



Chapter 3

Primes and Greatest Common Divisors

邱錫彥 老師



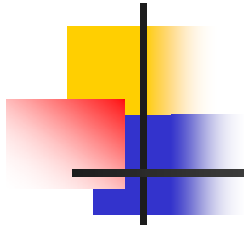
Content

3.1 Prime Numbers	3
3.2 The Distribution of Primes	11
3.3 Greatest Common Divisor.....	14
3.4 The Euclidean Algorithm.....	22
3.5 The Fundamental Theorem of Arithmetic.....	33
3.6 Factorization methods and the Fermat numbers.....	44
3.7 Linear Diophantine Equations.....	52



3.1 Prime numbers

- **Def:** Prime p satisfies
 - (a) $p > 1$, and $p \in \mathbb{Z}^+$
 - (b) If $a|p$ then $a = 1$ or p
- **Def:** n is a composite if
 - (a) $n > 1$, and $n \in \mathbb{Z}^+$
 - (b) n is not prime
- **Lemma:** Every positive integers greater than one has a prime divisor.



- Thm: There are infinitely many primes.

- Proof:

Let n be the largest prime and $Q_n = n! + 1$.

Then Q_n has at least one prime divisor q_n and $q_n > n$.

(If $q_n < n$, then $q_n | n!$, and then $q_n | (Q_n - n!) = 1$, impossible.)

So, we have found a prime q_n larger than n , $\forall n$.

\therefore there must be infinitely many primes.

- Thm: If n is a composite integer, then n has a prime factor not exceeding \sqrt{n}



The Sieve of Ero*tosthenes

- Goal: Find all the **primes** less than or equal to a given positive integer n .
- Steps:
 - (1) List all integers $\leq n$
 - (2) **Line out** the integers that can be divided by all the primes less than or equal to \sqrt{n}

Ex: Find all the primes ≤ 20

(1) **1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20**

(2) Since $\lfloor \sqrt{20} \rfloor = 4$ and the primes less than 4 are **2** and **3**.
We **line out** the integers that can be divided by **2** and **3**.

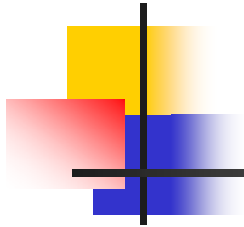


- The **complexity** of Sieve of Eratosthenes is $O(\sqrt{n})$.
- The **prime distribution**:
Facts:
 - (1) They become **rarer and rarer** the larger they get.
 - (2) Apart from this regularity in their mean density, their distribution seems rather **irregular**.

Ex: Show that the approximate probability $W(x)$ that x is a prime satisfies $W(x) \approx 1/\ln x$

Proof:

Assume that divisibility by different prime is independent. (Note that is not true!)



$$\text{Then } W(x) \approx (1-1/2)(1-1/3)\dots \approx \prod_{p_i < x} \left(1 - \frac{1}{p_i}\right)$$

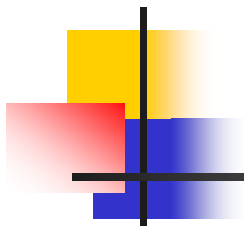
$$\ln W(x) \approx \sum_{p_i < x} \ln\left(1 - \frac{1}{p_i}\right)$$

$$\approx - \sum_{p_i < x} \frac{1}{p_i} \quad \because \ln(1-\varepsilon) \approx -\varepsilon \text{ if } \varepsilon \ll 1$$

$$\approx - \sum_2^x \frac{W(n)}{n} \quad (\text{a given term } 1/n \text{ in the sum}$$

$$\approx - \int_2^x \frac{W(n)}{n} dn \quad \text{occurs with probability } W(n))$$

Let $A(x) = 1/W(x)$, i.e. $A(x)$ is the average distance.



$$\text{Then } \ln A(x) = \int_2^x \frac{1}{nA(n)} dn$$

$$\frac{A'(x)}{A(x)} \approx \frac{1}{xA(x)} \quad \text{or} \quad A'(x) \approx \frac{1}{x}$$

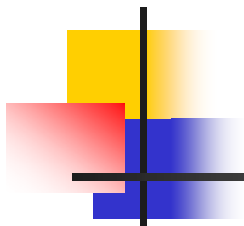
$$\Rightarrow A(x) \approx \ln(x) \Rightarrow W(x) \approx \frac{1}{\ln x}$$

Ex: $x = 20$. $\ln 20 \approx 3$. The average spacing of the primes closest to 20 is 3. Check(17,19,23)

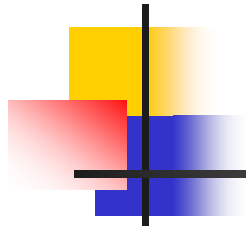


$$x = 150, \ln 150 \approx 5$$

$$x = 10^{50}, \ln 10^{50} \approx 115$$



- Def: The function $\pi(x)$, $x \in \mathbb{Z}^+$, denotes the no. of primes not exceeding x .
- Ex: $\pi(10) = 4$, $\pi(100) = 25$
Q: $\pi(20) = ?$, $\pi(30) = ?$



➤ Complexity of showing n is a prime

by the Sieve of Eratosthenes:

Given n , there are approximately $\frac{\sqrt{n}}{\ln \sqrt{n}} = \frac{2\sqrt{n}}{\ln n}$ primes not exceeding \sqrt{n} .

