solutions, we can say that $f(x) \equiv (x-a_1)(x-a_2)\cdots(x-a_k)q(x) \pmod{p}$. Applying $x = a_{k+1}$, we have

$$0 \equiv f(a_{k+1}) \equiv (a_{k+1} - a_1)(a_{k+1} - a_2)\cdots(a_{k+1} - a_k)q(a_{k+1}) \pmod{p}$$

Since a_{k+1} is different from $a_1, \cdots, a_k$ in modulo p, $(a_{k+1} - a_i)$ is not 0 for $i = 1, \cdots, k$. Therefore, $q(a_{k+1}) \equiv 0 \pmod{p}$. By the above claim, we have $q(x) \equiv (x - a_{k+1})s(x) \pmod{p}$. With the fact that $f(x) \equiv (x-a_1)(x-a_2)\cdots(x-a_k)q(x) \pmod{p}$, we can conclude that $f(x) \equiv (x-a_1)(x-a_2)\cdots(x-a_k)(x-a_{k+1})s(x) \pmod{p}$. Hence the statement is true for $j = k+1$. This completes the proof. $\square$.

Problem 2.8.2 We should find a such that $a^{22} \equiv 1 \pmod{23}$ and $a^i \not\equiv 1 \pmod{23}$ for any other $i \mid 22$. Note that the positive divisors of 22 are $1, 2, 11, 22$.

For the case $a = 2$, we can find that

$$2^{11} \equiv 2048 \equiv 23 \cdot 89 + 1 \equiv 1 \pmod{23}$$

.

Therefore the order of 2 modulo 23 is ≤ 11, (Actually, is equal to 11), so 2 is not a primitive root of 23.

For the case $a = 3$, we can find that

$$3^{11} \equiv (3^3)^3 \cdot 3^2 \equiv 27^3 \cdot 9 \equiv 4^3 \cdot 9 \equiv (-5) \cdot 9 \equiv -45 \equiv 1 \pmod{23}$$

.

Therefore, the order of 3 modulo 23 is ≤ 11, (Actually, is equal to 11), so 3 is not a primitive root of 23.

For the case $a = 5$, we can find that

$$5^1 \not\equiv 1 \pmod{23},$$

$$5^2 \equiv 2 \not\equiv 1 \pmod{23},$$

$$5^{11} \equiv 25^5 \cdot 5 \equiv 2^5 \cdot 5 = 160 \equiv -1 \not\equiv 1 \pmod{23}.$$

$5^{22} \equiv 1 \pmod{23}$ is clearly true by Euler's theorem, hence 5 is a primitive root of 23.

(Of course, the cases of $a = 2$ and $a = 3$ are needless when you have *good intuition* or *good luck* or page 514.)

$\square$

Problem 2.8.6 Suppose that $a^i \equiv a^j \pmod{m}$ for some different $i, j \in \{1, \cdots h\}$. Without loss of generality, we may assume that $i > j$. Then $a^{i-j} \equiv 1 \pmod{m}$ where $1 \leq i - j < h$. But by definition, h is the smallest positive integer such that $a^h \equiv 1 \pmod{m}$, hence this is a contradiction. Therefore, no two of them are congruent modulo m. □

Problem 2.8.9 Let h be the order of 3 modulo 17. By Euler's theorem, we already have $3^{16} \equiv 1 \pmod{17}$. Therefore, $h \mid 16$. Because of $16 = 2^4$, if $h \nmid 2^3$,then $h = 16$. But $3^8 \equiv -1 \not\equiv 1 \pmod{17}$ implies that $h \nmid 2^3$. Thus we can have $h = 16$, which implies that 3 is the primitive root of 17. □

Problem 2.8.14 Let $\bar{a}$ has order of $\bar{h}$ modulo p. From

$$1 \equiv 1^h \equiv (a\bar{a})^h \equiv a^h \cdot \bar{a}^h \equiv \bar{a}^h \,(\text{mod} p),$$

we can find that $\bar{h} \mid h$. Also, from

$$1 \equiv 1^{\bar{h}} \equiv (a\bar{a})^{\bar{h}} \equiv a^{\bar{h}} \cdot \bar{a}^{\bar{h}} \equiv a^{\bar{h}} \,(\text{mod} p),$$

we can find that $h \mid \bar{h}$. Therefore, $h = \bar{h}$.

From $a \equiv g^i \pmod{p}$, multiplying $\bar{a}$ by both sides, we have

$$\bar{a} \cdot g^i \equiv \bar{a}a \equiv 1 \equiv g^{p-1} (\text{ mod } p).$$

Since $i < p - 1$, we can conclude that $\bar{a} \equiv g^{p-1-i} (\text{ mod } p)$, as desired. □

Problem 2.8.18 The fact that g is a primitive root of p implies that $g^i \not\equiv 1 \pmod{p}$ for any integer $0 < i < p - 1$. In particular, $g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. The proof of Corollary 2.38 implies that this gives $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Similarly, $g'^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Thus we can find that

$$(gg')^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} g'^{\frac{p-1}{2}} \equiv (-1) \cdot (-1) \equiv 1 (\text{mod} p).$$

Hence gg' has order equal to or less than $\frac{p-1}{2}$, so gg' is not a primitive root of p. □

We need to solve more exercises to prove the statement of Exercise 2.8.27.

