數論講義

呂彥德

February 17, 2017

前言

筆者相信很多人討厭看前言，但這邊還是要把一些重要事項講一講，讓讀者能最高效率地利用這份講義。

首先這篇文章分成兩部曲，第一部是筆者將高中時做過的講義統整來的，主要是關於數學競賽的部分，也加了五六個最近整理時想到的註解還有題目 (只是筆者稍微看了一下發現現在競賽好像都不會用到這些東西了 $\cdots$)。第二部算是大一大二弄的，是一些初等解析數論的東西，比較適合大一大二數學系的，有些內容也可以看成是第一部的延伸 (事實上也有幾題是 ISL N7/8)。這裡要告訴讀者本文是給有一定基礎的人看的，不會從最基本的數論性質開始談，那要怎麼知道適不適合你呢？請先從第一部第一章記號與預備知識開始看起，如果幾個標 $*$ 號的性質都會證明了，那看下去大概就沒什麼問題。

第一部介紹了些數學競賽裡會用到的結論，但是想當然競賽的東西那麼雜，不可能把所有內容都放進來，所以僅介紹了幾個較有背景理論的，如果不想浪費時間看有的沒的可以直接跳到最後一章總整理。各個章節大致上是獨立的，所以可以隨便挑自己想看的看。有些章節最後會有補充教材，那是筆者花最多心力的地方，主要是關於該領域的一些文化及背景介紹。特別要介紹一下第七章整係數多項式，我高二大概花了半年在編，算是這整份文章第一部最精彩的部分。

其次因為例題的特殊性，所以不會更新它們 (絕對不是因為我怕麻煩不想打解答所以才不更新)，這也可能造成例題不夠好、過時，但相信大家可以自己想辦法，反正競賽數學基本上學幾個概念後難題就可以做出來了，而且自己做也會比較好。還有一些建議，如果做不出來的習題是競賽題那就看答案吧，多看答案也是可以學很多東西的。

有個網站叫 AoPS (http://www.artofproblemsolving.com/community/c13_contests)，給還不熟悉競賽的讀者一點介紹，裡面可以找到世界各國各年度大大小小的競賽題目。然後三個常會聽到的名稱是：

1. $\times$ MO：這代表 $\times$ 國家的國內賽。
2. ISL：這是 IMO shortlist 的縮寫，也就是 IMO 的預選題。裡面的題目會按難度排序，題號 1 為最簡單，數論 N 的題號大概會到 7 或 8。
3. TST：這是 team selection test 的縮寫，也就是某國家選訓營的題目。

下面不管是例題或是習題通常會標示來源。剛進到這個網站你一定很迷惑，因為東西太多不知道從哪開始做起。筆者這裡可以推薦幾個競賽：Romania TST、Iran MO、Iran TST、USAMO、USA TST/TSTST、MOSP (美國的營隊)、ISL、ELMO (在美國區)，其中 ISL 是題目平均而言美感及難度兼具的。另外單就數論來看中國的題目也不錯，很難，只是有時候很沒美感。還有一個叫 KöMaL 的徵題解答，題目也很有水準。不過這些都是筆者在高中時的資訊，至於現在這些競賽還優不優或是有其他好的競賽加入就要等其他人補充了。

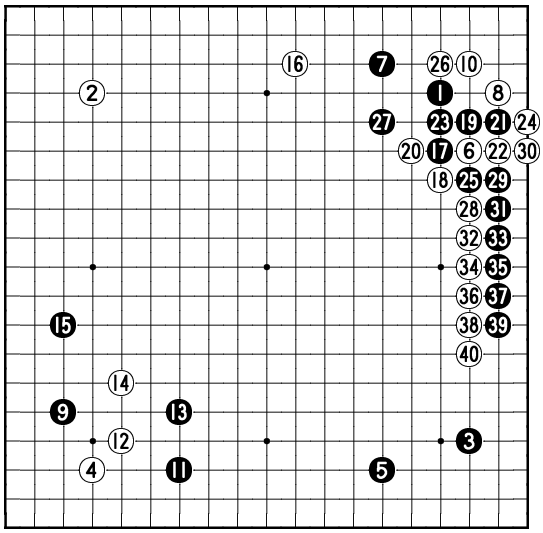
內文會用

例題 0.1: ● Master v.s. ○ XIUZHI (朴廷桓)

對戰日：2016/12/31

貼目：6 目半

以下進行至白 40，試評價 al 老師的二路連爬。



這樣的框框包住例題，然後非常重要一定要認識的性質會用重要性質——★或者是該行直接紅色顯示，所以看到紅色要特別注意。雖然這兩種呈現方式超不專業很像數學外行，不過反正是給高中生看的就沒差了。

目錄

Part I

第一部

Chapter 1

記號與預備知識

雖然有點無聊，但我們還是得從最基本的東西開始。因為這是一份數論的講義，所以這裡的變數/未知數基本上都是整數，除非有另外特別說明。還有 p 都是表示質數，而 q 也有時候是。以下是一點記號說明：

- $\gcd(a_1, \ldots, a_n)$：代表整數 $a_1, \ldots, a_n$ 的最大公因數，有時候 gcd 會省略直接用小括號。
- $\mathrm{lcm}[a_1, \ldots, a_n]$：代表整數 $a_1, \ldots, a_n$ 的最小公倍數，有時候 lcm 會省略。
- $a \mid b$：代表 a 整除 b。
- $p^k \,||\, a$：代表質數次方 p^k 恰整除 a，也就是說 $p^k \mid a$ 但 $p^{k+1} \nmid a$。
- $\mathbb{Z}/n\mathbb{Z}$：代表模 n 的集合，也就是 $= \{0, 1, \ldots, n-1\}$ 而且在上面可以進行模 n 運算，例如 $1 + (n-1) = 0$。
- $\mathbb{Z}/p\mathbb{Z}$：上面的特例，代表模質數 p 的集合。注意在這個集合裡可以進行加減乘除。另外又可以記為 $\mathbb{F}_p, \mathbb{Z}_p$。(其實 $\mathbb{Z}/p\mathbb{Z}$ 和 $\mathbb{F}_p$ 是分情況用的，但是在本文裡不會區別它們)
- $v_p(\cdot)$：表示 p 進指數。也就是說當正整數 $n = p^a m$ 且 $(p, m) = 1$ 時，$v_p(n) = a$.

再來是一些數學競賽裡最基本的定理或性質們，其中標 $*$ 號者希望讀者會證明。另外最後一個 lifting the exponent lemma 其實算是比較高級的方法，讀者後面念到指數與原根一章的時候可能會看出它的用法。因為已經有講義所以就不在本文提了。

- **(Euler's theorem)*** 當 $(a, m) = 1$ 時 $a^{\phi(m)} \equiv 1 \pmod{m}$，其中 ϕ 表示 Euler 函數，也就是 $\phi(m)$ 為小於等於 m 的正整數中與 m 互質的整數個數。
- **(Fermat's theorem)*** 當 $(a, p) = 1$ 時 $a^{p-1} \equiv 1 \pmod{m}$.
- **(Wilson's theorem)*** 對質數 p 總有 $(p-1)! \equiv -1 \pmod{p}$.

- **(中國剩餘定理)*** 若整數 $m_1 \ldots, m_n$ 兩兩互質，則對於任意的整數 $a_1, \ldots, a_n$，以下一元同餘方程組必定有解。

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

- **(Bézout's theorem)*** 令 a, b 為整數，則存在整數 m, n 使得 $am + bn = \gcd(a, b)$.
- **(Chebyshev's theorem)** 若整數 $n > 3$，則至少存在一個質數 p，符合 $n < p < 2n - 2$.
- **(Lagrange's four-square theorem)** 每個正整數都可以表示成四個整數的平方和。
- **(Lifting the exponent lemma)** http://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/lifting-the-exponent.pdf

Chebyshev's theorem 的估計稍微加強一點就可以得到很 king 的定理，在第二部的第一章數論函數會介紹。往下閱讀還會發現很多東西，雖然競賽裡可以隨便 call 定理，但還是要自己知道證明比較好，這樣對以後進階的學習也有幫助。

最後是一些數論常用基本技巧，本文不會提。以下內容節錄自謝宇觀的某篇講義，我是蓄意抄襲的：

1. **(比大小、壓界)** N1 和 N2 根本比大小的天下，看到不定方程的題目，幾乎都是想辦法壓界再亂模。常用的大小關係確定方法，包括：
   (a) 不失一般性假設大小關係再討論
   (b) 指數函數成長速度大於多項式函數
   (c) 整除式右邊不為 0 左邊絕對值小於右邊絕對值
   (d) 用整除關係模進而判斷出一些因倍數關係並假設 $n = kt$ 之類的
   (e) 嘗試確定某個完全平方數的範圍
2. **(無窮遞降法)** 相信大家跟無窮遞降法肯定也頗熟悉，通常都是用來反證不存在，會假設某個東西是最小的，然後證明存在更小的故矛盾。又或假設某個分數化為最簡後發現分母分子有公因數，此外如超神的 vieta jumping 也可以算是無窮遞降法的一員。
3. **(數學歸納法)** 這裡只是要提醒一下而已。

Chapter 2

數論函數

所謂的數論函數指的是定義域為整數而值域為複數的函數，是所有數論研究的根本，藉由了解一些數論函數的性質，可以估計某些數的最大質因數、最小質因數、質因數個數等等，而我們知道這些是數論最重要的幾個問題。一些常見的數論函數有質因數個數函數 ω、Euler 函數 ϕ、因數和函數 τ 以及因數個數函數 d 等等。

從一個簡單的例子開始：取因數和函數 τ，我們知道

$$\begin{aligned}\sum_{n\le x}\tau(n) &= \sum_{n\le x}\sum_{d|n}1 = \sum_{d\le x}\sum_{n\le x,d|n}1\\ &= \sum_{d\le x}\sum_{n\le x,d|n}\frac{x}{d}+O(1)\\ &= x\log x+O(x).\end{aligned}$$

其中 $O(f)$ 表示一個取絕對值後小於等於函數 f 的某個固定常數倍的項，讀者可以將它想像成誤差的估計，例如 $O(1)$ 是一個取絕對值後小於等於某個固定常數的項 (在上面的等式裡這項是 ≤ 1 的)。當我們把兩邊同時除以 x 後，一個有趣的結論便出現了：在 $1,2,\ldots,x$ 中，「平均」每個數的因數和會是 $\log x$，其中的誤差大約是一個固定常數。

2.1 積性函數

定義 2.1 數論函數 f 若滿足對任意 $(m,n)=1$ 都有

$$f(mn)=f(m)f(n)$$

則稱 f 為積性函數。若是 f 強到對所有正整數 m,n 都有 $f(mn)=f(m)f(n)$ 則稱為完全積性函數。

上面所提到的質因數個數函數、Euler 函數、因數和函數以及因數個數函數都是積性函數 (但都不是完全積性的)。可以從定義看出，欲決定一個積性函數，只需要求出它在質數的次方上的取值就行了；而對於一個完全積性函數，更只需要知道他在質數上的取

值。另外當我們已經有一個數論函數 f 時，還可以考慮由以下定義的和函數 g：

$$g(n) = \sum_{d|n} f(d).$$

定理 2.1 若 f 是積性函數，則其和函數 g 亦為積性函數。

證明： 取互質的兩個正整數 m, n，那麼

$$g(mn) = \sum_{d'|mn} f(d') = \sum_{d|m,\, e|n} f(de) = \sum_{d|m} f(d) \sum_{e|n} f(e) = f(m)f(n). \qquad \square$$

例題 1.1: 初試身手

對所有正整數 n，以 $S(n)$ 記使得 $xy = n$ 且 $\gcd(x, y) = 1$ 的正整數對 (x, y) 的個數。試證

$$\sum_{d|n} S(d) = d(n^2).$$

證明： 首先分析題目：左邊長得好像剛剛才說過的和函數，它有可能是積性的；而右邊是因數個數函數，它剛好真的是積性的。我們於是可以藉由先證明左右兩式當 n 為質數次方時必定成立，再證明 S 是積性函數 (所以左式—它的和函數—也是積性的)，而說明兩邊對於所有正整數 n 都相同 (把它分成相異質數次方的乘積就可以看出來了)。