To divide n by an integer m takes $O(\log_2 n \cdot \log_2 m)$ bit operations.

So, we need $\frac{2\sqrt{n}}{\ln n} (c \log_2 |n| \log_2 |m|) \approx c\sqrt{n}$ bit operations

Therefore, the complexity is $O(\sqrt{n})$



3.2 The Distribution of Primes

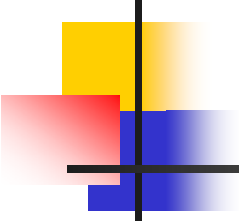
Estimation of $\pi(x)$

1. By Gauss(1793): $\pi(x) \approx x / \ln x$ (1)

2. By Legendre(1778): $\pi(x) \approx x / (\ln x - 1.08366)$ (2)

- (2) is better than (1), if $x < 4 \times 10^6$
- (2) \approx (1), if $4 \times 10^6 < x < 5 \times 10^6$
- (1) is better than (2), if $x > 5 \times 10^6$





3. $\pi(x) \approx \int_2^x \frac{dt}{\ln t} = Li(x)$

4. By Riemann

$$\pi(x) \approx Li(x) - \frac{1}{2} Li(\sqrt{x}) - \frac{1}{3} Li(\sqrt[3]{x}) - \dots$$

➤ Thm: $\lim_{x \rightarrow \infty} \pi(x) / \frac{x}{\log x} = 1$

- Conjectured by Gauss in 1793 and be proven by Hadamard and Vall'ee-Poussin in 1896.



- **Thm:** For any $n \in \mathbb{Z}^+$, there are at least n consecutive composite positive integers.
Proof: Consider the n consecutive positive integers,
 $(n+1)!+2, (n+1)!+3, \dots, (n+1)!+(n+1)$
Since $j|(n+1)!, \forall 2 \leq j \leq n+1$,
these n consecutive integers are all composite.

- **Def: Twin primes:**
Pairs of primes differ by two.
Ex: 5 and 7, 11 and 13, 101 and 103, 4967 and 4969.

- **Goldbach's conjecture**
Every even positive integer greater than two
can be written as the sum of two primes.
Ex: $100=3+97=11+89=17+83=29+71=41+59=47+53$



3.3 Greatest Common Divisor

Def : If $a, b \in \mathbb{Z}$ and $a \neq b \neq 0$, then (a, b) is the largest integers which divides both a and b . $(0, 0) = 0$

Def : Let $a, b \in \mathbb{Z}$, then a and b are called relatively prime if $(a, b) = 1$.

Thm: If $a, b, c \in \mathbb{Z}$ with $(a, b) = d$, then

- (i) $(a/d, b/d) = 1$
- (ii) $(a+cb, b) = (a, b)$.

• Special case:

Let $c = -[a/b] = -q$

and $a+cb = a-qb = r, 0 \leq r < b-1$, then

$(r, b) = (a, b)$.



proof:

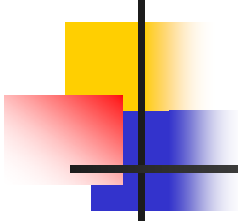
(i) Let $e = (a/d, b/d)$, then $\exists k, l \in \mathbb{Z}$ with
 $a/d = ke$ and $b/d = le \Rightarrow a = dek$ and $b = del$.
 $\therefore de|a$ and $de|b$

Since $(a, b) = d$, $\therefore de \leq d \Rightarrow e = 1$.

(ii) \rightarrow Let $e \in \mathbb{Z}$, $\exists e|a$ and $e|b$, then $e|(a+cb)$..
By Thm 1.8...so, $e|(a+cb)$ and $e|b$.

\rightarrow Let $f \in \mathbb{Z}$, $\exists f|(a+cb)$ and $f|b$, then
 $f|(a+cb) - cb = a$. $f|a$ and $f|b$.

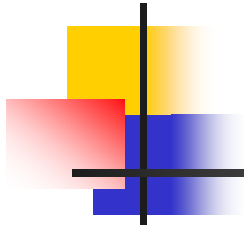
Hence $(a+cb, b) = (a, b)$

A decorative graphic on the left side of the slide consists of overlapping yellow, red, and blue squares with a black crosshair.

Def : If $a, b \in \mathbb{Z}$, then a linear combination of a and b is the sum of the form $ma + nb$, where $m, n \in \mathbb{Z}$.

Thm : Let $a, b \in \mathbb{Z}$ and $a \neq b \neq 0$, then (a, b) is the least positive integer that is a linear combination of a and b .

proof: Let d be the least positive integer of linear combination and $d = ma + nb$, where $m, n \in \mathbb{Z}$.
We must show (i) $d|a$ and $d|b$
(ii) if $c|a$ and $c|b$, then $c|d$.



(i) By the division algorithm, $a = dq+r$, $0 \leq r < d$, then
 $r = a - qd = a - q(ma + nb) = (1 - qm)a - qnb$
 r is a linear combination of a and b , $0 \leq r < d$,
and d is the least positive linear combination
of a and b .

