

# 「抽象代數」真的抽象嗎？(上)

沈淵源

「抽象代數」一詞是從英文的「abstract algebra」翻譯而來；作為數學的一門學科，主要研究對象是代數結構，比如群 (Groups)、環 (Rings)、體 (Fields)、模 (Modules)、向量空間 (Vector Spaces) 和代數 (Algebras)。這些代數結構，有的在十九世紀就已經有了正式的定義。這裡所謂的抽象 (abstract) 指的是純理論的，而不是一般所理解<sup>1</sup>「泛指籠統概括，難以想像」或是「具體」的相反詞。其實，「abstract」當成動詞乃是「提煉、萃取」；而當成名詞則為「萃取物、摘要」。在此文中，我們要從不同的個例如整數集、實係數的多項式集等，萃取其中之所以得到唯一分解性的關鍵性質；進而將這些關鍵性質當成此等代數結構的公設 (或公理)，由此建立並發展其上的理論架構。從這個層面上來看，正因為已經剔除了其他不相關的性質，那麼就很容易會令人感覺到太抽象了 (或有點抽象)、不容易理解。然而，這一切的一切都是由耳熟能詳、具體的例子當中所萃取出來的，絕非憑空想像得到；否則的話，整個建造出來的理論就不會有任何的應用價值。

首先，我們利用眾所周知整數系  $\mathbb{Z}$  的唯一分解性來求出不定方程

$$x^2 + y^2 = z^2$$

所有的整數解；並依樣畫葫蘆地，求出不定方程

$$y^3 = x^2 + 2$$

所有的整數解。然而，若想繼續仿照此法；來算出不定方程

$$y^3 = x^2 + 23$$

的整數解，那可就要碰一鼻子灰了。因此，我們得回頭詳細考察之所以擁有唯一分解性之代數結構的關鍵性質為何；如此一來，才能理解之所以碰了一鼻子灰的真正緣由。

<sup>1</sup>見教育部國語辭典簡編本 [網路版]，網址為 <http://140.111.34.46/jdict/main/cover/main.htm>

爲了方便討論起見，我們接著簡要的介紹最簡單也最常見的幾個代數結構群、環、體以及一些常用的術語；然後再回到整數環  $(\mathbb{Z}, +, \cdot)$  當中討論跟整除性相關的一些性質，並歸結在唯一分解性上。其次，我們轉向一樣耳熟能詳的多項式環並且刻意作了一個平行的考察；同樣地，也歸結在唯一分解性上。顯而易見，這兩者當中有諸多的相似之處。有一股莫名的興奮湧上心頭，讓你無可抗拒地想要抽取當中之所以擁有唯一分解性的關鍵條件；再將這些關鍵性質當成此等代數結構的公設（或公理），並發展其對應的理論。最後，回歸來時路；也就是前面所碰到的那些個別的實例  $\mathbb{Z}[\sqrt{-2}]$  以及  $\mathbb{Z}[\sqrt{-23}]$ ，在這個地方看來，那只不過是上面所建立之理論的一個特例或推論而已。至此，大功告成；你說，「抽象代數」真的抽象嗎？

## 1. 從畢達哥拉斯定理說起

打從國中開始，你就對畢達哥拉斯定理<sup>2</sup> 瞭若指掌；不僅如此，其實你或快或慢可以脫口說出好幾個邊長爲整數的直角三角形如  $(3,4,5)$ ,  $(5,12,13)$ ,  $(7,24,25)$  等。

當然你會問，到底這樣子的直角三角形其個數有多少呢？聰明的你立刻回答說：有無窮多個！因爲對任意的正整數  $n$ ,  $(3n, 4n, 5n)$  也是。但心理卻說：笨蛋，這還用問嗎？簡單極了！那麼爲了避開你的喃喃咕咕，我們就把這一類的算一個就是了；也就是說，我們假設三邊長爲整數且互質（亦即沒有公共的因子）。或許沉默幾分鐘之後，你會說：對任意的正偶數（爲何不要奇數？） $n$ ，數串  $(n^2 - 1, 2n, n^2 + 1)$  就是一個直角三角形彼此互質的三邊長。

其實，我們想知道的不僅僅是個數是否無限的問題而已；我們所要的乃是找出所有邊長爲整數的直角三角形。換句話說，我們要找出不定方程式

$$x^2 + y^2 = z^2$$

所有的整數解  $(x, y, z)$ 。上面提到的，只不過暗示我們可將所要求的解簡化爲彼此互質的三元數  $(x, y, z)$ 。當然，我們也只消求出正整數解即可。此等三元數通常稱之爲畢達哥拉斯原始三元數（primitive Pythagorean triples），簡稱畢氏原始三元數又稱素勾股數。

所以我們現在的任務是求出所有的素勾股數。假設  $(x, y, z)$  就是這樣子的一組素勾股數。首先，考慮奇偶性。對三元數  $(x, y, z)$  而言，共有 8 種不同的組合方式，如下表所顯示；這當中僅第三跟第五兩種組合是可能的素勾股數，而其他六種組合都是不可能發生的，其原因<sup>3</sup> 列在最右側一欄（注意：平方之後奇偶性不會改變）。

<sup>2</sup>畢達哥拉斯定理（簡稱畢氏定理），又稱勾股弦定理（簡稱勾股定理）；是幾何學上的一個基本定理，傳統上認爲是古希臘的畢達哥拉斯所證明。據說畢達哥拉斯證明了這個定理後，即斬了百頭牛慶祝，因此又稱百牛定理。在中國，《周髀算經》記載了勾股弦定理的一個特例，相傳是商代的商高發現，故又稱之爲商高定理。

<sup>3</sup>因爲奇數平方之後被 4 除餘 1，但偶數平方之後被 4 除盡。

序號	$x$ 或 $x^2$	$y$ 或 $y^2$	$z$ 或 $z^2$	可能嗎?	原因
1	奇	奇	奇	否	奇 + 奇 = 偶
2	奇	奇	偶	否	見註解 3
3	奇	偶	奇	✓	
4	奇	偶	偶	否	奇 + 偶 = 奇
5	偶	奇	奇	✓	
6	偶	奇	偶	否	偶 + 奇 = 奇
7	偶	偶	奇	否	偶 + 偶 = 偶
8	偶	偶	偶	否	三數不互質

