Proposition 3.1.4 (即 congruence relation 是 equivalent relation) 告訴我們當固定 $m\in\mathbb{N}$ 時 "$\equiv$" 有和等號相同的法則. 另一方面在 Lemma 3.2.1 中若令 $c=-1$, 則當 $a\equiv b \pmod m$ 時我們有 $-a\equiv -b \pmod m$. 所以套用 Proposition 3.2.2 知我們可以將 $\equiv$ "看成" 是等號 (即將同餘的元素看成是相同) 而將同餘類的運算如一般整數作加, 減, 乘的運算. 例如在計算 5742 除以 11 的餘數時, 我們可以寫成 $5742=5\times10^3+7\times10^2+4\times10+2$. 由於 $10\equiv-1 \pmod{11}$ 故得 $5742\equiv5\times(-1)^3+7\times(-1)^2+4\times(-1)+2\equiv-5+7-4+2\equiv0 \pmod{11}$. 也就是說 5742 可以被 11 整除, 這和我們中學時代所學判別 11 的倍數法則相同. 同理判別 9 的倍數法則也可由 $10\equiv1 \pmod 9$ 而得. 你也可以利用 $10\equiv3 \pmod 7$ 整理出一套判別 7 的倍數之法則 (當然會複雜多了).

關於同餘有兩點要特別注意: 首先, 在 modulo 不同的數之下所得的分類法不同, 所以不能將 $\equiv$ 混用. 例如若 $a=3$, 我們可以說 $a\equiv3 \pmod 5$ 且 $a\equiv3 \pmod 7$, 但你不能因為 $a^2\equiv3^2\equiv4 \pmod 5$ 而說 $a^2\equiv4 \pmod 7$. 一般來說要處理 modulo 不同的整數 m,n 的問題，我們可以考慮 modulo m,n 的最小公倍數再處理。例如當 m,n 互質時，若 $a\equiv r \pmod m$ 且 $a\equiv r \pmod n$，則因 $m\mid a-r$ 且 $n\mid a-r$ 以及 $\gcd(m,n)=1$，可得 $mn\mid a-r$ (Proposition 1.2.6(2))，所以我們可利用 $a\equiv r \pmod{mn}$ 來處理。處理 modulo 不同整數的問題有點複雜，我們以後再探討。

另外要注意的就是在一般等式中的除 (約) 在 congruence 並不一定適用. 也就是說若 $a\neq0$ 且 $ab=ac$, 我們知 $b=c$; 但這在 congruence 的情況有可能出問題. 例如當 $a=2,b=2,c=5$ 在 modulo 6 之下我們有 $a\neq0 \pmod 6$ 且 $ab\equiv ac \pmod 6$, 但很明顯的 $b\not\equiv c \pmod 6$. 所以在處理 congruence 的問題時要用除法消去一個數時要特別注意. 以下定理告訴我們何時可消, 何時不可消.

Proposition 3.2.3. 給定 $m\in\mathbb{N}$ 且假設 $a,b,c\in\mathbb{Z}$. 令 $d=\gcd(m,a)$ 則 $ab\equiv ac \pmod m$ 若且唯若 $b\equiv c \pmod{m/d}$.

Proof. 因 $d=\gcd(m,a)$, 我們令 $m=m'd$ 且 $a=a'd$, 由 Corollary 1.2.11 知 $\gcd(m',a')=1$.

現假設 $ab\equiv ac \pmod m$, 即 $m|ab-ac$. 因此由 Lemma 1.1.2(2) 知 $(m/d)|(a/d)(b-c)$, 即 $m'|a'(b-c)$. 故因 $\gcd(m',a')=1$ 利用 Proposition 1.2.6(1) 得證 $m'|b-c$, 即 $b\equiv c \pmod{m/d}$.

反之, 若 $b\equiv c \pmod{m/d}$, 即 $m'|b-c$. 因此由 Lemma 1.1.2(1) 得 $dm'|d(b-c)$, 即 $m|d(b-c)$. 也就是說 $db\equiv dc \pmod m$. 故由 Lemma 3.2.1 知 $a'db\equiv a'dc \pmod m$, 得證 $ab\equiv ac \pmod m$. □

例如之前的例子, 因為 $m=6$ 且 $a=2$, 得 $\gcd(m,a)=2$. 故由 $ab\equiv ac \pmod 6$ 得 $b\equiv c \pmod 3$. 事實上, 上例中 $b=2,c=5$, 我們確實有 $2\equiv5 \pmod 3$.

