CH1、基本數學

集合論、數學歸納法與基礎數論

目錄：

1.1 集合論

定義：

Set 為一堆物品的搜集

A={1, 2, 3, 4}, A={a, 1, O, 口}

1. $x \in A \Leftrightarrow x$ 為 A 之元素
   $A=\{1, 3, 5, \ldots\} \equiv A=\{2k+1 \mid k=0, 1, 2, \ldots\}$
   $A=\{1, 2, \{1, 2\}, 3\}$：4 個元素
   $1\in A$、$2\in A$、$\{1, 2\}\in A$、$3\in A$；但$\{1, 3\}\notin A$
2. $|A|$表示 A 之元素個數，稱為 A 之 Cardinality
   $|A|=4$
3. $A\subseteq B \Leftrightarrow \forall x\in A \Longrightarrow x\in B$
   子集 Subset：$\{1\}\subseteq A$、$\{1, 2\}\subseteq A$、$\{\{1, 2\}\}\subseteq A$；但$\{\{1, 3\}\}\notin A$
4. $A\subset B \Leftrightarrow A\subseteq B$ 但 $A\neq B$
5. $A=B \Leftrightarrow A\subseteq B$ 且 $B\subseteq A$
6. $\Phi=\{\}, x\in\Phi$(一定錯)：Empty Set

Note：

$\{1, 2, 3\} = \{1, 3, 2\} = \{3, 1, 2\} = \{1, 1, 2, 3, 3\}$

例：A={5, 5, {5}, {5, 5, }, {5, {5, 5, }}, {5, 5, {5}, 5, 5}}

$=\{5, \{5\}, \{5, \{5\}\}\}$

$\Longrightarrow |A| = 3$

Note：

1. $|\Phi|=0$
   $\{\Phi\}\neq\Phi$
2. $\Phi\subseteq A$

例(99 成大)：True/False

1. $\Phi\subseteq\{\Phi\}$
2. $\Phi\subseteq\Phi$
3. $\Phi\subset\{\Phi\}$
4. $\Phi\subset\Phi$
5. $\Phi\in\Phi$

True：1, 2, 3, 5；False：4

例(98 台大)：True/False

1. $\Phi\in\Phi$
2. $\{\Phi, \{\Phi\}\} \in \{\Phi, \{\Phi\}, \{\Phi, \{\Phi\}\}\}$
3. $\{\Phi, \{\Phi\}\} \subset \{\Phi, \{\Phi\}, \{\Phi, \{\Phi\}\}\}$
4. $\{a, \{b, c\}\} = \{\{c, b\}, a\}$

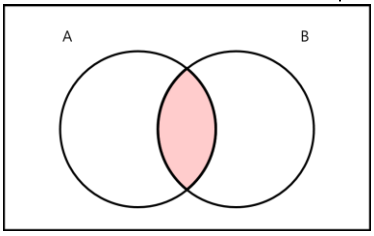
True：2, 3, 4；False：1

常見數系：

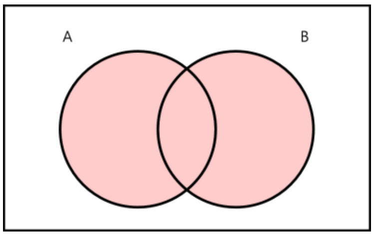
1. $\mathbb{N} = \{0, 1, 2, \ldots\}$ *(80% 自然數從 0；20% 從 1 開始)*
2. $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
3. $\mathbb{Z}^{+} = \{1, 2, 3, \ldots\}$
4. $\mathbb{Q} = \{q/p \mid p, q \in \mathbb{Z}, p \neq q\}$
5. $\mathbb{R}$ = Real Number
6. $\cancel{\mathbb{Q}}$ = Irrational Number
7. $\mathbb{C}$ =Complex Number：$2+3i$, $i=\sqrt{(-1)}$

運算(文氏圖 Venn Diagram)：

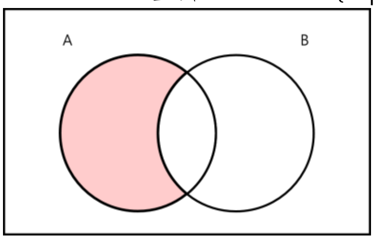
1. Union 聯集：$A \cap B = \{x \mid x \in A \cap x \in B\}$



