

1. (3 points) Given that $x = 6$ is a solution for $6x \equiv 15 \pmod{21}$, determine all solutions to $6x \equiv 15 \pmod{21}$.

$$x_0 = 6, \text{ the other solutions are } 6 + \frac{21}{d}, 6 + 2 \cdot \frac{21}{d} + \dots 6 + (d-1) \frac{21}{d}.$$

where $d = \gcd(21, 6)$
 $= 3$

$$\text{so } 6, 6+7, 6+14 \text{ i.e. } x \equiv 6, 13, 20 \pmod{21}.$$

2. (8 points) Solve the system of congruences using the Chinese remainder theorem:

$$x \equiv 2 \pmod{3}$$

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

$$x \equiv 5 \pmod{7}$$

First solve

$$(5 \cdot 7) y_1 \equiv 1 \pmod{3} \Leftrightarrow y_1 \equiv 2 \pmod{3} \equiv -1 \pmod{3}.$$

$$(3 \cdot 7) y_2 \equiv 1 \pmod{5} \Leftrightarrow y_2 \equiv 1 \pmod{5}.$$

$$(5 \cdot 3) y_3 \equiv 1 \pmod{7} \Leftrightarrow y_3 \equiv 1 \pmod{7}.$$

Solution to given system

$$X \equiv (35y_1) \cdot 2 + (21y_2) \cdot 3 + (15y_3) \cdot 5.$$

$$\equiv -70 + 21 \cdot 3 + 75.$$

$$\equiv \overset{5}{40} + 63 \equiv 68 \pmod{(3 \cdot 5 \cdot 7)} \\ = 105).$$

$$\left[\begin{array}{l} 3 \cdot 7 = 21 \equiv 1 \pmod{5} \\ 5 \cdot 3 = 15 \equiv 1 \pmod{7} \\ 5 \cdot 7 = 35 \equiv -1 \pmod{3} \end{array} \right.$$

3. (4 points) Use Fermat's theorem to show that $5^{32} - 3$ is divisible by 11.

$$\text{By Fermat, } 5^{10} \equiv 1 \pmod{11}$$

$$\text{so } 5^{32} = 5^{30} \cdot 5^2 = (5^{10})^3 \cdot 5^2 \\ \equiv 1 \cdot 25 \equiv 3 \pmod{11}.$$

$$\text{so } 11 \mid 5^{32} - 3.$$