然而，不定方程中的  $x, y$  是對稱的；這意味著，第三跟第五兩種組合可當成同一個來看待。因此之故，我們可假設  $x, z$  為奇數而  $y$  則為偶數；所以我們得到下面三個數

$$\alpha = \frac{z+x}{2}, \quad \beta = \frac{y}{2}, \quad \gamma = \frac{z-x}{2}$$

都是正整數，而且不難證明  $\alpha, \gamma$  兩數彼此互質<sup>4</sup>。將原不定方程寫成

$$y^2 = z^2 - x^2 = (z+x)(z-x) \implies \left(\frac{y}{2}\right)^2 = \frac{z+x}{2} \cdot \frac{z-x}{2},$$

因而得到這三個正整數的一個關係式如下：

$$\beta^2 = \alpha\gamma$$

根據算術基本定理<sup>5</sup>，不難看出  $\alpha, \gamma$  兩者本身都是完全平方數<sup>6</sup>；也就是說，存在二正整數  $m, n$  使得

$$\alpha = m^2, \quad \gamma = n^2。$$

故得原先的畢達哥拉斯三元數為

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2。$$

至此，我們已經找出所有的素勾股數；不僅僅有無窮多組，更帥的是可用上面很簡單的公式表達出來。而其他的勾股數就是這些素勾股數的常數倍冠上自由選取的正負號，如此這般的我們得到不定方程式  $x^2 + y^2 = z^2$  所有的整數解。

<sup>4</sup>因為任何這兩個數的質因子  $p$  必整除這兩個數的和(=  $z$ ) 還有這兩個數的差(=  $x$ )，但這又導致  $p$  整除  $y$  (∵  $p \mid y^2 = z^2 - x^2 \implies p \mid y$ )；因而  $p$  為  $x, y, z$  的一個公因數，此與假設  $(x, y, z)$  是一組素勾股數不合。

<sup>5</sup>任何正整數都可以寫成其質因數的乘積且此種表示法是唯一的。

<sup>6</sup>將這兩個數寫成質因數的乘積  $\alpha = p_1^{a_1} \cdots p_k^{a_k}$ ， $\gamma = q_1^{b_1} \cdots q_k^{b_k}$ 。但  $\alpha$  與  $\gamma$  互質，因而得知這些質因數  $p_i, q_j$  必定兩兩互異，所以  $\beta^2 = \alpha\gamma$  的質因數乘積表示法就是  $p_1^{a_1} \cdots p_k^{a_k} q_1^{b_1} \cdots q_k^{b_k}$ ；因此這些次幂  $a_i, b_j$  都是偶數，故得證  $\alpha, \gamma$  都是完全平方數。

定理. 不定方程式  $x^2 + y^2 = z^2$  的整數解  $(x, y, z)$  如下:

$$x = \pm k(m^2 - n^2), \quad y = \pm k(2mn), \quad z = \pm k(m^2 + n^2);$$

其中正負號可自由選取,  $k$  為任意正整數; 而  $m, n$  則為一奇一偶彼此互質的兩個正整數。

下面網頁<sup>7</sup> 中提供了一個 Javascript 計算器, 用以計算這些數串; 不妨試試如何。下表列出當  $m, n$  限制在 10 以內的情況下所有的素勾股數。

$n$	$m$	$(x, y, z)$	$n$	$m$	$(x, y, z)$
1	2	(3, 4, 5)	3	8	(55, 48, 73)
1	4	(15, 8, 17)	4	5	(9, 40, 41)
1	6	(35, 12, 37)	4	7	(33, 56, 65)
1	8	(63, 16, 65)	4	9	(65, 72, 97)
2	3	(5, 12, 13)	5	6	(11, 60, 61)
2	5	(21, 20, 29)	5	8	(39, 80, 89)
2	7	(45, 28, 53)	6	7	(13, 84, 85)
2	9	(77, 36, 85)	6	9	(45, 108, 117)
3	4	(7, 24, 25)	7	8	(15, 112, 113)
3	6	(27, 36, 45)	8	9	(17, 144, 145)

## 2. 求 $y^3 = x^2 + 2$ 的整數解

在上一節中, 我們稍稍的品嚐到算術基本定理的美妙滋味; 這裡所用到的, 說穿了其實就是整數的唯一分解性。現在讓我們依樣畫葫蘆, 試著來找出不定方程

$$y^3 = x^2 + 2$$

所有的整數解。

假設  $x, y \in \mathbb{Z}$  滿足不定方程式  $y^3 = x^2 + 2$ , 並將此式寫成

$$y^3 = x^2 + 2 = (x + \sqrt{-2})(x - \sqrt{-2}).$$

<sup>7</sup><http://www.math.clemson.edu/~simms/neat/math/pyth/>

很自然的, 上式引導我們去思考長的像  $a + b\sqrt{-2}$ ,  $a, b \in \mathbb{Z}$  之類的複數; 在代數上, 通常以符號  $\mathbb{Z}[\sqrt{-2}]$  表示之, 故

$$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}.$$

這個集合  $\mathbb{Z}[\sqrt{-2}]$  跟整數集  $\mathbb{Z}$  有許許多多相似的地方。

首先, 兩者都是複數集  $\mathbb{C}$  的子集; 所以也都承繼了當中加法與乘法的運算, 以及其上的一些代數結構。這兩個耳熟能詳的加、乘運算就是一般所謂的二元運算。更明確的說, 集合  $S$  上的一個二元運算其實就是一個從  $S \times S$  到  $S$  的函數而已,

$$f : S \times S \rightarrow S.$$

所以集合  $S$  上面的兩個元素  $\alpha, \beta$  經過  $f$  運算之後, 得到的結果即函數值  $f(\alpha, \beta)$  仍然還是在集合  $S$  上。因此之故, 當我們說這個運算具有封閉性, 只不過爲了強調此點而已。習慣上, 我們將運算符號寫在兩個元素的中間; 所以

$$\alpha f \beta$$

指的就是  $f(\alpha, \beta)$ , 就如同「和」與「積」我們習慣寫成  $\alpha + \beta$  與  $\alpha \cdot \beta$  而不是  $+(\alpha, \beta)$  與  $\cdot(\alpha, \beta)$  一樣的道理。

