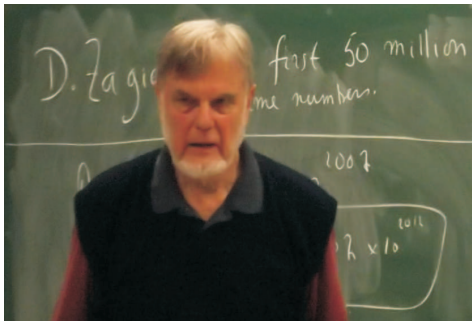
數學傳播　42卷1期, pp. 40-70

質數

演講者：Frans Oort



時　間：民國 101 年 12 月 17 日
地　點：天文數學館 101 室
翻　譯：編輯室[1]

Frans Oort 教授 1935 年生於荷蘭 Bussum, 1961 獲荷蘭 Leiden 大學博士學位, 1977 起任教於 Utrecht 大學, 2000 年退休。他對數論及代數幾何有傑出貢獻, 主要研究領域爲 abelian varieties 及其 moduli spaces。[2]

Don Zagier 曾說：「質數在自然數中像野草一樣成長, 似乎除了偶然的機運外不服從其他法則, 而且沒有人能預測下一個會從哪裡冒出來」。

摘要: 在這個演講, 我將提出幾個與質數相關的問題。我們將看到, 有些問題簡單到幾行論證就能解決, 有些則引導出深刻的問題及猜想, 至今未獲理解。這是數學研究的一般模式, 好奇心引導出『容易的』問題, 而這問題與非常深刻的結構相關。我會給出一些例子、建議及參考資料, 以供進一步的學習。這個基礎性的演講是針對大一學生, 雖不是要介紹數論, 但可以當作入門課, 介紹「數學是什麼? 如何享受問題和洞察力的魔力?」

導論

我們將在這演講探討質數。我們對下述問題尤其感興趣：「有多少個質數? 它們在何處?」我們將以更爲精確的方式陳述這些問題。在下一節, 我們會介紹更多符號和定義。

[1]原講稿中部份網址目前已無法連結, 譯稿中已逕行修改或刪除, 不另註明。

[2]參見數學傳播 38 卷 1-3 期「有朋自遠方來」專訪。

這個演講在基本層次要傳達的訊息是： 數學家是好奇的, 我們喜歡陳述問題、尋找結構、享受奇妙新奇的洞見。以下將提出一些問題, 其中一些有顯而易見的答案, 但另有一些看似單純的問題, 我們卻對之毫無頭緒; 它們的答案應該是什麼? 該開發什麼工具來了解可能的門路? 這些都是令人著迷的未解問題。

0.1 定義. 對任意 $x \in \mathbb{R}$, 我們定義 $\pi(x)$ 爲不大於 x 的質數個數：

$$\pi(x) = \#\{p \mid p \text{ 是質數且 } p \le x\}; \quad \pi : \mathbb{R} \to \mathbb{Z}$$

這裡 $\#(V)$ 表示 V 中的元素個數。這是一個階梯函數。當 $0 < x < 2$, $\pi(x) = 0$; 接著, 函數值跳躍, 對 $2 \le x < 3$, 有 $\pi(x) = 1$。這個函數如此拾階而上, 每一階的高度都是 1。

繪製 $\pi(x)$, $1 \le x < 100$ (亦即, 小規模) 的函數圖形時, 覺得階梯呈現怪異且毫無規律的形狀; 但在乍見 $\pi(x)$, $1 \le x < 50,000$ 的函數圖形時, 我們卻覺得函數似乎是平滑的 (但它不是)。這暗示我們或可談談 $\pi(x)$ 的大域行爲。事實上, 高斯在很久以前就有這個想法; 他在他的對數表寫下筆記：「1792或1793年 $\cdots$ 在 $a(=\infty)$ 之下 $\dfrac{a}{\ln(a)}$ $\Big($Im Jahr 1792 oder 1793 $\cdots$ Primzahlen unter $a(=\infty)$, $\dfrac{a}{\ln(a)}$.$\Big)$」Gauss 並未發表這個筆記, 但在他與朋友 Encke 的通信中提到它 [12]。這也正是 Legendre 在 1797/1798 年提出的猜想。

我們稱這個想法/猜想/結果爲質數定理 (prime number theory, 簡稱 PNT)。該定理由 Chebyshev、Hadamard 及 De la Vallée-Poussin 證明 (始自 1848 年有相關結果發表, 完整的證明於 1896 年提出)。這是個驚人 (而且深刻) 的結果：不須得知所有質數, 也不用具備計算它們的能力, 我們仍能討論在某處 (譬如：大於某個數, 或者在給定區間約有多少個) 能否找到它們 (而不用明確計算它們)。我們在不規則函數看到規則的行爲。

在 §7, 我們將引用這個結果 (但不能提出簡單且基礎性的證明)。但我們會看到, 較弱的敘述很容易證明, 且可用以得到驚人的結果 (我們將看到例子)。

0.2. 問題的底層結構是什麼?

接下來我會開始提出問題。對每一個問題, 請你試著判斷： 你是否了解它? 答案顯而易見或難以預見? 我們會看到, 一些問題可迅速找到簡單的答案; 另有一些問題很困難, 隱藏著未解決的問題, 一些大數學家試圖揭露寶石內隱藏的秘密卻徒勞無功, 於是我們突然間面臨知識匱乏的窘境 (我至今常對數學研究有此感覺); 這使得這個領域成爲靈感及挑戰的豐富泉源。

這就是數學研究的特色：問題引發好奇心。有時你看出 (或被告知) 某問題很簡單, 但下一個形式同樣簡單的問題卻找不到解, 而你越加沉思, 就越覺得自己對其真實結構一無所知。

我們會看到 (有時) 計算例題能提供洞察力, 但 (如你所經驗過的), 它也可能給了完全錯誤的提示和想法。我們也會看到, 抽象的方法可能會給出驚人的洞察力與結果。

我們應該試圖找出問題的基礎結構。數學家 Yuri Manin 在接受 "Good proofs are proofs that make us wiser (好的證明讓人更有智慧)" 的訪談 [28] 時說 :「我將數學創作視爲辨識既存模式的過程」; 我同意這個信念 :「我們正在找的東西都已然存在, 我們『只是』需要找到正確的語言, 解密的鑰匙」。

因此, 對以下述及的每件事, 試著找出問題的基礎模式及基本想法。

對初等數論的概念及問題的瞭解, 可能會引導出深奧的理論, 揭露代數、幾何及分析的優美結構。『簡單』問題的解決經常仰賴其他領域的進展。

0.3. 如何運用這篇文章

- 首先閱讀 §1 中的問題。試著了解它們、尋找答案 (並尋找隱藏的結構)。那些問題有容易的解法? 將這類問題謹記在心。
- 這篇文章只涵蓋這塊有趣的領域之一小部分。如果你想多學些, 可用 google 搜尋下列關鍵字 : prime number, prime number theorem, Fermat primes, Mersenne primes, Sophie Germain primes, twin primes, prime number races, Chebotarev density theorem, heuristic argument, Riemann hypothesis, ABC conjecture, $3x+1$ problem, odd perfect number, scientific calculator, factoring calculator, prime constellations, ...。譬如, 你用 google 搜尋『prime number』時, 會找到網址 : `http://en.wikipedia.org/wiki/Prime_number`。而搜尋『prime number theorem』時, 會找到網址 : `https://en.wikipedia.org/wiki/Prime_number_theorem`.
- 很多關於質數的問題源自幾何、數論及其他領域中完全不同的問題。做數學時要注意這類相互滋養的情況。參見 §5 及 §6。
- 第 8 節較不尋常。一些論述絕對是錯的 (你可試著以那些方法證明『有無限多個偶質數』, 這是正確的敘述嗎?) 譬如問題 :「給定正整數 N, 它爲質數的機率是多少?」聽來無稽, 一個數要嘛是質數、要嘛不是質數, 有隨機性? 然而,『啟發式方法 (heuristic)』的要義是 : 讓你對該有的答案產生感覺與直覺。理解第 8 節後, 試著對你想考慮的問題套用這個方法。
- 你會在 §10 看到四個習題。看了很多困難的問題及猜想後, 自己解幾個簡單問題可能會讓你開心。
- 嘗試做一些與 §1 中的問題相關的計算, 看看是否能獲得一些洞察力。有時它會引導你做出正確的期待, 有時你會一事無成。以此方式, 你會感覺出數學家如何思考、如何嘗試找到新

的結構與想法。在 1996 年 BBC 製作 的紀錄片中, Andrew Wiles 說 :「若要最貼切地形容我做數學的經驗, 可借用進入一棟黑暗的大廈來比喻。進入第一個房間時, 徹底黑暗, 跌跌撞撞, 不時被家具絆倒, 你也因而逐漸得知每樣家具座落何處。終於, 六個月左右後, 你發現電燈的開關; 打開開關時, 突然大放光明, 你於是確切知道自己身在何處。」

- 在 §9, 我們會介紹一些 open problems, 迄今未解決, 甚至大數學家也不知從何處著手, 該發展什麼理論, 該往什麼新的方向探勘。年輕數學家想想, 有那麼多東西在等待你。
- **一個小警告。**做些計算是好的。事實上, 我們有好夥伴 (Gauss 年輕時, 在閒暇時計算質數, 從而感受質數的數量。) 但你不能無止無盡做計算; 你要知道在何處進行計算, 也要知道該在何處停下來思考。譬如, 你可嘗試將偶數寫成兩個質數的和 : $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7$, $\cdots$ 但你要無止無盡算下去嗎?
- 對我來說, 這個領域有下述的大驚喜 :
  - 看來簡單的問題可能很難; 只要還欠缺對基礎理論的描述, 大部分問題都得不到精確解。
  - 但我們不用對任何相關案例做計算, 就能給出精確的逼近; 且這些方法通常很簡單。

書單 [8, 18, 25] 是小說, 讀起來很有趣。[30] 也是小說, 描述 Sophie Germain 的 (數學) 童年, 很好讀。在 `http://kasmana.people.cofc.edu/MATHFICT/default.html` 有更多推薦書。

若想瞭解初等數論的基本概念, 請讀 [4] 和 [19]。關於代數的基本知識, 有很多書可讀, 我們建議 [24]。

0.4. 有些網站可以用來做計算, 提供科學計算器, 譬如 `http://web2.0calc.com/#`. 要分解因數, 可前往: `http://www.numberempire.com/factoringcalculator.php`. 要找第 N 個質數 ($N < 10^{12}$) 可至 `http://primes.utm.edu/nthprime/` 要找 Collatz trees 請到 `https://www.nitrxgen.net/collatz_php`. 若知道起始值, 可在 `http://oeis.org/` 找到整數序列。

§1. 一些問題

1.1 問題1. 質數的個數爲有限? 無限? [你從何處著手? 只是計算和製作 (有限) 質數列表會有幫助嗎? 還是應該開始思考?] 有關答案, 請參閱第 3 節。

我們探討相繼質數的間隙, 它們相距甚遠或十分靠近? 若一系列質數中存在兩個質數 p, q 使得 $p - q = N$, 則稱 N 爲此系列質數的間隙長度 (length of the gap)。

1.2 問題2. 質數系列的間隙長度是有界或無界? [你嘗試做什麼? 思考? 或者舉個例子?] 參見 (4.1) 及 §7。我們探討 :「質數是否會盡可能地接近彼此?」

定義: 我們稱質數對 p, q 爲『孿生質數(twin primes)』若且唯若 $p < q$ 且 $q - p = 2$。我們稱三質數 p, q, r 爲『質數三聯體 (3-sequence of prime numbers)』 (不是標準術語) 若且唯若 $p < q < r$, $q - p = 2$ 且 $r - q = 2$.

