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 $a > b \leq 1, d = \gcd(a, b)$ *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

1. Modular Arithmetic
2. Euclid's Algorithm
3. Chinese Remainder Theorem

Pairwise relatively prime

(TC 31.2–9)

$$n_1, n_2, n_3, n_4 \text{ are pairwise relatively prime}$$
$$\iff$$
$$\gcd(n_1 n_2, n_3 n_4) = \gcd(n_1 n_3, n_2 n_4) = 1$$

Pairwise relatively prime

(TC 31.2–9)

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

$$\Longleftrightarrow$$

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

Pairwise relatively prime

(TC 31.2–9)

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

$$\Longleftrightarrow$$

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

$$\binom{k}{2} = \Theta(k^2) \quad \text{(complete graph)}$$

Pairwise relatively prime

(TC 31.2–9)

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

$$\Longleftrightarrow$$

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

$$\binom{k}{2} = \Theta(k^2) \quad \text{(complete graph)}$$

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

Pairwise relatively prime

(TC 31.2–9)

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

$$\iff$$

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

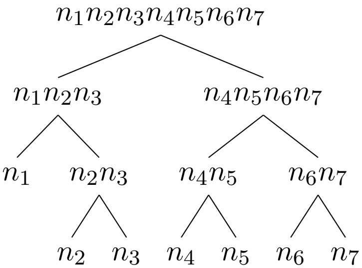
$$\binom{k}{2} = \Theta(k^2) \quad \text{(complete graph)}$$

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

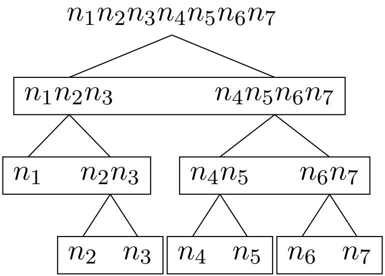
$$k = 3: \quad gcd(n_1, n_2 n_3) = gcd(n_2, n_3) = 1$$

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

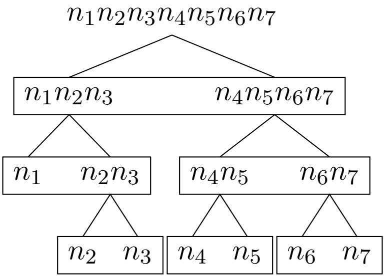
Pairwise relatively prime: divide-and-conquer



Pairwise relatively prime: divide-and-conquer

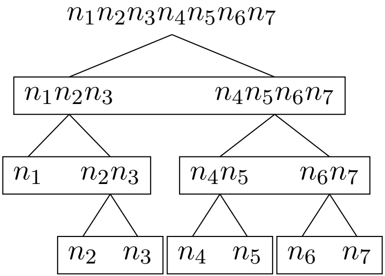


Pairwise relatively prime: divide-and-conquer



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

Pairwise relatively prime: divide-and-conquer



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

Pairwise relatively prime: smarter combine

TODO: figure here.

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

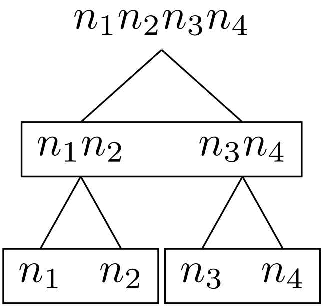
Pairwise relatively prime: smarter combine

TODO: figure here.

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

Pairwise relatively prime: the dividing pattern

Not exactly the same



gcd ???

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

Can we do even better?

$$T(k) \geq \lceil \lg k \rceil.$$

Can we do even better?

$$T(k) \geq \lceil \lg k \rceil.$$

Prove by (strong) mathematical induction.

Can we do even better?

