Steven Rosendahl
Homework 7

1. If p is prime and $x, y \in \mathbb{Z}_p$, prove that $(x-y)^p \equiv x^p - y^p \mod p$.

$$\begin{aligned}(x-y)^p &\equiv (x-y) \mod p \qquad \text{by the corollary to FLT}\\ &\equiv (x \mod p) - (y \mod p)\\ &\equiv (x^p \mod p) - (y^p \mod p) \qquad \text{by the corollary to FLT}\\ &\equiv x^p - y^p \mod p\end{aligned}$$

2. Suppose that p is prime and k is a positive integer, and $x \in \mathbb{Z}_p$.

   (a) Prove that $x^{p^k} \equiv x \mod p$.

   We can rewrite x^{p^k} as $(((x^p)^p)^p ...)^p$, where there are k p's. We can mod out by p, and we get $(((x^p)^p)^p ...)^p$, where there are $k-1$ p's. If we mod out $k-2$ more times, we get $x^p \equiv x \mod p$, which by the corollary to Fermat's Little Theorem means $x^{p^k} \equiv x \mod p$.

   (b) Prove that $x^{p^k-1} \equiv 1 \mod p$ if and only if $\gcd(x,p) = 1$.

   $\Rightarrow$) Assume that $gcd(x,p) \neq 1$. Then $x \equiv 0 \mod p$, since the only thing not coprime with p is a multiple of p. We can raise both sides of the congruence to the $p^k - 1$ power to produce

   $$x^{p^k-1} \equiv 0^{p^k-1} \equiv 0 \not\equiv 1 \mod p.$$

   $\Leftarrow$) Suppose $gcd(x,p) = 1$. Then x has an inverse in $\mathbb{Z}_p$. We know by part (a) that $x^{p^k} \equiv x \mod p$, so $x^{-1} \cdot x^{p^k} \equiv x \cdot x^{-1} \equiv 1 \mod p$.

3. Let p, n, and r be non-negative integers with p prime. Further, assume that r is the remainder when n is divided by $p-1$. Prove that $a^n \equiv a^r \mod p$.

   Since r is the remainder, we have that $n = q(p-1) + r$ by the division algorithm. Since p, n, and r are non-negative, we can say $a^n = a^{q(p-1)+r}$, which is the same as $a^n = a^{q(p-1)}a^r$. By Fermat's Little Theorem, we have that $a^{p-1} = 1 \mod p$, so $a^n \equiv 1^q a^r \mod p$, or $a^n \equiv a^r \mod p$.

4. Assume that n is a positive integer. Prove that $1^n + 2^n + 3^n + 4^n$ is divisible by 5 if and only if n is not divisible by 4.

   $\Rightarrow$) Suppose $4 \mid n$. Then $n = 4k,\ k \in \mathbb{Z}$, so we have

   $$\begin{aligned}1^n + 2^n + 3^n + 4^n &\equiv 1^{4k} + 2^{4k} + 3^{4k} + 4^{4k}\\ &\equiv 1^{4^k} + 2^{4^k} + 3^{4^k} + 4^{4^k}\\ &\equiv 1^k + 1^k + 1^k + 1^k \mod 5\\ &\not\equiv 0 \mod 5.\end{aligned}$$

   $\Leftarrow$) Suppose $4 \nmid n$. Then $n \not\equiv 0 \mod 4$. Suppose that $n \equiv 1 \mod 4$. We now have $n = 4k+1$ for some $k \in \mathbb{Z}$. By (3), we know that $a^n \equiv a^r \mod p$. Similarly, we can say $a^n + b^n + c^n + d^n \equiv a^r + b^r + c^r + d^r \mod p$. Then, we have $1^n + 2^n + 3^n + 4^n \equiv 1 + 2 + 3 + 4 \mod 5 \equiv 0 \mod 5$. Suppose $n \equiv 2 \mod 4$. Then we have $1^n + 2^n + 3^n + 4^n \equiv 1 + 4 + 9 + 16 \equiv 1 - 1 + 1 - 1 \mod 5 \equiv 0 \mod 5$. Finally, suppose $n \equiv 3 \mod 4$. Then $1^n + 2^n + 3^n + 4^n \equiv 1 + 8 + 27 + 64 \equiv 1 + 2 + 3 - 1 \equiv 0 \mod 5$.

5. Determine whether there exists a solution to each of the following systems of congruences. If there is a solution, find all solutions to the system by writing the solution set as a single residue class modulo n for some $n \geq 2$. If there is no solution, prove that there is no solution.

