Dividing the sides of a congruence

Unlike addition and multiplication, one needs to be careful when dividing the two sides of a congruence. For example, consider $30 \equiv 12 \pmod{9}$, dividing by 3 yields $10 \equiv 4 \pmod{9}$, which is wrong! In general, we can do so only when that number is relatively prime to the modulus.

Proposition: (No proof)
If $ac \equiv bc \pmod{n}$, and $\gcd(c,n) = 1$, then $a \equiv b \pmod{n}$.

Intuitively, $\gcd(c,n) = 1$ implies that we can shorten the "cycle" of the modulus, e.g., the previous example $30 \equiv 12 \pmod{9}$, after division by 3, the "cycle" is $9/3 = 3$, thus $10 \equiv 4 \pmod{3}$.

On the other hand, if we divide by 2, we get $15 \equiv 6 \pmod{9}$, which is incorrect, as $\gcd(9,2) = 1$.

Example:
By the proposition, the solutions to $2x \equiv 1 \pmod{9}$, $6x \equiv 3 \pmod{9}$ are not the same ($0 \equiv 3 \pmod{9}$). Indeed, the solutions are:

$2x \equiv 1 \pmod{9} \Rightarrow x = 5$.
$6x \equiv 3 \pmod{9} \Rightarrow x = 2, 5, 8$. 
Problems: Solve the following pair of congruences, or explain why a solution does not exist.

\[ 2x + 3y \equiv 1 \pmod{6} \]
\[ x + 3y \equiv 4 \pmod{6}. \]

Solution:
Adding the two congruences yields:

\[ 3x + 6y \equiv 5 \pmod{6} \]
[Recall that mod is close under addition.]

Since \( 6y \equiv 0 \pmod{6} \), we have:

\[ 3x \equiv 5 \pmod{6}. \]

But this has no solution! The values of \( 3x \pmod{6} \) are only 0 and 3. Thus no \( x,y \) satisfy the solution.

Additive Inverse:
Every integer \( a \) has an additive inverse \( \pmod{n} \n \)
That is, an integer \( x \) satisfying:

\[ a + x \equiv 0 \pmod{n} \]

For example, \( x = -a \), or \( x = n - a \) are additive inverse \( \pmod{n} \) of \( a \).
This implies that the congruence:
\[
\frac{a + x \equiv b \pmod{n}}{}
\]
always has a solution of the form:
\[
x = b + (-a) = b - a.
\]
On the other hand, not every congruence of the form \(ax \equiv b \pmod{n}\) has a solution, e.g.,
\[
3x \equiv 1 \pmod{6}
\]
does not have a solution as \(3x \pmod{6}\) is always 0 or 3.
However, \(3x \equiv 1 \pmod{7}\) has a solution, for example \(x = 5\) is a solution.
Why is that?
- Here, the difference is in the modulus. In the last example, 3 and 7 are relatively primes,
  whereas 3 and 6 are not.

Small observation: consider again \(3x \equiv 1 \pmod{7}\).
We can quickly verify that each integer
between 0 and 6 is \(3x \pmod{7}\) for some \(x\). In other words, \(3x \pmod{7}, x=0,1,...,6\)
spans the entire range \([0,6]\) of integers.
So we don't miss any integer in \([0,6]\)!
On the other hand, with \(3x \pmod{6}\), we
miss some of the integers in \([0,5]\),
in fact, we have only 0 or 3. That is, after a multiplication by 3, all integers \((\pmod{6})\)
"fall" on 0 or 3 only.
This property is shown more formally below:

**Proposition:**

Let \( n > 1 \) be a natural number, and let \( a \) be an integer with \( \gcd(a, n) = 1 \). Then:

1. There exists an integer \( s \), s.t. \( sa \equiv 1 \pmod{n} \). This integer is called a *multiplicative inverse*.
2. For any integer \( b \), the congruence \( ax \equiv b \pmod{n} \) has a solution.
3. The solution to \( ax \equiv b \pmod{n} \) is unique \( \pmod{n} \). That is, if \( ax_1 \equiv b \pmod{n} \) and \( ax_2 \equiv b \pmod{n} \) then \( x_1 \equiv x_2 \pmod{n} \).