1.3 問題3. (1) 孿生質數對的個數爲有限? 無限? (2) 質數三聯體所構成的集合是什麼? [算出很多例子會有幫助嗎? 如何獲得洞察力?] 參見 (4.4)。

1.4 問題4. 考慮

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537, \ldots, F_i = 2^{2^i} + 1.$$

這序列中的數都是質數嗎? 如若不然, 這序列中質數的個數爲有限或無限? [即使在 i 還算小時, F_i 就已頗大; 你要如何計算? 還是你要先思考? 爲了瞭解這些數, 你需要做什麼其他的工作? 參見 §5 及 (9.6)。

1.5 問題5. 將所有質數由小至大列爲

$$p_1 = 2 < p_2 = 3 < \cdots < p_i < p_{i+1} < \cdots$$

任取 i, 是否有公式讓你能計算第 i 個質數 p_i? [問題的陳述方式正確嗎? 這問題有意義嗎?] 參見 (4.5) 及 §7。

1.6 問題6. 我們觀察到

$$4 = 2 + 2,\ 6 = 3 + 3,\ 8 = 3 + 5,\ \cdots,\ 36 = 5 + 31 = 7 + 29, \cdots (?)$$

每個偶數 $N = 2n \geq 4$ 都能寫成兩個質數的和嗎? [如何著手? 逕自開始計算, 直到發現反例? 有其他方案嗎?] 參見 Goldbach Conjecture (9.2), (9.3)。

(1.6)* 另一問題。我們觀察到

$$2 = 5 - 3,\ 4 = 47 - 43,\ 6 = 13 - 7, \ldots, 18 = 47 - 29, \cdots$$

每個偶數都能寫成兩個質數的差嗎? 參見 (9.5)。

1.7 問題7. 是否存在十進制下有 2013 位數的質數? [如何著手? 任意寫下某介於 10^{2012} 和 10^{2013} 之間的數, 而後試著決定該數是否爲質數? 如此建構出質數的機會是大是小? 像隨機廣告嗎? 你還能試什麼方法?] 參見 (4.9), 也請看 (7.4), (7.8).

1.8 問題8. 試著找到整數 A, a, D, $d \geq 2$ 使得

$$A^a + 1 = D^d.$$

亦即是否存在差 1 的兩個純冪 (純冪是形如 A^a 的整數, 其中 A, $a \geq 2$)。我們看到有一組解 $2^3 + 1 = 8 + 1 = 9 = 3^2$。有其他解嗎? [寫下純冪 4, 8, 9, 16, 25, 36, 49, ...。觀察是否有某配對差數爲 1, 這是好方法嗎? 還有其他方案嗎? 這問題到底是簡單、困難, 亦或無解? 參見 (4.10)。

1.9 問題9. 稱質數 p 爲 Sophie Germain 質數, 若且唯若 $q := 2p + 1$ 也是質數。Sophie Germain 質數的個數爲有限或無限? 參見 (9.8)。

1.10 問題10. 定義函數 $C : \mathbb{N} \to \mathbb{N}$ 爲

$$C(2m) := m, \quad C(2m + 1) = 3(2m + 1) + 1.$$

(亦即, 當 n 爲偶數, 令 $C(n) = n/2$; 當 n 爲奇數, 令 $C(n) = 3n + 1$). 任取 $a_1 \in \mathbb{N}$, 可得序列 $\{a_1, \ldots, a_{i+1} := C(a_i) \cdots\}$, 而 1 這個數是否總會出現在序列中? 參見 (9.9)

我們可以提出更多這樣的問題。但這十個問題已提供足夠的材料讓你思考, 也足夠讓你發展出對這類數學的感覺。試著判斷哪一個問題有簡單的答案, 哪一個問題可以從一般理論中得到答案。也許你被困在其中的一些問題 (這發生在每位思索好問題的數學家身上)。(在你的數學生涯中, 不要因爲無法解決的問題而灰心喪氣; 那是我們這一行業的一部分美好。)

下面我會討論答案, 截至目前的結果列於 (9.11)。

§2. 一些定義

2.1. 我們令 $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, 3, \cdots\}$ 爲所有整數的集合。給定 $a, b \in \mathbb{Z}$, 我們稱 a 爲 b 的一個因數 (divisor) 若且唯若存在整數 $d \in \mathbb{Z}$ 使得 $da = b$。符號約定爲 $a \mid b$.

我們稱大於 1 的整數 p 爲質數, 若且唯若 p 的因數只有 1 和 p, 換言之, 任何整數 i, $1 < i < p$, 都不是 p 的因數, 例如：2, 3, 5, 7, 11, 13, 17, 19, $\cdots$, 61, 67, 71, $\cdots$, 613, 617, 619, $\cdots$ 等。

備註：以現代術語來說, 整數 1 不是質數 (儘管 Euler 稱 1 爲質數)。

2.2. 最大公約數。 給定不爲零的整數 m, n, 考慮它們的共同因數所成的的集合 :

$$\{d \in \mathbb{Z} \mid 1 \le d, d \mid m, d \mid n\}.$$

因 $1 \mid m$ 且 $1 \mid n$, 此集合非空。稱此集合的最大元素爲最大公約數, 記爲 $\gcd(m,n)$。若 $\gcd(m,n) = 1$, 我們稱『m 和 n 互質』。

備註 : 我們能證明 : 若 $\gcd(m,n) = d$, 則存在 $x, y \in \mathbb{Z}$ 使得 $xm + yn = d$。

備註 : 我們能證明 : $\gcd(m,n) = d$ 是集合 $\{xm + yn \mid x, y \in \mathbb{Z}\}$ 的最小正整數。見 §11。

2.3. 對數。 對數是用基數定義和計算的。對 $a \in \mathbb{Z}$, $a > 1$, 我們記

$$\log_a x = y \;\Leftrightarrow\; x = a^y.$$

且記

$$\log x = \log_e x; \qquad \text{其中 } e \text{ 爲 Euler 常數。}$$

可能你已習慣 $\ln(x) = \log_e x$ 及 $\log(x) = \log_{10}(x)$。但數學家 (及本文中) 稱 $\log(x) = \log_e(x)$。

§3. 歐幾里得的證明

3.1 定理 (Euclid)**.** 有無限多個質數。

證明: 我們知道至少有一個質數, 譬如 37。假設僅存在有限多個質數 $P_1, \ldots, P_m$, $m > 0$。藉由這些質數, 我們建構出不在此列的質數, 從而證得定理。

建議. 考慮

$$M = P_1 \times \cdots \times P_m + 1.$$

注意到 $M > 1$。取 $P > 1$ 爲 M 的最小因數。我們能證明 P 爲質數; 事實上, P 的任何因數 $d \mid P$ $(1 < d \le P)$ 必然也是 M 的因數, 因此 $d = P$, 亦即 P 爲質數。接著, 我們

聲稱. **質數** $P \notin \{P_1, \ldots, P_m\}$. 如若不然, 設對某 $1 \le i \le m$ 有 $P = P_i$。則有

$$BP_i + 1 = M = AP, \text{ 其中 } B := P_1 \times \cdots \times P_{i-1} \times P_{i+1} \times \cdots \times P_m;$$

因此 $(A - B)P = 1$, 所以 $B - A = \pm 1$ 且 $P = \pm 1$, 違背了 $P > 1$ 的假設, 因此 P 是質數且 $P \notin \{P_1, \ldots, P_m\}$。 得證

備註: **我的建議**. 記住這個證明。你可以用有限的論證談論無限集合, 這不是很不尋常嗎? 你不用列出所有質數, 就可以斷言有無限多個質數。這就是數學推理的優勢。如果有人想知道你爲何在做數學, 你可以介紹這論證, 當作展現數學之美的第一個例子。

在 5.1 可看到『存在無限多個質數』另一證明。

3.2. 一個變體. 對質數集合 $\{P_1, \ldots, P_m\}$ 及上述 $M = P_1 \times \cdots \times P_m + 1$, 我們可定義 $P_{m+1}, \ldots, P_r$ 爲所有 M 的質因數 (用 (11.2))。可對 $\{P_1, \ldots, P_m, \ldots, P_r\}$ 運作歸納法以完成 (3.1) 的證明。

備註: 我們並沒有證明上述 M 爲質數。譬如, 對 $P = P_1 = 2$, 我們令 $P_2 = 3$, $P_3 = 2 \times 3 + 1 = 7$, $P_4 = 2 \times 3 \times 7 + 1 = 43$, 但 $2 \times 3 \times 7 \times 43 + 1 = 1807 = 13 \times 139$。事實上, 少有形如 $N! + 1$ 的質數; 參見 [5] 4.6。

我們並未證明所有質數皆可循此途徑造出。事實上, 我預期：始自任意非空的質數集合, 如 (3.2) 般運作歸納法, 會得到無限多個質數, 但這不能涵蓋所有質數。能證明這件事嗎?

§4. 一些答案

4.1. 質數序列的間隙. 這裡有 (1.2) 的答案。我們將證明：對任意大於或等於 3 的整數 N, 存在一對相繼的質數 (p_i, p_{i+1}) 其間隙

$$p_{i+1} - p_i \geq N,$$

亦即質數序列的間隙長度沒有上界。我們給一個簡單的證明。考慮

$$M := N! = 2 \times \cdots \times (N-1) \times N.$$

令 p_i 爲小於或等於 $M + 1$ 的最大質數。注意:

$$M + 2,\ M + 3,\ \cdots,\ M + N + 1, \quad M + N \text{ 都不爲質數。}$$

事實上, 任何 j, $2 \leq j \leq N$, 都是 M 的因數。因此下一個質數 $p_{i+1} \geq M + N + 1$。由 $p_{i+1} \geq M + N + 1$ 及 $p_i \leq M + 1$ 我們導出 $p_{i+1} - p_i \geq M + N + 1 - M - 1 = N$。得證

儘管這證明實在很短, 但在很多情況, 這個證明並未建構出大間隙的最小案例。

例: 對 $1 \leq j \leq 33$, $1327 + j$ 不爲質數, 因此我們看到長度至少爲 34 的間隙; 但注意

$$34! \approx 2.95 \times 10^{38}$$

因此, 相較於上述證明所構造的 34!, 發端於 1327 而長度爲 34 的間隙早很多出現。

例: 對 $p_i = 31397$ 我們有 $p_{i+1} - p_i = 72$, 但

$$72! \approx 6.12 \times 10^{103}.$$

見 https://en.wikipedia.org/wiki/Prime_gap 亦參見 [13], page 10。

備註:「質數序列中的間隙長度無上界」的另一個證明：
設任何間隙的長度都不大於 N, 亦即任意長度爲 N 的區間內都至少存在一個質數, 則對任意 $x \in \mathbb{R}$, 都有 $\pi(x) > x/N$。但在 §7 我們將得知：存在常數 B, 使 $\pi(x) < Bx/(\log(x))$ (當 $B = 3$ 時很容易證明)。因此, 當 $B/(\log(x)) > N$ 時, 我們導出矛盾。

我們想知道會出現什麼間隙。任意正整數都可以是某間隙的長度嗎? (這是個簡單的問題, 我們將看到某些部分的答案非常容易。)

備註: 不存在質數 p 及 q 使得 $q - p = 7$。

證明: 若 p 和 q 都爲奇數, 則它們的差是偶數, 因此不等於7。而當 $p = 2$, 數 $q := 2 + 7 = 9$ 不是質數。 得證

對長度爲奇數之情況的討論見 (10.3)。並請參閱 (9.5) 對長度爲偶數之情況的討論。

4.2. 如果我們足夠了解間隙長度, 也許我們可以解決：

猜想 (Legendre, 1798): 對任意 $n \in \mathbb{N}$ 存在質數 p 使得

$$n^2 < p < (n+1)^2. \quad (?)$$

見 [26]; 見 http://arxiv.org/pdf/1201.1787v3.pdf.

