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 $6 \equiv 9 \bmod m$, what would the value of $m > 1$ be?

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

Solution:
(a) If $6 \equiv 9 \bmod m$, then $9 - 6 = 3$ is divisible by m. Thus, we must have $m = 3$.

(b) If $6 \equiv 69 \bmod m$, then $69 - 6 = 63 = 3^2 \cdot 7$ is divisible by m. Thus, m can be any of the positive divisors of 63. Hence, $m \in \{3, 7, 9, 21, 63\}$.

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

Solution:
We begin by calculating the least residue of 120120 modulo every prime < 20, i.e. modulo $2, 3, 5, 7, 11, 13, 17$ and 19. Respectively, these congruences are:

$$120120 \equiv 0, 0, 0, 0, 0, 0, 15, 2.$$

Notice that all the zeros follow from the divisibility tests that we have learned in class. Therefore, the number $120120 + 1$ must be congruent to:

$$120121 \equiv 1, 1, 1, 1, 1, 1, 16, 3$$

modulo $2, 3, 5, 7, 11, 13, 17$ and 19, respectively. Hence, it is not divisible by any of those primes and it is the least with such property (it is in fact a prime number).

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) $6x \equiv 9 \bmod 11$,

(b) $6x \equiv 11 \bmod 9$,

(c) $6x \equiv 9 \bmod 15$.

Solution:

(a) The congruence $6x \equiv 9 \bmod 11$ has a solution if and only if 11 divides $6x - 9$, if and only if the line $6x + 11y = 9$ has an integral solution (x, y). Since $\gcd(6, 11) = 1$, we know that there are solutions. Using Euclid on 6 and 11, and solving Bezout's identity, we obtain a formula for all integral solutions

$$x = 7 + 11k,\ y = -3 - 6k, \quad \text{for all } k \in \mathbb{Z}.$$

Thus, the solution to the congruence is $x = 7 + 11k$, for all $k \in \mathbb{Z}$, or equivalently, $x \equiv 7 \bmod 11$.

(b) The congruence $6x \equiv 11 \bmod 9$ has a solution if and only if the line $6x + 9y = 11$ has an integral solution. However, $\gcd(6, 9) = 3$ does not divide 11, so the line has no integral points. Thus, the congruence has no solutions with $x \in \mathbb{Z}$.

(c) The congruence $6x \equiv 9 \bmod 15$ has a solution if and only if the line $6x + 15y = 9$ has an integral solution. Since $\gcd(6, 15) = 3$ and 3 divides 9, we do have solutions. Using Euclid for 6 and 15 and then backwards to solve Bezout's identity, we can find all solutions to $6x + 15y = 3$, and multiplying through by 3, we can find all solutions to $6x + 15y = 9$. These are given by:

$$x = 4 + 5k,\ y = -1 - 2k, \quad \text{for all } k \in \mathbb{Z}.$$

Hence, the solutions to the congruence are the numbers of the form $x = 4 + 5k$, or equivalently, $x \equiv 4 \bmod 5$.

Question 4. Solve the following systems:

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

Solution:
We first solve the following easier systems:

$$\begin{cases} x_1 \equiv 1 \bmod 7 \\ x_1 \equiv 0 \bmod 8 \\ x_1 \equiv 0 \bmod 9 \end{cases}, \quad \begin{cases} x_2 \equiv 0 \bmod 7 \\ x_2 \equiv 1 \bmod 8 \\ x_2 \equiv 0 \bmod 9 \end{cases}, \quad \begin{cases} x_3 \equiv 0 \bmod 7 \\ x_3 \equiv 0 \bmod 8 \\ x_3 \equiv 1 \bmod 9 \end{cases}.$$

Let me know if you need help solving these! The solutions are: $x_1 \equiv 288 \bmod 504$, $x_2 \equiv 441 \bmod 504$ and $x_3 \equiv 280 \bmod 504$. Therefore, now we can solve the original problems:

$$\begin{aligned} x &\equiv 2 \cdot x_1 + 4 \cdot x_2 + 3 \cdot x_3 \equiv 2 \cdot 288 + 4 \cdot 441 + 3 \cdot 280 \equiv 156 \bmod 504, \\ z &\equiv 5 \cdot x_1 + 2 \cdot x_2 + 1 \cdot x_3 \equiv 5 \cdot 288 + 2 \cdot 441 + 1 \cdot 280 \equiv 82 \bmod 504, \\ y &\equiv 1 \cdot x_1 + 3 \cdot x_2 + 6 \cdot x_3 \equiv 1 \cdot 288 + 3 \cdot 441 + 6 \cdot 280 \equiv 267 \bmod 504. \end{aligned}$$