首先取 $n = p^k$ 為某個質數次方。顯然 $d(n^2) = d(p^{2k}) = 2k + 1$，另一方面 $S(1) = 1$ 而 $S(p^t) = 2$ 對所有 $t \geq 1$，因此左式也等於 $2k + 1$。這代表 n 為質數次方時兩式總是相等的。

再來要證明 S 是積性函數，於是取 m, n 是兩個互質的正整數。可以看出當我們有兩組正整數對 (x_1, y_1), (x_2, y_2) 滿足 $x_1y_1 = m$, $x_2y_2 = n$ 且 $\gcd(x_1, y_1) = \gcd(x_2, y_2) = 1$ 時，會對應到一組正整數對 $(x_3, y_3) = (x_1x_2, y_1y_2)$ 滿足 $x_3y_3 = mn$ 且 $\gcd(x_3, y_3) = 1$；而相反過來當有一組正整數對 (x_3, y_3) 滿足 $x_3y_3 = mn$ 且 $\gcd(x_3, y_3) = 1$ 時也可以由同樣的對應方法把它拆成兩組分別在在 $S(m)$, $S(n)$ 對應到的集合裡的正整數對。綜合以上有 $S(mn) = S(m)S(n)$，命題至此得證。 $\square$

例題 1.2: China TST 2008

取 n 為正整數，使得 n 可以整除 $2^{\phi(n)} + 3^{\phi(n)} + \cdots + n^{\phi(n)}$。令 $p_1, p_2, \ldots, p_k$ 為 n 的所有不同的質因數，試證

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_k} + \frac{1}{p_1 p_2 \cdots p_k}$$

是一個正整數。

證明： 我們可以把和通分成一個分數，其中分母是 $p_1p_2\cdots p_k$，而欲證和為正整數即是要證明對所有 $1\le i\le k$ 都有 p_i 整除分子，由對稱性僅須證明此對 p_1 成立。再來藉由注意到

$$\frac{1}{p_2}+\cdots+\frac{1}{p_k}=\frac{p_1\times \text{某正整數}}{p_1p_2\cdots p_k}.$$

又可以把問題簡化成證明 p_1 整除

$$\frac{1}{p_1}+\frac{1}{p_1p_2\cdots p_k}$$

的分子，即證明 p_1 整除 $1+p_2\cdots p_k$。

現在來分析條件 $n\mid 2^{\phi(n)}+3^{\phi(n)}+\cdots+n^{\phi(n)}$：記 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，那麼由於

$$\begin{aligned}
0\equiv 2^{\phi(n)}+3^{\phi(n)}+\cdots+n^{\phi(n)} &\equiv \frac{n}{p_1}\left(\sum_{i=1}^{p_1} i^{\phi(n)}\right)-1^{\phi(n)} \pmod{p_1}\\
&\equiv \frac{n}{p_1}\left(\sum_{i=1}^{p_1-1} i^{\phi(n)}\right)-1 \pmod{p_1}\\
&\equiv \frac{n}{p_1}\left(\sum_{i=1}^{p_1-1} 1\right)-1 \pmod{p_1}\ \text{(Euler 定理)}\\
&\equiv -\frac{n}{p_1}-1 \pmod{p_1}.
\end{aligned}$$

我們將得到 $\alpha_1=1$。同理對所有 i 都要有 $\alpha_i=1$，把這些條件代進最後一行的同餘式可以得到 $p_1\mid 1+p_2\cdots p_k$，為所求。 □

在做習題前，我們最後來看一個定理，用該定理再加上一點構造力可以比較許多數論函數的大小，例如習題 8~12 等等，至於細節就留給讀者慢慢體會了。

重要性質——★ 所有質數的倒數和發散。

證明： 這個定理牽扯到級數的知識，可以要大一學過微積分的讀者才能給出嚴謹的證明，不過筆者覺得維基百科上的這個證法高中生應該也可以接受。我們以下在 $\mathbb{R}\cup\{+\infty\}$ 裡面做事。

$$\begin{aligned}
\log\left(\sum_{n=1}^{\infty}\frac{1}{n}\right)=\log\left(\prod_p\frac{1}{1-p^{-1}}\right)&=\sum_p\log\left(\frac{1}{1-p^{-1}}\right)=\sum_p-\ln(1-p^{-1})\\
&=\sum_p\left(\frac{1}{p}+\frac{1}{2p^2}+\frac{1}{3p^3}+\cdots\right)=\left(\sum_p\frac{1}{p}\right)+\sum_p\frac{1}{p^2}\left(\frac{1}{2}+\frac{1}{3p}+\frac{1}{4p^2}+\cdots\right)\\
&\le\left(\sum_p\frac{1}{p}\right)+\sum_p\frac{1}{p^2}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)\\
&=\left(\sum_p\frac{1}{p}\right)+\sum_p\left(\frac{1}{p(p-1)}\right)=\left(\sum_p\frac{1}{p}\right)+C
\end{aligned}$$

對某個常數 $C<1$。由於左式發散，故右式亦發散。 □

Problem set

P1. For every positive integer n, $S_k(n)$ denote the number of pairs of positive integers $(x_1, x_2, \cdots, x_k)$ such that $x_1x_2\cdots x_k = n$. Calculate

$$\sum_{d|n} S_k(d).$$

P2. Liouville's theorem

Prove that

$$\sum_{d|n} \Big(\tau(d)\Big)^3 = \Big(\sum_{d|n} \tau(d)\Big)^2.$$

P3. Let n be an integer with $n \geq 2$. Show that $\phi(2^n - 1)$ is divisible by n.

P4. Bulgaria MO 2011/5

Find all natural numbers n for which n has exactly two different prime divisors and n satisfies

$$\phi(\tau(n)) = \tau(\phi(n)).$$

P5. ISL 2004 N1

Prove that there exist infinitely many positive integers a such that the equation $\tau(an) = n$ does not have a positive integer solution n.

P6. ISL 2004 N2

The function f from the set $\mathbb{N}$ into itself is defined by the equality

$$f(n) = \sum_{k=1}^{n} \gcd(k, n), \quad n \in \mathbb{N}.$$

(a) Prove that $f(mn) = f(m)f(n)$ for every relatively prime $m, n \in \mathbb{N}$.

(b) Prove that for each $a \in \mathbb{N}$ the equation $f(x) = ax$ has a solution.

(c) Find all $a \in \mathbb{N}$ such that the equation $f(x) = ax$ has a unique solution.

P7. USA TSTST 2016

Suppose that n and k are positive integers such that

$$1 = \underbrace{\phi(\phi(\cdots\phi}_{k \text{ times}}(n)\cdots)).$$

Prove that $n \leq 3^k$.

P8. Romania TST 2010

Given a positive integer a. Prove that $\tau(am) < \tau(am + 1)$ for infinitely positive integers m.

P9. Iran MO 2012

Prove that for each $n \in \mathbb{N}$ there exist natural numbers $a_1 < a_2 < \cdots < a_n$ such that $\phi(a_1) > \phi(a_2) > \cdots > \phi(a_n)$.

P10. China TST 2012

For a positive integer n, if $\tau(m) < \tau(n)$ for all $m < n$, we call n a good number. Prove that for any positive integer k, there are only finitely many good numbers not divisible by k.

P11. ISL 2005 N5

A positive integer n is called highly divisible if $\tau(n) > \tau(m)$ for all positive integers $m < n$. Two highly divisible integers m and n with $m < n$ are called consecutive if there exists no highly divisible integer s satisfying $m < s < n$.

(a) Show that there are only finitely many pairs of consecutive highly divisible integers of the form (a, b) with $a \mid b$.

(b) Show that for every prime number p there exist infinitely many positive highly divisible integers r such that pr is also highly divisible.

P12. CGMO 2014

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ be the prime factorisation of n. Define $\omega(n) = t$ and $\Omega(n) = a_1 + a_2 + \cdots + a_t$. Prove or disprove: For any fixed positive integer k and positive reals α, β, there exists a positive integer $n > 1$ such that

- $\dfrac{\omega(n+k)}{\omega(n)} > \alpha$
- $\dfrac{\Omega(n+k)}{\Omega(n)} < \beta$.

P13. Taiwan TST 2011

Determine if there exist a infinite positive integer sequence $a_1, \ldots, a_n, \ldots$, satisfying:

(a) $a_1 = (2011)!$.

(b) $a_i = \phi(a_{i+1})$ for all $i \in \mathbb{N}$.

P14. USA TSTST 2015

Let $\phi(n)$ denote the number of positive integers less than n that are relatively prime to n. Prove that there exists a positive integer m for which the equation $\phi(n) = m$ has at least 2015 solutions in n.

2.2 Mőbius 反演

我們想要進一步地探討一個數論函數與它和函數的關係，具體來說，已知某個數論函數的和函數，那是否有可能把原本的數論函數求出來呢？讀者可以從幾個小的質開始嘗試，容易會發現這是可行的。為了方便計算，引入以下函數：

定義 2.2 Mőbius 函數 μ 定義為：

$$\mu(n) = \begin{cases} 1 & , \quad n = 1 \\ (-1)^r & , \quad n = p_1 p_2 \cdots p_r \\ 0 & , \quad \text{其他情況} \end{cases}$$

定理 2.2 (Mőbius 反演公式) 設 F 是數論函數 f 的和函數，則

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

證明：

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \Big(\sum_{c|\frac{n}{d}} f(c) \Big) = \sum_{d|n} \sum_{c|\frac{n}{d}} \mu(d) f(c) \quad = \sum_{c|n} \Big(\sum_{d|\frac{n}{c}} \mu(d) \Big) f(c) = f(n)$$

因為當 $\frac{n}{c} > 1$ 時，$\sum_{d|\frac{n}{c}} \mu(d) = 0$. □

Problem set

P1. Let F and f be two arithmetic functions related by the formula

$$F(n) = \prod_{d|n} f(d).$$

Then

$$f(n) = \prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)}.$$

P2. ILL 1989/11

Define the sequence (a_n) by

$$\sum_{d|n} a_d = 2^n.$$

Show that $n \mid a_n$.

P3. China TST 2009

Let (a_n) be a sequence of positive integers satisfying $(a_m, a_n) = a_{(m,n)}$. Prove that for any $n \in \mathbb{N}$,

$$\prod_{d|n} a_d^{\mu\left(\frac{n}{d}\right)}$$

is an integer.

Chapter 3

指數與原根

3.1 二次剩餘

數論上一個很自然的問題是研究一個多項式在模某個正整數下的解，其中中國剩餘定理又是特別有用的。一次 (線性) 方程式的研究是最簡單的，相信讀者已經認識結論，如果不知道也可以試著自行嘗試做做看。而研究完線性同餘方程後，再來便會想繼續研究二次同餘方程，也就是型如：

$$ax^2 + bx + c \equiv 0 \pmod{m}$$

的方程。在 17,18 世紀之間，如 Fermat, Euler, Lagrange, Legendre 等偉大的數論學家都對這方面做出了許多貢獻，他們證明了一些基本的結果，也提出了一些猜想，不過第一個有系統研究該領域的是著名的 Carl Friedrich Gauss，他在 1801 年發表了著作《Disquisitiones Arithmeticae》，其中自第四章開始正是他研究的心血結晶。

現在讓我們回到最開始的問題，型如 $ax^2 + bx + c \equiv 0 \pmod{m}$ 的方程到底要怎麼解？第一個大家可能會聯想到配方法，因此回憶國中解二次方程的方法，我們把兩邊先同乘 $2a$，也就是配成

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{m}$$

的型式，總之，我們先將原問題化簡為 $y^2 \equiv d \pmod{m}$ 這種看起來較簡單的型式了。再來便能夠作質因數分解 $m = p_1^{n_1} \cdots p_k^{n_k}$，並且由中國剩餘定理可知同餘式 $y^2 \equiv d \pmod{m}$ 有解會等價於對每個 p^n，同餘式 $y^2 \equiv d \pmod{p^n}$ 有解。因此現在的問題就是：給定整數 a 以及質數次方 p^n，同餘方程 $x^2 \equiv a \pmod{p^n}$ 何時有解？

首先我們討論最特殊的情況：$n = 1$ 且 p 是奇質數。而且為方便，定義下列兩個名稱：

定義 3.1 對於二次同餘式

$$x^2 \equiv a \pmod{m}.$$

如果有解，則 a 為模 m 的**二次剩餘**，反之，稱 a 為模 m 的**二次非剩餘**。

許多重要的數學性質或是理論總是從小數字代入開始嘗試而找出的，也許我們也該這樣做：比方說對模 5，會有 $1^2 \equiv 4^2 \equiv 1,\ 2^2 \equiv 3^2 \equiv 4$，也就是 $1, 4$ 是模 5 的二次剩餘，而 $2, 3$ 是模 5 的二次非剩餘。在這之中我們似乎找到了一點規律：是否 $x^2 \equiv a \pmod{p}$ 恰有兩組解或無解呢？

