1.4. 最大公因數與最小公倍數

我們已經知道如何求得最大公因數, 接下來便是探討如何求得最小公倍數. 我們也會探討多個 (多於兩個) 整數的最大公因數與最小公倍數.

首先我們有以下最小公倍數的定義.

Definition 1.4.1. 令 $a,b\in\mathbb{Z}$ 且皆不等於 0.

(1) 若 $m\in\mathbb{Z}$, 且 $a\mid m, b\mid m$, 則稱 m 為 a,b 的 *common multiple* (公倍數).

(2) 若 $l\in\mathbb{N}$ 是 a,b 的正公倍數中最小的, 則稱 l 為 a,b 的 *least common multiple* (最小公倍數), 通常我們會用 $\mathrm{lcm}(a,b)$ 來表示之.

首先我們探討兩整數 a,b 的最小公倍數的性質. 考慮集合 $S=a\mathbb{Z}\cap b\mathbb{Z}$。因為 $a\mathbb{Z}$ 是 a 的所有倍數所成的集合且 $b\mathbb{Z}$ 是 b 的所有倍數所成的集合，所以依集合交集的定義 S 就是 a,b 所有的公倍數所成的集合。很容易檢查 S 滿足整係數線性組合的封閉性（即對任意 $s_1,s_2\in S$ 以及 $m,n\in\mathbb{Z}$ 皆有 $ms_1+ns_2\in S$)，因此由 Theorem 1.2.2 知：若 l 是 S 中最小的正整數，則 $S=l\mathbb{Z}$。由於 $l\in S$，所以 l 是 a,b 的公倍數。又因所有 a,b 的公倍數都在 S 中且 l 是 S 中最小的正整數，所以 l 就是 a,b 的最小公倍數。更重要的是，因為 S 中的元素都是 l 的倍數，所以我們也同時證得 a,b 的公倍數都是最小公倍數 l 的倍數。我們有以下最小公倍數相對應於最大公因數 Proposition 1.2.3 以及 Corollary 1.2.4 的性質：

Proposition 1.4.2. 假設 $a,b\in\mathbb{Z}$ 且考慮集合 $a\mathbb{Z}\cap b\mathbb{Z}$ 中最小的正整數 l，則 $\mathrm{lcm}(a,b)=l$ 而且 $m\in\mathbb{Z}$ 是 a,b 的公倍數若且唯若 $l\mid m$.

由 Proposition 1.4.2 知：如同最大公因數的情形一樣，要說明 $l=\mathrm{lcm}(a,b)$ 便要證明兩件事。首先證明 l 是 a,b 的正的公倍數, 再來就是證明對任意 a,b 的公倍數 m 皆會滿足 $l\mid m$。如此一來就能擔保 l 是 a,b 的最小公倍數。我們試著用此方式證明以下定理。

Proposition 1.4.3. 假設 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=d$ 則 $\mathrm{lcm}(a,b)=ab/d$。

Proof. 由假設 $d=\gcd(a,b)$ 知存在 $a',b'\in\mathbb{N}$ 使得 $a=a'd$, $b=b'd$ 且 $\gcd(a',b')=1$ (Proposition 1.2.11). 現在我們依上述兩個步驟證明 $ab/d=a'b=b'a$ 是 a,b 的最小公倍數.

首先由 $ab/d=b'a$ 知 $a\mid(ab/d)$ 同理知 $b\mid(ab/d)$, 也就是說 ab/d 為 a 和 b 的公倍數. 又因為 a,b,d 皆為正數, 所以 ab/d 為 a,b 之正的公倍數.

