Mathematics for Computer Science – CRT

Libin Wang

School of Computer Science, South China Normal University

April 25, 2025

导引.

Chinese Remainder Theorem（中国剩余定理），或称为*中国余数定理*则更准确。

历史.

中国剩余定理有着满满的中国传统文化元素，与之相关的名人包括：春秋时期的孙子、秦汉时期的韩信、宋朝的沈括和秦久韶等。南北朝时期（公元 5 世纪）的数学著作《孙子算经》卷下第二十六题所谓“物不知数”问题则为国人所熟知：有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何?

Motivation.

中国剩余定理讨论一元同余方程组的高效解法。

Example

Example 1. Suppose we wish to solve:

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

Motivation.

中国剩余定理讨论一元同余方程组的高效解法。

Example

Example 1. Suppose we wish to solve:

$$x \equiv 2 \pmod 5$$

$$x \equiv 3 \pmod 7$$

Solution.

1. We have $x = 5t + 2$ from the first congruence, for $t \in \mathbb{N}$;

Motivation.

中国剩余定理讨论一元同余方程组的高效解法。

Example

Example 1. Suppose we wish to solve:

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

Solution.

1. We have $x = 5t + 2$ from the first congruence, for $t \in \mathbb{N}$;
2. Substitute for x in the second congruence, $5t + 2 \equiv 3 \pmod 7$;

Motivation.

中国剩余定理讨论一元同余方程组的高效解法。

Example

Example 1. Suppose we wish to solve:

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

Solution.

1. We have $x = 5t + 2$ from the first congruence, for $t \in \mathbb{N}$;
2. Substitute for x in the second congruence, $5t + 2 \equiv 3 \pmod 7$;
3. Simplifies, get $5t \equiv 1 \pmod 7$;

Motivation.

中国剩余定理讨论一元同余方程组的高效解法。

Example

Example 1. Suppose we wish to solve:

$$x \equiv 2 \pmod 5$$

$$x \equiv 3 \pmod 7$$

Solution.

1. We have $x = 5t + 2$ from the first congruence, for $t \in \mathbb{N}$;
2. Substitute for x in the second congruence, $5t + 2 \equiv 3 \pmod 7$;
3. Simplifies, get $5t \equiv 1 \pmod 7$;
4. Multiplies both sides with 5^{-1} to get $t = 7s + 3$ for $s \in \mathbb{N}$;

Motivation.

中国剩余定理讨论一元同余方程组的高效解法。

Example

Example 1. Suppose we wish to solve:

$$x \equiv 2 \pmod 5$$

$$x \equiv 3 \pmod 7$$

Solution.

1. We have $x = 5t + 2$ from the first congruence, for $t \in \mathbb{N}$;
2. Substitute for x in the second congruence, $5t + 2 \equiv 3 \pmod 7$;
3. Simplifies, get $5t \equiv 1 \pmod 7$;
4. Multiplies both sides with 5^{-1} to get $t = 7s + 3$ for $s \in \mathbb{N}$;
5. Finally, $x = 35s + 17$, means $x \equiv 17 \pmod{35}$.

The Chinese Remainder Theorem–CRT.

For any system of equations like this, the *Chinese Remainder Theorem*, short for CRT, tells us there is always a unique solution up to a certain modulus, and describes how to find the solution efficiently.

Theorem

Let p, q be primes, $n = pq$. For each $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_q$, there is unique x, $0 \leq x < n$ such that $x \equiv a \pmod{p}$ and $x \equiv b \pmod{q}$.

The Chinese Remainder Theorem–CRT.

Theorem

Let p, q be coprime positive integers, $n = pq$. For each $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_q$, there is a unique x, $0 \leq x < n$ such that $x \equiv a \pmod{p}$ and $x \equiv b \pmod{q}$.

Proof Idea

1. Given a and p, how can we find some 1_p s.t. $a * 1_p \equiv a \pmod{p}$?

The Chinese Remainder Theorem–CRT.

Theorem

Let p, q be coprime positive integers, $n = pq$. For each $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_q$, there is a unique x, $0 \leq x < n$ such that $x \equiv a \pmod{p}$ and $x \equiv b \pmod{q}$.

