基礎數論

李華介

國立台灣師範大學數學系

前言

本講義主要目的是針對大一學生介紹有關整數論一些基本的代數和算數上的性質, 以作為將來學習抽象代數之準備. 基於這樣的理由, 在此我們將不介紹有關於整數論之歷史和典故以及其應用. 對整數論之應用 (尤其在資訊方面的應用) 有興趣的讀者, 我們推薦 Silverman 的「A Friendly Introduction to Number Theory」(Prentice Hall, Third Edition 2006). 相信若對本講義內容有相當認識之後應可輕鬆閱讀這本書.

Chapter 7

略談 Diophantine Equations

我們利用探討 Diophantine equations 的問題來作為本講義之總結. 一般而言若 $f(x_1,\ldots,x_n)$ 是一個多變數的整係數多項式, 求 $f(x_1,\ldots,x_n)=0$ 的所有整數解就是 Diophantine equation 的問題. 由於是求整數解有無限多種可能, 所以解 Diophantine equations 的問題比起解有限問題的 congruence equations 是困難許多. 事實上我們目前學的理論僅能論及一些簡單的 Diophantine equations. 在這裡我們僅希望利用前幾章所學的結果讓大家了解如何用它們來解決問題, 而不想深入的談論 Diophantine equations.

7.1. 兩個處理 Diophantine Equations 的方法

我們簡單的介紹兩種處理 Diophantine equations 的方法. 這兩種方法都是用來處理 Diophantine equations 無解的情況.

第一種方法是用 congruence 的方法處理. 也就是說如果一個 Diophantine equation $f(x_1,\ldots,x_n)=0$ 有整數解, 則對任意的 $m\in\mathbb{N}$ 在 modulo m 之下 $f(x_1,\ldots,x_n)\equiv 0 \pmod m$ 當然有解. 因此若能找到一個 m 使得 $f(x_1,\ldots,x_n)\equiv 0 \pmod m$ 無解, 那麼原 Diophantine equation $f(x_1,\ldots,x_n)=0$ 就無解.

Proposition 7.1.1. 假設 $f(x_1,\ldots,x_n)$ 是一個 n 個變數的整係數多項式. 若存在 $m\in\mathbb{N}$ 使得 $f(x_1,\ldots,x_n)\equiv 0 \pmod m$ 無解, 則 $f(x_1,\ldots,x_n)=0$ 無整數解.

Proof. 利用反證法假設 $x_1=c_1,\ldots,x_n=c_n$ 是 $f(x_1,\ldots,x_n)=0$ 的一組整數解. 由於 $f(c_1,\ldots,c_n)=0$, 自然有 $f(c_1,\ldots,c_n)\equiv 0 \pmod m$, 也就是說 $x_1\equiv c_1 \pmod m,\ldots,x_n\equiv c_n \pmod m$ 會是 $f(x_1,\ldots,x_n)\equiv 0 \pmod m$ 的一組解. 此和 $f(x_1,\ldots,x_n)\equiv 0 \pmod m$ 無解的假設相矛盾故知 $f(x_1,\ldots,x_n)=0$ 無整數解. □

要注意 Proposition 7.1.1 說的是若能找到一個 $m\in\mathbb{N}$ 使得 $f(x_1,\dots,x_n)\equiv 0 \pmod m$ 無解, 則 $f(x_1,\dots,x_n)=0$ 無整數解. 並不是說若能找到 $m\in\mathbb{N}$ 使得 $f(x_1,\dots,x_n)\equiv 0 \pmod m$ 有解, 則 $f(x_1,\dots,x_n)=0$ 有整數解. 千萬別搞錯了, 我們來看個例子.

Example 7.1.2. 考慮 Diophantine equation $11x^2-7y^2=2$. 在 modulo 11 之下, 我們要解 $-7y^2\equiv 2 \pmod{11}$. 由於 $-7\times 3\equiv 1 \pmod{11}$, $-7y^2\equiv 2 \pmod{11}$ 兩邊乘上 3 可得 $y^2\equiv 6 \pmod{11}$. 考慮 Legendre symbol $\left(\frac{6}{11}\right)=\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$. 由於 $11\equiv 3 \pmod 8$ 故由 Theorem 5.4.3 知 $\left(\frac{2}{11}\right)=-1$ 且由 Theorem 5.4.6 知 $\left(\frac{3}{11}\right)=-\left(\frac{11}{3}\right)=-\left(\frac{2}{3}\right)=1$. 因此得 $\left(\frac{6}{11}\right)=-1$, 也就是說 $y^2\equiv 6 \pmod{11}$ 無解. 換言之, $11x^2-7y^2-2\equiv 0 \pmod{11}$ 無解, 因而由 Proposition 7.1.1 知 $11x^2-7y^2=2$ 無整數解.

注意若將 $11x^2-7y^2=2$ 考慮在 modulo 7 的情形, 也就是解 $11x^2\equiv 2 \pmod 7$. 由於 $11\times 2\equiv 1 \pmod 7$, $11x^2\equiv 2 \pmod 7$ 兩邊乘上 2 得 $x^2\equiv 4 \pmod 7$. 很明顯的此式有 $x\equiv 2 \pmod 7$ 為其解, 但由前已知 $11x^2-7y^2=2$ 並無整數解. 所以由此例可知, 並不能因找到 $m\in\mathbb{N}$ 使得 $f(x_1,\dots,x_n)\equiv 0 \pmod m$ 有解, 便斷言 $f(x_1,\dots,x_n)=0$ 有解.

或許大家會好奇, 若對於任意的正整數 m, $f(x_1,\dots,x_n)\equiv 0 \pmod m$ 皆有解, 是否就能得 $f(x_1,\dots,x_n)=0$ 有整數解呢? 由下面的例子我們可以知道, 這仍是不一定對的.

Example 7.1.3. 令 $f(x)=(x^2-17)(x^2-19)(x^2-323)$ 考慮 Diophantine equation $f(x)=0$. 很明顯的這個 Diophantine equation 並無整數解. 但是我們將說明, 對任意 $m\in\mathbb{N}$, $f(x)\equiv 0 \pmod m$ 皆有解.

由 Corollary 4.4.3 我們知道要證明對任意 $m\in\mathbb{N}$, $f(x)\equiv 0 \pmod m$ 皆有解, 等同於要證明對任意質數 p 以及 $n\in\mathbb{N}$, $f(x)\equiv 0 \pmod{p^n}$ 皆有解.

當 $p=2,n=1$ 時, $f(x)\equiv(x^2-1)^3 \pmod 2$, 故 $f(x)\equiv 0 \pmod 2$ 有解. 而當 $p=2,n=2$ 時, $f(x)\equiv(x^2-1)(x^2-3)^2 \pmod 4$, 所以 $f(x)\equiv 0 \pmod 4$ 亦有解. 當 $p=2,n\geq 3$ 時, 由於 $17\equiv 1 \pmod 8$, Proposition 5.2.1 告訴我們 $x^2\equiv 17 \pmod{2^n}$ 必有解, 所以 $f(x)=(x^2-17)(x^2-19)(x^2-323)\equiv 0 \pmod{2^n}$ 當然有解.

當 $p=17$ 時由於 $17\equiv 1 \pmod 8$, 故由 Theorem 5.4.3 知 $x^2\equiv 19\equiv 2 \pmod{17}$ 有解. 因此由 Proposition 5.2.4 知對任意 $n\in\mathbb{N}$, $x^2\equiv 19 \pmod{17^n}$ 皆有解. 因此知 $f(x)\equiv 0 \pmod{17^n}$ 有解. 而當 $p=19$ 時, 由於 $17\equiv 1 \pmod 8$ 故得 $\left(\frac{17}{19}\right)=\left(\frac{19}{17}\right)=\left(\frac{2}{17}\right)=1$, 也就是說 $x^2\equiv 17 \pmod{19}$ 有解. 再由 Proposition 5.2.4 知對任意 $n\in\mathbb{N}$, $x^2\equiv 17 \pmod{19^n}$ 皆有解. 因此知 $f(x)\equiv 0 \pmod{19^n}$ 有解.

