18.781, Fall 2007 Problem Set 2

Solutions to Selected Problems

Problem 2.1.17 By Wilson's theorem, we have

$$70! \equiv -1 \pmod{71},$$

where

$$70! \equiv 63! \cdot 64 \cdots 70 \equiv 63! \cdot (-7) \cdot (-6) \cdots (-1) \equiv (-1)^7 \cdot 63! \cdot (7!) \pmod{71}.$$

Notice that

$$7! \equiv (7 \cdot 5 \cdot 2 \cdot)(6 \cdot 4 \cdot 3) \equiv 70 \cdot 72 \equiv -1 \pmod{71}.$$

Therefore, we have

$$(-1) \equiv 70! \equiv (-1) \cdot (63!) \cdot (7!) \equiv (-1) \cdot (63!) \cdot (-1) \equiv 63! \pmod{71}.$$

That is,

$$63! + 1 \equiv 0 \pmod{71}.$$

Also, $62 \cdot 63 \equiv (-9) \cdot (-8) \equiv 72 \equiv 1 \pmod{71}$, hence

$$61! + 1 \equiv 61! \cdot (1) + 1 \equiv 61! \cdot (62 \cdot 63) + 1 \equiv 63! + 1 \equiv 0 \pmod{71},$$

as desired. $\square$

Problem 2.1.25 $91 = 7 \cdot 13$ and $7, 13$ are prime numbers. By given condition, a, n are both prime to $7, 13$. Then, by Fermat's theorem, we have

$$n^6 \equiv 1 \pmod{7} \text{ and } a^6 \equiv 1 \pmod{7}.$$

By squaring both sides of each equation, we get

$$n^{12} \equiv 1 \pmod{7} \text{ and } a^{12} \equiv 1 \pmod{7}.$$

Hence $7 \mid n^{12} - a^{12}$.

Again by Fermat's theorem,

$$n^{12} \equiv 1 \pmod{13} \text{ and } a^{12} \equiv 1 \pmod{13}.$$

Hence $13 \mid n^{12} - a^{12}$.

Since (7,13)=1, we have $91 \mid n^{12} - a^{12}$. $\square$

Problem 2.1.28 This problem is equivalent to find the residue of 3^{400} divided by 10. Then,

$$3^{400} \equiv (3^4)^{100} \equiv 81^{100} \equiv 1^{100} \equiv 1(\text{mod } 10).$$

Therefore, the answer is 1. $\square$

Problem 2.1.46 First of all, by Fermat's theorem,

$$a \equiv a^p \equiv b^p \equiv b\,(\text{mod p}).$$

Then

$$a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1})$$

Because $a \equiv b\,(\text{mod p})$, we have $p \mid (a-b)$, and also have

$$(a^{p-1}+a^{p-2}b+\cdots+ab^{p-2}+b^{p-1}) \equiv (a^{p-1}+a^{p-2}a+\cdots+aa^{p-2}+a^{p-1}) \equiv pa^{p-1} \equiv 0(\text{mod p}).$$

Hence, $a^p - b^p$ is a multiple of two integers which are both multiple of p, that is, a multiple of p^2. Therefore we get $a^p \equiv b^p(\text{mod } p^2)$. $\square$

Problem 2.1.54 (a) By Fermat's theorem, $2^{10} \equiv 1(\text{mod } 11)$. Hence $2^{340} \equiv (2^{10})^{34} \equiv 1(\text{mod } 11)$. This gives $2^{341} - 2 = 2(2^{340} - 1)$ is divisible by 11. Similarly, $2^{340} \equiv (2^5)^{68} \equiv 1(\text{mod } 31)$, and this gives $2^{341} - 2 = 2(2^{340} - 1)$ is divisible by 31. Therefore, $341 \mid 2^{341} - 2$.

But $3^{340} \equiv (3^{30})^{11} \cdot 3^{10} \equiv 3^{10} \equiv (3^3)^3 \cdot 3 \equiv 27^3 \cdot 3 \equiv (-4)^3 \cdot 3 \equiv (-64) \cdot 9 \equiv (-2) \cdot 9 \equiv 13(\text{mod } 31)$, hence $3^{341} \equiv 39 \equiv 8 \not\equiv 3(\text{mod } 31)$. This implies that $3^{341} \not\equiv 3(\text{mod } 341)$.

