Computer Science and Information Engineering
National Chi Nan University

Discrete Mathematics

Dr. Justie Su-Tzu Juan

Chap 4 Properties the Integers: Mathematical Induction

§ 4.2 Recursive Definitions (2)

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

§ 4.2 Recursive Definitions

EX4.17 : [$\cup$]

Consider $A_1, A_2, \ldots, A_{n+1}$, where $A_i \subseteq \mathcal{U}\ \forall\ 1 \le i \le n + 1$, we define their union recursively:

1) The union of A_1, A_2 is $A_1 \cup A_2$.

2) The union of $A_1, A_2, \ldots A_n, A_{n+1}$, for $n \ge 2$ is

$$A_1 \cup A_2 \cup \ldots \cup A_n \cup A_{n+1} = (A_1 \cup A_2 \cup \ldots \cup A_n) \cup A_{n+1}.$$

ex : "Generalized Associative Law for $\cup$":

If $n, r \in Z^+$, with $n \ge 3$ and $1 \le r < n$, then

$$S(n) = (A_1 \cup A_2 \cup \ldots \cup A_r) \cup (A_{r+1} \cup \ldots \cup A_n)$$
$$= A_1 \cup \ldots \cup A_r \cup A_{r+1} \cup \ldots \cup A_n.$$

Where $A_i \subseteq \mathcal{U}$ for all $1 \le i \le n$.

§ 4.2 Recursive Definitions

Proof.

① S(3) is true from the associative law of $\cup$.

② Assuming the truth of $S(k)$ for some $k \in \mathbb{Z}^+$, where $k \geq 3$ and $1 \leq r < k$.

Now consider $n = k + 1$:

case 1. $r = k$:

$$(A_1 \cup A_2 \cup \ldots \cup A_k) \cup A_{k+1} = A_1 \cup A_2 \cup \ldots \cup A_k \cup A_{k+1}$$

∵ The given recursive definition.

case 2. $1 \leq r < k$:

$$(A_1 \cup A_2 \cup \ldots \cup A_r) \cup (A_{r+1} \cup \ldots \cup A_k \cup A_{k+1})$$
$$= (A_1 \cup A_2 \cup \ldots \cup A_r) \cup [(A_{r+1} \cup \ldots \cup A_k) \cup A_{k+1}]$$
$$= [(A_1 \cup \ldots \cup A_r) \cup (A_{r+1} \cup \ldots \cup A_k)] \cup A_{k+1}$$
$$\text{(by } I.\ H.\text{)} = (A_1 \cup \ldots \cup A_r \cup A_{r+1} \cup \ldots \cup A_k) \cup A_{k+1}$$
$$= A_1 \cup \ldots \cup A_r \cup A_{r+1} \cup \ldots \cup A_k \cup A_{k+1}$$

∴ By the Principle of Mathematical Induction, $S(n)$ is true for all integer $n \geq 3$.

§ 4.2 Recursive Definitions

Note : [∩] Consider $A_1, A_2, \ldots, A_{n+1}$, where

$$A_i \subseteq \mathcal{U} \ \forall\, 1 \le i \le n + 1,$$

we define their intersection recursively:

1) The intersection of A_1, A_2 is $A_1 \cap A_2$.

2) For $n \ge 2$, the intersection of $A_1, A_2, \ldots, A_n, A_{n+1}$ is

$$A_1 \cap A_2 \cap \ldots \cap A_n \cap A_{n+1}$$
$$= (A_1 \cap A_2 \cap \ldots \cap A_n) \cap A_{n+1}.$$

§ 4.2 Recursive Definitions

<u>EX4.18</u> : Let $n \in \mathbf{Z}^+$ Where $n \geq 2$, and let $A_1, A_2, \ldots, A_n, \subseteq \mathcal{U}$

then $\overline{A_1 \cap A_2 \cap \ldots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \ldots \cup \overline{A_n}$

Proof.

Let $S(n) = \overline{A_1 \cap A_2 \cap \ldots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \ldots \cup \overline{A_n}$, $n \in \mathbf{Z}^+$.

① $n = 2$, $\overline{A_1 \cap A_2} = \overline{A_1} \cup \overline{A_2}$, ∵ the second of DeMorgan's Laws.