當 p 是奇質數且 $p\neq 17,19$ 時, 若 $x^2\equiv 17 \pmod p$ 有解, 則 Proposition 5.2.4 告訴我們對任意 $n\in\mathbb{N}$, $x^2\equiv 17 \pmod{p^n}$ 亦有解. 所以此時 $f(x)\equiv 0 \pmod{p^n}$ 有解. 同理若 $x^2\equiv 19 \pmod p$ 有解, 可得對任意 $n\in\mathbb{N}$, $f(x)\equiv 0 \pmod{p^n}$ 亦有解. 而若 $x^2\equiv 17 \pmod p$ 和 $x^2\equiv 19 \pmod p$ 皆無解, 即 $\left(\frac{17}{p}\right)=\left(\frac{19}{p}\right)=-1$, 則由 $\left(\frac{232}{p}\right)=\left(\frac{17}{p}\right)\left(\frac{19}{p}\right)=1$ 知

$x^2 \equiv 232 \pmod{p}$ 有解, 因此得對任意 $n \in \mathbb{N}$, $x^2 \equiv 232 \pmod{p^n}$ 皆有解. 我們仍得 $f(x) \equiv 0 \pmod{p^n}$ 有解.

綜合以上結果我們知, 對任意質數 p 以及 $n \in \mathbb{N}$, $f(x) \equiv 0 \pmod{p^n}$ 皆有解. 所以對任意 $m \in \mathbb{N}$, $f(x) \equiv 0 \pmod{m}$ 皆有解. 但是事實上 $f(x) = 0$ 並沒有整數解.

再次強調一次, 我們介紹的 congruence 方法僅能拿來證明 Diophantine equation 無解. 所以若有一個 Diophantine equation 你認為它並無整數解, 那你可以考慮用 congruence 的方法去證明它無解. 也就是說試著找到一個 $m \in \mathbb{N}$ 使其在 modulo m 之下無解, 那麼就證得此 Diophantine equation 無整數解. 若你認為一個 Diophantine equation 有解, 那麼 congruence 的方法頂多可以提供你其解的可能形式, 並無法告訴你原 Diophantine equation 有解.

另一種常用的方法稱為 *descent* 的方法. 它也是拿來證明一個 Diophantine equation 沒有正整數解. 其背後的原理是用到正整數的 well-ordering principle. 方法仍然是用反證法: 假設 Diophantine equation $f(x_1,\ldots,x_n) = 0$ 有正整數解且 $x_1 = c_1,\ldots,x_i = c_i,\ldots,x_n = c_n$ 為其一組解. 若我們能利用 $x_1 = c_1,\ldots,x_i = c_i,\ldots,x_n = c_n$ 這一組正整數解找到另一組正整數解 $x_1 = c_1',\ldots,x_i = c_i',\ldots,x_n = c_n'$, 其中對某個特定 $i \in \{1,\ldots,n\}$ 會有 $c_i' < c_i$, 則接下來可利用 $x_1 = c_1',\ldots,x_i = c_i',\ldots,x_n = c_n'$ 這一組正整數解找到另一組正整數解 $x_1 = c_1'',\ldots,x_i = c_i'',\ldots,x_n = c_n''$ 滿足 $c_i'' < c_i'$. 如此一直下去我們可得一個嚴格遞減的無窮正整數數列 $c_i > c_i' > c_i'' > \cdots$ 此和正整數的 well-ordering principle 相違背, 故得證 $f(x_1,\ldots,x_n) = 0$ 沒有整數解.

以後我們會利用 descent 的方法證明某個有名的 Diophantine equation 無正整數解. 底下我們先舉一個簡單的例子讓大家了解 descent 的方法.

Example 7.1.4. 大家都知道 $\sqrt{2}$ 是無理數, 所以我們可知 $x^2 - 2y^2 = 0$ 這個 diophantine equation 無正整數解. 我們利用 descent 的方法來解釋 $x^2 - 2y^2 = 0$ 無正整數解.

假設 $x = c_1, y = d_1$ 是 $x^2 - 2y^2 = 0$ 的一組正整數解. 則由於 $c_1^2 = 2d_1^2$, 我們知 c_1 必為正偶數, 也就是說存在 $c_2 \in \mathbb{N}$ 使得 $c_1 = 2c_2$. 因此得 $4c_2^2 = 2d_1^2$, 即 $2c_2^2 = d_1^2$. 由此又得 d_1 是正偶數, 故存在 $d_2 \in \mathbb{N}$ 使得 $d_1 = 2d_2$. 因此得 $2c_2^2 = 4d_2^2$, 即 $c_2^2 = 2d_2^2$. 也就是說 $x = c_2, y = d_2$ 為 $x^2 - 2y^2 = 0$ 的一組正整數解. 我們利用 $x = c_1, y = d_1$ 這一組正整數解得到 $x = c_2, y = d_2$ 這一組正整數解且滿足 $c_1 = 2c_2 > c_2$, 故利用 descent 的方法知 $x^2 - 2y^2 = 0$ 無正整數解.

這裡有一個邏輯上的問題需注意. 所謂 descent 的方法是指一個 Diophantine equation 若能證明「任給一組」正整數解都能產生另一組 "較小" 的正整數解, 則該 Diophantine equation 無正整數解. 僅由「特定的一組」正整數解可以得到另一組 "較小" 的正整數解並無法推得矛盾的結論. 例如 $x = 8, y = 6, z = 10$ 是 $x^2 + y^2 = z^2$ 的一組正整數解, 將 x, y, z 皆除以 2 得 $x = 4, y = 3, z = 5$ 也是 $x^2 + y^2 = z^2$ 的一組正整數解, 但此組解並不能再依此推得更小的一組解, 所以無法推得矛盾的結論. 事實上 $x^2 + y^2 = z^2$ 當然是有正整數解, 這並沒有和 descent 的方法相違背.

7.2. Pythagorean Triple 和 Fermat's Last Theorem

我們都知道直角三角形的兩股平方和等於斜邊的平方. 若一個直角三角形其三邊長皆為正整數則此三個正整數就稱為是一組 Pythagorean triple. 換言之, 滿足 Diophantine equation $x^2+y^2=z^2$ 的一組正整數解就是 Pythagorean triple. 我們將找到所有 Pythagorean triples 的形式且利用其來探討和 Fermat's Last Theorem 有關的問題.

7.2.1. Pythagorean Triples. 我們希望能找到所有的 Pythagorean triples. 不過若沒有限制條件要找到所有的解實在有點困難, 更何況有些 Pythagorean triple 其實是從某些 Pythagorean triple 輕易得到的. 因此我們希望找的 Pythagorean triples 雖然有限制條件但希望都能由這些 Pythagorean triples 得到所有可能的 Pythagorean triples. 該多加哪些限制能達到這個目的呢? 例如我們可以僅考慮 $x^2+y^2=z^2$ 的正整數解. 這是因為一來若 $x=0$ 或 $y=0$ 那麼 $x^2=z^2$ 或 $y^2=z^2$ 這樣的 Diophantine equation 根本沒有意思; 再來其他的負整數解都可以輕鬆地由正整數解得到, 所以僅考慮正整數解就足以表達所有的解.

類似的思考方向, 我們也可很輕易的從 $x^2+y^2=z^2$ 的一組正整數解得到無窮多組正整數解. 例如 $x=3,y=4,z=5$ 是一組正整數解, 因此可得對任意 $\lambda\in\mathbb{N}$, $x=3\lambda,y=4\lambda,z=5\lambda$ 也是一組正整數解. 所以我們知有無窮多組 Pythagorean triples. 不過這樣所得的 Pythagorean triple 對我們來說是沒多大興趣的. 我們比較有興趣的是一組 Pythagorean triple "原始" 是來自哪個 Pythagorean triple. 也就是我們有興趣於那些最大公因數為 1 的 Pythagorean triple. 事實上任一組 Pythagorean triple 都是來自於某一組最大公因數為 1 的 Pythagorean triple. 這是因為若 $x=a,y=b,z=c$ 是一組 Pythagorean triple 且 $\gcd(a,b,c)=d$, 則存在 $a',b',c'\in\mathbb{N}$ 使得 $a=da',b=db',c=dc'$ 且 $\gcd(a',b',c')=1$. 另一方面由於 $a^2+b^2=c^2$ 可得 $a'^2+b'^2=c'^2$, 所以 $x=a',y=b',z=c'$ 就是一組最大公因數為 1 的 Pythagorean triple. 因此我們只要專注於最大公因數為 1 的 Pythagorean triple 即可.