4.3. 孿生質數. 我們知道 (1.3) (1) 的答案嗎? 我們已得知許多對孿生質數, 預期有無限多對, 見 (9.4)。我們已得知數值很大的孿生質數對, 如 [5] 的前幾行所述。啟發式方法極具說服力, 能提供我們漸近估計。而每當孿生質數在一定範圍內的確切數量可實際計算, 我們總會發現啟發式預測的精確度極高。因此, 我們堅信有無限多對孿生質數。但是這個問題尚未解決, 我覺得我們基本上不了解這個問題背後的結構。

可用兩種方式推廣孿生質數的概念。或者我們可以研究相距更遠的質數對 (這可以通過兩種方式來達成：考慮相繼的質數, 或考慮任意兩質數之間的可能差異), 或者, 對給定的間隙長度, 我們可以探討更長串的相繼質數鏈。在所有這些情況, 我們獲得有趣的問題、很多部分結果和有趣的期望, 但其中沒有一個得到解決。

4.4. 質數三聯體. (1.3) (3) 的答案。我們證明：$\{3, 5, 7\}$ 是唯一的質數三聯體。

證明: 設 $\{p, p+2, p+4\}$ 爲 3 質數三聯體。我們有 $p = 3i$, 或 $p = 3i+1$ 或 $p = 3i+2$.

若 $p = 3i$, 我們得到序列 $\{3, 5, 7\}$.

若 $p = 3i + 1$, 則 $p + 2$ 被 3 整除, 因此 $p + 2 = 3$, 亦即 $p = 1$, 但這不是質數。

若 $p = 3i + 2$, 則 $p + 4$ 被 3 整除, 因此 $p = -1$, 亦爲矛盾。 QED

我們看到「質數三聯體」的概念不是很有意思, 忘掉它吧, 我們有個更好的想法：

定義: 一組質數 $\{p, q, r\}$ 被稱爲質數三元組若且唯若「$q = p + 2$ 且 $r = q + 4$」, (例如 $\{5, 7, 11\}, \cdots, \{41, 43, 47\}, \cdots, \{857, 859, 863\}, \cdots$), 或「$q = p + 4$ 且 $r = q + 2$」, (例如 $\{7, 11, 13\}, \ldots, \{613, 617, 619\}, \ldots$)。

你可以很容易地找到許多質數三元組。
見 https://en.wikipedia.org/wiki/Prime_triplet

期望: 質數三元組的數量是無限的 (?) 這個問題還沒有答案。
參見 https://en.wikipedia.org/wiki/Prime_triplet
及 http://primes.utm.edu/glossary/xpage/PrimeTriple.html

我們可以更進一步, 考慮質數四元組：它們是一串相繼的質數

$$\{p = p_i, p_{i+1}, p_{i+2}, p_{i+3} = p + 8\}.$$

我們預計存在無限多個質數四元組。長度爲四的質數星座 (質數四元組) 符合單一模式 $(p, p + 2, p + 6, p + 8)$。(例子：(5, 7, 11, 13), (11, 13, 17, 19)。)

如果長度爲五或六, 我們有模式 $(p, p + 2, p + 6, p + 8, p + 12)$, $(p, p + 4, p + 6, p + 10, p + 12)$ 及 $(p, p + 4, p + 6, p + 10, p + 12, p + 16)$。合格的質數星座預計有無限多組。這些問題都尚未解決。見 http://primes.utm.edu/glossary/xpage/Quadruple.html 及 http://primes.utm.edu/glossary/xpage/PrimeConstellation.html

4.5. 是否存在一個計算第 i 個質數 p_i 的公式?遺憾的是, 這問題的表述不夠精準。我們對這樣的公式有什麼期望? 若已得知所有的質數, 則下例證明這樣的公式存在。

4.6. 例: 存在一個具有下述性質的 $\alpha \in \mathbb{R}$：對第 n 個質數 p_n, $n \geq 2$, 有

$$p_n = \lfloor 10^{1+\cdots+n} \cdot \alpha \rfloor - 10^n \cdot \lfloor 10^{1+\cdots+(n-1)} \cdot \alpha \rfloor;$$

其中, 約定符號：對 $\beta \in \mathbb{R}$, $\lfloor \beta \rfloor$ 表示小於或等於 β 的最大整數：

$$\lfloor \beta \rfloor = m \in \mathbb{Z} \Leftrightarrow m \leq \beta < m + 1.$$

事實上, 如此的 $\alpha \in R$ 存在：

$$\alpha = 0.2030050007000110000 13 \cdots = \sum_{n=1}^{\infty} p_n \times 10^{-f(n)}$$

其中 $f(n) = 1+1+2+\cdots+n-$(p_n在十進制的位數)。我們用到 $p_n < 10^n$ (這可以很容易地看出來)。很明顯的是, 上面的公式確實可以爲每個 i 給出 p_i。

這有用嗎? 爲了得知 α, 你需要所有質數的精確訊息: 精確知道 $p_1, \ldots, p_n$, 可以計算 p_n; 這不太讓人驚訝: 如果你已得知所有質數, 就可以很容易地找到給出所有質數的公式。見 http://primes.utm.edu/glossary/xpage/FormulasForPrimes.html. 而 [43] 提出一個問題: 一般公式和好的公式之間有什麼區別? 另請參閱 [20]。

4.7. 例: Euler證明: 當 $0 \le i \le 39$ 時, 將 $T = i$ 代入 $T^2 + T + 41$ 會得到質數。是否存在一個「帶入任意整數都會得到質數的多項式」?

Matiyasevich 在 1971 年證明: 存在一個多項式, 正整數的取值皆爲質數。隨後, 滿足該性質的 25 次 26 元多項式被明確建構出來, 見 [21]。

這有用嗎? 是的, 從抽象的角度來看。這個定理在邏輯上非常重要。但我們能用這種方式輕鬆地計算質數嗎? 事實上, 以這種方式計算質數很困難。而且, 使用這個方法, 我不知道如何決定一個給定的數字是否爲質數。

見 http://primes.utm.edu/glossary/xpage/MatijasevicPoly.html.

4.8. 現代技術和網際網路允許我們確認小於 10^{12} 的質數,
參見 http://primes.utm.edu/nthprime/. 例如 $p_{100} = 541$, $p_{500} = 3,571$,
$p_{10,000} = 104,729$, $p_{1,000,000} = 15,485,863$, $p_{100,000,000} = 2,038,074,743$,
$p_{100,000,000,000} = 2,760,727,302,517$, $\cdots$ 這有趣嗎? 在該網站上, 你還可以爲任意 $x < 3 \cdot 10^{13}$ 計算 $\pi(x)$。

4.9. 是否存在 2013 位數的質數? 要找這樣一個質數, 有沒有我們可供參考的表格? 沒有, 當然沒有: 小於 10^{2012} 的質數數目大約是 10^{874}; 而我們認爲宇宙中基本粒子的數量約爲 10^{78}, 因此不能製作這樣的表格。

那麼, 我們如何回答這個問題呢? 在 (0.1), 我們以函數 $\pi : \mathbb{R} \to \mathbb{Z}$ 計算質數的數量; 而在 §7 中, 我們將證明 $\pi(10^{2012}) < \pi(10^{2013})$ (基於簡單的想法, 沒有使用深奧的定理), 從而斷定: 確實存在一個 2013 位數的質數 (然而我們沒有給出一個精確的例子, 我們只是證明其存在)。參見 (7.4), (7.8)。

4.10. Catalan **猜想**. 考慮

$$A^a + 1 = D^d, \quad A, D > 1,\ a, d \ge 2,\ A, D, a, d \in \mathbb{Z}.$$

Eugène Charles Catalan 在 1844 年提出猜想: 對 $A, D > 1$, $a, d \ge 2$, $A, D, a, d \in \mathbb{Z}$, $8 + 1 = 9$ 是這個方程的唯一解。事實上, 對較小的整數做計算後, 這猜想看似合理; 當你做完

計算時, 可能仍未找到反例。Tijdeman 在 1976 年證明此方程式的解有上界; 然而, 由於上界過大, 約爲 $\exp(\exp(\exp(\exp(730))))$ (其中我們使用符號 $\exp(a) := e^a$), 用電腦求解仍不可行。這個上界已獲改善, 但直接的計算仍遙不可及。

我們曾以爲這個問題對我們來說太過困難。然而其實現有的代數方法即足以解決這個問題; 事實上, $8 + 1 = 9$ 的確是唯一解, Preda Mihăilescu 在 2004 年證明 Catalan 猜想是對的; 見 [29]。他沒用大電腦, 只用純粹的思維和"容易"的理論; 對我們中的一些人來說, 這是個驚喜。參見 `https://en.wikipedia.org/wiki/Catalan%27s_conjecture`.

§5. 費馬(質) 數

考慮正整數

$$F_i = 2^{2^i} + 1, \qquad i \in \mathbb{Z}, i \geq 0,$$

稱這些整數爲費馬數 (Fermat number)。費馬 (Pierre de Fermat) 想知道這些數是否都是質數。我們發現

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$$

的確是質數, 但 Euler 在 1732 年證明

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417;$$

因此 F_5 不是質數。參見 (12.7)。

爲發現新的費馬質數, 衆人已從事了很多的研究和大量的計算搜索。
請見 `https://en.wikipedia.org/wiki/Fermat_number`.

目前, 我們不知道任何 $i > 4$ 的費馬質數。而對許多 i 值, 我們已知 F_i 不是質數。

5.1. 習題. 證明: (1) 對任意 $i > 0$, 我們有 $F_i = F_0 \times \cdots \times F_{i-1} + 2$. (2) 對任意 $0 < i < j$ 我們有 $\gcd(F_i, F_j) = 1$. (3) 令 P_i 爲 F_i 最小的因數。證明 $\{P_i \mid i \in \mathbb{Z} > 0\}$ 是無限集合。
結論: 所有質數組成無限集合。(對此我們給過另一個證明 (3.1))。

5.2. 習題. 假設 $2^m + 1$ 是一個質數, 則存在 i 使得 $m = 2^i$。
提示: 對於奇數 $a \geq 3$, 使用等式 $Y^a+1 = (\sum_{j=0}^{a-1}(-1)^j Y^j)(Y+1)$ [考慮 $2^m+1 = (2^b)^a+1$, 其中 $m = ba$ 有一個大於 1 的奇數因數, 判斷它們是否爲質數, 並不是非常有趣的問題 $\cdots$]

5.3. 建構正多角形. 始自古代希臘的數學, 人們就知道如何用直尺和圓規建構出正三角形和正五角形, 也知道如何二等分角。若 $n \in \mathbb{Z}$, $n > 3$, 什麼正 n-多角形可以用直尺及圓規建構? 這

個問題懸宕數世紀之久。在你繼續閱讀之前, 請仔細思索一下：這是一個幾何問題? 還是在另一個數學分支中有其自然的一席之地?