性質 3.1 若 p 是奇質數，且 $p \nmid a$，則 $x^2 \equiv a \pmod{p}$ 恰有兩組解或無解。

證明： 假設這個方程有解 x_1，那麼顯見 $p - x_1$ 也是一組解。而如果還有解 x_2，那麼我們由

$$\begin{cases} x_1^2 & \equiv & a \pmod{p} \\ x_2^2 & \equiv & a \pmod{p} \end{cases}$$

相減可得 $p \mid (x_1 + x_2)(x_1 - x_2)$，因此只有 $x_2 = p - x_1$ 或是 $x_2 = x_1$。 □

並且在證明中可以看到，$1^2, 2^2, \ldots, (p - 1/2)^2$ 正好是 mod p 的所有二次剩餘，因此便找到一個生成所有二次剩餘的方法了！然而，這僅能給出「二次剩餘是哪些數」的回答，我們依舊不能判斷「給定的數是不是二次剩餘」。

於是我們重新思考 $x^2 \equiv a \pmod{p}$ 有解的意義為何？這其實是告訴你在 mod p 下 a 這個數扮演的是不是一個平方數的角色，因此它跟非二次剩餘的最大的不同點可能就會反映在它們關於指數的性質上。

定理 3.1 (Euler's Criterion) a 為模 p 的二次剩餘當且僅當

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

證明： 首先我們先看一下 $a^{\frac{p-1}{2}}$ 可以取值多少，顯見 $(a^{\frac{p-1}{2}})^2 \equiv a^{p-1} \equiv 1 \pmod{p}$，然後由**性質 3.1** 知道 $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.

由 Fermat 小定理可以知道 $x^{p-1} \equiv 1 \pmod{p}$ 對所有數都成立，現在假設 a 為模 p 的二次剩餘，並且 x_1 是它的一個方根，那麼會有 $a^{\frac{p-1}{2}} \equiv x_1^{p-1} \equiv 1 \pmod{p}$。另一方面如果 a 不是二次剩餘，對於任一模 p 簡化剩餘系裡的數 i，必定存在另一數 j 使得 $ij \equiv a \pmod{p}$，並且必定 $i \neq j \pmod{p}$，因此我們可將 $1, 2, \ldots, p-1$ 中的數兩兩配對，乘積都是 a，所以 $a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \pmod{p}$，這就證完了定理。 □

好的，現在我們已經解決了一開始的問題，要判斷 a 是不是二次剩餘，只要算算看 $a^{\frac{p-1}{2}}$ 就好啦！想也知道，這方法數字大一點就只能硬爆，根本不可能實際應用，所以必須要先定義一些好記算的東東。

定義 3.2 (Legendre's symbol) 如果 p 是奇質數，那麼定義符號

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & , \ a \text{ 為模 } p \text{ 的二次剩餘} \\ -1 & , \ a \text{ 不為模 } p \text{ 的二次剩餘} \\ 0 & , \ p \mid a \end{cases}$$

這時你可能覺得有點奇怪，為什麼把 0 跟別的數分開定義？真要說的話，我們有 $0^2 \equiv 0 \pmod{p}$，也就是說 0 應該也算是二次剩餘啊。其中一個理由是這樣做可以方便直接陳述某些定理及性質，而不用一直提 0 這個反例。另外的理由就是關於抽象代數裡特徵 (character) 的概念了，這個符號會在第二部裡 Dirichlet 特徵的章節介紹，而那之後會常用到這個東西，有興趣的讀者可以自己再精進。

比較一下這個符號的定義以及剛剛提到的 Euler's Criterion，會發現根本就有

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

所以你就發現了重要事實：這個運算是積性的！也就是說，兩個二次剩餘或兩個二次非剩餘的積會變成二次剩餘，而一個二次剩餘及一個二次非剩餘的積會是二次非剩餘！稍微整理一下，就是：

重要性質——★ Legendre 符號滿足以下性質：

(1) 若 $a \equiv b \pmod{p}$，則 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) 若 $p \nmid a$，則 $\left(\frac{a^2}{p}\right) = 1$.

(3) 若 $p \nmid ab$，則 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

藉由這三個性質的幫助，我們僅需算出 $\left(\frac{-1}{p}\right), \left(\frac{2}{p}\right), \left(\frac{q}{p}\right)$ (q 是奇質數)，就可以給出一般 $\left(\frac{a}{p}\right)$ 的值！以下分別處理這三個值：

性質 3.2

⊡ **Case I.** 對於奇質數 p，會有：

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & , \ p \equiv 1 \pmod{4} \\ -1 & , \ p \equiv 3 \pmod{4} \end{cases}$$

⊡ **Case II.** 對於奇質數 p，會有：

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & , \ p \equiv \pm 1 \pmod{8} \\ -1 & , \ p \equiv \pm 3 \pmod{8} \end{cases}$$

證明： 對於 **I.** 只要直接代入 Euler's Criterion 計算即可得。而對於 **II.**，我們考慮同餘式：

$$\begin{aligned} p-1 &\equiv 1(-1) \pmod{p} \\ 2 &\equiv 2(-1)^2 \pmod{p} \\ p-3 &\equiv 3(-1)^3 \pmod{p} \\ 4 &\equiv 4(-1)^4 \pmod{p} \\ &\vdots \\ \frac{p \pm 1}{2} &\equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \pmod{p} \end{aligned}$$

將所有式子相乘便得到

$$2\cdot 4\cdot 6\cdots(p-3)\cdot(p-1)\equiv\left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+\frac{p-1}{2}}\pmod p.$$

然後再注意到左邊都是偶數，因此

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}}\pmod p.$$

然後因為 $p\nmid\left(\frac{p-1}{2}\right)!$，並且 $2^{\frac{p-1}{2}}\equiv\left(\frac{2}{p}\right)\pmod p$，因此

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$ □

我們會發現到 **Case II.** 的證明似乎也不太直觀。另外其實這並不是當初 Gauss 所提出的證法。為了減化計算過程，他先證明了：

定理 3.2 (Gauss's Lemma) 設 p 是奇質數，$(p,a)=1$，如果在數

$$a,2a,\ldots,\left(\frac{p-1}{2}\right)a\pmod p.$$

中有 m 個數大於 $p/2$，那麼 $\left(\frac{a}{p}\right)=(-1)^m$.

至於他是怎麼想到這件事會發生的，大概只有神才知道。由此出發便能把大數字的次方運算降到乘積運算，然後就可以直接計算出 $\left(\frac{n}{p}\right)$ 的值。更進一步的，他還用此引理證明了

定理 3.3 (Quadratic Reciprocity Law) 若 p,q 為兩互異奇質數，則

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

就連 Euler 以及 Legendre 都只能把這個性質當作猜想。而且 Gauss 一生中總共對此提出了八種證法，私下裡他把二次互反律譽為數論中的寶石，是一個黃金定律，現今二次互反律已有超過 200 個不同的的證明。

1900 年 Hilbert 提出的數學問題中的第九個即是希望推廣到更高次的互反律，亦即要在一般代數數域中找到可以對應質數階範式剩餘的互反律，儘管此問題已有許多進展，但仍未完全解決。

3.2 Hensel's Lifting Lemma

有一個數學競賽中關於指數超好用的性質：「如果有 $p^N\mid\mid x-c$，那可以多模一次寫成 $x\equiv c+tp^N\pmod{p^{N+1}}$」，這邊要用這樣的想法來處理二次剩餘中模是奇質數的次方的情況 (在上一小節裡已經處理完模是奇質數的情況)。比方我們已知 $1,4$ 是模 5 的二次剩餘，那麼繼續考慮模 5^2：當有 a 是二次剩餘，就是說有 $x^2\equiv a\pmod{5^2}$ 時，就會

有 $x^2 \equiv a \pmod 5$，因此 a 也要是模 5 的二次剩餘。所以我們僅須確定 1, 6, 11, 16, 21, 4, 9, 14, 19, 24 中哪些數是模 25 的二次剩餘。

比方說我們要看 6 是不是模 25 的二次剩餘。首先注意到 $6 \equiv 1 \pmod 5$，也就是說如果有 $x^2 \equiv 6 \pmod{5^2}$，那麼必定有 $x \equiv 1$ 或 $4 \pmod 5$。反過來說，我們能不能直接由 1 或 4 去生成 6 呢？也就是說，能否找到適當的 t 使得

$$(1+5t)^2 \equiv 6 \pmod{5^2} \text{ 或 } (4+5t)^2 \equiv 6 \pmod{5^2}?$$

現在先看左式，我們展開得到 $1 + 10t + 25t^2 \equiv 6 \pmod{5^2}$，再來把高次項直接消掉並移項得 $10t - 5 \equiv 0 \pmod{5^2}$，兩邊同除以 5 得到 $2t - 1 \equiv 0 \pmod 5$，發現這 t 在模 5 下是有解的！也就是說在這個例子裡 6 是模 5^2 的二次剩餘，而且是由某個模 5 的二次剩餘所生成的。

我們馬上聯想到，這個過程根本可以一般化，換言之可以從模 p^n 的二次剩餘去生成 p^{n+1} 的二次剩餘，反正只要二項式展開再一直消掉質數次方就好了！具體來說：

性質 3.3 如果 a 是模 p^n 的二次剩餘，那麼 $a + p^n k$ 全都是模 p^{n+1} 的二次剩餘。

證明： 假設有 $x^2 \equiv a \pmod{p^n}$，現在我們考慮 $(x + p^n t)^2$ 去模 p^{n+1}。我們希望找到適當的 t 使得

$$(x + p^n t)^2 \equiv a + p^n k \pmod{p^{n+1}}.$$

展開之後先把高次項直接消掉，得到 $(x^2 - a) + 2p^n tx \equiv 0 \pmod{p^{n+1}}$，再來除掉 p^n 即得 $\left(\dfrac{x^2 - a}{p^n} - k\right) + 2tx \equiv 0 \pmod p$，由於變數 t 的係數是 $2x$ 會與 p 互質，因此這個 t 是存在的！ □

並且在上面的證明會發現，從模 p^n 的二次剩餘去生成 p^{n+1} 的二次剩餘的方法是唯一的！也就是說如果現在我們知道 p 的二次剩餘 a 是由哪個 $x^2 \equiv a \pmod p$ 解得的，那就也可以知道模 p^{n+1} 的二次剩餘 $a + p^n k$ 是從哪個 $(x + p^n t)^2 \equiv a + p^n k \pmod{p^{n+1}}$ 生成的了！運用 Tylor 展開式，這方法可以被推廣成好的定理：

定理 3.4 (Hensel's Lemma) 設 $f(x)$ 為一整係數多項式，且令 m, k 為兩正整數使得 $m \leq k$。若整數 r 使得

$$f(r) \equiv 0 \pmod{p^k} \text{ 且 } f'(r) \not\equiv 0 \pmod p.$$

那麼存在整數 s 使得

$$f(s) \equiv 0 \pmod{p^{k+m}} \text{ 且 } r \equiv s \pmod{p^k}.$$

而且 s 在模 p^{k+m} 下是唯一的，可以寫成 $s = r + tp^k$。

在這邊要注意到的是如果 $f'(r) \equiv 0 \pmod p$，並不代表去模 p 大一點的次方時就會無解，而是說它的解在模 p^{k+m} 時並不會是唯一的，當然有些情況下就真的代表模 p^{k+m} 時會無解。最後由此方法，我們可以證明：

性質 3.4 設 $n \geq 3$ 且 a 是奇數。則 a 是模 2^n 的二次剩餘當且僅當 $a \equiv 1 \pmod 8$.

這裡的證明留給讀者。至於 a 是偶數的情況，發現此時 x 也要是偶數，因此可以每次將 a 分解式中 2 的冪次減 2，就可以降至奇數或直接證明 a 根本不是二次剩餘。至此，我們已經將所有二次剩餘的情況討論完畢！

Problem set

P1. Let $p = 2^n + 1$ for $n \geq 2$ is a prime number, then prove that p divides $3^{\frac{p-1}{2}} + 1$.