最後我們發現若 $x=a,y=b,z=c$ 是一組最大公因數為 1 的 Pythagorean triple, 當然 $x=b,y=a,z=c$ 也是一組最大公因數為 1 的 Pythagorean triple, 也就是說藉由交換 x,y 的順序所得的解也沒多大意思. 所以我們想找一個方法僅考慮一組 x,y 的順序即可. 例如我們可僅考慮 $x>y$ 的情形. 不過這樣的限制對我們找解沒有多大的幫助. 我們可以考慮另一種限制. 首先注意最大公因數的限制使得我們的 Pythagorean triple 其 x,y 的值不能同為偶數, 否則由 $z^2=x^2+y^2$ 知 z 必為偶數, 造成 x,y,z 的最大公因數會大於等於 2. 另一方面 x,y 的值也不能同為奇數. 這是因為若 x,y 皆為奇數, 則 $x^2\equiv y^2\equiv 1 \pmod 4$. 因此會造成 $x^2+y^2\equiv 2 \pmod 4$, 然而 x^2+y^2 是偶數, 故由 $z^2=x^2+y^2$ 得 z 為偶數. 也就是說 $z^2\equiv 0 \pmod 4$. 這會造成 $0\equiv z^2\equiv x^2+y^2\equiv 2 \pmod 4$ 的矛盾. 因此若我們要求的 Pythagorean triple 其最大公因數是 1, 則 x 和 y 必一奇一偶. 所以我們可以考慮限制我們的 Pythagorean triple 其 x 值為奇數而 y 值為偶數. 我們給有這些限制的 Pythagorean triples 一個特別的名字.

Definition 7.2.1. 假設 $a,b,c\in\mathbb{N}$ 滿足 $a^2+b^2=c^2$ 且 $\gcd(a,b,c)=1$ 又 a 為奇數而 b 為偶數, 則稱 a,b,c 為一個 *primitive Pythagorean triple*.

我們希望能找到所有的 primitive Pythagorean triples. 事實上 primitive Pythagorean triples 會有無窮多個, 所以這裡指的找到並不是將所有的 primitive Pythagorean triples 都列出, 我們是要找到一個方法將所有的 primitive Pythagorean triples 表示出來.

Theorem 7.2.2. 給定任一組 *primitive Pythagorean triple* x,y,z 皆存在一組 $m,n\in\mathbb{N}$ 其中 $m>n$, $\gcd(m,n)=1$ 且 m,n 中有一個是奇數一個是偶數使得

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

反之對任意一組 $m,n\in\mathbb{N}$ 滿足 $m>n$, $\gcd(m,n)=1$ 且 m,n 中有一個是奇數一個是偶數, 若令 $x=m^2-n^2$, $y=2mn$ 且 $z=m^2+n^2$, 則 x,y,z 為一組 *primitive Pythagorean triple.*

Proof. 假設 x,y,z 是一組 primitive Pythagorean triple. 由於 $x^2+y^2=z^2$, 我們得 $y^2=(z+x)(z-x)$. 依定義 y 是偶數而 x,z 是奇數, 所以 $y/2,(z+x)/2$ 和 $(z-x)/2$ 皆為正整數且 $(y/2)^2=((z+x)/2)((z-x)/2)$. 注意此時 $(z+x)/2$ 和 $(z-x)/2$ 互質. 要不然會有一質數 p 為 $(z+x)/2$ 和 $(z-x)/2$ 的公因數, 因而得 p 為 $(z+x)/2+(z-x)/2=z$ 和 $(z+x)/2-(z-x)/2=x$ 的公因數. 如此會造成 $p|y^2=z^2-x^2$, 即 $p|y$, 因而與 $\gcd(x,y,z)=1$ 相矛盾.

既然 $(z+x)/2$ 和 $(z-x)/2$ 互質, 故由 $(y/2)^2=((z+x)/2)((z-x)/2)$ 可得 $(z+x)/2$ 和 $(z-x)/2$ 皆為某個整數之平方, 亦即存在 $m,n\in\mathbb{N}$ 使得 $m^2=(z+x)/2$ 及 $n^2=(z-x)/2$. 此時我們得

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

至於 m 和 n, 由於 $x>0$, 即 $m^2-n^2>0$, 故知 $m>n$. 又因為 $(z+x)/2$ 和 $(z-x)/2$ 互質, 即 $\gcd(m^2,n^2)=1$, 我們得 $\gcd(m,n)=1$. 最後依定義 $x=m^2-n^2$ 是奇數, 故知 m 和 n 中有一個是奇數一個是偶數.

反之對任意一組 $m,n\in\mathbb{N}$ 滿足 $m>n$, $\gcd(m,n)=1$ 且 m,n 中有一個是奇數一個是偶數, 若令 $x=m^2-n^2$, $y=2mn$ 且 $z=m^2+n^2$, 則自然知 $x,y,z\in\mathbb{N}$ 且 $x^2+y^2=z^2$, 也就是說 x,y,z 是一組 Pythagorean triple. 因此我們僅剩下要說明它們是 primitive, 即 $\gcd(x,y,z)=1$, x 為奇數且 y 為偶數. 依定義 $y=2mn$ 所以 y 當然是偶數, 而 m,n 中一個是奇數一個是偶數所以 $x=m^2-n^2$ 當然是奇數. 至於 $\gcd(x,y,z)=1$ 是因為如果 $\gcd(x,y,z)>1$, 則 $\gcd(x,y,z)$ 必為奇數 (因為已知 x 是奇數) 所以存在一奇質數 p 為 x,y,z 的公因數. 因為 p 整除 $z+x=2m^2$ 且 p 整除 $z-x=2n^2$ 又因為 p 為奇質數, 我們得 $p|m$ 且 $p|n$. 此與 m,n 互質的假設相矛盾, 故知 $\gcd(x,y,z)=1$. □

Theorem 7.2.2 告訴我們每一個 primitive Pythagorean triple 都可由一組一奇一偶且互質的正整數 m,n 得到, 而且每給一組這樣的正整數就可得一組 primitive Pythagorean triple. 雖然我們可以輕易的找到無窮多組這樣的 m,n 但這並不表示可以產生無窮多組 primitive Pythagorean triples, 除非我們知道不同的一組 m,n 可產生不同的 Pythagorean triple. 事實上若 m,n 和 m',n' 是兩組一奇一偶且互質的正整數其中 $m>n$ 且 $m'>n'$, 假設 m,n 和 m',n' 產生一樣的 primitive Pythagorean triple. 亦即 $m^2-n^2=m'^2-n'^2$ 且 $m^2+n^2=m'^2+n'^2$. 將兩式相加可得 $2m^2=2m'^2$, 故由 m,m' 皆為正整數得 $m=m'$. 同理得 $n=n'$. 因此我們有以下之結果.

Corollary 7.2.3. 存在無窮多組 *primitive Pythagorean triple.* 事實上對任意的一組 *primitive Pythagorean triple* 皆存在唯一的一組 $m,n\in\mathbb{N}$ 其中 $m>n$, $\gcd(m,n)=1$ 且 m,n 中有一個是奇數一個是偶數使得 $x=m^2-n^2,\quad y=2mn,\quad z=m^2+n^2$.