So, $r = 0$ $d|a$. Similarly, $d|b$.

(ii) Let $c|a$ and $c|b$, $\therefore d = ma + nb$, we have $c|d$. #

Def: (a_1, a_2, \dots, a_n) is the largest integer which is the
largest common divisor of a_1, a_2, \dots, a_n .



Lemma:

$$(a_1, a_2, \dots, a_{n-1}, a_n) = (a_1, a_2, \dots, a_{n-2}, (a_{n-1}, a_n))$$

This Lemma shows a recursive way to find (a_1, a_2, \dots, a_n) by using $n - 1$ times of evaluating (a, b) .

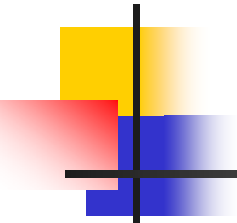
Ex: Find $(105, 140, 350)$.

<Sol>:

$$(105, 140, 350) = (105, (140, 350)) = (105, 70) = 35.$$

Def: The integers a_1, a_2, \dots, a_n are called mutually relatively prime if $(a_1, a_2, \dots, a_n) = 1$.

Def: The integers a_1, a_2, \dots, a_n are called pairwise relatively prime if $(a_i, a_j) = 1, \forall i \neq j$.



<Note>: If the integers are pairwise relatively prime, they must be mutually relatively prime. However, the converse is false.

Ex : $(15, 21, 35) = (15, 7) = 1$, \therefore they are mutually relatively prime but not pairwise relatively prime.

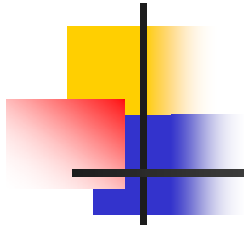
補充
教材

Def : Coprime : a and b are coprime if $(a, b) = 1$.

- Coprime probability $\cong 0.608$

Proof:

Let w_2 be the prob. that $(a, b) = 1$, where a and b are chosen from a large range randomly and independently.



Given prime p_i , the prob. that $p_i|a$ is $\frac{1}{p_i}$.
The prob. that both $p_i|a$ and $p_i|b$ is approximately $\frac{1}{p_i^2}$.

$$\therefore w_2 \cong \prod_{p_i} \left(1 - \frac{1}{p_i^2}\right)$$

$$\text{or } \frac{1}{w_2} \cong \prod_{p_i} \frac{1}{\left(1 - \frac{1}{p_i^2}\right)} = \prod_{p_i} \left(1 + \frac{1}{p_i^2} + \frac{1}{p_i^4} + \dots\right)$$

$$\cong \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

$$\therefore w_2 \cong \frac{6}{\pi^2} = 0.608 \text{ (for large primes)}$$



補充
教材

- The prob. that a randomly selected integer n is

“Square free” is $1 - \frac{1}{p_i^2}$

$$\because P(p_i^2 \nmid n) \cong \left(1 - \frac{1}{p_i^2}\right) + \frac{1}{p_i} \left(1 - \frac{1}{p_i}\right) = 1 - \frac{1}{p_i^2}$$

補充
教材

- The prob. that $(a_1, a_2, \dots, a_n) = 1$ is $w_n \cong \sum_{n=1}^{\infty} \frac{1}{i^n}$, 怪!
- where a_i are randomly selected

$$\text{Ex : } w_2 \cong 0.608, w_3 \cong 0.832, w_4 \cong \frac{90}{\pi^4} = 0.9239.$$

補充
教材

- The prob. that a_1, a_2, \dots, a_k are pairwise coprime is

$$\prod_{p_i} \left[\left(1 - \frac{1}{p_i}\right)^k + \frac{k}{p_i} \left(1 - \frac{1}{p_i}\right)^{k-1} \right]$$

For $k = 3$, the prob. is about 0.28.



3.4 The Euclidean Algorithm

A systematic method to find the **GCD** of two positive integers

Lemma : If $c, d \in \mathbb{Z}$ and $c = dq + r$, where $q, r \in \mathbb{Z}$, then $(c, d) = (d, r)$.

<proof>:

(1) $\because r = c - dq$, if $e|c$ and $e|d$, then $e|r$.

(2) $\because c = dq + r$, if $e|d$ and $e|r$, then $e|c$.

$\Rightarrow (c, d) = (d, r)$

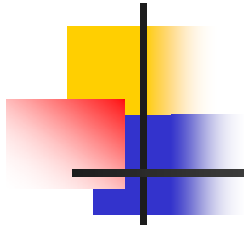


Thm : The Euclidean Algorithm

Let $r_0 = a$, $r_1 = b$ be integers $\ni a \geq b > 0$. If the division algorithm is successively applied to obtain $r_j = r_{j+1}q_{j+1} + r_{j+2}$, with $0 < r_{j+2} < r_{j+1}$, for $j = 0, 1, \dots, n-2$ and $r_{n+1} = 0$, then $(a, b) = r_n$ (the last nonzero remainder.)