接著證明若 m 為 a,b 的公倍數, 則 $(ab/d)\mid m$. 由假設知存在 $m',n'\in\mathbb{N}$ 使得 $m=m'a=n'b$. 換言之 $m=m'a'd=n'b'd$, 故消掉 d (因 $d\neq0$) 得 $m'a'=n'b'$. 也就是說 $a'\mid n'b'$. 但由於 $\gcd(a',b')=1$, 故由 Proposition 1.2.6(1) 知 $a'\mid n'$. 也就是說存在 $h\in\mathbb{N}$ 使得 $n'=a'h$. 代回 $m=n'b$ 得 $m=ha'b$, 故得知 $a'b=(ab/d)\mid m$。 □

要注意雖然 Proposition 1.4.3 中假設 $a,b\in\mathbb{N}$, 但其目的僅是利用其為正數方便描述最小公倍數. 若 $a,b\in\mathbb{Z}$ 不一定為正時, 我們只要適當的加上負號仍可利用 Proposition 1.4.3

的式子寫下最小公倍數. Proposition 1.4.3 的主要精神就是：雖然沒有特殊的工具幫我們求最小公倍數，不過我們可以利用輾轉相除法幫我們找到最大公因數，再求得最小公倍數。

我們目前談的是針對兩個整數的最大公因數和最小公倍數. 事實上最大公因數和最小公倍數的定義是可以推廣到任意有限多個 (多於兩個) 整數的情況. 我們有以下的定義.

Definition 1.4.4. 令 $a_1,a_2,\ldots,a_n \in \mathbb{Z}$ 且皆不等於 0.

(1) 若 $c \in \mathbb{Z}$, 且 $c \mid a_1, c \mid a_2, \ldots, c \mid a_n$, 則稱 c 為 $a_1,a_2,\ldots,a_n$ 的 *common divisor* (公因數).

(2) 若 $d \in \mathbb{N}$ 是 $a_1,a_2,\ldots,a_n$ 的公因數中最大的, 則稱 d 為 $a_1,a_2,\ldots,a_n$ 的 *greatest common divisor* 最大公因數, 通常我們會用 $\gcd(a_1,a_2,\ldots,a_n)$ 來表示之.

(3) 若 $m \in \mathbb{Z}$, 且 $a_1 \mid m, a_2 \mid m, \ldots, a_n \mid m$, 則稱 m 為 $a_1,a_2,\ldots,a_n$ 的 *common multiple* (公倍數).

(4) 若 $l \in \mathbb{N}$ 是 $a_1,a_2,\ldots,a_n$ 的正的公倍數中最小的, 則稱 l 為 $a_1,a_2,\ldots,a_n$ 的 *least common multiple* 最小公倍數, 通常我們會用 $\operatorname{lcm}(a_1,a_2,\ldots,a_n)$ 來表示之.

接下來讓我們來看看有關多個 (多於兩個) 整數的最大公因數性質. 我們試著著推廣前面的方法, 看看前面的結果對多個整數是否適用.

Proposition 1.4.5. 假設 $a_1,\ldots,a_n \in \mathbb{N}$, 令 d 為集合 $S = \{m_1a_1 + \cdots + m_na_n \mid m_1,\ldots,m_n \in \mathbb{Z}\}$ 中最小的正整數. 則 $\gcd(a_1,\ldots,a_n) = d$.

Proof. 和前面的情形相同, 利用 well-ordering principle 知 S 中必有最小的正整數. 也就是說敘述中的 d 一定存在. 接著和前面一樣, 我們知 S 是封閉的, 故由 Theorem 1.2.2 得 $S = d\mathbb{Z}$. 因此可按照前面證明最大公因數的步驟證明 d 為 $a_1,\ldots,a_n$ 的最大公因數.

首先檢查對所有 $i \in \{1,\ldots,n\}$, 皆有 $d \mid a_i$. 由於 $a_i \in S = d\mathbb{Z}$, 故知 $d \mid a_i$. 也就是說 d 為 $a_1,\ldots,a_n$ 的公因數.

接著我們要證明 d 是 $a_1,\ldots,a_n$ 的公因數中最大的數. 也就是要證明若 d' 是 $a_1,\ldots,a_n$ 的公因數, 則 $d' \le d$. 依定義, 存在 $m_1,\ldots,m_n \in \mathbb{Z}$ 使得 $d = m_1a_1 + \cdots + m_na_n$. 今由於對任意 $i \in \{1,\ldots,n\}$, 皆有 $d' \mid a_i$ 故知 $d' \mid m_1a_1 + \cdots + m_na_n$. 即 $d' \mid d$, 因此由已知 $d > 0$ 當然得 $d' \le d$. □

有了 Proposition 1.4.5 我們當然可以和前面的方法一樣得到以下之結果, 證明就不再贅述.