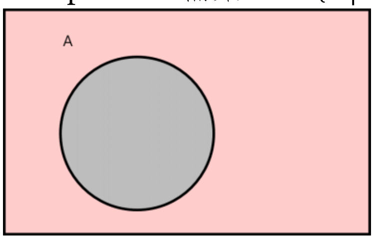
2. Intersection 交集：$A \cup B = \{x \mid x \in A \cup x \in B\}$



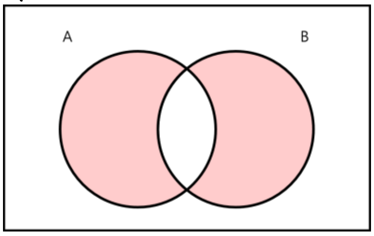
3. Difference 差集：$A - B = \{x \mid x \in A \cap x \notin B\}$



4. Complement 補集：$\cancel{A} = \{x \mid x \notin A\} = U - A$

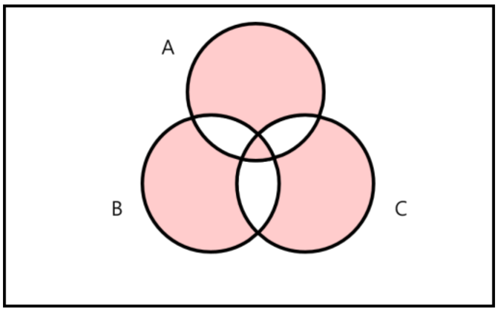


5. Symmetric Difference 對稱差：$A \oplus B = (A \cup B)-(A \cap B) = (A-B) \cup (B-A)$



Property：

1. 交換性
   $A \cap B=B \cap A$
   $A \cup B=B \cup A$
   $A \oplus B=B \oplus A$
2. 結合性
   $(A \cap B) \cap C = A \cap (B \cap C)$
   $(A \cup B) \cup C = A \cup (B \cup C)$
   $(A \oplus B) \oplus C = A \oplus (B \oplus C)$



3. 分配性
   $(A \cup B) \cap C = (A \cup B) \cap (A \cap C)$
   $(A \cap B) \cup C = (A \cap B) \cup (A \cap C)$
   $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$

Note：

1. $A \cap \overline{B} = A-B$
2. $A \oplus \Phi=A$

例(99 台大)：True/False

1. $A-(B \cup C) = (A-B) \cup (A-C)$
2. $A-(B \cap C) = (A-B) \cap (A-C)$
3. $A-(B \cup C) = (A-B) -C$
4. $A \cup B = A \cup C \Longrightarrow B=C$
5. $A \cap B = A \cap C \Longrightarrow B=C$
6. $A \oplus B = A \oplus C \Longrightarrow B=C$

True：3, 6；False：1, 2, 4, 5

例(98 清大)：證：$(A\cap B)\cup C=A\cap(B\cup C) \Leftrightarrow C\subseteq A$

$(\Leftarrow)$：$(A\cap B)\cup C = (A\cup C)\cap(B\cup C) = A\cap(B\cup C)$
$(\Rightarrow)$：$\forall x\in C \Rightarrow x\in(A\cap B)\cup C = A\cap(B\cup C)$
$\Rightarrow x\in A\cap(B\cup C) \Rightarrow x\in A$

定理：De-Morgan's Law 迪摩根
1. $\cancel{A\cup B} = A\cap B$
2. $\cancel{A\cap B} = A\cup B$

定義：
A：Set，定義：
$P(A) = \{x \mid x\subseteq A\}$
$A=\{1, 2, 3\}$，則 $P(A)=\{\Phi, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

定理：
$|A|=n \Rightarrow |P(A)|=2^n$

證明：
Given $x\in A$
A 之每個元素可以屬於 A or 不屬於 A。故有 2 種可能
$\because |A|=n$，$\therefore x$ 之可能性的個數為 2^n，也記作 2^A

Note：
1. $P(\Phi) = \{\Phi\}$
2. $P(P(\Phi)) = \{\Phi, \{\Phi\}\}$
3. $P(P(P(\Phi))) = \{\Phi, \{\Phi\}, \{\{\Phi\}\}, \{\Phi, \{\Phi\}\}\}$

例(95 交大)：
$2^{2^{2^{2^{2^{\{\,\}}}}}}$

2^{16}

例(5 個)(97 輔大)：True/False
1. $P(A\cup B) = P(A)\cup P(B)$
2. $P(A\cap B) = P(A)\cap P(B)$