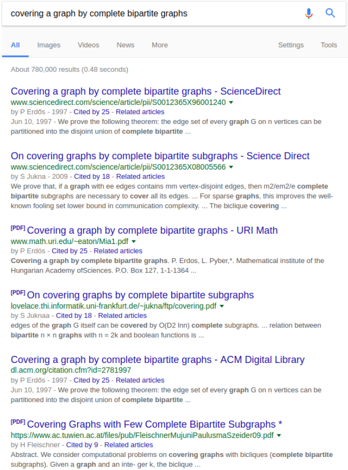
$$T(k) \geq \lceil \lg k \rceil.$$

Prove by (strong) mathematical induction.

$$\begin{aligned} T(k) &\geq 1 + T(\lceil \frac{k}{2} \rceil) \\ &\geq 1 + \lceil \lg \lceil \frac{k}{2} \rceil \rceil \\ &= \lceil \lg k \rceil \end{aligned}$$

Biclique covering

Covering a complete graph with few complete bipartite subgraphs.



covering a graph by complete bipartite graphs

All Images Videos News More Settings Tools

About 780,000 results (0.48 seconds)

Covering a graph by complete bipartite graphs - ScienceDirect
www.sciencedirect.com/science/article/pii/S0012365X96001240
by P Erdős - 1997 - Cited by 25 - Related articles
Jun 10, 1997 - We prove the following theorem: the edge set of every **graph** G on n vertices can be partitioned into the disjoint union of **complete bipartite** ...

On covering graphs by complete bipartite subgraphs - Science Direct
www.sciencedirect.com/science/article/pii/S0012365X08005566
by S Jukna - 2009 - Cited by 18 - Related articles
We prove that, if a **graph** with ee edges contains mm vertex-disjoint edges, then m2/em2/e **complete bipartite** subgraphs are necessary to **cover** all its edges. ... For sparse **graphs**, this improves the well-known fooling set lower bound in communication complexity. ... The biclique **covering** ...

[PDF] Covering a graph by complete bipartite graphs - URI Math
www.math.uri.edu/~eaton/Mia1.pdf
by P Erdös - Cited by 25 - Related articles
Covering a graph by complete bipartite graphs. P. Erdos, L. Pyber,*. Mathematical institute of the Hungarian Academy ofSciences. P.O. Box 127, 1-1-1364 ...

[PDF] On covering graphs by complete bipartite subgraphs
lovelace.thi.informatik.uni-frankfurt.de/~jukna/ftp/covering.pdf
by S Juknaa - Cited by 18 - Related articles
edges of the **graph** G itself can be **covered** by O(D2 lnn) **complete** subgraphs. ... relation between **bipartite** n × n **graphs** with n = 2k and boolean functions is ...

Covering a graph by complete bipartite graphs - ACM Digital Library
dl.acm.org/citation.cfm?id=2781997
by P Erdős - 1997 - Cited by 25 - Related articles
Jun 10, 1997 - We prove the following theorem: the edge set of every **graph** G on n vertices can be partitioned into the disjoint union of **complete bipartite** ...

[PDF] Covering Graphs with Few Complete Bipartite Subgraphs *
https://www.ac.tuwien.ac.at/files/pub/FleischnerMujuniPaulusmaSzeider09.pdf
by H Fleischner - Cited by 9 - Related articles
Abstract. We consider computational problems on **covering graphs** with bicliques (**complete bipartite** subgraphs). Given a **graph** and an inte- ger k, the biclique ...

Biclique covering: rethinking the first divide-and-conquer

$$T(k) = k - 1$$

Biclique covering: rethinking the first divide-and-conquer

$$T(k) = k - 1$$

edge-disjoint biclique partition

Biclique covering: rethinking the first divide-and-conquer

$$T(k) = k - 1$$

edge-disjoint biclique partition

Reference for $T(k) \geq k - 1$

"On the Addressing Problem for Loop Switching" by Graham and Pollak, 1971.

Biclique covering: rethinking the first divide-and-conquer

$$T(k) = k - 1$$

edge-disjoint biclique partition

Reference for $T(k) \geq k - 1$

"On the Addressing Problem for Loop Switching" by Graham and Pollak, 1971.

Reference for *weighted* biclique partition

"Covering a Graph by Complete Bipartite Graphs" by P. Erdos and L. Pyber, 1997.

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?