Homework 6, solutions

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 $2^9 \equiv -72 \equiv 1(\mod 72)$ (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 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 suqaring 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

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

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 $m = 2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 = 65520$.