2.2. 正因數個數及正因數和

我們可以用 multiplicative arithmetic function 的概念很快的求出一正整數其正因數之個數及正因數和.

所謂 *positive divisors function* 指的是形如：$\sigma_z(n)=\sum_{d|n,d\in\mathbb{N}} d^z$ 這樣的 arithmetic function。這裡 z 可以是任意固定的複數；不過我們僅探討 $z=0,1$ 的情況。給定 z，若令 $f(n)=n^z$，很容易知道 $f(n)$ 是 completely multiplicative，所以 $\sigma_z(n)=\sum_{d|n,d\in\mathbb{N}} f(d)$ 也是 multiplicative。

給定一正整數 n, $\sigma_0(n)$ 就是 n 的正因數個數. 事實上

$$\sigma_0(n)=\sum_{d|n,d>0} 1.$$

上式的意思就是每次你看到 d 滿足 $d|n$ 且 $d>0$ 就加一次, 所以很自然得到 n 的正因數個數.

Proposition 2.2.1. 對任意 $n\in\mathbb{N}$, 令 $\sigma_0(n)$ 表示 n 的正因數個數. 則 $\sigma_0:\mathbb{N}\to\mathbb{N}$ 是一個 *multiplicative arithmetic function.* 而且若 $n=p_1^{n_1}\cdots p_r^{n_r}$, 其中 p_i 為相異質數, 則 $\sigma_0(n)=(n_1+1)\cdots(n_r+1)$.

Proof. 前面已知 σ_0 是 multiplicative, 我們可以利用 Proposition 2.1.3 求對任意 $n\in\mathbb{N}$, $\sigma_0(n)$ 之值. 也就是說我們要先探討對任意質數 p 以及正整數 t, $\sigma_0(p^t)$ 之值. 由於 p^t 的正因數就是 p^i, 其中 $i\in\{0,1,\ldots,t\}$, 我們得到 $\sigma_0(p^t)=t+1$. 因此對任意 $n\in\mathbb{N}$, 若 $n=1$, 我們知 $\sigma_0(n)=\sigma_0(1)=1$; 而若 $n=p_1^{n_1}\cdots p_r^{n_r}$ 其中 p_i 為相異質數, 則由 σ_0 是 multiplicative 知

$$\sigma_0(n)=\sigma_0(p_1^{n_1})\cdots\sigma_0(p_r^{n_r})=(n_1+1)\cdots(n_r+1).$$

□

舉例來說, 我們要求 360 的正因數個數, 由於 $360=2^3\cdot 3^2\cdot 5$, 利用 Proposition 2.2.1, 我們很快就可得 $\sigma_0(360)=(3+1)(2+1)(1+1)=24$. 從這裡大家應更能體會 multiplicative arithmetic function 的好處. 或許求 $\sigma_0(n)$ 的公式大家在高中時學排列組合時就用乘法原理得到過. 可以用乘法原理的原因其實就和 σ_0 是 multiplicative 息息相關.

Question 2.1. $\sigma_0:\mathbb{N}\to\mathbb{N}$ 是否為 completely multiplicative?

接下來我們探討正因數和. 給定一正整數 n, $\sigma_1(n)$ 表示 n 的所有正因數之和. 事實上

$$\sigma_1(n)=\sum_{d|n,d>0} d.$$

上式的意思就是每次你看到 d 滿足 $d|n$ 且 $d>0$ 就加 d, 所以很自然得到 n 的正因數和.

Proposition 2.2.2. 對任意 $n \in \mathbb{N}$, 令 $\sigma_1(n)$ 表示 n 的所有正因數之和. 則 $\sigma_1 : \mathbb{N} \to \mathbb{N}$ 是一個 *multiplicative arithmetic function.* 而且若 $n = p_1^{n_1} \cdots p_r^{n_r}$, 其中 p_i 為相異質數, 則

$$\sigma_1(n) = \frac{p_1^{n_1+1}-1}{p_1-1} \cdots \frac{p_r^{n_r+1}-1}{p_r-1}.$$