② Assume for some $n = k$, where $k \geq 2$:

$$\overline{A_1 \cap A_2 \cap \ldots \cap A_k} = \overline{A_1} \cup \overline{A_2} \cup \ldots \cup \overline{A_k}$$

Now consider $n = k + 1$ (≥ 3):

$$\overline{A_1 \cap A_2 \cap \ldots \cap A_k \cap A_{k+1}} = \overline{(A_1 \cap A_2 \cap \ldots \cap A_k) \cap A_{k+1}}$$

$$= \overline{(A_1 \cap A_2 \cap \ldots \cap A_k)} \cup \overline{A_{k+1}} = (\overline{A_1} \cup \overline{A_2} \cup \ldots \cup \overline{A_k}) \cup \overline{A_{k+1}}$$

$$= \overline{A_1} \cup \overline{A_2} \cup \ldots \cup \overline{A_k} \cup \overline{A_{k+1}} \qquad \text{(by } \mathit{I.\ H.}\text{)}$$

∴ By the Principle of Mathematical Induction,

The generalized DeMorgan Law for $n \geq 2$ obtained.

§ 4.2 Recursive Definitions

Remark : +, · can also be defined in this way. In fact, **EX4.1**, **EX4.3** already used.

ex : ① Define the sequence of harmonic numbers H_1, H_2, …, by

1) $H_1 = 1$; and

2) $\forall\, n \geq 1,\ H_{n+1} = H_n + \left(\frac{1}{n+1}\right)$

② Define $n!$ by

1) $0! = 1$; and

2) $\forall\, n \geq 0,\ (n + 1)! = (n + 1) \cdot n!$

③ The sequence $b_n = 2n$, $n \in$ N can be defined recursively by

1) $b_0 = 0$; and

2) $\forall\, n \geq 0,\ b_{n+1} = b_n + 2$

§ 4.2 Recursive Definitions

EX4.19 : ***The Fibonacci numbers*** **may be defined recursively by**

1) $F_0 = 0, F_1 = 1$**; and**

2) $F_n = F_{n-1} + F_{n-2}$**, for** $n \in \mathbb{Z}^+$ **with** $n \geq 2$**.**

$$F_2 = F_1 + F_0 = 1 + 0 = 1$$
$$F_3 = F_2 + F_1 = 1 + 1 = 2$$
$$F_4 = F_3 + F_2 = 2 + 1 = 3$$
$$F_5 = F_4 + F_3 = 3 + 2 = 5$$

Observation:

$$F_0^2 + F_1^2 + F_2^2 + F_3^2 + F_4^2$$
$$= 0^2 + 1^2 + 1^2 + 2^2 + 3^2 = 15 = 3 \cdot 5$$

$$F_0^2 + F_1^2 + F_2^2 + F_3^2 + F_4^2 + F_5^2$$
$$= 0^2 + 1^2 + 1^2 + 2^2 + 3^2 + 5^2 = 40 = 5 \cdot 8$$

§ 4.2 Recursive Definitions

ex : $\forall\, n \in \mathbf{Z}^+, \Sigma_{i=0,\, n} F_i^{\,2} = F_n \cdot F_{n+1}$

Proof.

① For $n = 1, \Sigma_{i=0,\,1} F_i^{\,2} = F_0^{\,2} + F_1^{\,2} = 0^2 + 1^2 = 1 = 1 \cdot 1 = F_1 \cdot F_2$

The conjecture is true.

② Assume $n = k, \Sigma_{i=0,\,k} F_i^{\,2} = F_k \cdot F_{k+1}$.

Now, consider $n = k + 1$ (≥ 2):

$$\Sigma_{i=0,\,k+1} F_i^{\,2} = \Sigma_{i=0,\,k} F_i^{\,2} + F_{k+1}^{\,2} = (F_k \cdot F_{k+1}) + F_{k+1}^{\,2} \text{ (by } I.\ H.\text{)}$$

$$= F_{k+1} \cdot (F_k + F_{k+1}) = F_{k+1} \cdot F_{k+2}$$

$\therefore$ The truth of the case for $n = k + 1$ follows from the case for $n = k$.

By the Principle of Mathematical Induction, the given conjecture is true for all $n \in \mathbf{Z}^+$.

§ 4.2 Recursive Definitions

EX4.20 : ***Lucas numbers***: **defined recursively by**

1) $L_0 = 2, L_1 = 1$; and

2) $L_n = L_{n-1} + L_{n-2}$, for $n \in \mathbb{Z}^+$ with $n \geq 2$.