P2. Determine all positive integers n for which there exists an integer m such that $2^n - 1$ divides $m^2 + 9$.

P3. Let $m, n \geq 3$ be two odd numbers. Prove that

$$2^m - 1 \nmid 3^n - 1.$$

P4. Let F_k denotes the k^{th} Fibonacci number. Prove that

$$F_p \equiv \left(\frac{p}{5}\right) \pmod p.$$

P5. Prove that for every prime p, there exists an integer x such that

$$x^{2^{n+1}} \equiv 2^{2^n} \pmod p$$

for all $n \geq 2$.

P6. Prove Hensel's Lemma.

P7. Iran MO 2011

Let n and k be two natural numbers such that k is even and for each prime p if $p \mid n$ then $p - 1 \mid k$. let $\{a_1, \ldots, a_{\phi(n)}\}$ be all the numbers coprime to n. What's the remainder of the number $a_1^k + ... + a_{\phi(n)}^k$ when it's divided by n?

P8. USA TSTST 2016

Decide whether or not there exists a nonconstant polynomial $Q(x)$ with integer coefficients with the following property: for every positive integer $n > 2$, the numbers

$$Q(0),\ Q(1),\ Q(2), \ldots,\ Q(n-1)$$

produce at most $0.499n$ distinct residues when taken modulo n.

P9. Iran MO 2016

Let P be a polynomial with integer coefficients. We say P is good if there exist infinitely many prime numbers q such that the set

$$X = \{P(n) \pmod q \mid \quad n \in \mathbb{N}\}$$

has at least $(q+1)/2$ members. Prove that the polynomial x^3+x is good.

P10. ISL 2004 N4

Let k be a fix integer greater than 1, and let $m=4k^2-5$. Show that there exist positive integers a and b such that the sequence $\langle x_n\rangle$ defined by

$$x_0=a,\ x_1=b,\ x_{n+2}=x_{n+1}+x_n$$

has all of its terms relatively prime to m.

P11. An ordered pair (a,b) of numbers $a,b\in\mathbb{N}$ is called *interesting*, if for any $n\in\mathbb{N}$ there exists k such that the number a^k+b is divisible by 2^n. Find all *interesting* ordered pairs of numbers.

P12. ISL 2006 N7

For all positive integers n, show that there exists a positive integer m such that n divides 2^m+m.

P13. Show that there exist a polynomial with degree 5 and don't have rational roots, but have a root mod n for any positive integer n.

(Note: In fact, the number "5" is minimum.)

3.3 指數與原根

終於進入本章最重要的部分，指數一直是數學競賽裡最重要相對來說也最常考的一塊。在數論中，研究某數冪次去模質數一直是個重要的問題，比方說，能否找到某質數 p 讓 $x^n+y^n\equiv z^n \pmod p$ 無 (x,y,z) 正整數解？如果有好的結論，那 Fermat 最後猜想根本就是 trivial。因此現在我們希望把焦點放在次方數上。

考慮無窮數列 $a,a^2,a^3,\ldots \pmod m$，由於他至多只能取 $m-1$ 個值，由鴿子先生原理我們知道必定有兩數相等，假設最近的兩個是 $a^i\equiv a^j \pmod m$，兩邊相除即得到 $a^{i-j}\equiv 1 \pmod m$，也就是說這數列每隔 $i-j$ 項就會重複。可以合理猜測這個數列的最小週期會隱含許多和 a 相關的性質，因此定義：

定義 3.3 *若 d 為最小的正整數使*

$$a^d\equiv 1 \pmod m.$$

我們稱 d 為 a 對模 m 的**指數**，記作 $\mathrm{ord}_m(a)$ (但在本文中，為方便我們記為 $\delta_m(a)$).
而且由 Euler 定理我們知道當 $(a,m)=1$ 時會有

$$a^{\phi(m)}\equiv 1 \pmod m.$$

所以使得 $\delta_m(a)=\phi(m)$ 的那些 a 可能地位又更特殊，額外稱那些 a 為對模 m 的**原根**。

重要性質——★

(1) 若兩正整數 a 和 m 互質，且 $a^k \equiv 1 \pmod{m}$ 則 $\delta_m(a) \mid k$。

(2) 若兩正整數 a 和 m 互質，且 $\delta_m(a) = d$，則 $\delta_m(a^k) = \dfrac{d}{\gcd(d,k)}$。

證明：

(1) 由輾轉相除法得 $k = \delta_m(a)t + r$，其中 $\delta_m(a) > r \geq 0$，因此 $a^r \equiv a^k \cdot (a^{\delta_m(a)})^{-t} \equiv 1 \pmod{m}$，然而我們已定義 $\delta_m(a)$ 是滿足此式的最小正整數，因此只有 $r = 0$。

(2) 為了方便，先定義 $e = \gcd(d,k)$。首先有 $(a^k)^{d/e} \equiv (a^d)^{k/e} \equiv 1 \pmod{m}$，因此 $\delta_m(a^k) \mid (d/e)$。再來由於 $(a^k)^{\delta_m(a^k)} \equiv 1 \pmod{m}$，所以要有 $d \mid k\delta_m(a^k)$，因此 $(d/e) \mid \delta_m(a^k)$。這就得到了 $\delta_m(a^k) = k/e$。 □

可以看出這兩個性質根本太讚！其中 (1) 保證了所有週期必是最小正週期的倍數，這對週期函數來講是個好性質，如果想要研究大的冪次時，只需把次方去模最小正週期即可大幅化簡計算量！至於性質 (2) 則是給出了計算次方數的指數 (order) 的方法，於是你可能會想：如果能找到某數，讓他的次方生成簡化剩餘系，那我們不就可以直接算出所有數的指數了嗎?!

回憶一下原根的定義，就是使得 $\delta_m(a) = \phi(m)$ 的那些 a。誒?! $\phi(m)$ 好像是小於等於 m 且與 m 互質的整數個數，那這不就是告訴我們說原根可以生成簡化剩餘系嗎！因此作為一隻喜愛數學的貓咪，當然會想看模哪些數會有原根，以及原根還有什麼性質。

首先如果模 m 有原根 g，由於簡化剩餘系被他生成，所以所有數可以寫成 g^i 的型式，由性質 (2) 馬上知道另外的原根一定型如 g^j，其中 $(j, \phi(m)) = 1$，以是：

定理 3.5 *若模 m 有原根，則共有 $\phi(\phi(m))$ 個。*

現在，我們想要找出有原根的那些數。首先由小數字開始慢慢試，你會發現似乎對 $2, 3, 5, 7, \ldots$ 好像都找得到原根，又由於質數的特殊性，可以先合理的猜測：對所有質數 p，原根總是存在的。

那我們到底要如何來分析這個性質呢？先看一下上面給出的性質：會有 $\phi(p-1)$ 個原根。嗯 $\cdots$，似乎不太有用，因為我們甚至連有一個都證不了。不過讓我們再回憶更貼近原根本質的性質 (2)：假設 g 是模 p 的一個原根，那會有 $\delta_m(g^k) = (p-1)/\gcd(p-1,k)$，這似乎暗示我們可以依照 $\delta_m(a)$ 的值對整數 a 進行分類。

現在假設 $\psi(d)$ 是指數為 d 的數的個數，那麼因為所有數都有指數，故

$$\sum_{d \mid p-1} \psi(d) = p - 1.$$

並且由已知的 $\delta_m(g^k) = (p-1)/\gcd(p-1,k)$，我們最後必定要有 $\psi(d) = \phi(d)$，所以現在的問題是如何證明這個等式。

為此考慮任意指數為 d 的數 a，那麼易看出

$$a, a^2, a^3, \ldots, a^d$$

都滿足 $x^d \equiv 1 \pmod{p}$，並且他們在 mod p 下又兩兩相異，然後由性質 (2) 可以知道這之中恰有 $\phi(d)$ 個數個指數為 d。那會不會有指數也為 d 的數不能被 a 的冪次生成呢？等等！前面已給出了 $x^d \equiv 1 \pmod{p}$ 的 d 個解，如果在 mod p 下我們有類似代數基本定理的東東不就代表指數為 d 的數一定在裡面嗎！所以猜測：

定理 3.6 (Lagrange 定理) 設 $\deg(f(x)) = d$，且 $f(x)$ 在模 p 下不為零多項式，則使 $f(x) \equiv 0 \pmod{p}$ 的 x 至多有 d 個 (模 p 下)。

證明： 首先 $d = 1$ 易證。假設 $d = D$ 時成立，則 $d = D+1$ 時：若 $f(x) \equiv 0 \pmod{p}$ 無解則成立。若 $f(x) \equiv 0 \pmod{p}$ 有解 a，我們知道有 $f(x) \equiv (x-a)r(x) \pmod{p}$，並且 $\deg(r(x)) = D$，由歸納假設知此時命題亦成立。 □

到目前為止已經證明了：如果 $\psi(d) \neq 0$，那麼 $\psi(d) = \phi(d)$。所以剩下的就是要問：會不會有 $\psi(d) = 0$ 呢？重新回頭審視每個式子後，會發現那是不可能的！因為我們有

$$\sum_{d|p-1} \psi(d) = p - 1 = \sum_{d|p-1} \phi(d).$$

然後使得 $\psi(d) \neq 0$ 必定滿足 $\psi(d) = \phi(d)$，所以 $\psi(d) = 0$ 會造成

$$\sum_{d|p-1} \psi(d) < \sum_{d|p-1} \phi(d).$$

矛盾！因此我們證完所有質數都有原根了！

好的，接下來手算一下，你就可以合理的猜測：所有有原根的數必定型如 $1, 2, 4, p^n, 2p^n$。其他的數不存在原根就留給讀者自行練習，我們這邊給出如何從模為質數的原根找出模為質數次方的原根的方法，事實上也只是 Hensel 引理的一點應用而已：

重要性質——★ 取 p 為一奇質數，且 $a \neq \pm 1$ 不被 p 整除。設 $\delta_p(a) = d$，而 k_0 是使得 $a^d \equiv 1 \pmod{p^{k_0}}$ 成立的最大的正整數，則

$$\delta_{p^k}(a) = \begin{cases} d & , \quad k \leq k_0 \\ dp^{k-k_0} & , \quad k > k_0 \end{cases}$$

證明： 設 $a^d = 1 + p^{k_0}u_0$ (其中 $(u_0, p) = 1$)。

當 $k > k_0$ 時，我們可以簡單的用數學歸納法證明對任意 $j \geq 0$，總存在整數 u_j 使得

$$a^{dp^j} = 1 + p^{j+k_0}u_j \quad \text{且} \quad (u_j, p) = 1.$$

接著令 $j = k - k_0$，並假設 $\delta_{p^{k-1}}(a) = dp^{j-1}$，由

$$a^{\delta_{p^k}(a)} \equiv 1 \pmod{p^k}.$$

可以有

$$a^{\delta_{p^k}(a)} \equiv 1 \pmod{p^{k-1}}.$$

因此 $dp^{j-1} \mid \delta_{p^k}(a)$。又

$$a^{dp^{j-1}} = 1 + p^{k-1}u_{j-1} \not\equiv 1 \pmod{p^k}.$$
$$a^{dp^j} = 1 + p^k u_j \equiv 1 \pmod{p^k}.$$

因此 $\delta_{p^k}(a) \mid dp^j$，但 $\delta_{p^k}(a) \nmid dp^{j-1}$，所以 $\delta_{p^k}(a) = dp^j$。 □

有了這個引理，就可以馬上推出：

定理 3.7 *若 p 為一奇質數，且 g 為模 p 的原根，則對所有正整數 k，g 或 $g+p$ 中有一數為模 p^k 的原根，也有一數是模 $2p^k$ 的原根。*

3.4 Carmichael 函數

上面提了一些關於 order 函數的性質，而這是一種讓我們更了解某一數在剩餘系裡所扮演角色的重要指標，但是我們也看到了，一般要求出某數的 order 根本沒有好的方法，不會有所謂的公式存在，這對於想再深入探討其他性質時是不利的。或許我們該把目標降低一點，不要妄想能夠做出所有特例的性質，有沒有一些東東是剩餘系裡所有的數都會滿足的性質呢？

定義 3.4 *對任意正整數 m，記 $\lambda(m)$ 為使得同餘式 $x^d \equiv 1 \pmod{m}$ 對所有 $(x,m)=1$ 都成立的最小正整數。$\lambda(m)$ 即是所謂的 Carmichael 函數。*

