Quick Summary

Definition: Integers a, b are ***congruent modulo m*** if and only if $m|a - b$

Congruence mod m is an equivalence relation

Theorem: $a \equiv b\ (mod\ m) \Leftrightarrow rem(a, m) = rem(b, m)$

Modular Arithmetic

Lemma:

1. $a \equiv b \ (mod\ m) \implies a + c \equiv b + c \ (mod\ m)$ Add common term to both sides.
2. $a \equiv b \ (mod\ m) \implies a \cdot c \equiv b \cdot c \ (mod\ m)$ Multiply by common term on both sides.
3. $a \equiv b \ (mod\ m) \ \wedge \ c \equiv d \ (mod\ m) \implies a + c \equiv b + d \ (mod\ m)$ Add equal numbers.
4. $a \equiv b \ (mod\ m) \ \wedge \ c \equiv d \ (mod\ m) \implies a \cdot c \equiv b \cdot d \ (mod\ m)$ Multiply equal numbers.

So far it looks just like normal arithmetic …..

Modular Arithmetic Calculations

What is $rem(999+376,7)$?
Recall: $a \equiv b\ (mod\ m)\ \wedge\ c \equiv d\ (mod\ m) \implies a+c \equiv b+d\ (mod\ m)$

$$\begin{aligned} 999 &\equiv rem(999,7) \equiv 5 \quad (mod\ 7) \\ 376 &\equiv rem(376,7) \equiv 5 \quad (mod\ 7) \\ 999+376 &\equiv 5+5 \equiv 3 \quad (mod\ 7) \end{aligned}$$

Similarly:

$$999 \times 376 \equiv 5 \times 5 \equiv 4 \quad (mod\ 7)$$

Furthermore:

$$\begin{aligned} &999+(999+376)^2+376^2 \\ &\equiv 5+3^2+5^2 \quad (mod\ 7) \\ &\equiv 5+2+4\ \ (mod\ 7) \\ &\equiv 4\ (mod\ 7) \end{aligned}$$

Moral: Keep reducing numbers to their class representative in $\mathbb{Z}_m$

Modular Arithmetic

Lemma:

1. $a \equiv b \ (mod\ m) \implies a + c \equiv b + c \ (mod\ m)$ Add common term to both sides.
2. $a \equiv b \ (mod\ m) \implies a \cdot c \equiv b \cdot c \ (mod\ m)$ Multiply by common term on both sides.
3. $a \equiv b \ (mod\ m) \ \wedge \ c \equiv d \ (mod\ m) \implies a + c \equiv b + d \ (mod\ m)$ Add equal numbers.
4. $a \equiv b \ (mod\ m) \ \wedge \ c \equiv d \ (mod\ m) \implies a \cdot c \equiv b \cdot d \ (mod\ m)$ Multiply equal numbers.

So far it looks just like normal arithmetic …..

Where things go haywire

If $a \cdot c \equiv b \cdot c \ (mod\ m)$ does it mean that $a \equiv b \ (mod\ m)$?

No, not always! But …

Theorem: If $a \cdot c \equiv b \cdot c \ (mod\ m)$ and $\gcd(c, m) = 1$ then $a \equiv b \ (mod\ m)$.

Solving Congruences

Solve for x: $3x \equiv 4\ (mod\ 17)$.

In regular arithmetic, to solve the equation $3x = 4$:

multiply both sides by $3^{-1} = 1/3$ to get $x = 4/3$.

But what's the analogue of 1/3 in arithmetic modulo 17 ???

Modular Inverses

Definition: If $a \cdot x \equiv 1\ (mod\ m)$ then we say that x is the inverse of a modulo m.

Note: $a, x \in \mathbb{Z}_m$

Notation: $x \equiv a^{-1}\ (mod\ m)$.

$x \equiv a^{-1}\ (mod\ m)$ also means that $a \equiv x^{-1}\ (mod\ m)$

Example: $3 \cdot 4\ \equiv 1\ (mod\ 11)$, so $3^{-1} \equiv 4\ (mod\ 11)$

Unfortunately, inverses modulo m don't always exist. For example, there is no element $x \in \mathbb{Z}_{12}$ such that $4x \equiv 1$. So, $4^{-1}(mod\ 12)$ doesn't exist.

How do we know when a number has an inverse?

GCD to the rescue again!