(a) $x \equiv 5 \mod 7$
$x \equiv 0 \mod 4$

Since $gcd(7,4) = 1$, we can use Chinese remainder theorem, which tells us

$$\begin{aligned} x_0 &= a_1c_1d_1 + 1_2c_2d_2 \\ &= 5c_1d_1 + 0c_2d_2 \\ &= 5 \cdot 4 \cdot d_1 \\ &= 5 \cdot 4 \cdot 2 \\ &= 40 \\ &\equiv 12 \mod 28 \end{aligned}$$

(b) $x \equiv 5 \mod 7$
$x \equiv 1 \mod 4$
$x \equiv 0 \mod 5$

The $\gcd(7,4,5) = 1$, so by the Chinese remainder theorem, we have a solution.

$$\begin{aligned} x_0 &= a_1c_1d_1 + a_2c_2d_2 + a_3c_3d_3 \\ &= 5 \cdot c_1 \cdot d_1 + 1 \cdot c_2 \cdot d_2 + 0 \\ &= 5 \cdot 20 \cdot d_1 + 1 \cdot 35 \cdot d_2 \\ &= 5 \cdot 20 \cdot -1 + 1 \cdot 35 \cdot 3 \\ &= -100 + 105 \\ &= 5 \\ &\equiv 5 \mod 140 \end{aligned}$$

(c) $x \equiv 5 \mod 6$
$x \equiv 2 \mod 4$

We cannot use Chinese remainder theorem here since 6 and 4 are not coprime. Suppose, however, that there is a solution. We can form a new system by determining the prime factorization of 6.

$$\begin{cases} x \equiv 5 \mod 2 \\ x \equiv 5 \mod 3 \\ x \equiv 2 \mod 4 \end{cases} \to \begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ x \equiv 2 \mod 4 \end{cases}$$

If this is the case, then $x \equiv 1 \mod 2$ implies that the solution is odd, and $x \equiv 2 \mod 4$ implies the solution is even. This is not possible; therefore there is no solution.

(d) $3x \equiv 1 \mod 10$
$5x \equiv 2 \mod 7$

We cannot initially use Chinese remainder theorem to solve this problem. If we find 3^{-1} in $\mathbb{Z}_{10}$, then we can multiply both sides of the congruence by that value to produce a new congruence. We have $3x \equiv 1 \mod 10$, which is satisfied by $x = 7 = 3^{-1}$. We can rewrite this congruence as $x \equiv 7 \mod 10$. Similarly, we can find 5^{-1} in $\mathbb{Z}_7$. We have that $5x \equiv 1 \mod 7$, so $x = 3 = 5^{-1}$. Multiplying both sides of the congruence yields the new system

$$\begin{cases} x \equiv 7 \mod 10 \\ x \equiv 3 \mod 7 \end{cases}.$$

We know this has a solution by the Chinese remainder theorem, since 10 and 7 are coprime.

$$\begin{aligned} x_0 &= a_1c_1d_1 + a_2c_2d_2 \\ &= 7 \cdot 7 \cdot d_1 + 3 \cdot 10 \cdot d_2 \\ &= 7 \cdot 7 \cdot 3 + 3 \cdot 10 \cdot 5 \\ &= 147 + 150 \\ &= 297 \\ &\equiv 13 \mod 70 \end{aligned}$$

6. Find all solutions to the congruence $97x \equiv 301 \mod 315$. It may be helpful to note that $315 = 3^2 \cdot 4 \cdot 7$.

We can split this congruence into several parts.

$$\begin{cases} 97x \equiv 301 & \mod 9 \\ 97x \equiv 301 & \mod 5 \\ 97x \equiv 301 & \mod 7 \end{cases} \rightarrow \begin{cases} 7x \equiv 4 & \mod 9 \\ 2x \equiv 1 & \mod 5 \\ 6x \equiv 0 & \mod 7 \end{cases} \rightarrow \begin{cases} x \equiv 7 & \mod 9 \\ x \equiv 3 & \mod 5 \\ x \equiv 0 & \mod 7 \end{cases}$$

By the Chinese remainder theorem, which we can use since 9, 7, and 5 are coprime, we have that

$$\begin{aligned} x_0 &= 7c_1d_1 + 3c_2d_2 + 0c_3d_3 \\ &= 7 \cdot 35 \cdot d_1 + 3 \cdot 63 \cdot d_2 + 0 \\ &= 7 \cdot 35 \cdot -1 + 3 \cdot 63 \cdot 2 + 0 \\ &= -245 + 378 \\ &= 133 \\ &\equiv 133 \mod 315. \end{aligned}$$

7. Find all solutions to the congruence $x^{1000} \equiv 1 \mod 10$.

By the prime factorization of 10, we have that

$$5 \mid (x^{1000} - 1) \qquad \text{and} \qquad 2 \mid (x^{1000} - 1).$$

Since $2 \mid (x^{1000} - 1)$, we have that $x^{1000} \equiv 1 \mod 2$, implying that x is odd. This leaves us with two possibilities in $\mathbb{Z}_5$, namely $\{1, 3\}$. We can express 1000 as $5 \cdot 5 \cdot 5 \cdot 8$, so we have $((((x)^8)^5)^5)^5 \equiv (((x)^8)^5)^5 \equiv ((x)^8)^5 \equiv x^8 \equiv 1 \mod 5$. We can express 8 as $4 \cdot 2$, so we have $(x^2)^4 \equiv 1 \mod 5$, which means $x^2 \equiv 1 \mod 5$ by Fermat's Little Theorem. We know x is either 1 or 3, so we can test the values. If we try 3, we get that $9 \equiv 1 \mod 5$, which is not true, whereas if we try 1, we get $1 \equiv 1 \mod 5$, which is true. Therefore, $x = 1$.