當你像江泓先生一樣盡力把眼睛張到最大時可能會發現，這和 order 函數的意義非常像，所以很有可能他也會滿足 order 函數的某些性質。首先易看出這個 $\lambda(m)$ 其實就是所有滿足 $(x,m)=1$ 的 x 對 m 的指數的最小公倍數。注意到，我們不需要依次知道每個 x 對 m 的指數，仍然可能求出他們最小公倍數。

假設今天你代 $m=15$，你想要求出所有滿足 $(x,15)=1$ 的 x 對 15 的指數的最小公倍數，然而仔細想一下，由中國剩餘定理我們似乎能把它看成「所有滿足 $(x,3)=1$ 的 x 對 3 的指數的最小公倍數」以及「所有滿足 $(x,5)=1$ 的 x 對 5 的指數的最小公倍數」這兩個數再求一次最小公倍數。也就是說，我們應該要有：

引理 3.1 *對任意互質的 a,b，有 $\lambda(ab) = \mathrm{lcm}[\lambda(a), \lambda(b)]$.*

證明： 設 $\lambda(a)=d_1$，$\lambda(b)=d_2$，$\lambda(ab)=d$。由定義知 $x^d \equiv 1 \pmod{ab}$ 成立，這代表

$$x^d \equiv 1 \pmod{a} \text{ 且 } x^d \equiv 1 \pmod{b}$$

同時成立。由 order 的性質有 $d_1 \mid d$ 且 $d_2 \mid d$，因此 $\mathrm{lcm}[d_1,d_2] \mid d$。而又有

$$x^{\mathrm{lcm}[d_1,d_2]} \equiv 1 \pmod{a} \text{ 且 } x^{\mathrm{lcm}[d_1,d_2]} \equiv 1 \pmod{b}$$

同時成立。因此 $x^{\mathrm{lcm}[d_1,d_2]} \equiv 1 \pmod{ab}$，所以也有 $d \mid \mathrm{lcm}[d_1,d_2]$。綜上 $d = \mathrm{lcm}[d_1,d_2]$.
□

這引理他告訴我們說，假設今天 m 的質因數分解式叫作 $m = p_1^{k_1} \cdots p_t^{k_t}$，那麼只需求出 $\lambda(p_i^{k_i})$ 即可！更甚者，我們又已經知道如果數 y 形如 $2, 4, p^k, 2p^k$ (p為奇質數)，那麼就會有原根，所以這時候一定會有 $\lambda(y) = \phi(y)$！最終問題被歸結成要求出 $\lambda(2^k)$！

你代了一下，發現 $\lambda(8) = 2$，$\lambda(16) = 4$，$\lambda(32) = 8$，所以很快就猜到 $\lambda(2^k) = 2^{k-2}$，但是這看起來好像不好證。現在回憶一下我們學會的工具，可能有個叫做 Hensel 提升引理的，它又好像在處理模為質數次方的指數同餘方程上很好用，所以嘗試代入這個引理的想法來證明：

引理 3.2 令 $k \geq 3$，則 $\lambda(2^k) = 2^{k-2}$.

證明： 首先觀察到對所有奇數 x 都有 $x^2 \equiv 1 \pmod 8$。
用數學歸納法，我們可以假設 $x^{2^{k-2}} \equiv 1 \pmod{2^k}$ 對所有奇數 x 及某個 k 恆成立。因此

$$x^{2^{k-2}} \equiv 1 \pmod{2^{k+1}} \quad 或 \quad x^{2^{k-2}} \equiv 1 + 2^k \pmod{2^{k+1}}.$$

而不管是哪種情況，都有 $x^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$，所以 $\lambda(2^k) \leq 2^{k-2}$.
反過來取 x 是滿足 $\delta_{16}(x) = 4$ 的整數 (取 x 模 8 餘 3 或 5 即可)，也有 $\delta_8(x) = 2$。
用數學歸納法，我們可以假設 $\delta_{2^k}(x) = 2^{k-2}$ 且 $\delta_{2^{k+1}}(x) = 2^{k-1}$ 對某個 k 成立。因此有 $x^{2^{k-2}} \equiv 1 \pmod{2^k}$ 以及 $x^{2^{k-2}} \not\equiv 1 \pmod{2^{k+1}}$，所以

$$x^{2^{k-2}} \equiv 1 + 2^k \pmod{2^{k+1}}.$$

因此只有

$$x^{2^{k-2}} \equiv 1 + 2^k \pmod{2^{k+2}} \quad 或 \quad x^{2^{k-2}} \equiv 1 + 2^k + 2^{k+1} \pmod{2^{k+2}}.$$

不管是哪種情況都有 $x^{2^{k-1}} \equiv 1 + 2^{k+1} \not\equiv 1 \pmod{2^{k+2}}$。所以 $\delta_{2^{k+2}}(x) > 2^{k-1}$，但又有 $\delta_{2^{k+2}}(x) \mid \phi(2^{k+2}) = 2^{k+1}$，因此 $\delta_{2^{k+2}}(x) = 2^k$ 或 2^{k+1}。注意到 $\delta_{2^{k+2}}(x)$ 不能超過 $\lambda(2^{k+2})$，而我們已知 $\lambda(2^{k+2}) \leq 2^k$，故 $\lambda(2^{k+2}) = 2^k$。 □

至此，我們已經解出了這函數的一般公式，整理如下。另外有兩個性質留作習題。

定理 3.8 對任一大於 1 的正整數 m 有

$$\lambda(m) = \begin{cases} \phi(m) & , \quad m = 2, 4, p^k, 2p^k \ (p\text{為奇質數}) \\ 2^{k-2} & , \quad m = 2^k \ (k \geq 3) \\ \operatorname{lcm}[\lambda(p_1^{k_1}), \cdots, \lambda(p_t^{k_t})] & , \quad m = p_1^{k_1} \cdots p_t^{k_t} \end{cases}$$

例題 4.1: AoPS 題

試找出所有質數數對 (p, q)，使得

$$\frac{(7^p - 2^p)(7^q - 2^q)}{pq}$$

是一個整數。

證明： 首先當至少有一個質數是 5 時 (不失一般性設 $p=5$)：如果 $q \mid 7^q - 2^q$，那麼由 Fermat 定理有 $q \mid 7-2=5$，此時也要有 $q=5$。如果 $q \mid 7^5 - 2^5$，那麼計算知 $q=11$ 或 61.

再來當兩個質數都大於 5 時：如果 $q \mid 7^q - 2^q$，那麼由 Fermat 定理亦有 $q \mid 7-2=5$，這是不可能的，因此 $q \mid 7^p - 2^p$，所以 $(7\cdot 2^{-1})^p \equiv 1 \pmod q$，這代表 $\delta_q(7\cdot 2^{-1}) = 1$ 或 p.

如果 $\delta_q(7\cdot 2^{-1}) = 1$，那麼 $7\cdot 2^{-1} \equiv 1 \pmod q$，即是說 $7 \equiv 2 \pmod q$，這是不可能的。因此 $\delta_q(7\cdot 2^{-1}) = p$。此時 $p \mid q-1$。同理 $q \mid p-1$。而這蘊含了 $p \le q-1 \le p-2$，矛盾。

綜上只有 $(p,q) = (5,5),(5,11),(5,61),(11,5),(61,5)$。 □

例題 4.2: 很久以前的題

假設正整數 $k \ge 2, n_1, n_2, \ldots, n_k$ 滿足：

$$n_2 \mid 2^{n_1} - 1, n_3 \mid 2^{n_2} - 1, \ldots, n_k \mid 2^{n_{k-1}} - 1, n_1 \mid 2^{n_k} - 1.$$

試證 $n_1 = n_2 = \cdots = n_k = 1$.

證明： 若存在 $(n_1, n_2, \ldots, n_k)$ 滿足整除關係但不全為 1，則顯然全不為 1。因此可假設每個 n_i 都有質因數，並且設 n_i 的最小質因數為 p_i，而 $\delta_{p_i}(2) = a_i > 1$。由

$$p_i \mid n_i \mid 2^{n_{i-1}} - 1.$$

我們可以得到：

$$a_i \mid n_{i-1} \quad \text{且} \quad a_i \mid p_i - 1.$$

所以 n_{i-1} 的最小質因數小於 n_i 的最小質因數，這產生了矛盾 (繞一圈回來就爆了)。 □

例題 4.3: APMO 2012

試找出所有數對 (p,n)，其中 p 是質數，n 是正整數，使得

$$\frac{n^p + 1}{p^n + 1}$$

是一個整數。

證明： 首先 $p=2$ 時易驗證只有 $n=2,4$ 是解。當 $p\geq 3$ 時由 $n^p+1\geq p^n+1$ 我們可以得到 $p\geq n$，並且此時還有分母是偶數，所以分子也要是偶數，就是說 n 是奇數。現任取 $p+1$ 的某質因數最大次方 q^k，會有：

$$q^k \mid\mid p+1 \mid\mid p^n+1.$$

所以必有 $q^k \mid n^p+1$，故 $q^k \mid n^{2p}-1$，得到 $\delta_{q^k}(n)=2$ 或 $2p$。但是當 $\delta_{q^k}(n)=2p$ 時，會有：

$$2p \mid \phi(q^k).$$

所以會有

$$2p \leq q^{k-1}(q-1) < q^k < p+1.$$

矛盾。因此必定有 $\delta_{q^k}(n)=2$，所以

$$n\equiv -1 \pmod{q^k} \quad (\text{對}p+1\text{的任質因數最大次方})$$

這等價於 $n\equiv -1 \pmod{p+1}$，而這綜合 $p\geq n$ 會得到 $n=p$.

綜上，所有解為 $(2,4),(p,p)$. □

例題 4.4: Fibonacci 原根

這個例題來自 Daniel Shanks, *Fibonacci Primitive Roots,* Fibon. Quart., Vol. 10, 1972, pp. 163-181.。從前有個數學家，他叫 Daniel Shanks。有一天他心血來潮的研究了如下的命題：如果質數 p 有一個原根 g 滿足：

$$g^2\equiv g+1 \pmod{p}.$$

則稱這個原根為 Fibonacci primitive root (簡稱 F.P.R)。在他 1972 年的論文中，以計算機的幫助，找到了 200 以下有 F.P.R 的質數，並且歸納出以下結果：

1. 除了 $p=5$ 之外，每個有 F.P.R 的質數都型如 $10k\pm 1$。但不是每個型如 $10k\pm 1$ 的質數都有 F.P.R。
2. 除了 $p=5$ 之外，如果有 F.P.R，那麼滿足 $0<g<p$ 的數量剛好是 1 個或 2 個，分別對應到 $p\equiv 3 \pmod 4$ 和 $p\equiv 1 \pmod 4$ 的情況。

證明： 首先不管怎樣，同餘方程

$$x^2\equiv x+1 \pmod{p}.$$

一定要有解。而解剛好是 $x_1=(1+\sqrt{5})/2$, $x_2=(1-\sqrt{5})/2$，因此 $\sqrt{5}$ 在 mod p 下要存在，這代表 $p=10k\pm 1$，這就證完 1.。

等等！你剛剛在說什麼?! 什麼叫「$\sqrt{5}$ 在 mod p 下要存在」? 好的，我們回憶一下那個同餘方程的根到底是怎麼解出來的，首先有

$$\begin{aligned} \Rightarrow \quad 4x^2 - 4x &\equiv 4 \pmod{p}. \\ \Rightarrow \quad (2x-1)^2 &\equiv 5 \pmod{p}. \\ \Rightarrow \quad 2x - 1 &\equiv \pm\sqrt{5} \pmod{p}. \end{aligned}$$

注意到第二式推第三式是怎麼來的，這代表說在 mod p 之下 5 是他的二次剩餘，因此 $p = 10k \pm 1$。而此時我們以 $\sqrt{5}$ 這符號代表在 mod p 之下扮演某個平方之後等於 5 的數。丫內瞭改嘸？

而從他們對應到的二次方程還可以有更多資訊。首先注意到我們已把兩個解表示出來，假設他們是 g_1, g_2，其中 g_1 是 F.P.R 。又由根與係數的關係，會有 $g_1 g_2 \equiv -1 \pmod{p}$，因此 $g_2^m \equiv (-1)^m g_1^{-m} \pmod{p}$，可以看出這就證完了 2.。 □

評論 3.1 讀者有興趣的還可以練習證明：如果 g 是 F.P.R，那 $g-1$ 也是原根。特別當 $p \equiv 3 \pmod{4}$ 時 $g-2$ 也是原根。

Problem set

P1. Let $n \geq 2$ be an integer. Prove that if n divides $3^n + 4^n$, then 7 divides n.