到底在何時才能把 a 消掉且保持原來 modulo m 的 congruence 呢? 由 Proposition 3.2.3 我們知只有在 $\gcd(m,a)=1$, 即 m 和 a 互質時才可保證對. 我們將這個重要的性質寫下.

Corollary 3.2.4. 給定 $m\in\mathbb{N}$ 且假設 $a,b,c\in\mathbb{Z}$. 若 m 和 a 互質, 則 $ab\equiv ac \pmod m$ 若且唯若 $b\equiv c \pmod m$.

其實若限制在整數時, 若 $a \neq 0$ 且 $ab = ac$ 可將 a 消去推得 $b = c$, 正確來說不能用 "除" 的概念來說, 而是用整數 $a \neq 0$ 且 $b \neq 0$ 則 $ab \neq 0$ 的性質得到. 這個概念在 congruence 的情況就不一定對, 例如 $2 \not\equiv 0 \pmod 6$ 且 $3 \not\equiv 0 \pmod 6$ 但是 $2 \times 3 \equiv 0 \pmod 6$. 這也是一般來說在 congruence 不能用約的方法消去的主要原因. 然而在考慮有理數時, 若 $a \neq 0$, 因為必存在另一有理數 a^{-1} 使得 $a \cdot a^{-1} = 1$, 所以若 $ab = bc$, 則兩邊同乘 a^{-1}, 可得 $b = c$. 這就是用除法 "約" 的概念消去 a. 由於有理數中對任意非 0 元素 a, 其乘法反元素 (即 a^{-1}) 必存在, 使得我們在解有理數的方程式時更容易找到解. 在一般整數時雖然僅有 ± 1 其乘法反元素為整數, 但在討論 congruence 時有更多元素其乘法反元素會存在.

Proposition 3.2.5. 給定 $m \in \mathbb{N}$, 假設 $a \in \mathbb{Z}$, 則存在 $b \in \mathbb{Z}$ 滿足 $ab \equiv 1 \pmod m$ 若且唯若 a 和 m 互質.

Proof. 假設 $b \in \mathbb{Z}$ 滿足 $ab \equiv 1 \pmod m$, 即 $m | ab - 1$. 令 $d = \gcd(m, a)$, 可得 $d | m$ 且 $d | ab$. 故利用 $m | ab - 1$ 及 $d | m$ 可得 $d | ab - 1$, 再利用 $d | ab$ 得 $d | 1$. 也就是說 a 和 m 互質.

反之, 若 a 和 m 互質, 即 $\gcd(m, a) = 1$, 則由 Corollary 1.2.4 知存在 $r, s \in \mathbb{Z}$ 使得 $mr + as = 1$. 故令 $b = s$, 我們有 $m | ab - 1$, 亦即 $ab \equiv 1 \pmod m$. □

最後要強調, 當 a 和 m 互質時雖然有無窮多的整數 b 會滿足 $ab \equiv 1 \pmod m$, 但是這樣的 b 在 modulo m 之下是唯一的. 也就是說若 $c \in \mathbb{Z}$ 亦滿足 $ac \equiv 1 \pmod m$, 則由於 $ab \equiv 1 \equiv ac \pmod m$ 以及 $\gcd(m, a) = 1$, 套用 Corollary 3.2.4 我們得知 $b \equiv c \pmod m$. 有此唯一性, 我們特別稱 b 為 a 在 modulo m 之下的乘法反元素.

Exercise 3.2. 假設 $m \in \mathbb{N}$ 且 n 的 10 進位表示為 $mabcabc$, 其中 $a, b, c \in \mathbb{N}$ 且 $0 \leq a, b, c \leq 9$ (例如 $m = 37$, $n = 37123123$). 試證明 $m \equiv n \pmod 7$ 且 $m \equiv n \pmod{13}$.

Exercise 3.3. 假設 $a \in \mathbb{Z}$ 且 $2 \nmid a$.

(1) 試證明 $a^2 \equiv 1 \pmod 8$.

(2) 試說明並列出 a^2 在 modulo 24 之下所有可能的同餘類.