$x \in P(A\cap B)$
$\Leftrightarrow$ $x \subseteq A\cap B$
$\Leftrightarrow$ $x \subseteq A$ 且 $x \subseteq B$
$\Leftrightarrow$ $x \in P(A)$ 且 $x \in P(B)$
$\Leftrightarrow$ $x \in P(A)\cap P(B)$

定義：

A, B：Sets，定義：

$A \times B = \{a, b \mid a\in A, b\in B\}$，稱為 A, B 之卡氏積 Cartesian Product

$A=\{1, 2, 3\}$、$B=\{a, b\}$

$A\times B = \{(1, a), (2, a), (3, a), (1, b), (2, b), (3, b)\}$

Note：

$|A|=m, |B|=n \Longrightarrow |A\times B|=m\times n$

例(98 交大)：$|A|=3, |B|=2$，求$|2^{2^A\times 2^B}|$

$2^A=2^3=8,\ 2^B=2^2=4,\ 2^A\times 2^B=32 \Longrightarrow$ 原式$=2^{32}$

Note：

1. $A_1\times A_2\times\ldots\times A_n$
   $=\{(a_1, a_2, \ldots, a_n) \mid a_1\in A_1, a_2\in A_2, \ldots, a_n\in A_n\}$
2. $R\times R = R^2 = \{(a, b) \mid a, b \in R\}$

1.2 數學歸納法

定理(3 個)：(數學歸納法 TMathematical Induction)
P(n)為一命題，$n \in \mathbb{Z}^+$
1. Basis Step：P(1) is true.
2. Inductive Step：設 P(k) is true，則 P(k+1) is true too.
3. 則 P(n) is true, $\forall n \in \mathbb{Z}^+$

參考：
Well-order：$A \subseteq \mathbb{Z}^+$, $A \neq \Phi$，則 A 中存在最小元素

證明：
令$\mathbb{F}=\{n \in \mathbb{Z}^+ \mid P(n) \text{ is false}\}$, Claim $\mathbb{F} = \Phi$(矛盾$\mathbb{F} \neq 0$)
by well-order $\mathbb{F}$中存在最小元素 $s \in \mathbb{F}$
$\because$P(1) is true, $\therefore s-1 \neq \mathbb{F}$, $\therefore$P(s-1) is true
by inductive step, P(s) is true $\rightarrow\leftarrow$

例(98 中原)：證：$3 \mid (7^n-4^n), \forall n \geq 1$

1. *$3 \mid 7-4$ 成立*
2. *設 n=k 時成立，即 $3 \mid (7^k-4^k)$*
   當 n=k+1 時，$7^{k+1}-4^{k+1} = 3(7^k)+4(7^k-4^k)$, $\because 3 \mid (7^k-4^k)$且 $3 \mid 3(7^k) \Longrightarrow 3 \mid 3(7^k)+4(7^k-4^k)$
3. *by Mathematic Induction：$3 \mid (7^n-4^n), \forall n \geq 1$*

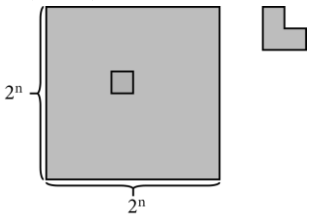
例(97 淡大)：證：$n^2 \leq n!, \forall n \geq 4$

1. *$n=4$, $4^2 \leq 4!=24$ 成立*
2. *設 n=k 時成立，即 $k^2 \leq k!$*
   當 n=k+1 時，$(k+1)^2=k^2+2k+1 < k!+2k+1 < k!+k! = k(k!)+k! = (k+1)k! = (k+1)!$
3. *by Mathematic Induction：$n^2 \leq n!, \forall n \geq 4$*

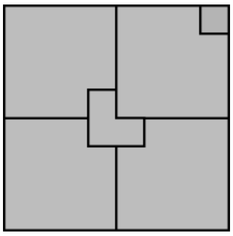
例(5 個)：$Hm = 1/1 + 1/2 + 1/3 + \ldots + 1/m$(調和級數 Harmonic Number)
證：$H_{2n} \geq 1+ n/2, \forall n \geq 0$

1. *$H_4=1 + 1/2 + 1/3 + 1/4 \geq 1 + 2/2$*
2. *設 n=k 時成立，即 $H_{2k} \geq 1 + k/2$*
   當 n=k+1 時：$H_{2(k+1)} = H_{2k} + 1/(2^k+1) + \ldots + 1/(2^k+2^k) \geq H2k + 1/(2^k+2^k) + \ldots + 1/(2^k+2^k)$
   $= 1+k/2 + 2^k/(2^k+2^k) = 1 + k/2 + 1/2 = 1 + (k+1)/2$
3. *by Mathematic Induction：$H_{2n} \geq 1+ n/2, \forall n \geq 0$*

