Solutions to Homework 4

Solution to Problem 34c): We are asked to solve the system

$$5x \equiv 3(\mod 7),\ \ 2x \equiv 4(\mod 8)\ \ 3x \equiv 6(\mod 9).$$

This problem may be slighly confusing. When we deal with one congruence modulo some integre m then solving the congruence means finding all residues modulo m which satisfy the congreunce. In the above problem we have several congruences, with different moduli, so what do we mean by solving it? Well, one answer is that we want to describe all integers x which satisfy the system of congruences. We will do just that.

In the first congruence, 5 is relatively prime to 7, so it is invertible modulo 7 and the inverse of 5 modulo 7 is easily seen to be 3. Multiplying the congruence by 3, we get equivalent congruence $x \equiv 2(\mod 7)$. For the second congruence, note that x satisfies $2x \equiv 4(\mod 8)$ if and only if x satisfies $x \equiv 2(\mod 4)$. Finally, x satisfies the third congruence if and only if $x \equiv 2(\mod 3)$. Thus, the set of all integers satisfying our original system of congruences is the same as the set of integral solutions to the system

$$x \equiv 2(\mod 7),\ \ x \equiv 2(\mod 4)\ \ x \equiv 2(\mod 3).$$

his system qualifies for the Chinese remainder theorem. Following the method provided by this theorem, we find that the unique solution modulo $3 \cdot 4 \cdot 7 = 84$ to this system is $x = 2$ (in this particular case the system is so simple that we do not need to involve the Chinese remainder theorem: we are looking for x such that $x - 2$ is divisible by 7, 4, and 3, which is the same as $x - 2$ divisible by 84). Thus the solutions to the system all all integers x such that $x \equiv 2(\mod 84)$.

Remark. The original problem could be phrased as follows: find all solutions modulo $7 \cdot 8 \cdot 9 = 504$ of the given system. In this case, the answer would be that there are 6 solutions modulo 504: $2, 86, 170, 254, 338, 422$.

Solution to Problem 35: We want to find a smallest positive integer n such that

$$n \equiv 1(\mod 2),\ n \equiv 2(\mod 3),\ n \equiv 3(\mod 4),$$

$$n \equiv 4(\mod 5),\ n \equiv 5(\mod 6),\ n \equiv 0(\mod 7).$$

We can not apply the Chinese reminder theorem right away as the moduli are not pairwise relatively prime. We note however that some of the congruences are consequences of the others. In fact, suppose that n satisfies

$$n \equiv 2(\mod 3),\ n \equiv 3(\mod 4),\ n \equiv 4(\mod 5),\ n \equiv 0(\mod 7).$$

The second congruence tells us that n is odd, so $n \equiv 1(\mod 2)$. Also, as n is odd and $n \equiv 2(\mod 3)$, we have $n \equiv 5(\mod 6)$ (the system $x \equiv 1(\mod 2)$, $x \equiv 2(\mod 3)$ has a unique solution modulo 6, and 5 is that solution). So we reduced our problem to a system of 4 congruences which satisfy the requirements of the Chinese remainder theorem, as the moduli $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, and $m_4 = 7$ are pairwise relatively prime. We have $b_1 = 2$, $b_2 = 3$, $b_3 = 4$, $b_4 = 0$. To solve the system, we take $M = 3 \cdot 4 \cdot 5 \cdot 7 = 420$. Then $M_1 = 420/3 = 140$, $M_2 = 420/4 = 105$, $M_3 = 420/5 = 84$, $M_4 = 420/7 = 60$. Now we need to find the inverse x_i of M_i modulo m_i, $i = 1, 2, 3, 4$. Then

$$n \equiv M_1 x_1 b_1 + M_2 x_2 b_2 + M_3 x_3 b_3 + M_4 x_4 b_4 (\mod M)$$

will be our solution. Finding the inverses is rather easy as the moduli m_i are small. As $M_1 \equiv 2(\mod 3)$, we see that $x_1 = 2$. Similarly, $M_2 \equiv 1(\mod 4)$, so $x_2 = 1$. Now $M_3 \equiv 4(\mod 5)$ so $x_3 = 4$. Finally $M_4 \equiv 4(\mod 7)$so $x_4 = 2$. It follows that

$$n \equiv 140 \cdot 2 \cdot 2 + 105 \cdot 1 \cdot 3 + 84 \cdot 4 \cdot 4 + 60 \cdot 2 \cdot 0 = 560 + 315 + 1404 \equiv 119(\mod 420).$$

The smallest positive solution is therefore 119.