(3) 若再假設 $3 \nmid a$, 試證明 $a^2 \equiv 1 \pmod{24}$. (Hint：$a^2 \equiv 1 \pmod 8$ 且 $a^2 \equiv 1 \pmod 3$)

Exercise 3.4. 已知 $\gcd(58, 63) = 1$, 故知 58 在 modulo 63 之下有乘法反元素 (即存在 $a \in \mathbb{Z}$ 使得 $58 \times a \equiv 1 \pmod{63}$). 以下是有關乘法反元素之問題.

(1) 試利用輾轉相除法找出 $58x + 63y = 1$ 的一組整數解. 並依此找出 58 在 modulo 63 之下的乘法反元素.

(2) 試找出 $b \in \mathbb{Z}$ 且滿足 $1 \leq b \leq 63$, 使得 $58 \times b \equiv 47 \pmod{63}$.

3.3. Euler's Theorem

一般在解方程式時, 我們經常需要乘法反元素來幫忙. 所以當 $m \in \mathbb{N}$, $a \in \mathbb{Z}$ 且 $\gcd(a, m) = 1$ 時, 若能確實知道哪些 $b \in \mathbb{Z}$ 會滿足 $ab \equiv 1 \pmod m$ 將是很有用的. 由 Proposition 3.2.5 的

證明中我們知可以利用輾轉相除法解 $mx+ay=1$ 的整數解來得到 b, 但這要在 m 和 a 皆是具體的數時才能操作. 我們將利用 Euler's Theorem 對一般的 m,a 都能將 b 確實找到.

給定 $m\in\mathbb{N}$, 若 $a,b\in\mathbb{Z}$ 滿足 $ab\equiv 1 \pmod m$, 則由 Proposition 3.2.5 知 a 和 b 皆與 m 互質. 換言之, 我們只要考慮和 m 互質的數即可, 所以我們自然考慮 reduced residue system modulo m.

Lemma 3.3.1. 給定 $m\in\mathbb{N}$, 考慮 $a\in\mathbb{Z}$ 滿足 $\gcd(m,a)=1$. 若 $\{r_1,\dots,r_{\phi(m)}\}$ 是一個 *reduced residue system modulo m*, 則 $\{ar_1,\dots,ar_{\phi(m)}\}$ 也是一個 *reduced residue system modulo m*.

Proof. 複習一下, $\{r_1,\dots,r_{\phi(m)}\}$ 是一個 reduced residue system modulo m 表示 $\gcd(m,r_i)=1$ 且對任意 $i\neq j$, 皆有 $r_i\not\equiv r_j \pmod m$. 現要證明 $\{ar_1,\dots,ar_{\phi(m)}\}$ 也是 reduced residue system modulo m, 我們需要證明 $\gcd(m,ar_i)=1$ 且對任意 $i\neq j$ 皆有 $ar_i\not\equiv ar_j \pmod m$.

現假設 $\gcd(m,ar_i)\neq 1$, 即存在一質數 p 滿足 $p|m$ 且 $p|ar_i$. 因 p 是質數, 故由 Lemma 1.5.2 得 $p|a$ 或 $p|r_i$. 換言之, p 為 m,a 的公因數或是 m,r_i 的公因數. 此和 $\gcd(m,a)=1$ 且 $\gcd(m,r_i)=1$ 相矛盾, 故得證 $\gcd(m,ar_i)=1$.

另一方面, 若 $i\neq j$ 且 $ar_i\equiv ar_j \pmod m$, 則由 $\gcd(m,a)=1$, 利用 Corollary 3.2.4 得 $r_i\equiv r_j \pmod m$. 此和 $r_i\not\equiv r_j \pmod m$ 矛盾, 故得證 $ar_i\not\equiv ar_j \pmod m$. □

前面提過, 給定 $m\in\mathbb{N}$, 利用除以 m 同餘的分類, 我們可以將與 m 互質的數分成 $\phi(m)$ 類. 而將每一類中挑出一代表元素所成之集合就是一個 reduced residue system modulo m. 今假若 $S=\{a_1,\dots,a_{\phi(m)}\}$ 和 $T=\{b_1,\dots,b_{\phi(m)}\}$ 皆為 reduced residue system modulo m, 任取 $a_i\in S$, 由於它代表與 m 互質的某一同餘類, 而 T 中也有一元素是在和 a_i 同類的元素中挑出. 換言之, 存在 $b_j\in T$ 滿足 $a_i\equiv b_j \pmod m$. 又由於這些 b_j 兩兩皆不同類, 所以 S 和 T 中元素在 modulo m 之下有一對一的對應關係. 也就是說經過適當的排序, 我們有 $a_i\equiv b_i \pmod m$. 因此得 $a_1\cdots a_{\phi(m)}\equiv b_1\cdots b_{\phi(m)} \pmod m$. 利用這個結果我們可以得證 Euler's Theorem.