Question 5. Solve the following systems:

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

Solution:
First, we simplify the systems to:

$$\begin{cases} x \equiv 8 \bmod 11 \\ x \equiv 12 \bmod 13 \\ x \equiv 3 \bmod 15 \end{cases}, \quad \begin{cases} y \equiv 3 \bmod 11 \\ y \equiv 9 \bmod 13 \\ y \equiv 1 \bmod 15 \end{cases}.$$

Now find solutions to the basic systems:

$$\begin{cases} x_1 \equiv 1 \bmod 11 \\ x_1 \equiv 0 \bmod 13 \\ x_1 \equiv 0 \bmod 15 \end{cases}, \quad \begin{cases} x_2 \equiv 0 \bmod 11 \\ x_2 \equiv 1 \bmod 13 \\ x_2 \equiv 0 \bmod 15 \end{cases}, \quad \begin{cases} x_3 \equiv 0 \bmod 11 \\ x_3 \equiv 0 \bmod 13 \\ x_3 \equiv 1 \bmod 15 \end{cases}.$$

The solutions are: $x_1 \equiv 1365 \bmod 2145$, $x_2 \equiv 495 \bmod 2145$ and $x_3 \equiv 286 \bmod 2145$. Thus:

$$x \equiv 8 \cdot x_1 + 12 \cdot x_2 + 3 \cdot x_3 \equiv 8 \cdot 1365 + 12 \cdot 495 + 3 \cdot 286 \equiv 558 \bmod 2145,$$
$$y \equiv 3 \cdot x_1 + 9 \cdot x_2 + 1 \cdot x_3 \equiv 3 \cdot 1365 + 9 \cdot 495 + 1 \cdot 286 \equiv 256 \bmod 2145.$$

Question 6. Solve:

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

Solution:
Be careful! The Chinese Remainder Theorem does not apply directly to this problem because some of the moduli are not relatively prime. However, note that $x \equiv 1 \mod 2$ and $x \equiv 5 \mod 6$ are redundant (because if $x \equiv 5 \mod 6$ then it must be also $\equiv 1 \mod 2$). Also, $x \equiv 5 \mod 6$ and $x \equiv 5 \mod 12$ are redundant, because if $x \equiv 5 \mod 12$ then it is also $\equiv 5 \mod 12$. Thus, the original system is equivalent to:

$$\begin{cases} x \equiv 2 \mod 5 \\ x \equiv 5 \mod 12. \end{cases}$$

Now the Chinese Remainder Theorem applies, and the solution is $x \equiv 17 \mod 60$.

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 $p \equiv 2 \bmod 3$.

(b) Show that $p \equiv 3 \bmod 4$.

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

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

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

Solution:

(a) ($p \equiv 2 \bmod 3$). Suppose $p > 7$. If $q \equiv 1 \bmod 3$ then p would be $p \equiv 0 \bmod 3$ and therefore not prime. Thus $q \equiv 2 \bmod 3$ and $p \equiv 2 \cdot 2 + 1 \equiv 2 \bmod 3$.

(b) ($p \equiv 3 \bmod 4$). Suppose $p > 7$. If q is prime then $q \equiv 1$ or $3 \bmod 4$. In both cases $p \equiv 2 \cdot 1 + 1 \equiv 2 \cdot 3 + 1 \equiv 3 \bmod 4$.

(c) ($p \not\equiv 1 \bmod 5$). Suppose $p \equiv 1 \bmod 5$. Since $q > 5$ is prime then $q \equiv 1, 2, 3, 4 \bmod 5$ and $2q + 1 \not\equiv 1 \bmod 5$ in any case. Thus $p \not\equiv 1 \bmod 5$.

(d) Therefore, a safeprime must be a prime p which is a solution of the following system:

$$\begin{cases} p \equiv 2 \bmod 3 \\ p \equiv 3 \bmod 4 \\ p \equiv 2, 3, \text{ or } 4 \bmod 5 \end{cases}$$

or equivalently:

$$\begin{cases} p \equiv 11 \bmod 12 \\ p \equiv 2 \bmod 5 \end{cases}, \quad \begin{cases} p \equiv 11 \bmod 12 \\ p \equiv 3 \bmod 5 \end{cases}, \quad \begin{cases} p \equiv 11 \bmod 12 \\ p \equiv 4 \bmod 5 \end{cases}$$

Hence: $p \equiv 23, 47$ or $59 \bmod 60$.

(e) Hence, to find more safeprimes, look for primes in the congruence classes $p \equiv 23, 47$ or $59 \bmod 60$ and then check if they are of the form $p = 2q + 1$, i.e., check that p is a prime, and check also that $q = (p-1)/2$ is a prime. The first few safe primes are

5, 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467, 479, 503, 563, 587, 719, 839, 863, 887, 983, 1019, 1187, 1283, 1307, 1319, 1367, 1439, 1487, 1523, 1619, 1823, 1907.