2, 1, 3, 4, 7, 11, 18, 29, …

ex : $\forall\, n \in \mathbb{Z}^+, L_n = F_{n-1} + F_{n+1}$

Proof.(1/2)

① when $n = 1$ and $n = 2$:

$L_1 = 1 = 0 + 1 = F_0 + F_2 = F_{1-1} + F_{1+1}$, and

$L_2 = 3 = 1 + 2 = F_1 + F_3 = F_{2-1} + F_{2+1}$,

$\therefore$ The result is true for $n = 1$ and $n = 2$.

§ 4.2 Recursive Definitions

Proof.(2/2)

② **Assume** $L_n = F_{n-1} + F_{n+1}$

$\forall\, n = 1, 2, \ldots , k-1, k$, **where** $k \geq 2$

and then consider L_{k+1} **:**

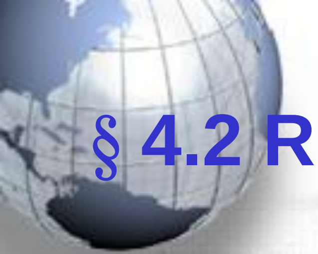
$$L_{k+1} = L_k + L_{k\text{-}1} = (F_{k-1} + F_{k+1}) + (F_{k-2} + F_k) \text{ (by } I.\ H.\text{)}$$

$$= (F_{k-1} + F_{k-2}) + (F_{k+1} + F_k)$$

$$= F_k + F_{k+2} = F_{(k+1)-1} + F_{(k+1)+1}$$

∴ **By the Principle of Strong Mathematical Induction,**

$L_n = F_{n-1} + F_{n+1}\ \forall\, n \in Z^+.$



§ 4.2 Recursive Definitions

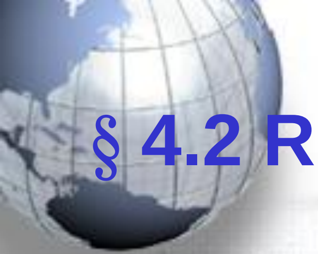
EX4.21 : ① **Define the binomial coefficients recursively by :**

$$\begin{cases} ({}_0^{0}) = 1;\ ({}_r^{n}) = 0, & \text{if } r < 0 \text{ or } r > n; \\ ({}_r^{n+1}) = ({}_r^{n}) + ({}_{r-1}^{n}), & \text{if } n \ge r \ge 0 \end{cases}$$

② **For $m \in Z^+$, $k \in N$, the *Eulerian number $a_{m,k}$* are defined recursively by**

$$\begin{cases} a_{0,0} = 1;\ a_{m,\,k} = 0, \text{ if } k < 0 \text{ or } k \ge m; \\ a_{m,k} = (m - k)a_{m-1,\,k-1} + (k + 1)a_{m-1,\,k}, \text{ if } 0 \le k \le m - 1. \end{cases}$$

						Row Sum
$(m = 1)$	$a_{1,0}$ 1					1 = 1!
$(m = 2)$	$a_{2,0}$ 1	$a_{2,1}$ 1				2 = 2!
$(m = 3)$	$a_{3,0}$ 1	4	1			6 = 3!
$(m = 4)$	$a_{4,0}$ 1	11	11	1		24 = 4!
$(m = 5)$	$a_{5,0}$ 1	26	66	$a_{5,3}$ 26	1	120 = 5!



§ 4.2 Recursive Definitions

Conjecture : $\Sigma_{k=0}^{m-1} a_{m,k} = m! \ \forall \ m \in Z^+$

Proof.

① For $1 \le m \le 5$, it's true.

② Assume the result is true for some fixed m (≥ 1)

Now, consider $m + 1$:

$$\Sigma_{k=0}^{m} a_{m+1,k} = \Sigma_{k=0}^{m} [(m - k + 1)a_{m,k-1} + (k + 1)a_{m,k}]$$

$$= [(m + 1)a_{m,-1} + a_{m,0}] + [m\, a_{m,0} + 2a_{m,1}] +$$

$$[(m - 1)a_{m,1} + 3a_{m,2}] + \ldots + [3a_{m,m-3} + (m - 1)a_{m,m-2}] +$$

$$[2a_{m,m-2} + m\, a_{m,m-1}] + [a_{m,m-1} + (m + 1)\, a_{m,m}]$$

$\because a_{m,-1} = 0 = a_{m,m}$

$$\therefore \Sigma_{k=0}^{m} a_{m+1,k} = [a_{m,0} + m\, a_{m,0}] + [2a_{m,1} + (m - 1)a_{m,1}]$$

$$+ \ldots + [(m - 1)a_{m,m-2} + 2a_{m,m-2}] + [m\, a_{m,m-1} + a_{m,m-1}]$$

$$= (m + 1)\, \Sigma_{k=0}^{m-1} a_{m,k} = (m + 1)\, m\,! = (m + 1)\,! \text{ (by } I.\ H.\text{)}$$

$\therefore$ the result is true for all $m \ge 1$ by the Principle of Math. Ind.

