

**Instructions:** Write each solution in claim-proof form, even if the solution is short. Make sure your handwriting is legible and that your proofs **use complete sentences**. Provide enough detail so that it is clear to me that you understand why each step of your proof is correct. I will not accept late assignments, so it is in your best interests to submit your homework on time *even if it is incomplete*.

1. (8 points) Solve the linear congruence:  $140x \equiv 133 \pmod{301}$ .

**Solution:** Since  $\gcd(140, 301) = 7 \mid 133$ , this congruence has 7 distinct solutions modulo 301. Since

$$140x \equiv 133 \pmod{301}$$

$$20x \equiv 19 \pmod{43}$$

$$40x \equiv 38 \pmod{43}$$

$$-3x \equiv -5 \pmod{43}$$

$$-42x \equiv -70 \pmod{43}$$

$$x \equiv 16 \pmod{43}$$

we have that  $x = 16$  is the unique solution modulo 43. Then

$$x = 16, 16 + 43, 16 + 2 \cdot 43, 16 + 3 \cdot 43, 16 + 4 \cdot 43, 16 + 5 \cdot 43, 16 + 6 \cdot 43$$

$$x = 16, 59, 102, 145, 188, 231, 274$$

are the 7 distinct solution modulo 301.

2. (8 points) Solve the following system of linear congruences:

$$2x \equiv 1 \pmod{5}$$

$$3x \equiv 9 \pmod{6}$$

$$4x \equiv 1 \pmod{7}$$

$$5x \equiv 9 \pmod{11}$$

**Solution:** Since we can verify that each of these congruences is solvable (individually), we proceed by reducing this system of congruences to one resembling the form found in the CRT:

$$2x \equiv 1 \pmod{5} \quad 3x \equiv 9 \pmod{6} \quad 4x \equiv 1 \pmod{7} \quad 5x \equiv 9 \pmod{11}$$

$$6x \equiv 3 \pmod{5} \quad x \equiv 3 \pmod{2} \quad 8x \equiv 2 \pmod{7} \quad 45x \equiv 81 \pmod{11}$$

$$x \equiv -2 \pmod{5} \quad x \equiv 1 \pmod{2} \quad x \equiv 2 \pmod{7} \quad x \equiv 4 \pmod{11}$$

Since the moduli of this new system (5, 2, 7, 11) are all pairwise relatively prime, we can apply the CRT to find a unique solution modulo  $n = 770 = 5 \cdot 2 \cdot 7 \cdot 11$ . To do this, we first let

$$n_1 = 5 \quad a_1 = -2 \quad N_1 = \frac{n}{5} = 154$$

$$n_2 = 2 \quad a_2 = 1 \quad N_2 = \frac{n}{2} = 385$$

$$n_3 = 7 \quad a_3 = 2 \quad N_3 = \frac{n}{7} = 110$$

$$n_4 = 11 \quad a_4 = 4 \quad N_4 = \frac{n}{11} = 70$$

Now we solve each congruence of the form  $N_k y \equiv 1 \pmod{n_k}$  and call its solution  $y_k$ :

$$\begin{array}{cccc}
 154y \equiv 1 \pmod{5} & 385y \equiv 1 \pmod{2} & 110y \equiv 1 \pmod{7} & 70y \equiv 1 \pmod{11} \\
 -y \equiv 1 \pmod{5} & y \equiv 1 \pmod{2} & -2y \equiv 1 \pmod{7} & 4y \equiv 1 \pmod{11} \\
 y \equiv -1 \pmod{5} & & 8y \equiv -4 \pmod{7} & 12y \equiv 3 \pmod{11} \\
 & & y \equiv 3 \pmod{7} & y \equiv 3 \pmod{11} \\
 \\ 
 y_1 = -1 & y_2 = 1 & y_3 = 3 & y_4 = 3
 \end{array}$$

Finally, we can form the unique solution (modulo 770) of our system:

$$\begin{aligned}
 \bar{x} &= a_1 N_1 y_1 + a_2 N_2 y_2 + a_3 N_3 y_3 + a_4 N_4 y_4 \\
 &= (-2)(154)(-1) + (1)(385)(1) + (2)(110)(3) + (4)(70)(3) \\
 &= 308 + 385 + 660 + 840 \\
 &= 2193 \\
 &\equiv -117 \pmod{770}
 \end{aligned}$$

3. (8 points) Use Fermat's Theorem to prove that if  $\gcd(a, 133) = \gcd(b, 133) = 1$ , then  $133 \mid a^{18} - b^{18}$ .