Corollary 1.4.6. 假設 $a_1,\ldots,a_n \in \mathbb{N}$ 且 $d = \gcd(a_1,\ldots,a_n)$ 則存在 $m_1,\ldots,m_n \in \mathbb{Z}$ 使得 $d = m_1a_1 + \cdots + m_na_n$. 而且對任意 $d' \in \mathbb{Z}$, d' 是 $a_1,\ldots,a_n$ 的公因數若且唯若 $d' \mid d$.

要注意並不是所有有關兩個整數的最大公因數的性質都可以推廣到多個整數的情形. 例如 Proposition 1.2.6(2) 告訴我們若 $\gcd(a,b) = 1$ 且 $a \mid l$ 及 $b \mid l$, 則 $ab \mid l$. 此性質在兩個以上整數的情形就不一定對. 主要原因就是依多個整數互質的定義 $a_1,a_2,\ldots,a_n$ 互質是表

示這些數除了 ± 1 之外沒有共同的因數, 但不表示任取其中兩個數都互質. 其實有可能任意 a_i, a_j 都不互質但是 $a_1, \ldots, a_n$ 仍互質. 例如 $a_1 = 6$, $a_2 = 15$ 以及 $a_3 = 10$ 的情形. 我們有 $\gcd(a_1, a_2) = 3$, $\gcd(a_2, a_3) = 5$ 以及 $\gcd(a_1, a_3) = 2$ 但是 $\gcd(a_1, a_2, a_3) = 1$. 所以有些情形僅假設 $a_1, \ldots, a_n$ 互質是不夠的, 我們須用到任取兩個都互質 (即對任意 $i, j \in \{1, \ldots, n\}$ 且 $i \neq j$, 皆有 $\gcd(a_i, a_j) = 1$) 這一個較強的互質性才行. 這種較強的互質性我們稱之為 "兩兩互質" (*pairwise relatively prime*). 當然了若 $a_1, \ldots, a_n$ 兩兩互質, 則 $a_1, \ldots, a_n$ 必互質. 大家一定要清楚這兩種互質性之不同. Proposition 1.2.6(2), 在多個整數的情形之下若改為兩兩互質就會成立. 由於這裡牽涉到任意多個整數, 所以得用到數學歸納法來證明. 數學歸納法的原理我們假設大家已了解, 此處不再贅述.

從上一節我們知道可以用輾轉相除法求兩個整數的最大公因數, 是否我們可以兩個兩個地求得多個整數的最大公因數? 也就是說可以先求 $d_1 = \gcd(a_1, a_2)$ 求得 $d_2 = \gcd(a_1, a_2, a_3) = \gcd(d_1, a_3)$, 這樣一直下去以求得 $\gcd(a_1, a_2, \cdots, a_n)$ 嗎? 答案是肯定的, 我們的證明方法還是利用前述證明最大公因數方法進行.

Proposition 1.4.7. *若 $a_1, \ldots, a_n \in \mathbb{N}$ $(n > 2)$, 則*

$$\gcd(a_1, \ldots, a_{n-1}, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n).$$

Proof. 令 $d = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n)$ 首先我們要證明 d 是 $a_1, \ldots, a_n$ 的公因數. 由於 $d \mid \gcd(a_1, \ldots, a_{n-1})$ 由 Corollary 1.4.6 知 d 是 $a_1, \ldots, a_{n-1}$ 的公因數. 再加上 $d \mid a_n$, 故知 d 是 $a_1, \ldots, a_{n-1}, a_n$ 的公因數.

