18.781, Fall 2007 Problem Set 3

Solutions to Selected Problems

Problem 2.3.17 First of all, we can observe that $143 = 11 \cdot 13$ and

$$x^3 - 9x^2 + 23x - 15 = (x-1)(x-3)(x-5).$$

Hence, x is a solution of given equation if and only if

$$(x-1)(x-3)(x-5) \equiv 0 (\text{mod } 11) \text{ and } (x-1)(x-3)(x-5) \equiv 0 (\text{mod } 13).$$

Clearly, this means that

$$x \equiv 1, 3, 5 (\text{mod } 11) \text{ and } x \equiv 1, 3, 5 (\text{mod } 13).$$

Using the relation $6 \cdot 11 + (-5) \cdot 13 = 1$, we have

$$x \equiv a_1 (\text{mod } 11) \text{ and } x \equiv a_2 (\text{mod } 13)$$
$$\Updownarrow$$
$$x \equiv -65a_1 + 66a_2 (\text{mod } 143).$$

(Using the Chinese Remainder theorem with $m_1 = 11, m_2 = 13, b_1 = -5, b_2 = 6.$)

Therefore, we can conclude that the solutions are

$$\text{For } (a_1, a_2) = (1,1), \ x \equiv 1 (\text{mod } 143).$$
$$\text{For } (a_1, a_2) = (1,3), \ x \equiv 133 (\text{mod } 143).$$
$$\text{For } (a_1, a_2) = (1,5), \ x \equiv 265 \equiv 122 (\text{mod } 143).$$
$$\text{For } (a_1, a_2) = (3,1), \ x \equiv -129 \equiv 14 (\text{mod } 143).$$
$$\text{For } (a_1, a_2) = (3,3), \ x \equiv 3 (\text{mod } 143).$$
$$\text{For } (a_1, a_2) = (3,5), \ x \equiv 135 (\text{mod } 143).$$
$$\text{For } (a_1, a_2) = (5,1), \ x \equiv -259 \equiv 27 (\text{mod } 143).$$
$$\text{For } (a_1, a_2) = (5,3), \ x \equiv -127 \equiv 16 (\text{mod } 143).$$
$$\text{For } (a_1, a_2) = (5,5), \ x \equiv 5 (\text{mod } 143).$$

□

Problem 2.3.21 First we prove "if" part. This is quite trivial. Suppose that $a_i \equiv a_r \pmod{p^{\alpha_i}}$ for $i = 1, 2, \cdots, r$. Then $x = a_r$ is the solution of the given system.

Now we prove "only if" part. Suppose that there is a simultaneous solution x. Then for any i, $x \equiv a_i \pmod{p^{\alpha_i}}$, hence we can express x as $x = a_i + t_i p^{\alpha_i}$.
Then for fixed i, $a_i + t_i p^{\alpha_i} = x = a_r + t_r p^{\alpha_r}$, that is,

$$a_i - a_r = t_r p^{\alpha_r} - t_i p^{\alpha_i} = p^{\alpha_i}(t_r p^{\alpha_r - \alpha_i} - t_i),$$

where $\alpha_r - \alpha_i \geq 0$.
This gives that $a_i \equiv a_r \pmod{p^{\alpha_i}}$ for $i = 1, 2, \cdots, r$. □

Problem 2.3.29 For any even positive integer n, we can express n as $n = 2^t m$ where $(2, m) = 1$ and $t \geq 1$. Then

$$\phi(2n) = \phi(2^{t+1}m) = \phi(2^{t+1})\phi(m) = (2^{t+1} - 2^t)\phi(m) = 2^t\phi(m)$$

$$\phi(n) = \phi(2^t m) = \phi(2^t)\phi(m) = (2^t - 2^{t-1})\phi(m) = 2^{t-1}\phi(m)$$

Thus $\phi(2n) = \phi(n)$ if and only if $2^t = 2^{t-1}$, which never happen. Therefore, there is no such even number n.