P2. If p is a prime and n an integer with $1 < n \leq p$, then

$$\phi\left(\sum_{k=0}^{p-1} n^k\right) \equiv 0 \pmod{p}.$$

P3. Positive integers m, k are given, and $p = 2^{2^m} + 1$ is a prime. Prove that $\delta_{p^{k+1}}(2) = 2^{m+1}p^k$.

P4. Prove that for all positive integer m, one can always find x such that $\delta_m(x) = \lambda(m)$.

P5. Given positive integers m and d, prove that there exists integer x satisfying $\delta_m(x) = d$ if and only if $d \mid \lambda(m)$.

P6. ISL 2006 N5

Prove that the equation

$$\frac{x^7 - 1}{x - 1} = y^5 - 1$$

doesn't have integer solution.

P7. Suppose a, b, p are given. Prove that the exponential congruence

$$a^k \equiv b \pmod{p^k}$$

has only finitely many solutions k.

P8. Let $N > 1$ be an odd integer. Show that the congruence $a^{N-1} \equiv -1 \pmod{N}$ is impossible.

P9. Let $k \geq 2$ be an integer. Prove that there are infinitely many composite numbers n with the property that $n \mid a^{n-k} - 1$ for all integers a relatively prime to n.

P10. Find all integers $k \geq 2$ such that for all integers $n \geq 2$, n does not divide the greatest odd divisor of $k^n + 1$.

P11. Let p be a prime number and let $a_1, a_2, \ldots, a_{p-2}$ be positive integers such that p does not divide a_k nor $a_k^k - 1$ for any k. Prove that for any $1 < c \leq p - 1$, one can find some of the a_i so that their product is congruent to c modulo p.

P12. USA TST 2003

Find all ordered triples of primes (p, q, r) such that

$$p \mid q^r + 1, \quad q \mid r^p + 1, \quad r \mid p^q + 1.$$

P13. Italy TST 2003

For each positive integer n, let A_n denote the set of positive integers $a \leq n$ such that $n \mid a^n + 1$.

(a) Find all n for which A_n is nonempty.

(b) Find all n for which $|A_n|$ is even and nonzero.

(c) Is there an n with $|A_n| = 130$?

P14. ISL 2001 N4

Let $p \geq 5$ be a prime number. Prove that there exists an integer a with $1 \leq a \leq p-2$ such that neither $a^{p-1} - 1$ nor $(a+1)^{p-1} - 1$ is divisible by p^2.

P15. ISL 2005 N4

Find all positive integers n such that there exists a unique integer a such that $0 \leq a < n!$ with the following property:

$$n! \mid a^n + 1.$$

P16. ISL 2012 N6

Let x and y be positive integers. If $x^{2^n} - 1$ is divisible by $2^n y + 1$ for every positive integer n, prove that $x = 1$.

P17. ISL 2003 N6

Let p be a prime number. Prove that there exists a prime number q such that for every integer n, the number $n^p - p$ is not divisible by q.

P18. China TST 2005

For every positive integer n, define the *Fermat number* $F_n = 2^{2^n} + 1$.Let $n \geq 3$, and let q be a prime divisor of F_n, then prove that F_n has a prime factor which is larger than $2^{n+2}(n+1)$.

P19. Bulgaria TST 2015

Let $p > 10^9$ be a prime number such that $4p+1$ is also prime. Prove that the decimal expansion of $\frac{1}{4p+1}$ contains all the digits $0, 1, \ldots, 9$.

3.5 補充教材——分布

上面已簡介了關於二次剩餘及原根的一點性質，很自然的，我們會想要問這些數是怎麼分布的。例如說，模 101 的原根中有幾個數連續啊、1∼50 及 51∼101 裡面誰的二次剩餘比較多啊、等等。

首先要了解的是：為什麼這些問題是有意義的？ 筆者當初高中時在講這篇講義的這一小節時，就有人 (他的名字可能曾出現在前面) 問了：「這些東西在 $\mathbb{F}_p$ 裡面明明是用乘法的意義去定義的，怎麼會去研究它們對於加法的性質？」這是一個非常棒的問題，筆者認為原因就如同為什麼要研究 abc 猜想一樣，因為這命題象徵的是一種離散程度的概念。也就是說，給定一組基底，它們在某種運算 (乘法) 與在另一種運算 (加法) 下的差別會不會是有界的？當然這個敘述可能還是挺抽象，但由於我們目前的預備知識還不多沒辦法進一步說明，讀者如果繼續看下去會在這一部的整係數多項式一章看到一些例子說明。

常常問自己為什麼要研究某某東西、為什麼又要如此定義某某？這些問題都仍讓自己的數學能力上升的更高的境界，這也是筆者在《集合中的組合數學》一文裡想讓讀者做到的事。在這個章節中我們主要會以解問題的方式讓各位思考這些問題背後的結構，也順便讓各位體會前面提到的那些性質及定理是如何使用的，希望大家也能自己動手算。另外如果對這裡的東西有興趣想了解更多，可以自行 google 一些關鍵字，預祝大家都有所收穫。

研究 5.1

如果 n 不是完全平方數，那麼是否一定存在質數 p，使得 n 不是模 p 的二次剩餘？

Step$_1$. 首先來分析這個問題：如果說 n 是完全平方數，那麼顯然對所有質數 p，n 都是模 p 的二次剩餘。所以我們自然會問：這是不是給出了一個平方數的判別法則？

Step$_2$. 然後來看這個問題的合理性。由於每次碰到與整數相關的問題，大致上都可以把它丟進質數或質數冪次的情況做處理 (背後更深的理論叫做 local-global principle)，然後我們在之前也證明了，一個數是模 p^n 的二次剩餘等價於是模 p 的二次剩餘，因此只需考慮質數的情況。

Step**3.** 了解問題所在後，我們開始做這題。首先很自然會想這樣的 p 一定存在，畢竟平方數跟其他一般正整數本質上有很大的不同嘛，怎麼可能表現出一樣的性質呢。問題就在於如何找出這樣的 p。

Step**4.** 首先列式出來，我們的目標是找到質數 p 使得

$$\left(\frac{n}{p}\right) = -1.$$

由 Legendre's symbol 的性質自然會想到，作 n 的質因數分解，由於他不是平方數，所以至少存在某個質數的冪次是奇數。首先把偶數次全都消光光，可以寫成

$$\left(\frac{q_1 q_2 \cdots q_m}{p}\right) = -1. \tag{3.1}$$

其中 $n = q_1 q_2 \cdots q_m A^2$。由於我們已知 q_i，欲求 p，所以上式中 p 在分母的位置很難處理，可是由二次互反律會發現，如果我們先取 $p = 4k+1$，那麼欲求就是

$$\left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\cdots\left(\frac{p}{q_m}\right) = -1.$$

現在希望某個值是 1，其他都是 -1，而這顯然是取得到的！因為對任意質數總有二次剩餘及二次非剩餘。假設 a_1 是模 q_1 的二次剩餘，$a_2, \ldots, a_m$ 分別是模 $q_2, \ldots, q_m$ 的二次非剩餘，由中國剩餘定理及 Dirichlet 定理可取到質數 p 使得 $p \equiv a_i \pmod{q_i}$，以及 $p \equiv 1 \pmod 4$，因此式 (1) 成立！

Step**5.** 上面的證明還有一點小問題：如果 q_i 中有 2 就不能用二次互反律了，不過也不是什麼大不了的，反正還是可以取到 p 讓 $(2/p) = -1$，以及其他的值都是 1。然後，顯然類似的方法可以證明：對任意正整數 n，一定存在質數 p，使得 n 是模 p 的二次剩餘。

有了這樣的結果後，自然會問：這命題能否推廣到高次剩餘呢? 也就是說，如果 n 不是 k 次方數，那麼是否一定存在質數 p，使得 n 不是模 p 的 k 次剩餘? 事實上這命題的特例被當成是 2007 年 IMO 的預選題之一：

Problem.(ISL 2007 N2) 令 $b, n > 1$ 是正整數，假設對所有 $k > 1$ 總存在整數 a_k 使得 $b - a_k^n$ 被 k 給整除，試證 b 是 n 次方數。

在 AoPS 上有人說背後的理論為 **Schinzel's Theorem**：令 $b, n > 1$ 是正整數，假設對所有質數 p 總存在整數 a_p 使得 $b - a_p^n$ 被 p 給整除，那麼：
(1) 如果 $8 \nmid n$，則 b 是 n 次方數。　　(2) 如果 $8 \mid n$，則 b 是 $n/2$ 次方數。

然而可以看到這個定理稍微弱化了一些題目。在第二部的分布密度一章中，將帶領讀者用 Gallagher 篩法證明另一個類似的命題：假設正整數 a, b 滿足對所有質數次方 q 都存在正整數 v_q 使得 $b \equiv a^{v_q} \pmod q$，那麼存在正整數 v 使得 $b = a^v$。這種關於 order 的問題也許你會想要從代數數論的角度來解釋，但其實基本上都會變成很難的猜想，偶爾有人做出來變定理，總之絕對不是高中生做得出來的，請放棄這條路。(另外在整係數

多項式一章的補充教材研究 6.3 裡，筆者用了 abc 猜想來研究另一道類似的題目，讀者也可以參考看看。)

我們當然不會滿足於此，類似的命題要多少就可以問多少。在這裡給出最後一個留給讀者思考的問題：如果一個整係數多項式 f 滿足對所有正整數 n 以及質數 p 都有 $f(n)$ 是模 p 的二次剩餘，那麼 f 本身一定是多項式的平方嗎？

研究 5.2

給定整數 n，能不能找到質數 p 使得 $1, 2, \ldots, n$ 都是模 p 的二次剩餘？

Step**1.** 這問題的基礎是，我們從小質數開始試，會發現好像二次剩餘的數分布得不是很有規律，於是會想問說：連續的二次剩餘到底可以排多長？

Step**2.** 這個問題是簡單的，假設 $1, 2, \ldots, n$ 的質數是 $q_1, \ldots, q_m$，由上一題的取法我們可以取到質數 p 使得 $q_1, \ldots, q_m$ 全都是模 p 的二次剩餘，然後由 Legendre's symbol 的性質就知道此時 $1, 2, \ldots, n$ 全都是模 p 的二次剩餘了！

Step**3.** 現在你可能會問：如果 $1, 2, \ldots, n$ 都是模 p 的二次剩餘，那這些 p 有什麼性質? 例如說比例 n/p 可以有多大？

Step**4.** 首先顯然 n/p 不可能超過 $1/2$，因為二次剩餘的個數以及二次非剩餘的個數是一樣多的。然而仔細想一下會發現不用說 $1/2$ 了，大概更小一點的比例都到不了，因為兩個二次剩餘的乘積還會是二次剩餘，所以隨便乘一乘都很容易讓二次剩餘的比例超過 $1/2$ 而產生矛盾，因此應有更好的估計。事實上 Gauss 證明出以下：

Theorem. 令 $N_{\min}(p)$ 表示模 p 的最小的二次非剩餘，那麼

$$N_{\min}(p) < p^{\frac{1}{2\sqrt{e}}} (\log p)^2.$$

Step**5.** 我們已證出了：給定整數 n，總能找到質數 p 使得模 p 下有至少 n 個連續的二次剩餘。然而，當我們改問：給定整數 n，能不能找到質數 p 使得模 p 下有至少 n 個連續的二次非剩餘，或是 n 個連續的原根？顯然問題變困難許多，因為兩個二次非剩餘 (原根) 乘積會變成二次剩餘 (非原根)，所以當有一些數是二次非剩餘 (原根) 時，便會限制住其他數的性質。

Step**6.** 甚至只問：給定整數 n，是否總存在數 M，使得對所有質數 $p \geq M$，模 p 下有至少 n 個連續的二次剩餘？這問題都是很難的。先作一些定義：

定義 3.5 給定 l，令 p 是質數，定義 $r = r(k, l, p)$ 是使得

$$r,\ r+1,\ r+2, \ldots,\ r+l-1.$$

在模 p 下都是 k 次剩餘的最小正整數。然後自然會問：隨著 p 變大，那這些 r 會不會有個上界，還是趨近於無限大呢？因此再定義

$$\Lambda(k,l) = \limsup_{p\to\infty} r(k,l,p).$$

如讀者不知道 $\limsup$ 的定義，可理解為當有一個實數數列 (a_n) 時，$\limsup_{n\to\infty} a_n$ 的定義是使對所有足夠大的 n 都有 a_n 小於等於該實數的最小者。例如 $\limsup_{n\to\infty}(-1)^n = 1$.