顯而易見, 複數的加法與乘法運算在集合  $\mathbb{Z}[\sqrt{-2}]$  之中跟在整數集  $\mathbb{Z}$  之中一樣都具有封閉性; 這是代數結構的第一步, 其他的代數性質等下一節再詳細解說。當務之急乃是找出不定方程

$$y^3 = x^2 + 2$$

所有的整數解。如上所說, 在集合  $\mathbb{Z}[\sqrt{-2}]$  中; 上式可分解爲

$$y^3 = x^2 + 2 = (x + \sqrt{-2})(x - \sqrt{-2}),$$

而且也可證明右側的兩個數  $x + \sqrt{-2}$  與  $x - \sqrt{-2}$  彼此是互質的。假設  $(\mathbb{Z}[\sqrt{-2}], +, \cdot)$  跟整數系  $(\mathbb{Z}, +, \cdot)$  一樣擁有所需要的代數結構。因此唯一分解性告訴我們, 這兩個數本身都是複數集  $\mathbb{Z}[\sqrt{-2}]$  之中的完全立方數; 也就是說, 存在  $a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$  使得

$$x + \sqrt{-2} = (a + b\sqrt{-2})^3.$$

將右式展開, 整理後得到

$$x + \sqrt{-2} = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2};$$

並比較等號兩側的虛部, 得知

$$1 = 3a^2b - 2b^3 = (3a^2 - 2b^2)b \in \mathbb{Z}。$$

因而得到

$$b = \pm 1 \quad \text{且} \quad 3a^2 - 2b^2 = \pm 1;$$

故得

$$b^2 = 1 \implies 3a^2 - 2 = \pm 1 \implies 3a^2 = 2 \pm 1 = 3 \text{ 或 } 1。$$

因此, 我們一定有

$$a^2 = 1 \implies a = \pm 1;$$

再回到上面的展開式, 得知

$$x = a^3 - 6ab^2 = (\pm 1)^3 - 6(\pm 1) = \mp 5。$$

最後, 將  $x = \pm 5$  代回原不定方程

$$y^3 = x^2 + 2;$$

故得  $y = 3$ , 因而原不定方程之整數解為

$$x = \pm 5, \quad y = 3。$$

至此, 我們已經成功地找到了兩個不定方程之整數解; 第一個在上節, 擁有無窮多組解; 第二個就在上面, 僅有兩組解。因為是如此的成功, 我們得打鐵趁熱一起來找出另一個不定方程式

$$y^3 = x^2 + 23$$

的整數解。如上, 假設  $x, y \in \mathbb{Z}$  滿足不定方程  $y^3 = x^2 + 23$ ; 將此式寫成

$$y^3 = x^2 + 23 = (x + \sqrt{-23})(x - \sqrt{-23})。$$

很自然的, 我們工作的地方變成

$$\mathbb{Z}[\sqrt{-23}] = \{a + b\sqrt{-23} \mid a, b \in \mathbb{Z}\}。$$

不難證明右側的兩個數  $x + \sqrt{-23}$  與  $x - \sqrt{-23}$  彼此是互質的; 因此這兩個數本身都是  $\mathbb{Z}[\sqrt{-23}]$  中的完全立方數; 也就是說, 在  $\mathbb{Z}[\sqrt{-23}]$  當中有某個數  $a + b\sqrt{-23}$  使得

$$x + \sqrt{-23} = (a + b\sqrt{-23})^3。$$

將右式展開, 整理後得到

$$x + \sqrt{-2} = (a^3 - 69ab^2) + (3a^2b - 23b^3)\sqrt{-23};$$

並比較等號兩側的虛部, 得知

$$1 = 3a^2b - 23b^3 = (3a^2 - 23b^2)b \in \mathbb{Z}.$$

因而得到

$$b = \pm 1 \quad \text{且} \quad 3a^2 - 23b^2 = \pm 1;$$

故得

$$b^2 = 1 \implies 3a^2 - 23 = \pm 1 \implies 3a^2 = 23 \pm 1 = 24 \text{ 或 } 22.$$

因此, 我們一定有

$$a^2 = 8.$$

顯而易見, 沒有這樣子的整數存在; 結論是, 原不定方程

$$y^3 = x^2 + 23$$

無解。然而, 隨便觀察即可得知原不定方程有整數解為

$$x = \pm 2, \quad y = 3.$$

這到底是怎麼一回事呢? 幾分鐘前, 還悠然自得的沉醉在成功的高山上; 怎麼才一下下的功夫而已, 卻跌落至深不可測的山坳低谷裡。聰明的你, 可告訴我?

### 3. 代數結構簡介

為了方便介紹所要學的代數結構, 難免需要採用一些術語; 雖說是單調乏味, 在此盡可能用閒話家常的方式為之, 還請忍耐片刻。

我們接著談一個集合上之二元運算的種種性質。一個集合若是沒有任何的二元運算, 那當然就沒什麼代數結構可言。這就好比在一個團體裡面, 若當中兩兩彼此都沒有任何互動、沒有任何關係; 那麼這樣子的一個團體只不過是互不相干的一些個體所成的一個集合體而已, 沒有任何的結構可言。當然, 這樣子的團體就沒有被研究的價值, 因為不可能具有任何的影響力。