Theorem 3.3.2 (Euler's Theorem)**.** 給定 $m\in\mathbb{N}$, 若 $a\in\mathbb{Z}$ 滿足 $\gcd(m,a)=1$, 則

$$a^{\phi(m)}\equiv 1 \pmod m.$$

Proof. 取 $S=\{r_1,\dots.r_{\phi(m)}\}$ 為一個 reduced residue system modulo m. 首先我們證明 $\gcd(m,r_1\cdots r_{\phi(m)})=1$. 若 $\gcd(m,r_1\cdots r_{\phi(m)})\neq 1$, 即存在一質數 p 使得 $p|m$ 且 $p|r_1\cdots r_{\phi(m)}$. 利用 Corollary 1.5.3 知存在 $r_i\in S$ 使得 $p|r_i$, 也就是說 $\gcd(m,r_i)\neq 1$. 此和 S 是 reduced residue system modulo m 且 $r_i\in S$ 相矛盾, 故得證 $\gcd(m,r_1\cdots r_{\phi(m)})=1$.

現由於 $\gcd(m,a)=1$, 故利用 Lemma 3.3.1 知 $\{ar_1,\dots,ar_{\phi(m)}\}$ 也是一個 reduced residue system modulo m, 因此得

$$r_1\cdots r_{\phi(m)}\equiv(ar_1)\cdots(ar_{\phi(m)})\equiv a^{\phi(m)}(r_1\cdots r_{\phi(m)}) \pmod m.$$

再因為 $\gcd(m,r_1\cdots r_{\phi(m)})=1$, 故利用 Corollary 3.2.4 得證 $a^{\phi(m)}\equiv 1 \pmod m$. □

給定 $m \in \mathbb{N}$ 及 $a \in \mathbb{Z}$ 滿足 $\gcd(m,a) = 1$, 若令 $b = a^{\phi(m)-1}$, 則利用 Euler's Theorem 得知 $ab \equiv a^{\phi(m)} \equiv 1 \pmod{m}$. 因此我們找到了 a 在 modulo m 之下的乘法反元素.

Corollary 3.3.3. 給定 $m \in \mathbb{N}$, 若 $a \in \mathbb{Z}$ 滿足 $\gcd(m,a) = 1$, 則令 $b = a^{\phi(m)-1}$, 會滿足 $ab \equiv ba \equiv 1 \pmod{m}$.

特別地, 當 m 是一個質數 p 時, Euler's Theorem 就是所謂的 Fermat's Little Theorem. 我們特別將它寫下來.

Theorem 3.3.4 (Fermat's Little Theorem)**.** 給定一質數 p, 若 $a \in \mathbb{Z}$ 滿足 $p \nmid a$, 則

$$a^{p-1} \equiv 1 \pmod{p}.$$

特別地, 若令 $b = a^{p-2}$, 則 $ab \equiv ba \equiv 1 \pmod{p}$.

Proof. 因 p 是一質數, 由 $p \nmid a$ 之假設知 $\gcd(p,a) = 1$. 又此時 $\phi(p) = p-1$, 故直接套用 Theorem 3.3.2 得證 $a^{p-1} \equiv 1 \pmod{p}$. □

當 $p|a$ 時 Ferma's Little Theorem 並不對, 因為此時 $a \equiv 0 \pmod{p}$, 故 $a^{p-1} \equiv 0 \pmod{p}$. 不過我們可以推導出下一個對任意整數 a 皆成立的式子.