<proof>: Since

$$\begin{array}{ll} r_0 = r_1 q_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = r_2 q_2 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & \\ r_{j-2} = r_{j-1} q_{j-1} + r_j & 0 \leq r_j < r_{j-1} \\ \vdots & \\ r_{n-2} = r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} = r_n q_n & \end{array}$$



we will obtain a remainder of zero since $a = r_0 > r_1 > \dots \geq 0$

$$\therefore (a, b) = (r_0, r_1) = (r_1, r_2) = \dots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, 0) = r_n$$

Ex : Find $(252, 198)$.

<sol>: $252 = 198 \times 1 + 54$

$$198 = 54 \times 3 + 36$$

$$54 = 36 \times 1 + 18$$

$$36 = 18 \times 2$$

$$(252, 198) = 18$$

2	252	198
	126	99
3	42	33
	14	11
$(252, 198) = 2 \times 3 \times 3 = 18$		



- **Thm:** Let f_{n+1} and f_{n+2} be the successive terms of the Fibonacci sequence with $n > 1$. Then the **Euclidean Algorithm** takes exactly n divisions to show that $(f_{n+1}, f_{n+2}) = 1$.

<proof>:

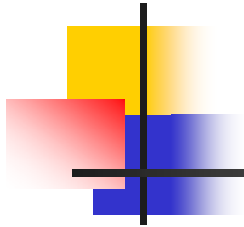
$\therefore f_j = f_{j-1} + f_{j-2}$, we have

$$f_{n+2} = f_{n+1} + f_n$$

$$f_{n+1} = f_n + f_{n-1}$$

$$f_3 = f_2 \times 2$$

\therefore It takes exactly n divisions to show $(f_{n+1}, f_{n+2}) = f_2 = 1$.

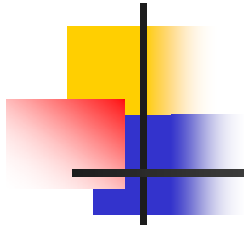


- Complexity of the Euclidean Algorithm

Thm : (By G. Lamé' 1845)

The number, $T(b)$, of divisions needed to find (a, b) ,
 $a > b$, using the Euclidean Algorithm satisfies

$$T(b) \leq 5 \log_{10} b.$$



<Proof.>

From the proof of the Euclidean Algorithm,

$$\begin{aligned}r_0 &= r_1 q_1 + r_2 & 0 \leq r_2 < r_1 \\r_1 &= r_2 q_2 + r_3 & 0 \leq r_3 < r_2 \\&\vdots \\r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\r_{n-1} &= r_n q_n\end{aligned}$$

we have used $T(b) = n$ divisions to find (a, b) .

Note that $q_i \geq 1$ ($1 \leq i \leq n - 1$) and $q_n \geq 2$, since $r_n < r_{n-1}$.



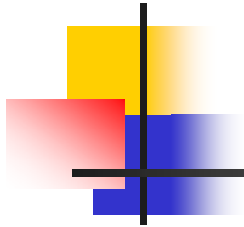
Therefore,

$$\begin{aligned}r_n &\geq 1 = f_2 \\r_{n-1} &\geq 2r_n \geq 2f_2 = f_3 \\r_{n-2} &\geq r_{n-1} + r_n \geq f_3 + f_2 = f_4 \\&\vdots \\r_2 &\geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n\end{aligned}$$

$$b = r_1 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1} > \alpha^{n-1} \left(\alpha = \frac{1+\sqrt{5}}{2} \right)$$

$$\therefore \log_{10} b > (n-1) \log_{10} \alpha > (n-1)/5 \quad (\because \log_{10} \alpha > 1/5)$$

$$\therefore n-1 < 5 \cdot \log_{10} b \Rightarrow T(b) < 5 \log_{10} b \blacksquare$$



[Note] This is the **worst case** for $T(b)$, in average,

$$T(b) \approx \frac{12 \ln 2}{\pi^2} \ln(b) \approx 1.9405 \log_{10} b$$

[Corollary]

The number of **bit operations** needed to find (a, b) with $a > b$ is $O((\log_2 b)^3)$.

• Given a and b , how to find s_n and $t_n \ni (a, b) = s_n a + t_n b$?



Thm : Let a and b be positive integers. Then

$$(a, b) = s_n a + t_n b \quad (\text{for } n = 0, 1, 2, \dots)$$

where s_n and t_n are the n th terms of the sequences defined recursively by

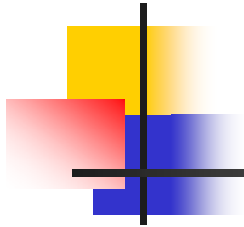
$$s_0 = 1, t_0 = 0$$

$$s_1 = 0, t_1 = 1$$

and

$$s_j = s_{j-2} - q_{j-1} s_{j-1}, t_j = t_{j-2} - q_{j-1} t_{j-1} \quad (\text{for } j = 2, 3, \dots, n)$$

where q_j are the quotients in the divisions of the Euclidean Algorithm when it is used to find (a, b) .



[pf Hint] If we can prove that $r_j = s_j a + t_j b$ for $j = 1, 2, \dots, n$,
then since $(a, b) = r_n$, we have $(a, b) = s_n a + t_n b$.

