Chinese Remainder Theorem

Debabrota Basu

Department of Computer Science
School of Computing

October 5, 2016

"You probably said or were told at some point that diamonds are forever, right? That depends on your definition of forever! A theorem – that really is forever."
– Eduardo Sánz de Cabezón

History

- Sun Tzu first mentioned this problem in his 3^{rd} century book *Sunzi Suanjing*.
- Aryabhata described an algorithm to solve it in 6^{th} century A.D.
- Fibonacci mentioned a special case of it in *Liber Abaci*, published in 1202.

- Gauss used congruences to give it the modern formulation in his *Disquisitiones Arithmeticae* of 1801.

An Example

> There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?
>
> -Sun Tzu

Chinese Remainder Theorem (I)

Theorem (Remainder Version)

If

i. $\{n_i\}_{i=1}^K$ *are* **pairwise coprime** *integers greater than* 1,

ii. $N = \prod_{i=1}^K n_i$, *and*

iii. $\{a_i\}_{i=1}^K$ *are* K *integers, such that* $a_i \in \{0, 1, \dots, n_i - 1\}$ *for every* i,

then **there exists an unique integer** $x \in \{0, 1, \dots, N-1\}$ *such that the remainder of* x *divided by* n_i *is* a_i *for every* i.

Chinese Remainder Theorem (I)

Theorem (Remainder Version)

If

i. $\{n_i\}_{i=1}^{K}$ *are* **pairwise coprime** *integers greater than* 1,

ii. $N = \prod_{i=1}^{K} n_i$, *and*

iii. $\{a_i\}_{i=1}^{K}$ *are* K *integers, such that* $a_i \in \{0, 1, \dots, n_i - 1\}$ *for every* i,

then **there exists an unique integer** $x \in \{0, 1, \dots, N-1\}$ *such that the remainder of* x *divided by* n_i *is* a_i *for every* i.

– Primitive version

Chinese Remainder Theorem (I)

Theorem (Remainder Version)

If

i. $\{n_i\}_{i=1}^K$ *are* **pairwise coprime** *integers greater than* 1,
ii. $N = \prod_{i=1}^K n_i$, *and*
iii. $\{a_i\}_{i=1}^K$ *are* K *integers, such that* $a_i \in \{0, 1, \dots, n_i - 1\}$ *for every* i,

then **there exists an unique integer** $x \in \{0, 1, \dots, N-1\}$ *such that the remainder of* x *divided by* n_i *is* a_i *for every* i.

– Primitive version

– Two integers a and b are called **pairwise coprime** or *relatively prime*, if $gcd(a, b) = 1$.

Chinese Remainder Theorem (I)

Theorem (Remainder Version)

If

i. $\{n_i\}_{i=1}^{K}$ *are* **pairwise coprime** *integers greater than* 1,

ii. $N = \prod_{i=1}^{K} n_i$, *and*

iii. $\{a_i\}_{i=1}^{K}$ *are* K *integers, such that* $a_i \in \{0, 1, \ldots, n_i - 1\}$ *for every* i,

then **there exists an unique integer** $x \in \{0, 1, \ldots, N - 1\}$ *such that the remainder of* x *divided by* n_i *is* a_i *for every* i.

– Primitive version

– Two integers a and b are called **pairwise coprime** or *relatively prime*, if $gcd(a, b) = 1$.

– n_i's are called *modulis* or *divisors*.

Chinese Remainder Theorem (II)

Theorem (Congruence Modulo Version)

If

i. $\{n_i\}_{i=1}^K$ *are* **pairwise coprime** *integers greater than* 1*,*

ii. $N = \prod_{i=1}^K n_i$*, and*

iii. $\{a_i\}_{i=1}^K$ *are* K *integers,*

then **there exists an unique residue class** $x(modN)$ *such that,*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_K \pmod{n_K}. \end{aligned}$$

Chinese Remainder Theorem (III)

Theorem (Ring Isomorphism Version)

If

- i. $\{n_i\}_{i=1}^{K}$ *are* **pairwise coprime** *integers greater than* 1*, and*
- ii. $N = \prod_{i=1}^{K} n_i$,

then the map $x \bmod N \mapsto (x \bmod n_1, \dots, x \bmod n_K)$ *defines a* **ring isomorphism**,

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_K\mathbb{Z}.$$

Chinese Remainder Theorem (III)

Theorem (Ring Isomorphism Version)

If

i. $\{n_i\}_{i=1}^{K}$ *are* **pairwise coprime** *integers greater than* 1, *and*
ii. $N = \prod_{i=1}^{K} n_i$,

then the map $x \bmod N \mapsto (x \bmod n_1, \ldots, x \bmod n_K)$ *defines a* **ring isomorphism**,

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_K\mathbb{Z}.$$

– $\mathbb{Z}/n_i\mathbb{Z}$ is the quotient ring of $\mathbb{Z}$ generated by the equivalence class $[n_i]$.