Problem 2.8.25 Express m as $m = \prod p^\alpha$. Then

$$a^{m-1} \equiv 1 (\text{mod} m) \quad \Leftrightarrow \quad a^{m-1} \equiv 1 (\text{mod} p^\alpha) \text{ for each } p \text{ such that } p \mid m.$$

By Corollary 2.42, $x^{m-1} \equiv 1 (\text{mod} p^\alpha)$ has $(m - 1, \phi(p^\alpha))$ solutions modulo p^α. Here, $\phi(p^\alpha) = p^{\alpha-1}(p-1)$. Also, $p \mid m$ implies that $(p, m-1) = 1$. Therefore, $(m-1, \phi(p^\alpha)) = (m-1, p-1)$. In short, $x^{m-1} \equiv 1 (\text{mod} p^\alpha)$ has $(m - 1, p - 1)$ solutions for each $p \mid m$. By Chinese remainder theorem, we can conclude that $x^{m-1} \equiv 1 \pmod{m}$ has exactly $\prod_{p|m}(p - 1, m - 1)$ solutions, which is the claim in Exercise 25. □

Problem 2.8.26 First we show that if m is a Carmichael number, m is composite, square-free and $(p-1) \mid (m-1)$ for all primes p dividing m.

m is composite by definition of Carmichael number in page 59. By Exercise 25, the number of reduced residues a (mod m) such that $a^{m-1} \equiv 1$ (mod m) is exactly $\prod_{p|m}(p-1, m-1)$. Since m is a Carmichael number, all the reduced residues a (mod m) satisfy $a^{m-1} \equiv 1$ (mod m). Therefore, we can have

$$\phi(m) = \prod_{p|m}(p-1, m-1).$$

But when $m = \prod p^{\alpha}$,

$$\phi(m) = \prod_{p|m} p^{\alpha-1}(p-1) \geq \prod_{p|m}(p-1) \geq \prod_{p|m}(p-1, m-1),$$

thus all the equality should hold. This implies that each α should be 1 and $(p-1, m-1) = (p-1)$ which means that $(p-1) \mid (m-1)$.

Now we assume that m is composite, square-free and $(p-1) \mid (m-1)$ for all primes p dividing m. Then these condition give us $\phi(m) = \prod_{p|m}(p-1, m-1)$ as we just observed. By exercise 25, that is the number reduced residues a (mod m) satisfy $a^{m-1} \equiv 1$ (mod m). Since that is equal to $\phi(m)$, all the reduced residues a (mod m) satisfy $a^{m-1} \equiv 1$ (mod m). Because m is composite, we can conclude that m is a Carmichael number. □

Problem 2.8.27 First assume that m is composite and $a^m \equiv a$ (mod m) for all integers a. Then for any a such that $(a, m) = 1$, we can divide the both side of congruence by a, so we have $a^{m-1} \equiv 1$ (mod m). By definition, m is a Carmichael number.

Now assume that m is a Carmichael number. Then m is a composite number by definition. Also by Exercise 26, m is square-free and $(p-1) \mid (m-1)$ for any $p \mid m$.

Fix any prime p such that $p \mid m$. For an integer a such that $(a, p) = 1$, $a^{p-1} \equiv 1$ (mod p). Since $(p-1) \mid (m-1)$, this gives $a^{m-1} \equiv 1$ (mod p), hence, $a^m \equiv a$ (mod p). For an integer a such that $p \mid a$, clearly $a^m \equiv 0 \equiv a$ (mod p).

In conclusion, for any integer a and for any prime p such that $p \mid m$, $a^m \equiv a$ (mod p). This implies that for any integer a, $a^m \equiv a$ (mod $\prod_{p|m} p$), where $\prod_{p|m} p = m$ since m is square-free. Thus we complete the proof. □

Problem 2.8.31 First we prove the following claim.

For the rational number r, its decimal expansion
$r = \sum_{i=-\infty}^{m}(r_i 10^i) = r_m r_{m-1} \cdots r_0 . r_{-1} r_{-2} \cdots$ where $r_m \neq 0$ (m may be negative)
is periodic with period k if and only if $(10^{k-m}r - 10^{-m}r)$ is an integer.

Suppose there exist a rational number r whose decimal expansion $r = \sum_{i=-\infty}^{m}(r_i 10^i) = r_m r_{m-1} \cdots r_0 . r_{-1} r_{-2} \cdots$ where $r_m \neq 0$ (m may be negative).

If this expression is periodic with period k, then $10^{k-m}r$ and $10^{-m}r$ have same fractional part. That is, $10^{k-m}r - 10^{-m}r$ is an integer.

