Number-Theoretic Algorithms

Hengfeng Wei

hfwei@nju.edu.cn

March 31 $\sim$ April 2, 2017

Number-Theoretic Algorithms

"Mod"

(TC 31.4.2)

$$ad \equiv bd \pmod{n}, a \perp n \implies a \equiv b \pmod{n}$$

$$3 \cdot 2 \equiv 5 \cdot 2 \pmod{4} \quad 3 \not\equiv 5 \pmod{4}$$

"Mod"

(TC 31.4.2)

$$ad \equiv bd \pmod{n}, a \perp n \implies a \equiv b \pmod{n}$$

$$3 \cdot 2 \equiv 5 \cdot 2 \pmod{4} \quad 3 \not\equiv 5 \pmod{4} \quad 3 \equiv 5 \pmod{2}$$

Changing the modulus

$$ad \equiv bd \pmod{nd} \iff a \equiv b \pmod{n} \quad (d \neq 0)$$

$$ad \equiv bd \pmod{n} \iff a \equiv b \pmod{\frac{n}{\gcd(d, n)}}$$

Changing the modulus

$$a \equiv b \pmod{100} \implies a \equiv b \pmod{20} \implies a \equiv b \pmod{5}$$

$$a \equiv b \pmod{nd} \implies a \equiv b \pmod{n}, d \in \mathbb{Z}$$

$$a \equiv b \pmod{n_1}, a \equiv b \pmod{n_2} \iff a \equiv b \pmod{\operatorname{lcm}(n_1, n_2)}$$

$$a \equiv b \pmod{n_1}, a \equiv b \pmod{n_2} \iff a \equiv b \pmod{n_1 n_2}, \text{ if } n_1 \perp n_2$$

$$a \equiv b \pmod{n} \iff a \equiv b \pmod{p^{n_p}}, \quad n = \prod_p p^{n_p}$$

Changing the modulus

Number-Theoretic Algorithms

Pairwise relatively prime (Problem 31.2-9)

n_1, n_2, n_3, n_4 are pairwise relatively prime

$$\iff$$

$$\text{gcd}(n_1 n_2, n_3 n_4) = \text{gcd}(n_1 n_3, n_2 n_4) = 1$$

$n_1, n_2, \ldots, n_k$ are pairwise relatively prime

$$\iff$$

a set of $\lceil \lg k \rceil$ pairs of numbers derived from the n_i are relatively prime.

$n_1, n_2, \ldots, n_k$ are pairwise relatively prime

$$\Longleftrightarrow$$

a set of $\lceil \lg k \rceil$ pairs of numbers derived from the n_i are relatively prime.

$$\text{gcd}(\boxed{1_L}, \boxed{1_R}) = \text{gcd}(\boxed{2_L}, \boxed{2_R}) = \cdots = \text{gcd}(\boxed{\lceil \lg k \rceil_L}, \boxed{\lceil \lg k \rceil_R}) = 1$$

$$n_1, n_2, \ldots, n_k \text{ are pairwise relatively prime}$$

$$\iff$$

a set of $\lceil \lg k \rceil$ pairs of numbers derived from the n_i are relatively prime.

$$\text{gcd}(\boxed{1_L}, \boxed{1_R}) = \text{gcd}(\boxed{2_L}, \boxed{2_R}) = \cdots = \text{gcd}(\boxed{\lceil \lg k \rceil_L}, \boxed{\lceil \lg k \rceil_R}) = 1$$

$$k = 4: \quad \text{gcd}(n_1 n_2, n_3 n_4) = \text{gcd}(n_1 n_3, n_2 n_4) = 1$$

$$k = 3: \quad \text{gcd}(n_1, n_2 n_3) = \text{gcd}(n_2, n_3) = 1$$

$$k = 2: \quad \text{gcd}(n_1, n_2) = 1$$

$$k = 7: \quad n_1, n_2, n_3, n_4, n_5, n_6, n_7$$

$$k = 7: \quad n_1, n_2, n_3, n_4, n_5, n_6, n_7$$

$$\text{gcd}(n_1 n_2 n_3, n_4 n_5 n_6 n_7) = 1$$

TODO: figure here.

$$\begin{cases} T(1) = 0 \\ T(2) = 1 \\ T(k) = 2T(\frac{k}{2}) + 1 \end{cases}$$

$$k = 7: \quad n_1, n_2, n_3, n_4, n_5, n_6, n_7$$

$$\text{gcd}(n_1 n_2 n_3, n_4 n_5 n_6 n_7) = 1$$

TODO: figure here.

$$\begin{cases} T(1) = 0 \\ T(2) = 1 \\ T(k) = 2T(\frac{k}{2}) + 1 \end{cases} \implies T(k) = k - 1 = \Theta(k)$$

$$k = 7: \quad n_1, n_2, n_3, n_4, n_5, n_6, n_7$$

$$k = 7 : \quad n_1, n_2, n_3, n_4, n_5, n_6, n_7$$

$$\text{gcd}(n_1 n_2 n_3, n_4 n_5 n_6 n_7) = 1$$

TODO: figure here.

$$\begin{cases} T(1) = 0 \\ T(2) = 1 \\ T(k) = T(\frac{k}{2}) + 1 \end{cases}$$

$$k = 7: \quad n_1, n_2, n_3, n_4, n_5, n_6, n_7$$

$$\text{gcd}(n_1 n_2 n_3, n_4 n_5 n_6 n_7) = 1$$

TODO: figure here.

$$\begin{cases} T(1) = 0 \\ T(2) = 1 \\ T(k) = T(\frac{k}{2}) + 1 \end{cases} \implies T(k) = \lceil \lg k \rceil$$

Looking into the divide steps

Not exactly the same

Can we do even better?

Biclique covering

Biclique covering

Number-Theoretic Algorithms

Chinese Remainder Theorem (CRT)

Where do m_i, c_i, and a come from?

History of CRT

Proof of CRT (1)

Proof of CRT (2)

Proof of CRT (3)

CRT

Meaning of Figure 31.3

$\equiv 1$ and $\equiv 0$ elsewhere

ϕ function

CRT with non-pairwise coprime moduli

Application?

Application?