Solution to Problem 38. Let $d = \gcd(m_1, m_2)$. If x is a solution to

$$x \equiv b_1(\mod m_1), \quad x \equiv b_2(\mod m_2)$$

then x satisfies also the congruences

$$x \equiv b_1(\mod d), \quad x \equiv b_2(\mod d).$$

Subtracting the last two congruences, we get $b_1 - b_2 \equiv 0(\mod d)$, so indeed d must divide $b_1 - b_2$.

Suppose converesely, that d divides $b_1 - b_2$. We look for a solution x of the form $b_1 + ym_1$ for appropriate integer y. Any such x is a solution to the first congruence

and in order to be a solution to the second congruence we must have $b_1 + ym_1 \equiv b_2($ mod $m_2)$. This congruence is equivalent to

$$m_1 y \equiv b_2 - b_1(\mod m_2).$$

Since $\gcd(m_1, m_2) = d | b_2 - b_1$, we know that this congruence has a solution y and then $x = b_1 + m_1 y$ is a solution to our sytem of congruences.

Finally, suppose that x_1 and x_2 both are solutions to our system. Then

$$x_1 \equiv x_2 \equiv b_1(\mod m_1) \text{ and } x_1 \equiv x_2 \equiv b_2(\mod m_2).$$

It follows that both m_1 and m_2 divide $x_1 - x_2$, and threfore also the $\text{lcm}(m_1, m_2)$ divies $x_1 - x_2$. This means that the solution is unique modulo $\text{lcm}(m_1, m_2)$.

Solution to Problem 47. a) Wilson's Theorem tells us that

$$(p-1)! \equiv -1(\mod p).$$

Now, in the product $1 \cdot 2 \cdot 3 \ldots \cdot (p-1)$ we can pair 1 and $p-1$, 2 and $p-2$, 3 and $p-3$, ..., $\frac{p-1}{2}$ and $p - \frac{p-1}{2} = \frac{p+1}{2}$ to get

$$(p-1)! = [1 \cdot (p-1)][2(p-2)][3(p-3)] \ldots \cdot \left[\frac{p-1}{2} \cdot (p - \frac{p-1}{2})\right].$$

Since $p - k \equiv -k(\mod p)$, we get

$$(p-1)! \equiv [1 \cdot (-1)][2(-2)][3(-3)] \ldots \cdot \left[\frac{p-1}{2} \cdot (-\frac{p-1}{2})\right] = (-1)^{(p-1)/2} \left[(\frac{p-1}{2})!\right]^2.$$

Thus, by Wilson's theorem, we get

$$(-1)^{(p-1)/2} \left[(\frac{p-1}{2})!\right]^2 \equiv -1(\mod p).$$

Multiplying both sides by $(-1)^{(p-1)/2}$ we have

$$\left[(\frac{p-1}{2})!\right]^2 \equiv (-1)^{1+(p-1)/2} = (-1)^{(p+1)/2}(\mod p).$$

When $p \equiv 1(\mod 4)$ then $(-1)^{(p+1)/2} = -1$ so $x = (\frac{p-1}{2})!$ satisfies $x^2 \equiv -1(\mod p)$. This shows part b).

When $p \equiv 3(\mod 4)$ then $(-1)^{(p+1)/2} = 1$ so $x = (\frac{p-1}{2})!$ satisfies $x^2 \equiv 1(\mod p)$. This shows part c).

