Computer Science and Information Engineering
National Chi Nan University

Discrete Mathematics

Dr. Justie Su-Tzu Juan

Chap 4 Properties the Integers: Mathematical Induction

§ 4.3 The Division Algorithm: Prime Numbers (2)

Slides for a Course Based on the Text
Discrete & Combinatorial Mathematics **(5th Edition)**
by Ralph P. Grimaldi

§ 4.3 The Division Algorithm: Prime Numbers

Ex 4.26 : ∵乘法為“連加”，故考慮以“連減”來計算除法.
See Fig 4.10, 連減並用 Ex 4.25 (d)

Ex 4.27 : 利用上述 Algorithm 計算“改進位制”：
Write 6137 in the octal system (base 8)
i.e. find $r_0, r_1, r_2, \ldots, r_k$ with $r_k > 0$ s.t. $(r_k \ldots r_1 r_0)_8 = 6137$

Sol. ∵ $6137 = r_0 + r_1 \cdot 8 + r_2 \cdot 8^2 + \ldots + r_k \cdot 8^k = r_0 + 8(r_1 + 8(r_2 + \ldots + 8(r_k)\ldots))$

and $6137 = 1 + 8 \cdot 767 \Rightarrow r_0 = 1$

$= 1 + 8[7 + 8(95)] \Rightarrow r_1 = 7$

$= 1 + 8[7 + 8(7 + 8 \cdot 11)] \Rightarrow r_2 = 7$

$= 1 + 8\{7 + 8[7 + 8(3 + 8 \cdot 1)]\} \Rightarrow r_3 = 3$

$r_4 = 1$

8 |		Remainders
8	6137	
8	767	$1(r_0)$
8	95	$7(r_1)$
8	11	$7(r_2)$
8	1	$3(r_3)$
	0	$1(r_4)$

i.e. $6137 = 1 \cdot 8^4 + 3 \cdot 8^3 + 7 \cdot 8^2 + 7 \cdot 8^1 + 1 = (13771)_8$

§ 4.3 The Division Algorithm: Prime Numbers

Ex 4.28 : (1/3)

① 2位進: see book, Table 4.3

four bits: $0 \sim 15 = 0 \sim 2^4 - 1$

leading 1: $8 \sim 15 = 2^3 \sim 2^4 - 1$

six bits: $0 \sim 63 = 0 \sim 2^6 - 1$

n bits: $0 \sim 2^n - 1$

$$\begin{cases} \text{leading 0: } 0 \sim 2^{n-1} - 1 \\ \text{leading 1: } 2^{n-1} \sim 2^n - 1 \end{cases}$$

② eight bits = one bytes

one bytes: $0 \sim 2^8 - 1 = 0 \sim 255$

two bytes: $0 \sim 2^{16} - 1 = 0 \sim 65535$

four bytes: $0 \sim 2^{32} - 1 = 0 \sim 4294967295$

§ 4.3 The Division Algorithm: Prime Numbers

Ex 4.28 : (2/3) (base - 16)

③ Table 4.4:

Base 10	Base2	Base 16
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Represent the integer 13874945 in the hexadecimal system:

		Remainders	
16	13874945		
16	867184	1	(r_0)
16	54199	0	(r_1)
16	3387	7	(r_2)
16	211	11=B	(r_3)
16	13	3	(r_4)
	0	13=D	(r_5)

$\therefore\ 13874945 = (D3B701)_{16}$

§ 4.3 The Division Algorithm: Prime Numbers

Ex 4.28 : (3/3)

④ **Converting between base 2 and base 16.**

(i) Convert the binary integer 01001101 to its base-16 counterpart

$$\underbrace{0100}_{4}\underbrace{1101}_{D} \qquad \therefore (01001101)_2=(4D)_{16}$$

(ii) Convert the two-byte number $(A13F)_{16}$ in base 2

$$\overbrace{1010}^{A}\ \overbrace{0001}^{1}\ \overbrace{0011}^{3}\ \overbrace{1111}^{F}$$

$$\therefore (A13F)_{16}=(1010000100111111)_2$$

Ex 4.29 :

負數如何表示： $n < 0$: two's complement method.

① First consider the binary representation of $|n|$,

② Replace each 0 by 1, 1 by 0; the result is called the one's complement of $|n|$.

③ Add 1 to ②; the result is called the two's complement of $|n|$.

ex: – 6: ① 6 → 0110

② 0110 ↔ 1001

③ 1001 + 0001 = 1010

Note: ① See Table 4.5 (p. 225): 7 ~ – 8 need four-bit patterns

② Other obtained: $-8 \leq n \leq -1 \leftrightarrow 7 \geq n^c \geq 0$

③ nonnegative integer start with 0, negative integer start with 1 (first bit).

§ 4.3 The Division Algorithm: Prime Numbers

<u>Ex 4.30</u> : (1/2)

① Perform 33 – 15 in base 2, using the two's complement of 8 bits.

