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

Worst-case analysis of Euclid's algorithm

(TC 31.2–5)

1. If $a > b \geq 0$, $\textsc{Euclid}(a, b)$ makes $\leq r \triangleq 1 + \log_\phi b$ recursive calls.

$$a > b \geq 1, b < F_{k+1} \implies r < k.$$

$$r \leq 1 + \log_\phi b \implies k = 2 + \log_\phi b, b < F_{3+\log_\phi b}$$

$$F_k = \frac{\phi^k - \hat{\phi}^k}{\sqrt{5}} = [\frac{\phi^k}{\sqrt{5}}] \geq \frac{\phi^k}{\sqrt{5}}$$

Worst-case analysis of Euclid's algorithm

(TC 31.2–5)

1. If $a > b \geq 0$, $\textsc{Euclid}(a, b)$ makes $\leq r \triangleq 1 + \log_\phi b$ recursive calls.

$$a > b \geq 1, b < F_{k+1} \implies r < k.$$

$$r \leq 1 + \log_\phi b \implies k = 2 + \log_\phi b, b < \boxed{?} \leq F_{3+\log_\phi b}$$

$$F_k = \frac{\phi^k - \hat{\phi}^k}{\sqrt{5}} = [\frac{\phi^k}{\sqrt{5}}] \geq \frac{\phi^k}{\sqrt{5}}$$

Worst-case analysis of Euclid's algorithm

(TC 31.2–5)

2. Improve this bound to $1 + \log_\phi(\frac{b}{\gcd(a,b)})$.

$$(a,b) = (a,b) \cdot (\frac{a}{(a,b)}, \frac{b}{(a,b)})$$

$$\textsc{Euclid}(a,b) \leftrightarrow \textsc{Euclid}(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})$$

$$\textsc{Euclid}(b, a \mod b) \leftrightarrow \textsc{Euclid}(\frac{b}{\gcd(a,b)}, \frac{a}{\gcd(a,b)} \mod \frac{b}{\gcd(a,b)})$$

$$\frac{a}{\gcd(a,b)} \mod \frac{b}{\gcd(a,b)} = \frac{a \mod b}{\gcd(a,b)}$$

Worst-case analysis of Euclid's algorithm

(TC 31.2–5)

2. Improve this bound to $1 + \log_\phi(\frac{b}{\gcd(a,b)})$.

Lemma (Generalization of Lemma 31.10)

If $a > b \geq 1, d = \gcd(a, b)$ *and the call* $\textsc{Euclid}(a, b)$ *performs* $k \geq 1$ *recursive calls, then* $a \geq dF_{k+2}$ *and* $b \geq dF_{k+1}$.

Average-case analysis of Euclid's algorithm

$$T(m,0) = 0; \quad T(m,n) = 1 + T(n, m \mod n)\ n \geq 1$$

When m is chosen at random:

$$T_n = \frac{1}{n} \sum_{0 \leq k < n} T(k,n)$$

Assume that, for $0 \leq k < n$, $(n \mod k)$ is "random":

$$T_n \approx 1 + \frac{1}{n}(T_0 + T_1 + \cdots + T_{n-1})$$

Average-case analysis of Euclid's algorithm

$$T(m,0)=0; \quad T(m,n)=1+T(n,m \mod n)\ n\geq 1$$

When m is chosen at random:

$$T_n=\frac{1}{n}\sum_{0\leq k<n} T(k,n)$$

Assume that, for $0\leq k<n$, $(n \mod k)$ is "random":

$$T_n\approx 1+\frac{1}{n}(T_0+T_1+\cdots+T_{n-1})=1+\frac{1}{2}+\cdots+\frac{1}{n}=H_n\approx \ln n+O(1)$$

Reference

"The Art of Computer Programming, Vol 2: Seminumerical Algorithms (Section 4.5.3)" by Donald E. Knuth, 3rd edition.

Number-Theoretic Algorithms

Pairwise relatively prime (Problem 31.2-9)

n_1, n_2, n_3, n_4 are pairwise relatively prime

$$\Longleftrightarrow$$

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

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

$$\Longleftrightarrow$$

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

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

$$\Longleftrightarrow$$

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

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

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

$$\Longleftrightarrow$$

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

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

$$k = 4: \quad \gcd(n_1 n_2, n_3 n_4) = \gcd(n_1 n_3, n_2 n_4) = 1$$
$$k = 3: \quad \gcd(n_1, n_2 n_3) = \gcd(n_2, n_3) = 1$$
$$k = 2: \quad \gcd(n_1, n_2) = 1$$

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

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

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

TODO: figure here.

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

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

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

TODO: figure here.

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

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

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

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

TODO: figure here.

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

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

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

TODO: figure here.

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

Looking into the divide steps

Not exactly the same

Can we do even better?

Biclique covering

Biclique covering

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?