Solution to Problem 48. Note that when k varies over all odd numbers between 1 and $p-1$ then $p-k$ varies over all even numbers form $p-1$ to 1. Thus

$$(p-1)! = 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (p-2) \cdot (p-1)(p-3)(p-5) \cdot \ldots \cdot (p-(p-2)) \equiv$$

$$\equiv 1{\cdot}3{\cdot}5{\cdot}\ldots{\cdot}(p{-}2)(-1)(-3)(-5)\ldots(-(p{-}2)) = (-1)^{(p-1)/2}(1{\cdot}3{\cdot}5{\cdot}\ldots{\cdot}(p{-}2))^2 (\mod p).$$

Using Wilson's Theorem, we get

$$(-1)^{(p-1)/2}(1 \cdot 3 \cdot 5 \cdot \ldots \cdot (p-2))^2 \equiv -1(\mod p)$$

and, as in problem 47, this is the same as

$$(1 \cdot 3 \cdot 5 \cdot \ldots \cdot (p-2))^2 \equiv (-1)^{(p+1)/2}(\mod p).$$

Solution to Problem 55. Let $n = 2{\cdot}73{\cdot}1103 = 161038$. Note that 2, 73, and 1103 are prime numbers. We need to show that $2^n \equiv 2(\mod n)$, which is equivalent to $2^n \equiv 2(\mod 2)$, $2^n \equiv 2(\mod 73)$, and $2^n \equiv 2(\mod 1103)$. The first congruence is clear. Unfortunately, to show the other congruences, we need a bit more than just Fermat's Little Theorem. We have $2^6 = 64 \equiv -9(\mod 73)$. Multiplying by 8, we get $2^9 \equiv -72 \equiv 1(\mod 73)$ (note that FLT only gives us $2^{72} \equiv 1(\mod 73)$, which is not good enough). Now $161038 \equiv 1(\mod 9)$, i.e. $161038 = 9s + 1$ for some natural number s. Thus

$$2^{161038} = 2^{9s+1} = 2(2^9)^s \equiv 2(1)^s = 2(\mod 73).$$

Finally, note that $1102 = 2{\cdot}19{\cdot}29$. We need smallest k such that $2^k \equiv 1(\mod 1103)$. We start with $2^{10} = 1024 \equiv -79(\mod 1103)$. Squaring, we get $2^{20} \equiv 79^2 \equiv -377(\mod 1103)$. Multiply by 32 to get $2^{25} \equiv -12064 \equiv 69(\mod 1103)$. Now multiply by 16 and get $2^{29} \equiv 16 \cdot 69 = 1104 \equiv 1(\mod 1103)$. Since $161038 = 29 \cdot 5553 + 1$, we see that

$$2^{161038} = 2(2^{29})^{5553} \equiv 2(1)^{5553} = 1(\mod 1003).$$

This completes our verification that n is a pseudoprime number.

Solution to Problem 57c). We have $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$. We need to prove that each of the following congruences holds:

$$n^{13} \equiv n(\mod 2),\ n^{13} \equiv n(\mod 3),\ n^{13} \equiv n(\mod 5),\ n^{13} \equiv n(\mod 7),\ n^{13} \equiv n(\mod 13).$$

Clearly $n^{13} \equiv n(\mod 2)$.

Fermat's Little Theorem tealls us that $n^3 \equiv n(\mod 3)$. Raising both sides to the third power yields $n^9 \equiv n^3 \equiv n(\mod 3)$. We also have $n^4 \equiv n^2(\mod 3)$, and multiplying the last 2 congruences gives us $n^{13} \equiv n^3 \equiv n(\mod 3)$.

By FLT, by have $n^5 \equiv n(\mod 5)$. Multiplying both sides by n^4, we have $n^9 \equiv n^5 \equiv n(\mod 5)$. Multiplying again by n^4, we have $n^{13} \equiv n^5 \equiv n(\mod 5)$.

By FLT, $n^7 \equiv n(\mod 7)$. Multiplying by n^6, we get $n^{13} \equiv n^7 \equiv n(\mod 7)$.

Finally, $n^{13} \equiv n(\mod 13)$ is a consequence of FLT for the prime 13.

Solution to Problem 58. a) Suppose that $a^p \equiv b^p(\mod p)$. Since $a^p \equiv a(\mod p)$ and $b^p \equiv b(\mod p)$ by Fermat's Little Theorem, we conclude that

$$a \equiv a^p \equiv b^p \equiv b(\mod p).$$

b) Note that

$$a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1}) = (a-b)\sum_{k=0}^{p-1} a^k b^{p-1-k}.$$

By part a) we know that $a \equiv b(\mod p)$. Thus $a^k \equiv b^k(\mod p)$ and $a^k b^{p-1-k} \equiv b^k b^{p-1-k} = b^{p-1}(\mod p)$, for $k = 0, 1, \ldots, p-1$. Therefore,

$$\sum_{k=0}^{p-1} a^k b^{p-1-k} \equiv \sum_{k=0}^{p-1} b^{p-1} = pb^{p-1} \equiv 0(\mod p).$$

Thus, in the product $(a-b)(a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1})$ both factors are divisible by p, so the product, which is $a^p - b^p$, is divisible by p^2, i.e.

$$a^p \equiv b^p(\mod p^2).$$

Remark. The assumption that a and b are not divisible by p is not needed for this problem. If p divides one of them then p divides both of them and the result is obvious in this case.

