

*If the Sun refused to shine,  
 I don't mind, I don't mind.  
 If the mountains fell in the sea,  
 Let it be, it ain't me.  
 Now, if six turned out to be nine,  
 Oh I don't mind, I don't mind...*  
 Jimi Hendrix, "If Six Was Nine," from the album *Axis: Bold as Love*, 1967.

**Question 1.** If six turned out to be nine...

(a) ... that is, if  $6 \equiv 9 \pmod{m}$ , what would the value of  $m > 1$  be?

(b) Now, if  $6 \equiv 69 \pmod{m}$ , what are the possible values for  $m > 1$ ?

**Question 2.** Find the smallest number  $\geq 120120$  which is divisible by no prime  $p < 20$ , using congruences. (Hint: calculate  $120120 \pmod{p}$ , for every prime  $p < 20$ .)

**Question 3.** Find all  $x \in \mathbb{Z}$  that satisfy the following linear congruence, or explain why no integral solutions exist (these are individual congruences, and not a system!).

(a)  $6x \equiv 9 \pmod{11}$ ,

(b)  $6x \equiv 11 \pmod{9}$ ,

(c)  $6x \equiv 9 \pmod{15}$ .

**Question 4.** Solve the following systems:

$$\begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 4 \pmod{8} \\ x \equiv 3 \pmod{9} \end{cases}, \quad \begin{cases} z \equiv 5 \pmod{7} \\ z \equiv 2 \pmod{8} \\ z \equiv 1 \pmod{9} \end{cases}, \quad \begin{cases} y \equiv 1 \pmod{7} \\ y \equiv 3 \pmod{8} \\ y \equiv 6 \pmod{9} \end{cases}.$$

**Question 5.** Solve the following systems:

$$\begin{cases} x \equiv -3 \pmod{11} \\ x \equiv 103 \pmod{13} \\ x \equiv 3 \pmod{15} \end{cases}, \quad \begin{cases} y \equiv 25 \pmod{11} \\ y \equiv 35 \pmod{13} \\ y \equiv 31 \pmod{15} \end{cases}.$$

**Question 6.** Solve:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{5} \\ x \equiv 5 \pmod{6} \\ x \equiv 5 \pmod{12} \end{cases}.$$

**Question 7.** A prime  $p$  is a safe prime if  $p = 2q + 1$  where  $q$  is also prime. The prime  $q$ , in turn, is called a Sophie Germain prime. For instance,  $p = 5 = 2 \cdot 2 + 1$  and  $p = 7 = 2 \cdot 3 + 1$  are the first two safe primes, and  $q = 2$  and  $q = 3$  are the first two Sophie Germain primes. Suppose that  $p > 7$  is a safe prime and prove the following.

(a) Show that  $p \equiv 2 \pmod{3}$ .

(b) Show that  $p \equiv 3 \pmod{4}$ .

(c) Show that if  $p > 11$ , then  $p \not\equiv 1 \pmod{5}$ .

(d) Use the previous congruences to show that  $p \equiv 23, 47$  or  $59 \pmod{60}$ .

(e) Use (d) to find 10 safe primes larger than 1000.

**Question 8.**

(a) Find all solutions for the congruence  $x^2 \equiv 1 \pmod{8}$ .

(b) Find all solutions for  $x^2 \equiv 1 \pmod{5}$ .

(c) Use (a) and (b) and the Chinese remainder theorem to find all solutions for  $x^2 \equiv 1 \pmod{40}$ .

**Question 9.**

(a) Find all the congruence classes modulo 35 that are zero-divisors in  $\mathbb{Z}/35\mathbb{Z}$ .

(b) Find all the congruence classes modulo 35 that are units in  $\mathbb{Z}/35\mathbb{Z}$ .

(c) For each unit modulo 35, find its multiplicative inverse.

(d) Repeat parts (a), (b) and (c) for the ring  $\mathbb{Z}/11\mathbb{Z}$ .

**Question 10.**

(a) Justify the following congruence modulo 11:

$$\begin{aligned} 10! &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\ &\equiv 1 \cdot 2 \cdot 2^{-1} \cdot 3 \cdot 3^{-1} \cdot 5 \cdot 5^{-1} \cdot 7 \cdot 7^{-1} \cdot 10 \\ &\equiv 1 \cdot 10 \equiv -1 \pmod{11}. \end{aligned}$$

(b) Generalize the formula in (a) to prove that if  $p$  is any prime then  $(p-1)! \equiv -1 \pmod{p}$ .