Chinese Remainder Theorem

Yan Huang

$n = \{2, 5, 8, 11, 14, 17, 20, 23, 26, \dots\}$

mod 7

2 5 1 4 0 3 6 2 5

$\mathbb{Z}_7^*$

$3^{-1} \cdot 3 = 1 \bmod 7$

- There is a pile of n apples. If divide the pile into groups of 3, there are 2 apples left. If divided into groups of 7, there 4 apples left. What is the minimal value of n?

$k \in \mathbb{Z}$

$$\begin{cases} n = 2 \bmod 3 \\ n = 4 \bmod 7 \end{cases} \Rightarrow n = 3k + 2.$$

Substitute n with $3k+2$ in the 2nd equation:

$3k + 2 = 4 \bmod 7$

$\boxed{3k = 2 \bmod 7}$

least positive

$n = 11$

Hard to solve manually $\longrightarrow$ 177

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ b/c $3 \times 5 = 1 \bmod 7$

$5 = 3^{-1}$

so $3^{-1} = 5 \bmod 7$

$(x, y, d) \leftarrow EGCD(a, b)$ $\Rightarrow$ you can find $a^{-1} = ? \bmod b$.

such that $ax + by = d$ so $a^{-1} = x \bmod b$.

Assuming $\gcd(a, b) = 1$, then $ax + by = 1$ $\Rightarrow ax + by = 1 \bmod b$

$\Rightarrow ax = 1 \bmod b$

To find $3^{-1} \bmod 7$, we call

$(5, -2, 1) \leftarrow \text{EGCD } 3 \quad 7$

So, $3^{-1} \equiv 5 \bmod 7$

$3k \equiv 2 \bmod 7$.

$5 \cdot 3k \equiv 5 \times 2 \bmod 7$

$k \equiv 3 \bmod 7$

$n = 3k + 2 = 3 \times 3 + 2 = 11$

$4^{-1} \bmod 5$. $\quad EGCD(4,5) \to (4,-3,1)$

- There is a pile of n apples. If divide the pile into groups of 4, there are 2 apples left. If divided into groups of 5, there 1 apples left. What is the minimal value of n?

$$\begin{cases} n = 2 \bmod 4 \\ n = 1 \bmod 5 \end{cases}$$

let $n = 4k+2$, then $4k+2 = 1 \bmod 5 \iff 4k = -1 \bmod 5$

$= 4 \bmod 5$

$\iff k = 1 \bmod 5 \iff n = 4 \times 1 + 2 = 6$

Chinese Remainder Theorem

gcd $(n_1, n_2) = 1$

Assume n_1 and n_2 are coprime. Let x be the solution to the following systems of modulo identities

$$x = a_1 \mod n_1$$

$$x = a_2 \mod n_2.$$

Then $x = (X_2 n_2 a_1 + X_1 n_1 a_2) \mod N$, where $N = n_1 \times n_2$ and $X_1 n_1 + X_2 n_2 = 1$.

proof:

Since $x = a_1 \bmod n_1$, Let $x = a_1 + n_1 K$ for some K.

we hope to decide K such that $x = a_2 \bmod n_2$.

that is $a_1 + n_1 K = a_2 \bmod n_2$

that is $n_1 K = (a_2 - a_1) \bmod n_2$ .... (1)

because $\gcd(n_1, n_2) = 1$. we can call extended Euclidean algorithm egcd n_1 n_2 to learn X_1, X_2 s.t.

$$X_1 n_1 + X_2 n_2 = 1. \Rightarrow X_1 n_1 = (1 - X_2 n_2) = 1 \bmod n_2.$$

multiply X_1 on both sides of (1), we get

$$\underline{X_1 n_1 K} = X_1 (a_2 - a_1) \bmod n_2$$

$X_1 n_1 K \bmod n_2 = 1 \cdot K \bmod n_2.$

$\therefore$ $K = X_1 (a_2 - a_1) \bmod n_2.$

Let $K = X_1 (a_2 - a_1) + n_2 \cdot m$ for some integer m.

then $x = a_1 + n_1 K = a_1 + n_1 (X_1 (a_2 - a_1) + n_2 m) = a_1 + X_1 n_1 a_2 - X_1 n_1 a_1 + n_1 n_2 \cdot m$

$= X_1 n_1 a_2 + a_1 (1 - X_1 n_1) + n_1 n_2 m = X_1 n_1 a_2 + X_2 n_2 a_1 \pmod{n_1 n_2}$

More Generally

p, q are primes.

- Chinese Remainder Theorem establishes a *bijection* between $\mathbb{Z}_p \times \mathbb{Z}_q$ and $\mathbb{Z}_{pq}$.