令  $*$  為集合  $S$  上的一個二元運算。

- 我們說運算  $*$  是可結合的 (associative); 若

$$(a * b) * c = a * (b * c), \quad \forall a, b, c \in S。$$

- 我們說運算  $*$  是可交換的 (commutative); 若

$$a * b = b * a, \quad \forall a, b \in S。$$

- 元素  $e \in S$  稱之為運算  $*$  的一個單位元素 (identity element); 若

$$a * e = e * a = a, \quad \forall a \in S。$$

- 若集合  $S$  擁有運算  $*$  的一個單位元素  $e$ ; 則我們說元素  $u \in S$  在集合  $S$  中具有反元素 (inverse), 如果存在  $v \in S$  使得

$$u * v = v * u = e。$$

現在回到複數集  $\mathbb{C}$ 。在  $\mathbb{C}$  中有兩個我們熟悉的二元運算加  $+$  與乘  $\cdot$ ; 就是這兩個二元運算使得複數集  $\mathbb{C}$  擁有豐富無比的代數結構。

- (i) 加法運算  $(+)$  在複數集  $\mathbb{C}$  上具有封閉性 (封)、結合性 (結) 並擁有單位元素  $0 + 0i$  (單) 且每一元素  $a + bi$  都有反元素  $(-a) + (-b)i$  (反), 這就是所謂的群 (group) 的代數結構。

一般而言, 集合  $S$  上的一個二元運算  $*$ ; 若滿足上述的封、結、單、反四個性質, 我們就說  $S$  在運算  $*$  之下形成一個群或說  $(S, *)$  是一個群。如果運算  $*$  是可交換的; 那麼理所當然, 我們就說  $(S, *)$  是一個交換群 (commutative group)。通常又稱為阿貝爾群 (abelian group), 為的是要紀念數學家阿貝爾<sup>8</sup>。複數集  $(\mathbb{C}, +)$  在加法運算之下當然是一個阿貝爾群。

- (ii) 乘法運算  $(\cdot)$  在複數集  $\mathbb{C}$  上具有封閉性、結合性並擁有單位元素  $1 + 0i$  而且每一個非零元素  $a + bi \neq 0$  都有反元素  $\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$ , 又乘法也有交換性; 換句話說,  $(\mathbb{C} \setminus \{0\}, \cdot)$  也是一個阿貝爾群。

<sup>8</sup> 尼爾斯·亨利克·阿貝爾 (Niels Henrik Abel, 1802年~1829年), 挪威數學家, 以證明五次方程的根式解的不可能性而聞名。1825年得到政府資助, 遊學柏林和巴黎。生前不得志, 無法獲得教席俾專心研究, 最後因肺結核在挪威的弗魯蘭逝世。死後兩天, 來自柏林的聘書才寄到家中。跟同樣早逝的伽羅華一同被奉為群論的先驅。現代有以他名字命名的阿貝爾獎。



(iii) 這兩個運算, 並不是獨立存在毫無關連的; 其相關性就是所謂的乘法運算  $(\cdot)$  對加法運算  $(+)$  的分配律, 即

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma, \quad \forall \alpha, \beta, \gamma \in \mathbb{C}.$$

這就是所謂的體 (field) 的代數結構。一般而言, 擁有兩個二元運算  $*_1, *_2$  的集合  $S$ ; 若滿足如上述  $\mathbb{C}$  之性質者, 我們就說  $S$  在運算  $*_1, *_2$  之下形成一個體或說  $(S, *_1, *_2)$  是一個體。更明確的說, 令  $*_1, *_2$  為集合  $S$  的兩個二元運算; 我們說  $(S, *_1, *_2)$  是一個體, 若滿足下述三個性質:

- (i)  $(S, *_1)$  是一個阿貝爾群。
- (ii)  $(S \setminus \{e_1\}, *_2)$  也是阿貝爾群, 此處  $e_1$  為運算  $*_1$  的單位元素。
- (iii) 運算  $*_2$  對 運算  $*_1$  的分配律成立:

$$a *_2 (b *_1 c) = (a *_2 b) *_1 (a *_2 c), \quad \forall a, b, c \in S.$$

在我們所熟悉的例子當中, 除了有理數體  $(\mathbb{Q}, +, \cdot)$ 、實數體  $(\mathbb{R}, +, \cdot)$  以及複數體  $(\mathbb{C}, +, \cdot)$  之外;

$$(\mathbb{Q}, +, \cdot) \subset (\mathbb{R}, +, \cdot) \subset (\mathbb{C}, +, \cdot)$$

還有那些介於有理數體及複數體之間許許多多的數體<sup>9</sup> (number fields), 更有那數也數不清擁有質數個數的有限體<sup>10</sup>  $\mathbb{Z}_p$  (prime finite fields)。

那我們前面的老朋友整數系  $(\mathbb{Z}, +, \cdot)$  又是怎麼樣的一付德性呢? 萬事俱備, 只欠東風; 不過這個缺陷乃是先天的, 無法補救。所缺的就是非零元素的乘法反元素除了  $\pm 1$  之外, 都不存在。這就是所謂的環 (ring) 的代數結構。更明確的說, 擁有兩個二元運算  $*_1, *_2$  的集合  $S$ ; 若滿足下述三個性質者, 我們就說  $S$  在運算  $*_1, *_2$  之下形成一個環或說  $(S, *_1, *_2)$  是一個環。

- (i)  $(S, *_1)$  是一個阿貝爾群。
- (ii) 運算  $*_2$  是可結合的。

<sup>9</sup>這些體可看成是佈於有理數體的向量空間, 若其維數是有限的就稱之為數體。

<sup>10</sup>當然也有非質數個數的有限體, 但其個數必定是某一質數的次幂。

(iii) 運算  $*_2$  對運算  $*_1$  的左、右分配律都成立：

$$a *_2 (b *_1 c) = (a *_2 b) *_1 (a *_2 c), \quad \forall a, b, c \in S,$$

$$(b *_1 c) *_2 a = (b *_2 a) *_1 (c *_2 a), \quad \forall a, b, c \in S.$$

習慣上，我們把環裡面的第一個運算稱之為加法，用符號「+」來表示；而第二個運算則稱之為乘法，用符號「 $\cdot$ 」來表示。因此，我們也習慣將第一個運算的單位元素稱之為加法單位元素且用「0」來表示；而第二個運算的單位元素，若存在則稱之為乘法單位元素且用「1」來表示。記住，這只是一個習慣用法；所以當你看到在一個環或體裡面的0(或1)，那指的就是加法單位元素0(或乘法單位元素1)，而跟整數裡的0(或1)一點關係也沒有。