Step**7**. 我們馬上會發現某些 $\Lambda(k,l)$ 是有限的，例如 $\Lambda(2,2) = 9$。事實上可以考慮三對數：(1,2), (4,5), (9,10)。首先 1, 4, 9 都一定是二次剩餘，再來由於 $2\cdot 5 = 10$，因此 2, 5, 10 之中至少有一數是二次剩餘，故 $\Lambda(2,2) \le 9$，而易證明有無窮多個質數使得 (1,2), (4,5) 都不全是二次剩餘，故 $\Lambda(2,2) = 9$.

Step**8**. 另外還有人定義 $r = \Omega(a,b)$ 是使得 $r, r+a, r+b$ 在模任意大質數 p 下都是二次剩餘的最小的正整數。讀者有興趣可以研究看看，甚至推到 $\Omega(a,b,c,\dots)$ 的情況。作為一個例子，請試著證明 $\Omega(5,23) = 16$.

Step**9**. 我們繼續研究 Λ 函數的性質。上面已證明了 $\Lambda(2,2) = 9$，那 $\Lambda(2,3)$、$\Lambda(2,4)$ 之後呢? 很不幸的，我們已經有 $\Lambda(2,3) = \infty$ (另外還可以證明 $\Lambda(k,4) = \infty$)：假設 $\Lambda(2,3) = N$ 是有限的，也就是說對任意夠大的質數 p，數對 $(1,2,3), (2,3,4), \dots, (N, N+1, N+2)$ 中至少有一組全都是完全平方數。現在我們希望找到某個質數 p 產生矛盾，假設 $1, 2, \dots, N$ 中的質數是 $q_1, \dots, q_m$，由**研究 5.1** 的取法可找到質數 p 使得

$$\left(\frac{q_i}{p}\right) \equiv q_i \pmod 3, \quad \forall q_i \neq 3.$$

此時由 Legendre's symbol 的性質會知道必有

$$\left(\frac{m}{p}\right) \equiv m \pmod 3, \quad \forall m \not\equiv 0 \pmod 3,\ m \le N.$$

此時對所有數對 $(a, a+1, a+2)$，由於當中至少有一數 $\equiv 2 \pmod 3$，所以此數對必不全是二次剩餘，矛盾！

上面還留了非常多沒有解的問題，筆者希望有興趣的讀者能夠自己繼續研究 (或是做專題？)，思考的過程中讀者可能會用到下面這個定理 (Szemerédi 定理)：給定 m 以及 $0 < \delta < 1$，那麼對所有夠大的數 L，當我們取 $\{1, 2, \dots, L\}$ 裡至少 δL 個元素的子集合 A 時，A 中一定找得到長度為 m 的算術數列。

評論 3.2 前面提到關於連續二次剩餘以及二次非剩餘長度的問題，已有相當好的結果。Burgess 在 1963 年證明了：令 H 表示模 p 下連續二次 (非) 剩餘的最長長度，那麼 $H = O(p^{1/4}\log p)$。而 Hummel 則在 2003 年用完全初等的方法證明了：連續二次非剩餘的最長長度 $< \sqrt{p}$，只有 $p = 13$ 這個例外。另外在第二部的 N 次剩餘一章中，將會介紹一個估計 $N_{\min}(p)$ 的方法。

最後是關於原根的分布，我想讀者大概可以猜到我們期待會有什麼樣的結論，只是這個東西還是一個猜想 (如果想更深入了解的讀者可以參考這篇論文 D. R. Heath-Brown, *Artins conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) 37 (1986), no. 145, 27–38. 裡面證明了 Artin 猜想裡某些很有趣的特例)：

猜想 3.1 (Artin 猜想) 令 $g \neq \pm 1$，且無平方因子，那麼存在無窮多個質數 p 以 g 為原根。

研究 5.3

上面已經看到一些關於二次剩餘及非剩餘的分布，不過都是對「足夠大」的質數才能夠成立，那有沒有一些分布的性質對所有質數都成立呢？

Step$_1$. 一個自然的問題是，我們上面關注的是連續的二次 (非) 剩餘可以有多長，所以估計值可能對小的情況不成立，那如果我們僅僅關注連續的二次剩餘會有幾對呢？更一般的，定義：

定義 3.6 令 p 是奇質數，定義集合

$$A_{ij} = \{k \in \{1, 2, \ldots, p-2\} \mid \left(\frac{k}{p}\right) = (-1)^i, \ \left(\frac{k+1}{p}\right) = (-1)^j\}.$$

並且令 $\alpha_{ij} = |A_{ij}|$.

比方說對 $p = 17$，他的剩餘系為

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}.$$

(其中藍色部分為二次剩餘)。那麼 $A_{00} = \{1, 8, 15\}$, $A_{01} = \{2, 4, 9, 13\}$, $A_{10} = \{3, 7, 12, 14\}$, $A_{11} = \{5, 6, 10, 11\}$.

Step$_2$. 好的，在上面的例子中，我們可以看到四種集合的元素個數幾乎是一樣多的。一般性的，該如何記數每個集合的大小？比方說我們要先計算 α_{01}，事實上就是求

$$\sum_{k\text{是二次剩餘}, k+1\text{是二次非剩餘}} 1.$$

其中 k 跑遍 $1, \ldots, p-2$。因此，我們希望找到一個相關的函數 f，使得

$$f(k) = \begin{cases} 1 & , \ k \text{ 是二次剩餘}, k+1 \text{ 是二次非剩餘} \\ 0 & , \ \text{其他情況} \end{cases}$$

如此，我們就可以變成改求

$$\sum_{k=1}^{p-2} f(k).$$

這種看起來較容易的型式。

Step**3.** 現在問題是如何找到這樣的函數 f。思考一下，我們現在對二次剩餘最好用的了解就是 Legendre's symbol ，於是我們希望的東西就是

$$f(k)=\begin{cases}1 & , \ \left(\frac{x^2+1}{p}\right)=-1, \text{ 其中 } k\equiv x^2 \pmod p\\ 0 & , \ \text{其他情況}\end{cases}$$

這樣的函數超好找，我們只要令：

$$f(k)=\begin{cases}\frac{1-\left(\frac{x^2+1}{p}\right)}{2} & , \ k\equiv x^2 \pmod p\\ 0 & , \ \text{其他情況}\end{cases}$$

Step**4.** 現在我們已經找到了這樣的函數 f，代回去欲求就變為

$$\frac{1}{2}\sum_{x=1}^{\frac{p-1}{2}}\left(1-\left(\frac{x^2+1}{p}\right)\right).$$

(然而，這邊要注意的是原本我們求和是求到 $k=p-2$，但當 -1 是模 p 的二次剩餘時上式會求到 $k=p-1$，所以這邊我們還要分 p 模 4 的情況分開討論)。簡單看出，事實上我們就是要求

$$\sum_{x=1}^{p-1}\left(\frac{x^2+1}{p}\right). \tag{3.2}$$

Step**5.** 上式感覺沒什麼方法可以算了，Legendre's symbol 到底還可以有什麼性質呢？現在回想一下當初 Legendre's symbol 為什麼要這樣定義。啊！其實 Euler's Criterion 才是更基本的結構吧。於是帶入式子裡，變成

$$\sum_{x=1}^{p-1}\left(\frac{x^2+1}{p}\right)\equiv\sum_{x=1}^{p-1}(x^2+1)^{\frac{p-1}{2}} \pmod p. \tag{3.3}$$

然後我們利用二項式展開以及基本性質：

$$\sum_{x=1}^{p-1}x^n\equiv\begin{cases}-1 \pmod p & , \ \text{如果 } p-1\mid n\\ 0 \pmod p & , \ \text{其他情況}\end{cases}$$

(這可以用原根來證)。代回去便得到式 (2)$\equiv -1 \pmod p$，而顯然又 $<p$，因此式 (2)$=-1$。至此，我們已求出了 α_{01}！

Step**6.** 最後，α_{00} 可以直接計算得到 (事實上也可以直接推到 α_{01}，而不用上面那種麻煩的計算方式)，α_{10} 可用這方法做出，α_{11} 則是可以用扣的作出來。因此我們可以計算出所有 α_{ij} 的值！

⊡ **Case I.** 若 $p\equiv 1 \pmod 4$，則

$$\alpha_{00}=\frac{p-5}{4},\ \alpha_{01}=\alpha_{10}=\alpha_{11}=\frac{p-1}{4}.$$

⊡ **Case II.** 若 $p\equiv 3 \pmod 4$，則

$$\alpha_{01}=\frac{p+1}{4},\ \alpha_{00}=\alpha_{10}=\alpha_{11}=\frac{p-3}{4}.$$

評論 3.3 如同最後一步驟說的，我們可以不用這種手段變計算出 α_{ij}，這邊只是要介紹一種求和方法。這種另求函數 f 的手法也用在證明 Chevalley-Waring Theorem, Hermite's Criterion 等等，更一般地，這個方法是用來找有限體裡面指數方程式解數的一種工具，詳情可見第二部 Dirichlet 特徵一章。讀者可以試著做這題 (Iran TST 2016)：令 $p \neq 13$ 是形如 $8k+5$ 的質數，而且 -39 不是模 p 的二次剩餘，證明

$$x_1^4 + x_2^4 + x_3^4 + x_4^4 \equiv 0 \pmod{p}$$

有 $p \nmid x_1x_2x_3x_4$ 的整數解。

Problem set

P1. Iran MO 2013

Let $p = 3k+1$ is a prime number. For each $m \in \mathbb{Z}_p$, define function L as follow:

$$L(m) = \sum_{x \in \mathbb{Z}_p} \left(\frac{x(x^3+m)}{p} \right).$$

(a) (5 points) Denote ${\mathbb{Z}_p}^* = \mathbb{Z}_p \setminus \{0\}$. For every $m \in \mathbb{Z}_p$ and $t \in {\mathbb{Z}_p}^*$ prove that $L(m) = L(mt^3)$.

(b) (7 points) Prove that there is a partition of ${\mathbb{Z}_p}^* = A \cup B \cup C$ such that $|A| = |B| = |C| = \frac{p-1}{3}$ and L on each set is constant. Equivalently there are a, b, c for which

$$L(x) = \begin{cases} a & , \quad x \in A \\ b & , \quad x \in B \\ c & , \quad x \in C \end{cases}$$

(c) (4 points) Prove that $a + b + c = -3$.

(d) (12 points) Prove that $a^2 + b^2 + c^2 = 6p + 3$.

(e) (2 points) Let $X = \frac{2a+b+3}{3}, Y = \frac{b-a}{3}$, show that $X, Y \in \mathbb{Z}$ and also show that $p = X^2 + XY + Y^2$.

評論 3.4 這道題組所引入的和 L 又稱為 Jacobsthal sum，算是在橢圓曲線理論裡挺有名的東西。很可惜這一題在 AoPS 上面沒有解答，這裡可以建議讀者參考 Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography (Discrete Mathematics and Its Applications).* Chapman and Hall/CRC; 2 edition. 的第四章。該書只包含初等方法，筆者認為較適合高中生或大一學生看。

Chapter 4

Diophantine 方程

Diophantine 方程又稱不定方程，是僅容許變數為整數的多項式等式如：

$$a_1x_1^{b_1} + a_2x_2^{b_2} + \cdots + a_nx_n^{b_n} = c.$$

他的名稱源自於西元 3 世紀的希臘數學家 Diophantine，是為紀念他對這類方程的研究，並且首次將符號引入代數領域中的這重要貢獻。關於此類方程的理論研究一直是數論當中最重要的領域，現已有丟番圖逼近 (Diophantine Approximation)、代數數論 (Algebraic Number Theory)、超越數論 (Transcendental Number Theory) 等等分支來研究。

1900 年 Hilbert 提出了 23 個數學問題，當中的第十個就牽扯到了最根本的問題：一般來說，給定一 Diophantine 方程，能否判斷出它是否有解？而此問題在 1970 年被 Matiyasevich 否證了：不可能存在演算法能在有限步驟內判斷任何 Diophantine 方程是否可解!