(b) For any integer a satisfying $3 \mid a$, clearly $a^{561} \equiv a(\text{mod } 3)$. For an integer a such that $(a, 3) = 1$, $a^2 \equiv 1(\text{mod } 3)$ by Fermat's theorem. Then $a^{561} \equiv (a^2)^{280} \cdot a \equiv a(\text{mod } 3)$. Therefore for any integer a, $a^{561} \equiv a(\text{mod } 3)$.

We will go on similarly for 11 and 17. For any integer a satisfying $11 \mid a$, clearly $a^{561} \equiv a(\text{mod } 11)$. For an integer a such that $(a, 11) = 1$, $a^{10} \equiv 1(\text{mod } 11)$ by Fermat's theorem. Then $a^{561} \equiv (a^{10})^{56} \cdot a \equiv a(\text{mod } 11)$. Therefore for any integer a, $a^{561} \equiv a(\text{mod } 11)$.

For any integer a satisfying $17 \mid a$, clearly $a^{561} \equiv a(\text{mod } 17)$. For an integer a such that $(a, 17) = 1$, $a^{16} \equiv 1(\text{mod } 17)$ by Fermat's theorem. Then $a^{561} \equiv (a^{16})^{35} \cdot a \equiv a(\text{mod } 17)$. Therefore for any integer a, $a^{561} \equiv a(\text{mod } 17)$.

Therefore $a^{561} - a$ is divisible by $3, 11, 17$, hence we can conclude that $a^{561} \equiv a(\text{mod } 561)$ for any integer a.

Problem 2.1.55 Hint : Consider the determinant in the modulus 4.

Problem 2.2.8 (a) $x^2 \equiv 1 \pmod{p^\alpha}$ gives that $p^\alpha \mid (x-1)(x+1)$. If $x-1, x+1$ are both divided by p, $2 = (x+1)-(x-1)$ is divided by p, which is a contradiction. Therefore, $(p, x-1) = 1$ or $(p, x+1) = 1$, so $p^\alpha \mid (x-1)(x+1)$ implies that

$$x \equiv 1 \pmod{p^\alpha} \text{ or } x \equiv -1 \pmod{p^\alpha}.$$

And it is clear that these are solutions of the given equation. □

Problem 2.2.11 $1-(1-ax_1)^s \equiv 1-1^s \equiv 0 \pmod{a}$ implies that x_s is an integer. Also, by definition of x_s ,

$$ax_s - 1 = (1-ax_1)^s.$$

Since $m \mid 1-ax_1$, we have $m^s \mid (1-ax_1)^s$. Therefore, x_s is a solution of $ax \equiv 1 \pmod{m^s}$.

Problem 2.2.12 First of all, since $(a, m) = 1$, $(a, m^s) = 1$. Then by theorem 2.17, the solution of $ax \equiv 1 \pmod{m^s}$exists and is unique in $\pmod{m^s}$.

By exercise 2.2.11, we know that x_s is that solution. Hence it is enough to show that x_s is the nearest integer to $A := -\left(\frac{1}{a}\right)(1-ax_1)^s$. But it is trivial since $0 \le x_s - A = \frac{1}{a} \le \frac{1}{3}$. (For nonzero integer m, $m \le (x_s+m) - A \le m + \frac{1}{3}$, so for positive m, $1 \le m \le\mid (x_s+m) - A \mid$, and for negative m, $\frac{2}{3} = \mid (-1) + \frac{1}{3} \mid \le \mid (x_s+m) - A \mid$. So if m is nonzero, $\mid (x_s+m) - A \mid$ is bigger than $\mid x_s - A \mid$.) □

Problem 2.3.7 We are going through this problem similarly with Example 2.

$$5x \equiv 1 (\text{mod } 6) \;\Leftrightarrow\; 5x \equiv 1 (\text{mod } 3) \text{ and } 5x \equiv 1 (\text{mod } 2) \;\Leftrightarrow\; x \equiv 2 (\text{mod } 3) \text{ and } x \equiv 1 (\text{mod } 2)$$

$$4x \equiv 13 (\text{mod } 15) \;\Leftrightarrow\; 4x \equiv 13 (\text{mod } 3) \text{ and } 4x \equiv 13 (\text{mod } 5) \;\Leftrightarrow\; x \equiv 1 (\text{mod } 3) \text{ and } x \equiv 2 (\text{mod } 5)$$

Therefore the given congruences are inconsistent because there is no x for which both $x \equiv 1 (\text{mod } 3)$ and $x \equiv 2 (\text{mod } 3)$. □

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