當然啦，整數環  $(\mathbb{Z}, +, \cdot)$  遠比一般的環還好很多；那就是第二個運算不僅有單位元素而且還是可交換的，這一種環通常稱之為具乘法單位元素的交換環 (commutative ring with unit)。與此相對的有佈於實數體的  $n$  階方陣環  $(M_n(\mathbb{R}), +, \cdot)$ ，這是一個擁有乘法單位元素的非交換環 (noncommutative ring with unit)；還有那偶整數環  $(2\mathbb{Z}, +, \cdot)$  則是不具乘法單位元素的交換環 (commutative ring without unit)。

其實，整數環還有更細膩的性質；譬如說，任何兩個非零元素相乘還是非零元素。這就是所謂的整域 (integral domain)<sup>11</sup> 的代數結構。一般的環，如  $\mathbb{Z}_6$  就包含有非零元素 2 及 3 相乘之後等於零；還有矩陣環中，

$$\begin{pmatrix} 7 & 11 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 11 \\ 0 & -7 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

也有類似的現象發生 (這樣子的非零元素就是所謂的零因子)。

總而言之，整數環既然擁有如此多采多姿的面貌；那就值得我們打著燈籠，再一次聚精會神的來把這位交往多年的老朋友瞧個仔細。

#### 4. 整數的唯一分解性

現在回到小學生所學的整數  $\mathbb{Z}$ ，包括正整數、負整數及零；當然對負數的理解得等到高年級的時候才比較成熟，因此讓我們先停留在自然數(即正整數)上且做一回的小小學生。數學

<sup>11</sup>沒有零因子的交換環就稱為整域。

家克羅內克 L. Kronecker<sup>12</sup> 曾說：「上帝創造了自然數，其餘都是人的工作。」其實他對上帝的認識，不僅太膚淺而且層次不高。上帝的創造，除了大自然外還有許許多多的活物；而其創造的最高峰乃是按著祂自己形像、樣式所造的人，所以人只不過是上帝的傑作而已。

這裡實在是有太多的東西好講，在此只能談談與代數結構相關的部分。先從整除性說起。我們說一個數  $a$  整除一個數  $b$ ，如果有一個數  $c$  使得

$$b = ac;$$

而以符號  $a \mid b$  表示之。換句話說， $a$  除  $b$  之後沒有餘數。 $a$  稱為  $b$  的一個因子，而  $b$  則稱為  $a$  的一個倍數。例如： $6 \mid 12$ ， $(-14) \mid 98$ ，然而  $7 \nmid 11$ 。

若給你一個數，你就試著要把這個數分解成兩個數的乘積；還不夠，那就再分解，一直到沒辦法再分解為止。此乃基於小數容易掌控的心理罷！如

$$360 = 36 \times 10 = 6 \times 6 \times 2 \times 5 = 2 \times 3 \times 2 \times 3 \times 2 \times 5。$$

不能再分解的數就是所謂的質數 (prime numbers)。更明確的說，一個數  $p > 1$  稱之為質數；若此數僅有的因子為 1 及  $p$ 。質數是非常的重要，如下面主要定理所顯示的；對乘法而言，質數乃是建造整數的磚塊，是整數當中最基本的元素。

也許你會說，所有這些東東我老早就知道了；沒什麼新奇的，簡直無聊透頂。那麼，我請問你；你雖然知道質數有無窮多個，但你可知道

「目前已知最大的質數是多少嗎？」

答案當然不是「要有多大就有多大」，為什麼呢？想想看，隨便給你一個整數，你能馬上回答此數就是質數嗎？也許你說：給我些許時間我就可以給你答案。好吧！那你就隨便挑一個一百位數，再試試看如何？其實，你的知道只是理論上的知道，而不是實作上的知道。判斷一個整數是否為質數乃是一個大挑戰，但已被證實存在有演算法，可在多項式時間內完成[1]。在此先介紹兩類有趣的質數：梅仙質數 (Mersenne Primes) 及費馬質數 (Fermat Primes)。

---

<sup>12</sup>利奧波德·克羅內克 (Leopold Kronecker, 1823年12月7日~1891年12月29日)，德國數學家與邏輯學家，出生於利格尼茨 (現屬波蘭的萊格尼察)，卒於柏林。他認為算術與數學分析都必須以自然數為基礎。這與數學家喬治·康脫 (Georg Cantor) 的觀點相互對立。克羅內克是恩斯特·庫默爾 (Ernst Kummer) 的學生和終身摯友。

- 梅仙質數: 形如  $M_p = 2^p - 1$  的質數稱之為梅仙質數。此類質數與完全數有關, 目前已知最大的質數就是這一類的質數為

$$2^{43112609} - 1.$$

這是已被發現的第四十五個 (按時間順序) 梅仙質數, 是一個擁有約一千三百萬 12,978,189 位數的龐然大數; 由 GIMPS<sup>13</sup> 團隊於 2008 年 8 月 23 日在美國洛杉磯 UCLA 數學系的一部電腦發現, Edson Smith 是負責安裝及維護 GIMPS 軟體於其上的人。在此特別推薦克瑞斯·迦爾德威爾 (Chris K. Caldwell) 所精心設計的質數網頁[7], 值得進去遨遊一番。

- 費馬質數: 形如  $F_n = 2^{2^n} + 1$  的質數稱之為費馬質數。前面五個費馬質數為

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257 \text{ 與 } F_4 = 65537.$$

當年費馬因此推斷所有這一類型的數都是質數, 但奇怪的是, 這五個數是目前僅有的費馬質數。於是有人猜測說: 僅存在有限多個費馬質數。你認為呢?