Theorem. If $\gcd(a, m) = 1$ then $a^{-1} (mod\ m)$ exists.

Corollary: If m is prime then every non-zero element in $\mathbb{Z}_m$ has an inverse.

Proof: $\gcd(a, m) = 1$

$\Rightarrow \exists s, t{:}\ \ sa + tm = 1$

$\Rightarrow tm = 1 - sa$

$\Rightarrow tm \equiv 1 - sa\ (mod\ m)$

$\Rightarrow 1 - sa \equiv 0\ (mod\ m)$ (since $m \mid tm$)

$\Rightarrow sa \equiv 1\ (mod\ m)$

$\Rightarrow s \equiv a^{-1}\ (mod\ m)$

So, given a, m: Check that $\gcd(a, m) =\ 1$, and use the Pulverizer to calculate $s = a^{-1}$.

Why calculate inverses?

Solve for x: $3x \equiv 4\ (mod\ 17)$.

$$3x \equiv 4\ (mod\ 17)$$

$$3^{-1} \cdot 3x \equiv 3^{-1} \cdot 4\ (mod\ 17)$$

$$1 \cdot x \equiv 3^{-1} \cdot 4\ (mod\ 17)$$

$$x \equiv 3^{-1} \cdot 4\ (mod\ 17)$$

Does $3^{-1}(mod\ 17)$ exist? Yes, 17 is prime.

Apply the Pulverizer to get $1 = 3 \cdot 6 - 17$

So, $3^{-1} \equiv 6\ (mod\ 17)$.

Final solution $x \equiv 6\ \cdot 4(mod\ 17)$

$x = 7, 24, 41, 58, \ldots$ all members of the equivalence class of 17.

Systems of Linear Congruences

Solve for x:

$$\begin{gathered} x \equiv 2\ (mod\ 3) \\ x \equiv 3\ (mod\ 5) \\ x \equiv 2\ (mod\ 7) \end{gathered}$$

Does a solution exist?

How many solutions exist?

How many solutions in $\mathbb{Z}_{105}$?

The Chinese Remainder Theorem

If $m_1, m_2, \ldots, m_n$ are pairwise relatively prime, the system

$$\begin{aligned} &x \equiv a_1 \ (mod\ m_1) \\ &x \equiv a_2 \ (mod\ m_2) \\ &: \\ &x \equiv a_n \ (mod\ m_n) \end{aligned}$$

has a *unique* solution modulo $m = m_1 \cdot m_2 \cdots m_n$

In the system $x \equiv 2\ (mod\ 3);\ x \equiv 3\ (mod\ 5);\ x \equiv 2\ (mod\ 7)$

the moduli 3, 5, and 7 are pairwise relatively prime.

Therefore, there is a unique solution modulo 105.

Arithmetic with Large Integers

Suppose our computer performs fast on numbers less than 100 but is slow on larger numbers.

We need to add 123,684 and 413,456. What should we do?

Pick a set of pairwise relatively prime moduli: e.g. 99, 98, 97, 95
Represent each number less than 89,403,930 uniquely as a 4-tuple of residues of the chosen moduli.

$$\begin{aligned} 123{,}684 &= (33, 8, 9, 89) \\ 413{,}456 &= (32, 92, 42, 16) \\ 123684 + 413456 &= (33, 8, 9, 89) + (32, 92, 42, 16) \\ &= (rem(33+32{,}99), rem(8+92{,}98), rem(9+42{,}97), rem(89+16{,}95)) \\ &= (65{,}2{,}51{,}10) \end{aligned}$$

Only need to convert large integers into tuples and back to recover the result. All intermediate calculations involve small numbers.

On a 32-bit computer choose moduli $2^{31}-1, 2^{30}-1, 2^{29}-1, 2^{25}-1, 2^{23}-1$ to uniquely represent numbers up to 2^{135}.

Fermat’s Last Theorem

There are no non-zero integer solutions to $a^n + b^n = c^n$ for $n \geq 3$.

Conjectured in 1637.

Fermat proved it for $n = 4$.

By 1839 was proved for $n = 3,5,7$

Stimulated the development of new branches of number theory.

Listed in the Guinness Book of World Records as “the most difficult mathematical problem”

Following advances in seemingly unrelated areas, finally proved by Andrew Wiles in 1995.

Fermat’s Enigma, by Simon Singh