Sol.

$\because$ $33 - 15 = 33 + (-15)$;

$33 = (00100001)_2$

$15 = (00001111)_2$

$\rightarrow -15 = (11110000+00000001)_2 = (11110001)_2$

$$\begin{array}{r} 33 \\ -\ 15 \\ \hline \end{array} \longrightarrow \begin{array}{r} 00100001 \\ +\ \ 11110001 \\ \hline 1\underbrace{00010010} \end{array}$$

discarded

nonnegative

Answer = $(00010010)_2 = 18$

§ 4.3 The Division Algorithm: Prime Numbers

Ex 4.30 : (2/2)

② 15 – 33=? 15+(– 33)

$15 = (00001111)_2$

$33 = (00100001)_2$

$\rightarrow -33 = (11011110+00000001)_2 = (11011111)_2$

$$\begin{array}{r} 15 \\ -\ 33 \\ \hline \end{array} \longrightarrow \begin{array}{r} 00001111 \\ +\ 11011111 \\ \hline 11101110 \end{array}$$

negative

① Take the one's complement

$11101110 \rightarrow (00010001)_2$

$\rightarrow (00010010)_2 = 18$

② Add 1

∴ Answer = – 18

③ [overflow error] ex: 117+88

$$\begin{array}{r} 117 \\ +\ 88 \\ \hline \end{array} \longrightarrow \begin{array}{r} 01110101 \\ +\ 01011000 \\ \hline 11001101 \end{array}$$

Negative!! →←

§ 4.3 The Division Algorithm: Prime Numbers

<u>Remark</u> : In general, let $x, y \in Z^+$ with $x > y$, $2^{n-2} \leq x < 2^{n-1}$

Then the binary rep. for x is made up of $n - 1$ bits $\rightarrow$ n bits

The one's complement of $y = (2^n - 1) - y = \underbrace{11\ldots1}_{n個1} - y$

The two's complement of $y = (2^n - 1) - y + 1$

$\therefore\ x - y = x + [(2^n - 1) - y + 1] - 2^n$

removal of the extra bit

§ 4.3 The Division Algorithm: Prime Numbers

Ex 4.31 : If $n \in \mathbb{Z}^+$ and n is composite, then $\exists\, p$: a prime s.t. $p \mid n$ and $p \le \sqrt{n}$.

Proof.

① $\because$ n is composite

$\therefore$ We can write $n = n_1 n_2$, where $1 < n_1 < n$, $1 < n_2 < n$.

If $(n_1 > \sqrt{n}\,)$ and $(n_2 > \sqrt{n}\,)$,

then $n = n_1 n_2 > (\sqrt{n}\,)(\sqrt{n}\,) = n$ $\rightarrow\leftarrow$

$\therefore$ $n_1 \le \sqrt{n}$ or $n_2 \le \sqrt{n}$, W.L.O.G. say $n_1 \le \sqrt{n}$.

(without loss of generality)

② If n_1 is a prime: the result follows.

If n_1 is not a prime: by Lemma 4.1,

$\exists$ a prime $p < n_1$ s.t. $p \mid n_1$,

$\because$ $p \mid n_1 \wedge n_1 \mid n$,

$\therefore$ $p \mid n$ and $p \le \sqrt{n}$.

Computer Science and Information Engineering
National Chi Nan University

Discrete Mathematics

Dr. Justie Su-Tzu Juan

Chap 4 Properties the Integers: Mathematical Induction

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

Slides for a Course Based on the Text
Discrete & Combinatorial Mathematics **(5th Edition)**
by Ralph P. Grimaldi

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

Def4.2 : For $a, b \in Z$, $c \in Z^+$ is said to be a *common divisor* of a and $b \equiv c \mid a \wedge c \mid b$.

EX4.32 : The common divisors of 42 and 70 = 1, 2, 7, 14

G.C.D.

Def4.3 : Let $a, b \in Z$, either $a \neq 0$ or $b \neq 0$. $c \in Z^+$ is called a *greatest common divisor* (G. C. D.) of a and $b \equiv$

a) $c \mid a$ and $c \mid b$,

b) $\forall$ common divisor d of a and b, $d \mid c$.

Question : ① A G. C. D. always exist? If so, how to find?

② How many G. C. D. can a pair of integers have?

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

Thm4.6 : $\forall\, a, b \in \mathbb{Z}^+$, $\exists!\, c \in \mathbb{Z}^+$ is the greatest common divisor of a, b. (denoted by $gcd(a, b)$.)

Proof.(1/2)

$\exists$: Let $S = \{as + bt \mid s, t \in \mathbb{Z},\ as + bt > 0\}$.

$\because S \neq \phi$,

$\therefore$ by the Well-Ordering Principle, S has a least element c.

b) $\because c \in S$, $\exists\, x, y \in \mathbb{Z}$ s.t. $c = ax + by$.