與質數相關的趣事, 還有一籬筐; 值得提的, 至少有底下兩個響叮噹的猜測: 孿生質數猜測 (Twin Prime Conjecture) 及哥德巴赫猜測 (Goldbach Conjecture)。

- 孿生質數猜測: 即使從小質數表觀察, 不難察覺有如下的質數對出現

$$(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), \dots;$$

稱之為孿生質數。此種孿生質數是否有無窮多呢? 答案是, 不知道。等你來解決!

- 哥德巴赫猜測: 是否每一個大於 2 的偶數都可以寫成兩個奇質數的和呢? 這就是名滿天下哥德巴赫猜測; 即使有電腦侍候在旁的今天, 至今尚未找到反例, 是數論中存在最久的未解問題之一。目前, 這方面的進展還是停留在 1937 年維諾格拉多夫 (Vinogradov) 所證明的結果<sup>14</sup> 還有陳景潤在 1966 年的結果<sup>15</sup>。

<sup>13</sup>The Great Internet Mersenne Prime Search 的縮寫, 這是此大搜索團隊所發現的第 11 個。巧的是, 無獨有偶; 才隔了兩個禮拜 (2008 年 9 月 6 日), 在德國科隆 (Cologne) 附近 Langenfeld 的 Hans-Michael Elvenich 又發現第四十六個。不過, 比上面那一個小; 為  $2^{37156667} - 1$ 。七個月後, 2009 年 4 月 12 日又發現第四十七個, 還是比上面那一個小; 為  $2^{42643801} - 1$ 。最大梅仙質數發現之前的三個是  $2^{32582657} - 1$ ,  $2^{30402457} - 1$  與  $2^{25964951} - 1$  分別在 2006 年 9 月 4 日, 2005 年 12 月 15 日與 2005 年 2 月 18 日發現。詳情請進入其網站, 網址為 <http://www.mersenne.org>。

<sup>14</sup>他證明了: 「每一個足夠大的奇數可以寫成三個奇質數的和。」

<sup>15</sup>他證明了: 「任何一個足夠大的偶數, 都可以寫成兩個數的和; 其一為奇質數, 另一則為奇質數的乘積其個數不超過 2。」(簡稱「1+2」) 此乃哥德巴赫猜想研究上的里程碑, 而他所發表的成果也被稱之為陳氏定理。

這裡我們要專注在數的乘法結構上，此間最主要定理可追溯到歐幾里得的年代；這就是唯一分解性定理，通常稱之為算術基本定理。因有甚多與整數相關的重要結果，都是由它推論而來；故冠此頭銜，也是理所當然，更是實至名歸。這定理簡單說就是，每一個數可唯一寫成其質因子的乘積。譬如說， $360 = 2 \times 3 \times 2 \times 3 \times 2 \times 5 = 2^3 \times 3^2 \times 5$ 。唯一指的是，其質因子為 2, 3 及 5 而其次幂分別是 3, 2 及 1；這些數乃是由 360 所唯一決定的。

必須一提的是所謂的良好序原理 (Well-Ordering Principle)，此原理乃是自然數最基本的假設；跟數學歸納法原理 (Principle of Mathematical Induction) 是等價的，在很多的場合我們需要此二老的幫忙。

**良序原理：**任何正整數的非空集合必擁有一最小的元素。

**數學歸納法原理：**令  $P(n)$  是一個與整數有關的敘述使得  $P(n_0)$  成立且<sup>16</sup> 對所有整數  $n_0 \leq j \leq k$ ,  $P(j)$  成立  $\implies P(k+1)$  也成立。則對所有的整數  $n \geq n_0$ ,  $P(n)$  都成立。

現在回到整數環  $\mathbb{Z}$  來，因為在這兒工作比較方便一些。整除的觀念暢行無阻，甚至於連文字都不需修改；只消把那邊的「數」，理解成整數即可。質數的觀念也是一樣，變成多出來負質數而已。底下我們列出來一些整除性的基本性質，得勞駕動動手將這些簡單的證明完成。

1.  $a \mid a, \quad \forall a \neq 0$  (反身律)
2.  $a \mid b$  且  $b \mid c \implies a \mid c$  (遞移律)
3.  $a \mid b$  且  $a \mid c \implies a \mid mb + nc$  (線性律)
4.  $a \mid b \implies ma \mid mb$  (乘法律)
5.  $ma \mid mb$  且  $m \neq 0 \implies a \mid b$  (消去律)
6.  $\pm 1 \mid a$  ( $\pm 1$  整除每一個數)
7.  $a \mid 0$  (每個數都整除零)
8.  $0 \mid a \implies a = 0$  (唯零整除零)
9.  $a \mid b$  且  $b \neq 0 \implies |a| \leq |b|$  (比較律)
10.  $a \mid b$  且  $b \mid a \implies |a| = |b|$

<sup>16</sup>這是比較一般化的版本；通常的版本，我們取  $n_0 = 1$  而此處的條件也可取代為：對某一整數  $k \geq n_0$ ,  $P(k)$  成立  $\implies P(k+1)$  也成立。

11.  $a \mid b$  且  $a \neq 0 \implies (b/a) \mid b$

令  $n \in \mathbb{Z}$  且令  $p$  為一質數。則若  $n \neq 0$ , 必存在一非負整數  $a$  使得

$$p^a \mid n \quad \text{但} \quad p^{a+1} \nmid n。$$

這個  $a$  就稱之為  $n$  在質數  $p$  的階數 (the order of  $n$  at  $p$ ), 以符號  $\text{ord}_p n$  表示之。粗略言之,  $\text{ord}_p n$  就是  $p$  整除  $n$  的次數。若  $n = 0$ , 則我們定義  $\text{ord}_p n = \infty$ 。注意到, 另一個極端為

$$\text{ord}_p n = 0 \iff p \nmid n。$$

因此對一個非零整數  $n$  而言, 只有在其質因子的階數會是正的; 而在其他不整除  $n$  的質數, 其階數則全部都是 0。

接著我們逐步預備好要證明算術基本定理 (Fundamental Theorem of Arithmetic) 的工具。首先處理存在性的部分, 這只是良序原理或數學歸納法原理的一個簡單練習而已。按慣例, 應該勞駕您動動手將這簡單的證明完成才是; 然而為了完全起見, 特別附上兩個不同的論證方式提供初學者參考。

