A Concrete Introduction to Number Theory and Algebra–CRT

Libin Wang

School of Computer Science, South China Normal University

November 17, 2020

Motivation.

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

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

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

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

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

Chinese Remainder Theorem（中国剩余定理），或称为*中国余数定理*则更准确。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, $0 \le x < n$ 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 c s.t. $ac \equiv a \pmod p$?

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, $0 \le x < n$ 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 c s.t. $ac \equiv a \pmod{p}$?
2. c must be some 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 c s.t. $ac \equiv a \pmod{p}$?
2. c must be some 1 under modulo p
3. Recall something from linear algebra, what is similar matrix?

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 c s.t. $ac \equiv a \pmod{p}$?
2. c must be some 1 under modulo p
3. Recall something from linear algebra, what is similar matrix?
4. Find some c s.t. $acc^{-1} \equiv a \pmod{p}$

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 c s.t. $ac \equiv a \pmod{p}$?
2. c must be some 1 under modulo p
3. Recall something from linear algebra, what is similar matrix?
4. Find some c s.t. $acc^{-1} \equiv a \pmod{p}$
5. Then x must be something like that $x = (acc^{-1} + bdd^{-1})$, 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, $0 \le x < n$ 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 $p_1 \equiv p^{-1} (\bmod\ q)$ and $q_1 \equiv q^{-1} (\bmod\ p)$ 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.

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 f as a function mapping from $\mathbb{Z}_n$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ as:

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

2. Show f is bijective.
3. Check that $f(x)$ 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 f as a function mapping from $\mathbb{Z}_n$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ as:

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

2. Show f is bijective.
3. Check that $f(x)$ 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. $\square$

Example.

Example

Example 3. Take $15 = 5 \cdot 3$. $\mathbb{Z}_n^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ 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 4. To compute 11^{53} mod 15. Since $11 \leftrightarrow (1,2)$ and $2 \equiv -1$ mod 3 we have:

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

Thus, 11^{53} mod $15 = 11$

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.