7.2.2. Fermat's Last Theorem. 我們已找到所有 $x^2+y^2=z^2$ 的正整數解, 很自然的會問 $x^3+y^3=z^3$ 的正整數解, 甚至問對任意大於等於 3 的正整數 n, $x^n+y^n=z^n$ 的正整數解. Fermat 認為當 $n\geq 3$ 時 $x^n+y^n=z^n$ 並無正整數解. 他僅簡短的說有一個很聰明的方法證明此事但並沒有提出證明, 所以我們稱此結果為 Fermat's Last Theorem.

事實上當時應稱 Fermat's Last Theorem 為一個 conjecture (猜想) 因為並沒有人給出完整的證明. 三百多年來許許多多的數學家想要證出此定理, 但一直到 1995 年才被完整的證明. 不過所用的方法牽涉到許多複雜艱深的數學理論, 當然不會是 Fermat 當初所指的方法. 由此我們可以知道 Diophantine equation 雖然僅是討論整數解的問題, 不過有的 Diophantine equation 確實牽涉到很深的數學問題.

其實解 Fermat's Last Theorem 不必考慮所有大於等於 3 的正整數. 若 n 有奇的質因數 p, 此時 $n=pm$, 故若 $x=a,y=b,z=c$ 是 $x^n+y^n=z^n$ 的一組正整數解, 則因 $a^{pm}+b^{pm}=c^{pm}$ 知 $x=a^m,y=b^m,z=c^m$ 是 $x^p+y^p=z^p$ 的一組正整數解. 換言之若能證得 $x^p+y^p=z^p$ 無正整數解, 則對任意 $n=pm$, $x^n+y^n=z^n$ 也無正整數解. 同理若 n 無奇的質因數, 即 $n=2^r$, 此時因 $r\geq 2$ 知 $4|n$, 所以若能證得 $x^4+y^4=z^4$ 無正整數解, 則對任意 $n=2^r>2$, $x^n+y^n=z^n$ 無正整數解. 因此要證明 Fermat's Last Theorem, 我們只要證明對任意奇質數 p, $x^p+y^p=z^p$ 無正整數解, 以及 $x^4+y^4=z^4$ 無正整數解即可. 目前我們無法處理奇質數的情形, 接下來我們將利用 descent 的方法證明 $x^4+y^4=z^4$ 無正整數解.

我們先處理一個比 $x^4+y^4=z^4$ 更一般的 Diophantine equation.

Proposition 7.2.4. $x^4+y^4=z^2$ 無正整數解.

Proof. 我們利用 descent 的方法證明 $x^4+y^4=z^2$ 無正整數解. 假設 $x=a_1,y=b_1,z=c_1$ 是 $x^4+y^4=z^2$ 的一組正整數解, 我們將利用它們得到另一組正整數解 $x=a_2,y=b_2,z=c_2$ 且 $c_1>c_2$. 如此一直下去會和正整數的 well-ordering principle 相違背, 故知原式無正整數解.

現假設 $x=a_1,y=b_1,z=c_1$ 是 $x^4+y^4=z^2$ 的一組正整數解. 如果 $\gcd(a_1,b_1)=d>1$, 由於 $d|a_1$ 且 $d|b_1$ 知 $d^4|a_1^4+b_1^4=c_1^2$, 故得 $d^2|c_1$. 因此 $x=a_1/d,y=b_1/d,z=c_1/d^2$ 是 $x^4+y^4=z^2$ 的一組正整數解且 $c_1/d^2<c_1$.

若 $x=a_1,y=b_1,z=c_1$ 是 $x^4+y^4=z^2$ 的一組正整數解且 $\gcd(a_1,b_1)=1$. 此時由於 $\gcd(a_1^2,b_1^2,c_1)=1$ (因 $\gcd(a_1^2,b_1^2)=1$) 且 $x=a_1^2,y=b_1^2,z=c_1$ 滿足 $x^2+y^2=z^2$. 利用前面討論 primitive Pythagorean triple 的結果, 不失一般性我們假設 a_1^2 是奇數而 b_1^2 是偶數, 亦即 $x=a_1^2,y=b_1^2,z=c_1$ 是一組 primitive Pythagorean triple. 故利用 Theorem 7.2.2 知存在 $m,n\in\mathbb{N}$ 滿足 $m>n$ 且 $\gcd(m,n)=1$ 使得

$$a_1^2=m^2-n^2,\quad b_1^2=2mn,\quad c_1=m^2+n^2.$$

又由於 $\gcd(a_1,m,n)=1$ (因 $\gcd(m,n)=1$), 且 $x=a_1,y=n,z=m$ 滿足 $x^2+y^2=z^2$, 故由 a_1 是奇數之假設以及前面討論 primitive Pythagorean triple 之性質知 n 必為偶數 (且 m 為奇數), 也就是說 $x=a_1,y=n,z=m$ 又是一組 primitive Pythagorean triple. 因此再用一次 Theorem 7.2.2 知存在 $u,v\in\mathbb{N}$ 滿足 $u>v$ 且 $\gcd(u,v)=1$ 使得

$$a_1=u^2-v^2,\quad n=2uv,\quad m=u^2+v^2.$$

這裡要注意, 由於 b_1 和 n 皆為偶數, 我們可假設 $b_1=2b_1'$ 且 $n=2n'$. 此時由 $b_1^2=2mn$ 知 $b_1'^2=mn'$. 又由於 $\gcd(m,n')=1$ 我們知 m 和 n' 皆為某個整數之平方, 亦即存在 $c_2,e\in\mathbb{N}$ 使得 $m=c_2^2$ 且 $n'=e^2$. 又由於 $2e'^2=2n'=n=2uv$ 以及 $\gcd(u,v)=1$, 我們得 u 和 v 皆為某個整數之平方, 亦即存在 $a_2,b_2\in\mathbb{N}$ 使得 $u=a_2^2$ 且 $v=b_2^2$. 因此由 $m=u^2+v^2$ 即 $c_2^2=(a_2^2)^2+(b_2^2)^2$ 知 $x=a_2,y=b_2,z=c_2$ 是 $x^4+y^4=z^2$ 的一組正整數解. 此時因 $c_1=m^2+n^2>m^2=c_2^4$, 知 $x=a_2,y=b_2,z=c_2$ 確實是另一組 $x^4+y^4=z^2$ 的正整數解且滿足 $c_2<c_1$. 故利用 descent 的方法得證本定理. □

Proposition 7.2.4 告訴我們 $x^4+y^4=z^2$ 無正整數解, 我們可以輕鬆的利用這個結果證明 $x^4+y^4=z^4$ 無正整數解. 這是因為若 $x=a,y=b,z=c$ 是 $x^4+y^4=z^4$ 的一組正整數解, 則 $x=a,y=b,z=c^2$ 就會是 $x^4+y^4=z^2$ 的一組正整數解. 此和 Proposition 7.2.4 相矛盾, 故有以下之結論.

Corollary 7.2.5. $x^4+y^4=z^4$ 無正整數解.

7.3. 平方和問題

在此最後一節中我們要探討整數論另一個有趣的問題, 就是將正整數寫成一些整數的平方和問題. 我們將完整的回答哪些正整數可以寫成兩個整數的平方和, 而且證明所有的正整數都可以寫成四個整數的平方和.

7.3.1. Sum of Two Squares. 當一個正整數不是某個整數的平方時, 我們有興趣知道它是否可寫成兩個整數的平方和. 若 n 本身是某個整數的平方, 即存在 $m\in\mathbb{N}$ 使得 $n=m^2$, 當然我們可以將 n 寫成 $n=m^2+0^2$. 所以我們可以將可寫成兩個整數的平方和的數視為平方數的推廣.