§ 4.2 Recursive Definitions

EX4.22 : [implicit] Define the set X recursively by

1) $1 \in X$; and

2) For each $a \in X$, $a + 2 \in X$

Claim that X consists (precisely) of all positive odd integers

Proof.(1/2)

Let $Y = \{2n + 1 \mid n \in \mathrm{N}\}$.

Claim : $X = Y$ (i.e. $X \subseteq Y$ and $Y \subseteq X$)

Proof.

① $Y \subseteq X$: $\forall\ a \in Y \Rightarrow a = 2n + 1$ for some n ($\rightsquigarrow a \in X$)

let $S(n)$: $2n + 1 \in X$, $\forall\ n \in \mathrm{N}$.

i) $S(0)$: $2 \cdot 0 + 1 = 1 \in X$ is true.

ii) Assume $S(k)$ is true for some $k \geq 0$,

i.e. $2k + 1$ is an element in X.

§ 4.2 Recursive Definitions

Proof.(2/2)

By (2) of the recursive definition of X ;

$(2k + 1) + 2 = 2(k + 1) + 1 \in X$

$\therefore$ $S(k + 1)$ is also true.

$\therefore$ $S(n)$ is true by the Principle of Mathematical Induction for all $n \in$ N.

② $X \subseteq Y$: (1) : $1 = 2 \cdot 0 + 1 \in Y$.

(2) : If $b \in X$ and $b \in Y$ is true,

then there exist some $k \geq 0$, s.t. $b = 2k + 1$.

Consider $b + 2 \in X$,

$b + 2 = (2k + 1) + 2 = 2(k + 1) + 1 \in Y$

$\therefore$ $b \in Y$ by the Principle of Mathematical Induction for all $b \in X$. So, $X \subseteq Y$.

$\therefore$ By ①, ② $X \subseteq Y$ and $Y \subseteq X \Rightarrow X = Y$.

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

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

§ 4.3 The Division Algorithm: Prime Numbers

Def 4.1 : $a, b \in Z$ and $b \neq 0$:

① **b divides a, write $b \mid a \equiv \exists\, n \in Z$ s.t. $a = bn$.**

② **b is a divisor of a.**

③ **a is a multiple of b.**

Note : ① $\because \forall\, a, b \in Z, ab = 0 \Rightarrow$ **either** $a = 0$ **or** $b = 0$.

$\therefore$ **say "Z has no proper divisor of 0".**

② **cancel: ex:** $2x = 2y \Rightarrow 2(x - y) = 0$

$\Rightarrow 2 = 0$ **or** $x - y = 0$

$\Rightarrow x = y.$

(not $\times\, ½$, $\because ½ \notin Z$**)**

§ 4.3 The Division Algorithm: Prime Numbers

Thm 4.3 : $\forall\, a, b, c \in Z$

a) $1 \mid a$ and $a \mid 0$.

b) $[(a \mid b) \wedge (b \mid a)] \Rightarrow a = \pm b$.

c) $[(a \mid b) \wedge (b \mid c)] \Rightarrow a \mid c$

d) $a \mid b \Rightarrow a \mid bx$ for all $x \in Z$

e) $\forall\, x, y, z \in Z$ s.t. $x = y + z$

① $[(a \mid x) \wedge (a \mid y)] \Rightarrow a \mid z$ ② $[(a \mid y) \wedge (a \mid z)] \Rightarrow a \mid x$

③ $[(a \mid x) \wedge (a \mid z)] \Rightarrow a \mid y$

f) $[(a \mid b) \wedge (a \mid c)] \Rightarrow a \mid (bx + cy)$ for all $x, y \in Z$

Def : $bx + cy$ is called a *linear combination* of b and c.

g) For $1 \leq i \leq n$, let $c_i \in Z$

$[\forall\, 1 \leq i \leq n, (a \mid c_i)] \Rightarrow a \mid (c_1x_1 + c_2x_2 + \ldots + c_nx_n)$,

where $x_i \in Z$ for all $1 \leq i \leq n$.

