Modular Arithmetic

Remark: What may we not do in modular arithmetic?

1. Divide by integers:
   \[ a \equiv c \pmod{n}, \quad b \equiv d \pmod{n} \]
   But \[ c \not\equiv b \pmod{n} \].
   For example: \[ 4 \equiv 2 \pmod{2} \] but \[ 2 \not\equiv 1 \pmod{2} \].

2. Take roots:
   \[ a^2 \equiv b^2 \pmod{n}, \quad \not\equiv a \equiv b \pmod{n} \]
   For example: \[ 8 \equiv 1 \pmod{7} \] but \[ 2 \not\equiv 1 \pmod{7} \].

Suppose that \[ x \equiv 1 \pmod{2} \]
Show that either \[ x \equiv 1 \pmod{6}, x \equiv 3 \pmod{6} \],
or \[ x \equiv 5 \pmod{6} \).

Since \[ x \equiv 1 \pmod{2} \], \( x \) is odd. Now suppose that \[ x \equiv r \pmod{6} \]
for \( r = 0, 2, \) or \( 4 \). Then \( \exists b \in \mathbb{Z} \) such that \[ x = r + 6b \],
so in particular \( x \) is even. This is a contradiction.
So \( r \) must be 1, 3, or 5.
What does $\mathbb{Z}$ tell us? A single congruence class modulo 2 is equal to the union of three congruence classes modulo 6.

In general: one congruence class modulo $n$ is equal to the union of $\phi(n)$ congruence classes modulo $n$.

**Lemma:** Suppose that $b$ is divisible by $g = \gcd(a, m)$. Then $a \equiv b \pmod{n}$ has $\frac{\phi(n)}{g}$ distinct congruence (mod $n$) class solutions.

**Proof:**

Let $x$ be a solution of $a \equiv b \pmod{n}$. Then there exists $y \in \mathbb{Z}$ such that $(x, y)$ solves the linear Diophantine equation $ax - ny = b$.

Both sides of this equation are divisible by $g$, so if we rewrite

\[
\begin{cases}
  b = \frac{a}{g} \\
  l = \frac{n}{g} \\
  m = \frac{b}{g}
\end{cases}
\]

then we have that $lx - ly \equiv m \pmod{l}$, or that $lx \equiv m \pmod{l}$.

Crucially, now $gcd(b, l) = 1$, so this congruence equation
has a unique congruence (mod $k$) class solution. This congruence (mod $k$)
class is equal to a union of $g$ (since $m = kg$) congruence (mod $n$) classes.

[2] Solve $6x \equiv 3 \pmod{27}$

Since $\gcd(6, 27) = 3$, there are three congruence (mod $27$) class
solutions.

Since $6x \equiv 3 \pmod{27}$, $6x - 27y = 3$ for some $y \in \mathbb{Z}$,
we use the Euclidean Algorithm:

\[ 27 = 4 \cdot 6 + 3 \]
\[ 6 = 2 \cdot 3 \]

Therefore $3 = 27 - 4 \cdot 6$, i.e. $(x, y) = (-4, -1)$ is a particular solution.

This tells us that $x = -4 \pmod{27}$ is a solution.

Since $\frac{2x}{3} = 9$, the other two solutions are $x \equiv -4 + 9 \equiv 5 \pmod{27}$
and $x \equiv -4 + 9 \equiv 14 \pmod{27}$.

[3] Solve $2x \equiv 1 \pmod{9}$ and $6x \equiv 3 \pmod{9}$. What conclusion
can you make about multiplying a congruence equation by an
integer?
(a) Solving $2x \equiv 1 \pmod{9}$.

Since \(\gcd(2,9) = 1\), there is a unique congruence \((\mod 9)\) class solution.

By using the Euclidean Algorithm, or by inspection, we see that \(x \equiv 5 \pmod{9}\) is the solution.

(b) Solving $6x \equiv 3 \pmod{9}$.

Since \(\gcd(6,9) = 3\), there are three congruence \((\mod 9)\) class solutions. By using the Euclidean Algorithm, or by inspection, we see that \(x \equiv 2 \pmod{9}\) is a solution. Since \(\frac{9}{\gcd(6,9)} = \frac{9}{3} = 3\), the other two solutions are \(x \equiv 5 \pmod{9}\) and \(x \equiv 8 \pmod{9}\).

Multiplying a congruence equation by an integer may thus create additional solutions. This shows that multiplying a congruence equation by an integer is not a reversible operation, and that is precisely why we cannot always divide congruence equations by integers.