

**Steven Rosendahl**  
**Homework 7**

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

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

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

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

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

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  $a^n \equiv a^r \pmod{p}$ .

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.

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)  $x \equiv 5 \pmod{7}$   
 $x \equiv 0 \pmod{4}$

$$\begin{aligned} x_0 &= a_1 c_1 d_1 + 1_2 c_2 d_2 \\ &= 5c_1 d_1 + 0c_2 d_2 \\ &= 5 \cdot 4 \cdot d_1 \\ &= 5 \cdot 4 \cdot 2 \\ &= 40 \\ &\equiv 12 \pmod{28} \end{aligned}$$

(b)  $x \equiv 5 \pmod{7}$   
 $x \equiv 1 \pmod{4}$   
 $x \equiv 0 \pmod{5}$

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

$$\begin{aligned} x_0 &= a_1 c_1 d_1 + a_2 c_2 d_2 + a_3 c_3 d_3 \\ &= 5 \cdot c_1 \cdot d_1 + 1 \cdot c_2 \cdot d_2 + 0 \\ &= 5 \cdot 20 \cdot d_1 + 1 \cdot 35 \cdot d_2 \\ &= 5 \cdot 20 \cdot -1 + 1 \cdot 35 \cdot 3 \\ &= -100 + 105 \\ &= 5 \\ &\equiv 5 \pmod{140} \end{aligned}$$

(c)  $x \equiv 5 \pmod{6}$   
 $x \equiv 2 \pmod{4}$

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.

$$\begin{cases} x \equiv 5 \pmod{2} \\ x \equiv 5 \pmod{3} \\ x \equiv 2 \pmod{4} \end{cases} \rightarrow \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{4} \end{cases}$$

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

(d)  $3x \equiv 1 \pmod{10}$   
 $5x \equiv 2 \pmod{7}$

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  $3x \equiv 1 \pmod{10}$ , which is satisfied by  $x = 7 = 3^{-1}$ . We can rewrite this congruence as  $x \equiv 7 \pmod{10}$ . Similarly, we can find  $5^{-1}$  in  $\mathbb{Z}_7$ . We have that  $5x \equiv 1 \pmod{7}$ , so  $x = 3 = 5^{-1}$ . Multiplying both sides of the congruence yields the new system

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

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

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

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

We can split this congruence into several parts.

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

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

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

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

By the prime factorization of 10, we have that

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

Since  $2 \mid (x^{1000} - 1)$ , we have that  $x^{1000} \equiv 1 \pmod{2}$ , 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

$((((x)^8)^5)^5)^5 \equiv (((x)^8)^5)^5 \equiv ((x)^8)^5 \equiv x^8 \equiv 1 \pmod{5}$ . We can express 8 as  $4 \cdot 2$ , so we have  $(x^2)^4 \equiv 1 \pmod{5}$ , which means  $x^2 \equiv 1 \pmod{5}$  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  $9 \equiv 1 \pmod{5}$ , which is not true, whereas if we try 1, we get  $1 \equiv 1 \pmod{5}$ , which is true. Therefore,  $x = 1$ .