現假設 d' 是 $a_1, \ldots, a_{n-1}, a_n$ 的公因數. 當然 d' 是 $a_1, \ldots, a_{n-1}$ 的公因數, 故由 Corollary 1.4.6 知 $d' \mid \gcd(a_1, \ldots, a_{n-1})$. 再加上 $d' \mid a_n$, 故知 d' 是 $\gcd(a_1, \ldots, a_{n-1})$ 和 a_n 的公因數, 故再由 Corollary 1.2.4 知 $d' \mid \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n) = d$. 得證 d 是 $a_1, \ldots, a_n$ 的公因數中最大的數, 故為 $a_1, \ldots, a_n$ 的最大公因數. □

最後我們看看多個整數的最小公倍數的性質. 首先要注意的是 Proposition 1.4.3 中 $\operatorname{lcm}(a, b) = ab/\gcd(a, b)$ 這個性質在多個整數時並不一定對. 例如前面所提 $a_1 = 6$, $a_2 = 15$ 以及 $a_3 = 10$ 的例子, 我們有 $a_1 a_2 a_3 = 900$, $\gcd(a_1, a_2, a_3) = 1$ 但是 $\operatorname{lcm}(a_1, a_2, a_3) = 30$. 雖然如此, 我們仍有公倍數為最小公倍數之倍數的性質。證明方法和之前一就不再贅述.

Proposition 1.4.8. *假設 $a_1, \ldots, a_n \in \mathbb{Z}$ 且考慮集合 $a_1\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z}$ 中最小的正整數 l，則 $\operatorname{lcm}(a_1, \ldots, a_n) = l$ 而且 $m \in \mathbb{Z}$ 是 $a_1, \ldots, a_n$ 的公倍數若且唯若 $l \mid m$.*

前面 Proposition 1.4.3 提及，我們可以利用輾轉相除法求出兩個整數的最大公因數，再求其最小公倍數。至於求多個整數之最小公倍數也可如最大公因數一樣兩個兩個進行.

Proposition 1.4.9. *若 $a_1, \ldots, a_n \in \mathbb{Z}$ $(n > 2)$, 則*

$$\operatorname{lcm}(a_1, \ldots, a_{n-1}, a_n) = \operatorname{lcm}(\operatorname{lcm}(a_1, \ldots, a_{n-1}), a_n).$$

Proof. 為了方便起見，令 $l' = \operatorname{lcm}(a_1, \ldots, a_{n-1})$ 且 $l = \operatorname{lcm}(l', a_n)$ 我們要證明 l 是 $a_1, \ldots, a_n$ 的最小公倍數.

由於 $l=\operatorname{lcm}(l',a_n)$ 是 $l'=\operatorname{lcm}(a_1,\ldots,a_{n-1})$ 的倍數, 故知 l 為 $a_1,\ldots,a_{n-1}$ 的公倍數. 再加上 l 也是 a_n 的倍數, 故得知 l 是 $a_1,\ldots,a_n$ 的公倍數. 另一方面若 m 是 $a_1,\ldots,a_{n-1},a_n$ 的公倍數, 當然 m 是 $a_1,\ldots,a_{n-1}$ 的公倍數. 故由 Proposition 1.4.8 知 $l'=\operatorname{lcm}(a_1,\ldots,a_{n-1})\mid m$. 再加上 $a_n\mid m$, 知 m 為 l' 和 a_n 之公倍數，故同理知 $l=\operatorname{lcm}(l',a_n)\mid m$. 因而得知 l 確為 $a_1,\ldots,a_n$ 的正公倍數中最小者, 也就是說 $l=\operatorname{lcm}(a_1,\ldots,a_n)$. □

Exercise 1.11. 假設 $a_1,a_2,\ldots,a_n\in\mathbb{N}$ 且令 $M=a_1\cdots a_n$. 試證明以下是等價的.

(1) $a_1,a_2,\ldots,a_n$ 兩兩互質 (pairwise relatively prime).

(2) 對任意 $i\in\{1,\ldots,n\}$ 皆有 $\gcd(a_i,M/a_i)=1$.

(3) $\operatorname{lcm}(a_1,a_2,\ldots,a_n)=M$.