Question 8.

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

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

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

Solution:

First, note that $40 = 8 \cdot 5$. We want to solve $x^2 \equiv 1 \mod 40$, so we solve instead:

$$\begin{cases} x^2 \equiv 1 \mod 8 \\ x^2 \equiv 1 \mod 5. \end{cases}$$

This is equivalent to:

$$\begin{cases} x \equiv 1, 3, 5, 7 \mod 8 \\ x \equiv 1, 4 \mod 5. \end{cases}$$

The possible solutions are: $x \equiv 1, 9, 11, 19, 21, 29, 31, 39 \mod 40$.

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 $\mathbb{Z}/11\mathbb{Z}$.

Solution:

1. The zero-divisors in $\mathbb{Z}/35\mathbb{Z}$ are those congruences $a \bmod 35$ such that $1 \leq a \leq 34$ and $\gcd(a, 35) > 1$, i.e., a is divisible by 5 or 7. Thus, the zero-divisors are

$$5, 7, 10, 14, 15, 20, 21, 25, 28, 30 \bmod 35.$$

2. The units in $\mathbb{Z}/35\mathbb{Z}$ are those congruences $a \bmod 35$ such that $1 \leq a \leq 34$ and $\gcd(a, 35) = 1$. Thus, the units are

$$1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34 \bmod 35.$$

Notice that $\varphi(35) = \varphi(5)\varphi(7) = 4 \cdot 6 = 24$.

3. For each unit $a \bmod 35$ listed above, you need to find $a^{-1} \bmod 35$, i.e., find $b \bmod 35$ such that $a \cdot b \equiv 1 \bmod 35$. For instance,

$$2^{-1} \equiv 18, \quad 3^{-1} \equiv 12, \quad 4^{-1} \equiv 9 \bmod 35.$$

4. Since 11 is prime, $\mathbb{Z}/11\mathbb{Z}$ is a field, and there are no zero-divisors. Every non-zero element $1, \ldots, 10 \bmod 11$ is a unit. Find each multiplicative inverse, as above. For instance,

$$2^{-1} \equiv 6, \quad 3^{-1} \equiv 4, \quad 4^{-1} \equiv 4 \bmod 11.$$

Question 10.

(a) Justify the following congruence modulo 11:

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

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

Solution:
Let $p \geq 2$ be a prime. The congruence classes in $U_p = \{1, 2, \ldots, p-1\}$ are all units in $\mathbb{Z}/p\mathbb{Z}$ because they are all relatively prime to p. First we prove two preliminary results:

1. Every unit in $\mathbb{Z}/p\mathbb{Z}$ has a unique inverse element modulo p. Let u be a unit, thus $ux \equiv 1 \bmod p$ has a solution (because $(u, p) = 1$). Let us call the solution v. Thus v is also a unit and it is an inverse for u. Suppose that v' is also an inverse, i.e. $uv' \equiv 1 \bmod p$. Then:
$$uv' \equiv uv \bmod p$$
and since u is a unit, we also have that $v' \equiv v \bmod p$ and therefore they are the same unit modulo p.

2. The only units u in $\mathbb{Z}/p\mathbb{Z}$ that are their own inverse (i.e. $u \cdot u \equiv 1 \bmod p$) are $u \equiv \pm 1 \bmod p$. To prove this, suppose x is such that $x \cdot x \equiv x^2 \equiv 1 \bmod p$. Then $x^2 - 1$ is divisible by p and hence p divides $(x-1)(x+1)$. Since p is prime and p divides a product of two factors, it must divide one of the factors, so either p divides $x - 1$ or $x + 1$. And this is equivalent to $x \equiv 1$ or $x \equiv -1 \bmod p$.

Therefore, every unit has a unique inverse and only ± 1 are their own inverses. This implies that we can arrange the numbers $2, 3, \ldots, p-2$ in pairs: $u_1, v_1, u_2, v_2, \ldots u_{(p-3)/2}, v_{(p-3)/2}$ such that v_i is the inverse of u_i. Hence:

$$\begin{aligned}
(p-1)! &\equiv 1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1) \\
&\equiv 1 \cdot u_1 \cdot v_1 \cdot u_2 \cdot v_2 \cdots u_{(p-3)/2} \cdot v_{(p-3)/2} \cdot (p-1) \\
&\equiv 1 \cdot (p-1) \equiv p - 1 \equiv -1 \bmod p
\end{aligned}$$

as claimed.