**引理 1.** 任何非零整數都可以寫成質數的乘積。

**證明一.** 若否, 則下列集合為非空集合

$$S = \{x \in \mathbb{N} \mid x \text{ 不是質數的乘積} \} \neq \emptyset。$$

良序性告訴我們,  $S$  擁有一最小的正整數  $s$ ; 故  $s$  本身不是質數, 因此我們有  $s = mn$ , 此處  $1 < m, n < s$ 。然而,  $m, n$  都是比  $s$  小的正整數; 因而都是質數的乘積, 所以  $s$  也是質數的乘積。矛盾出現, 故得證。

**證明二.** 僅需證明  $\geq 2$  的正整數可寫成質數的乘積。

- (i) 2 是一個質數。
- (ii) 假設  $2 < N$  且假設對所有介於 2 與  $N$  的整數都可寫成質數的乘積。若  $N$  是質數, 則證明完畢; 否則我們有

$$N = mn, \quad \text{此處} \quad 2 \leq m, n < N。$$

然而, 假設告訴我們;  $m, n$  都是質數的乘積, 所以  $N$  也是質數的乘積。據數學歸納法原理, 故得證。

物以類聚，將同一質數擺在一起；我們可以將一個整數  $n$  寫成  $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ ，其中  $p_i$  為質數且  $a_i$  為正整數。我們會採用底下更方便的方式來表達：

$$n = (-1)^{\text{sgn}(n)} \prod_p p^{a(p)},$$

此處  $\text{sgn}(n) = 0$  或  $1$  隨著  $n$  的正、負來決定，而乘積中的  $p$  是對所有的質數。次冪  $a(p)$  乃是非負整數；當然，除了有限多個質數外，此次冪都是零。譬如說，前面所看到過的那個數  $n = 360$ ；我們有  $\text{sgn}(n) = 0$ ， $a(2) = 3$ ， $a(3) = 2$ ， $a(5) = 1$ ，而其餘的  $a(p) = 0$ 。

**算術基本定理.** 對任何非零整數  $n$  存在一質數分解式

$$n = (-1)^{\text{sgn}(n)} \prod_p p^{a(p)},$$

其次冪由  $n$  所唯一決定。實際上，我們有  $a(p) = \text{ord}_p n$ 。

**引理 2.** 若  $a, b \in \mathbb{Z}$  且  $b > 0$ ，則  $\exists q, r \in \mathbb{Z}$  使得

$$a = qb + r, \quad \text{其中 } 0 \leq r < b.$$

**證明.** 考慮集合  $S$  如下： $S = \{a - xb \mid x \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$ 。顯而易見， $S$  為非空集合；良序性告訴我們， $S$  擁有一最小的非負整數  $r$ ，故有一整數  $q$  使得  $0 \leq r = a - qb$ 。我們必須證明  $r < b$ 。若否，則

$$r = a - qb \geq b \implies 0 \leq r - b = a - (q+1)b < r;$$

因而得到在  $S$  中比  $r$  還小的非負整數  $r - b$ ，這跟  $r$  的身分不合，故得證。

引理 2 就是所謂的長除法 (long division)，又稱為歐幾里德演算法 (Euclid's Algorithm)；雖然不醒眼，卻是相當關鍵的性質。多項式環也具有這個性質。所以談完多項式環的唯一分解性後，我們會將此性質抽象化；而滿足此等性質的整域，理所當然就稱為歐幾里德整域 (Euclidean Domains)。歐幾里德整域也同樣會具有唯一分解性。

**定義.** 若  $a_1, \dots, a_n \in \mathbb{Z}$ ，定義集合  $(a_1, \dots, a_n)$  為

$$(a_1, \dots, a_n) = \{a_1 x_1 + \cdots + a_n x_n \mid x_1, \dots, x_n \in \mathbb{Z}\}.$$

令  $I = (a_1, \dots, a_n)$ 。顯而易見，這個集合在加法與減法之下都具有封閉性；亦即，任何  $I$  裡頭的兩個元素的和或差仍然還是裡頭的元素。不僅如此，若將裡頭的元素乘上任何的整數仍

然還是裡頭的元素。也就是說，不管你的整數來源如何；或在  $I$  裡頭，或不在  $I$  裡頭；一旦乘上  $I$  裡頭的元素，就會被吸入，成為裡頭的一份子。在環論的術語，這就是所謂的理想；因此  $I$  是整數環  $\mathbb{Z}$  中的一個理想。

**引理 3.** 若  $a, b \in \mathbb{Z}$ ，則存在  $d \in \mathbb{Z}$  使得  $(a, b) = (d)$ 。

**證明.** 若  $a = b = 0$ ，那麼樣就沒甚好證的；故假設  $a, b$  不全為零，因而  $S = (a, b) \cap \mathbb{N} \neq \emptyset$ 。良序性告訴我們， $S$  擁有一最小的正整數  $d$ 。顯而易見， $(d) \subseteq (a, b)$ ；我們必須證明，反方向  $(a, b) \subseteq (d)$  也對。

假設  $x \in (a, b)$ 。引理 2 告訴我們，存在  $q, r \in \mathbb{Z}$  使得

$$x = qd + r, \quad \text{其中 } 0 \leq r < d.$$

顯而易見， $r = x - qd \in (a, b)$ ；因此  $0 \leq r < d$  及  $d$  是  $(a, b)$  裡最小的正整數，讓我們看見  $r = 0$  是唯一的歸宿。所以得到  $x = qd \in (d)$ ，故得證。

**定義.** 令  $a, b \in \mathbb{Z}$ 。  $d$  稱之為  $a$  與  $b$  的一個最大公因數；若

- (i)  $d$  是  $a$  與  $b$  的公因數，
- (ii) 任何其它  $a$  與  $b$  的公因數都整除  $d$ 。

特別注意到，定義中說的是一個最大公因數。那到底有幾個呢？若  $c$  是另一個，那麼我們就必定有

$$c \mid d \quad \text{且} \quad d \mid c,$$

因而  $c = \pm d$ 。故兩個整數的最大公因數，若存在，就剛剛好有兩個，其間只差一個符號。通常用符號  $\gcd(a, b)$  來表示那個正的最大公因數。

