就是因為質數這麼不容易出現, 再加上很難判別一個很大的數是否為質數, 所以質數常被應用在密碼學中. 底下我們介紹一種最簡單判斷質數的方法.

Proposition 1.5.8. 假設 $n>1$ 是一整數. 則 n 不是質數若且唯若存在質數 p 小於等於 $\sqrt{n}$ 且整除 n.

Proof. 首先若存在 $p\le\sqrt{n}$ 且 $p\mid n$. 因 $1<p<n$, 得 n 除了 1 和 n 以外還有其他的正因數, 故知 n 不是 prime. 另一方面, 假設 n 不是質數, 依定義知存在 $a,b\in\mathbb{Z}$ 滿足 $1<a\le b<n$ 且 $n=ab$. 由此我們可以確定 $a\le\sqrt{n}$, 否則若 $a>\sqrt{n}$ 會造成 $ab>(\sqrt{n})^2=n$ 而與 $n=ab$ 不合. 而由 Lemma 1.5.4 知存在質數 p 使得 $p\mid a$. 既然 $p\mid a$ 我們得 $p\le a\le\sqrt{n}$ 且 $p\mid n$. □

Proposition 1.5.8 告訴我們的是一個判別 composite number 的等價關係, 所以它也就告訴了我們判別 prime 的方法. 也就是說 n 是質數若且唯若所有小於等於 $\sqrt{n}$ 的質數都不能整除 n. 這種判別質數方法稱為篩法 (sieve method). 它可以幫助我們篩得哪些數是質數. 例如若要找出所有小於 100 的質數. 我們只要將小於 $\sqrt{100}=10$ 的質數 (即 2,3,5,7) 找出, 留下 2,3,5,7 然後將其餘 2,3,5,7 的倍數刪除, 經過這樣篩選後留下來小於 100 的數就都是小於 100 的質數. 這是因為若 $n<100$ 且不是質數, 則由 Proposition 1.5.8 知 n 必有一質因數小於等於 $\sqrt{n}<\sqrt{100}=10$. 因此被我們所刪除 2,3,5,7 的倍數就是所有小於 100 的合成數, 自然剩下的便都是質數了.

Question 1.8. 你能找到連續 8 個整數都不是質數嗎?

Question 1.9. 大於 100 的合成數中, 第一個不能用刪除 2,3,5,7 的倍數篩選出來的是哪一個整數?

Exercise 1.16. 假設 $a,b\in\mathbb{Z}$, 試證明 $\gcd(a,b)=1$ 若且唯若 $\gcd(a+b,ab)=1$.

(Hint: 反證法，利用 Euclid 的 Lemma 1.5.2 以及大於 1 的整數皆有質因數處理)

Exercise 1.17. 假設 a,n 皆為大於 1 的整數. 利用等式

$$x^k-1=(x-1)(x^{k-1}+x^{k-2}+\cdots+x+1);\quad x^{2k+1}+1=(x+1)(x^{2k}-x^{2k-1}+\cdots+x^2-x+1)$$

證明以下問題.

(1) 若 a^n-1 是質數, 則 $a=2$ 且 n 是質數.

(2) 若 a^n+1 是質數, 則 a 為偶數且 $n=2^r$, 其中 $r\in\mathbb{N}$.

Exercise 1.18. 給定 $n\in\mathbb{N}$ 且 $n>1$, 令 $l(n)$ 表示 n 最小的質因數, 例如 $l(91)=7$. 試問集合 $\{l(n)\mid n$ 是合成數且 $1<n<300\}$ 的最大值為何？

1.6. 算術基本定理

算術基本定理 (The fundamental theorem of arithmetic) 即唯一分解定理, 告訴我們每一個大於 1 的整數若不是質數都可以寫成有限多個質因數的乘積且經過適當排序其寫法唯一. 此定理看似自然且明顯, 但仍需一個正式的證明.

這裡我們又碰到一個典型的有關存在性與唯一性的問題. 這裡的存在性指的就是對一大於 1 的整數可以找到有限多個質數使其可以寫成這些質數的乘積, 而唯一性就是指的就是寫法唯一. 由於正整數和負整數的分解只差一個負號, 我們只需考慮正整數的情況.