Corollary 3.3.5. 給定一質數 p, 則對任意整數 a 皆滿足

$$a^p \equiv a \pmod{p}.$$

Proof. 因為 p 是質數所以對任意 $a \in \mathbb{Z}$, 我們可以分成 $p|a$ 和 $p \nmid a$ 之情況處理. 當 $p|a$ 時, 由於 $a \equiv 0 \pmod{p}$, 故得 $a^p \equiv 0 \equiv a \pmod{p}$. 當 $p \nmid a$ 時, 由 Theorem 3.3.4 知 $a^{p-1} \equiv 1 \pmod{p}$, 故兩邊乘上 a 可得 $a^p \equiv a \pmod{p}$. □

Exercise 3.5. 以下是有關 Euler's Theorem 的應用.

(1) 試求 99^{999999} 除以 26 的餘數.

(2) 假設 $n \in \mathbb{Z}$ 且 $3 \nmid n$. 試證明 $9 \mid n^7 - n$ 並依此證明 $n^7 \equiv n \pmod{63}$.

(3) 假設 $m,n \in \mathbb{N}$ 且 $\gcd(m,n) = 1$. 試證明 $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$.

Exercise 3.6. 以下是有關 Fermat's Little Theorem 的應用.

(1) 試證明 11 整除 $456^{654} + 123^{321}$.

(2) 假設 p 是一質數且 $a,b \in \mathbb{Z}$。證明以下是等價的：
- $a \equiv b \pmod{p}$
- $a^p \equiv b^p \pmod{p}$
- $a^p \equiv b^p \pmod{p^2}$

(3) 假設 p,q 是相異質數且滿足 $p-1 \mid q-1$. 試證明若 $a \in \mathbb{Z}$ 且 $\gcd(a,pq) = 1$, 則 $a^{q-1} \equiv 1 \pmod{pq}$.

3.4. Wilson's Theorem

當 p 是一個質數時, 若 $p \nmid a$, 則 Fermat's Little Theorem 告訴我們 a^{p-2} 在 modulo p 之下是 a 的乘法反元素. 雖然 a 的乘法反元素在 modulo p 之下是唯一的, Wilson's Theorem 給了我們在 modulo p 之下 a 的乘法反元素的另一種表法.

給定 $m \in \mathbb{N}$, 對於任意和 m 互質的整數 a, 由 Proposition 3.2.5 知都可以找到一個和 m 互質的整數 b 使得 $ab \equiv 1 \pmod{m}$, 我們也提及雖然這樣的 b 並不唯一, 但在 modulo m 的分類之下它會是唯一的. 也就是說只有在除以 m 之下和 b 同餘的整數才會符合. 這種在 modulo m 之下乘法反元素的存在唯一性用 modulo m 之下的 reduced residue system 最容易表達.

Lemma 3.4.1. 給定 $m \in \mathbb{N}$, 假設 $S = \{r_1, \ldots, r_{\phi(m)}\}$ 是一個 *reduced residue system modulo* m. 則對於任意 $r_i \in S$ 皆存在唯一的 $r_j \in S$ 使得 $r_i r_j \equiv 1 \pmod{m}$.

Proof. 因為 S 是一個 reduced residue system modulo m, 每一個 S 中的元素 r_i 皆和 m 互質, 故利用 Proposition 3.2.5 知存在 $b \in \mathbb{Z}$ 使得 $r_i b \equiv 1 \pmod{m}$. 由於 b 和 m 也是互質的, 故由 S 是一個 reduced residue system modulo m 之定義知必存在 $r_j \in S$ 和 b 在 modulo m 之下是同類的, 也就是說 $b \equiv r_j \pmod{m}$. 因此由 Lemma 3.1.3 知, $r_i r_j \equiv r_i b \equiv 1 \pmod{m}$. 證得存在性.

對於唯一性, 我們先假設 $r_j, r_k \in S$ 皆滿足 $r_i r_j \equiv 1 \pmod{m}$ 以及 $r_i r_k \equiv 1 \pmod{m}$. 因此得 $r_i r_j \equiv r_i r_k \pmod{m}$. 但由於 $\gcd(m, r_i) = 1$, 利用 Corollary 3.2.4 得 $r_j \equiv r_k \pmod{m}$. 但 S 是 reduced residue system modulo m 表示 S 中相異的元素在 modulo m 之下應是不同類的, 故由 $r_j \equiv r_k \pmod{m}$ 知 $r_j = r_k$. 得證唯一性. □

例如 $S = \{1,2,3,4,5,6,7,8,9,10\}$ 是一個 reduced residue system modulo 11, 在 modulo 11 之下我們有

$$1 \times 1 \equiv 2 \times 6 \equiv 3 \times 4 \equiv 5 \times 9 \equiv 7 \times 8 \equiv 10 \times 10 \equiv 1 \pmod{11}.$$

在這個例子, S 中除了 1 和 10 以外其他的元素皆需與另外的元素相乘, 這在 modulo 一般的質數都是對的.