Proof. 已知 σ_1 是 multiplicative, 同樣利用 Proposition 2.1.3 可求對任意 $n \in \mathbb{N}$, $\sigma_1(n)$ 之值. 也就是說我們要先探討對任意質數 p 以及正整數 t, $\sigma_1(p^t)$ 之值. 由於 p^t 的正因數就是 p^i, 其中 $i \in \{0,1,\ldots,t\}$, 我們得到 $\sigma_1(p^t) = 1 + p + \cdots + p^t$. 由於 $1, p, \ldots, p^t$ 是一個公比為 p 的等比數列, 我們得

$$\sigma_1(p^t) = \frac{p^{t+1}-1}{p-1}.$$

因此對任意 $n \in \mathbb{N}$, 若 $n = 1$, 我們知 $\sigma_1(n) = \sigma_1(1) = 1$; 而若 $n = p_1^{n_1} \cdots p_r^{n_r}$ 其中 p_i 為相異質數, 則由 σ_1 是 multiplicative 知

$$\sigma_1(n) = \sigma_1(p_1^{n_1}) \cdots \sigma_1(p_r^{n_r}) = \frac{p_1^{n_1+1}-1}{p_1-1} \cdots \frac{p_r^{n_r+1}-1}{p_r-1}.$$

□

舉例來說, 我們要求 360 的正因數和, 由於 $360 = 2^3 \cdot 3^2 \cdot 5$, 利用 Proposition 2.2.2, 我們很快就可得

$$\sigma_1(360) = \frac{2^4-1}{2-1}\frac{3^3-1}{3-1}\frac{5^2-1}{5-1} = 15 \cdot 13 \cdot 6 = 1170.$$

Question 2.2. $\sigma_1 : \mathbb{N} \to \mathbb{N}$ 是否為 completely multiplicative?

Exercise 2.3. 對於 $n \in \mathbb{N}$，若存在 $a \in \mathbb{N}$ 使得 $n = a^2$，則稱 n 為平方數（square integer）。

(1) 證明 $\sigma_0(n)$ 為奇數若且唯若 n 是平方數。

(2) 證明 $\sigma_1(n)$ 為奇數若且唯若 n 是平方數或是一個平方數的 2 倍。

2.3. The Euler ϕ-function

我們要探討比 n 小且與 n 互質的正整數個數.

Definition 2.3.1. 給定 $n \in \mathbb{N}$, $\phi(n)$ 表示比 n 小且與 n 互質的正整數個數. 這樣定出的函數 $\phi : \mathbb{N} \to \mathbb{N}$, 稱之為 Euler ϕ-function.

我們要證明 Euler ϕ-function 是 multiplicative, 並求其在任意正整數之取值. 由於不容易找到簡單的 multiplicative arithmetic function f 使得 ϕ 表示成如 Theorem 2.1.5 的形式, 所以我們要直接證明 ϕ 是 multiplicative. 也就是說對任意 $a, b \in \mathbb{N}$ 滿足 $\gcd(a,b) = 1$, 我們要證明 $\phi(ab) = \phi(a)\phi(b)$.

首先我們看一個 $a=5,b=4$ 的例子. 我們要說明 $\phi(20)=\phi(5)\phi(4)$. 由於 $\phi(20)$ 表示比 20 小且與 20 互質的正整數個數, 所以我們將小於等於 20 的正整數如下列出:

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

很容易看出最後一列 5 10 15 20 中每一個數都是 5 的倍數所以不可能和 20 互質, 因此我們要刪除這一列. 而其餘 4 列每一列中的數除以 5 的餘數都相同且都不等於 0 所以這 4 列的數都和 5 互質. 因此我們只要考慮這 4 列的數哪些和 4 是互質的. 仔細觀察這每一列中的數除以 4 的餘數都相異因此每列中只有餘 1 和餘 3 的兩個數和 4 互質. 總結來說我們發現共有 $\phi(5)=4$ 列的數和 5 互質, 而這 4 列的數中每列皆有 $\phi(4)=2$ 個數和 4 互質, 因此 1 到 20 之中共有 $\phi(5)\phi(4)=8$ 個數和 5 且和 4 互質. 這些數就是 1 到 20 之中和 20 互質的數, 所以知 $\phi(20)=\phi(5)\phi(4)$.