Chinese Remainder Theorem (IV)

Theorem (Generalized Version)

If

i. $\{I_i\}_{i=1}^{K}$ *are* **pairwise coprime** *two-sided ideals of a ring* R*, and*

ii. $I = \cap_{i=1}^{K} I_i$,

then the map $x \bmod I \mapsto (x \bmod I_1, \ldots, x \bmod I_K)$ *defines a* **ring isomorphism**,

$$R/I \cong R/I_1 \times \ldots \times R/I_K.$$

Chinese Remainder Theorem (IV)

Theorem (Generalized Version)

If

i. $\{I_i\}_{i=1}^{K}$ *are* **pairwise coprime** *two-sided ideals of a ring* R*, and*

ii. $I = \cap_{i=1}^{K} I_i$,

then the map $x \bmod I \mapsto (x \bmod I_1, \dots, x \bmod I_K)$ *defines a* **ring isomorphism**,

$$R/I \cong R/I_1 \times \ldots \times R/I_K.$$

– $x \bmod I$ denotes the image of the element x in the quotient ring R/I defined by the ideal I.

Linear Diophantine's Equation

Problem

Given $a, b, c \in \mathbb{Z}$*,*

$$ax + by = c,$$

find integers x *and* y *satisfying this equation.*

Linear Diophantine's Equation

Problem

Given $a, b, c \in \mathbb{Z}$*,*

$$ax + by = c,$$

find integers x *and* y *satisfying this equation.*

- Solution methods–
  - Geometric approach
  - Modular or algebraic approach
  - General solution : not possible to obtain (Hilbert's 10^{th} problem)

Geometric approach

Step 1: Find out the equation of curve

$$x = -\frac{b}{a}y + \frac{c}{a}.$$

The solutions to the Diophantine equation correspond to *lattice points* that lie on the curve.

Geometric approach

Step 1: Find out the equation of curve

$$x = -\frac{b}{a}y + \frac{c}{a}.$$

The solutions to the Diophantine equation correspond to *lattice points* that lie on the curve.

Step 2: Find out the minimal element
Plug in $y = 0$.The basic solution is $(\frac{c}{a}, 0)$.

Geometric approach

Step 1: Find out the equation of curve

$$x = -\frac{b}{a}y + \frac{c}{a}.$$

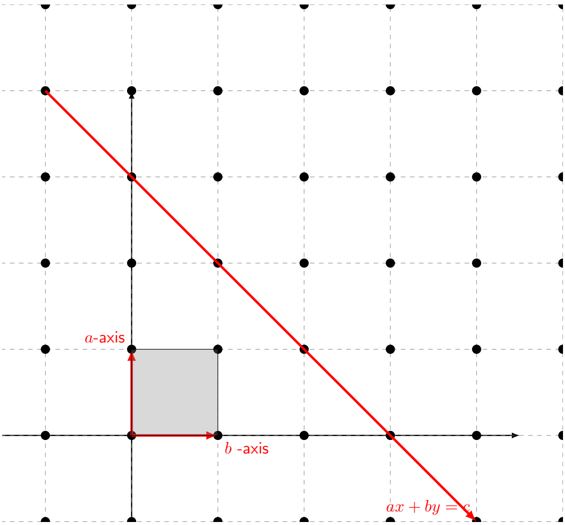
The solutions to the Diophantine equation correspond to *lattice points* that lie on the curve.

Step 2: Find out the minimal element
Plug in $y = 0$.The basic solution is $(\frac{c}{a}, 0)$.

Step 3: The general solution is

$$x = -bt + \frac{c}{a}$$
$$y = at$$

for $t \in \mathbb{Z}$.



a-axis
b -axis
$ax + by = c$

Modular or Algebraic approach

$$\begin{aligned} & ax + by = c \\ \Rightarrow \quad & ax = -by + c \\ \Rightarrow \quad & ax \equiv c \pmod b \\ \Rightarrow \quad & x \equiv ca^{-1} \pmod b \end{aligned}$$

Modular or Algebraic approach

$$\begin{aligned} & ax + by = c \\ \Rightarrow \quad & ax = -by + c \\ \Rightarrow \quad & ax \equiv c (\bmod b) \\ \Rightarrow \quad & x \equiv ca^{-1} (\bmod b) \end{aligned}$$

– Thus, the problem reduces to finding out the equivalence class $\left[ca^{-1}\right]$ for $\bmod b$.

– This is canonical to finding the isomorphism $\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ and to evaluate it for ca^{-1}.

System of Linear Diophantine's Equations

Problem

Given integers $\{n_i\}_{i=1}^K$ *and* $\{a_i\}_{i=1}^K$,

$$\begin{aligned} x &= a_1 + x_1 n_1, \\ &\vdots \\ x &= a_K + x_K n_K, \end{aligned}$$

find integers x *and* $\{x_i\}_{i=1}^K$ *satisfying this equation.*

System of Linear Diophantine's Equations

Problem

Given integers $\{n_i\}_{i=1}^K$ *and* $\{a_i\}_{i=1}^K$,

$$\begin{aligned} x &= a_1 + x_1 n_1, \\ &\vdots \\ x &= a_K + x_K n_K, \end{aligned}$$

find integers x *and* $\{x_i\}_{i=1}^K$ *satisfying this equation.*

– Does there exist a solution?