$\forall\, d \in \mathbb{Z}$ with $d \mid a$ and $d \mid b$, by Thm4.3(f), $d \mid ax + by$, i.e. $d \mid c$.

a) If $c \nmid a$, then $\exists\, g, r \in \mathbb{Z}^+$ and $0 < r < c$ s.t. $a = gc + r$.

$$\therefore r = a - gc = a - g(ax + by)$$

$$= (1 - gx)\, a + (-gy)\, b.$$

$\therefore r \in S$. $\rightarrow\leftarrow$ ($\because 0 < r < c$). $\therefore c \mid a$.

In the same way, $c \mid b$.

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

Proof.(2/2)

!: If $c_1, c_2 \in \mathbb{Z}^+$ both satisfy Def 4.3 (a), (b),
then c_1, c_2 both are common divisor of a, b.
by (b), $\because$ c_1 as a greatest common divisor, $\therefore$ $c_2 \mid c_1$;
and, $\because$ c_2 as a greatest common divisor, $\therefore$ $c_1 \mid c_2$.
$\Rightarrow$ By Thm4.3(b), $c_1 = c_2$ $\because$ $c_1, c_2 \in \mathbb{Z}^+$.

Note : $\forall\, a, b \in \mathbb{Z}^+$:

① $\gcd(a, b) = \gcd(b, a)$.
② $\gcd(a, 0) = |a|$, if $a \neq 0$.
③ $\gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b) = \gcd(a, b)$.
④ $\gcd(0, 0)$ is not defined.
⑤ $\gcd(a, b)$ is the smallest positive integer we can write a linear combination of a and b.

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

Def : $\forall$ $a, b \in$ Z, a, b are called ***relatively prime*** when gcd(a, b) = 1.
i.e. $\exists\, x, y \in$ Z such that $ax + by = 1$.

EX4.33 : ① gcd(42, 70) = 14 :

$\exists\, x, y \in$ Z such that $42x + 70y = 14$,

$\Leftrightarrow \exists\, x, y \in$ Z such that $3x + 5y = 1$.

let $x_0 = 2$, $y_0 = -1$: $3(2) + 5(-1) = 1$.

but $\forall k \in$ Z : $3(2 - 5k) + 5(-1 + 3k) = 1$,

$\Leftrightarrow \forall k \in$ Z : $42(2 - 5k) + 70(-1 + 3k) = 14$.

$\therefore$ the solution for x, y are not unique!

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

EX4.33 : ② In general, if $\gcd(a, b) = d$:

$$\exists\, x, y \in Z \text{ s.t. } ax + by = d,$$

$$\Leftrightarrow \exists\, x, y \in Z \text{ s.t. } (a/d)x + (b/d)y = 1,$$

$$\Leftrightarrow \gcd(a/d, b/d) = 1.$$

let x_0, y_0 be a solution, i.e. $(a/d)x_0 + (b/d)y_0 = 1$.

then $\forall\, k \in Z : (a/d)(x_0 - (b/d)k) + (b/d)(y_0 + (a/d)k) = 1$,

$\Leftrightarrow \forall\, k \in Z : a(x_0 - (b/d)k) + b(y_0 + (a/d)k) = d$.

$\therefore \exists$ infinitely many solution for $ax + by = d$.

Remark : ① If $a \mid b$, then $\gcd(a, b) = a$.

② If $b \mid a$, then $\gcd(a, b) = b$.

③ Otherwise?

Solution: use *Euclidean Algorithm*.

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

Thm 4.7 : ***Euclidean Algorithm*** :

If $a, b \in \mathbb{Z}^+$, then apply the division algorithm :

$$
\begin{aligned}
a &= q_1 b + r_1, & 0 < r_1 < b. \\
b &= q_2 r_1 + r_2, & 0 < r_2 < r_1. \\
r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2. \\
&\vdots \\
r_{k-2} &= q_k r_{k-1} + r_k, & 0 < r_k < r_{k-1} \\
r_{k-1} &= q_{k+1} r_k.
\end{aligned}
$$

Then r_k, the last nonzero remainder, = gcd (a, b).

Proof.(1/2)

ⓑ $\forall c \in \mathbb{Z}^+$ with $c \mid a$ and $c \mid b$,

$\because a = q_1 b + r_1, \therefore c \mid r_1;$

$\because b = q_1 r_1 + r_2, \therefore c \mid r_2;$

$\vdots$

$\because r_{k-2} = q_k r_{k-1} + r_k, \therefore c \mid r_k.$

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

Proof.(2/2)

ⓐ $\because r_{k-1} = q_{k+1} r_k, \quad \therefore r_k \mid r_{k-1}$

$\because r_{k-2} = q_k r_{k-1} + r_k, \quad \therefore r_k \mid r_{k-2}$

$\vdots$

$\because r_1 = q_3 r_2 + r_3, \quad \therefore r_k \mid r_1;$

$\because b = q_2 r_1 + r_2, \quad \therefore r_k \mid b;$

$\because a = q_1 b + r_1, \quad \therefore r_k \mid a.$

i.e. $(r_k \mid a) \wedge (r_k \mid b)$.