接下來我們就是要用前面的方法證明一般的情形. 要注意前面的方法我們並無真正點出哪些數和 20 互質, 因為我們只想知道個數. 再加上我們的方法幾乎和 $a=5,b=4$ 無關所以比實際找出哪些數和 20 互質更能運用在一般的狀況. 首先我們用到和 20 互質的數就是和 5 且和 4 互質的數, 這個性質在一般的情況都對. 下一個 Lemma 其實就是 Lemma 1.2.7, 這裡我們再用質數的性質重新證明.

Lemma 2.3.2. 假設 $a,b,c\in\mathbb{Z}$. 則 $\gcd(ab,c)=1$ 若且唯若 $\gcd(a,c)=1$ 且 $\gcd(b,c)=1$.

Proof. 假設 $\gcd(ab,c)=1$. 若 $d=\gcd(a,c)$, 表示 d 是 a,c 的公因數, 所以 d 也是 ab 和 c 的公因數, 故得 $d=1$. 同理知 $\gcd(b,c)=1$.

反之, 假設 $\gcd(a,c)=1$ 且 $\gcd(b,c)=1$. 若 $\gcd(ab,c)\neq 1$, 表示存在一質數 p 滿足 $p|\gcd(ab,c)$. 也就是說 $p|ab$ 且 $p|c$. 但 p 是質數, 故由 Lemma 1.5.2 知 $p|a$ 或 $p|b$. 得知 p 是 a,c 或 b,c 的公因數. 此和 $\gcd(a,c)=1$ 且 $\gcd(b,c)=1$ 相矛盾, 故知 $\gcd(ab,c)=1$. □

在前面求與 20 互質的數中, 另一個重要步驟是任一排中每一個數除以 4 的餘數都相異, 這在一般 $\gcd(a,b)=1$ 的情況都是對的.

Lemma 2.3.3. 假設 $a,b,l\in\mathbb{Z}$, $b>1$ 且 $\gcd(a,b)=1$. 則在 $l,l+a,l+2a,\ldots,l+(b-1)a$, 中每一個數除以 b 的餘數皆相異. 而且其中共有 $\phi(b)$ 個元素和 b 互質.

Proof. 若 $u,v\in\mathbb{Z}$ 且 u,v 除以 b 的餘數相同, 表示 $b|u-v$. 因此要說 $l,l+a,\ldots,l+(b-1)a$ 中的元素除以 b 的餘數皆相異, 就是說任取 $l+ia,l+ja$, 其中 $0\leq i<j\leq b-1$, 都無法使得 b 整除 $(l+ja)-(l+ia)$. 今假設 $b|(l+ja)-(l+ia)$, 也就是說 $b|(j-i)a$. 由於 $\gcd(a,b)=1$, Proposition 1.2.6(1) 告訴我們 $b|j-i$. 但此與 $0\leq i<j\leq b-1$ 相矛盾, 故由反證法知 b 不整除 $(l+ja)-(l+ia)$. 也就是說任取 $l+ia,l+ja$, 其中 $0\leq i<j\leq b-1$, 則它們除以 b 之餘數皆相異.

對於 $i\in\{0,1,\ldots,b-1\}$ 若令 r_i 表示 $l+ia$ 除以 b 的餘數, 由於 $0\le r_i\le b-1$ 且這 b 個 r_i 皆相異, 我們知 $\{r_0,r_1,\ldots,r_{b-1}\}$ 這一個集合和 $\{0,1,\ldots,b-1\}$ 是相同的. 然而 Lemma 1.3.1 告訴我們 $\gcd(l+ia,b)=\gcd(r_i,b)$, 所以 $\{l,l+a,\ldots,l+(b-1)a\}$ 中和 b 互質的數和 $\{0,1,\ldots,b-1\}$ 中和 b 互質的數之個數相同. 依定義知 $\{0,1,\ldots,b-1\}$ 中共有 $\phi(b)$ 個數與 b 互質, 故得證. □

接下來我們證明 ϕ 是一個 multiplicative arithmetic function.