1796 年 3 月 29 日 (早上躺在床上, 18歲), 高斯證明：可以用直尺和圓規建造正 17 角形。後來他在 [11] 第七章發表了下述結果：

定理 (**高斯**, 1796 **年**). *直尺和圓規可以構造一個正 n-多角形若且唯若 $n \geq 3$ 可寫爲*

$$n = 2^\alpha \times P_1 \times \cdots \times P_t, \text{ 其中 } \alpha \in \mathbb{Z},\ \alpha \geq 0 \text{ 且 } P_1 < \cdots < P_t \text{ 是相異的費馬質數。}$$

討論. 我們不知道高斯是否對這個結果確實給出過證明; 他從未發表過任何證明。$n = 17$ 的情況在 [11] 中經由直接計算得到證明 (並明確給出了一個正 17-角形的邊長)。Pierre Wantzel 於 1837 年發表了這個定理的完整證明。

現代版本的證明可藉由 Galois 理論得到; 但高斯的時代還不知道 Galois 理論。我很想知道高斯究竟有什麼想法。他是否預見了 Galois 理論的這種意涵? (這裡 Galois 群是可交換的 (abelian)。) 他是否幾乎要得到這個結果 (譬如在可交換的情況下), 卻沒有進一步發展他的想法? 也許我們永遠無法斷定。這些是有趣的歷史資料和問題。

我們看到這個問題 (用尺和圓規來構造正 n-角形) 其實是數論的問題 (哪些費馬數是質數? 尚未解決), 而不是幾何問題。

關於費馬數的已知因數分解狀況, 見 `http://www.prothsearch.com/fermat.html`. 你還可以找到下述訊息：對 $i > 4$ 沒有已知的費馬質數 F_i, 已知 269 個費馬數爲合成數, $F_{2543548}$ 不是質數, 等等。

§6. Mersenne (質) 數

現介紹 Mersenne 整數：

$$M_n := 2^n - 1.$$

哪些這類整數是質數?

6.1. 習題. M_n 是質數 $\Rightarrow$ n 是質數。
提示. 對 $a, b \in \mathbb{Z}$, $a, b \geq 2$, 給出 $Y^{ab} - 1$ 的分解因式。

6.2. 然而, 反命題是不正確的：11 是整數, 但是 23 整除 M_{11}。事實上：

$$M_{11} = 2^{11} - 1 = 2047 = 23 \times 89.$$

6.3. 習題. 假設 p 和 $q = 2p + 1$ 是質數。(在這種情況下, 質數 p 稱爲 Sophie Germain 質數, 參見 (9.8)。) 證明在這種情況下, 若 p 形如 $4k + 3$, $k \in \mathbb{N}$, 則 q 整除 M_p。

6.4. 習題. 219, 975, 517 是質數; 它們是 Sophie Germain 質數嗎?
提示: Sophie Germain 質數除以六的餘數是多少?

目前我們知道 48 個 Mersenne 質數, 見 `https://en.wikipedia.org/wiki/Mersenne_prime` 及 `http://primes.utm.edu/largest.html#largest`.

這是否提供了證據, 讓你能判斷 Mersenne 質數個數爲有限或無限? 例如 : 正好 20 個 Mersenne 質數 $M_i < 10^{2916}$; `http://primes.utm.edu/mersenne/` 給出這個區間內 Mersenne 質數密度的估計。(這是否說服你 : Mersenne 質數很少?)

6.5. 對 Mersenne 數的興趣源自一個極爲經典的話題 :
定義 (**上古希臘**). 如果 $N \in \mathbb{N}$ 之正因子的和等於 $2N$, 亦即小於 N 的因子和等於 N, 則稱 N 爲完美數 (perfect number)。

$$N \text{是完美數} \iff \sum_{1\le d<N, d|N} d = N.$$

我們看到 : $6 = 2 \cdot M_2$ 是完美數, $28 = 2^2 \cdot M_3$ 是完美的, $496 = 24 \cdot M_5$ 是完美的; 可以繼續下去嗎? 試證 $2^{10} \cdot M_{11}$ 不是完美的。

6.6. 定理 (Euclid **第九卷** Proposition 36 **及** Euler). $N = 2m$ 是完美數若且唯若存在質數 p 使得

$$M_p \text{是質數且} N = 2^{p-1} \cdot (2^p - 1) = 2^{p-1} \cdot M_p.$$

例如 : $p = 2, 3, 5, 7, 13, 17, \ldots$。警告 : 該定理僅處理偶數的完美數。

以下僅證明其中一個方向的蘊含關係 :

$$M_p \text{是質數} \Rightarrow N := 2^{p-1} \cdot M_p \text{ 是完美的。}$$

證明: 定義 $\sigma(N)$ 爲 N 的正因子 d 之和, $1 \le d \le N$。檢查 :

$$\sigma(2^{p-1} \cdot M_p) = \sigma(2^{p-1}) \cdot \sigma(M_p) = (1+2+4+\cdots+2^{p-1}) \cdot (1+M_p) = (2^p-1) \cdot 2^p = 2N. \quad \text{得證}$$

6.7. 習題: 證明這個定理的另一方向的蘊含關係。

6.8. 2013 年 1 月 25 日, 中央密蘇里州立大學的 Curtis Cooper 發現新的 Mersenne 質數

$$2^{57,885,161} - 1.$$

這是一個驚人的結果, 而多台私人電腦形成的架構也令人印象深刻。但是, 我們是否因此而『更有智慧』? 這個數有 17,425,170 位數,
參見 http://www.isthe.com/chongo/tech/math/prime/mersenne.html.

6.9. 習題: 1603 年, Pietro Cataldi 聲稱 $2^{29}-1$ 和 $2^{31}-1$ 是質數; 你能判斷他的正確程度嗎?

我們看到 : 對 Mersenne 質數的興趣源於對完美數字的探詢。而我們當前對這個主題的興趣, 主要聚焦於因數分解程式效率的觀察。若能在此找到基礎結構, 將會是個偉大的成就。

關於 Mersenne 的生平及他對 (我們現在所稱的) Mersenne 質數的追尋,
見 http://primes.utm.edu/glossary/page.php?sort=MersennesConjecture.

6.10. Mersenne **質數在哪裡**? 在 [5] 第 15 頁的圖 1 可看到 : 就已知的 Mersenne 質數而言, $\log_2(\log_2($第 n 個 Mersenne 質數$))$ 與 n 的關係非常接近線性。我們又在不規則行爲裡看到『規律性』。參見 http://primes.utm.edu/mersenne/heuristic.html 及 http://primes.utm.edu/notes/faq/NextMersenne.html.

6.11. 習題: Mersenne 認爲 M_{67} 是一個質數。他是對的嗎? 提示 : 使用科學計算器, 例如 http://web2.0calc.com/#及https://www.numberempire.com/factoringcalculator.php.

6.12. 習題: 數字 2536475896746352436487568 34 是一個完美的數字嗎? (就基礎結構來說, 你可能要先判斷 : 完美數字的最後一位數字可能是什麼? 用純思維來證明你的結果, 之後再完成習題。) 見 (12.8)。

我們已看到, 一個幾何問題 (構造正 n 角形) 引發了對費馬數的深入研究 (問題基本上仍未解), 而追尋偶數的完美數相當於尋找 Mersenne 質數 (而其最終結果基本上仍開放未決)。

§7. 質數定理 (The Prime Number Theorem) PNT

正如導論中所言, 我們希望對『函數』$\pi:\mathbb{R}\to\mathbb{Z}$ 進行了解。儘管高斯和 Legendre 提出了想法, 數學家公認他們的猜想難以證明, 直到 1852 年 Chebyshev 才證明了第一個相關結果, 其論述驚人地簡單但威力強大。其後, Hadamard 和 De la Vallée-Poussin 在 1896 年證明了這個深刻的定理。(以下, 請記住 $\log(x)$ 表示以 e 爲基底的對數, 見 (2.3)。)

7.1. 質數定理 (Chebyshev, Hadamard **及** De la Vallée-Poussin).

$$\pi(x) \sim \frac{x}{\log x},$$

亦即

$$\lim_{n\to\infty} \pi(x) \Big/ \frac{x}{\log x} = 1.$$

亦可陳述如下: $\forall E \in \mathbb{R}$, $E > 0$, $\exists N \in \mathbb{N}$ 使得:

$$x > N \Rightarrow (1-E)\frac{x}{\log x} < \pi(x) < (1+E)\frac{x}{\log x}$$

或 : 對任意實數 A, B, $0 < A < 1 < B$ 存在 $N \in \mathbb{N}$, 使得

$$A\frac{x}{\log x} < \pi(x) < B\frac{x}{\log x}, \quad \forall\ x > N.$$

7.2. 比較好的估計是

$$\pi(x) \sim \frac{x}{\log x - 1}.$$

參見 [34], 2.19。

回溯歷史, Chebyshev 首先證明: 對很大的 x, 我們有

$$\frac{92}{100} < \pi(x) \Big/ \Big(\frac{x}{\log x}\Big) < \frac{111}{100}.$$

參見 [6]。顯然, 這不足以證明極限存在, 遑論證明極限等於 1。但是這是一個突破。有關這個結果的簡單而基本的證明, 請參見 [44] 中的描述。40 多年後, 優美且深刻的質數定理 PNT 才被證明, 參見 [16, 17, 38, 39]。隨後, 又有很多新的證明。有些是『初等的』(雖然既不容易, 也不簡單)。這個引人入勝的故事和許多我們用過的參考文獻可見諸 [7]。

Sylvester 在 1882 年證明

$$0.95695 < \pi(x) \Big/ \Big(\frac{x}{\log x}\Big) < 1.04423, \quad x \gg 0.$$

Sylvester 用 Chebyshev 的方法來改進 Chebyshev 的結果

在文獻中, 我們發現了許多明示估計的版本(固定 A, B, N), 基本上比 PNT 弱, 但是非常有用。我們引用 (並將使用) 以下內容。

7.3. 定理 (**一個明示估計的版本**, **比** PNT **弱**)

$$\frac{x}{\log x} < \pi(x), \quad x > 17; \quad \pi(x) < \frac{5}{4}\frac{x}{\log x}, \quad x > 113.6.$$

(見 [34], Corollary 1 和 Corollary 2 (第 69 頁)。另見 https://en.wikipedia.org/wiki/Prime_number_theorem). 例如 :

$$x \geq 55 \Rightarrow \frac{x}{\log x + 2} < \pi(x) < \frac{x}{\log x - 4}.$$

7.4. 例: 因 $2013 < 8 \times 2012$, 我們有

$$\pi(10^{2012}) < \frac{5}{4}\frac{10^{2012}}{2012 \cdot \log x} < \frac{10^{2013}}{2013 \cdot \log x} < \pi(10^{2013}).$$

因此存在一個在十進制爲 2013 位數的質數。請注意, 我們證明了存在性, 從而回答了 (1.7), 但對這樣的質數, 我們並沒有舉出例子。

備註: 另一弱很多的版本 $x/(3\log(x)) < \pi(x) < 3x/(\log(x))$ (易於證明) 也能證明這結果。

7.5. PNT **的推論**. 所有質數所成的序列 $\{p_n \mid n \in \mathbb{N}\},\ p_i < p_{i+1}, \forall\, i$, 滿足

$$p_n \sim n \log n.$$

換言之: 對任意實數 $0 < C < 1 < D$, 存在 $N \in \mathbb{N}$ 使得

$$n \geq \mathbb{N} \Rightarrow C \cdot n \log n < p_n < D \cdot n \log n.$$

還有更精緻的版本 : $p_n \sim n(\log(n) + \log(\log(n)) - 1)$, 見 [34], 2.19.