Theorem 1.6.1 (The Fundamental Theorem of Arithmetic)**.** 假設 $a \in \mathbb{N}$ 且 $a > 1$, 則存在 $p_1, \ldots, p_r$, 其中 p_i 是相異的質數, 滿足

$$a = p_1^{n_1} \cdots p_r^{n_r}, \quad n_i \in \mathbb{N}, \forall i \in \{1, \ldots, r\}.$$

如果 a 可以分解成另外的形式 $a = q_1^{m_1} \cdots q_s^{m_s}$, 其中 q_i 是相異的質數, 則 $r = s$ 且經過變換順序可得 $p_i = q_i$, $n_i = m_i$, $\forall i \in \{1, \ldots, r\}$.

Proof. 我們分開來證存在性與唯一性.

首先來看存在性: 簡單來說存在性就是要證明每一個大於 1 的整數都可以寫成有限多個 (可以相同) 質數的乘積. 我們用數學歸納法來證明. 當 $a = 2$ 時由於 2 是質數, 所以在這情況存在性是對的. 接著假設對所有從 2 到 $a-1$ 的整數存在性是對的. 如果 a 是質數, 那存在性自然成立. 如果 a 不是質數, 則知 $a = a_1 \cdot b_1$ 其中 $a_1, b_1 \in \mathbb{N}$ 且 $1 < a_1 < a$ 及 $1 < b_1 < a$. 故利用歸納假設知 a_1 和 b_1 都可寫成有限多個質數的乘積, 所以得證 $a = a_1 \cdot b_1$ 也可以寫成有限多個質數的乘積.

要證明唯一性, 我們假設

$$a = p_1^{n_1} \cdots p_r^{n_r} = q_1^{m_1} \cdots q_s^{m_s},$$

其中 $p_1, \ldots, p_r$ 是兩兩相異的質數, 且 $q_1, \ldots, q_s$ 也是兩兩相異的質數. 首先我們證明 $P = \{p_1, \ldots, p_r\}$ 和 $Q = \{q_1, \ldots, q_s\}$ 這兩個集合是一樣的. 任取 $p_i \in P$, 由於 $p_i \mid a$, 而 $a = q_1^{m_1} \cdots q_s^{m_s}$, 故由 p_i 是質數以及 Corollary 1.5.3 知存在 $q_j \in Q$ 使得 $p_i \mid q_j$. 再由 q_j 亦為質數, 得 $p_i = q_j \in Q$. 我們證明了 $P \subseteq Q$. 同理可證 $Q \subseteq P$. 因此得 $P = Q$, 亦即 $r = s$, 且經由適當排列, 我們有 $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_r$. 換言之現在我們有

$$a = p_1^{n_1} \cdots p_r^{n_r} = p_1^{m_1} \cdots p_r^{m_r}. \tag{1.1}$$

接下來我們要說明, 對所有 $i \in \{1, \ldots, r\}$ 皆有 $n_i = m_i$, 因而證得唯一性. 我們可以用反證法, 也就是說假設存在 $n_i \neq m_i$, 會造成矛盾. 不失一般性, 我們假設 $n_1 \neq m_1$, 我們更進一步假設 $n_1 > m_1$. 此時將式子 (1.1) 同除以 $p_1^{m_1}$, 我們得

$$p_1^{n_1 - m_1} p_2^{n_2} \cdots p_r^{n_r} = p_2^{m_2} \cdots p_r^{m_r}.$$

由於 p_1 是質數, 且 $n_1 - m_1 > 0$, 故由 $p_1 \mid p_2^{m_2} \cdots p_r^{m_r}$ 以及 Corollary 1.5.3 知 $p_2, \ldots, p_r$ 中必存在某個 p_j 滿足 $p_1 \mid p_j$, 此和當初假設 $p_1, p_2, \ldots, p_r$ 為相異質數相矛盾. 故得證唯一性. □

一般來說我們將一正整數 a 寫成質數之乘積 $a = p_1^{n_1} \cdots p_r^{n_r}$ 時, 為了唯一性我們要求每個質數 p_i 的次方 n_i 都是正的, 也就是說我們只挑出 a 的質因數 $p_1, \ldots, p_r$. 不過當要討論兩正數 a, b 時為了方便比較, 我們通常會挑出 a 和 b 所有的質因數再將 a, b 寫成這些質數之乘積的樣子. 也就是說可寫成 $a = p_1^{n_1} \cdots p_r^{n_r}$ 以及 $b = p_1^{m_1} \cdots p_r^{m_r}$ 其中對於 $i \in \{1, \ldots, r\}$, $n_i \geq 0$ 且 $m_i \geq 0$. 注意這裡由於 a 的質因數未必就是 b 的質因數, 反之亦然, 所以 n_i, m_i 有可能為

0. 這樣寫法的方便性就是我們不必區分哪些 p_i 是 a 的質因數, 哪些是 b 的質因數. 利用這樣的寫法我們很容易將 a,b 的最大公因數表示出來.