**Solution:**

Claim:  $\forall a, b \in \mathbb{Z}$ , if  $\gcd(a, 133) = \gcd(b, 133) = 1$ , then  $a^{18} \equiv b^{18} \pmod{133}$ .

Proof: Let  $a, b \in \mathbb{Z}$  such that  $\gcd(a, 133) = \gcd(b, 133) = 1$ . Noticing that  $133 = 7 \cdot 19$ , this implies that  $7 \nmid a$  and  $19 \nmid a$ . Hence we can apply Fermat's Little Theorem for each prime to get

$$\begin{array}{cccc}
 a^6 \equiv 1 \pmod{7} & a^{18} \equiv 1 \pmod{19} & b^6 \equiv 1 \pmod{7} & b^{18} \equiv 1 \pmod{119} \\
 a^{18} \equiv 1 \pmod{7} & & b^{18} \equiv 1 \pmod{7} & 
 \end{array}$$

Since  $\gcd(7, 19) = 1$ , we can consider the two congruences involving  $a^{18}$  as a system and apply the CRT to obtain a unique solution modulo  $133 = 7 \cdot 19$ . However, we observe that  $a^{18} \equiv 1 \pmod{133}$  is a solution, so it must be the unique solution guaranteed by the CRT. The same reasoning tells us that  $b^{18} \equiv 1 \pmod{133}$ . Thus  $a^{18} \equiv b^{18} \pmod{133}$ .

4. (8 points) Derive the congruence:  $a^{21} \equiv a \pmod{15}$  for all  $a \in \mathbb{Z}$ .

**Hint:** You may not be able to use Fermat's Theorem (why not?) but what about its corollary?

**Solution:**

Claim:  $\forall a \in \mathbb{Z}, \quad a^{21} \equiv a \pmod{15}$ .

Proof: Let  $a \in \mathbb{Z}$ . Noticing that  $15 = 3 \cdot 5$ , we can apply the corollary to Fermat's Theorem to get

$$\begin{array}{ll} a^3 \equiv a \pmod{3} & a^5 \equiv a \pmod{5} \\ a^{21} \equiv a^7 \pmod{3} & a^{20} \equiv a^4 \pmod{5} \\ a^{21} \equiv (a^3)^2 a \pmod{3} & a^{21} \equiv a^5 \pmod{5} \\ a^{21} \equiv (a)^2 a \pmod{3} & a^{21} \equiv a \pmod{5} \\ a^{21} \equiv a^3 \pmod{3} & \\ a^{21} \equiv a \pmod{3} & \end{array}$$

Since  $\gcd(3, 5) = 1$ , we can consider the two final congruences involving  $a^{21}$  as a system and apply the CRT to obtain a unique solution modulo  $15 = 3 \cdot 5$ . However, we observe that  $a^{21} \equiv a \pmod{15}$  is a solution, so it must be the unique solution guaranteed by the CRT.

5. (8 points) Determine whether 17 is prime by determining whether  $16! \equiv -1 \pmod{17}$ .

**Solution:** Notice that

$$\begin{aligned} 16! &= 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \\ &= 16(15 \cdot 8)(14 \cdot 11)(13 \cdot 4)(12 \cdot 10)(9 \cdot 2)(7 \cdot 5)(6 \cdot 3) \\ &= 16 \cdot 120 \cdot 154 \cdot 52 \cdot 120 \cdot 18 \cdot 35 \cdot 18 \\ &\equiv (-1) \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \pmod{17} \\ &\equiv -1 \pmod{17}. \end{aligned}$$

Thus 17 is prime by Wilson's Theorem.