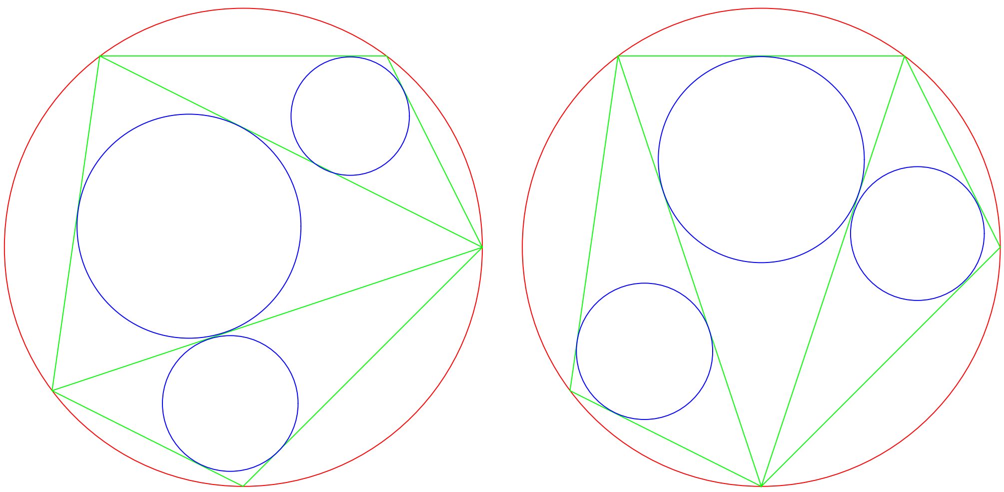
# 算術講義

許 志 農

國立台灣師範大學數學系

December 28, 2004



左圖三小圓半徑和＝右圖三小圓半徑和

# 目 錄

# 1 胡言亂語的算術

就如同標題所講的，這是無意義的談話，同時也是你對這裡的談論所應抱持的期望。我把「算術」這個字加在我的標題上是對數學王子高斯的一種讚揚。因為他在二十四歲時出版了不朽傑作「算術講話」，而這裡用算術之詞並無冒犯之意。我將從唯一的偶質數 2 開始，而以不祥數字 65 作結束。[1]

## 2

- 除了 $(3,4,5),(5,12,13)$ 之外，還可以找到無窮多個邊長是正整數的直角三角形（彼此不相似）。換言之，方程式

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

有無窮多對正整數解 $(x,y,z)$（彼此不成比例）。如果將 2 改成比 2 大的次方 $n$，則費馬最後定理告訴我們：方程式

$$x^n+y^n=z^n$$

無正整數解 $(x,y,z)$。

- 像 $(3,5),(5,7),(11,13),(17,19)$ 的質數數對稱為孿生質數（即兩質數的差為 2 之數對）。數對 $(p,p+2)$ 為孿生質數的充分必要條件為

$$4\left[(p-1)!+1\right]+p\equiv 0 \pmod{p(p+2)}.$$

直到目前為止，仍然不知道是否有無窮多對孿生質數？

- 若奇質數 $p$ 滿足

$$2^{p-1}\equiv 1 \pmod{p^2}$$

則叫 $p$ 為 Wieferich 質數。 1093 是質數而且是最小的 Wieferich 質數，即

$$2^{1092}\equiv 1 \pmod{1093^2}.$$

我們一直不知道是否有無窮多個 Wieferich 質數。

- 如果 $d$ 是一個正整數，則符號 $[(3/2)^d],\{(3/2)^d\}$分別代表分數 $(3/2)^d$ 化為小數之後的整數及小數部分。一個尚未解決的難題：是否對每個正整數 $d$，恆有

$$2^d\{(3/2)^d\}+[(3/2)^d]\le 2^d.$$

如果這個難題（不等式）對正整數 $d$ 是正確的，那麼可以知道：每個正整數皆可以表為至多

$$2^d+[(3/2)^d]-2$$

[1]本文是 Paulo Ribenboim 在 Mathematics Magazine 71 (5) Dec. 1998 上的文章 Galimatias Arithmeticae，經本人翻譯、改編而成。