**Proof:**

1. We know that \( \gcd(a, n) \) is a linear combination of \( a \) and \( n \). Since \( \gcd(a, n) = 1 \), we have:

\[
1 = sa + tn, \quad \text{for some integers } s, t.
\]

\[
\frac{1}{t} \left( sa - t - 1 \right) = s - t.
\]

\[
\left( sa - 1 \right) \text{ is divisible by } n.
\]

\[
sa \equiv 1 \pmod{n}
\]

\[
\Rightarrow s \text{ is our multiplicative inverse.}
\]
2. By part 1, we have $sa \equiv 1 \pmod{n}$. Multiplying the congruence $ax \equiv b \pmod{n}$ by $s$, we obtain:

\[ s \cdot ax \equiv s \cdot b \pmod{n} \]

\[ x \equiv sb \pmod{n}, \text{ since } sa \equiv 1 \pmod{n} \]

Indeed, let us verify that $x = sb$ is a solution to $ax \equiv b \pmod{n}$:

\[ a(sb) = (as) \cdot b \equiv 1 \cdot b \equiv b \pmod{n}. \]

Therefore $x = sb$ is a solution.

3. Uniqueness follows from the fact that if $a \cdot c \equiv b \cdot c \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$. [Dividing the sides of a congruence when $c, n$ are relatively primes].

In our case, $\gcd(c, n) = 1$, then if $a \cdot x_1 \equiv a \cdot x_2 \equiv b \pmod{n}$, we must have

\[ x_1 \equiv x_2 \pmod{n}. \]

Thus the solution is unique.

Finding the multiplicative inverse:

We use the method in the proof above in order to find the multiplicative inverse. That is, we use the fact that $\gcd(a, n) = 1$ in order to claim that there are integers $s, t$, such that $sa + t \cdot n = 1$. 

Example: Find $s$, such that $3s \equiv 1 \pmod{7}$.

Here, $1 = 5 \cdot 3 + 2 \cdot 7 \Rightarrow 3s - 1 = 7t$.

We now need to search among all integers $s, t$, which satisfy $3s - 1 = 7t$.

We test all values of $t$ (in $[0, 6]$):

$t=0 \Rightarrow s = \frac{1}{3}$ →

$t=1 \Rightarrow s = \frac{8}{3}$ →

$t=2 \Rightarrow s = 5$ →

$t=3 \Rightarrow s = \frac{22}{3}$ →

$t=4 \Rightarrow s = 29/3$ →

$t=5 \Rightarrow 3s = 36 \Rightarrow s = 12 \equiv 5 \pmod{7}$, but we already have this solution.

$t=6 \Rightarrow s = \frac{43}{3}$ →

$\Rightarrow s = 5$ is the multiplicative inverse.

Fermat's Little Theorem

This is another application of proposition (x).

Theorem (FLT)

If $p$ is a prime number and $p \nmid c$ (p does not divide c), then $c^{p-1} \equiv 1 \pmod{p}$.

We do not prove it, but let us see a few examples:

$p=2, c=7, p \nmid c, 7^7 \equiv 1 \pmod{2}$

$p=3, c=8, p \mid c, c^{p-1} = 8^2 = 64 \equiv 1 \pmod{3}$

$p=11, c=9, p \mid c, c^{p-1} = 9^{10} \equiv 1 \pmod{11}$. 
The Chinese Remainder Theorem

This is a strong tool to solve a system of simultaneous congruences.
For example:
\[
\begin{align*}
  x &\equiv 1 \pmod{4} \\
  x &\equiv 0 \pmod{30}.
\end{align*}
\]

This system does not have a solution, as the first congruence implies that \( x \) is odd, and the second implies that \( x \) is even.
Let us notice that the two moduli \( 4, 30 \) are not relatively primes.

Claim: suppose \( m, n \) are relatively primes; \( m, n \in \mathbb{N} \). Then for any integers \( a, b \), the system:
\[
\begin{align*}
  x &\equiv a \pmod{m} \\
  x &\equiv b \pmod{n}
\end{align*}
\]
has a solution.