我們有下述明示估計但較弱的版本 :

7.6. 另一較弱形式. 對 $n \geq 6$ 我們有:

$$\log n < \frac{p_n}{n} < \log n + \log(\log n).$$

見 https://en.wikipedia.org/wiki/Prime_number_theorem; 亦見 [34] 69 頁, Theorem 3 的 Corollary.

7.7. 例. 計算結果顯示

$$p_{100,000,000,000} = 2,760,727,302,517;$$

而對 $n = 100,000,000,000$ 我們有

$$n\log(n) \approx 2,532,843,602,293 \text{ 及 } \log(n) + \log(\log(n)) \approx 2,856,036,374,098$$

事實上

$$2,532,843,602,293 < 2,760,727,302,517 < 2,856,036,374,098,$$

我們看到, 靠純思維及很少的計算, 就得到誤差小於 5% 的下限, 及誤差小於 4% 的上限。

7.8. 應用. 選取 $n = 22 \times 10^{2007}$, 我們看到

$$\log(10^{2007}) \approx 4621.288281639 \text{ 且 } \log(n) = \log(22) + \log(10^{2007}) \approx 4622.630704319;$$

因此

$$1.01 \times 10^{2012} < n \log n < p_n.$$

另外, 我們有 $\log(\log n) \approx 8.439097441$; 因此

$$p_n < n(\log n + \log(\log n)) < 22 \times 10^{2007} \cdot (4622.63 + 8.44) \approx 101883.54 \times 10^{2007}$$
$$< 1.02 \times 10^{2012}.$$

結論:

$$10^{2012} + 10^{2010} < p_n < 10^{2012} + 2 \cdot 10^{2010}.$$

我們看到這個質數位於給定的區間內, 因此 $p_{22\times 10^{2007}}$ 正好有 2013 個十進制數字。但是, 我們並不知道這個質數的確切值。你能給出合理的猜測或估計嗎? 你能給出一個確切的下限嗎?

在給定的區間 $(10^{2012} + 10^{2010}, 10^{2012} + 2 \cdot 10^{2010})$ 內有多少個質數? 你能給出合理的猜測或估計? 你可以給出該數量的確切下界嗎? 但是我認爲很難 (抑或不可能?) 藉由抽象方法來計算確切的數量。由於數量似乎過大而無法精確計算, 似乎沒有方法可用以確定該區間內質數的確切數量 (我們真的很想知道嗎?)。

§8. 啓發式方法

"顯然, 在優雅的狀態下, 沒有人會把這些機率論證誤認爲嚴謹的數學。儘管如此, 當我們要對數論函數的『行爲』做有素養的猜測時, 它們非常有用。" 見 [1], 第 248 頁。

本節將討論『啟發式論證』, 另請參閱 `http://primes.utm.edu/glossary/xpage/Heuristic.html`. 這種『有素養的猜測』通常不能證明任何事情。但是, 我們將會看到, 它可以引導我們的直覺。我們也將會看到, 只要我們做了必要的繁瑣計算, 它就會帶來預期的結果, 而這些結果多次與事實極其吻合。因此, 它給了我們堅定的信念, 相信自己走在正軌上。請嘗試消化下面的這些想法。不過 (再次), 請注意, 你不能以這種方式證明任何事情。但仍請將這些直觀的方法應用於你感興趣的任何問題(我們將舉例說明)。

考慮下述聲明：

$$『數\ n \in \mathbb{N}\ 爲質數的機率等於\ \frac{1}{\log n}』。$$

這純屬無楮。『$n = 1000$ 是質數』的機率是零, 而『997 是質數』的機率等於 1。那麼這到底在說什麼呢? 然而, 事實顯示, 這種方法很有用。

基本上這方法有兩個優點。考慮 $n \in \mathbb{N}$ 及包含 n、長度爲 Δ 的正整數區間; 這個區間內的質數數量約爲 $\Delta/\log n$。我們在 §7 中看到, 該估計做得很精確, 可以給出質數數量的確切上下界 (不是猜測, 不涉及統計, 而是可以證明的具體結果)。藉此途徑, 我們逐步接近數學證明。

我們也可以使用這種 (可疑的) 方法來感知可能的答案。只要我們意識到這只是猜測 (我們意識到：這方法並不能證明什麼), 就並無不妥。這裡有一個例子 (Fermat 數)：

8.1. 費馬數 F_i 是質數的機會 (?) 等於 $1/\log(2^{2^i}) = (1/2^i)(1/\log 2)$。讓我們假設費馬數是『隨機選擇』的 (不管數字是什麼, 結果也不用很正確; 這些數字都是奇數, 所以有更大的『機會』是質數, 而且兩個不同的費馬數互質, 所以它們不完全『隨機』)。讓我們不要爲這些細節操心, 逕自將這些機會加總：

$$\sum_{i=1}^{\infty} \frac{1}{\log 2^{2^i}} = \frac{1}{\log 2} \sum_{i=1}^{\infty} \frac{1}{2^i} \le \frac{2}{\log 2}.$$

因此, 我們有合理的猜測：Fermat 質數的數量應該是有限的。

8.2. 這裡有一個例子, 提醒我們務必小心。讓我們來『證明』『有無限多個質數』(??)

『證明』如下：$2n$ 是質數的『機會』等於 $1/\log(2n)$ (?), 並且顯然總和 $\sum 1/\log(2n)$ 發散到 ∞ (最後的敘述是正確的, 就如 Euler 很久以前所證明)。

8.3. 習題: 對 Mersenne 數套用這種啟發式方法。雖然已知的 Mersenne 質數極少, 但我們堅信有無限多個 Mersenne 質數。我們可用啟發式方法, 預測下一個待發現的 Mersenne 質數大約在何處, 而每次這樣的預測結果都相當準確。

嘗試估計第 n 個 Mersenne 質數的位置, 並確認 (6.10)。
請參閱 `http://primes.utm.edu/mersenne/heuristic.html`.

8.4. 習題: 對孿生質數套用啟發式方法。這方法也對此暗示了最終的結果 (我們相信是正確的)。

這樣的方法已然完善。我們可以使用啟發式方法來預測某個上界之下的孿生質數對數量。一旦完成此純思維的過程, 簡單的計算就可預測該數量。接著可以嘗試計算實際的數量 (進行艱難且冗長的計算, 以獲得確切的數字)。在 10^{15} 以下, 預期值與實際值相差不到 $1/10^6$, 見

[5], Table 1. (在現實生活中, 或在法庭上, 這將立即被接受爲『證明』)。

8.5. 習題: 用啟發式方法說服自己, 應該有無限多個 Sophie Germain 質數; 見 (9.8)。

8.6. 習題: 使用啟發式方法說服自己, 應該有無限多組質數三元素。

8.7. 習題: 使用啟發式方法得到對 Polignac 猜想的感覺, 參見 (9.5) (1)。

只要我們仍堅持要求正確的事實及證明過的結果, 就應對本節提到的方法持保留態度。然而, 我們仍可使用這些方法來感受出尋找結果應採取的方向。

啟發式方法的討論可參見[5]。將 [5] 中許多表格與實際計算的數量相比較, 顯示這樣的方法以驚人的精確度給出預測。

8.8. 習題: 所有 $n \in \mathbb{N}$, 考慮形如 $p = n^2 + 1$ 的所有質數。這種質數的個數有限或無限? 如果對此問題套用啟發式方法, 你會期望什麼? 見 [5], 3.8。

§9. 一些未解問題 (open problems)

警告: 下面我們記錄一些未解的問題。它們看似很容易 (至少就其陳述來說); 然而, 許多數學家已努力攻堅而未果。你可以隨心所欲做一些計算 (但請注意, 龐大的電腦和複雜的演算法已投入研究, 但迄今仍未發現任何結論性證據)。如果你夠明智, 請不要把你的數學餘生用於解決這些問題。(但是, 如果你爲下述之任何問題提出證明或反例, 你將成爲頭版新聞。)

數學家似乎還沒有找到看待這些問題的正確角度, 也還沒有處理它們的決定性技術。通常一個全新的見解是需要的 (這是美麗的未解問題的優點)。

這裡有個例子 : Fermat's Last Theorem (費馬最後定理, 以下簡稱 FTL)

$$x, y, z, n \in \mathbb{Z}, \quad n \geq 3, \; x^n + y^n = z^n \overset{(??)}{\Rightarrow} xyz = 0.$$

大約在 1637 年被提出, 之後有很長一段時間是個『孤立的問題』(對 $n = 1$ 和 $n = 2$, 有無限多解。對 $n \geq 3$, 費馬聲稱已證明無正整數解)。在十九世紀, 一種新的方法 (ideal 理論) 看起來極具成效; 事實上, 它確實解決了一些情況 (太棒了, 它並引導出重要的新工具; 你看到一個問題如何觸發新的發展)。但是, 一般來說, 當時 FLT 仍是遙不可及。

晚近, 用大型電腦並沒有發現任何反例, 但解決了巨量 (但有限的) 特殊情況。

1985 年, Gerhard Frey 指出 : FLT 可能與另一個未解決的問題存在著關聯, 該問題即 Shimura-Taniyama-Weil 猜想, 簡記爲 STW, 涉及橢圓曲線。隨後 Ribet 證明 STW⇒ FLT。突如其來的, FLT 不再是一個孤立的問題, 而是某件公認屬實之事的必然結果。Andrew Wiles 從小就知道 FLT 問題, 而橢圓曲線和 STW 猜想正是他專業的核心。一旦這個聯繫成

立, Wiles 著手研究; 這兩個問題的解決方案是項偉大的勝利 (對 Wiles 而言, 也對純數學而言)。純粹的思維贏得了這場 350 年前開始的比賽, 電腦沒上陣 (除了處理文書和流通文稿)。

猜想或期望? 我們有時對某敘述套用『猜測』這個詞, 意指我們對它有堅定的想法, 但尚無任何它應屬實的證據。我個人使用這個詞是有限制的。如果沒有任何結構性的證據, 或無其他跡象顯示什麼樣的基層結構會蘊含結果, 但我們仍然堅信它是對的, 我傾向用『期望』這個詞。

對於下面所有的問題,『啟發式方法』將在期望的方向給出提示, 一如 §8 中所述。而抽象的方法、複雜的演算法、廣泛的電腦搜索和許多其他方法都已被使用。

9.1. 奇數完美數字. 關於完美數字的定義請見 6.5。我們對偶數的完美數字的問題有適當的了解 (但沒有明確的結論)。

問題: *是否存在一個奇數的完美數字*?