Proof Idea

1. Given a and p, how can we find some 1_p s.t. $a * 1_p \equiv a \pmod{p}$?
2. 1_p must be a 1 under modulo p

The Chinese Remainder Theorem–CRT.

Theorem

Let p, q be coprime positive integers, $n = pq$. For each $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_q$, there is a unique x, $0 \leq x < n$ such that $x \equiv a \pmod{p}$ and $x \equiv b \pmod{q}$.

Proof Idea

1. Given a and p, how can we find some 1_p s.t. $a * 1_p \equiv a \pmod{p}$?
2. 1_p must be a 1 under modulo p
3. Recall something from our previous courses, we have many options.

The Chinese Remainder Theorem–CRT.

Theorem

Let p, q be coprime positive integers, $n = pq$. For each $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_q$, there is a unique x, $0 \leq x < n$ such that $x \equiv a \ (mod\ p)$ and $x \equiv b \ (mod\ q)$.

Proof Idea

1. Given a and p, how can we find some 1_p s.t. $a * 1_p \equiv a \pmod{p}$?
2. 1_p must be a 1 under modulo p
3. Recall something from our previous courses, we have many options.
4. We try this: find some c s.t. $1_p \equiv cc^{-1} \equiv 1 \pmod{p}$

The Chinese Remainder Theorem–CRT.

Theorem

Let p, q be coprime positive integers, $n = pq$. For each $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_q$, there is a unique x, $0 \leq x < n$ such that $x \equiv a \ (mod\ p)$ and $x \equiv b \ (mod\ q)$.

Proof Idea

1. Given a and p, how can we find some 1_p s.t. $a * 1_p \equiv a \pmod{p}$?
2. 1_p must be a 1 under modulo p
3. Recall something from our previous courses, we have many options.
4. We try this: find some c s.t. $1_p \equiv cc^{-1} \equiv 1 \pmod{p}$
5. Similarly, for the q-part, we find $1_q \equiv dd^{-1} \equiv 1 \pmod{q}$

The Chinese Remainder Theorem–CRT.

Theorem

Let p, q be coprime positive integers, $n = pq$. For each $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_q$, there is a unique x, $0 \leq x < n$ such that $x \equiv a \, (mod\ p)$ and $x \equiv b \, (mod\ q)$.

Proof Idea

1. Given a and p, how can we find some 1_p s.t. $a * 1_p \equiv a \pmod{p}$?
2. 1_p must be a 1 under modulo p
3. Recall something from our previous courses, we have many options.
4. We try this: find some c s.t. $1_p \equiv cc^{-1} \equiv 1 \pmod{p}$
5. Similarly, for the q-part, we find $1_q \equiv dd^{-1} \equiv 1 \pmod{q}$
6. And then x must be something like that $x = (a * 1_p + b * 1_q) = (acc^{-1} + bdd^{-1})$, what should be c and d?

The Chinese Remainder Theorem–CRT.

Theorem

Let p, q be coprime positive integers, $n = pq$. For each $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_q$, there is a unique x, $0 \leq x < n$ such that $x \equiv a \pmod{p}$ and $x \equiv b \pmod{q}$.

Proof.

By construction. Since p, q are coprime, these must exist p_1 and q_1 such that $p_1 \equiv p^{-1} \pmod{q}$ and $q_1 \equiv q^{-1} \pmod{p}$. Let integer x be:

$$y = aqq_1 + bpp_1$$

It is easy to check that y satisfies both equations. It remains to show no other solutions exist modulo n. Suppose $\exists z \neq y$ is another solution. Then $(z - y) = tp$ and $(z - y) = sq$, for some $t, s \in \mathbb{N}$. Since p and q are coprime, then $(z - y) = kpq$, for $k \in \mathbb{N}$. Hence $z \equiv y \pmod{n}$. □

Example.

Example

Example 2. Suppose we wish to solve:

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

Solution.