個正整數的 $d$ 次方和。例如：$d=2$ 時，上述不等式成立，所以每個正整數皆可以表為至多 4 個正整數的平方和。這就是 Lagrange 的四平方和定理。

# 5

- 如果 $a, b, c, d$ 是四個正整數而且滿足

  $$a^5+b^5=c^5+d^5,$$

  則數學家猜想：$a=c, b=d$ 或者 $a=d, b=c$。將 5 次改為 3 次時，是有反例的：印度數學家 Ramanujan 發現的

  $$1729=9^3+10^3=1^3+12^3.$$

- 如果 $p$ 是一個質數且 $p \geq 5$，則

  $$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}.$$

  到目前為止仍然不知道它的反敘述是否也是正確的？

- 設費氏數列：$f_0=0, f_1=1$ 及 $f_n=f_{n-1}+f_{n-2}$ $(n \geq 2)$，且 5 次多項式

  $$F(x,y)=2xy^4+x^2y^3-2x^3y^2-y^5-x^4y+2y.$$

  下列兩個集合是一樣的：

  $$\{f_n \mid n=1,2,3,\cdots\}$$

  與

  $$\{F(x,y) \mid x, y \text{ 為非負整數且 } F(x,y)>0\}.$$

- 數列 $<u_n>$: $u_1=1, u_2=2, u_{n+2}=5u_{n+1}-u_n$ 為

  $$U=\{1,2,9,43,206,\cdots\};$$

  而數列 $<v_n>$: $v_1=1, v_2=3, v_{n+2}=5v_{n+1}-v_n$ 為

  $$V=\{1,3,14,67,321,\cdots\}.$$

  設 $N$ 是使 $21n^2-20$ 為完全平方數的所有正整數 $n$ 所構成的集合。我們知道

  $$N=U \cup V.$$

# 11

- 11 是最小重複 1 的質數。所謂的重複 1 的數是指所有數字都是 1 的數，在此以符號 $R_n$ 表示重複 1 的數 $11\cdots1$（有 $n$ 個 1），例如 $R_2=11, R_3=111$。下面是眾所周知的重複 1 的質數：$R_n$, $n=2,19,23,317$ 及 1031。是否有無限多個重複 1 的質數就不得而知了。

- 我們不知道是否有一長、寬、高及所有對角線的長度皆是正整數的長方體。換句話說，不知道下面的方程式是否有非零的整數解：

$$\begin{cases} a^2+b^2=d^2, \\ b^2+c^2=e^2, \\ c^2+a^2=f^2, \\ a^2+b^2+c^2=g^2. \end{cases}$$

  假如這種非零整數解存在，則 $abc$ 是 11 的倍數。

- 當 $n$ 超過 11 時，$n(n+1)(n+2)(n+3)$ 一定會有一個超過 11 的質因數。馬勒（Mahler）定理：假如 $f(x)$ 是一個二次或更多次的整係數多項式（二次的情形稱為波利亞定理）且 $P$ 是由有限個質數所組成的集合（例如集合 $P=\{2,3,5,7,11\}$ 等）。那麼可以找到一個整數 $N_{f,P}$ 使得：若 $f(n)$ 的所有質因數都在 $P$ 裡，則 $n\le N_{f,P}$。

- 梅森尼（Mersenne）數是指可表為 $2^p-1$ 的整數，其中 $p$ 是質數並以符號 $M_p$ 表示。例如 $M_{11}=2^{11}-1=2047=23\times89$ 是梅森尼數中最小的合數，而梅森尼數中已知的最大合數為 $M_p$，其中

$$p=8069496435\times10^{5072}-1.$$

# 19

- 拿破崙在 19 歲時打贏了戰爭，而高斯 19 歲時發現了二次互反定理（一旦你知道了，你就不能忘記）。

- 三位數 $abc$ 是 19 的倍數之充分必要條件為：$10a+b+2c$ 也是 19 的倍數。

- 19 是使下數為質數的最大整數值 $n$：

$$n!-(n-1)!+(n-2)!-\cdots\pm1!.$$

  具有此種性質的其它整數還有 $n=3,4,5,6,7,8,9,10$ 及 15。

- 重複 1 的數 $R_{19}$ 和梅森尼數 $M_{19}$ 都是質數。

- 費氏數列：$f_0=0, f_1=1$ 及 $f_n=f_{n-1}+f_{n-2}$ $(n\ge2)$。假如 $f_p$ 是質數，則 $p$ 必也是質數，但反過來並不一定對，例如 $f_{19}=4181=37\times113$ 提供此種反例。

- Balasubramanian, Dress, Deshoullers 在 1986 年證明每一個正整數都可以表為 19 個整數的四次方和。Davenport 在 1939 年就證明了每一個充分大的正整數可表為 16 個整數的四次方和。這些證明解決了華林問題在四次方的情形。