By ⓐ, ⓑ, hence $r_k = \gcd(a, b)$.

Note : ① Algorithm : precise instruction, not just for one special case, input, output, same result, unambiguous manner, cannot go on indefinitely (finite instruction).

② Thm 4.5 : 基於傳統才稱之為 algorithm, ∵ 其不具有 "precise instructions". ∴ 以 EX 4.36 中Fig 4.9 之procedure補足此缺點.

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

EX 4.34 : ① Find the greatest common divisor of 250 and 111.
② Express the result as a linear combination of 250 and 111.
Sol.

① $250 = 2\,(111) + 28, \quad 0 < 28 < 111$
$111 = 3\,(28) + 27, \quad 0 < 27 < 28$
$28 = 1\,(27) + 1, \quad 0 < 1 < 27$
$27 = 27\,(1).$ (the last nonzero remainder is 1)
$\therefore 1 = \gcd(250, 111)$. i.e. 250, 111 are relatively prime.

② $1 = 28 - 1\,(27) \quad = 28 - 1\,[111 - 3\,(28)]$
$= (-1)\,111 + 4\,(28) = (-1)\,111 + 4\,[250 - 2\,(111)]$
$= 4\,(250) - 9\,(111) = 250\,(4) + 111\,(-9),$
$\Rightarrow 1 = 250\,(4 - 111\,k) + 111\,(-9 + 250\,k), \forall k \in Z.$

note: $\gcd(-250, 111) = \gcd(250, -111) = \gcd(-250, -111)$
$= \gcd(250, 111) = 1.$

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

EX 4.35 : $\forall\, n \in \mathbb{Z}^+$, prove $8n + 3$ and $5n + 2$ are relatively prime.

Proof.

① when $n = 1$, $\gcd(8n + 3, 5n + 2) = \gcd(11, 7) = 1$.

when $n \geq 2$, $\because\ 8n + 3 > 5n + 2$:

$$\begin{aligned}
8n + 3 &= 1(5n + 2) + (3n + 1), && 0 < 3n + 1 < 5n + 2\\
5n + 2 &= 1(3n + 1) + (2n + 1), && 0 < 2n + 1 < 3n + 1\\
3n + 1 &= 1(2n + 1) + n, && 0 < n < 2n + 1\\
2n + 1 &= 2(n) + 1, && 0 < 1 < n\\
n &= n(1). && \text{(the last nonzero remainder is 1)}
\end{aligned}$$

$\therefore\ \gcd(8n + 3, 5n + 2) = 1,\ \forall n \geq 1$.

② 另解: $\because\ (8n + 3)(-5) + (5n + 2)8 = -15 + 16 = 1$,

$\therefore$ 1 is expressed as a linear combination of $8n + 3$, $5n + 2$.

and no smaller positive integer can have this property,

$\therefore$ the G. C. D. of $8n + 3$ and $5n + 2$ is 1, $\forall\, n \in \mathbb{Z}^+$.

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

EX 4.36 : Def : $\forall$ *x*, *y* $\in$ Z^+, *x mod y* = the remainder after *x* is divided by *y*. **ex : 7 mod 3 = 1; 18 mod 5 = 3.**

```
procedure gcd (a, b : positive integers)
begin
  r := a mod b
  d := b
  while r > 0 do
    begin
      c := d
      d := r
      r := c mod d
    end
end {gcd(a, b) is d, the last nonzero remainder}
```

Figure 4.9

ex : a = 168, b = 456:

r_0 = 168 and
d_0 = 456.
$\because$ $r > 0$
$\therefore$ c_1 = 456, d_1 = 168,
r_1 = 456 mod 168 = 120 > 0;
c_2 = 168, d_2 = 120,
r_2 = 168 mod 120 = 48 > 0;
c_3 = 120, d_3 = 48,
r_3 = 120 mod 48 = 24 > 0;
c_4 = 48, d_4 = 24,
r_4 = 48 mod 24 = 0.
STOP.
$\therefore$ gcd(a, b) = 24 (= d_4).

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

EX 4.37 : 2 containers : 17 ounces and 55 ounces. How to use this two containers to measure exactly one ounce?

(一盎司= 0.283494 kg　17 → 4.8 kg　55 → 15.6 kg)

Sol.

$$55 = 3\,(17) + 4, \quad 0 < 4 < 17$$

$$17 = 4\,(4) + 1, \quad 0 < 1 < 4$$

$$\Rightarrow 1 = 17 - 4\,(4) = 17 - 4\,[55 - 3\,(17)]$$

$$= 13\,(17) - 4\,(55).$$

∴ 小的裝13次, 逐次倒至大的;

清掉大的4次, 最後會只剩 1 ounce.