有大量的部分結果及關於這個問題的文獻。迄今未發現任何奇數的完美數字, 我們知道在某個大的上界之下不存在 (上界不斷上修)。目前已知, 若存在奇數的完美數字, 則該數在十進制至少爲 300 位數, 且必定有大於 10^{20} 的質因子; 這可能會讓你沒勇氣動手去找奇數的完美數字。請參閱 `http://mathworld.wolfram.com/OddPerfectNumber.html`.

期望: *沒有奇數的完美數字* (?)

爲什麼這是對的? 迄今尚未發現任何例子。但是我沒看到任何支持這種期望的結構或證據。進一步的參考資料, 請參閱 `http://primes.utm.edu/mersenne/`.

除了『數值證據』(迄今尚未發現許多計算數據), 我幾乎沒有看到這方面的證據。我也沒有看到任何啟發式的方法。數值證據是主觀的論證; 而已檢查過的有限數量的數, 占所有可能情況的 0%。

9.2. Goldbach **猜想**. 1762 年, Christian Goldbach 寫信給 Euler, 陳述了一個猜想。(順便一提, 據我所知, 這是有史以來第一次, 在這種含意下用『猜想』這個詞。)

期望: *每個偶數 $N = 2n \geq 4$ 都可寫成兩個質數的和* (?)
見 `https://en.wikipedia.org/wiki/Goldbach%27s_conjecture`.
這猜想已被證明對 4×10^{18} 以下的偶數都成立, 且這猜想通常被認爲是對的。但儘管已做了相當大的努力, 仍未證明此猜想。見 `http://en.wikipedia.org/wiki/Prime-number#Open-question`.

啟發式方法顯示: Goldbach 猜想應該成立 (但正如我們先前看到和爭論的, 這不是數學證明)。

循著歷史查閱論文很有意思, 你會看到『Goldbach 問題』和『Goldbach 猜想』兩個術

語不斷被轉換著使用, 如潮水一般。

9.3. 變體. 我們說質數 p 是一個 t-prime 若且唯若 $p-2$ 或 $p+2$ 是質數 (亦即 p 屬於某孿生質數對)。

期望 (**對** t-primes **的** Goldbach **猜想**): *每個夠大的偶數都是兩個 t-primes 的和。*

9.4. 孿生質數. 孿生質數是一對質數 $\{p, q\}$, $q = p + 2$。已得知很多例子。

期望: *有無數對的孿生質數* (?)

請參見 https://en.wikipedia.org/wiki/Twin_prime#First_Hardy.E2.80.93Littlewood_conjecture

計算孿生質數對時, 你會發現有時接續的質數對非常靠近 (不可能更靠近), 有時候則相距甚遠。令

$$\pi_2(x) = \#(\{p \mid p \le x, \text{ 且 } p \text{ 和 } p+2 \text{ 都是質數}\})。$$

$\pi_2(-)$ 函數似乎又是一個『不規則函數, 但在大尺度下表現很規則』的例子。事實上, 我們可以有較爲精確之期望如下述：

$$\pi_2(x) \overset{(?)}{\approx} 2 \times 0.66 \times \frac{x}{(\log x)^2}.$$

見 https://en.wikipedia.org/wiki/Twin_prime. 數值結果 (大量的計算) 與此非常吻合。例如：

$$\pi_2(10^{18}) = 808,675,888,577,436$$

而

$$2 \times 0.66 \times \frac{10^{18}}{(\log 10^{18})^2} \approx 768,418,024,862,131.$$

預測的數量是實際數量的 95%。

經由計算已找到很大的孿生質數：『2011 年 12 月 25 日, PrimeGrid 發現了創數值新高的孿生質數對 $37568016956852^{666669} \pm 1$。這些數字在十進制的位數爲 200700』。

關於孿生質數猜想的歷史見 http://arxiv.org/abs/1205.0774.

孿生質數的概念已以下述方式推廣了。

9.5. 質數序列的間隙.

(1) **期望**, Polignac **猜想**, 1849 **年**; (**見** [31, 32])：*對任意偶數 $m = 2n \in \mathbb{N}$, 都有無窮多對相鄰質數 (p_i, p_{i+1}) 具間隙 $p_{i+1} - p_i = m$* (?)

對於任何偶數 $m = 2n \geq 2$, 這既沒被證明也沒被反證。參見 https://en.wikipedia.org/wiki/Twin_prime.

(2) **期望**. 對任意偶數 $m = 2n \in \mathbb{N}$, 都有無窮多對質數 (p, q) 具間隙 $q - p = m$。

顯然, 若 9.5 (1) 成立, 則 9.5 (2) 也成立。

對於 Polignac 猜想的啟發式證據見諸 [5], 在其 Table 2, 對 $m = 210$ 及 $p < 10^9$, 考慮可能的質數對 $(p, p + 210)$; 啟發式方法預測其個數爲 10,960,950; 而精確計算得知個數爲 10,958,370; 預測偏差低於 0.03‰。這個例子顯示了啟發式預測的驚人精確度 (對於可以驗證的情況)。

備註. 我們僅需考慮的偶數長度的間隙; 關於奇數長度的間隙, 見 (10.3)。

9.6. 費馬質數的數目有限嗎? (回顧第 5 節。對 $i \in \mathbb{Z}$, $i \geq 0$, 令 $F_i := 2^{2^i} + 1$。)

期望. 費馬質數的個數爲有限。(?) 更多訊息請見 [22]。

9.7. Mersenne **質數的數目是否無界**? (回顧第 6 節。對 $n \in \mathbb{N}$, 令 $M_n = 2n - 1$。)
我們知道：若 M_n 是質數, 則 n 是質數。

期望. 有無限多個 Mersenne 質數。
我們的經驗及計算顯示：『大多數的 Mersenne 數是合成數』。但對下述問題我們尚無答案：

(**(9.7)之二**). 合成的 Mersenne 數有無限多個?

9.8. Sophie Germain **質數的數量是否無限**?
我們稱一個質數 p 爲 Sophie Germain 質數, 若且唯若 $q := 2p + 1$ 也是一個質數,
http://oeis.org/ 給出下列 Sophie Germain 質數：

> 2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293, 359, 419, 431, 443, 491, 509, 593, 641, 653, 659, 683, 719, 743, 761, 809, 911, 953, 1013, 1019, 1031, 1049, 1103, 1223, 1229, 1289, 1409, 1439, 1451, 1481, 1499, 1511, 1559, ・・・

還有更多例子：

$$\ldots, 137211941292195 \times 2^{171960} - 1, \ldots, 18543637900515 \times 2^{666667} - 1, \ldots.$$

期望. 有無限多個 Sophie Germain 質數?
小於 10^4 的 Sophie Germain 質數有 190 個; 小於 10^7 的 Sophie Germain 質數則有 56032 個。見 https://en.wikipedia.org/wiki/Sophie_Germain_prime 並請參見猜

想 (3.6) 和 [5] 中的 Table 6 (對 Sophie Germain 質數在某上界之下的數量可做啟發式的預測, 而在我們能夠檢查的情況, 預測的數量非常精確)。

Sophie Germain 和高斯曾以書信來往 (最初她取名爲 Monsieur Le Blanc (勒布朗先生)), 給高斯極爲深刻的印象。當指數爲上述類型之質數時, 她證明了 FLT。身爲一個女人, 她的數學貢獻未獲足夠的認可, 但高斯促使 Göttingen 頒發榮譽博士頭銜給她; 然而, 她尚未得知此事就過世了 (在她有可能得到這個榮譽之前)。

9.9. Collatz **問題**, **或稱** $3x+1$ **猜想**.
參見 (1.10)。我們定義一個函數 $C : \mathbb{N} \to \mathbb{N}$ 如下 :

$$C(2m) := m,\ C(2m+1) = 3(2m+1)+1;$$

亦即, 若 n 爲偶數, 則 $C(n) = n/2$, 而若 n 爲奇數, 則 $C(n) = 3n+1$。對 $a_1 \in \mathbb{N}$, 我們漸次得到序列 $\{a_1, \ldots, a_{i+1} := C(a_i), \ldots\}$, 名爲 Collatz 序列。例如, 若 $a_1 = 17$, 我們得到序列

$$17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, \ldots$$

我們觀察到, 這序列結束於

$$4 \to 2 \to 1 \to 4 \to 2 \to 1 \to 4 \cdots .$$

期望. 每個 Collatz 序列都以 $\{4, 2, 1, \ldots\}$ 結束。(?)

這問題尚未解決。我們似乎不明白用哪個機制得以探勘這個問題。

建議. 建構一些這樣的序列 (每次選擇不同的 a_1), 觀察令人費解的經驗 : 序列的確以一如預期的形式結束 (或者你是否試圖找到反例? 在這種情況, 您的起始數字最好超過 500 位數。)

對這個問題的討論和許多參考文獻見諸 J. C. Lagarias. The ultimate challenge: the $3x+1$ problem, AMS, 2010, 並參見 `http://www.math.lsa.umich.edu/~lagarias/` 另見 : `http://arxiv.org/pdf/math/0608208v6.pdf`, `http://www.math.grin.edu/~chamberl/papers/3x_survey_eng.pdf`, `https://en.wikipedia.org/wiki/Collatz_conjecture` 你也可以去 `https://www.nitrxgen.net/collatz_php`; 起步於某正整數 (十進制的位數最多爲 500), 我們可觀察 Collatz 序列。例如 : 從 27 開始。經過 111 步後, 我們看到 Collatz 序列的末尾 :

> 27, 82, 41, 124, 62, 31, 94, 47, 142, 71, 214, 107, 322, 161, 484, 242, 121, 364, 182, 91, 274, 137, 412, 206, 103, 310, 155, 466, 233, 700, 350, 175, 526, 263, 790, 395, 1186, 593, 1780, 890, 445, 1336, 668, 334, 167, 502, 251, 754,

377, 1132, 566, 283, 850, 425, 1276, 638, 319, 958, 479, 1438, 719, 2158, 1079, 3238, 1619, 4858, 2429, 7288, 3644, 1822, 911, 2734, 1367, 4102, 2051, 6154, 3077, 9232, 4616, 2308, 1154, 577, 1732, 866, 433, 1300, 650, 325, 976, 488, 244, 122, 61, 184, 92, 46, 23, 70, 35, 106, 53, 160, 80, 40, 20, 10, 5, 16, 8, 4, 2, 1

問題. 是否有公式, 對任意 $a_1 \in \mathbb{N}$, 能計算數字 1 首次出現前之 Collatz 序列的長度?

經驗顯示, 隨著 a_1 成長, 此長度上下跳動 (以相當不可預測的方式?)。

我們只提到了關於質數的一小部分猜想。我們應該討論其中最有趣的 (有很多重要意涵的) 黎曼猜想 (Riemann hypothesis)。遺憾的是, 這會把我們帶太遠。

9.10. 1912年, 國際數學家大會上, Landau 列舉了四個問題 : (1) Goldbach (9.2), (2) $n^2 < p < (n+1)^2$ (4.2), (3) 孿生質數 (9.4) 和 (4) 形如 $p = n^2 + 1$ (8.8) 的質數有無限多個。這些是當年未解決的 (舊的) 猜測, 但迄今滿意的答案或結果似乎仍遙不可及。見 [9]; 也請參閱 http://arxiv.org/pdf/1205.0774v1.pdf 的第 2 頁。

我應該再討論一些其他主題, 但這會使論文太長 : 關於 RSA 密碼學, 參見 [37] 和 https://en.wikipedia.org/wiki/RSA_(cryptosystem) 關於 ABC 猜想, 參看 https://en.wikipedia.org/wiki/Abc_conjecture, http://www.math.leidenuniv.nl/~desmit/abc/index.php?set=1, http://www.kurims.kyoto-u.ac.jp/~motizuki/top-english.html.