例(5 個)：



1. *$n=1$ 時成立*
2. *令 $n=k$ 時成立，consider $n=k+1$*



3. *by Mathematic Induction，得證*

例(94 中央)：證：任 n 匹馬顏色相同

1. *$n=1$ 時成立*
2. *設 $n=k$ 時成立，consider $n=k+1$，k 個 k 個顏色相同，所以 k+1 個顏色相同，因此得證？*

不正確：此為數學歸納法之誤用，因為當 $n=2$ 時，與 $n=1$ 並無重疊，兩隻馬顏色只有『個自相同』，故不能使用此法證明之

Note：
Storng Form of Induction：Inductive Step：設 P(1), …, P(k)為真，則 P(k+1) is true too.

例(99 台大)：證：$\forall\ n \geq 14$ 元，皆可用 3 元 or 5 元組合之？

$14 = 8+3+3$
$15 = 3+3+3+3+3$
$16 = 8+8$
設 $k-3<k$, $\therefore k-3$ 元的郵資可用 3 及 8 元郵票可組合成 k 元

例(97 台大)：證：除了 1, 2, 4, 7 之外，所有價格都可用 3, 5 元組合？

$8 = 3+5$
$9 = 3+3+3$
$10 = 5+5$
$11 = 5+3+3$

1.3 基礎數論

定義：

$n \geq 2$，若 n 除了 1 與 n 之外，不再有其他的正因數 Factor，稱 n 為質數 Prime，否則稱 n 為組合數 Composite

定理：

$\mathbb{Z}+$中，質數的個數為∞

證明：

設質數的個數有限，令 $P_1, \ldots, P_k$ 為所有質數，取 $E = P_1 \times P_2 \times \ldots \times P_k + 1$

$\Longrightarrow$ E 為組合數 $\Longrightarrow \exists P_j \ni P_j | E$

$\because P_j | P_1 \times P_2 \times \ldots P_k$

$\Longrightarrow P_j \mid E - P_1 \times P_2 \times \ldots P_k = 1 \Longrightarrow P_j = 1 \rightarrow\leftarrow$

Note：

$n = p_1^{e1} \times p_2^{e2} \times \ldots \times p_k^{ek}$：實因數分解

1. n 的正因數為$(e_1+1)(e_2+1)\ldots(e_k+1)$
2. Euler Function(Φ)

   $\Phi(n)$表 1~n 中，與 n 互質的個數

   $\Phi(12) = 4$ 個(1, 5, 7, 11)

   $\Phi(n) = n(1 - 1/p_1)(1 - 1/p_2)\ldots(1 - 1/p_k)$

   $\Phi(12) = 12(1-1/2)(1-1/3) = 4$

例(3 個)(95 東華)：證：2^n-1 為質數 $\Longrightarrow$ n 為質數

(反證法：$p \rightarrow q \equiv \cancel{q} \rightarrow \cancel{p}$)

設 n 為 Composite：$n=r \times s$, $1< r, s < n$

Claim 2n-1 is Composite

$n = 2^{rs}-1 = (2^r)^s -1 = (2^r-1)[(2^r)^{s-1} + (2^r)^{s-2} + \ldots + (2^r) + 1]]$

其中： $1< 2^r-1 < 2^n-1$，$\therefore$2n-1 is Composite

$[1.2]_f$：floor = 1, $[-2.7]_f = -3$

$[1.2]_c$：celling=2, $[-2.7]_c = -2$

例(99 中央)：100!的尾數有幾個 0？

5：20

25：4

125：0

$\Longrightarrow 20+4+0 = 24$

例(97 中原)：70!之二進位表示法，尾數有幾個 0？

2：35
4：17
8：8
16：4
32：2
64：1
$\Longrightarrow 35+17+8+4+2+1 = 67$

例(5 個)：證：$\sqrt{(2)}$為無理數

設$\sqrt{(2)}$為有理數，即$\sqrt{(2)} = q/p$ (p, q 互質)
$\Longrightarrow 2=q^2/p^2 \Longrightarrow 2p^2=q^2 \Longrightarrow 2|q$
$\Longrightarrow$ *令 $q=2r$*
$\Longrightarrow 2p^2=4r^2 \Longrightarrow p^2=2r^2,\ 2|p$
$\Longrightarrow gcd(p, q) = 2 \ \rightarrow\leftarrow$