Proposition 2.3.4. 若 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$, 則 $\phi(ab)=\phi(a)\phi(b)$.

Proof. 我們將小於 ab 的正整數依下列方法排成 b 列:

$$\begin{array}{cccc} 1 & 1+a & \cdots & 1+(b-1)a \\ 2 & 2+a & \cdots & 2+(b-1)a \\ \vdots & \vdots & \ddots & \vdots \\ a & 2a & \cdots & ba \end{array}$$

其中第 l 列為 $l,l+a,\ldots,l+(b-1)a$. 由 Lemma 1.3.1 知這裡每一數和 a 的最大公因數皆與 l 和 a 的最大公因數相同. 換言之, 若 l 和 a 互質則第 l 列中每一數皆和 a 互質; 而若 l 和 a 不互質則第 l 列中每一數皆和 a 不互質. 又因為 $1\le l\le a$, 故依定義共有 $\phi(a)$ 個 l 會與 a 互質. 而我們就僅考慮這 $\phi(a)$ 列的數 (其餘的數都和 a 不互質故和 ab 不互質).

這 $\phi(a)$ 列的數雖都和 a 互質但並不都和 b 互質. 然而每一列皆為 $l,l+a,\ldots,l+(b-1)a$ 的形式, 故由 $\gcd(a,b)=1$ 以及 Lemma 2.3.3 知每一列皆有 $\phi(b)$ 個數和 b 互質. 故 1 到 ab 中總共有 $\phi(a)\phi(b)$ 個元素和 a 且和 b 互質. 由 Lemma 2.3.2 這些數就是和 ab 互質的數. 故得證 $\phi(ab)=\phi(a)\phi(b)$. □

既然 ϕ 是 multiplicative, 我們就可以利用 Proposition 2.1.3 算出 ϕ 之值.

Proposition 2.3.5. 若 $n=p_1^{n_1}\cdots p_r^{n_r}$, 其中 p_i 為相異質數, 則

$$\phi(n)=(p_1^{n_1}-p_1^{n_1-1})\cdots(p_r^{n_r}-p_r^{n_r-1})=n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_r}).$$

Proof. 我們先求對任意質數 p 以及正整數 t, $\phi(p^t)$ 之值. 由於 p 是 p^t 唯一的質因數, u 和 p^t 不互質表示 p 必為 u 之因數. 因此要計算小於 p^t 的正整數中有多少與 p^t 互質, 只要算出這些數中有哪些是 p 的倍數再扣掉即可. 然而 1 到 p^t 中共有 p^t/p 個數是 p 的倍數. 故得知 1 到 p^n 中共有 p^t-p^{t-1} 個整數和 p^t 互質.

現考慮任意 $n\in\mathbb{N}$. 若 $n=1$, 我們知 $\phi(n)=\phi(1)=1$; 而若 $n=p_1^{n_1}\cdots p_r^{n_r}$ 其中 p_i 為相異質數, 則由 ϕ 是 multiplicative 知

$$\phi(n)=\phi(p_1^{n_1})\cdots\phi(p_r^{n_r})=(p_1^{n_1}-p_1^{n_1-1})\cdots(p_r^{n_r}-p_r^{n_r-1})=n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_r}).$$

□

既然 ϕ 是 multiplicative, 我們可以利用 Theorem 2.1.5 造出另一個 multiplicative arithmetic function. 考慮 $F:\mathbb{N}\to\mathbb{N}$ 其定義為對任意 $n\in\mathbb{N}$, $F(n)=\sum_{d|n,d>0}\phi(d)$. 由於 F 是 multiplicative, 且對任意質數 p 以及 $t\in\mathbb{N}$, 我們有

$$F(p^t)=\phi(1)+\phi(p)+\phi(p^2)+\cdots+\phi(p^t)=1+(p-1)+(p^2-p)+\cdots+(p^t-p^{t-1})=p^t.$$

因此我們有以下之結果.