[Proof] By induction,

(i) $j = 0$ is true, $a = r_0 = 1 \times a + 0 \times b = s_0 a + t_0 b$

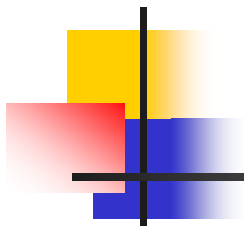
$j = 1$ is true, $b = r_1 = 0 \times a + 1 \times b = s_1 a + t_1 b$

(ii) Assume that $r_j = s_j a + t_j b$, for $j = 1, 2, \dots, k-1$

$$\therefore r_k = r_{k-2} - r_{k-1} q_{k-1}$$

(in the k th step of E.A.)

$$\begin{aligned} \text{Then } r_k &= (s_{k-2} a + t_{k-2} b) - (s_{k-1} a + t_{k-1} b) q_{k-1} \\ &= (s_{k-2} - s_{k-1} q_{k-1}) a - (t_{k-2} - t_{k-1} q_{k-1}) b \\ &= s_k a + t_k b \end{aligned}$$



[Note] (a, b) can be expressed in an infinite no. of different ways as a linear combination of a and b .

Since if $(a, b) = d$ and $d = sa + tb$, then
$$d = (s + k(\frac{b}{d}))a + (t - k(\frac{a}{d}))b, \forall k \in \mathbb{Z}.$$



3.5 The Fundamental Theorem of Arithmetic

Lemma : Let $a, b, c \in \mathbb{Z}^+$. If $(a, b) = 1$ and $a|bc$, then $a|c$.

<proof>: Since $(a, b) = 1$, $\exists s$ and $t \ni sa + tb = 1$.

$\therefore sac + tbc = c$. If $a|bc$, then $a|sac + tbc = c$. ■

Lemma : If $p|(a_1 a_2 \dots a_n)$,
where p is a prime and $a_i \in \mathbb{Z}^+$, $\forall i$,
then $\exists i$ with $1 \leq i \leq n$, $\ni p|a_i$.

<proof>: (1) It is true for $n = 1$.

(2) Assume that it is true for n .

A decorative graphic on the left side of the slide, featuring a vertical black line intersected by a horizontal black line. To the left of the intersection are three overlapping squares: a yellow one on top, a red one on the left, and a blue one on the bottom.

If $p|(a_1 a_2 \dots a_n a_{n+1})$, then

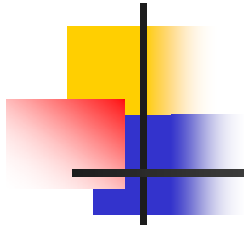
$$p|(a_1 a_2 \dots a_n) \times a_{n+1}.$$

From above Lemma,

either $p|(a_1 a_2 \dots a_n)$ or $p|a_{n+1}$

$\Rightarrow p|a_i$ for some i with $1 \leq i \leq n + 1$. ■

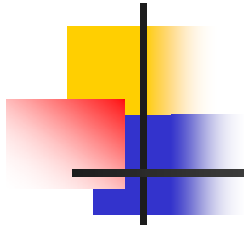
Thm: Let $n \in \mathbb{Z}^+$, p_i 's are primes, then n can be written uniquely as $n = p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}$ with $p_i < p_j$ if $i < j$ and $t_i \geq 0$



<proof>:

[Existence] (1) By contradiction, assume that n is the smallest number that cannot be written as the product of primes. If n is prime, then the Thm is true. So n must be composite.

Let $n = ab$, $1 < a < n$ and $1 < b < n$. But since $a, b < n$, a, b must be the product of primes. Then since $n = ab$, n is also a product of primes. This is contradiction.



[Unique] (2) If $n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$
where p_i, q_j are primes, $p_i \neq q_j, \forall 1 \leq i \leq s, 1 \leq j \leq t$,
with $p_1 \leq p_2 \leq \dots \leq p_s$ and $q_1 \leq q_2 \leq \dots \leq q_t$.
Remove all common primes from both sides,
 $p_{i_1} p_{i_2} \dots p_{i_u} = q_{j_1} q_{j_2} \dots q_{j_v}, u \geq 1, v \geq 1$.

However, it is a contradiction of above Lemma, since p_{i_j} must divide q_{j_j} for some j , which is impossible, since each q_{j_j} is a prime and is different from p_{i_j} , the prime factorization of n is unique.



Def: The least common multiple $\text{lcm}(a, b)$ of a and b , where $a, b \in \mathbb{Z}^+$, is the smallest positive integer that is divisible by a and b .

Fact: (1) Let $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$, where p_i is a prime $\forall i$, and $\min(a_i, b_i)$ denote the minimum of a_i and b_i . Then

$$\text{gcd}(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)} = \prod_{i=1}^n p_i^{\min(a_i, b_i)}$$

(2) Let $\max(a_i, b_i)$ denote the maximum of a_i and b_i . Then

$$\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)} = \prod_{i=1}^n p_i^{\max(a_i, b_i)}$$



Lemma: If $x, y \in R$, then $\max(x, y) + \min(x, y) = x+y$.

Thm: If $a, b \in \mathbb{Z}^+$, then $\text{lcm}(a, b) = \frac{ab}{\text{gcd}(a, b)}$
or $ab = \text{lcm}(a, b) \cdot \text{gcd}(a, b)$.

