Applications of CRT

2021.11

Jiageng Chen

Ring morphisms

Let *R* and *S* be two rings

(a) A **ring homomorphism** (or, for short, **ring morphism**, or, more informally, **ring homo** or **ring hom** or **ring map**) from R to S means a map $f : R \to S$ that

- **respects addition** (i.e., satisfies $f(a+b) = f(a) + f(b)$ for all $a, b \in R$);
- **respects multiplication** (i.e., satisfies $f(ab) = f(a) \cdot f(b)$ for all $a, b \in R$);
- **respects the zero** (i.e., satisfies $f(0_R) = 0_S$);
- **respects the unity** (i.e., satisfies $f(1_R) = 1_S$).

(b) A **ring isomorphism** (or, informally, **ring iso**) from R to S means an invertible ring morphism $f : R \to S$ whose inverse $f^{-1} : S \to R$ is also a ring morphism.

(c) The rings R and S are said to be **isomorphic** (this is written $R \cong S$) if there exists a ring isomorphism from R to S.

Chinese Remainder Theorem (CRT)

If the n_i are pairwise coprime, and if $a_1, \ldots, a_k$ are any integers, then the system

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a solution, and any two solutions, say x_1 and x_2, are congruent modulo N,

$$x_1 \equiv x_2 (\bmod N) \qquad N = n_1 \cdots n_k$$

Algebraic interpretation

if the n_j are pairwise coprime, the map $x \bmod N \mapsto (x \bmod n_1, \ldots, x \bmod n_k)$

defines a ring isomorphism

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

Z/6Z -> Z/2Z X Z/3Z

- Z/6Z: Quotient ring of Z by ideal 6Z
  - Six cosets (residue classes) modulo 6Z
  - 0+6Z, 1+6Z, 2+6Z, 3+6Z, 4+6Z, 5+6Z
  - Isomorphic to ring Z_6
- Z/2Z: Quotient ring of Z by ideal 2Z
  - 0+2Z, 1+2Z
- Z/3Z: Quotient ring of Z by ideal 3Z
  - 0+3Z, 1+3Z, 2+3Z

Map Z/6Z -> Z/2Z X Z/3Z

0+6Z -> (0+2Z, 0+3Z)
1+6Z -> (1+2Z, 1+3Z)
2+6Z -> (0+2Z, 2+3Z)
3+6Z -> (1+2Z, 0+3Z)
4+6Z -> (0+2Z, 1+3Z)
5+6Z -> (1+2Z, 2+3Z)

Z/2Z X Z/3Z ->Z/6Z

Applying Chinese remainder theorem on equations:

$$x \equiv a_1(mod\ 2)$$
$$x \equiv a_2(mod\ 3)$$

In case we have r equations with modulo $m_1, \dots, m_r$
Let $M = m_1 \cdots m_r$ and $M_k = M/m_k$, thus $\gcd(M_k, m_k) = 1$.
From extended Euclidean algorithm, we can derive y_k such that $M_k y_k \equiv 1(mod\ m_k)$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r$$

$x = a_1 3 y_1 + a_2 2 y_2$ for Z/2Z X Z/3Z ->Z/6Z

Rabin Trapdoor (wiki)

Key generation

The keys for the Rabin cryptosystem are generated as follows:

1. Choose two large distinct prime numbers p and q such that $p \equiv 3 \bmod 4$ and $q \equiv 3 \bmod 4$.
2. Compute $n = pq$.

Then n is the public key and the pair (p, q) is the private key.

Encryption

A message M can be encrypted by first converting it to a number $m < n$ using a reversible mapping, then computing $c = m^2 \bmod n$. The ciphertext is c.

Rabin Trapdoor (wiki)

Decryption

1. Compute the square root of c modulo p and q using these formulas:

$$m_p = c^{\frac{1}{4}(p+1)} \bmod p$$
$$m_q = c^{\frac{1}{4}(q+1)} \bmod q$$

2. Use the extended Euclidean algorithm to find y_p and y_q such that $y_p \cdot p + y_q \cdot q = 1$.
3. Use the Chinese remainder theorem to find the four square roots of c modulo n :

$$r_1 = (y_p \cdot p \cdot m_q + y_q \cdot q \cdot m_p) \bmod n$$
$$r_2 = n - r_1$$
$$r_3 = (y_p \cdot p \cdot m_q - y_q \cdot q \cdot m_p) \bmod n$$
$$r_4 = n - r_3$$

Example

- Parameters
  - p = 7, q=11, n=77, m=20
- Encryption
  - $c = m^2\, mod\, n = 400\, mod\, 77 = 15$
- Decryption

$$m_p = c^{\frac{1}{4}(p+1)} \bmod p = 15^2 \bmod 7 = 1 \text{ and } m_q = c^{\frac{1}{4}(q+1)} \bmod q = 15^3 \bmod 11 = 9$$

Use the extended Euclidean algorithm to compute $y_p = -3$ and $y_q = 2$.

$$y_p \cdot p + y_q \cdot q = (-3 \cdot 7) + (2 \cdot 11) = 1$$

Compute the four plaintext candidates:

$$r_1 = (-3 \cdot 7 \cdot 9 + 2 \cdot 11 \cdot 1) \bmod 77 = 64$$
$$r_2 = 77 - 64 = 13$$
$$r_3 = (-3 \cdot 7 \cdot 9 - 2 \cdot 11 \cdot 1) \bmod 77 = \mathbf{20}$$
$$r_4 = 77 - 20 = 57$$