Corollary 2.3.6 (Gauss)**.** 若 $n\in\mathbb{N}$ 則

$$\sum_{d|n,d>0}\phi(d)=n.$$

Proof. 令 $F(n)=\sum_{d|n,d>0}\phi(d)$, 由前知 F 不是 0 函數故由 F 是 multiplicative, 利用 proposition 2.1.3 知 $F(1)=1$. 若 $n\in\mathbb{N}$ 且 $n>1$ 時, 將 n 寫成 $n=p_1^{n_1}\cdots p_r^{n_r}$, 其中 p_i 為相異質數, 再由上面 $F(p^t)=p^t$ 的結果及 Proposition 2.1.3 知

$$F(n)=F(p_1^{n_1})\cdots F(p_r^{n_r})=p_1^{n_1}\cdots p_r^{n_r}=n,$$

得證本定理. □

Exercise 2.4. 以下是幾個關於 Euler ϕ-function 的性質. 此處 $m,n\in\mathbb{N}$.

(1) 假設 $n=p_1^{n_1}\cdots p_r^{n_r}$ 是 n 的質因數分解. 試證明

$$\phi(n)=\big(p_1^{n_1-1}\cdots p_r^{n_r-1}\big)\big((p_1-1)\cdots(p_r-1)\big).$$

並依此證明 $\sqrt{n}/2\le\phi(n)\le n$.

(2) 試證明若 n 為奇數則 $\phi(2n)=\phi(n)$, 而若 n 為偶數則 $\phi(2n)=2\phi(n)$.

(3) 假設 n 有 m 個相異奇質因數, 試證明 $2^m\mid\phi(n)$.

(4) 試證明 $\phi(n^m)=n^{m-1}\phi(n)$.

(5) 假設 $m\mid n$, 試證明 $\phi(m)\mid\phi(n)$ 且 $\phi(mn)=m\phi(n)$.

Chapter 3

Congruences

同餘 (congruence) 的概念就是將整數適當的分成有限多類, 使其仍能和整數一樣的運算, 從而得到一些整數的重要性質. 本章就是探討 congruence 的定義以及得到一些有關 congruence 的重要式子.

3.1. 同餘的分類

Congruence relation 是一個 equivalent relation. 首先我們探討 equivalent relation 的基本概念.

一般來說要將一個集合分類必須符合以下三個要素. 第一個就是, 自己和自己是同類的; 另一要素是若甲和乙是同類的則乙也必須和甲是同類的; 最後一個要素是如果甲和乙同類且乙和丙同類, 則甲必須和丙同類. 很多同學應該知道這樣的分類同類間的關係稱之為 *equivalence relation*. 我們還是用數學的方法給 equivalence relation 正式的定義.

Definition 3.1.1. 若一集合 S 中我們用 $a \sim b$ 表示 a 和 b 是同類的, 則這樣的分類若符合以下性質我們稱之為 equivalence relation:

(equiv1): 對所有 $a \in S$, 我們都有 $a \sim a$ (reflexivity).

(equiv2): 若 $a \sim b$, 則 $b \sim a$ (symmetry).

(equiv3): 若 $a \sim b$ 且 $b \sim c$, 則 $a \sim c$ (transitivity).

我們常用的 "=" 就是一個典型的 equivalent relation.

到底用 equivalence relation 分類有什麼好處呢? 首先當然是如前所說由 (equiv1) 可得每一個元素都會被分到某一類. 另外由 (equiv2) 和 (equiv3) 知兩個不同類的集合不會有交集; 這是因為如果 b 在 A 類且在 B 類中, 則在 A 類中的任一元素 a 因和 b 是同類的故 $a \sim b$ 而 B 類中的任一元素 c 因也和 b 同類故 $b \sim c$. 故由 (equiv2) 和 (equiv3) 知 $a \sim c$. 也就是說 A 中的所有元素和 B 中的所有元素都同類. 這和 A 與 B 是不同類的假設相矛盾. 總而言之利用一個 equivalent relation 我們可以將一集合分割成兩兩互不相交的類別.

接下來我們就來探討同餘的分類法.