首先我們來看一個有趣的等式:

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2. \tag{7.1}$$

這個等式可以直接將等號兩邊展開來求證, 也可以用大家熟悉的複數運算來說明. 假設 $z_1=a+b\mathbf{i},z_2=d+c\mathbf{i}\in\mathbb{C}$ (這裡 $\mathbb{C}$ 表示複數所成之集合, 而 $\mathbf{i}\in\mathbb{C}$ 滿足 $\mathbf{i}^2=-1$). 我們知 z_1,z_1 的共軛複數分別為 $\overline{z_1}=a-b\mathbf{i},\overline{z_2}=d-c\mathbf{i}$ 且 $|z_1|^2=z_1\overline{z_1}=a^2+b^2$ 及 $|z_2|^2=z_2\overline{z_2}=c^2+d^2$. 因此

$$(a^2+b^2)(c^2+d^2)=z_1\overline{z_1}z_2\overline{z_2}=z_1z_2\overline{z_1z_2}=|(ad-bc)+(ac+bd)\mathbf{i}|^2=(ac+bd)^2+(ad-bc)^2.$$

利用式子 (7.1) 我們馬上有以下之結果.

Lemma 7.3.1. *若 $m,n\in\mathbb{N}$ 皆可以寫成兩個整數的平方和, 則 mn 亦可以寫成兩個整數的平方和.*

Proof. *若 $m=a^2+b^2$ 且 $n=c^2+d^2$, 其中 $a,b,c,d\in\mathbb{Z}$, 則利用式子 (7.1) 知 $mn=(ac+bd)^2+(ad-bc)^2$. 因 $ac+bd,ad-bc\in\mathbb{Z}$ 故知 mn 亦可以寫成兩個整數的平方和.* □

注意 Lemma 7.3.1 僅告訴我們當 m,n 皆可以寫成兩個整數的平方和時, mn 也可以寫成兩個整數的平方和; 它並沒有告訴我們若 m,n 中有一個不能寫成兩個整數的平方和時, mn 是否可以寫成兩個整數的平方和.

由於每個大於 1 的整數都可以寫成質因數的乘積, 所以由 Lemma 7.3.1 我們很自然的要探討哪些質數可以寫成兩個整數的平方和哪些質數不能. 由於 $2=1^2+1^2$, 即 2 可以寫成兩個整數的平方和, 因此以下我們僅考慮奇質數的情形. 利用 Lemma 7.3.1 我們可以得到一個判別一個質數是否可以寫成兩個整數的平方和的方法.

Lemma 7.3.2. *假設 p 是一個質數. 若存在 $a,b\in\mathbb{Z}$ 使得 $a^2+b^2=\lambda p$, 其中 $\lambda\in\mathbb{N}$ 滿足 $\lambda<p$, 則 p 可以寫成兩個整數的平方和.*

Proof. *考慮集合 $S=\{s\in\mathbb{N}\mid$ 存在 $u,v\in\mathbb{Z}$ 使得 $u^2+v^2=sp\}$. 依照 S 的定義, 要證明 p 可以寫成兩個整數的平方和就等同於要證明 $1\in S$. 要如何知 $1\in S$ 呢? 依假設知 S 為非空集合 (因 $\lambda\in S$) 且 S 的元素皆為正整數, 所以 $1\in S$ 若且唯若 S 中最小的元素就是 1 (注意依正整數的 well-ordering principle, 由於 S 不是空集合所以 S 中必存在最小的元素). 令 $m\in S$ 是 S 中最小的元素, 我們要證明 $m=1$.*

利用反證法, 假設 $m\neq 1$. 故由 $\lambda\in S$ 且 $\lambda<p$ 知 $1<m<p$. 我們希望在 S 中找到比 m 更小的數而得到矛盾. 由於 $m\in S$, 故存在 $u,v\in\mathbb{Z}$ 使得 $u^2+v^2=mp$, 我們分成 m 是偶數及 m 是奇數兩種情況討論.

(I) m 是偶數: 此時由於 $u^2+v^2=mp$ 是偶數, 我們知 u,v 必同奇同偶 (否則 u^2+v^2 不會是偶數), 即 $u+v$ 和 $u-v$ 皆為偶數. 此時 $(u+v)/2$ 和 $(u-v)/2$ 皆為整數且

$$(\frac{u+v}{2})^2+(\frac{u-v}{2})^2=\frac{u^2}{2}+\frac{v^2}{2}=\frac{m}{2}p.$$

故知 $m/2\in S$ 且 $m/2<m$, 此與 m 是 S 中最小的元素相矛盾.

(II) m 是奇數: 因為當 m 是奇數時

$$\{\frac{-m+1}{2},\frac{-m+1}{2}+1,\ldots,0,1,\ldots,\frac{m-1}{2}-1,\frac{m-1}{2}\}$$

是一個 complete residue system modulo m. 我們可找到 $c,d\in\mathbb{Z}$ 滿足 $c\equiv u\pmod m$ 且 $d\equiv v\pmod m$, 其中 $-(m-1)/2\leq c,d\leq(m-1)/2$. 注意這裡 c 和 d 不能同時等於 0, 這是因為如果 $c=d=0$ 表示 $u\equiv v\equiv 0\pmod m$, 即 $m|u$ 且 $m|v$. 因此 $m^2|u^2+v^2=mp$, 即 $m|p$. 如此會和 $1<m<p$ 相矛盾, 故知 c 和 d 不同時為 0. 因為 $c^2+d^2\equiv u^2+v^2\pmod m$ 以及 $u^2+v^2=mp$, 我們得 $c^2+d^2\equiv 0\pmod m$. 亦即存在 $k\in\mathbb{Z}$ 使得 $c^2+d^2=km$. 注意因 c 和 d 不同時為 0, 故 $k\neq 0$. 另一方面因為 $-(m-1)/2\leq c,d\leq(m-1)/2$, 所以

$c^2+d^2 \le (m-1)^2/4+(m-1)^2/4 = (m-1)^2/2 < m^2$, 故得 $0<k<m$. 也就是說 $k \in \mathbb{N}$ 且 $k<m$. 現在我們有兩個等式: $u^2+v^2 = mp$ 以及 $c^2+d^2 = km$. 利用式子 (7.1) 得

$$(uc+vd)^2+(ud-vc)^2 = m^2kp.$$

又因為 $u \equiv c \pmod m$ 且 $v \equiv d \pmod m$, 我們得

$$uc+vd \equiv u^2+v^2 \equiv 0 \pmod m \quad \text{and} \quad ud-vc \equiv uv-uv \equiv 0 \pmod m.$$

也就是說 $(uc+vd)/m \in \mathbb{Z}$ 且 $(ud-vc)/m \in \mathbb{Z}$. 因此知

$$(\frac{uc+vd}{m})^2+(\frac{ud-vc}{m})^2 = kp,$$

也就是說 kp 可以寫成兩個整數的平方和, 故又由 $k \in \mathbb{N}$ 知 $k \in S$. 然而我們又知 $k<m$, 此與 m 是 S 中最小的元素相矛盾.

我們證得若 $m \neq 1$ 會造成 m 不是偶數且不是奇數這樣的矛盾. 故由反證法知原假設 $m \neq 1$ 不成立, 也就是說 $m = 1$. 因此得證 p 可以寫成兩個整數的平方和. □

Lemma 7.3.2 的證明方法其實是類似於 descent 的方法都是由一個解得到更小的解而推得矛盾. 或許大家會疑惑為何同樣的推論方法, 一個會得到無解; 另一個卻推得有解. 這是因為在 descent 的方法推論中是沒有任何條件的, 所以若有正整數解則會沒有限制的推得無窮多個更小的正整數解而造成矛盾, 因此會得到無解的結論. 而這裡所用的方法中會得到比 m 更小的正整數是有條件的, 也就是說必須在 $m>1$ 的情形才可以. 因此同樣推得矛盾, 但此時矛盾會讓我們推得 $m=1$, 所以有解. 希望這兩者邏輯上的差異, 大家都能了解. 另外 Lemma 7.3.2 證得存在的方法表面上好像只是邏輯推演, 並沒有告訴我們如何找到解. 事實上其解法過程中包含了找到解的方法. 我們來看一個具體的例子.

