

Number Theory Test 2: Solution (Spring 2010)

Exercise 1. Prove that 1105 is an absolute pseudo-prime.

Solution. Since $1105 = 5 \times 13 \times 17$, we should just show that $1104 = 1105 - 1$ is divisible by 4, 12 and 16, which is easy to check.

Exercise 2. Prove that for any integer a , we have: $a^7 \equiv a \pmod{21}$.

Solution. By Fermat's Theorem we have $a^3 \equiv a \pmod{3}$, thus $a^7 \equiv (a^3)^2 a \equiv a^2 a \equiv a^3 \equiv a \pmod{3}$.

By Fermat's Theorem, we have $a^7 \equiv a \pmod{7}$. Since 3 and 7 are distinct primes, then $a^7 \equiv a \pmod{7}$ and $a^7 \equiv a \pmod{3}$ imply that $a^7 \equiv a \pmod{21}$.

Exercise 3. Find a solution of the quadratic congruence $x^2 \equiv -1 \pmod{17}$.

Solution. Since $17 \equiv 1 \pmod{4}$, then $\frac{17-1}{2}! = 8! = 40320$ is a solution. Thus, $x \equiv 40320 \equiv 13 \pmod{17}$ is a solution of the quadratic congruence.

Exercise 4. Show that $18! \equiv -1 \pmod{437}$.

Solution. If we apply Wilson's Theorem for $p = 19$, then we get $18! \equiv -1 \pmod{19}$. Now if we apply the same theorem for $p = 23$, we get $21! \equiv 1 \pmod{23}$. Hence, $21 \times 20 \times 19 \times 18! \equiv 1 \pmod{23}$. This implies that: $(-2)(-3)(-4)18! \equiv 1 \pmod{23}$. This means that $-24 \times 18! \equiv 1 \pmod{23}$. Since $-24 \equiv -1 \pmod{23}$, then $18! \equiv -1 \pmod{23}$.

Finally: $437 = 19 \times 23$, $18! \equiv -1 \pmod{19}$ and $18! \equiv -1 \pmod{23}$ implies that

$18! \equiv -1 \pmod{437}$. Note that we have used the fact that 19 and 23 are two distinct primes.

Exercise 5. Find an integer x which satisfies the three congruences: $x \equiv 2 \pmod{7}$, $x \equiv 5 \pmod{11}$ and $x \equiv 4 \pmod{13}$

Solution. We solve this problem using the Chinese Remainder Theorem. Let $N_1 = 11 \times 13 = 143$, $N_2 = 7 \times 13 = 91$ and $N_3 = 7 \times 11 = 77$. Now we should solve the congruences:

$143x \equiv 1 \pmod{7}$, $91x \equiv 1 \pmod{11}$ and $77x \equiv 1 \pmod{13}$.

The first equation $143x \equiv 1 \pmod{7}$ is equivalent to $3x \equiv 1 \pmod{7}$ and $x_1 \equiv 5 \pmod{7}$ is a solution.

The second equation $91x \equiv 1 \pmod{11}$ is equivalent to $3x \equiv 1 \pmod{11}$ and $x_2 \equiv 4 \pmod{11}$ is a solution.

The third equation $77x \equiv 1 \pmod{13}$ is equivalent to $12x \equiv 1 \pmod{13}$ and $x_3 \equiv 12 \pmod{13}$ is a solution.

By the Chinese Remainder Theorem: $x \equiv 2 \times 143 \times 5 + 5 \times 91 \times 4 + 4 \times 77 \times 12 \pmod{7 \times 11 \times 13}$ is a solution of the congruences. Finally, $x \equiv 6946 \equiv 940 \pmod{1001}$.

Exercise 6. Let p be an odd prime and $1 \leq k \leq p - 1$. Prove that if k is even, then we have $C_k^{p-1} \equiv 1 \pmod{p}$. (here C_k^{p-1} is the binominal coefficient)

Solution. $C_k^{p-1} = \frac{(p-1)!}{k!(p-1-k)!}$. First notice that $(p-1)! = [(p-1)(p-2)\dots(p-k)](p-k-1)!$ and that modulo p we have: $p-1 \equiv -1 \pmod{p}$, $p-2 \equiv -2 \pmod{p}$, $p-3 \equiv -3 \pmod{p}$... $p-k \equiv -k \pmod{p}$.

Thus, $[(p-1)(p-2)\dots(p-k)] \equiv (-1)(-2)\dots(-k) \equiv (-1)^k k! \pmod{p}$. Since k is even then $(-1)^k = 1$. Finally,

$$C_k^{p-1} = \frac{(p-1)!}{k!(p-1-k)!} = \frac{k!(p-1-k)!}{k!(p-1-k)!} \equiv 1 \pmod{p}.$$