For any odd positive integer n, $(2, n) = 1$. Then $\phi(2n) = \phi(2)\phi(n) = 1 \cdot \phi(n) = \phi(n)$. Therefore, every odd number n satisfies the given equation. □

Problem 2.3.32 Suppose that x satisfying $\phi(x) = 24$. If x has the canonical factorization $\prod p^\alpha$, then $p^{\alpha-1}(p-1) \mid \phi(x) = 24$, in particular, we have $(p-1) \mid 24$. Since all the positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, the possible values of p are $2, 3, 5, 7, 13$. (4, 9, 25 are not prime numbers.)
Now let's say $x = 2^{a_1}3^{a_2}5^{a_3}7^{a_4}13^{a_5}$. For each p, to satisfy $p^{\alpha-1}(p-1) \mid \phi(x) = 24$, it is easily verified that

a_1 can be $0, 1, 2, 3, 4$, and for each case, $\phi(2^{a_1}) = 1, 1, 2, 4, 8$, respectively.
a_2 can be $0, 1, 2$, and for each case, $\phi(3^{a_2}) = 1, 2, 6$, respectively.
a_3 can be $0, 1$, and for each case, $\phi(5^{a_3}) = 1, 4$, respectively.
a_4 can be $0, 1$, and for each case, $\phi(7^{a_4}) = 1, 6$, respectively.
a_5 can be $0, 1$, and for each case, $\phi(13^{a_2}) = 1, 12$, respectively.

We should find the proper $(a_1, a_2, a_3, a_4, a_5)$ such that $\phi(x) = \phi(2^{a_1})\phi(3^{a_2})\phi(5^{a_3})\phi(7^{a_4})\phi(13^{a_2}) = 24$.
Because that $3 \mid 24$, we can say that $\phi(3^{a_2}) = 6$ or $\phi(7^{a_4}) = 6$ or $\phi(13^{a_2}) = 12$ should hold. That is, $a_2 = 2$ or $a_4 = 1$ or $a_5 = 1$.

If $a_2 = 2$, $\phi(2^{a_1})\phi(5^{a_3})\phi(7^{a_4})\phi(13^{a_2}) = 4$, therefore, we have

$$(a_1, a_2, a_3, a_4, a_5) = (0, 2, 1, 0, 0), (1, 2, 1, 0, 0), (3, 2, 0, 0, 0).$$

If $a_4 = 1$, $\phi(2^{a_1})\phi(3^{a_2})\phi(5^{a_3})\phi(13^{a_2}) = 4$, therefore, we have

$$(a_1, a_2, a_3, a_4, a_5) = (0, 0, 1, 1, 0), (1, 0, 1, 1, 0), (3, 0, 0, 1, 0), (2, 1, 0, 1, 0).$$

If $a_5 = 1$, $\phi(2^{a_1})\phi(3^{a_2})\phi(5^{a_3})\phi(7^{a_4}) = 2$, therefore, we have

$$(a_1, a_2, a_3, a_4, a_5) = (0, 1, 0, 0, 1), (1, 1, 0, 0, 1), (2, 0, 0, 0, 1).$$

Thus we can conclude that the solutions are

$$x = 45, 90, 72, 35, 70, 56, 84, 39, 78, 52.$$

□

Problem 2.3.37 It is easy to find that $\phi(100) = 40$. Hence by Euler's theorem we have $3^{40} \equiv 1 \pmod{100}$.
Since each a_i is odd, we have $a_{i+1} = 3^{a_i} \equiv (-1)^{a_i} \equiv 3 \pmod 4$. Also note that $3^4 = 81 \equiv 1 \pmod{40}$. Then for each $i \geq 1$,

$$a_{i+1} = 3^{a_i} = 3^{4k+3} = 81^k \cdot 27 \equiv 27 (\text{mod } 40)$$

Hence

$$a_{i+2} = 3^{a_{i+1}} = 3^{40t+27} = (3^{40})^t \cdot 3^{27} = 3^{27} (\text{mod } 100).$$

So we have now that $a_j \equiv 3^{27} (\text{mod } 100)$ for $j \geq 3$. Also,

$$3^{27} = (3^4)^6 \cdot 3^3 = 81^6 \cdot 27 = (80+1)^6 \cdot 27 = (80^6 + \cdots + 6 \cdot 80 + 1) \cdot 27 \equiv 481 \cdot 27 \equiv 81 \cdot 27 \equiv 87 (\text{mod } 100).$$

Therefore we can conclude that the given sequence (mod 100) is nothing but

$$3, 27, 87, 87, 87, 87, 87, \cdots$$

□

Problem 2.3.44 If $m = 1$, there is nothing to prove. Now assume that $m > 1$.
Let I be the set of prime factors p of m which satisfy $(a, p) > 1$ (That is, $p \mid a$). Then m can be factorized by $m = (\prod_{p \in I} p^\alpha) \cdot M$, where $(a, M) = 1$. Also note that $(\prod_{p \in I} p^\alpha, M) = 1$ by our setting, hence $\phi(M) \mid \phi(m)$.