Solution to Problem 68 c) and d). c) It is easy to see that $\phi(14) = 6$. By Euler's Theorem, $3^6 \equiv 1(\mod 14)$. Now $1000000 \equiv 4(\mod 6)$, i.e. $1000000 = 6s + 4$ for some natural number s. Thus

$$3^{1000000} = 3^4 \cdot (3^6)^s \equiv 3^4(1)^s = 81 \equiv 11(\mod 14).$$

d) Again, it is easy to see that $\phi(26) = 12$. Also $99 \equiv -5(\mod 26)$. Now $999999 = 3 \cdot 333333 = 3(4s + 1) = 12s + 3$ for some natural number s. Thus

$$99^{999999} \equiv (-5)^{12s+3} = (-5)^3 \cdot (5^{12})^s \equiv -125 \equiv 5(\mod 26).$$

We used here Euler's theorem, which tells us that $5^{12} \equiv 1(\mod 26)$.

Solution to Problem 72. a) Note that $72 = 8 \cdot 9$. If n is relatively prime to 72, then it is relatively prime to both 8 and 9. Note that $\phi(8) = 4$ and $\phi(9)$=6. By Euler's theorem, $n^4 \equiv 1(\mod 8)$ and $n^6 \equiv 1(\mod 9)$. Raising the first congruence to the third power, and squaring the second we get

$$n^{12} \equiv 1(\mod 8) \text{ and } n^{12} \equiv 1(\mod 9).$$

These two congruences together are equivalent to $n^{12} \equiv 1 \mod (72)$.

b) Suppose that $n^{12} \equiv 1(\mod m)$ for every n relatively prime to m. We may write $m = 2^e m_1$ for some odd integer m_1, where $e = e_2(m)$. Since 2 and m_1 are relatively prime, the Chinese remainder theorem tells us that there is an integer n such that $n \equiv 3(\mod 2^e)$ and $n \equiv 1(\mod m_1)$. Clearly any such n is relatively prime to m. Since $n^{12} \equiv 1(\mod m)$, we have $n^{12} \equiv 1(\mod 2^e)$.

But $n \equiv 3(\mod 2^e)$, so $3^{12} \equiv 1(\mod 2^e)$. Now, $3^{12} - 1 = (3^3 - 1)(3^3 + 1)(3^6 + 1) = 2^4 \cdot (\text{odd number})$. It follws that $e \leq 4$.

Again by the Chinese remainder theorem, there is an integer k such that

$$k \equiv 1(\mod 2) \text{ and } k \equiv 2(\mod m_1).$$

Clearly k is relatively prime to m. Thus $k^{12} \equiv 1(\mod m)$, so also $k^{12} \equiv 1(\mod m_1)$. Since $k \equiv 2(\mod m_1)$, we conclude that $2^{12} \equiv 1(\mod m_1)$). In other words, m_1 divides $2^{12} - 1 = (2^3 - 1)(2^3 + 1)(2^6 + 1) = 7 \cdot 9 \cdot 65 = 3^2 \cdot 5 \cdot 7 \cdot 13$.

We proved that any m with the required property must divide the number $2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$. Using the same method as in part a), it is easy to show that $m = 2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$ has the property that $n^{12} \equiv 1 (\mod m)$ for every n relatively prime to m (just note that $\phi(13) = 12$, $\phi(7) = 6 = \phi(9)$, $\phi(5) = 4$ and that $n^4 - 1 = (n-1)(n+1)(n^2+1)$ is divisible by 2^4 for any odd n, as each factor is even and one of $n-1$, $n+1$ is divisible by 4).

The largest number m such that $n^{12} \equiv 1 (\mod m)$ for every m relatively prime to m is threfore $m = 2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 = 65520$.