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

EX 4.38 : Debug a Pascal program in 6 minutes. Debug a C++ program in 10 minutes. Work 104 minutes and doesn't waste any time. How many programs can he debug in each language?

Sol.

Let $x, y \in N$, $6x + 10y = 104 \Leftrightarrow 3x + 5y = 52$

$\because$ gcd(3, 5) = 1, and $3(2) + 5(-1) = 1$

$\therefore 3(104) + 5(-52) = 52$

$\Rightarrow 3(104 - 5k) + 5(-52 + 3k) = 52, \forall k \in Z$

$x = 104 - 5k \geq 0$ and $y = -52 + 3k \geq 0$

$\Rightarrow 17 + 1/3 = 52/3 \leq k \leq 104/5 = 20 + 4/5$

$\therefore \exists$ 3 possible solution:

a) $(k = 18) : x = 14, y = 2.$

b) $(k = 19) : x = 9, y = 5.$

c) $(k = 20) : x = 4, y = 8.$

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

Thm 4.8 : If $a, b, c \in Z^+$, the ***Diophantine equation*** $ax + by = c$ has an integer solution $x = x_0, y = y_0 \Leftrightarrow \gcd(a, b) \mid c$.

Def 4.4 : $\forall\ a, b, c \in Z^+$,

① c is called a ***common multiple*** of $a, b \equiv a \mid c$ and $b \mid c$.

② c is the ***least common multiple*** of a, b $\text{lcm}(a, b) \equiv$ the smallest of all common multiple of a, b.

EX 4.39 : a) $12 = 3 \cdot 4$, $\therefore$ $\text{lcm}(3, 4) = 12 = \text{lcm}(4, 3)$.

$90 = 6 \cdot 15$, but $\text{lcm}(6, 15) \neq 90$, $\text{lcm}(6, 15) = 30$.

b) $\forall\ n \in Z^+$, $\text{lcm}(1, n) = \text{lcm}(n, 1) = n$.

c) $\forall\ a, n \in Z^+$, $\text{lcm}(a, na) = na$.

d) $\forall\ a, m, n \in Z^+$, with $m \leq n$, $\text{lcm}(a^m, a^n) = a^n$, $\gcd(a^m, a^n) = a^m$.

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

Thm 4.9 : Let $a, b, c \in Z^+$, with $c = \text{lcm}(a, b)$.
If d is a common multiple of a and b, then $c \mid d$.

Proof.

If not, then by division algorithm, $d = qc + r$, where $0 < r < c$.

$\because$ $c = \text{lcm}(a, b)$, $\therefore$ $\exists\, m \in Z^+$ s.t. $c = ma$,

$\because$ d is a common multiple of a and b, $\therefore$ $\exists\, n \in Z^+$ s.t. $d = na$.

$\Rightarrow na = d = qc + r = qma + r$

$\Rightarrow (n - qm)\, a = r > 0$

$\therefore$ $a \mid r$.

In a similar way, $b \mid r$.

$\therefore$ $(a \mid r$ and $b \mid r) \Rightarrow r$ is a common multiple of a and b.

but $0 < r < c$ $\rightarrow\leftarrow$ ($\because$ c is the least common multiple of a, b)

Hence $c \mid d$.

§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

Thm 4.10 : $\forall\, a, b \in \mathbb{Z}^+$, $ab = \text{lcm}(a, b) \cdot \gcd(a, b)$

Proof. **(reader)**

EX 4.40 : a) $\forall\, a, b \in \mathbb{Z}^+$, of a, b are relatively prime, then

$\text{lcm}(a, b) = ab.$

b) $\because \gcd(168, 456) = 24$ (by EX 4.36)

$\therefore \text{lcm}(168, 456) = (168)\,(456) / 24 = 3192.$

Computer Science and Information Engineering
National Chi Nan University

Discrete Mathematics

Dr. Justie Su-Tzu Juan

Chap 4 Properties the Integers: Mathematical Induction

§ 4.5 The Fundamental Theorem of Arithmetic

Slides for a Course Based on the Text
Discrete & Combinatorial Mathematics **(5^{th} Edition)**
by Ralph P. Grimaldi

§ 4.5 The Fundamental Theorem of Arithmetic

Lemma 4.2 : If $a, b \in \mathbb{Z}^+$ and p is a prime, $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Proof.

If $p \mid a$, then we are finished.

If $p \nmid a$: $\because$ p is prime,

$\therefore$ $\gcd(p, a) = 1$. i.e. $\exists\, x, y \in \mathbb{Z}$ s.t. $px + ay = 1$.