Example 7.3.3. 考慮 $p = 89$. 由於 $89 \equiv 1 \pmod 4$, 我們知存在 $a \in \mathbb{Z}$ 使得 $a^2 \equiv -1 \pmod{89}$. 事實上當 $a = 34$ 時, $a^2 = 1156 \equiv -1 \pmod{89}$, 我們有 $(34)^2+1 = 13\times 89$. 因為 $13<89$ 故由 Lemma 7.3.2 知 89 可以寫成兩個整數的平方和. 我們要利用 Lemma 7.3.2 的證明方法將 89 寫成兩個整數的平方和.

對應到 Lemma 7.3.2 的證明, 我們知 $13 \in S$. 因 $13 \neq 1$, 我們要利用 13, 在 S 中找到更小的元素. 我們要找到 c,d 滿足 $34 \equiv c \pmod{13}$, $1 \equiv d \pmod{13}$ 以及 $-6 \le c,d \le 6$. 很容易得知 $c = -5$ 且 $d = 1$. 接著我們考慮 $c^2+d^2 = 25+1 = 26 = 2\times 13$. 故由式子 (7.1) 得

$$(34\times(-5)+1)^2+(34-(-5))^2 = 169^2+39^2 = 2\times 13^2\times 89.$$

由於 $169 = 13\times 13$ 且 $39 = 3\times 13$, 我們得 $13^2+3^2 = 2\times 89$, 也就是說 $2 \in S$. 注意到我們已將 $13 \in S$ 降到 $2 \in S$. 再利用處理偶數情況的方法, 將 2 縮小. 即得

$$(\frac{13+3}{2})^2+(\frac{13-3}{2})^2 = 8^2+5^2 = 89.$$

在 Example 7.3.3 中我們利用 $89 \equiv 1 \pmod 4$ 所以可以找到 $a \in \mathbb{Z}$ 滿足 $a^2 \equiv -1 \pmod{89}$. 再適當的選取 a (即選取 a 夠小) 使得 $a^1+1 = \lambda p$, 其中 $0<\lambda<p$, 以便套用 Lemma 7.3.2. 在一般的情形, 當 p 是一質數滿足 $p \equiv 1 \pmod 4$ 時, 我們都可以如此作. 所以我們有以下之結果.

Proposition 7.3.4. *若 p 是一質數且 $p \equiv 1 \pmod 4$, 則 p 可以寫成兩個整數的平方和.*

Proof. 由於 $p \equiv 1 \pmod 4$, Theorem 5.4.1 告訴我們 $x^2 \equiv -1 \pmod p$ 有解. 亦即存在 $a \in \mathbb{N}$ 使得 $a^2 \equiv -1 \pmod p$. 由於 $\{1,2,\ldots,p-1\}$ 是一個 reduced residue system modulo p, 所以我們可以選取 $1 \le a \le p-1$ 使得 $a^2 \equiv -1 \pmod p$ (事實上可選取 $1 < a < p/2$). 因此存在 $\lambda \in \mathbb{N}$ 使得 $a^2+1 = \lambda p$. 又因為 $a \le p-1$, 我們有 $\lambda p = a^2+1 \le (p-1)^2+1 = p^2-2(p-1) < p^2$. 也就是說 $\lambda < p$, 故利用 Lemma 7.3.2 得證 p 可以寫成兩個整數的平方和. □

接下來我們看怎樣的質數不能寫成兩個整數的平方和. 當 $p \equiv 1 \pmod 4$ 時, 在 Proposition 7.3.4 我們是利用此時 $x^2 \equiv -1 \pmod p$ 有解證得 p 可以寫成兩個整數的平方和. 我們也可以利用當 $p \equiv 3 \pmod 4$ 時, $x^2 \equiv -1 \pmod p$ 無解證得 p 不可以寫成兩個整數的平方和.

Lemma 7.3.5. *假設 p 是一個質數滿足 $p \equiv 3 \pmod 4$ 且 $n \in \mathbb{N}$ 滿足 $p \mid n$. 若 $a,b \in \mathbb{Z}$ 使得 $a^2+b^2 = n$, 則 $p \mid a$ 且 $p \mid b$.*

Proof. 我們要用反證法證明此定理. 不失一般性, 我們假設 $p \nmid a$. 此時由 $a^2+b^2 = n$ 且 $p \mid n$ 知 $p \nmid b$, 否則由 $a^2 = n-b^2$ 得 $p \mid a^2$ 會造成與 $p \nmid a$ 的假設相矛盾. 既然 $a^2+b^2 = n$ 且 $p \mid n$, 我們得 $a^2 \equiv -b^2 \pmod p$. 注意由於 a,b 皆與 p 互質, 我們可以用 Legendre symbol 處理問題. 利用 Legendre symbol 的性質 (Lemma 5.3.2) 知

$$1 = \left(\frac{a^2}{p}\right) = \left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{-1}{p}\right).$$

然而由 $p \equiv 3 \pmod 4$ 以及 Theorem 5.4.1 我們知 $\left(\frac{-1}{p}\right) = -1$. 由此矛盾知 $p \mid a$, 並由 $b^2 = n-a^2$ 得 $p \mid b$. □

Lemma 7.3.5 證明的想法類似於 Proposition 7.1.1 所提的方法, 即利用探討 $x^2+y^2 = n$ 這個 Diophantine equation 在 modulo p 的情形來推得此 Diophantine equation 無解. 利用 Lemma 7.3.5 我們馬上得到以下之結果.

Proposition 7.3.6. *若 p 是一質數且 $p \equiv 3 \pmod 4$, 則 p 不能寫成兩個整數的平方和.*

Proof. 我們用反證法. 假設存在 $a,b \in \mathbb{Z}$ 使得 $a^2+b^2 = p$. 由於 p 是質數, 我們知 a,b 皆不等於 0. 故知可取 $a,b \in \mathbb{N}$ 滿足 $1 \le a \le p-1$ 且 $1 \le b \le p-1$. 此時 a,b 皆與 p 互質故與 Lemma 7.3.5 的結果相矛盾. 由此矛盾知 p 不能寫成兩個整數的平方和. □

知道了哪些質數可以寫成兩個整數的平方和, 哪些質數不可以寫成兩個整數的平方和. 接下來我們就來探討哪些正整數可以寫成兩個整數的平方和. 給定一正整數 n. 若 $n = 1$ 當然可寫成兩個整數的平方和. 若 $n \ge 2$, 首先我們將 n 作質因數的分解. 我們可以將 2 和除以 4 餘 1 的質因數忽略, 因為它們可以寫成兩個整數的平方和. 而若 n 有除以 4 餘 3 的質因數, 我們又可以將有平方的部份忽略, 因為它們也可以寫成兩個整數的平方和. 由此看出質因數分解後的次數是重要的, 我們特別用以下名詞的定義: 若 $n = p_1^{n_1} \cdots p_r^{n_r}$, 其中這些 p_i

是相異質數. 我們稱 p_i 是 n 的質因數且 n_i 是 p_i 的次數. 例如 $2250 = 2\times 3^2\times 5^3$, 我們稱 2250 有 2 次 3 的質因數且有 3 次 5 的質因數. 依此定義我們有以下之結果.

Theorem 7.3.7. 假設 $n\in\mathbb{N}$. 則 n 可以寫成兩個整數的平方和若且唯若 n 沒有任何的除以 4 餘 3 的質因數其次數是奇數.

Proof. 假設 n 沒有任何的除以 4 餘 3 的質因數其次數是奇數. 我們僅需考慮 $n\geq 2$ 的情形. 此時可將 n 質因數分解成

$$n = 2^{n_0}q_1^{n_1}\cdots q_r^{n_r}\cdot p_1^{2m_1}\cdots p_s^{2m_s},$$

其中 q_i, p_j 皆為相異的奇質數且 $q_i\equiv 1 \pmod 4$ 及 $p_j\equiv 3 \pmod 4$. 由於我們可將 n 寫成

$$n = 2^{n_0}q_1^{n_1}\cdots q_r^{n_r}\cdot (p_1^{m_1}\cdots p_s^{m_s})^2,$$

而 2 可以寫成兩個整數的平方和, $q_1,\ldots,q_r$ 可以寫成兩個整數的平方和 (Proposition 7.3.4) 以及 $(p_1^{m_1}\cdots p_s^{m_s})^2$ 可以寫成兩個整數的平方和 (因為是一個平方數), 故由 Lemma 7.3.1 知 n 可以寫成兩個整數的平方和.