定理：
$m=nq+r,\ 0 \le r < n$
$\Longrightarrow \gcd(m, n) = \gcd(n, r)$

證明：
1. $g|m, g|n, r=m-nq$
   $\therefore g|r \Longrightarrow g$ 為 n, r 之公因數
   $\therefore h \ge g$
2. $h|n$ 且 $h|r$
   $\because m=nq+r,\ \therefore h|m$
   $\therefore h$ 為 m, n 之一公因數 $\Longrightarrow h\le g$

by 1, 2 $\Longrightarrow h=g$

例(99 中山)：求 $\gcd(7n+3, 5n+2),\ n\in\mathbb{Z}^+$

$(7n+3, 5n+2) = (2n+1, 5n+2) = (2n+1, n) = (n, 1)$ 互質

Note：
$\gcd(n+1, n) = \gcd(n, 1) = 1 \Longrightarrow$ 相鄰 2 數必互質
$\gcd(a, b)=g$
$\Delta\ \{as+bt \mid s, t \in \mathbb{Z}\} = \{gz \mid z\in \mathbb{Z}\}$
Δ $ax+by=c$ 有解 $\Leftrightarrow g|c$
Δ 利用 Euclidean Algorithm 求 x, y

例(99 北科)：下列整數解是否存在？

1. 154x+260y=5
2. 108x+30y=7
3. 45x+14y=1
4. 621x+736y=46

1. False，偶數
2. False，偶數
3. True
4. True

例(98 高大)：求所有整數解 131x+32y=2？

*131=4*32+3*
*32=10*3+2*
*3=1*2+1*

*1 = 3-2 = 3-(32-10*3) = 11*3 – 32 = 11*(131-4*32) -32 = 11*131 – 45*32*
*2 = 22*131 – 90*32*
⟹ (x, y) = (22, 90), (54, -221), (86, -352)

例(96, 97, 99 台大)：True/False

1. $a \equiv b \pmod{n} \Longrightarrow 2a \equiv 2b \pmod{n}$
2. $a \equiv b \pmod{2n} \Longrightarrow a \equiv b \pmod{n}$
3. $a \equiv b \pmod{n} \Longrightarrow 2a \equiv 2b \pmod{2n}$
4. $a \equiv b \pmod{n} \Longrightarrow a \equiv b \pmod{2n}$

True：1, 2, 3；False：4(a=1, b=3, c=2)

例(98 清大)：求 $7x \equiv 13 \pmod{19}$之所有解？

*19 = 7*2 + 5*
*7 = 5*1 + 2*
*5 = 2*2 + 1*
*1 = 5*1 – 2*2 = (7-2)*1 – 2*2 = 7*1 – 2*3 = 7*1 – (7-5)*3 = 7*(-2) + 5*3*
= 7(-2) + (19-7*2)*3 = 7*(-8) + 19*3 = 19*39 – 7*104*
*13 = 19*39 – 7*104*
⟹ x=-104 + 19k = 10 + 19k, ∀k∈ℤ

Note：

1. $a \equiv b \pmod{n},\ c \equiv d \pmod{n}$
   $\Longrightarrow a+c \equiv b+d \pmod{n}$
   $\Longrightarrow 2a \equiv 2b \pmod{n}$
   $\Longrightarrow ka \equiv kb \pmod{n}$
2. $ka \equiv kb \pmod{n} \Longrightarrow a \equiv b \pmod{n}$ 是錯誤的！

定義：

gcd(a, n)=1，若 $ab\equiv 1 \pmod n$，則稱 b 為 a 之 Inverse，記作 $a^{-1} \pmod n$

例(99 長庚)：求 $13^{-1} \pmod{57}$

*57 = 13*4 + 5*
*13 = 5*2 + 3*
*5 = 3*1 + 2*
*3 = 2*1 + 1*
1 = 3-2 = (5-2) – 2 = 5-1 + 2(-2) = 5*1 + (5-3)*(-2) = 5*(-1) + 3*2*
= 5(-1) + (13-5*2)*2 = 13*2 + 5*(-5) = 13*2 + (57-13*4)*(-5) = 13*22 + 57*(-5)*
$\Longrightarrow 13*22 - 57*5 = 1$
$\Longrightarrow 13^{-1} \pmod{57} = 22$, ex：$22+57k, \forall k\in\mathbb{Z}$

定理：(費馬小定理 Fermat Little Theorem)
p：Prime，pła
$\Longrightarrow a^{p-1}\equiv 1 \pmod a$

例(98 長庚)：$3^{302} \bmod 5 =$?