**引理 4.** 令  $a, b \in \mathbb{Z}$ 。若  $(a, b) = (d)$ ，則  $d$  是  $a$  與  $b$  的一個最大公因數。

**證明.** (i) 因為  $a, b \in (a, b) = (d)$ ，故  $d$  是  $a$  與  $b$  的公因數。

(ii) 假設  $c$  是  $a$  與  $b$  的公因數。因此  $c$  整除任何  $a$  與  $b$  的線性組合，而  $d \in (d) = (a, b)$  就是  $a$  與  $b$  的一個線性組合；故  $c \mid d$ 。

這就是最大公因數的存在性定理。有兩點值得一提：

- (i) 上面的證明方法，雖說是簡潔漂亮，但美中不足的是；在整個證明的過程當中，我們看不到怎麼去找  $x$  與  $y$  使得  $xa + yb = d$  的蛛絲馬跡。請參閱密碼學之旅[8] 第二章數論輕鬆遊中所提出的三個計算最大公因數的演算法。



(ii) 注意到, 此  $d$  在  $(a, b)$  中是最小的正整數; 但卻是  $a$  與  $b$  的最大公因數, 值得回味。

**定義.** 我們說整數  $a$  與  $b$  是互質的; 若其僅有的公因數只有  $\pm 1$ , 整數中的可逆元素。

**定理 Z.** 假設  $a \mid bc$  而且  $\gcd(a, b) = 1$ , 則  $a \mid c$ 。

**證明.** 因  $\gcd(a, b) = 1$ , 存在  $x, y \in \mathbb{Z}$  使得

$$xa + yb = 1。$$

兩邊同時乘上  $c$ , 得到

$$xac + ybc = c。$$

根據假設  $a \mid bc$ , 得知  $a$  整除上式左側的每一項; 因此

$$a \text{ 整除左側} = \text{右側} = c,$$

故得證。

**推論 1.** 若  $p$  為質數且  $p \mid bc$ , 則  $p \mid b$  或  $p \mid c$ 。

**證明.** 因  $p$  為質數, 僅有的因數為  $\pm 1, \pm p$ ; 故得

$$\gcd(p, b) = p \quad \text{或} \quad \gcd(p, b) = 1。$$

因此我們有

(i)  $\gcd(p, b) = p$ : 因  $\gcd(p, b) \mid b \implies p \mid b$ ,

(ii)  $\gcd(p, b) = 1$ : 定理 Z  $\implies p \mid c$ ;

故得證。若將推論 1 寫成其反逆敘述, 則有

**推論 1'.** 若  $p$  為質數滿足  $p \nmid b$  且  $p \nmid c$ , 則  $p \nmid bc$ 。

**推論 2.** 假設  $p$  是一個質數而且  $a, b \in \mathbb{Z}$ 。則

$$\text{ord}_p ab = \text{ord}_p a + \text{ord}_p b。$$

**證明.** 令  $\alpha = \text{ord}_p a$  且令  $\beta = \text{ord}_p b$ 。則

$$a = p^\alpha a' \quad \text{且} \quad b = p^\beta b'; \quad \text{其中} \quad p \nmid a' \quad \text{且} \quad p \nmid b'。$$

因此我們有

$$ab = p^{\alpha+\beta} a'b', \quad \text{其中 } p \nmid a'b' \text{ (推論1')};$$

所以  $\text{ord}_p ab = \alpha + \beta$ , 故得證。

至此, 準備工作完成; 回到唯一分解性之證明。

**算術基本定理之證明.** 引理 1 已經證明, 對任何非零整數  $n$  存在一質數分解式

$$n = (-1)^{\text{sgn}(n)} \prod_p p^{a(p)}.$$

兩邊同時取  $\text{ord}_q$ , 並使用推論 2; 我們有

$$\text{ord}_q n = \text{sgn}(n)\text{ord}_q(-1) + \sum_p a(p)\text{ord}_q(p). \quad (1)$$

根據  $\text{ord}_q$  之定義, 我們有

$$\text{ord}_q(-1) = 0 \quad \text{且} \quad \text{ord}_q(p) = \begin{cases} 1 & \text{若 } p = q \\ 0 & \text{若 } p \neq q \end{cases}.$$

所以實際上, (1) 式的右側僅剩單一的一項  $a(q)$  沒有陣亡; 我們有  $\text{ord}_q n = a(q)$ , 故得證。

## 參考文獻

1. Agrawal, Manindra/Kayal, Neeraj/Saxena, Nitin: “PRIMES is in P,” *Annals of Math* 160 (2004), 781-793.  
http://www.cse.iitk.ac.in/news/primality.html
2. Apostol, Tom M.: *Introduction to Analytic Number Theory*, UTM, Springer-Verlag, New York, First Edition, 1976, Corr. Fifth Printing, 1998.
3. Hardy, G./Wright E.: *An Introduction to the Theory of Numbers*, Fifth edition, Oxford University Press, 1979.
4. Hardy, G.H.: *A Course of Pure Mathematics*, Cambridge Mathematical Library, 1993 (First published in 1908).
5. Hardy, G.H.: *A Mathematician's Apology*, Cambridge University Press, London, 1940.  
摘要見網頁 [http://en.wikipedia.org/wiki/A\\_Mathematician%27s\\_Apology](http://en.wikipedia.org/wiki/A_Mathematician%27s_Apology)
6. Ireland, Kenneth F./Rosen, Michael I.: *A Classical Introduction to Modern Number Theory*, Volume 84 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, Second Edition, 1990, Corr. Fifth Printing, 1998.
7. 質數網頁 <http://www.utm.edu/research/primes/largest.html>
8. 沈淵源: 密碼學之旅 全華圖書有限公司, 2006.