反之, 若 $p\equiv 3 \pmod 4$ 是 n 的一個質因數且其次數為 $2k+1$, 即 $n = p^{2k+1}n'$, 其中 $p\nmid n'$. 我們用反證法證明 n 不可以寫成兩個整數的平方和. 假設存在 $a,b\in\mathbb{Z}$ 使得 $a^2+b^2 = n$. 則由 Lemma 7.3.5 知 $p|a$ 且 $p|b$. 令 $a = p^r c$ 且 $b = p^s d$, 其中 c,d 皆與 p 互質且 $r,s\in\mathbb{N}$. 不失一般性我們假設 $2r\leq 2s$, 我們要證明 $2k+1>2r$. 假設 $2k+1<2r$, 由 $p^{2r}c^2+p^{2s}d^2 = p^{2k+1}n'$ 知 $n' = p^{2r-2k-1}c^2+p^{2s-2k-1}d^2$. 又因為 $2s-2k-1\geq 2r-2k-1>0$ 知 $p|n'$. 此與 $p\nmid n'$ 相矛盾, 故知 $2k+1>2r$. 再由 $p^{2r}c^2+p^{2s}d^2 = p^{2k+1}n'$ 知

$$c^2+p^{2s-2r}d^2 = c^2+(p^{s-r}d)^2 = p^{2k+1-2r}n',$$

即 $p^{2k+1-2r}n'$ 可以寫成 c 和 $p^{s-r}d$ 的平方和. 由於 $p\equiv 3 \pmod 4$, $p|p^{2k+1-2r}n'$ 且 $p\nmid c$, 此與 Lemma 7.3.5 的結果相矛盾, 故知 n 不可以寫成兩個整數的平方和. □

例如 $2250 = 2\times 3^2\times 5^3$ 中唯一的除以 4 餘 3 的質因數是 3, 且 3 的次數為 2 是偶數, 所以 2250 可以寫成兩個整數的平方和. 事實上 $2250 = 45^2+15^2$. 另外 $6174 = 2\times 3^2\times 7^3$ 中除以 4 餘 3 的質因數是 3 和 7, 其中 7 的次數為 3 是奇數, 所以 6174 無法寫成兩個整數的平方和.

7.3.2. Sum of Four Squares. 我們已知並不是所有的正整數都可以寫成兩個整數的平方和, 所以很自然會問是否所有的正整數都可以寫成三個整數的平方和. 這其實仍不對, 例如 7 就不能寫成三個整數的平方和. 事實上我們可以證得一個正整數不能寫成三個整數的平方和若且唯若此正整數可表成 $4^m(8n+3)$ 這樣的形式. 不過這裡因為三個整數的平方和沒有如 Lemma 7.3.1 的性質, 所以此事實之證明會比處理兩個整數的平方和複雜的多. 由於在此我們著重於讓大家學習如何將已知的方法推廣, 我們將避談三個整數平方和的問題, 而直接談論四個整數的平方和問題.

我們要推廣處理兩個整數的平方和的方法來處理四個整數的平方和問題. 首先我們有一個和式子 (7.1) 相對應的式子.

$$(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2) = (ae+bf+cg+dh)^2+(af-be+ch-dg)^2 \\ +(ag-bh-ce+df)^2+(ah+bg-cf-de)^2. \tag{7.2}$$

這個等式可以直接將等號兩邊展開來求證. 或許大家會好奇這個等式是如何得到的, 事實上這個等式可以利用複數的推廣即所謂的 quaternion algebra 來說明. 不過由於 quaternion algebra 已偏離我們的主題太遠, 我們就不再多說明了.

利用式子 (7.2) 我們馬上有以下之結果.

Lemma 7.3.8. *若 $m,n\in\mathbb{N}$ 皆可以寫成四個整數的平方和, 則 mn 亦可以寫成四個整數的平方和.*

由於每個大於 1 的整數都可以寫成質因數的乘積, 所以由 Lemma 7.3.8 我們很自然的要探討哪些質數可以寫成四個整數的平方和. 由於 2 和除以 4 餘 1 的質數皆可寫成兩個整數的平方和, 所以它們皆可寫成四個整數的平方和 (多餘的兩個補 0), 因此我們僅剩下要討論除以 4 餘 3 的質數. 我們可以推廣 Lemma 7.3.2 的方法得到一個判別一個質數是否可以寫成四個整數的平方和的方法.

Lemma 7.3.9. *假設 p 是一個質數. 若存在 $a,b,c,d\in\mathbb{Z}$ 使得 $a^2+b^2+c^2+d^2=\lambda p$, 其中 $\lambda\in\mathbb{N}$ 滿足 $\lambda<p$, 則 p 可以寫成四個整數的平方和.*

Proof. 考慮集合 $S=\{s\in\mathbb{N}\mid$ 存在 $t,u,v,w\in\mathbb{Z}$ 使得 $t^2+u^2+v^2+w^2=sp\}$. 依照 S 的定義, 要證明 p 可以寫成四個整數的平方和就等同於要證明 $1\in S$. 要如何知 $1\in S$ 呢? 依假設知 S 為非空集合 (因 $\lambda\in S$) 且 S 的元素皆為正整數, 所以 $1\in S$ 若且唯若 S 中最小的元素就是 1. 令 $m\in S$ 是 S 中最小的元素, 我們要證明 $m=1$.

利用反證法, 假設 $m\neq 1$. 故由 $\lambda\in S$ 且 $\lambda<p$ 知 $1<m<p$. 我們希望在 S 中找到比 m 更小的數而得到矛盾. 由於 $m\in S$, 故存在 $t,u,v,w\in\mathbb{Z}$ 使得 $t^2+u^2+v^2+w^2=mp$, 我們分成 m 是偶數及 m 是奇數兩種情況討論.

(I) m 是偶數: 此時由於 $t^2+u^2+v^2+w^2=mp$ 是偶數, 我們知 t,u,v,w 必皆為奇數; 皆為偶數偶; 或是其中兩個是奇數兩個是偶數. 在所有的情況之下我們都可以將 t,u,v,w 分成同奇同偶的兩對. 不失一般性, 我們假設 t,u 同奇同偶且 v,w 同奇同偶, 即 $t+u$, $t-u$, $v+w$ 和 $v-w$ 皆為偶數. 此時 $(t+u)/2$, $(t-u)/2$, $(v+w)/2$ 和 $(v-w)/2$ 皆為整數且

$$(\frac{t+u}{2})^2+(\frac{t-u}{2})^2+(\frac{v+w}{2})^2+(\frac{v-w}{2})^2=\frac{m}{2}p.$$

故知 $m/2\in S$ 且 $m/2<m$, 此與 m 是 S 中最小的元素相矛盾.