Definition 3.1.2. 給定一正整數 m, 如果 $a,b\in\mathbb{Z}$ 在除以 m 之下其餘數相同, 我們稱 a,b 在除以 m 之下是同餘的 (a is *congruent* to b modulo m), 且用符號 $a\equiv b \pmod m$ 來表示. 若 a 和 b 在除以 m 之下不同餘 (a is *incongruent* to b modulo m), 則用 $a\not\equiv b \pmod m$ 來表示.

要注意在談同餘時一定要先固定一個 m 才能說. 沒有 a 和 b 是同餘的說法, 你必須完整的說出 a 和 b 在除以什麼之下是同餘的才對.

雖然檢查 a,b 在除以 m 之下是否同餘, 依定義要檢查 a 和 b 除以 m 之餘數是否相同, 但事實上只要檢查 m 是否整除 $a-b$.

Lemma 3.1.3. 給定一正整數 m, 且 $a,b\in\mathbb{Z}$, 則 $a\equiv b \pmod m$ 若且唯若 $m|a-b$.

Proof. 依定義若 $a\equiv b \pmod m$ 則依定義存在 $h_1,h_2\in\mathbb{Z}$ 使得 $a=mh_1+r$ 及 $b=mh_2+r$ 其中 $0\le r<m$. 故得 $a-b=m(h_1-h_2)$ 也就是說 $m|a-b$.

反之假設 a,b 除以 m 之餘數分別為 r_1 及 r_2, 即分別存在 $h_1,h_2\in\mathbb{Z}$ 使得 $a=mh_1+r_1$ 及 $b=mh_2+r_2$, 其中 $0\le r_1,r_2<m$, 則知 $a-b=m(h_1-h_2)+(r_1-r_2)$. 故由假設 $m|a-b$ 得 $m|r_1-r_2$. 又因 $0\le r_1,r_2<m$, 知 $-m<r_1-r_2<m$, 故由 $m|r_1-r_2$ 得 $r_1=r_2$. □

我們可以利用 Lemma 3.1.3 很快的得到 congruent relation 是一個 equivalent relation.

Proposition 3.1.4. 給定一正整數 m, 則整數在除以 m 同餘的分類之下是一個 *equivalent relation.* 也就是說符合以下三個性質.

(1) 若 $a\in\mathbb{Z}$ 則 $a\equiv a \pmod m$.

(2) 若 $a\equiv b \pmod m$ 則 $b\equiv a \pmod m$.

(3) 若 $a\equiv b \pmod m$ 且 $b\equiv c \pmod m$, 則 $a\equiv c \pmod m$.

Proof. (1) 若 $a\in\mathbb{Z}$, 因 $a-a=0$, 得 $m|a-a$. 故由 Lemma 3.1.3 知 $a\equiv a \pmod m$.

(2) 若 $a\equiv b \pmod m$ 由 Lemma 3.1.3 知 $m|a-b$, 故由 $m|b-a$ 得證 $b\equiv a \pmod m$.

(3) 若 $a\equiv b \pmod m$ 且 $b\equiv c \pmod m$, 則知 $m|a-b$ 且 $m|b-c$. 故知 $m|(a-b)+(b-c)$, 即 $m|a-c$. 也就是說 $a\equiv c \pmod m$. □

由於同餘的概念用分類的看法是很好的分類且這樣的看法談論一些性質很方便, 今後我們經常會用 "a 和 b 在 modulo m 之下是同類" 的說法來表達: a 和 b 除以 m 之餘數相同.

既然用同餘的概念可將整數分類, 我們自然會問給定 $m\in\mathbb{N}$, 在 modulo m 之下可以分成幾類呢? 所有整數在除以 m 之下的餘數總共可能為 $0,1,\ldots,m-1$, 所以得知共有 m 類. 分類好後在每一類中我們可以挑一個代表元素來代表這一類, 且每類中僅挑出一個代表而不重複, 這樣所挑出的代表我們給它一個特別名稱.