§ 4.3 The Division Algorithm: Prime Numbers

f) $[(a \mid b) \wedge (a \mid c)] \Rightarrow a \mid (bx + cy)$ for all $x, y \in Z$

Proof. (f)

$[(a \mid b) \wedge (a \mid c)] \Rightarrow (b = am) \wedge (c = an)$ for some $m, n \in Z$

$\therefore bx + cy = (am)x + (an)y = a(mx + ny)$ with $mx + ny \in Z$

i.e. $a \mid (bx + cy)$

Ex 4.23 : $\exists\, x, y, z \in Z$ s.t. $6x + 9y + 15z = 107$?

Sol.

by Thm 4.3(g), $\because [(3 \mid 6) \wedge (3 \mid 9) \wedge (3 \mid 15)] \Rightarrow 3 \mid 107$

$\rightarrow\leftarrow$

$\therefore$ there do not exist such integer x, y, z.

§ 4.3 The Division Algorithm: Prime Numbers

Ex 4.24 : Let $a, b \in \mathbb{Z}$ so that $2a + 3b$ is a multiple of 17.
Prove that 17 divides $9a + 5b$.

Proof.

$\because 17 \mid (2a + 3b) \Rightarrow 17 \mid (-4)(2a + 3b)$

$\because 17 \mid (17a + 17b) \Rightarrow 17 \mid [(17a + 17b) + (-4)(2a + 3b)]$

$\Rightarrow 17 \mid [(17 - 8)a + (17 - 12)b]$

$\Rightarrow 17 \mid (9a + 5b)$.

Def : ① *Number theory*: Using integer division in mathematics.

② An integer $n \in \mathbb{Z}^+$, $n > 1$, is called a **prime**.
$\equiv$ n has exactly two positive divisors, 1 and n itself.

③ All other positive integers ($> 1 \wedge$ not prime) are called **composite**.

§ 4.3 The Division Algorithm: Prime Numbers

Lemma 4.1 : $n \in Z^+$ and n is composite $\Rightarrow \exists$ prime p s.t. $p \mid n$.

Proof.

Let $S = \{x \mid x$ is composite and x have no prime divisor.$\}$

If $S \neq \phi$, By the Well-Ordering Principle, S has a least element m.

$\because m \in S$

$\therefore m$ is composite and m have no prime divisor.

$\because m$ is composite,

$\therefore \exists\, m_1, m_2 \in Z^+$ with $1 < m_1 < m, 1 < m_2 < m$

s.t. $m = m_1 \cdot m_2$

But $\because m_1 \notin S$ $\therefore m_1$ is prime or divisible by a prime

Consequently, $\exists$ prime p s.t. $p \mid m \rightarrow\leftarrow$

$\therefore S = \phi$.

§ 4.3 The Division Algorithm: Prime Numbers

Thm 4.4 (Euclid 400 B.C.): There are infinitely many primes.

Proof.

If not, let $p_1, p_2, \ldots , p_k$ be the finite prime.

Let $B = p_1 \cdot p_2 \cdot \ldots \cdot p_k +1$

$\because B > p_i, \forall\ 1 \leq i \leq k \quad \therefore B$ cannot be a prime

i.e. B is composite.

By Lemma 4.1, $\exists$ prime p_j, $1 \leq j \leq k$ s.t. $p_j \mid B$

$\because (p_j \mid p_1 p_2 \ldots p_k) \wedge (p_j \mid B) \wedge (B = p_1 p_2 \ldots p_k +1)$

$\therefore$ by Thm 4.3 (e), $p_j \mid 1$

$\rightarrow\leftarrow \quad (\because$ prime $> 1)$

$\therefore$ There are infinitely many primes.

§ 4.3 The Division Algorithm: Prime Numbers

Thm 4.5 : $\forall\, a, b \in Z$, with $b > 0$, $\exists!\, q, r \in Z$ s.t. $a = qb + r$,
where $0 \leq r < b$.

Proof. (1/2)

一、 ∃ (存在性)

① $b \mid a$: $\exists\, m \in Z$ s.t. $a = b{\cdot}m$, Let $q = m$, $r = 0$, it's hold.