9.11. 結論. 我們回到第一節列出的 10 個問題。一些問題事實上很容易, 我希望這讓你感到驚訝。對一些問題, 我們感覺得出來答案應該是什麼 (但沒有確鑿的證據)。另一些問題已有發展好的理論提供答案 :

- 問題 1 和 2 有答案, 證明非常簡單。
- 問題 3, 4, 5, 6, 9 和 10 引導出難以解決的問題, 我們甚至不知道從何著手。然而, 『啟發式方法』能夠非常準確地爲我們提供應該期待的事物 (不規則的過程中發現令人驚嘆的『規律性』)。
- 因基層結構已然理解, 可以給出問題 7 和問題 8 的答案。

§10. 四個簡單的習題

經過這麼多容易及困難的問題, 這裡有三個練習 : 只要稍機靈點就可以解決的問題。

10.1. 習題1: 證明質數形如 $p \equiv 3 \pmod 4$ 的質數有無限多。
備註. 我們可以證明形如 $p \equiv 1 \pmod 4$ 的質數有無窮多個; 參見 (12.4)。

10.2. 習題2: 給定 $n \in \mathbb{N}$。證明存在 $a \in \mathbb{N}$, 使得等差數列

$$\{a, a+n, a+2n, \ldots\} = \{a + in \mid i \in \mathbb{N}\}$$

中有無限多個質數。
備註. Dirichlet 的 (深奧) 結果說：對任意 $a, n \in \mathbb{N}$, 若 $\gcd(a, n) = 1$, 則等差數列

$$\{a, a+n, a+2n, \ldots\} = \{a + in \mid i \in \mathbb{N}\}$$

中有無限多個質數。在上述的習題中, 你應該給出一個 (簡單且初步時) 特殊情況的證明, 而不要使用 Dirichlet 定理。

10.3. 習題3: 證明存在無窮多個 $N \in \mathbb{N}$, 使得 N 不是兩個質數的差。

10.4. 習題4: $7^{100} + 1 = 19^{66}$ 是對的嗎?

§11. 附錄 I：整數分解

我們收錄了 (幾乎) 每一本代數教科書都可以找到的結果。你可以嘗試獨自證明下面的敘述。

11.1. 備註. 大於 1 的整數 a 都可以被一個質數整除。

11.2. 定理. 大於 1 的整數 a 都可以分解爲質因數的乘積 $a = p_1 \times \cdots \times p_t$; 這些質因數是唯一的 (若不計排序)。

11.3. 警告. 我們對因式分解 (整數) 的唯一性習以爲常, 因而可能沒注意到這個性質是其他數系不具備的。例如, 考慮環 (作爲 C 的子集)

$$T := \mathbb{Z}[\sqrt{-5}] = \{x + y \cdot \alpha \mid x, y \in \mathbb{Z}\}, \quad \text{其中 } \alpha^2 = -5,$$

注意到：在 T 中,

$$2 \cdot 3 = 6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

很容易看出, 因數 $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5}) \in T$ 都是不可約的。我們也知道 T 中的單位元素是 $+1, -1 \in T$。因此我們得出這樣的結論：T 中的因式分解不是唯一的 (甚至在選定單位元素和排序後亦然)。

費馬聲稱 FLT 成立時, 很可能忽略了這個事實。19 世紀時, 基於這個錯誤的假設, 有人提出了 FLT 的『證明』(見 http://fermatslasttheorem.blogspot.nl/2006/01/lams-proposed-proof.html), 儘管 Kummer 已證明：在分圓體 (cyclotomic field) 的整數環中, 因式分解的唯一性不一定成立。

11.4. 引理 (除法及餘數). *給定 $n \in \mathbb{Z}$, $d \in \mathbb{N}$。存在 $q, r \in \mathbb{Z}$ 使得 $n = dq + r$.*

11.5. 引理: *給定 $a, b \in \mathbb{Z}$, 令 $d := \gcd(a, b)$, 則存在 $x, y \in \mathbb{Z}$ 使得 $xa + yb = d$。*

給出 11.4, 11.5 的證明, 並用它們證明定理 11.2。

§12. 附錄 II：整數關於模 n 同餘

本節描述一種衆所周知的基本方法。

12.1. 計算關於模 n 的同餘. 設給定 $n \in \mathbb{Z}$, $n > 1$。考慮一組符號所成的集合

$$\mathbb{Z}/n := \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

在這個集合中, 我們定義加法, 減法和乘法如下。首先, 我們令 $\overline{m} = \overline{m - in}$, 並定義映射

$$\mathbb{Z} \to \mathbb{Z}/n, \quad m \mapsto \overline{m}.$$

亦即, 若 $m \in \mathbb{Z}$, $m = dn + r$, 其中 $0 \le r = r(m) < n$ (除法的餘數), 則 $m \in \mathbb{Z}$ 映射到 $\overline{r(m)} = r$。我們令 $\overline{a + b} = \overline{a} + \overline{b}$ (『模 n 的加法』), 對 $\overline{ab}$ 和 $\overline{a} - \overline{b}$ 也有類似的定義。

用專業術語來說：$\mathbb{Z}/n$ 是一個環, 映射 $\mathbb{Z} \to \mathbb{Z}/n$ 是一個環同態 (ring-homomorphism), 以符號記爲 $\overline{m} \equiv m \bmod n$。

請區分 $(m(\mathrm{mod}\, n)) \in \mathbb{Z}/n$ (m 關於模 n 的同餘類) 及 $a \equiv b \pmod n$。

例子. 方程式 $T^2 = 47440033367001212$ 是否在 $\mathbb{Z}$ 中有解? [計算 mod 3]
或者考慮：$\mathbb{Z}$ 中某數平方的末位數字可能是什麼? [亦即 計算 mod 10.]

更且, 正如我們所見：對任意質數 p, 每個不爲零的 $\overline{a} \in \mathbb{Z}/p$ 都有一個反元素。你能證明這一點嗎? 用專業術語來說：$\mathbb{Z}/n$ 是一個體 (field), 若且唯若 n 是一個質數。

我們經常使用下述定理。

12.2. 定理 (中國剩餘定理): *若 $m, n \in \mathbb{Z}$ 且 $\gcd(m, n) = 1$, 則有一個自然的映射*

$$Z/(mn) \xrightarrow{\sim} Z/m \times Z/n;$$

此映射爲同構 (isomorphism), 是保持 $+$, $\times$, $-$ 三種運算的雙映 (bijective mapping)。

12.3. 命題 (**平方和**): 設 $A, B \in \mathbb{N}$, 且設 p 爲質數, p 整除 $A^2 + B^2$ 但不整除 A (因此 p 不整除 B), 則

$$p \not\equiv 3 (\mathrm{mod}\, 4).$$

證明時, 你可能會想用乘法群 $(F_p)^* := F_p - \{0\}$ 的群結構。

備註. 形如 $p \equiv 3 \pmod 4$ 的質數有無限多個。參見 10.1。

12.4. 推論: 有無限多個質數 p 形如 $p \equiv 1 \pmod 4$。

證明: (我們提出一個 Euclid 證明的變體, 參見 (3.1)) 假設 $P_1, \ldots, P_t$ 是奇數質數且 $t > 0$。我們宣稱：存在質數 P 使得

$$P \equiv 1 (\mathrm{mod}\, 4) \text{ 且 } P \notin \{P_1, \ldots, P_t\}.$$

若然, 推論得證。事實上, 取

$$M := (P_1 \times \cdots \times P_t)^2 + 4.$$

請注意 M 是奇數。從 (12.3) 我們得出結論：每個整除 M 的質數都滿足 $P \equiv 1 \pmod 4$。若 $P \in \{P_1, \ldots, P_t\}$, 則可斷定 P 整除 $M - (P_1 \times \cdots \times P_t)^2 = 4$, 此爲矛盾。因此 $P \notin \{P_1, \ldots, P_t\}$。我們也順道建構了一個新的質數 $P \equiv 1 \pmod 4$。 得證

12.5. 備註: 由 (12.3) 可知, 形如 $p \equiv 3 \pmod 4$ 的任何質數都不是 $\mathbb{Z}$ 中的平方和。相反地, 2 和形如 $p \equiv 1 \pmod 4$ 的質數都可以寫成平方和。

12.6. 備註: 將滿足 $p \equiv 1 \pmod 4$ 及 $p \leq x$ 的質數數量記爲 $\pi_{4,1}(x)$; 類似地, 將滿足 $p \equiv 3 \pmod 4$ 及 $p \leq x$ 的質數數量記爲 $\pi_{4,3}(x)$。若試著爲小的整數 x 計算這兩個數量, 你將注意到這兩個數十分接近。(哪一個看起來更大?) 的確, 漸近地, 當 $x \to \infty$, 它們是相等的：

$$\lim_{x \to \infty} \frac{\pi_{4,1}(x)}{\pi_{4,3}(x)} = 1.$$

這可由更一般的 Chebotarev 的密度定理得到;
參見 `http://en.wikipedia.org/wiki/Chebotarev%27s_density_theorem`

1835 年, Chebyshev 在給 Fuss 的一封信中寫道：對於每一個 x, 似乎 $\pi_{4,3}(x) > \pi_{4,1}(x)$。現在這敘述被稱爲『Chebyshev 的偏見』。它開啟了一段引人入勝的歷史, 並獲致優美的結果。參見 `http://arxiv.org/pdf/1210.6946v1.pdf`.

事實上, 很久之後, Littlewood 於 1914 年證明：當 $x \to \infty$, $\pi_{4,3}(x) - \pi_{4,1}(x)$ 的正負號變換無限多次。參見 [27]。更精確的結果見諸 [35]。[14] 是篇關於這個迷人主題的優美論文, 證明 Chebyshev 幾乎是正確的：對於『許多』x 值, 我們有 $\pi_{4,3}(x) > \pi_{4,1}(x)$。

一個『容易』的問題可以引導出優美的研究, 一個想當然爾的問題可以引導出深刻的結果 (數學中經常出現這種情況)。我們也看到, 有限的計算量 (即使如 Chebyshev 這般偉大的數學家) 可能會導致錯誤的感知。

12.7. 備註: 計算模 n 的一個例子。我們證明 641 整除 F_5。我們看到

$$641 = 640 + 1 = 5 \cdot 2^7 + 1 = 625 + 16 = 5^4 + 2^4.$$

因此 $5 \cdot 2^7 \equiv -1 (\mathrm{mod}\, 641)$, 故而 $5^4 \cdot 2^{4\times 7} \equiv +1 (\mathrm{mod}\, 641)$; 所以

$$-2^4 \cdot 2^{28} \equiv 5^4 \cdot 2^{28} \equiv +1 (\mathrm{mod}\, 641);$$

因此 $F_5 \equiv 0 \pmod{641}$.