<proof>:

$$\begin{aligned} \text{lcm}(a, b) \text{gcd}(a, b) &= \prod_{i=1}^n p_i^{\max(a_i, b_i)} \prod_{i=1}^n p_i^{\min(a_i, b_i)} \\ &= \prod_{i=1}^n p_i^{\max(a_i, b_i) + \min(a_i, b_i)} \\ &= ab \quad \# \end{aligned}$$



Lemma: Let $m, n \in \mathbb{Z}^+$ and $(m, n) = 1$, if $d|mn$, then
 $\exists d_1, d_2 \in \mathbb{Z}^+ \ni d_1|m$ and $d_2|n$ and $d = d_1 d_2$.
Conversely, if $d_1|m$ and $d_2|n$, then $d|mn$, where
 $d = d_1 d_2$.

Thm 2.9: Dirichlet's Theorem on primes in
Arithmetic Progression(1837)

Let $a, b \in \mathbb{Z}^+$ and $(a, b)=1$, then $an + b, n = 1, 2, \dots$
contains infinitely many primes.

Lemma: If a and b are integers both of the form $4n+1$,
then ab is also of the form.

<proof>: Let $a = 4r+1, b = 4s+1$, then

$$\begin{aligned} ab &= (4r+1)(4s+1) = 16rs + 4r + 4s + 1 \\ &= 4(4rs+r+s) + 1 = 4k+1 \quad \blacksquare \end{aligned}$$



Thm 2.10: There are infinitely many primes of the form $4n+3$, where $n \in \mathbb{Z}^+$.

<proof>: By contradiction. Assume that there are only finite no. of primes of the form $4n+3$, say,

$p_0=3, p_1, p_2, \dots, p_r$

Let $Q = 4p_1p_2\dots p_r + 3$, then \exists a prime $q, q|Q$ and q is of the form $4n+3$. (If all these primes are of the form $4n+1$, the Q must be the form $4n+1$). But none of the primes p_0, p_1, \dots, p_r divides Q .

Hence, there are infinitely many primes of the form $4n+3$.



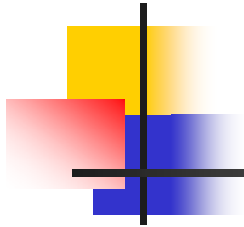
Thm 2.11: Let α be a root of the polynomial $x^n = c_{n-1}x^{n-1} + \dots + c_1x + c_0$ where the coefficients $c_0, c_1, \dots, c_{n-1} \in \mathbb{Z}$ with $c_0 \neq 0$. Then α is either an integer or an irrational number.

<proof>: Suppose α is rational, then $\alpha = a/b$, where $(a, b) = 1$ and $b \neq 0$. Since

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \dots + c_1\left(\frac{a}{b}\right) + c_0 = 0$$

we have $a^n + c_{n-1}a^{n-1}b + \dots + c_1ab^{n-1} + c_0b^n = 0$

Thus $a^n = b(-c_{n-1}a^{n-1} - \dots - c_1ab^{n-2} - c_0b^{n-1})$



It implies that $b|a^n$, since $(a, b) = 1$.
It is impossible, Unless $b = \pm 1$
 \therefore If α is rational then $\alpha = \pm a$, so
that α must be an integer.

Ex: Let a be a positive integer that is not the m -th
power of an integer. So that $\sqrt[m]{a}$ is not an
integer. Then $\sqrt[m]{a}$ is irrational.
(Note: a is the root of $x^m - a$.)



3.6 Factorization methods and the Fermat numbers

To factor n by the sieve of Eratosthenes, it needs $\pi\sqrt{N}$ divisions. So, the complexity is $O(\pi\sqrt{N} (\log N)^2) = O(\sqrt{N} (\log N)^2)$ bit operations.

<Note>: The fastest method (the so-called number field sieve) to factor N needs

$\exp((\log N)^{1/3} (\log \log N)^{2/3})$ bit operations

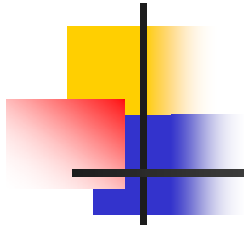


Table 2.1 Time Required for factorization of N (1992)

no. of decimal digits	no. of bit operation	Time
50	1.4×10^{10}	14 sec
75	9.0×10^{12}	3 hours
100	2.3×10^{15}	26 days
200	1.2×10^{23}	3.8×10^5 years
300	1.5×10^{29}	4.9×10^{21} years
500	1.3×10^{38}	4.2×10^{32} years

Assume the speed is 10^9 bit operations per second.



Fermat factorization

Lemma: If $n \in \mathbb{Z}^+$ and n is odd, then
 \exists a one-to-one correspondence between
factorizations of n into two positive integers and
difference of two squares that equal n .

$$\text{i.e., } n = ab = s^2 - t^2$$

Proof. Let $n = ab$, where $a, b \in \mathbb{Z}^+$, then

$$n = ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 = s^2 - t^2 \quad \blacksquare$$

Then we can factor n by $n = (s - t)(s + t)$.



Algorithm:

Look for solutions of the equation $n = x^2 - y^2$ by searching for **perfect squares** of the form $x^2 - n$, i.e., search

$$t^2 - n, (t+1)^2 - n, (t+2)^2 - n$$

where t is the smallest integer greater than \sqrt{n} .