② $b \nmid a$: Let $S = \{a - tb \mid t \in Z, a - tb > 0\}$

(i) $(S\neq\phi)$ $\begin{cases} \text{If } a > 0\text{: let } t = 0,\ a - tb = a \in S,\ \therefore S \neq \phi. \\ \text{If } a < 0\text{: let } t = a - 1,\ a - tb = a - (a - 1)b \end{cases}$

$= a(1 - b) + b \geq b > 0$

$(\because b > 0, b \geq 1, 1 - b \leq 0, a(1 - b) \geq 0)$

$\therefore a - tb = a(1 - b) + b \in S, \therefore S \neq \phi$

(ii) (find q, r): $\forall\, a \in Z$, S is a nonempty subset of Z^+
By the Well-Ordering Principle, S has a least
element r, where $0 < r = a - qb$ for some $q \in Z$.

§ 4.3 The Division Algorithm: Prime Numbers

Proof. (2/2)

(iii) $(0 \leq r < b)$: (a) $r = b \Rightarrow a = (q + 1)b \Rightarrow b \mid a \ \rightarrow\leftarrow \ (b \nmid a)$

(b) $r > b \Rightarrow r = b + c$ for some $c \in Z^+$,

$\because a - qb = r = b + c \Rightarrow c = a - (q + 1)b \in S$

$\rightarrow\leftarrow$ (r is least)

$\therefore$ by (a), (b), $r < b$.

二、!(唯一性)

Let $q_1, q_2, r_1, r_2 \in Z$ with $a = q_1b + r_1 = q_2b + r_2$,

where $0 \leq r_1, r_2 < b$.

$\because q_1b + r_1 = q_2b + r_2 \Rightarrow b|q_1 - q_2| = |r_2 - r_1|$

$\because 0 \leq r_1, r_2 < b \ \Rightarrow |r_2 - r_1| < b \ \Rightarrow b|q_1 - q_2| < b$

If $q_1 \neq q_2$, then $b|q_1 - q_2| \geq b \ \rightarrow\leftarrow$

$\therefore q_1 = q_2 \Rightarrow r_1 = r_2$

i.e. the quotient and remainder are unique.

§ 4.3 The Division Algorithm: Prime Numbers

Def : a: **dividend** b: **divisor** q: **quotient** r: **remainder**

Ex 4.25 : a) $a = 170, b = 11$

$\because\ 170 = 15 \cdot 11 + 5,\ 0 \le 5 < 11$

So when 170 is divided by 11, the quotient is 15 and the remainder is 5.

b) $a = 98, b = 7$

$\because\ 98 = 14 \cdot 7$, 7 (**exactly**) **divides** 98.

c) $a = -45, b = 8$

$\because\ -45 = (-6) \cdot 8 + 3$, where $0 \le 3 < 8$

d) Let $a, b \in \mathbb{Z}^+$

① $a = qb$ for some $q \in \mathbb{Z}^+$: $(-a) = (-q) \cdot b$

② $a = qb + r$ for some $q \in \mathbb{N}$ and $0 < r < b$:

$$(-a) = (-q)b - r = (-q)b - b + (b - r)$$

$$= (-q - 1)b + (b - r), \qquad 0 < b - r < b.$$

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

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

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

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

$r_4=1$

$8 \,\underline{\mid 6137}$	Remainders
$8 \,\underline{\mid 767}$	$1(r_0)$
$8 \,\underline{\mid 95}$	$7(r_1)$
$8 \,\underline{\mid 11}$	$7(r_2)$
$8 \,\underline{\mid 1}$	$3(r_3)$
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: $0\sim15 = 0\sim2^4 - 1$

leading 1: $8\sim15 = 2^3\sim2^4 - 1$

six bits: $0\sim63 = 0\sim2^6 - 1$

n bits: $0\sim2^n - 1$

$$\begin{cases} \text{leading 0: } 0\sim2^{n-1} - 1 \\ \text{leading 1: } 2^{n-1}\sim2^n - 1 \end{cases}$$

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

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

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

§ 4.3 The Division Algorithm: Prime Numbers

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

Ex 4.30 : (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 = $(11110000+00000001)_2 = (11110001)_2$

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

nonnegative

discarded

Answer = $(00010010)_2 = 18$

§ 4.3 The Division Algorithm: Prime Numbers

Ex 4.30 : (2/2)

② 15 – 33=? 15+(– 33)

$15 = (00001111)_2$

$33 = (00100001)_2$

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

$$\begin{array}{r} 15 \\ -\ 33 \\ \hline \end{array} \longrightarrow \begin{array}{r} 00001111 \\ +\ 11011111 \\ \hline 11101110 \end{array} \rightarrow (00010001)_2 \rightarrow (00010010)_2 = 18$$

① Take the one's complement

negative

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

Remark : 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 → n bits

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

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

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

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

(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 $p \leq \sqrt{n}$.