# 29

- 數學家尤拉發現：如果 29 整除 $a^4+b^4+c^4$，則 $a,b,c$ 都是 29 的倍數。

- 設 $p$ 是一個質數，定義 $p\sharp$ 為不超過 $p$ 的所有質數之乘積，例如

$$3\sharp = 2\times 3, 5\sharp = 2\times 3\times 5, 11\sharp = 2\times 3\times 5\times 7\times 11.$$

  歐幾里德已經會使用 $p\sharp+1$ 和 $p\sharp-1$ 這種數來證明：質數有無窮多個。經計算知道

$$5 = 3\sharp-1, 29 = 5\sharp-1, 2309 = 11\sharp-1$$

  都是質數。下面列出的是使 $p\sharp-1$ 是質數的質數 $p$：

$$p = 3, 5, 11, 13, 41, 89, 317, 991, 1873, 2053, \cdots$$

  我們並不知道是否有無窮多個質數 $p$ 使得 $p\sharp-1$ 也是質數。

- $f(x)=2x^2+29$ 是最佳產生質數的多項式。尤拉是第一位考慮這種多項式的數學家。設整係數多項式 $f(x)$ 的首項係數為正數，且 $f(0)$ 是一個質數，而正整數 $r$ 是下一個使得質數 $f(0)$ 整除 $f(r)$ 的正整數。如果 $f(0), f(1), \cdots, f(r-1)$ 都是質數，則稱多項式 $f(x)$ 為最佳產生質數的多項式。尤拉也觀察到 $f(x)=x^2+x+41$ 也是最佳產生質數的多項式，因為 $f(0)=41$ 且 $f(1), f(2), \cdots, f(39)$ 都是質數，而 $f(40)=40^2+40+41=41^2$ 是 41 的倍數。

# 30

- 邊長為 $5, 12, 13$ 的直角三角形是唯一面積等於周長的直角三角形（邊長值需是正整數），其周長（或面積）為 30。

- $d=30$ 是滿足下述條件的最大正整數：若整數 $a$ 滿足 $1<a<d$ 且 $a$ 與 $d$ 互質，則 $a$ 一定是質數。其它符合此種性質的數還有

$$d = 3, 4, 6, 8, 12, 18, 24.$$

  這結果是 Schatunowsky 在 1893 年及 Wolfskehl 在 1901 年證得。

# 60

- 60 進位制是蘇美人的計數系統（約西元前 3500 年）。今天我們在天文學和時間的分割上仍然是使用六十進位制。

- 60 是一個高度合成數。這種數是由印度數學家 Ramanujan 於 1915 年所介紹及研究。當我們稱正整數 $n$ 為高度合成數時，表示對於每一個正整數 $m, 1 \leq m < n$，恆有 $d(n) > d(m)$，其中 $d(m)$ 表示 $m$ 的正因數個數。下面所列的數皆為高度合成數：
$$2, 4, 6, 12, 24, 48, 60, 120, 180, 240, 360, 720, 840, \cdots .$$

- 60 是酉完美數。給定正整數 $n$，如果正整數 $d$ 滿足 $d < n, d|n$ 且 $d$ 與 $n/d$ 互質，則稱 $d$ 為 $n$ 的一個酉因數。如果 $n$ 的所有酉因數的和恰為 $n$，則稱 $n$ 為酉完美數。 60 的酉因素為 $1, 3, 4, 5, 12, 15, 20$ 且它們的和是 60，所以 60 是一個酉完美數。目前知道的酉完美數有 $6, 60, 90, 87360$ 和
$$2^{18} \times 3 \times 7 \times 11 \times 13 \times 19 \times 37 \times 79 \times 109 \times 157 \times 313.$$
猜測：酉完美數僅有有限個。

- 十二面體的十二個面總共可相交出 60 條直線。

# 61

- 假如 $k \geq 0$ 且 $k + 10$ 位數
$$a_1a_2 \cdots a_kxyxyxyxyxy$$
是一個完全平方數，則 $xy = 21, 61$ 或 84。例如：
$$1739288516161616161 = 1318820881^2, 258932382121212121 = 508853989^2.$$

- 梅森尼數 $M_{61} = 2^{61} - 1$ 是一個質數。目前已知的梅森尼數 $M_p = 2^p - 1$ 中是質數的為 $p = 2, 3, 5, 7, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021227$。

# 63

- 這個數出現在二位數的 Kaprekar's 演算法的循環中。Kaprekar's 演算法的規則是：給定 $k$ 位數 $a_1a_2a_3 \cdots a_k$，其中 $a_1, a_2, a_3, \cdots, a_k$ 不完全相同，且
$$a_1, a_2, a_3, \cdots, a_k \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