Then for $p(bx) + (ab)y = b$:

$\because$ $p \mid p \wedge p \mid ab$,

$\therefore$ $p \mid p(bx) \wedge p \mid (ab)y$. (by Thm 4.3(d))

$\because$ $[\, p(bx) + (ab)y = b \,] \wedge p \mid p(bx) \wedge p \mid (ab)y$,

$\therefore$ $p \mid b$. (by Thm 4.3(e))

Lemma 4.3 : Let $a_i \in \mathbb{Z}^+$, $\forall\, i \in \{1, 2, \ldots, n\}$.

$[(p \text{ is prime}) \wedge (p \mid a_1 a_2 \ldots a_n)] \Rightarrow \exists\, i \in \{1, 2, \ldots, n\}, p \mid a_i$.

Proof. (reader)

§ 4.5 The Fundamental Theorem of Arithmetic

EX 4.38 : **Show that $\sqrt{2}$ is irrational.** (Aristotle (384 – 322 B. C.))

Proof.

Suppose $\sqrt{2}$ is not irrational. say $\sqrt{2} = \frac{a}{b}$, where $a, b \in Z^+$, gcd $(a, b) = 1$.

$\because \sqrt{2} = \frac{a}{b}$, $\therefore 2 = \frac{a^2}{b^2} \Rightarrow 2\, b^2 = a^2 \Rightarrow 2 \mid a^2 \Rightarrow 2 \mid a$ (by Lemma 4.2)

Let $a = 2\, c$ for some $c \in Z^+$.

$\because 2\, b^2 = a^2$, $\therefore 2\, b^2 = 4\, c^2 \Rightarrow 2\, c^2 = b^2 \Rightarrow 2 \mid b^2 \Rightarrow 2 \mid b$ (by Lemma 4.2)

$\therefore 2 \mid a \wedge 2 \mid b \Rightarrow 2 \mid \gcd(a, b)$, i.e. $\gcd(a, b) \geq 2 \rightarrow\leftarrow$

$\therefore \sqrt{2}$ is irrational.

Note : $\sqrt{p}$ **is irrational for every prime** p (exercise)

Thm 4.11 : ***The Fundamental Theorem of Arithmetic***

$\forall\, n > 1$, $n \in Z^+$, n **can be written as a product of primes uniquely, up to the order of the primes.**

$\forall n > 1$, $n \in Z^+$, n can be written as a product of primes uniquely, up to the order of the primes.

Proof. (1/3)

$\exists$: If not exist such product :

Let $m > 1$ be the smallest integer not expressible as a product of primes.

$\because$ m is not a prime, (o.w. prime is a product of one factor $\rightarrow\leftarrow$)

$\therefore$ Let $m = m_1 m_2$, where $1 < m_1 \leq m_2 < m$.

$\because$ $m_1 < m$, $m_2 < m$,

$\therefore$ m_1, m_2 can be written as product of primes.

$\because$ $m = m_1 m_2$

$\therefore$ we can obtain a prime factorization of m. $\rightarrow\leftarrow$

$\forall n > 1$, $n \in$ Z+, n can be written as a product of primes uniquely, up to the order of the primes.

§ 4.5 The Fundamental Theorem of Arithmetic

Proof. (2/3)

! : Prove by induction on n :

Let $S(n)$: n have a unique prime factorization

$n = 2$: $S(2)$ is true.

Suppose $n = 2, 3, 4, \ldots, h - 1$, $S(n)$ is true.

Now, consider $n = h$:

Suppose $h = p_1^{s(1)} p_2^{s(2)} \ldots p_k^{s(k)} = q_1^{t(1)} q_2^{t(2)} \ldots q_r^{t(r)}$.

Where p_i, q_j are primes, $\forall\ 1 \le i \le k$, $1 \le j \le r$.

and $p_1 < p_2 < \ldots < p_k$ and $q_1 < q_2 < \ldots < q_r$.

and $s(i) \in Z^+$, $t(j) \in Z^+$, $\forall\ 1 \le i \le k$, $1 \le j \le r$.

$\forall n > 1, n \in Z^+$, **n can be written as a product of primes uniquely, up to the order of the primes.**

§ 4.5 The Fundamental Theorem of Arithmetic

Proof. (3/3)

$\because p_1 \mid h, \therefore p_1 \mid q_1^{t(1)} q_2^{t(2)} \ldots q_r^{t(r)}$.

By Lemma 4.3, $\exists\, 1 \le j \le r, p_1 \mid q_j$.

$\because p_1, q_j$ are primes. $\therefore p_1 = q_j$.

In the same way, $\because q_1 \mid h \Rightarrow \exists\, 1 \le e \le k, q_1 = p_e$.

$\Rightarrow p_1 \le p_e = q_1 \le q_j = p_1, \therefore e = j = 1$, i.e. $p_1 = q_1$.

Let $n_1 = h / p_1 = p_1^{s(1)-1} p_2^{s(2)} \ldots p_k^{s(k)} = q_1^{t(1)-1} q_2^{t(2)} \ldots q_r^{t(r)}$.