Proposition 1.6.2. 假設 $a,b\in\mathbb{N}$ 且 $a,b>1$. 若 $a=p_1^{n_1}\cdots p_r^{n_r}$ 且 $b=p_1^{m_1}\cdots p_r^{m_r}$, 其中 $p_1,\ldots,p_r$ 為相異質數且 $n_i,m_i\geq 0$, 則 a,b 的正公因數都可寫成 $p_1^{t_1}\cdots p_r^{t_r}$ 的形式, 其中 $0\leq t_i\leq \min\{n_i,m_i\}$. 特別地, 我們有

$$\gcd(a,b)=p_1^{\min\{n_1,m_1\}}\cdots p_r^{\min\{n_r,m_r\}}.$$

Proof. 首先回顧一下 $\min\{x,y\}$ 表示 x,y 中最小之數. 現假設 d 是 a,b 的正公因數, 則由 $d\mid a$ 我們知若 p 是 d 的質因數, 則由 $p\mid d$ 知 $p\mid a$. 故由 Corollary 1.5.3 知存在 $i\in\{1,\ldots,r\}$ 使得 $p\mid p_i$. 因此由 p,p_i 皆為質數得 $p=p_i$. 也就是說 d 的質因數必在 $\{p_1,\ldots,p_r\}$ 中, 故 d 一定可以寫成 $p_1^{t_1}\cdots p_r^{t_r}$ 的形式, 其中 $t_i\geq 0$. 又由於對任意 $i\in\{1,\ldots,r\}$ 皆有 $p_i^{t_i}\mid d$ 故 $p_i^{t_i}\mid a$, 亦即 $p_i^{t_i}\mid p_1^{n_1}\cdots p_r^{n_r}$. 由於當 $i\neq j$ 時 $p_i\neq p_j$, 因此 $\gcd(p_i^{t_i},p_j^{n_j})=1$, 故由 Proposition 1.2.6(1) 得 $p_i^{t_i}\mid p_i^{n_i}$. 此時若 $t_i>n_i$, 會造成 $p^{t_i-n_i}\mid 1$ 之矛盾, 因此知 $t_i\leq n_i$. 同理由 $d\mid b$ 可得 $t_i\leq m_i$, 故得證 $0\leq t_i\leq\min\{n_i,m_i\}$.

接著我們探討 $\gcd(a,b)$. 為了方便起見, 對於所有 $i\in\{1,\ldots,r\}$, 我們令 $d_i=\min\{n_i,m_i\}$. 首先說明 $p_1^{d_1}\cdots p_r^{d_r}$ 為 a,b 的公因數. 對於 $i\in\{1,\ldots,r\}$, 由於 $d_i\leq n_i$, 故知 $p_i^{d_1}\mid p_i^{n_i}$. 因此得 $p_i^{d_i}\mid a$. 由於這是對所有 $i=1,\ldots,r$ 皆成立又因為 $p_1^{d_1},\ldots,p_r^{d_r}$ 兩兩互質故由 Question 1.7 (2) 知 $p_1^{d_1}\cdots p_r^{d_r}\mid a$. 同理可得 $p_1^{d_1}\cdots p_r^{d_r}\mid b$. 最後對於任意 a,b 之公因數 d. 由上知 $d=p_1^{t_1}\cdots p_r^{t_r}$ 且 $0\leq t_i\leq d_i$, 故由前面的討論知 $d\mid p_1^{d_1}\cdots p_r^{d_r}$. 得證 $\gcd(a,b)=p_1^{d_1}\cdots p_r^{d_r}$. □

雖然 Proposition 1.6.2 也是一個求得兩個數之最大公因數之方法, 不過在實際情況 (尤其是處理很大的數時) 由於分解質因數是很困難的事情, 所以仍是以輾轉相除法得最大公因數較管用. Proposition 1.6.2 重要之處是它很明確的告訴我們最大公因數長什麼樣子, 這在一些抽象理論的推導是有用的.

