

SOLUTIONS TO HOMEWORK 7
Math 104 - Dr. Evans
UCSD Winter 2004

1. For the following congruence relations, either find a solution or show that no solution exists.

$$\begin{aligned}x &\equiv 27 \pmod{60} \\x &\equiv 12 \pmod{105}\end{aligned}$$

Proof. First we check that the difference of 27 and 12 is divisible by the greatest common divisor of 60 and 105. This is clear since $27 - 12 = 15$ and $\gcd(60, 105) = 15$. So a solution between 1 and $\text{lcm}(60, 105) = 420$ exists.

We may proceed either by substitution, or break into smaller relatively prime moduli. In the first method, $x \equiv 27 \pmod{60}$ implies $x = 27 + 60k$ for some integer k . Plugging this into the second equation, we have

$$\begin{aligned}27 + 60k &\equiv 12 \pmod{105} \\60k &\equiv -15 \pmod{105} \\60k &= -15 + 105l \quad \text{for some integer } l \\4k &= -1 + 7l \\4k &\equiv -1 \pmod{7} \\k &\equiv -2 \equiv 5 \pmod{7} \\k &= 5 + 7m \quad \text{for some integer } m \\x &= 27 + 60(5 + 7m) = 327 + 420m \\x &\equiv 327 \pmod{420}\end{aligned}$$

Alternatively, one could reduce the equations by $\gcd(60, 105) = 15$, $\frac{60}{\gcd(60,105)} = 4$, and $\frac{105}{\gcd(60,105)} = 7$ to get the equations:

$$\begin{aligned}x &\equiv 3 \pmod{4} \\x &\equiv 5 \pmod{7} \\x &\equiv 12 \pmod{15}\end{aligned}$$

Then one could solve these by the method illustrated in number 3. We omit the details, but the answer will be the same as with substitution.

2. For the following congruence relations, either find a solution or show that no solution exists.

$$\begin{aligned}x &\equiv 40 \pmod{253} \\x &\equiv 50 \pmod{429}\end{aligned}$$

Proof. In this case, the difference of 40 and 50 is 10, and $\gcd(253, 429) = 11$. Since 11 does not divide 10, no solution exists.

3. For the following congruence relations, either find a solution or show that no solution exists.

$$x \equiv 3 \pmod{11}$$

$$x \equiv 5 \pmod{12}$$

$$x \equiv 7 \pmod{13}$$

Proof. From class, the general solution to

$$x \equiv a \pmod{p}$$

$$x \equiv b \pmod{q}$$

$$x \equiv c \pmod{r}$$

is given by

$$x = aqr(qr)^{-1} + bpr(pr)^{-1} + cpq(pq)^{-1}$$

where the first inverse is modulo p , the second modulo q , and the third modulo r .

In this case,

$$(qr)^{-1} = (12 \cdot 13)^{-1} \equiv (1 \cdot 2)^{-1} \equiv 6 \pmod{11}$$

$$(pr)^{-1} = (11 \cdot 13)^{-1} \equiv (-1 \cdot 1)^{-1} \equiv -1 \pmod{12}$$

$$(pq)^{-1} = (11 \cdot 12)^{-1} \equiv (-1 \cdot -2)^{-1} \equiv 7 \pmod{13}$$

Therefore,

$$x = 3 \cdot 12 \cdot 13 \cdot 6 + 5 \cdot 11 \cdot 13 \cdot (-1) + 7 \cdot 11 \cdot 12 \cdot 7 = 8561 \equiv 1697 \pmod{1716}$$

4. Prove the identity

$$(z^2 + ab)(ax^2 + by^2 - cz^2 - abc) = a(xz + by)^2 + b(yz - ax)^2 - c(z^2 + ab)^2$$

Proof.

$$\begin{aligned} & (z^2 + ab)(ax^2 + by^2 - cz^2 - abc) \\ &= ax^2z^2 + by^2z^2 - cz^4 - abc z^2 + a^2bx^2 + ab^2y^2 - abc z^2 - a^2b^2c \\ &= (ax^2z^2 + 2abxyz + ab^2y^2) + (by^2z^2 - 2abxyz + ba^2x^2) - (c^4 + 2abcz^2 + ca^2b^2) \\ &= a(xz + by)^2 + b(yz - ax)^2 - c(z^2 + ab)^2 \end{aligned}$$