Proof: Observe that since \( \gcd(m, n) = 1 \), there are integers \( s, t \), such that:
\[
s \cdot m + t \cdot n = 1.
\]
\[
\begin{align*}
  \boxed{x = a \cdot t \cdot n + b \cdot s \cdot m}
\end{align*}
\]
is a solution.
Indeed, since \( t \cdot n = 1 - s \cdot m \), we have \( t \cdot n \equiv 1 \pmod{m} \).
Similarly, \( sm \equiv 1 \pmod{n} \), since \( sm \equiv 1 \pmod{n} \).

Thus:

\[(a \cdot t \cdot n) + b(sm) \bmod m = x\]

\[= (a \cdot 1 + 0) \bmod m = a \cdot 1 \pmod m.\]

\[\Rightarrow x \equiv a \pmod m.\]

Similarly,

\[(a(tn) + b(sm)) \bmod n = \]

\[= (a \cdot 0 + b \cdot 1) \bmod n = b \cdot 1 \pmod n.\]

\[\Rightarrow x \equiv b \pmod n.\]

Thus \(x\) is a solution, as claimed.

Moreover, this solution is unique \(\bmod (mn)\).

That is, if \(x'\) is another solution then

\[x \equiv x' \pmod{mn}.\]

This is because if both \(x, x'\) satisfy \(x \equiv x' \pmod{mn}\), then

\[(x-x')\) is divisible by \(m\), and also divisible by \(n\)

\[\Rightarrow (x-x')\) is divisible by \(mn).\]

Example:

\[x \equiv 2 \pmod{4}, \quad x \equiv 6 \pmod{7}\]

Solution:

\[1 = \frac{5}{3}\]

\[\Rightarrow x \equiv 3(-1) \cdot 7 + 6 \cdot 2 \pmod{28}\]

\[\Rightarrow 3u \equiv 6 \pmod{28}\) is the unique solution.
This was a special case of the Chinese Remainder theorem.

Theorem [CRT] Suppose \( m_1, m_2, \ldots, m_t \) are pairwise relatively primes, that is, \( \gcd(m_i, m_j) = 1 \), for any \( i \neq j, \), \( i, j = 1, \ldots, t \).
Then for any integers \( a_1, a_2, \ldots, a_t \), the system of congruences:

\[
\begin{align*}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
& \quad \vdots \\
x &\equiv a_t \pmod{m_t}
\end{align*}
\]

has a solution, which is unique modulo the product \( m_1, m_2, \ldots, m_t \).

In our discussion above, we solved the case \( t = 2 \). This theorem is an extension for any \( t \geq 2 \).
In our discussion above we solved the case $t = 2$, and this theorem is an extension to any $t \geq 2$.

Determinability numbers by their remainders.

Let $n \in \mathbb{N}$. By the Fundamental theorem in arithmetic, $n$ can be written as a product of prime numbers:

$$ n = p_1^{d_1} p_2^{d_2} \ldots p_t^{d_t} $$

where $p_1, \ldots, p_t$ are unique primes and the exponents $d_i \geq 0$ (are integers).

Let $a \geq 1$ be some integer and let $d_i$ be its remainder after division by $p_i^{d_i}$.

Then this implies $a \equiv a_i \pmod{p_i^{d_i}}$.

Specifically:

$$ a \equiv a_1 \pmod{p_1^{d_1}} $$
$$ a \equiv a_2 \pmod{p_2^{d_2}} $$
$$ \vdots $$
$$ a \equiv a_t \pmod{p_t^{d_t}} $$

Since $p_1^{d_1}, p_2^{d_2}, \ldots, p_t^{d_t}$ are relatively prime (check!), the Chinese remainder theorem implies that $a$ is unique mod $n = p_1^{d_1} \ldots p_t^{d_t}$.

That is, $a$ is uniquely determined.

This idea is to have important applications in CS. For example, instead of storing large numbers it is sufficient to store the set of remainders as above. Then $a$ can be recovered.