(II) m 是奇數: 因為當 m 是奇數時

$$\{\frac{-m+1}{2},\frac{-m+1}{2}+1,\ldots,0,1,\ldots,\frac{m-1}{2}-1,\frac{m-1}{2}\}$$

是一個 complete residue system modulo m. 我們可找到 $e,f,g,h\in\mathbb{Z}$ 滿足 $e\equiv t \pmod m$, $f\equiv u \pmod m$, $g\equiv v \pmod m$ 且 $h\equiv w \pmod m$, 其中 $-(m-1)/2\le e,f,g,h\le(m-1)/2$. 注意這

裡 e, f, g 和 h 不能同時等於 0, 否則會得 $m|p$ 而和 $1<m<p$ 相矛盾. 因為 $e^2+f^2+g^2+h^2 \equiv t^2+u^2+v^2+w^2 \pmod{m}$ 以及 $t^2+u^2+v^2+w^2 = mp$, 我們得 $e^2+f^2+g^2+h^2 \equiv 0 \pmod{m}$. 亦即存在 $k \in \mathbb{Z}$ 使得 $e^2+f^2+g^2+h^2 = km$. 注意因 e, f, g 和 h 不同時為 0, 故 $k \neq 0$. 另一方面因為 $-(m-1)/2 \leq e, f, g, h \leq (m-1)/2$, 所以 $e^2+f^2+g^2+h^2 \leq (m-1)^2 = (m-1)^2 < m^2$, 故得 $0<k<m$. 也就是說 $k \in \mathbb{N}$ 且 $k<m$. 現在我們有兩個等式: $t^2+u^2+v^2+w^2 = mp$ 以及 $e^2+f^2+g^2+h^2 = km$. 利用式子 (7.2) 得

$$(te+uf+vg+wh)^2+(tf-ue+vh-wg)^2+(tg-uh-ve+wf)^2+(th+ug-vf-we)^2 = m^2kp.$$

又因為 $e \equiv t \pmod{m}$, $f \equiv u \pmod{m}$, $g \equiv v \pmod{m}$ 且 $h \equiv w \pmod{m}$, 我們得

$$te+uf+vg+wh \equiv tf-ue+vh-wg \equiv tg-uh-ve+wf \equiv th+ug-vf-we \equiv 0 \pmod{m}.$$

也就是說若令

$$T = \frac{te+uf+vg+wh}{m}, U = \frac{tf-ue+vh-wg}{m},$$

$$V = \frac{tg-uh-ve+wf}{m} \quad \text{and} \quad W = \frac{th+ug-vf-we}{m},$$

則 $T, U, V, W \in \mathbb{Z}$ 且

$$T^2+U^2+V^2+W^2 = kp.$$

也就是說 kp 可以寫成四個整數的平方和, 故又由 $k \in \mathbb{N}$ 知 $k \in S$. 然而我們又知 $k<m$, 此與 m 是 S 中最小的元素相矛盾.

我們證得若 $m \neq 1$ 會造成 m 不是偶數且不是奇數的矛盾. 故由反證法知原假設 $m \neq 1$ 不成立, 也就是說 $m = 1$. 故得證 p 可以寫成四個整數的平方和. □

接下來我們將利用 Lemma 7.3.9 來證明所有的正整數皆可寫成四個整數的平方和. 我們僅剩下要說明除以 4 餘 3 的質數可以寫成四個整數的平方和. 由於此時 $x^2 \equiv -1 \pmod{p}$ 無解, 我們要利用此特性找出一個 $\alpha \in \mathbb{N}$ 使得 $x^2 \equiv -\alpha \pmod{p}$ 有解. 由於此時 $\left(\frac{-\alpha}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{\alpha}{p}\right) = -\left(\frac{\alpha}{p}\right)$, 得 $\left(\frac{-\alpha}{p}\right) = 1$ 若且唯若 $\left(\frac{\alpha}{p}\right) = -1$. 所以我們必須找到 $\alpha \in \mathbb{N}$ 使得 $x^2 \equiv \alpha \pmod{p}$ 無解. 這是可以辦到的, 因為 $S = \{1, 2, \ldots, p-1\}$ 是 modulo p 的 reduced residue system, 若 $p \nmid a$, 則 $x^2 \equiv a \pmod{p}$ 的解必和 S 中的某個元素在 modulo p 之下同餘. 也就是說 $x^2 \equiv a \pmod{p}$ 有解若且唯若存在 $c \in S$ 使得 $c^2 \equiv a \pmod{p}$. 所以我們只要將 S 中的每一個元素平方, 若 a 和平方後的某個數在 modulo p 之下同餘則 $x^2 \equiv a \pmod{p}$ 有解; 反之, 若 a 和平方後每個數在 modulo p 之下皆不同餘則 $x^2 \equiv a \pmod{p}$ 無解. 然而若 $c \in S$ 則 $p-c \in S$ 且 $(p-c)^2 \equiv (-c)^2 \equiv c \pmod{p}$, 又因為 p 是奇質數, 所以 $c \not\equiv p-c \pmod{p}$. 也就是說 S 中的元素平方後在 modulo p 之下僅有 $(p-1)/2$ 個不同餘類. 因此我們知道 S 中共有 $(p-1)/2$ 個元素 a 會使得 $x^2 \equiv a \pmod{p}$ 有解, 且有 $(p-1)/2$ 個元素 a 會使得 $x^2 \equiv a \pmod{p}$ 無解.

Theorem 7.3.10. 若 p 是一質數且 $p \equiv 3 \pmod{4}$, 則 p 可以寫成四個整數的平方和. 特別地, 所有的正整數皆可以寫成四個整數的平方和.

Proof. 假設 p 是一質數且 $p \equiv 3 \pmod 4$. 我們要找到 $a,b,c,d \in \mathbb{Z}$ 使得 $a^2+b^2+c^2+d^2 = \lambda p$, 其中 $\lambda \in \mathbb{N}$ 且 $\lambda < p$, 再利用 Lemma 7.3.9 證得 p 可以寫成四個整數的平方和.

現考慮 $S = \{1,2,\ldots,p-1\}$ 這一個 modulo p 的 reduced residue system. 令 $\alpha \in S$ 是 S 中最小的數使得 $x^2 \equiv \alpha \pmod p$ 無解, 也就是說 $\left(\frac{\alpha}{p}\right) = -1$. 由於 $\left(\frac{1}{p}\right) = 1$, 我們知 $\alpha > 1$, 因此 $\alpha - 1 \in S$, 且 $x^2 \equiv \alpha - 1 \pmod p$ 有解 (因 α 是 S 中最小的數使得 $x^2 \equiv \alpha \pmod p$ 無解). 另一方面 $p \equiv 3 \pmod 4$, 所以 $\left(\frac{-1}{p}\right) = -1$, 故得 $\left(\frac{-\alpha}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{\alpha}{p}\right) = 1$, 也就是說 $x^2 \equiv -\alpha \pmod p$ 有解. 現令 $a \in S$ 是 $x^2 \equiv \alpha - 1$ 之一解, 我們可選 a 使得 $1 \le a \le (p-1)/2$. 這是因為若 $(p+1)/2 \le a \le p-1$, 則考慮 $p-a$, 此時 $(p-a)^2 \equiv (-a)^2 \equiv \alpha - 1 \pmod p$ 仍為 $x^2 \equiv \alpha - 1 \pmod p$ 之一解且 $1 \le p-a < (p-1)/2$. 同理我們也可找到 $b \in S$ 是 $x^2 \equiv -\alpha \pmod p$ 之一解且 $1 \le b \le (p-1)/2$. 現由於

$$a^2+b^2+1 \equiv \alpha - 1 + (-\alpha) + 1 \equiv 0 \pmod p,$$

故存在 $\lambda \in \mathbb{N}$ 使得 $a^2+b^2+1 = \lambda p$. 又由於

$$\lambda p = a^2+b^2+1 \le (\frac{p-1}{2})^2 + (\frac{p-1}{2})^2 + 1 < \frac{p^2}{2} + 1 < p^2,$$

所以我們有 $\lambda < p$. 故利用 Lemma 7.3.9 得證 p 可以寫成四個整數的平方和.

現任取 $n \in \mathbb{N}$. 若 $n = 1$, 則 n 當然寫成四個整數的平方和. 若 $n > 1$, 則可將 n 寫成質因數之乘積 $n = p_1^{n_1} \cdots p_r^{n_r}$. 若 $p_i = 2$ 或 $p_i \equiv 1 \pmod 4$ 則 p_i 可以寫成兩個整數的平方和, 故可以寫成四個整數的平方和. 若 $p_i \equiv 3 \pmod 4$, 則由前知 p_i 也可以寫成四個整數的平方和. 故利用 Lemma 7.3.8 知 $n = p_1^{n_1} \cdots p_r^{n_r}$ 可以寫成四個整數的平方和. □

我們已介紹了一些基礎數論應有的基本知識, 本講義就此結束.