Definition 3.1.5. 給定一正整數 m, 若集合 S 有 m 個元素, 其中元素在 modulo m 之下兩兩不同類, 則稱 S 是一個 *complete residue system modulo m.*

若 S 是一個 complete residue system modulo m, 則因整數在 modulo m 之下是一個 equivalent relation, 所以 S 中的元素都會被分到某一類, 而且又已知 S 中的元素兩兩不同類, 再加上已知 $\mathbb{Z}$ 在 modulo m 之下共能被分成 m 類, 所以由 S 的元素個數為 m 知, 每一類中都可在 S 中找到唯一的元素代表此類. 換言之, S 中的元素足以代表 $\mathbb{Z}$ 在 modulo m 之下之分類. 例如 $\{0,1,\ldots,m-1\}$ 就是一個常用的 complete residue system modulo m. 不過有時我們會因問題的需要選擇別種 complete residue system modulo m. 例如在證明 Euler ϕ 為 multiplicative (Proposition 2.3.4) 所用到 Lemma 2.3.3，就是說當 $b>1$ 且 $\gcd(a,b)=1$ 時，集合 $\{l,l+a,l+2a,\ldots,l+(b-1)a\}$ 是一個 complete residue system modulo b。

Question 3.1. 給定 $m\in\mathbb{N}$，假設 $S\subseteq\mathbb{Z}$ 且 S 的元素個數為 m. 試說明以下為等價：

(1) S 為 complete residue system modulo m.

(2) 對任意 $a\in\mathbb{Z}$ 皆存在 $s\in S$ 滿足 $a\equiv s \pmod m$.

(3) 對任意 $a\in\mathbb{Z}$ 皆存在唯一的 $s\in S$ 滿足 $a\equiv s \pmod m$.

利用同餘分類除了是一個 equivalent relation 之外, 還有許多很好的性質. 例如在下一節我們會介紹可以在各類之間定義運算. 另外在 modulo m 之下, 我們發現其實同類的元素和 m 之最大公因數其實是相同的.

Lemma 3.1.6. 給定一正整數 m, 若 $a\equiv b \pmod m$, 則 $\gcd(a,m)=\gcd(b,m)$.

Proof. 若 $a\equiv b \pmod m$, 由定義知 a 和 b 在除以 m 之下之餘數相同, 設其為 r. 故由 Lemma 1.3.1 知 $\gcd(a,m)=\gcd(r,m)=\gcd(b,m)$. □

特別的若 a 和 m 是互質的, 則在 modulo m 之下和 a 同類的元素都和 m 互質. 也就是說若 S 是一個 complete residue system modulo m, 只要找出 S 中有哪些元素和 m 互質, 那麼這些元素所代表的分類裡每個元素都和 m 互質. 在 modulo m 之下到底有幾類的元素會和 m 互質呢? 我們就考慮 $S=\{0,1,\ldots,m-1\}$ 這個 complete residue system modulo m 吧! S 中和 m 互質的元素個數依 Euler ϕ-function 的定義就是 $\phi(m)$ 個, 故知整數在 modulo m 之下共有 $\phi(m)$ 類的元素和 m 是互質的. 有時在處理問題時我們需要將這 $\phi(m)$ 類的代表元素列出, 所以我們也給它一個特別名稱.

Definition 3.1.7. 給定一正整數 m, 若集合 S 有 $\phi(m)$ 個元素, 其中的元素皆與 m 互質且在 modulo m 之下兩兩不同類, 則稱 S 是一個 *reduced residue system modulo m*.

當 m 是一質數 p 時, $\{1,\ldots,p-1\}$ 就是最常用的 reduced residue system modulo p.

Question 3.2. 給定 $m\in\mathbb{N}$，假設 $S\subseteq\mathbb{Z}$ 且 S 中的元素皆與 m 互質。已知 S 的元素個數為 $\phi(m)$，試說明以下為等價：

(1) S 為 reduced residue system modulo m.

(2) 對任意滿足 $\gcd(a,m)=1$ 的整數 a 皆存在 $s\in S$ 滿足 $a\equiv s \pmod m$.

(3) 對任意滿足 $\gcd(a,m)=1$ 的整數 a 皆存在唯一的 $s\in S$ 滿足 $a\equiv s \pmod m$.