- This procedure is **guaranteed to terminate**. Since

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 \Rightarrow \left(\frac{n-1}{2}\right)^2 = \left(\frac{n+1}{2}\right)^2 - n$$

- Complexity: $O\left(\frac{n+1}{2} - \sqrt{n}\right)$ steps.



• The Fermat numbers

Def: $F_n = 2^{2^n} + 1$ are called the Fermat numbers.


- $F_0=3, F_1=5, F_2=17, F_3=257, F_4=65537=2^{16}+1$ are primes but $F_5=2^{32}+1$ is composite

Ex: $641|F_5$

<sol>: Since $641 = 5 \cdot 2^7 + 1 = 2^4 + 5^4$

$$\begin{aligned}\therefore F_5 &= 2^{32} + 1 = 2^4 \cdot 2^{28} + 1 = (641 - 5^4) \cdot 2^{28} + 1 \\ &= 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1 = 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\ &= 641(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4)\end{aligned}$$

$\Rightarrow 641|F_5$



Thm: Every prime divisor of $F_n = 2^{2^n} + 1$ is of the form $2^{n+2}k+1$.

Ex: Show that $F_3 = 257$ is prime.

<Sol> If \exists a prime $p|F_3$ then p must be of the form $2^{n+2}k+1 = 2^5k+1 = 32k+1$. Since there is no such a prime $\leq \sqrt{257}$. $\therefore F_3$ is prime.

Ex: Factor $F_6 = 2^{2^6} + 1 = 2^{64} + 1$

<sol>: If $p|F_6$, then p is of the form $2^8k+1 = 256k+1$.

Search primes of the form that $p \leq \sqrt{F_6}$.

We find $(256 \times 1071 + 1) = 274177|F_6$.



Lemma: $F_0 F_1 \dots F_{n-1} = F_n - 2.$

Proof.

By induction,

it is true for $n = 1$, since $F_0 = 3 = 5 - 2 = F_1 - 2.$

Assume that it is true for n , then

$$\begin{aligned} F_0 F_1 \dots F_{n-1} F_n &= (F_0 F_1 \dots F_{n-1}) F_n = (F_n - 2) F_n \\ &= (2^{2^n} - 1)(2^{2^n} + 1) = (2^{2^n})^2 - 1 = (2^{2^{n+1}} + 1) - 2 = F_{n+1} - 2. \blacksquare \end{aligned}$$



Thm: $(F_m, F_n) = 1 \quad \forall m, n \geq 0$ and $m \neq n$.

Proof.

Assume $m < n$.

Let $d|F_m$, and $d|F_n$.

Since $F_0 F_1 \dots F_{n-1} = F_n - 2$,

$$d|F_n - F_0 F_1 \dots F_m \dots F_{n-1} = 2$$

$$\Rightarrow d = 1 \text{ or } 2.$$

But F_m and F_n are odd,

$$\Rightarrow d = 1 = (F_m, F_n) \quad \blacksquare$$



補充
教材

$n \mid 2^n - 2$ iff n is prime.

$$2 \mid 2^2 - 2$$

$$3 \mid 2^3 - 2$$

$$5 \mid 2^5 - 2$$

$$7 \mid 2^7 - 2$$

$$341 \mid 2^{341} - 2$$

$$4 \nmid 2^4 - 2 = 14$$

$2^n - 1$ if n is prime.



3.7 Linear Diophantine Equations

Problem: Given $a, b, c \in \mathbb{Z}$, we want to find the solutions for $ax + by = c, \exists x, y \in \mathbb{Z}$

- (i) Is there any solution?
- (ii) If there are solutions, how many solutions?
 - (a) exactly one? (b) infinitely?
 - (c) how many solutions $\exists x, y \in \mathbb{Z}$

Def: $ax + by = c$, where $a, b, c \in \mathbb{Z}$, is called a linear Diophantine equations in two variables.



Thm: Let $a, b \in \mathbb{Z}$ and $d = (a, b)$. Then $ax + by = c$

(1) has no integral solutions if $d \nmid c$.

(2) If $d \mid c$, then there are infinitely many integral solutions.

(3) If (x_0, y_0) is a particular solution,

then all solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right)n, \quad y = y_0 - \left(\frac{a}{d}\right)n, \quad \text{where } n \in \mathbb{Z}.$$



Proof.

(i) If $x, y \in \mathbb{Z}$ and $ax + by = c$, then

$$\therefore d|a \text{ and } d|b$$

$$\Rightarrow d|c.$$

(ii) Assume that $d|c$, then

$$\exists s, t, e \in \mathbb{Z} \ni d = (a, b) = as + bt \text{ and } de = c$$

$$\Rightarrow c = de = (as + bt)e = a(se) + b(te)$$

\therefore One solution is given by $x = x_0 = se$, $y = y_0 = te$.

$$\text{Let } x = x_0 + \left(\frac{b}{d}\right)n \text{ and } y = y_0 - \left(\frac{a}{d}\right)n, n \in \mathbb{Z},$$

$$\text{then } ax + by = ax_0 + a\left(\frac{b}{d}\right)n + by_0 - b\left(\frac{a}{d}\right)n$$

$$= ax_0 + by_0 = c$$

\therefore there are infinitely many solutions.