$\because n_1 < h, \therefore$ by I. H.:

$k = r, p_i = q_i \;\forall\, 1 \le i \le k$,

$s(1) - 1 = t(1) - 1$, and $s(i) = t(i) \;\forall\, 2 \le i \le k = r$.

$\because s(1) - 1 = t(1) - 1 \Rightarrow s(1) = t(1)$.

$\Rightarrow$ The prime factorization of h is unique.

EX 4.39 : **Find the prime factorization of 980220.**

Sol.

$$
\begin{array}{r|r}
2 & 980220 \\ \hline
2 & 490110 \\ \hline
3 & 245055 \\ \hline
5 & 81685 \\ \hline
17 & 16337 \\ \hline
31 & 961 \\ \hline
 & 31
\end{array}
\qquad
\begin{array}{l}
= 2^1\,(490110) \\
= 2^2\,(245055) \\
= 2^2 \cdot 3^1\,(81685) \\
= 2^2 \cdot 3^1 \cdot 5^1\,(16337) \\
= 2^2 \cdot 3^1 \cdot 5^1 \cdot 17^1\,(961) \\
= 2^2 \cdot 3^1 \cdot 5^1 \cdot 17^1 \cdot 31^2
\end{array}
$$

EX 4.40 : Suppose $n \in Z^+$ and

$10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot n = 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14$,

$17 \mid n$ or not?

Sol.

$\because 17 \mid (21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14)$,

$\therefore 17 \mid (10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot n)$.

But $17 \nmid 10$, $17 \nmid 9$, $17 \nmid 8$, $17 \nmid 7$, $17 \nmid 6$, $17 \nmid 5$,

$17 \nmid 4$, $17 \nmid 3$, $17 \nmid 2$,

$\therefore$ By Lemma 4.3, $17 \mid n$.

§ 4.5 The Fundamental Theorem of Arithmetic

EX 4.41 : For $n \in \mathbf{Z}^+$, Find the number of positive divisors of n.

ex : 2 : 1, 2 ↝ 2

3 : 1, 3 ↝ 2

4 : 1, 2, 4 ↝ 3

Sol.

$\forall\, n \in \mathbf{Z}^+$, by Thm4.11, let $n = p_1^{e(1)} p_2^{e(2)} \ldots p_k^{e(k)}$,

where p_i is prime $\forall\, 1 \le i \le k$, $e(i) > 0\ \forall\, 1 \le i \le k$.

If $m \mid n$, then $m = p_1^{f(1)} p_2^{f(2)} \ldots p_k^{f(k)}$

where $0 \le f(i) \le e(i)$. $\forall\, 1 \le i \le k$.

$\therefore$ the number of positive divisors of n is

$$(e(1) + 1)\,(e(2) + 1) \ldots (e(k) + 1).$$

§ 4.5 The Fundamental Theorem of Arithmetic

<u>ex</u> : ① 29338848000 $= 2^8\, 3^5\, 5^3\, 7^3\, 11$:

有 $(8 + 1)\,(5 + 1)\,(3 + 1)\,(3 + 1)\,(1 + 1) = 9 \cdot 6 \cdot 4 \cdot 4 \cdot 2$

$= 1728$ 個 positive divisors.

② 其中有多少個為 $360 = 2^3 \cdot 3^2 \cdot 5$ 的倍數:

it must satisfy : $2^{t(1)}\, 3^{t(2)}\, 5^{t(3)}\, 7^{t(4)}\, 11^{t(5)}$ where

$3 \le t(1) \le 8,\ 2 \le t(2) \le 5,\ 1 \le t(3) \le 3,\ 0 \le t(4) \le 3,\ 0 \le t(5) \le 1$

$\Rightarrow [(8 - 3) + 1][(5 - 2) + 1][(3 - 1) + 1][(3 - 0) + 1][(1 - 0) + 1]$

$= 6 \cdot 4 \cdot 3 \cdot 4 \cdot 2 = 576.$

③其中有多少個為 perfect square :

it mast satisfy : $2^{s(1)}\, 3^{s(2)}\, 5^{s(3)}\, 7^{s(4)}\, 11^{s(5)}$ where

$s(1) = 0, 2, 4, 6, 8;\ s(2) = 0, 2, 4;\ s(3) = 0, 2;\ s(4) = 0, 2;\ s(5) = 0.$

i.e. $(2^2)^{r(1)}\, (3^2)^{r(2)}\, (5^2)^{r(3)}\, (7^2)^{r(4)}$ where

$0 \le r(1) \le 4,\ 0 \le r(2) \le 2,\ 0 \le r(3) \le 1,\ 0 \le r(4) \le 1,$

$\Rightarrow 5 \cdot 3 \cdot 2 \cdot 2 \cdot 1 = 60.$

§ 4.5 The Fundamental Theorem of Arithmetic

Def :($\prod_{i=m}^{n}$) = $\prod_{i=m}^{n} x_i = \underbrace{x_m \cdot x_{m+1} \cdot \ldots \cdot x_n}_{n-m+1 \text{ terms.}}$ where $m, n \in \mathbb{Z}$.