Conversely, Suppose that there is k such that $10^{k-m}r - 10^{-m}r$ is an integer. Then $10^{k-m}r$ and $10^{-m}r$ have same fractional part. Therefore, we have

$$\begin{array}{c} r_m r_{m-1} \cdots r_{m-k+1} \quad . \quad r_{m-k} \cdots r_{m-2k+1} \quad r_{m-2k} \cdots r_{m-3k+1} \quad r_{m-3k} \cdots \\ \| \\ 0 \quad . \quad r_m r_{m-1} \cdots r_{m-k+1} \quad r_{m-k} \cdots r_{m-2k+1} \quad r_{m-2k} \cdots \end{array}$$

Since the fractional parts are equal, by comparing first k terms of fractional part, the expression $r_m \cdots r_{m-k+1}$ is same with $r_{m-k} \cdots r_{m-2k+1}$. Comparing next k terms, the expression $r_{m-k} \cdots r_{m-2k+1}$ is identical with $r_{m-2k} \cdots r_{m-3k+1}$.
By comparing repeatedly, we can have that the decimal expansion of r is periodic. (To make this argument precise, you may use an induction.)

Now we prove the original problem. Suppose that the decimal expansion of $\frac{1}{p}$ has period $p-1$. It means that the decimal expansion of $\frac{1}{p}$ is periodic with **least** period $p-1$. Let $r = \frac{1}{p}$ and m be the number which appears in the above argument. Since $\frac{1}{p} < 1$, m is **negative**. By the above claim, $10^{p-1-m}r - 10^{-m}r$ is an integer. That is,

$$10^{-m}\frac{10^{p-1}-1}{p}$$

is an integer. It is easy to verify that p is neither 2 nor 5 in this assumption. Therefore p cannot divide 10^{-m}. Hence we can conclude that $10^{p-1} \equiv 1 \pmod{p}$. For any other k $(1 < k < p-1)$, If $10^k \equiv 1 \pmod{p}$,$10^{-m}\frac{10^k-1}{p}$ becomes an integer, so by the above claim,the decimal expansion of $\frac{1}{p}$ is periodic with period k, which is absurd. Therefore, $10^k \not\equiv 1$ (mod p) for each $(1 < k < p-1)$, and we can conclude that 10 is a primitive root of p.

Conversely, If 10 is the primitive root of p, it is clear that $10^{p-1-m}r - 10^{-m}r$ is an integer because $10^{p-1} \equiv 1 \pmod{p}$ and m is negative. For any k $(1 \le k < p-1)$, $10^{k-m}r - 10^{-m}r$ is not an integer because

1) $10^k \not\equiv 1 \pmod{p}$ implies that $10^k - 1$ is not a multiple of p.
2) The fact 10 is the primitive root of p implies that p is neither 2 nor 5, hence 10^{-m} is not a multiple of p.

Thus the decimal expansion of $\frac{1}{p}$ is periodic with **least** period $p-1$, as desired. □

We need to solve more exercises to prove the statement of Exercise 2.8.35.

Problem 2.8.33 It is clear that $a^k \equiv 1 \pmod{(a^k-1)}$. For any $0 < i < k$, $0 < a^i - 1 < a^k - 1$, so $a^i \not\equiv 1 \pmod{(a^k-1)}$. This means that k is the order of a modulo (a^k-1). Since $(a, a^k-1) = 1$, it is also clear that $a^{\phi(a^k-1)} \equiv 1 \pmod{(a^k-1)}$ by Euler's theorem. Therefore, $k \mid \phi(a^k-1)$, as desired. □

Problem 2.8.34 Express m as $m = \prod_{q|m} q^{\alpha}$. Then $\phi(m) = \prod_{q|m} q^{\alpha-1}(q-1)$. Since $p \mid \phi(m)$, $p = q$ or $p \mid (q-1)$ for some q such that $q \mid m$. But the previous case never happen because $p \nmid m$. Therefore there is a prime factor q of m such that $p \mid (q-1)$, that is, $q \equiv 1 \pmod{p}$. $\square$

Problem 2.8.35 Suppose that there are only finitely many prime numbers $q \equiv 1 \pmod{p}$. Let $q_1, \cdots, q_r$ are all the such primes. Let $a = pq_1q_2\cdots q_r$ and $k = p$. By applying Exercise 33, we have

$$p \mid \phi((pq_1q_2\cdots q_r)^p - 1).$$

If we let $m = (pq_1q_2\cdots q_r)^p - 1$, then $p \mid \phi(m)$ and $p \nmid m$. Thus by Exercise 34, there is a prime factor q of m such that $q \equiv 1 \pmod{p}$. By our assumption, q should be one of $q_1, \cdots, q_r$. But it is clear that $(m, q_i) = 1$ for each $i = 1, \cdots, r$, hence $q \nmid m$, this is a contradiction. Therefore there exist infinitely many prime numbers $q \equiv 1 \pmod{p}$. $\square$

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