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

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

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

Arithmetic with Large Integers

We want to perform a series of calculations on numbers that are too big for hardware to handle.

STRATEGY:

1. Break up each large number into smaller pieces.
2. Perform the calculations on the smaller pieces.
3. Combine the small results to obtain the final large result.

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}.

The Chinese Remainder Theorem

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

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

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.

Proof of Chinese Remainder Theorem

Consider the system

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

Observe that if x_1 is a solution to the first congruence, so is $x_1 + m_1$.

We can do this with any multiple of m_1: $x_1 + km_1 \equiv x_1 \equiv a_1 (mod\ m_1)$.

If we have an x that solves every congruence, we can add a multiple of m_1 and still solve the first congruence, a multiple of m_2 to still solve the second, etc.

The smallest number that we can add to x that preserves every congruence is then $lcm(m_1, m_2, \dots, m_n)$

Since the m_i's are pairwise relatively prime, $lcm(m_1, m_2, \dots, m_n) = m_1 m_2 \cdots m_n \coloneqq m$

Therefore, every solution to the system is congruent modulo m.

Proof of Chinese Remainder Theorem

Consider the system

$$x \equiv a_1 (mod\ m_1)$$
$$x \equiv a_2 (mod\ m_2)$$
$$\vdots$$
$$x \equiv a_n (mod\ m_n)$$

Goal: prove that the system has a solution by constructing one, starting with the assumption that the moduli are pairwise relatively prime.

Idea: what if we can solve each congruence individually, then add solutions together?

$$\forall 1 \leq i \leq n\colon\ X_i \equiv a_i\ (mod\ m_i)$$
$$x \equiv X_1 + X_2 + \cdots + X_n\ (mod\ m)$$

Proof of Chinese Remainder Theorem

$$\forall 1 \leq i \leq n\colon X_i \equiv a_i \ (mod\ m_i)$$
$$x \equiv X_1 + X_2 + \cdots + X_n \ (mod\ m)$$

Problem: the X_i's might interfere with each other.

To stop this, we require that $\forall i\ \forall j \neq i\colon X_i \equiv 0 \ (mod\ m_j)$.

How do we construct X_i's that satisfy these conditions?

Observe that $\forall i\ \forall j \neq i\colon M_i \coloneqq \frac{m}{m_i} \equiv 0 \ (mod\ m_j)$, but $M_i \not\equiv 0 \ (mod\ m_i)$.

Can we use these M_i's to find each X_i?

Proof of the Chinese Remainder Theorem

$$M_i = \frac{m}{m_i}$$

$$X_i \equiv a_i \ (mod\ m_i), \qquad X_i \equiv 0 \ \left(mod\ m_j\right), i \neq j$$

Notice that $\gcd(M_i, m_i) = \gcd(m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_n, m_i) = 1.$

Therefore, each M_i has an inverse $y_i = M_i^{-1}$ modulo m_i.

Then, $\forall i: y_i M_i \equiv 1 \ (mod\ m_i)$, and (by the last slide) $\forall i \ \forall j \neq i: y_i M_i \equiv 0 \ (mod\ m_j)$.

Now we can make our X_i's!

$$X_i = a_i y_i M_i \equiv a_i \ (mod\ m_i)$$

$$\forall j \neq i: X_i = a_i y_i M_i \equiv 0 \ (mod\ m_j)$$

Proof of the Chinese Remainder Theorem

Now we can put it all together:

$$x \equiv a_1 (mod\ m_1)$$
$$x \equiv a_2 (mod\ m_2)$$
$$\vdots$$
$$x \equiv a_n (mod\ m_n)$$

Where the moduli are pairwise relatively prime.

Construct $m = m_1 m_2 \cdots m_n,\ M_i = \frac{m}{m_i},\ \ y_i \equiv M_i^{-1} (mod\ m_i),\ X_i = a_i y_i M_i$.

Then,

$$x \equiv a_1 y_1 M_1 + a_2 y_2 M_2 + \cdots a_n y_n M_n\ (mod\ m)$$

We still need to prove that this solution is unique modulo m.

Using CRT

$$x \equiv 2 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 5)$$
$$x \equiv 2 \ (mod\ 7)$$

Step 1: Calculate $m = 3 \times 5 \times 7 = 105$

Step 2. Calculate $M_1 = 35,\ M_2 = 21,\ M_3 = 15$

Step 3. Calculate $y_1 \equiv M_1^{-1} \equiv 2 \ (mod\ 3)$ (using the pulverizer)

$y_2 \equiv M_2^{-1} \equiv 1 \ (mod\ 5)$

$y_3 \equiv M_3^{-1} \equiv 1 \ (mod\ 7)$

Step 4. Calculate $X = 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15$

$= 140 + 63 + 30 = 233 \equiv 23 \ (mod\ 105)$

Step 5. Double check the result. Does 23 satisfy the system of congruences?

CRT Proof of Uniqueness

Lemma: Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime, and $m = m_1 m_2 \cdots m_n$

Then, $(\forall i \leq n\colon\ m_i \mid A\ ) \ \Rightarrow\ m \mid A$.

Proof: next problem set!

Proof of Uniqueness of CRT: Let X, Y be two solutions to the system of congruences.

Since $\forall i\colon\ X \equiv a_i \equiv Y\ (mod\ m_i)$, it follows that $\forall i\colon m_i \mid X - Y$.

From the lemma it follows that $m \mid X - Y$, implying that $X \equiv Y\ (mod\ m)$.

Computing with Large Integers

Modular Arithmetic

- Convert large integer into a k-tuple of remainders modulo k pairwise relative primes
- Perform modular arithmetic operations on each element in the k-tuple separately
- Convert the resulting k-tuple into a large integer to obtain the final result
    - Chinese Remainder Theorem