$p = 3, \ q = 5.$

$Z_{15}^{+} = \{0, 1, 2, \ldots, 14\}$

$Z_3^{+} = \{0, 1, 2\}$

$Z_5^{+} = \{0, 1, 2, 3, 4\}.$

$Z_3^{+} \times Z_5^{+} = \{(0,0), (0,1), (0,2), (0,3), (0,4), (1,0), \ldots, (1,4), (2,0), (2,1), (2,2), \ldots (2,4)\}$

Example

$(i,j) \in \mathbb{Z}_3^+ \times \mathbb{Z}_5^+$ $\qquad\qquad$ $x \leftarrow \mathbb{Z}_{15}^+$

$(\overset{i}{x \bmod 3}, \overset{j}{x \bmod 5}) \longleftarrow x$

$(i, j) \longrightarrow x$

solving $\begin{cases} x \equiv i \bmod 3 \\ x \equiv j \bmod 5 \end{cases}$ for x.

Isomorphism

Let $\mathbb{G}, \mathbb{H}$ be groups with respect to the operations $\star_{\mathbb{G}}$ and $\star_{\mathbb{H}}$. A function $f: \mathbb{G} \to \mathbb{H}$ is an isomorphism if

1. f is a bijection, and f^{-1} exists.
2. For all $g_1, g_2 \in \mathbb{G}$, $f(g_1 \star_{\mathbb{G}} g_2) = f(g_1) \star_{\mathbb{H}} f(g_2)$.

If there exists an isomorphism between $\mathbb{G}$ and $\mathbb{H}$, we say $\mathbb{G}$ and $\mathbb{H}$ are *isomorphic* and write $\mathbb{G} \simeq \mathbb{H}$.

- $\mathbb{Z}_{pq}$ is a group with respect to either addition ~~or multiplication.~~
- $\mathbb{Z}_p \times \mathbb{Z}_q$ is also a group (with respect to entry-wise modulo either addition ~~or multiplication~~).
- $\mathbb{Z}_{pq} \simeq \mathbb{Z}_p \times \mathbb{Z}_q$.
  - modulo addition is an isomorphism between $\mathbb{Z}_{pq}$ and $\mathbb{Z}_p \times \mathbb{Z}_q$
  - modulo multiplication is also an isomorphism between $\mathbb{Z}_{pq}$ and $\mathbb{Z}_p \times \mathbb{Z}_q$

Modulo Addition is an Isomorphism between $\mathbb{Z}_{pq}$ and $\mathbb{Z}_p \times \mathbb{Z}_q$

$4 \in \mathbb{Z}_{15}$.

$4 \longrightarrow (4 \bmod 3,\ 4 \bmod 5) \in \mathbb{Z}_3 \times \mathbb{Z}_5$

$4 \xleftarrow{\text{CRT}} = (1,\ 4)$

$8 \longrightarrow (2,\ 3) \in \mathbb{Z}_3 \times \mathbb{Z}_5$

$8 \xleftarrow{\text{CRT}} (2,\ 3)$

$4+8 \bmod 15$

$= 12 \bmod 15$.

$(1,4)+(2,3)$

$= ((1+2) \bmod 3,\ (4+3) \bmod 5) = (0,2)$

$12 \longrightarrow (0,\ 2)$

Modulo Multiplication is an Isomorphism between $\mathbb{Z}_{pq}$ and $\mathbb{Z}_p \times \mathbb{Z}_q$

$\mathbb{Z}_{15}^*$ fast $\mathbb{Z}_3^* \times \mathbb{Z}_5^*$

$4 \qquad (1, 4)$

slow computation

$8 \qquad (2, 3)$

$4 \times 8 \bmod 15 = 32 \bmod 15$

$= 2$

$(1, 4) \times (2, 3)$

$= ((1 \times 2) \bmod 3, (4 \times 3) \bmod 5)$

$= (2, 2)$

2 fast

computes faster.

Using CRT to Simplify Modulo Computations

- Calculate

$35 = 5 \times 7$

$2838 \bmod 7 = (2800 + 38) \bmod 7$
$= 38 \bmod 7 = 3$

2838 mod 35

$\xrightarrow{f(2838)} (2838 \bmod 5,\ 2838 \bmod 7)$

$= (3 \bmod 5,\ 3 \bmod 7)$

$\xrightarrow{CRT} 3$

so we know $\underline{2838 \bmod 35 = 3}$.

solving
$$\begin{cases} x = 3 \bmod 5 \\ x = 3 \bmod 7 \end{cases}$$

Using CRT to Simplify Modulo Computations

- Calculate

2838*12345 mod 35