1. Let $a = 2$, $b = 3$, $p = 5$, $q = 7$, $n = pq = 35$;
2. Compute $p_1 \equiv p^{-1} (\text{mod } q)$ and $q_1 \equiv q^{-1} (\text{mod } p)$ using EGCD algorithm; $p_1 = 3$, $q_1 = 3$;
3. $y \equiv aqq_1 + bpp_1 \pmod{n}$; $y = 17$;
4. It is easy to check that y is a correct solution.

Exercise.

求解以下方程.

Suppose we wish to solve:

$$x \equiv 3 \pmod{11}$$

$$x \equiv 4 \pmod{13}$$

Exercise.

求解以下方程.

Suppose we wish to solve:

$$x \equiv 3 \pmod{11}$$

$$x \equiv 4 \pmod{13}$$

Ans.

...

The Chinese Remainder Theorem–CRT–另一种证明.

Proof.

By construction. Since p, q are coprime, these must exist p_1 and q_1 such that $pp_1 + qq_1 = 1$, by Bezout Theorem. Then we have:

$$\begin{aligned} pp_1 &\equiv 1 \pmod{q} \\ qq_1 &\equiv 1 \pmod{p} \end{aligned}$$

Let $t = aqq_1 + bpp_1$, we can check that, t is indeed a solution of the equations. $\square$

The Chinese Remainder Theorem–CRT–两种证明的对比.

Remark.

第一种证明有点啰嗦，但是它告诉你，如何去发现证明。第二种证明简洁，直观非常棒，但是你不容易想到。或者，你不知道如何去发现这种证明。后者看上去很容易，但是，如果你意识到，这种证明竟然不出现在大多数的数论教材，你就明白，它是一种颇为独到的见解。然而它也有缺点，从它出发难以找到“通解”，也就是说它不具备第一种证明的那种“思想”。

Generization.

For Several Equations, we have a generized version of CRT.

Theorem

Let $m_1, m_2, \cdots, m_n$ be a set of pairwise relatively prime integers. Then the system of n equations:

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

has a unique solution for x modulo M where $M = m_1 m_2 \cdots m_n$.

Generization.

Proof.

By construction. Let $M = \prod_{i=1}^{n} m_i$, $b_i = M/m_i$, $b_i' = b_i^{-1} \pmod{m_i}$. Then

$$y = \sum_{i=1}^{n} a_i b_i b_i' \pmod{M}$$

is the unique solution. □

A perspective from Abstract Algebra.

Motivation.

Let $n = pq$, $p, q > 1$ are relatively prime. Given a positive integer x, it can be expressed as a unique pair $([x \bmod p], [x \bmod q])$.

A perspective from Abstract Algebra.

Theorem

Let $p, q > 1$ be coprime, $n = pq$. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q \quad \text{and} \quad \mathbb{Z}_n^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*.$$

Proof.

1. Define ϕ as a function mapping from $\mathbb{Z}_n$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ as:

$$\phi(x) \triangleq ([x \bmod p], [x \bmod q])$$

2. Show ϕ is bijective.
3. Check that $\phi(x)$ preserves the group operation.

A perspective from Abstract Algebra.

Theorem

Let $p, q > 1$ be coprime, $n = pq$. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q \quad \textit{and} \quad \mathbb{Z}_n^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*.$$

Proof.

1. Define ϕ as a function mapping from $\mathbb{Z}_n$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ as:

$$\phi(x) \triangleq ([x \bmod p], [x \bmod q])$$

2. Show ϕ is bijective.
3. Check that $\phi(x)$ preserves the group operation.

The proof that it is an isomorphism from $\mathbb{Z}_n^*$ to $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ is similar. $\square$

Remark.

Remark

首先，注意到 $\mathbb{Z}_p \times \mathbb{Z}_q$ 是加法群，请验证！

How to prove the bijection?

Proof.

证明映射 ϕ 是一种双射，即证明 ϕ 是满射且单射。满射显然，因为根据中国剩余定理，任意序对中的两个同余式在模 n 下存在唯一解。证明单射即证明，如果对任意正整数 $a, b < n$，有 $([a \bmod p], [a \bmod q]) = ([b \bmod p], [b \bmod q])$，则 $a = b$。再次根据中国剩余定理可得。 $\square$

How to prove the isomorphism?