接下來我們可以利用 Proposition 1.4.3 將最小公倍數寫下.

Corollary 1.6.3. 假設 $a,b\in\mathbb{N}$ 且 $a,b>1$. 若 $a=p_1^{n_1}\cdots p_r^{n_r}$ 且 $b=p_1^{m_1}\cdots p_r^{m_r}$, 其中 $p_1,\ldots,p_r$ 為相異質數且 $n_i,m_i\geq 0$, 則

$$\operatorname{lcm}(a,b)=p_1^{\max\{n_1,m_1\}}\cdots p_r^{\max\{n_r,m_r\}}.$$

Proof. 由於 $ab=p_1^{n_1+m_1}\cdots p_r^{n_r+m_r}$ 利用 Proposition 1.4.3 以及 Proposition 1.6.2 知

$$\operatorname{lcm}(a,b)=\frac{ab}{\gcd(a,b)}=p_1^{n_1+m_1-\min\{n_1,m_1\}}\cdots p_r^{n_r+m_r-\min\{n_r,m_r\}}.$$

對任意二數 x,y, 不失一般性我們假設 $x\geq y$, 此時我們有 $\min\{x,y\}=y$ 且 $\max\{x,y\}=x$, 因此得 $x+y=\min\{x,y\}+\max\{x,y\}$. 所以對任意 $i\in\{1,\ldots,r\}$ 我們皆有 $\max\{n_i,m_i\}=n_i+m_i-\min\{n_i,m_i\}$, 因此得證本定理. □

當我們有多於兩個的整數時, 我們就可以利用質因數分解以及 Proposition 1.4.7 和 Proposition 1.4.9 將他們的最大公因數和最小公倍數寫下. 例如若 $a=p_1^{n_1}\cdots p_r^{n_r}$, $b=$

$p_1^{m_1}\cdots p_r^{m_r}$ 且 $c=p_1^{t_1}\cdots p_r^{t_r}$, 其中 $p_1,\ldots,p_r$ 為相異質數且 $n_i,m_i,t_i\geq 0$, 則

$$\gcd(a,b,c)=p_1^{\min\{n_1,m_1,t_1\}}\cdots p_r^{\min\{n_r,m_r,t_r\}},\quad \operatorname{lcm}(a,b,c)=p_1^{\max\{n_1,m_1,t_1\}}\cdots p_r^{\max\{n_r,m_r,t_r\}}.$$

Exercise 1.19. 試找出所有可能的數對 $a,b\in\mathbb{N}$ 滿足 $\gcd(a,b)=12$ 且 $\operatorname{lcm}(a,b)=360$.

Exercise 1.20. 假設 $a,b,n\in\mathbb{N}$ 若已知 $ab=n^2$ 且 $\gcd(a,b)=1$, 試證明存在 $c,d\in\mathbb{N}$ 滿足 $a=c^2$ 且 $b=d^2$.

Exercise 1.21. 假設 $m\in\mathbb{N}$ 且 p 是質數, 如果 $p^a\mid m$ 且 $p^{a+1}\nmid m$, 則我們稱 p^a 恰整除 m 且用 $p^a||m$ 表示之. 現假設 $p^a||m$ 且 $p^b||n$.

(1) 若已知 $a<b$, 試求 r 滿足 $p^r||m+n$.

(2) 試舉一個 $a=b$ 的例子使得 $p^r||m+n$ 且 $r>a$.

(3) 試求 s 滿足 $p^s||mn$.

(4) 試求 t 滿足 $p^t||m^n$.

(5) 假設 $m<p^{a+1}$, 試求 v 滿足 $p^v||m!$.

以下為 optional（不考）

Exercise 1.22. 利用以下步驟找出所有大於 1 的相異整數 a,b 滿足 $a^b=b^a$.

(1) 假設 $a<b$, 證明 $a\mid b$.

(2) 假設 $b=ak$, 證明 $a^{k-1}=k$.

(3) 證明若 a,k 皆為大於 1 的整數滿足 $a^{k-1}=k$, 則 $k=2$.

(4) 說明 $a=2,b=4$ 以及 $a=4,b=2$ 是所有滿足 $a^b=b^a$ 的相異正整數.