(iii) Suppose $x, y \in \mathbb{Z}$, $\exists ax + by = c$

$$\because ax_0 + by_0 = c \Rightarrow a(x - x_0) + b(y - y_0) = 0$$

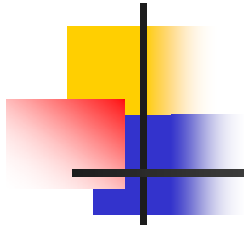
$$\Rightarrow a(x - x_0) = b(y_0 - y) \Rightarrow \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$$

$$\because \left(\frac{a}{d}, \frac{b}{d}\right) = 1 \Rightarrow \frac{a}{d} \mid (y_0 - y)$$

$$\Rightarrow \exists n \in \mathbb{Z} \exists \left(\frac{a}{d}\right)n = y_0 - y \Rightarrow y = y_0 - \left(\frac{a}{d}\right)n$$

$$\because a(x - x_0) = b(y_0 - y)$$

$$\therefore a(x - x_0) = b\left(\frac{a}{d}\right)n \Rightarrow x = x_0 + \left(\frac{b}{d}\right)n$$



Ex: Find solutions for $15x + 6y = 7$

$$\because (15, 6) = 3 \text{ and } 3 \nmid 7$$

\Rightarrow no solutions.

Ex: Find solutions for $21x + 14y = 70$

$$\because (21, 14) = 7 \text{ and } 7 \mid 70$$

\Rightarrow infinitely many solutions.

By Euclidean Algorithm, we can find

$$1 \times 21 + (-1) \times 14 = 7$$

$$\therefore 10 \times 21 + (-10) \times 14 = 70$$

therefore, all solutions are given by

$$x = 10 + 2n, y = -10 - 3n$$



Ex: Find $x, y \in \mathbb{Z}^+$, $20x + 50y = 510$, $x, y \geq 0$.

<sol>: Since $(20, 50) = 10$ and $10 | 510$,

\therefore there are solutions.

By Algorithm, we have

$$20(-2) + 50 \times 1 = 10 \Rightarrow 20(-2 \times 51) + 50(1 \times 51) = 510$$

$$\therefore x_0 = -102, y_0 = 51 \Rightarrow x = -102 + 5n \text{ and } y = 51 - 2n$$

$$\text{But } x, y \geq 0 \Rightarrow -102 + 5n \geq 0 \text{ and } 51 - 2n \geq 0$$

$$\Rightarrow n \geq 20 \frac{2}{5} \text{ and } n \leq 25 \frac{1}{2}$$

$$\therefore n = 21, 22, 23, 24 \text{ or } 25.$$

$$\therefore (x, y) = (3, 9), (8, 7), (13, 5), (18, 3) \text{ or } (23, 1).$$



Thm: If $a_1, a_2, \dots, a_n \in \mathbb{Z}^+$, then
the equation $a_1x_1 + a_2x_2 + \dots + a_nx_n = c$
has **integral solution** iff $d = (a_1, a_2, \dots, a_n) | c$.
Moreover, when there is a solution,
there are **infinitely many different solutions**.

<proof>:

(i) If $\exists x_1, x_2, \dots, x_n \ni a_1x_1 + a_2x_2 + \dots + a_nx_n = c$
 $\therefore d | a_i, \forall 1 \leq i \leq n, \Rightarrow d | c$.

Hence, if $d \nmid c, \Rightarrow$ no solution.

(ii) By **induction**, it is true for $n = 2$,

($\because a_1x_1 + a_2x_2 = c$ has ∞ solutions if $d | c$)



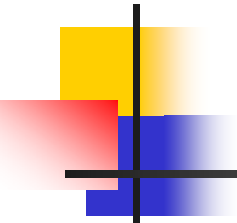
Assume there are ∞ solutions for n , we want to prove that $a_1x_1 + \dots + a_nx_n + a_{n+1}x_{n+1} = c$ has ∞ solutions if $d|c$.

Since $a_nx_n + a_{n+1}x_{n+1} = (a_n, a_{n+1})y$, $y \in \mathbb{Z}$.

$$\Rightarrow a_1x_1 + \dots + a_{n-1}x_{n-1} + (a_n, a_{n+1})y = c$$

$$\because d = (a_1, \dots, a_n, a_{n+1}) = (a_1, a_2, \dots, a_{n-1}, (a_n, a_{n+1}))$$

\therefore If $d|c \Rightarrow a_1x_1 + \dots + a_nx_n + a_{n+1}x_{n+1} = c$ has ∞ solutions.

- 
- Given $a_1, a_2, \dots, a_n \in \mathbb{Z}^+$ and $x_1, x_2, \dots, x_n \in \mathbb{Z}^+$
find $s = a_1x_1 + a_2x_2 + \dots + a_nx_n \rightarrow$ easy
 - Problem:
Given $a_1, a_2, \dots, a_n \in \mathbb{Z}^+$ and s
find $x_1, x_2, \dots, x_n \ni s = a_1x_1 + a_2x_2 + \dots + a_nx_n \rightarrow$ hard
 - Knapsack Problem: $x_1, x_2, \dots, x_n \in \{0, 1\}$.