Exercise 1.12. 假設 $a_1,\ldots,a_n\in\mathbb{N}$. 試證明

(1) 若 d 是 $a_1,\ldots,a_n$ 的公因數且 d' 是 $a_1/d,\ldots,a_n/d$ 的公因數, 則 dd' 是 $a_1,\ldots,a_n$ 的公因數.

(2) 若 $d=\gcd(a_1,\ldots,a_n)$. 則 $\gcd(a_1/d,\ldots,a_n/d)=1$.

Exercise 1.13. 假設 $a_1,a_2,\ldots,a_n\in\mathbb{Z}$ 且 $c\in\mathbb{Z}$. 證明方程式 $a_1x_1+a_2x_2+\cdots+a_nx_n=c$ 有整數解若且唯若 $\gcd(a_1,\ldots,a_n)\mid c$.

Exercise 1.14. 設 $d=\gcd(a,b)$ 且 $\gcd(a,b,c)=1$。已知 $x=m_0,y=n_0$ 是 $ax+by=d$ 的一組整數解。證明 $ax+by+cz=0$ 的所有整數解為：$\begin{cases} x=m_0cs+(b/d)t \\ y=n_0cs-(a/d)t \\ z=-ds \end{cases}$ $s,t\in\mathbb{Z}$

Exercise 1.15. 試寫出以下 diophantine equations 的所有整數解.

(1) $9x_1+12x_2+16x_3=13$.

(2) $8x_1-4x_2+6x_3=6$.

1.5. 質數

這一節我們要談整數的分解中最基本的元素: 質數. 大家都知道一個質數 p 就是正因數只有 1 和本身的數. 我們仍給一個正式的定義.

Definition 1.5.1. 若 $p\in\mathbb{Z}$, $p>1$ 且 p 的正公因數只有 p 和 1 則稱 p 是一個質數 (prime number). 若一正整數有其他的正因數則稱為合成數 (composite number).

簡單來說質數就是無法分解成兩個較小的正整數乘積的數. 質數這一種不可分解的特性讓它有很多特殊性質. 例如給定一質數 p 以及一整數 $a\in\mathbb{Z}$, 我們很容易判定 $\gcd(a,p)$ 為何. 若 $d=\gcd(a,p)$ 則因 $d\mid p$, 知 $d=1$ 或 $d=p$. 然而 $d=p$ 表示 $p\mid a$, 因此若已知 $p\nmid a$, 則可得 $d=1$. 所以利用 Proposition 1.2.6(1) 我們有以下之結論.

Lemma 1.5.2 (Euclid)**.** 假設 p 是一個質數, 且 $a,b\in\mathbb{Z}$. 若 $p\mid ab$, 則 $p\mid a$ 或 $p\mid b$.

Proof. 這裡我們要證明 $p \mid a$ 或 $p \mid b$. 如果 $p \mid a$ 當然就可以了 (不必擔心是否 $p \mid b$); 但若 $p \nmid a$, 那麼我們就得證明 $p \mid b$. 不過由前知 $p \nmid a$ 表示 $\gcd(p,a) = 1$, 故利用 Proposition 1.2.6(1) 得證 $p \mid b$. □

Euclid 這一個 Lemma 告訴我們一個質數若是 ab 的因數那它一定是 a,b 其中之一的因數. 事實上這個性質並不只適用在兩個整數相乘的情況, 我們很容易推廣至更多數相乘之情況.

Corollary 1.5.3. 假設 p 是一個質數, 且 $a_1,a_2,\ldots,a_n \in \mathbb{Z}$. 若 $p \mid a_1a_2\cdots a_n$, 則存在 $i \in \{1,\ldots,n\}$ 滿足 $p \mid a_i$.