By usual Euler's theorem, $a^{\phi(M)} \equiv 1 \pmod M$, so with the fact $\phi(M) \mid \phi(m)$, we have $a^{\phi(m)} \equiv 1 \pmod M$. Multiplying $a^{m-\phi(m)}$ to both sides and subtracting, we have

$$a^m - a^{m-\phi(m)} \equiv 0 (\text{mod} M).$$

Now for each $p \in I$, since $p \mid a$, we have $p^{m-\phi(m)} \mid (a^m - a^{m-\phi(m)})$. We know that $p^\alpha \mid m$ and $p^{\alpha-1} \mid \phi(m)$. Thus $p^{\alpha-1} \mid (m - \phi(m))$. With the fact $m - \phi(m) > 0$, we have $m - \phi(m) \geq p^{\alpha-1}$. Now let's prove the following :

Claim : $a^{x-1} \geq x$ holds for $a \geq 2$ and positive integer x.

It is enough to show the case of $a = 2$ holds because $a^{x-1} \geq 2^{x-1}$.
If $x = 1$, it is clearly true. If $x \geq 2$, consider 2^{x-1} as a binomial expansion $(1+1)^{x-1}$. Then it has x terms, and each term is clearly ≥ 1. Hence the above inequality holds.

By this claim, we can find that $\alpha \leq p^{\alpha-1}$. Thus, with the facts that $p^{m-\phi(m)} \mid (a^m - a^{m-\phi(m)})$ and $m - \phi(m) \geq p^{\alpha-1}$, we get

$$p^\alpha \mid (a^m - a^{m-\phi(m)})$$

for each p^α.

Therefore, $(a^m - a^{m-\phi(m)})$ is a multiple of $(\prod_{p\in I} p^\alpha)$. Combining with $a^m - a^{m-\phi(m)} \equiv 0(\text{mod} M)$, we can conclude that

$$a^m \equiv a^{m-\phi(m)}(\text{mod} m).$$

as desired. □

Problem 2.6.3 First we note that $x \equiv 4 \pmod 5$ is the only solution of $x^3 + x + 57 \equiv 0 \pmod 5$. For the simplicity of computation, say that $x \equiv (-1) \pmod 5$ is the solution.
Since $f'(x) = 3x^2 + 1$, we see that $f'(-1) = 4 \not\equiv 0 \pmod 5$, so this root is nonsingular. Taking $f'(\bar{1}) = (-1)$, we see by (2.6) on page 87 that the root $a = (-1) \pmod 5$ lifts to $a_2 = (-1) - f(-1) \cdot (-1) = (-1) - 55 \cdot (-1) = 54$. Since a_2 is considered (mod 5^2), we may take instead $a_2 = 4$.
Then $a_3 = 4 - f(4) \cdot (-1) = 4 - 125 \cdot (-1) = 129 \equiv 4$ (mod 5^3). Thus we conclude that 4 is the desired root and that there are no others. □

Problem 2.6.10 We will use an induction on j. If $j = 1$, it's just the given assumption, so the solution exists. Now assume that $x^2 \equiv a$ (mod p^j) has a solution. Let that solution be b. For $f(x) = x^2 - a$, $f'(x) = 2x$. Because $b^2 \equiv a$ (mod p^j)and $a \not\equiv 0$ (mod p), we have $b \not\equiv 0$ (mod p). Therefore, $f'(b) = 2b$ never be 0 in (mod p). (Here we should use the fact that $p \neq 2$.) Thus by theorem 2.23, $x^2 \equiv a$ (mod p^{j+1}) has a solution.
Therefore, we prove that $x^2 \equiv a$ (mod p^j) has a solution for all j. □

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