i : *index*, m : *lower limit*, n : *upper limit*.

ex : ① $\prod_{i=3}^{7} x_i = x_3 \cdot x_4 \cdot x_5 \cdot x_6 \cdot x_7 = \prod_{j=3}^{7} x_j$

② $\prod_{i=3}^{6} i = 3 \cdot 4 \cdot 5 \cdot 6 = 6! / 2!$

③ $\prod_{i=m}^{n} i = m\,(m+1)\,(m+2)\ldots(n-1)\,n = \dfrac{n!}{(m-1)!}$

$\forall\, m, n \in \mathbb{Z}^+$ with $m \le n$.

④ $\prod_{i=7}^{11} x_i = x_7 \cdot x_8 \cdot x_9 \cdot x_{10} \cdot x_{11}$

$= \prod_{j=0}^{4} x_{7+j} = \prod_{j=0}^{4} x_{11-j}$

§ 4.5 The Fundamental Theorem of Arithmetic

EX 4.42 : $m, n \in Z^+$, let $m = p_1^{e(1)} p_2^{e(2)} \ldots p_t^{e(t)}$, $n = p_1^{f(1)} p_2^{f(2)} \ldots p_t^{f(t)}$, where p_i is prime, $e(i) \geq 0$, $f(i) \geq 0$, $\forall\ 1 \leq i \leq t$.
Let $a_i = a(i) =$ **min**$\{e(i), f(i)\} \equiv$ the smaller of $e(i)$ and $f(i)$, $\forall 1 \leq i \leq t$
$b_i = b(i) =$ **max**$\{e(i), f(i)\} \equiv$ the larger of $e(i)$ and $f(i)$, $\forall 1 \leq i \leq t$
then ① $\gcd(m, n) = \prod_{i=1}^{t} p_i^{a(i)}$, ② $\operatorname{lcm}(m, n) = \prod_{i=1}^{t} p_i^{b(i)}$

ex : $m = 491891400 = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11^1 \cdot 13^2$
$n = 1138845708 = 2^2 \cdot 3^2 \cdot 7^1 \cdot 11^2 \cdot 13^3 \cdot 17^1$
$\rightarrow p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, p_6 = 13, p_7 = 17.$
$\rightarrow a_1 = 2, a_2 = 2, a_3 = 0, a_4 = 1, a_5 = 1, a_6 = 2, a_7 = 0$
$\therefore \gcd(m, n) = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^1 \cdot 13^2 \cdot 17^0 = 468468.$
$\rightarrow b_1 = 3, b_2 = 3, b_3 = 2, b_4 = 2, b_5 = 2, b_6 = 3, b_7 = 1$
$\therefore \operatorname{lcm}(m, n) = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^3 \cdot 17^1$
$= 1195787993400.$

§ 4.5 The Fundamental Theorem of Arithmetic

Note : Any two consecutive integers are relatively prime.
(HW 19. § 4.4)

EX 4.39 : Can we find three consecutive positive integers whose product is a perfect square?

(i.e. $\exists\, m, n \in Z^+$. s.t. $m(m+1)(m+2) = n^2$?)

Sol. (1/2)

Suppose $\exists\, m, n \in Z^+$, s.t. $m(m+1)(m+2) = n^2$.

1. $\because$ $\gcd(m, m+1) = 1 = \gcd(m+1, m+2)$,
   $\therefore$ $\forall$ prime p_i, $p_i \mid (m+1) \Rightarrow p_i \nmid m$ and $p_i \nmid (m+2)$.
   $\because$ $m(m+1)(m+2) = n^2$, $\therefore$ $p_i \mid (m+1) \Rightarrow p_i \mid n^2$.
   $\because$ n^2 is a perfect square,
   $\therefore$ the exponents t_i of p_i in the prime factorizations of n^2 must be even.

§ 4.5 The Fundamental Theorem of Arithmetic

EX 4.39 : Can we find three consecutive positive integers whose product is a perfect square?

(i.e. $\exists\, m, n \in \mathbb{Z}^+$. s.t. $m(m+1)(m+2) = n^2$?)

Sol. (2/2)

$\therefore$ **the exponents t_i of p_i in the prime factorizations of n^2 must be even.**

$\therefore$ **$m + 1$ is a perfect square.**

2. $\because$ **$n^2 = m(m+1)(m+2)$ and n^2, $m + 1$ are perfect square,**

$\Rightarrow$ **$m(m+2)$ is a perfect square.**

but $m^2 < m^2 + 2m = m(m+2) < m^2 + 2m + 1 = (m+1)^2$

$\therefore$ **$m(m+2)$ cannot be a perfect square.** $\rightarrow\leftarrow$

$\therefore$ **There are no three consecutive positive integer whose product is a perfect square.**