Proof. 我們依然用數學歸納法證明. 當 $k = 2$ 時由 Lemma 1.5.2 知若 $p \mid a_1a_2$, 則 $p \mid a_1$ 或 $p \mid a_2$. 假設 $k = n-1$ 時成立, 即若有 $n-1$ 個整數 $a_1,\ldots,a_{n-1}$ 滿足 $p \mid a_1\cdots a_{n-1}$, 則存在 $i \in \{1,\ldots,n-1\}$ 使得 $p \mid a_i$. 現考慮 $k = n$ 的情形, 若 $a_1,\ldots,a_n$ 是 n 個整數滿足 $p \mid a_1\cdots a_n$, 則令 $a = a_1\cdots a_{n-1}$, $b = a_n$. 此時由 $p \mid ab$ 及 Lemma 1.5.2 知 $p \mid a$ 或 $p \mid b$. 若 $p \mid a$, 則由數學歸納法假設知存在 $i \in \{1,\ldots,n-1\}$ 使得 $p \mid a_i$, 而若 $p \mid b$ 即 $p \mid a_n$, 故得證本定理. □

若一質數 p 是一整數 a 的因數, 則我們稱 p 是 a 的一個質因數. 當然了質數 p 本身就是 p 的質因數, 而一個合成數會不會有質因數呢? 大家很自然的覺得一定有, 我們還是給一個正式的證明.

Lemma 1.5.4. 假設 $a \in \mathbb{Z}$ 且 $a > 1$. 則必存在一質數 p 使得 $p \mid a$.

Proof. 我們用數學歸納法. 首先若 $a = 2$, 則由於 2 是質數我們得 $p = 2$ 為所求. 現假設對任意 $b \in \mathbb{Z}$ 滿足 $2 \le b \le n$ 的數皆存在質數 p 使得 $p \mid b$, 我們考慮 $a = n+1$ 的情形. 若 a 本身是質數那當然 $p = a$ 為所求. 反之, 如果 a 不是質數依定義存在 $b \in \mathbb{Z}$ 且 $2 \le b < a$ 使得 $b \mid a$. 故由數學歸納法假設知存在一質數 p 滿足 $p \mid b$. 因此由 $p \mid b$ 以及 $b \mid a$, 利用 Lemma 1.1.1(1) 得證 $p \mid a$. □

雖然正整數有無窮多個而 Lemma 1.5.4 告訴我們每一個大於 1 的正整數都有質因數, 但這並不代表會有無窮多個質數. 接著我們就是要探討質數確有無窮多個. 一般來說要證明質數有無窮多個或許會有的想法是希望利用現有的質數創造更大的質數. 不過這個想法是不可行的, 主要的原因是到目前為止我們沒有一個判別一個數是否為質數好的方法. 另類的思考是用反證法, 假設只有有限個質數而得到矛盾. 這個方法就不會碰到判別質數的問題, 相信由此大家更能體會到反證法的妙用.

Theorem 1.5.5 (Euclid)**.** 質數有無窮多個.

Proof. 我們用反證法假設只有有限個質數. 既然只有有限個我們可以將之一一列出, 就假設 $p_1,\ldots,p_n$ 是所有的質數. 現考慮 $a = p_1\cdots p_n + 1$, 由 Lemma 1.5.4 知必有一質數 p_i, $i \in \{1,\ldots,n\}$ 滿足 $p_i \mid a$. 然而 p_i 本身整除 $p_1\cdots p_n$ 故由 Corollary 1.1.1 知 $p_i \mid a - p_1\cdots p_n$, 也就是說 $p_i \mid 1$ 而得到矛盾. 故知不可能僅有有限多個質數, 而得證有無窮多個質數. □

質數既然有無窮多個, 接下來我們可以問是否有些特定形式的質數也會有無窮多個? 例如我們知道偶數中只有 2 是質數, 因此可以將所有奇數分類, 分成 $4n+1$ 和 $4n+3$ 這兩類然後問哪一類會有無窮多個質數. 要注意 $4n+1$ 這一類的數有一重要特性就是兩個 $4n+1$ 形式的數相乘仍然是 $4n+1$ 的形式. 因此任意有限多個 $4n+1$ 形式的數相乘仍是 $4n+1$ 的形式, 也就是說這一類的數有乘法封閉性. 另一方面 $4n+3$ 的形式的數就沒有這個特性, 事實上兩個 $4n+3$ 形式的數相乘會變成 $4n+1$ 的形式. 利用這兩類數的特性以及類似 Lemma 1.5.4 的證明, 我們有以下之結果.