Proof.

证明映射 ϕ 保持群操作，即需要证明：

$$\begin{aligned} \phi(a+b) &= ([(a+b) \bmod p], [(a+b) \bmod q]) \\ &= ([a \bmod p], [a \bmod q]) + ([b \bmod p], [b \bmod q]) \\ &= \phi(a) + \phi(b) \end{aligned}$$

$\square$

Example.

Example

Example 3. Take $n = 15 = 5 \cdot 3$. $\mathbb{Z}_n^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ is isomorphic to $\mathbb{Z}_5^* \times \mathbb{Z}_3^*$ since we can give following correspondence:

$$1 \leftrightarrow (1,1) \quad 2 \leftrightarrow (2,2) \quad 4 \leftrightarrow (4,1) \quad 7 \leftrightarrow (2,1)$$

$$8 \leftrightarrow (3,2) \quad 11 \leftrightarrow (1,2) \quad 13 \leftrightarrow (3,1) \quad 14 \leftrightarrow (4,2)$$

Example.

Example

Example 4. To compute $14 \cdot 13 \bmod 15$. Since $14 \leftrightarrow (4, 2)$ and $13 \leftrightarrow (3, 1)$, we have:

$$(4, 2) \cdot (3, 1) = ([4 \cdot 3 \bmod 5], [2 \cdot 1 \bmod 3]) = (2, 2).$$

Note that $(2, 2) \leftrightarrow 2$, which is the correct answer.

Example.

Example

Example 5. To compute $11^{53} \bmod 15$. Since $11 \leftrightarrow (1,2)$ and $2 \equiv -1 \bmod 3$ we have:

$$(1,2)^{53} = ([1^{53} \bmod 5], [-1^{53} \bmod 3]) = (1, -1 \bmod 3) = (1,2).$$

Thus, $11^{53} \bmod 15 = 11$

Example.

Example

Example 6. 设 $n = pq$ 为合数，p 和 q 是两个不同的素数。以下等式在模 n 的意义上有多少个解?

$$x^2 \equiv 1 \pmod{n}$$

为此，需要解以下两个同余方程

$$x^2 \equiv 1 \pmod{p}$$
$$x^2 \equiv 1 \pmod{q}$$

以上两式分别有两个不同的解。因此在模 n 的意义上总共有 4 个解。同时，这也就解决了上一章的一个遗留问题。

Example.

Example

Example 7. To compute $12^{12} \bmod 143$

Example.

Example

Example 7. To compute $12^{12} \bmod 143$ 解:

- 记 $n = 143$，$n = p * q = 13 * 11$；
- 求：$12^{12} \bmod 13$ 和 $12^{12} \bmod 11$；
- 所以，$12^{12} \bmod 143 = 1$.

Little thought.

Remark

A practical application: if we have many computations to perform on $x \in \mathbb{Z}_n^*$ *(e.g. RSA signing and decryption), we can convert* x *to* $(a, b) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ *and do all the computations on* a *and* b *instead before converting back.*
This is often cheaper because for many algorithms, doubling the size of the input more than doubles the running time.

Homeworks Exercises.

Homeworks.

1. Using CRT to solve:

$$x \equiv 8 \pmod{11}$$

$$x \equiv 3 \pmod{19}$$

2. Using CRT to solve the system of congruence:

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 2 \pmod{7} \\ x &\equiv 3 \pmod{9} \\ x &\equiv 4 \pmod{11} \end{aligned}$$

3. Write a program(C or Python) to solve CRT.

Homeworks Exercises.

Homeworks.

4. Complete the proof that it is an isomorphism from $\mathbb{Z}_n^*$ to $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$.
5. Let $p = 5$ and $q = 7$, $n = pq$. Please explicitly give the correspondece between $\mathbb{Z}_n^*$ and $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Hint: Programming is permitted.

Homeworks Exercises.

Homeworks.

6. 请求解 $x^{113} \equiv 15 \pmod{221}$[提示：这是一道似曾相识的习题，然而中国剩余定理能保证你顺利完成目标。]