$3^4 \bmod 5 = 1$(費馬小定理)
$\Longrightarrow 3^{302} = (3^4)^75 * 3^2 \Longrightarrow 3^2 \bmod 5 = 4$

例(99 清大)：求 $30^{16} \bmod 257$?

9008 mod 257
[法一]暴力法(4 次)
[法二]
$30^{16} = 2^{16} * 3^{16} * 5^{16} = 256^2 * 15^{16} \equiv (-1)^2 * 15^{16} = 15^{16}$
$15^2 = 225 \equiv -32 = -2^5$
$15^{16} \equiv (15^2)^8 \equiv (-2^5)^8 = (2^8)^5 \equiv (-1)^5 \equiv -1 = 256$

定理：(費馬小定理的推廣)
gcd(a, n)=1
$\Longrightarrow a^{\Phi(n)} = 1 \pmod n$

例(99 交大)：求 $2^{99} \bmod 33$?

$2^{99} \equiv (2^5)^{19} * 2^4 \equiv (-1)^{19} * 2^4 \equiv -16 \equiv 17$

定理：(中國餘式定理 Chinese Remainder Theorem, CRT)
$n_1, \ldots, n_k \in \mathbb{Z}+$，彼此互質
$x \equiv r_1 \pmod{n_1}$
…
$x \equiv r_k \pmod{n_k}$

例(99 政大)：

$x \equiv 5 \pmod 7$
$x \equiv 4 \pmod 9$
$x \equiv 3 \pmod{13}$

$n = n_1n_2n_3 = 819$
$N_1 = n/n_1 = 117$；　　$M_1 = N_1^{-1}(mod\ n_1) \equiv 3$
$N_2 = n/n_2 = 91$；　　$M_2 = N_2^{-1}(mod\ n_2) \equiv 1$
$N_3 = n/n_3 = 63$；　　$M_3 = N_3^{-1}(mod\ n_3) \equiv 6$
$x \equiv M_1*N_1*r_1 + M_2*N_2*r_2 + M_3*N_3*r_3 = 3*117*5 + 1*91*9 + 6*63*13 = 3253\ (mod\ 819)$
$\Longrightarrow x = 796 + 819k,\ \forall k \in \mathbb{Z}$

例(97 台科)：

$x \equiv 1 \pmod 2$
$x \equiv 2 \pmod 3$
$x \equiv 8 \pmod{15}$

$x \equiv 8\ (mod\ 15) \Longrightarrow\ x \equiv 3\ (mod\ 5)$
$n = n_1n_2n_3 = 30$
$N_1 = n/n_1 = 15$；　　$M_1 = N_1^{-1}(mod\ n_1) \equiv 1$
$N_2 = n/n_2 = 10$；　　$M_2 = N_2^{-1}(mod\ n_2) \equiv 1$
$N_3 = n/n_3 = 6$；　　$M_3 = N_3^{-1}(mod\ n_3) \equiv 1$
$x \equiv M_1*N_1*r_1 + M_2*N_2*r_2 + M_3*N_3*r_3 = 1*15*1 + 1*10*2 + 1*6*3 = 53\ (mod\ 30)$
$\Longrightarrow x = 23 + 30k,\ \forall k \in \mathbb{Z}$

例：

$x \equiv 1 \pmod 3$
$x \equiv 13 \pmod{16}$
$x \equiv 73 \pmod{81}$

將 $x \equiv 73\ (mod\ 81)$拆成可跟 3, 16 互質之數，但因為 81 不可能與 3 互質，故只需考慮以下兩式
$x \equiv 13\ (mod\ 16)$
$x \equiv 73\ (mod\ 81)$

$n = n_1n_2 = 1296$
$N_1 = n/n_1 = 81$；　　$M_1 = N_1^{-1}(mod\ n_1) \equiv 1$
$N_2 = n/n_2 = 16$；　　$M_2 = N_2^{-1}(mod\ n_2) \equiv -5$
$x \equiv M_1*N_1*r_1 + M_2*N_2*r_2 = 1*81*13 + (-5)*16*73 = -4787\ (mod\ 1296) = 397\ (mod\ 1296)$
$\Longrightarrow x = 397 + 1296k,\ \forall k \in \mathbb{Z}$