Exercise 3.1. 假設 $p \geq 5$ 是一個質數, 試證明

$$\{\frac{-(p-1)}{2}, \frac{-(p-3)}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-3}{2}, \frac{p-1}{2}\}$$

是一個 reduced residue system modulo p.

3.2. 同餘的運算

同餘分類最重要的性質就是, 各類之間可以如整數一般作加法以及乘法的運算 (在有些情況甚至可以作除法).

給定 $m \in \mathbb{N}$, 在 modulo m 之下我們將同一類的元素看成是同樣的東西 (也就是將一整類的元素看成是一個元素), 想看看各類之間要如何相加相乘呢? 很自然的想法是在要相加的兩類中各挑一個代表元素, 然後相加相乘看看落於哪一類. 不過這會碰到一個問題就是每一類中大家挑的代表元素若不同會不會相加相乘後所得結果不同呢? 例如在 modulo 5 之下, 我們要將除以 5 餘數為 2 的這一類和餘數為 3 的這一類相加或相乘. 若餘數為 2 和 3 的這兩類我們分別挑 2 和 3 來代表, 那麼由 $2+3=5$ 及 $2\times 3=6$ 得到相加相乘後會分別落在餘 0 和餘 1 的這兩類中. 如果挑不同的代表元素呢? 比方說餘 2 和餘 3 的這兩類我們分別挑 7 和 -12 當代表, 結果 $7+(-12)=-5$ 及 $7\times(-12)=-84$, 我們仍得到相加後落於除以 5 餘 0 這一類, 而相乘後落於除以 5 餘 1 這一類, 和前面結果一致. 我們不能由這個例子就認為這一定對, 需要想個方法來說明這是事實而不是巧合.

Lemma 3.2.1. 給定 $m \in \mathbb{N}$, 若 $a, b \in \mathbb{Z}$ 滿足 $a \equiv b \pmod{m}$, 則對任意 $c \in \mathbb{Z}$ 皆有

$$a+c \equiv b+c \pmod{m} \quad \text{and} \quad ac \equiv bc \pmod{m}.$$

Proof. 由假設 $a \equiv b \pmod{m}$ 知 $m|a-b$. 故得 $m|(a+c)-(b+c)$, 也就是說 $a+c \equiv b+c \pmod{m}$. 另一方面由於 $m|(a-b)c$ 故知 $m|ac-bc$, 得證 $ac \equiv bc \pmod{m}$. □

Lemma 3.2.1 告訴我們兩個同類的數分別加上同一個數後所得之數也會同類. 同類的數同乘一個數後所得之數也同類. 依此我們就可以得到兩個同類的數分別加上 (或乘上) 另兩個同類的數其結果仍會同類.

Proposition 3.2.2. 給定 $m \in \mathbb{N}$, 若 $a, b, c, d \in \mathbb{Z}$ 滿足 $a \equiv b \pmod{m}$ 且 $c \equiv d \pmod{m}$, 則

$$a+c \equiv b+d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}.$$

Proof. 因 $a \equiv b \pmod{m}$, 由 Lemma 3.2.1 知 $a+c \equiv b+c \pmod{m}$. 同理又因 $c \equiv d \pmod{m}$ 知 $b+c \equiv b+d \pmod{m}$, 故利用同餘是 equivalent relation (即 Proposition 3.1.4(3)) 知 $a+c \equiv b+d \pmod{m}$.

同樣的, 由 $a \equiv b \pmod{m}$ 及 $c \equiv d \pmod{m}$ 分別得 $ac \equiv bc \pmod{m}$ 及 $bc \equiv bd \pmod{m}$, 故知 $ac \equiv bd \pmod{m}$. □

由此定理, 我們以後要計算 1752 乘以 388 除以 5 之餘數, 我們不必將它們乘開後再看其除以 5 之餘數為何. 我們可以利用 $1752 \equiv 2 \pmod{5}$ 以及 $388 \equiv 3 \pmod{5}$ 很快的得到 $1752 \times 388 \equiv 6 \equiv 1 \pmod{5}$.