Lemma 3.4.2. 給定一質數 p. 則 $a \in \mathbb{Z}$ 滿足 $a^2 \equiv 1 \pmod{p}$ 若且唯若 $a \equiv \pm 1 \pmod{p}$.

Proof. 首先若 $a \equiv \pm 1 \pmod{p}$, 則 $a^2 \equiv (\pm 1)^2 \pmod{p}$. 得證 $a^2 \equiv 1 \pmod{p}$.

反之, 若 $a^2 \equiv 1 \pmod{p}$, 表示 $p | a^2 - 1$, 也就是說 $p | (a-1)(a+1)$, 故因 p 是質數, 利用 Lemma 1.5.2 得 $p | a-1$ 或 $p | a+1$. 也就是說 $a \equiv 1 \pmod{p}$ 或 $a \equiv -1 \pmod{p}$. □

要注意 Lemma 3.4.2 在 modulo 一般的非質數之下就不一定對了, 例如在 modulo 15 之下除了 1 和 14 外, 還有 4 會滿足 $4^2 \equiv 1 \pmod{15}$, 而且很顯然的 $4 \not\equiv \pm 1 \mod 15$. 所以要利用 Lemma 3.4.2, 我們必須限定在質數的情形, 此時我們可以得到 Wilson's Theorem.

Theorem 3.4.3 (Wilson's Theorem)**.** 給定一質數 p. 設 $\{r_1,\dots,r_{p-1}\}$ 為一 *reduced residue system modulo* p. 則

$$r_1\cdots r_{p-1}\equiv -1 \pmod{p}.$$

特別地, 我們有

$$(p-1)!\equiv -1 \pmod{p}.$$

Proof. 若 $p=2$, 則 modulo 2 之下的 reduced residue system 為 $\{r_1\}$ 一個元素, 其中 $r_1\equiv 1 \pmod 2$. 但在 modulo 2 之下我們有 $1\equiv -1 \pmod 2$, 故得證 $r_1\equiv -1 \pmod 2$.

現考慮 $p>2$ 的情形, 令 $S=\{r_1,\dots,r_{p-1}\}$ 由於 $\gcd(p,1)=\gcd(p,-1)=1$ 且 $1\not\equiv -1 \pmod p$ (否則 $p|2$), 故分別存在 $r_i,r_j\in S$ 其中 $r_i\neq r_j$ 滿足 $r_i\equiv 1 \pmod p$ 且 $r_j\equiv -1 \pmod p$. 因此不失一般性, 我們可假設 $r_1\equiv 1 \pmod p$ 且 $r_2\equiv -1 \pmod p$. 現考慮 $r_i\in S$, 其中 $3\le i\le p-1$. 依 Lemma 3.4.1 知存在唯一的 $r_j\in S$ 使得 $r_ir_j\equiv 1 \pmod p$. 因為 $r_i\not\equiv\pm 1 \pmod p$, 故知 $r_j\not\equiv\pm 1 \pmod p$, 也就是說 $3\le j\le p-1$. 又若 $r_i=r_j$, 會導致 $r_i^2\equiv 1 \pmod p$, 這與 Lemma 3.4.2 相矛盾, 故知 $i\neq j$. 也就是說在 $T=\{r_3,\dots,r_{p-1}\}$ 中任取一元素 r_i 必可找到唯一的另一元素 $r_j\in T$ 使得 $r_ir_j\equiv 1 \pmod p$. 因此我們可以對 T 中這 $p-3$ 個元素兩兩配對 (注意 p 是奇數), 使得每一對中元素相乘後除以 p 會餘 1. 也就是說 $r_3\cdots r_{p-1}\equiv 1 \pmod p$. 因此我們得證

$$r_1r_2r_3\cdots r_{p-1}\equiv r_1r_2\equiv -1 \pmod{p}.$$

最後由於 $\{1,2,\dots,p-1\}$ 是一個 modulo p 的 reduced residue system, 故知

$$1\times 2\times\cdots\times(p-1)=(p-1)!\equiv -1 \pmod{p}.$$

□

若 p 是一質數且 a 是和 p 互質的整數, 我們可以利用 Wilson's Theorem 找到在 modulo p 之下, a 的乘法反元素. 由於當 $a\equiv\pm 1 \pmod p$ 時 $a^2\equiv 1 \pmod p$, 也就是說 a 本身在 modulo p 之下是自己的乘法反元素, 所以我們僅討論 $a\not\equiv\pm 1 \pmod p$ 的情況.