– If it exists, how is it?

– Is it unique?

System of Linear Congruences

We can reformulate this problem as,

Problem

Given integers $\{n_i\}_{i=1}^{K}$ *and* $\{a_i\}_{i=1}^{K}$,

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ &\vdots \\ x &\equiv a_K \pmod{n_K}, \end{aligned}$$

find integer x *satisfying this equation.*

System of Linear Congruences

We can reformulate this problem as,

Problem

Given integers $\{n_i\}_{i=1}^K$ *and* $\{a_i\}_{i=1}^K$,

$$\begin{aligned} x &\equiv a_1 (\bmod n_1), \\ &\vdots \\ x &\equiv a_K (\bmod n_K), \end{aligned}$$

find integer x *satisfying this equation.*

- Claims of Chinese remainder theorem:
  - There exists a solution if n_i's are pairwise coprime.
  - The solution will have unique $\bmod N$.

Uniqueness Proof

Let x and y be two solutions of this system of equations.

$$\Rightarrow \quad x \equiv a_i (\bmod\, n_i) \wedge y \equiv a_i (\bmod\, n_i) \quad \forall i$$

$$\Rightarrow \quad x \equiv y (\bmod\, n_i) \quad \forall i$$

$$\Rightarrow \quad n_i \mid x - y \quad \forall i$$

$$\Rightarrow \quad N \mid x - y \quad \text{(since } n_i\text{'s are coprime)}$$

$\therefore$ The solution is unique in $\bmod N$. Q.E.D.

– Thus, the map $x \bmod N \mapsto (x \bmod n_1, \ldots, x \bmod n_K)$ is injective.

Existence Proof: Ring Isomorphism

$x \bmod N \mapsto (x \bmod n_1, \ldots, x \bmod n_K)$
maps congruence classes $\bmod N$ to K set of congruence classes $\bmod n_i$.

- The proof of uniqueness shows that this map is *injective*.
- As the domain and the codomain of this map have the same number of elements, N, the map is also *surjective*.
- Thus, the map induces an isomorphism $\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_K\mathbb{Z}$.

– This proves the existence of the solution.

Existence Proof: Computational (I)

–Shall be described in lecture

Existence Proof: Computational (II)

– Shall be described in lecture

Applications: Cryptography

i. RSA decryption
Most state-of-art implementations of RSA use the Chinese remainder theorem to optimize and speed-up decryption and signing.

ii. Secret sharing
Each of the shares of secrets is represented using a congruence, and the solution of the system of congruences using the Chinese remainder theorem is the secret to be recovered.

Applications: Fast computation

i. Fast Fourier Transform
The prime-factor FFT algorithm or Good-Thomas algorithm reduces the computation of a fast Fourier transform of size $n_1 n_2$ to the computation of two fast Fourier transforms of smaller sizes n_1 and n_2 which are coprime.

ii. Parallel computation
If we have an expensive computational task that involves adding, multiplying and subtracting integers on a finite set S. Then, we can choose primes $p_1, p2, \dots, p_r$ which do not divide any element of S and split the computation over r processors. Afterwards CRT is used to put the answers back together.

Applications: Mathematics

i. Lagrangian interpolation
Given a set of $k+1$ data points $(x_0, y_0), \ldots, (x_k, y_k)$ where no two x_j's are the same, the Lagrangian interpolation tries to fit a polynomial of degree k.

ii. Hermite interpolation
Given a set of $k+1$ data points $(x_0, y_0), \ldots, (x_k, y_k)$, the Hermite polynomial tries to find out a polynomial of the least possible degree, such that the polynomial and its first derivatives take given values at the given data points.

iii. Gödel's (First) incompleteness theorem
Proof of the theorem depends on choosing a way to encode formulas and proofs as numbers. The Chinese remainder theorem has been used to construct such a Gdel numbering for sequences.

“The elegance of a mathematical theorem is directly proportional to the number of independent ideas one can see in the theorem and inversely proportional to the effort it takes to see them.”

– George Pólya

Useful Links

- Wikipedia: Chinese remainder theorem
- `http://www.cut-the-knot.org/blue/chinese.shtml`
- Jane Liu's page on CRT
- Stanford's crypto group page
- `https://drexel28.wordpress.com/2011/09/06/the-chinese-remainder-theorem/`
- `http://math.stackexchange.com/questions/1102037/the-chinese-remainder-theorem-for-rings`

References

Ding, C., Pei, D., and Salomaa, A. (1996).
Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography.
World Scientific Publishing Co., Inc., River Edge, NJ, USA.

Gauss, C. F. (1986).
Disquisitiones arithmeticae, 1801. english translation by arthur a. clarke.

Ore, O. (2012).
Number theory and its history.
Courier Corporation.

Rosen, K. H. (2011).
Elementary number theory.
Pearson Education.