12.8. 習題:

(1) 證明：2^n 在十進制的最後一位數字必爲 2, 4, 6 或 8。

(2) 證明：Mersenne 質數在十進制的最後一位數是 1, 3 或 7; 證明這些情況確實都會發生。

(3) 證明：一個偶數的完美數在十進制的最後一位數字是 6 或 8。

參考文獻

1. E. Bach and J. Shallit, Algorithmic number theory. Vol. 1. Efficient algorithms, Foundations of Computing Series. MIT Press, Cambridge, MA, 1996.
2. A. H. Beiler, Recreations in the theory of numbers: The queen of mathematics entertains, Dover Publ., pocket, 1964.
3. E. T. Bell, Men of mathematics, Simon and Schuster. 1937.
4. D. M. Burton, Elementary number theory, Allyn and Bacon, 1980.
5. C. Caldwell, An amazing prime heuristic, `http://www.utm.edu/staff/caldwell/preprints/Heuristics.pdf`.
6. P. Chebyshev, Mémoire sur les nombres premiers. J. de Math. Pures Appl., 17 (1852), 366-390. Also in Mémoires présentésál' Académie Impériale des sciences de St. - Pétersbourg par divers savants 7 (1854), 15-33. Also in Oeuvres 1 (1899), 49-70.
7. H. Diamond, Elementary methods in the study of the distribution of prime numbers, Bulletin American Mathematical Society, 7 (1982), 553-589.
8. Apostolos Doxiades, Uncle Petros and Goldbach's conjecture: a novel of mathematical obsession. Originally in Greek: O Theios Petros kai i Eikasia tou Goldbach (1992). 參見 `https://en.wikipedia.org/wiki/Apostolos_Doxiadis`, `http://www.ams.org/notices/200010/rev-jackson.pdf`.
9. P. Erdös and J. Surányi, Topics in the Theory of Numbers, Springer, 2003.
10. A. Fröhlich and M. J. Taylor, Algebraic number theory, Cambridge Std. Advanc. Math. 27, Cambridge Univ. Press, 1991.

11. C. F. Gauss, Disquisitiones Arithmeticae, Written in 1798, published in 1801.
12. C. Gauss, Letter to Encke, 24 Dec. 1849, Werke, vol. 2, Kng. Ges. Wiss., Göttingen, 1863, 444-447.
13. A. Granville , Harald Cramér and the distribution of prime numbers, Scandinavian Actuarial Journal 1 (1995), 12-28. http://www.dms.umontreal.ca/~andrew/PDF/cramer.pdf
14. A. Granville and G. Martin , Prime number races, American Mathematical Monthly 113 (2006), 1-33.
15. R. K. Guy, Unsolved problems in number theory, Springer, 3rd Edition 2004.
16. J. Hadamard, Étude sur les propriétés des fonctions entières et en particulier d'une fonction considérée par Riemann, J. de Math. Pures Appl., 9 (1893), 171-215; reprinted in Oeuvres de Jacques Hadamard, C.N.R.S., Paris, 1968, vol. 1, 103-147.
17. J. Hadamard, Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques, Bull. Soc. Math. France, 24 (1896), 199-220; reprinted in Oeuvres, vol. 1, 189-210.
18. M. Haddon, The curious incident of the dog in the night-time, Jonathan Cape (UK) Doubleday (US), 2003. https://en.wikipedia.org/wiki/The_Curious_Incident_of_the_Dog_in_the_Night-Time.
19. G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Oxford, Claren- don Press, fourth edition, 1975.
20. J. Jones, Formula for the Nth prime number, Canad. Math. Bull., 18 (1975), 433-434.
21. J. Jones, D. Sato, H. Wada and D. Wiens, Diophantine representation of the set of prime numbers, Amer. Math. Monthly, 83 (1976), 449-464.
22. M. Krízek, F. Luca and L. Somer, 17 Lectures on Fermat numbers from number theory to geometry, CMS Books in Mathematics Springer, New York 2002.
23. S. Lang, Algebraic number theory, Graduate Texts in Mathematics, Vol. 110, Springer, 1986.
24. S. Lang, Algebra. Graduate Texts in Mathematics, Vol. 211. Springer, 2002.
25. D. Leavitt, The Indian Clerk. Bloomsbury, 2007.
26. A.-M. Legendre, Essai sur la théorie des Nombres, Duprat, Paris, 1798.
27. J. Littlewood, Sur la distribution des nombres premiers, Comptes Rendus, 158 (1914), 1869-1872.
28. Yuri I. Manin, Good proofs are proofs that make us wiser, Interview by Martin Aigner and Vasco A. Schmidt. The Berlin Intelligencer, 1998, 16-19.
29. P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture, Journ. Reine angew. Math., 572 (2004), 167-195.
30. D. Musielak, Sophie's diary: A historical fiction, AuthorHouse, 2004.
31. A. de Polignac, Six propositions arithmologiques déduites de crible d'Eŕatosthène. Nouv. Ann. Math., 8 (1849), 423-429.
32. A. de Polignac, Recherches nouvelles sur les nombres premiers, Comptes Rendus Paris, 29 (1849), 397-401 and 738-739.
33. H. Riesel, Prime numbers and computer methods for factorization, Progress Math. 57, Birkhäuser, 1985.

34. J. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math., 6 (1962), 64-94.
35. M . Rubinstein and P. Sarnak, Chebyshev's bias, Experiment. Math., 3 (1994), 173-197.
36. D. Shanks, Solved and unsolved problems in number theory, Chelsea Publ. Cy., 1978.
37. S. Singh, The code book: the evolution of secrecy from Mary, Queen of Scots to quantum cryptography, Simon Singh Doubleday Books, 1999.
38. C. de la Vallée Poussin, Recherches analytiques sur la théorie des nombres premiers, Ann. Soc. Sci. Bruxelles, 20 (1896), 183-256.
39. C. de la Vallée Poussin, Sur la fonction $\zeta(s)$ de Riemann et le nombre des nombres premiers inférieurs à une limite donnée. Memoires Couronnés de l'Acad. Roy des Sciences, Belgique 59 (1899-1900); reprinted in Colloque sur la Théorie des Nombres (Bruxelles, 1955), Thone, Liège, 1956, 9-66.
40. P. Vojta, Diophantine approximations and value distribution theory, Lect. Notes Math. 1239, Springer-Verlag, New York, 1987.
41. A. Weil, Number theory, an approach through history, from Hammurapi to Legendre, Birkhäuser, 1984.
42. E. Weiss, Algebraic number theory, Mc-Graw-Hill Cy, 1963.
43. H. Wilf, What is an answer? Amer. Math. Monthly, 89 (1982), 289-292.
44. D. Zagier, The first 50 milion prime numbers. `http://sage.math.washington.edu/edu/2007/simuw07/misc/zagier-the-first-50-million-prime-numbers.pdf`. Published in The Mathematical Intelligencer, Vol. 0, August 1977.

2017 全國技專院校「文以載數創作獎」作品選集

圓周率．情緣　文／陳映潔

是什麼
使我們繞著那亙古的圓心旋轉
命運安排彼此邂逅
小數點前那數字
是我今生許你的
三番回眸 三千繾綣
而小數點後
是你承諾我的無限
將在一個又一個的來生中實現
直到我們的依戀畫出完美的圓
然後驚喜發現
竟回到了當初 刻骨銘心的原點

—本文作者就讀文藻外語大學德國語文科—

§13. 一些數學家

我們列舉上文提到的一些數學家

(300 BC)	Euclid of Alexandria
(1552∼1626)	Pietro Antonio Cataldi
(1588∼1648)	Marin Mersenne
(1601 or 1607/8∼1665)	Pierre de Fermat
(1690∼1764)	Christian Goldbach
(1707∼1783)	Leonhard Euler
(1752∼1833)	Adrien-Marie Legendre
(1776∼1831)	Marie-Sophie (Sophie)& Germain
(1777∼1855)	Carl Friedrich Gauss
(1814∼1894)	Eugène Charles Catalan
(1817∼1890)	Alphonse de Polignac
(1821∼1894)	Pafnuty Chebyshev
(1865∼1963)	Jacques Solomon Hadamard
(1866∼1962)	Charles Jean de la Vallée-Poussin
(1906∼1998)	André Weil
(1910∼1990)	Lothar Collatz
(1927∼1958)	Yutaka Taniyama
(1943∼)	Robert Tijdeman
(1930∼)	Goro Shimura
(1937∼)	Yuri Ivanovitch Manin
(1944∼)	Gerhard Frey
(1947∼)	Yuri Matiyasevich
(1948∼)	Kenneth Alan Ribet
(1951∼)	Don Bernhard Zagier
(1953∼)	Andrew Wiles

Don Zagier 在 [44] 中的文字：
有關質數分佈的兩個事實, 我希望強勢說服你們, 永久銘刻在你們的心中。
第一, 儘管質數的定義極簡單, 角色是自然數的構成單元, 但在數學家所研究的東西中, 質數卻屬最爲任性：它們在自然數中像野草一樣成長, 似乎除了偶然的機運外不服從其他法則, 而且沒有人能預測下一個會從哪裡冒出來。
第二件事實更令人驚訝, 因爲與上個事實恰恰相反：質數表現出驚人的規律性, 受制於行爲上的法則, 且它們遵守這些幾乎是軍事精度的法則。

下面這張表比較 x 及 $\pi(x)$, 給我們 $\pi(x) - \dfrac{x}{\log x}$, $\dfrac{\pi(x)}{x \log x}$, 及給定的上界之下的質數間隙平均長度 $\dfrac{x}{\pi(x)}$; 由 https://en.wikipedia.org/wiki/Prime_number_theorem 複製

x	$\pi(x)$	$\pi(x) - x/\log x$	$\pi(x)/x/\log x$	$x/\pi(x)$
10	4	-0.3	0.921	2.5
10^2	25	3.3	1.151	4
103	168	23	1.161	5.952
104	1229	143	1.132	8.137
105	9592	906	1.104	10.425
106	78498	6116	1.084	12.740
107	664579	44158	1.071	15.047
108	5761455	332774	1.061	17.357
109	50847534	2592592	1.054	19.667
10^{10}	455052511	20758029	1.048	21.975
10^{11}	4118054813	169923159	1.043	24.283
10^{12}	37607912018	1416705193	1.039	26.590
10^{13}	346065536839	11992858452	1.034	28.896
10^{14}	3204941750802	102838308636	1.033	31.202
10^{15}	29844570422669	891604962452	1.031	33.507
10^{16}	279238341033925	7804289844393	1.029	35.812
10^{17}	2623557157654233	68883734693281	1.027	38.116
10^{18}	24739954287740860	612483070893536	1.025	40.420
10^{19}	234057667276344607	5481624169369960	1.024	42.725
10^{20}	2220819602560918840	49347193044659701	1.023	45.028
10^{21}	21127269486018731928	446579871578168707	1.022	47.332
10^{22}	201467286689315906290	4060704006019620994	1.021	49.636
10^{23}	1925320391606803968923	37083513766578631309	1.020	51.939
10^{24}	18435599767349200867866	339996354713708049069	1.019	54.243
10^{25}	176846309399143769411680	3128516637843038351228	1.018	56.546

以下列出小於 1000 的 168 個質數：

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103
107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199
211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313
317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433
439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563
569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673
677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811
821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941
947 953 967 971 977 983 991 997

參見 `http://dms.umontreal.ca/~andrew/PDF/cramer.pdf`, 有些間隙相當大：

p_n	$p_{n+1} - p_n$
31397	72
370261	112
2010733	148
20831323	210
25056082087	456
2614941710599	652
19581334192423	778