Corollary 3.4.4. 給定一質數 p 及 $a\in\mathbb{Z}$ 滿足 $p\nmid a$. 假設 $a\equiv r \pmod p$, 其中 $2\le r\le p-2$. 若令

$$b=(p-2)!/r$$

則 $ab\equiv 1 \pmod p$.

Proof. 由於 $2\le r\le p-2$, 即 $r\mid(p-2)!$, 我們知 $b=(p-2)!/r$ 是一個整數. 此時

$$ab\equiv r((p-2)!/r)\equiv (p-2)! \pmod{p}$$

又由於 $(p-1)!=(p-1)\cdot(p-2)!$ 且 $p-1\equiv -1 \pmod p$, 故得證

$$ab\equiv (p-2)!\equiv -((p-1)!)\equiv 1 \pmod{p}.$$

□

我們仍要強調一下雖然 Lemma 3.4.1 在一般的 $m \in \mathbb{N}$ 都成立, 但 Lemma 3.4.2 需限制在質數時才成立, 所以 Wilson's Theorem 在 modulo 一般的 m 並不一定成立. 也就是說若 $\{r_1, \ldots, r_{\phi(m)}\}$ 是一個 reduced residue system modulo m, 並不一定可以得 $r_1 \cdots r_{\phi(m)} \equiv -1 \pmod{m}$. 例如在 modulo 15 之下我們知還有 4 和 -4 滿足 $4^2 \equiv (-4)^2 \equiv 1 \pmod{15}$, 所以利用 Theorem 3.4.3 的證明方法 (或直接計算) 我們可得, 若 $\{r_1, \ldots, r_8\}$ 是一個 reduced residue system modulo 15, 則 $r_1 \cdots r_8 \equiv 1 \pmod{15}$. 雖然利用 Theorem 3.4.3 的方法我們可以將 Wilson's Theorem 推廣到一般 m 的情形, 不過此時對一個 modulo m 的 reduced residue system $\{r_1, \ldots, r_{\phi(m)}\}$ 滿足 $r_i^2 \equiv 1 \pmod{m}$ 的 r_i 會有很多種情形, 討論起來較複雜, 在這裡我們就不多探討了.

Exercise 3.7. 假設 p 是一個奇質數.

(1) 試證明若 $a \in \mathbb{N}$ 滿足 $(p-1)/2 < a < p$, 則存在 $b \in \mathbb{N}$ 滿足 $1 \le b \le (p-1)/2$ 使得 $a \equiv -b \pmod{p}$. 依此以及 Wilson's Theorem 證明

$$(\frac{p-1}{2}!)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

(2) 試證明若 a 是奇數滿足 $1 \le a < p-1$, 則存在偶數 b 滿足 $1 < b \le p-1$ 使得 $a \equiv -b \pmod{p}$. 依此以及 Wilson's Theorem 證明

$$1^2 3^2 5^2 \cdots (p-4)^2 (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

(3) 利用前兩小題結果證明當 $p \equiv 1 \pmod{4}$ 時 congruence equation $x^2 \equiv -1 \pmod{p}$ 有解.

Exercise 3.8. 假設 $m \in \mathbb{N}$ 且 $m > 2$. 若 $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ 是一個 modulo m 之下的 reduced residue system, 試證明 $r_1 + r_2 + \cdots + r_{\phi(m)} \equiv 0 \pmod{m}$.