由 $a_1, a_2, a_3, \cdots, a_k$ 這 $k$ 個數可以排列出一個最大的正整數 $M$，及最小的正整數 $N$。將此兩數相減，得到一個正整數（若不是 $k$ 位數，則在前面補 0 使之成為 $k$ 位數），這時再由相減所產生的這 $k$ 位數重複前面的步驟，並以此種方式重複算下去，最後可得一循環系統。例如給定二位數 35 可得

$$53-35=18 \to 81-18=\boxed{63} \to 63-36=\boxed{27} \to 72-27=\boxed{45}$$
$$\to 54-45=\boxed{09} \to 90-09=\boxed{81} \to 81-18=63 \to \cdots.$$

下面為 Karprekar's 演算法在二、三、四、五位數時的循環系統：

| | |
|---|---|
| 二位數 | $63 \to 27 \to 45 \to 09 \to 81.$ |
| 三位數 | 495. |
| 四位數 | 6174. |
| 五位數 | 有三種不同的循環系統如下： |
| | $99954 \to 95553,$ |
| | $98532 \to 97443 \to 96642 \to 97731,$ |
| | $98622 \to 97533 \to 96543 \to 97641.$ |

- 給定正整數 $a, b$ $(1 \le b < a)$。如果質數 $p$ 滿足 $p|(a^n-b^n)$，但是 $p$ 不整除

$$a^1-b^1, a^2-b^2, \cdots, a^{n-1}-b^{n-1}$$

則稱 $p$ 是 $a^n-b^n$ 的原生質因數。$2^6-1^6=63$ 沒有原生質因數，且當 $1<n, n\neq 6$ 時，$2^n-1^n$ 都至少有一個原生質因數。數學家 Zsigmondy 證明：除了

(1) $n=1, a-b=1.$

(2) $n=2$, $a, b$ 都是奇數且 $(a+b)$ 是 2 的某次方

(3) $n=6, a=2, b=1$

這三種情況之外，$a^n-b^n$ 都至少有一個原生質因數。

# 65

- $(63, 16, 65)$ 和 $(33, 56, 65)$ 是兩組整數邊長的直角三角形，其中斜邊都是 65。
- 65 是唯一的二位數 $ab$ $(0 \le b \le a \le 9)$ 使得 $ab^2-ba^2$ 是一個完全平方數。例如 $65^2-56^2=33^2$。
- 65 也許是尤拉-高斯方便數 (Numeri idonei, convenient numbers)的個數。滿足底下條件的正整數 $n$ 稱為尤拉-高斯方便數：對任何奇數 $p=x^2+ny^2$，其中 $x, y$ 是非負整數，如果下列兩個式子成立，則 $p$ 必定是一個質數。

(1) 非負整數 $x_1, y_1$ 滿足 $p = x_1^2 + ny_1^2$，則 $x = x_1, y = y_1$。

(2) $x$ 與 $ny$ 互質。

事實上，$n = 1$ 是尤拉-高斯方便數，而 $n = 11$ 不是尤拉-高斯方便數，這是因為 $15 = 2^2 + 11 \cdot 1^2$，其中 $(2, 1)$ 是唯一的一組非負整數解，且 2 與 $11 \cdot 1$ 互質，但是 15 卻不是質數。Grube 於 1874 年證明：$n$ 是一個尤拉-高斯方便數的充分必要條件為對所有滿足 $q = n + x^2 \leq (4n)/3$ 的正整數 $x$，如果 $q = rs$ $(2x \leq r \leq s)$，則 $r = s$ 或 $r = 2x$。例如：因為

$$\begin{aligned}
60 + 1^2 &= 61, \\
60 + 2^2 &= 64 = 4 \cdot 16 = 8 \cdot 8, \\
60 + 3^2 &= 69, \\
60 + 4^2 &= 76,
\end{aligned}$$

所以由 Grube 的判別法知道 60 是一個尤拉-高斯方便數。尤拉證明 1848 是一個尤拉-高斯方便數，而且

$$18518809 = 197^2 + 1848 \cdot 100^2$$

是一個質數。在尤拉的時代，這算是一項壯舉。下面列出的是尤拉找到的 65 個尤拉-高斯方便數：

$$\begin{aligned}
&1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, \\
&45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, \\
&177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, \\
&760, 840, 1320, 1365, 1848.
\end{aligned}$$

是否還有其它的尤拉-高斯方便數？Chowla 證明了尤拉-高斯方便數是有限個；稍後， Briggs, Grosswald, 及 Weinberger 指出至多有 66 個尤拉-高斯方便數。想要知道：是否存在著第六十六個尤拉-高斯方便數，可能是一項很高難度的挑戰。