Lemma 1.5.6. 假設 $a=4n+3$ 其中 $n\in\mathbb{N}\cup\{0\}$, 則必存在一質數 $p=4n'+3$ 其中 $n'\in\mathbb{N}\cup\{0\}$ 滿足 $p\mid a$.

Proof. 我們利用數學歸納法證明. 首先若 $a=3$, 則由於 3 是質數我們得 $p=3$ 為所求. 現假設對任意 $b=4k+3\in\mathbb{Z}$ 滿足 $0\le k\le n-1$ 的數皆存在質數 $p=4k'+3$ 使得 $p\mid b$, 我們考慮 $k=n$ 的情形. 若 $a=4n+3$ 本身是質數那當然 $p=a$ 為所求. 反之, 如果 a 不是質數依定義存在 $b,c\in\mathbb{N}$ 其中 $b<a$ 且 $c<a$ 使得 $a=bc$. 注意 b, c 中必有一個元素是 $4k+3$ 形式, 否則 b,c 都是 $4k+1$ 形式會造成 $bc=a$ 也是 $4k+1$ 形式的矛盾現象. 就假設 $b=4k+3$ 吧! 此時 $0\le k\le n-1$ (因 $b<a$), 故由歸納假設知存在 $p=4k'+3$ 使得 $p\mid b$, 因而得證 $p\mid a$. □

注意 $4n+1$ 形式的數並不一定有 $4n+1$ 形式的質因數. 9 就是最簡的的例子. 觀察由 Lemma 1.5.4 推得 Theorem 1.5.5 的關係, 同樣的我們也可利用 Lemma 1.5.6 推得 $4n+3$ 形式的質數有無窮多個.

Proposition 1.5.7. 集合 $S=\{4n+3\mid n\in\mathbb{Z},n\ge 0\}$ 中有無窮多個質數.

Proof. 我們依然用反證法假設 S 中只有有限多個質數並令 $p_0=3,p_1,\ldots,p_n$ 是 S 中所有的相異質數. 現考慮 $a=4(p_1\cdots p_n)+3$. 由於 $a\in S$ 利用 Lemma 1.5.6 知必有一質數 $p\in S$ 滿足 $p\mid a$, 故由假設知存在 $i\in\{0,\ldots,n\}$ 使得 $p=p_i$, .

若 $p=p_0=3$, 則由 $3\mid a$, $3\mid 3$ 以及 $a-3=4(p_1\cdots p_n)$ 得知 $3\mid 4(p_1\cdots p_n)$, 故由 Corollary 1.5.3 得到 $3\mid 4$ 或者 $3\mid p_i$, $i\in\{1,\ldots,n\}$ 這樣的矛盾.

若 $p=p_i$ 其中 $i\in\{1,\ldots,n\}$, 則由 p_i 本身整除 $p_1\cdots p_n$ 知 $p_i\mid a-4(p_1\cdots p_n)$, 也就是說 $p_i\mid 3$ 而得到矛盾. 故得證 S 中不可能僅有有限多個質數. □

因為 Lemma 1.5.6 並不適用於 $4n+1$ 形式的整數, 所以 Proposition 1.5.7 的方法不能用來討論 $4n+1$ 形式的質數, 不過 $4n+1$ 形式的質數仍有無窮多個. 事實上數論一個很重要的定理 (Dirichlet Theorem) 告訴我們對任意互質的兩整數 a,b 皆有無窮多個 $an+b$ 形式的質數. 這個定理的證明超出本講義範圍, 我們就不再多談了.

質數雖然有無窮多個不過他們的分布不是非常稠密的. 例如給定任意大的整數 n 我們可以找到 n 個連續整數都不是質數. 我們的找法是考慮

$$(n+1)!+2,(n+1)!+3,\ldots,(n+1)!+n+1$$

這 n 個連續整數. 很容意看出它們都不是質數.