3.5. Chinese Remainder Theorem

在 Mod 不同整數 m,n 之下同餘的分類方式不同，所以在 mod m 之下同餘的整數在 mod n 不同餘的情況有可能發生。之後我們探討 congruence equation 需要處理這方面的問題，在本節我們介紹其基本概念。

我們觀察 modulo 2 之下的 complete residue system $\{0,1\}$，其中 0 代表的是偶數、1 代表的是奇數；但在 modulo 4 之下的 complete residue system $\{0,1,2,3\}$，其中 0 代表的是 4 的倍數，也就是在 modulo 2 之下與 0 同類的，在 modulo 4 之下未必同類，例如 $2,6,10,\ldots$ 等，就被分到另一類 2。同樣的 modulo 2 之下與 1 同類的，也被分成 $\{1,5,9,\ldots\}$、$\{3,7,11,\ldots\}$，即 1、3 這兩類。這裡還有一個重點就是在 modulo 2 之下不同類的，在 modulo 4 之下也不會是同類。這現象可推廣到 modulo m 以及 modulo km 的情況，也就是在 modulo m 的 complete residue system $\{0,1,\ldots,i,\ldots,m-1\}$ 中，與 i 同類的，在 modulo km 之下會被分成 $i, i+m, i+2m, \ldots, i+(k-1)m$ 這 k 類。我們有以下的結果：

Proposition 3.5.1. 給定大於 1 的整數 m,k。若 $\{r_1,\dots,r_m\}$ 是 *modulo* m 之下的 *complete residue system*，則

$$S=\{r_1,\dots,r_m,r_1+m,\dots,r_m+m,\dots,r_1+(k-1)m,\dots,r_m+(k-1)m\}$$

是 *modulo* km 之下的 *complete residue system.*

Proof. 由餘 S 有 km 個元素，我們僅要說明在 modulo km 之下，這 km 個元素皆不同餘即可。假設 $r_i+jm\equiv r_{i'}+j'm \pmod{km}$，其中 $1\le i,i'\le m$ 且 $1\le j,j'\le k$. 由 $km\mid(r_i-r_{i'})+(j-j')m$，可知 $m\mid r_i-r_{i'}$。因 $\{r_1,\dots,r_m\}$ 是 complete residue system modulo m, 故得 $i=i'$。因此知 $km\mid(j-j')m$，即 $k\mid j-j'$。然而 $-k<j-j'<k$，故得 $j-j'=0$。也就是說 S 中不同元素在 modulo km 之下不會同餘，得證 S 是一個 complete residue system modulo km。 □

通常我們會把 modulo m 的 complete residue system 用 $\mathbb{Z}/m\mathbb{Z}$ 來表示。若熟悉函數概念，可以看出 Proposition 3.5.1 定義了一個 $\mathbb{Z}/km\mathbb{Z}$ 到 $\mathbb{Z}/m\mathbb{Z}$ 的函數，這個函數是 k to 1 且為 onto。

當 m,n 沒有倍數關係，modulo m 和 modulo n 的同餘類關係就沒有像前面一樣有相容的關係。例如在 modulo 2 之下，和 0 同類的 2、4、6 在 modulo 3 之下分別被分到不同類 2、1、0，同樣的在 modulo 2 之下，和 1 同類的 1、3、5 在 modulo 3 之下分別被分到不同類 1、0、2。如何處理這種互相交錯的情況呢？很自然的就是將它們用共同可以相容的方式分類，即考慮 modulo 它們的最小公倍數 6。我們可以發現在 modulo 6 之下，與 1 同類的會是在 modulo 2 和 modulo 3 之下皆與 1 同類的整數，其他情況整理如下表：

mod 6	mod 2	mod 3
0	0	0
1	1	1
2	0	2
3	1	0
4	0	1
5	1	2

若從剛才函數的概念來看：當 m,n 互質，我們可以得到一個 $\mathbb{Z}/mn\mathbb{Z}$ 到 $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ 的 one-to-one 且 onto 的函數。這可以推廣到更一般的情況，即 Chinese Remainder Theorem，在整數論的說法如下：

Theorem 3.5.2 (Chinese Remainder Theorem)**.** 給定一組 $m_1,\dots,m_r\in\mathbb{N}$ 其中這些 m_i 皆兩兩互質（即當 $i\neq j$ 時, $\gcd(m_i,m_j)=1$）. 則對任意的一組 $c_1,\dots,c_r\in\mathbb{Z}$ 皆可找到一整數 c 使得

$$c\equiv c_i \pmod{m_i},\forall i\in\{1,\dots,r\}. \tag{3.1}$$

另一方面，滿足式子 (3.1) 的整數 c 在 *modulo* $m_1\cdots m_r$ 之下是唯一的