Diophantine 方程的特點就是隨時都可提出看似簡潔的問題，但背後卻可能隱藏著一大片高等理論，例如證明：對所有正整數 N，總存在整數 $a_1, a_2, \ldots, a_m$ 使得 $N = \sum ia_i^2$。或是證明 $A^4 = B^4 + C^4 + D^4$ 存在無窮多個解 (A, B, C, D) 使四數最大公因數為 1、$A^3+B^3+C^3 = 1$ 有無限多組整數解 (A, B, C) 等等。有時候這些解的形式是初等的，但求解的過程往往涉及到複雜的理論。另外，你還可以在 (https://sites.google.com/site/tpiezas/) 找到許多扯爆的恆等式 ...

1909 年，挪威數學家 Axel Thue 證明了以下事實：

定理 4.1 (Thue's Theorem) 若 $H(x, y)$ 是次數不小於 3 且齊次的整係數不可約多項式，那麼不定方程 $H(x, y) = c$ 僅有有限組整數解 (x, y)。

我們把這個定理的證明留到本章的補充教材。由這個定理出發可以證明競賽裡 call 了就直接電爆全場的兩個定理：Pólya-Størmer's Theorem 以及 Kobayashi's Theorem，這兩個定理的敘述也同樣留到補充教材。另外不斷地運用此定理可以證明更強的 (證明留給讀者)：

定理 4.2 (Thue's Theorem) 僅當 $H(x, y) = q_n(ax + by)^n$ 或是 $q_n(ax^2 + bxy + cy^2)^{n/2}$

時 (其中 q_n 是有理數)，不定方程 $H(x,y)=c\neq 0$ 才可能有無限多組整數解 (x,y)，其中 c 是給定的非 0 整數。

4.1 Pell 方程

Pell 方程不論在競賽或是關於更高深的研究中都是相當重要的，這類的方程式為 Diophantine 方程式的二次形式，最早可追朔至一千多年前的古希臘文獻。西元 7 世紀時，印度數學家 Brahmagupta 得出 Pell 方程式的一般解形式，但並未給出方程式解的判別條件及通式解。到了 17 世紀，法國數學家 Fermat 出了一道求 $61x^2+1=y^2$ 整數解的問題，才引起數學家對於 Pell 方程的重視，而最終關於通式解的部份則由 Lagrange 所解決，他也發展出連分數法 (continued fractions) 以求取初始解。另外，Pell 方程乃是 Euler 將找到解此類方程方法的 Brouncker 誤認為 John Pell，後來以訛傳訛的結果。

此講義專注在 Pell 方程中解的性質，並未介紹如何快速找出初始值的方法，而這是目前數學家還在不斷努力改進的地方。另外，由於筆者不會連分數，所以也未介紹，請多多見諒。這個章節將用引導式題型帶領讀者了解一些 Pell 方程的基本結論，基本上競賽會用到的就是第 5. 小題的結論。

■ 習題部分 ■

這個部分要研究的是 Pell 方程解的性質。所謂的 Pell 方程指的是關於 (x,y) 的整係數方程式 $ax^2-by^2=c$，而簡單的運算告訴我們這其實只須研究 $a=1$ 且 $b>0, c\neq 0$ 且 b 也不是平方數的情況。在前幾個問題中，我們討論 $x^2-dy^2=1$ 的正整數對解。

1. 假設 d 是一個非平方數的正整數，利用第一部分第 (3) 小題 (a) 的結果證明：存在正整數 $k<1+2\sqrt{d}$ 使得 $x^2-dy^2=k$ 有無窮多組正整數對解 (x,y).

2. 如果 (x_1,y_1) 和 (x_2,y_2) 是上一題的兩組解，滿足 $k\mid x_1-x_2$ 且 $k\mid y_1-y_2$，那麼

$$x=\frac{x_1x_2-dy_1y_2}{k},\qquad y=\frac{x_1y_2-y_1x_2}{k}$$

   就會是 $x^2-dy^2=1$ 的一組整數對解 (x,y)。由此證明 $x^2-dy^2=1$ 有無窮多對正整數對解。

3. 現在我們想討論這些解的性質。定義 $\mathbb{Z}[\sqrt{d}]=\{x+y\sqrt{d}\mid (x,y)\in\mathbb{Z}^2\}$，在這個集合定義函數 $\overline{x+y\sqrt{d}}=x-y\sqrt{d}$ 以及 $N(x+y\sqrt{d})=x^2-dy^2$。證明 $\mathbb{Z}[\sqrt{d}]$ 是一個環 (也就是說對加法減法乘法運算封閉)，而對於 $z_1=x_1+y_1\sqrt{d}, z_2=x_2+y_2\sqrt{d}$ 總有 $\overline{z_1z_2}=\overline{z_1}\cdot\overline{z_2}$ 和 $N(z_1z_2)=N(z_1)N(z_2)$.

4. 證明存在 $z_0=x_0+y_0\sqrt{d}\in\mathbb{Z}[\sqrt{d}]$ 滿足

   (a) $(x_0,y_0)\in\mathbb{N}^2$.

   (b) $N(z_0)=1$.

(c) 對所有 $z = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ 滿足 $(x, y) \in \mathbb{N}^2$, $N(z) = 1$ 者，都有 $x_0 < x$ 且 $y_0 < y$.

我們稱 z_0 為 Pell 方程 $x^2 - dy^2 = 1$ 的基本解，或是 $\mathbb{Z}[\sqrt{d}]$ 的基本解。

5. 利用 $z_0 > 1$ 以及函數 N，證明如果 (x, y) 是 $x^2 - dy^2 = 1$ 的一組正整數對解，那麼存在正整數 n 使得 $x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^n$。也就是說所有解都被基本解生成。

6. 現在開始研究一般 Pell 方程

$$x^2 - dy^2 = C \tag{4.1}$$

其中 d 是一個非平方的正整數而 C 為非零整數。證明如果 (x, y) 是方程 (3) 的整數解，且 $z_0 = x_0 + y_0\sqrt{d}$ 是 $x^2 - dy^2 = 1$ 的基本解，那麼對任意正整數 n，滿足 $x_n + y_n\sqrt{d} = (x + y\sqrt{d})(x_0 + y_0\sqrt{d})^n$ 的整數對 (x_n, y_n) 都會是方程 (3) 的整數解。

7. 利用上題，證明如果在 $\mathbb{Z}^2$ 上定義等價關係：$(u, v) \sim (u', v')$ 當且僅當

$$u'' = \frac{uu' - dvv'}{C}, \quad v'' = \frac{uv' - vu'}{C}$$

都是整數。那麼對所有整數對 (x, y)，(x, y) 是方程 (3) 的整數對解當且僅當任意與他在同一個等價類的整數對也是方程 (3) 的整數對解。

8. 由此得出：若 z_0 是 $\mathbb{Z}[\sqrt{d}]$ 的基本解。則存在有限個數 $z_1, z_2, \ldots, z_m \in \mathbb{Z}[\sqrt{d}]$，使得對所有 $z \in \mathbb{Z}[\sqrt{d}]$ 滿足 $N(z) = C$ 者，必有某整數 n, i 及適當正負號使 $z = \pm z_i z_0^n$。這些數 $z_1, z_2, \ldots, z_m$ 仍被稱為基本解。這個結論很重要。

難9. 利用上上題定義的等價關係證明如果 $z = x + y\sqrt{d}$ 是方程 (3) 的一組基本解，而 $z_0 = x_0 + y_0\sqrt{d}$ 是 $\mathbb{Z}[\sqrt{d}]$ 的基本解，那麼我們可以給出限制：

$$0 \le |x| \le \frac{y_0}{\sqrt{2(x_0 + 1)}}\sqrt{|C|}, \quad 0 < |y| \le \sqrt{\frac{1}{2}(x_0 + 1)}\sqrt{|C|}.$$

(可以依序討論 C 的正負號。)

10. 如果 D 是模 4 同餘 0 或 1 的非平方正整數。證明解 $x^2 - Dy^2 = 1$ 和解 $x^2 - Dy^2 = 4$ 是一樣的。

順便提一下，有一類方程叫做 Markoff-Hurwitz 方程：

$$x_1^2 + \cdots + x_n^2 = ax_1 \cdots x_n$$

其中 $n \ge 3$。當 $a > n$ 時無解，$a = n$ 時所有解可由 $(1, \ldots, 1)$ 生成 (這兩個都可以用下一小節要介紹的 Vieta jumping 做出)，但當 $a < n$ 時會有不只一組基本解，然而所有解還是可以用這些基本解生成，這和 Pell 方程不是一樣的結論嗎?! 是否對某類的二次方程都會有類似的結論呢? 看誰有興趣要研究看看。另外，Baragar 在 1994 年證明了對任意 r，總存在數對 (a, n) 使對應到的 Markoff-Hurwitz 方程其基本解的個數至少有 r 個，這個結論是否也能對應到 Pell 方程呢？最後，關於高次 Pell 方程的研究也有一些成果，例如三次的：

定理 4.3 (Delone-Nagell Theorem) 對所有整數 d，方程式 $x^3 - dy^3 = 1$ 除了 $(1,0)$ 外至多只有一個整數解。
(更一般的，當 $a, b, n \geq 3$ 是正整數時，$|ax^n - by^n| = 1$ 至多只有一組正整數解。)

Problem set

P1. Show that there are infinitely many integers n such that $n+1, 2n+1$ and $3n+1$ are all perfect squares, and that such n must be multiples of 40.

P2. Prove that if

$$\frac{x^2+1}{y^2} + 4$$

is a perfect square, then this square equals 9.

P3. Fermat's theorem

Prove that no triangular number larger than 1 is a fourth power.

P4. For positive integer n, find all positive integers x and y such that

$$x^2 + (x+1)^2 + \cdots + (x+n-1)^2 = y^2 + (y+1)^2 + \cdots + (y+n)^2$$

P5. China TST 2002

Find all non-negative integers m and n, such that $(2^n - 1)(3^n - 1) = m^2$.

P6. In geometry, a *Heronian triangle* is a triangle which has side lengths and area that are all integers. Find all Heronian triangles.

P7. ISL 2009 N7

Let a and b be distinct integers greater than 1. Prove that there exists a positive integer n such that $(a^n - 1)(b^n - 1)$ is not a perfect square.

P8. Prove that there exists only finitely many k such that there are infinitely many positive integers x and y such that $(x+i)(y+i)$ is a square for all $i = 1, 2, \cdots, k$.

P9. Michael A. Bennett, *On consecutive integers of the form* ax^2, by^2 *and* cz^2, Acta Arith., 88(1999) 363-370.

Prove that for given intgers a, b, c, there is at most one solution (x, y, z) for the simultaneous equations

$$ax^2 - by^2 = 1, \quad by^2 - cz^2 = 1.$$

後面 3 題你可能需要一些關於 Pell 方程解的成長速率的預備知識，可以回去參考上面的結果。

4.2 Vieta Jumping

這個技巧最早在 1988 年的 IMO 上出現，當年第六題難到連選題委員都沒做出來，有一位學生就是使用此法而拿到特別獎。思路是對於特定的二次方程我們假設出一組最小解，然後利用根與係數的關係設法找到一組更小解而導致矛盾。現在讓我們來看他到底是怎麼做的：

例題 2.1: IMO 1988/6

令 a 和 b 是兩個正整數，使得 $ab+1$ 整除 a^2+b^2。試證

$$\frac{a^2+b^2}{ab+1}$$

是個完全平方數。

證明： 我們使用歸謬法：假設存在滿足 $ab+1$ 整除 a^2+b^2 但其商不為平方數的數對，我們假設在這些數對的集合中 (a_0,b_0) $(a_0 \geq b_0)$ 為滿足 $a+b$ 最小者 (若不只一組，則任取)。現在我們將原方程式改為 $a_0^2+b_0^2=k(a_0b_0+1)$，其中 k 不為完全平方數。再來將他視作是一個關於 a 的二次方程，則他還會有另外一個根 a_1，且滿足：

$$\begin{cases} a_0+a_1=kb_0 & (1) \\ a_0a_1=b_0^2-k & (2) \end{cases}$$

由 (1) 式我們知道 a_1 也是整數。若又有 a_1 是正整數，則由 $a_0a_1=b_0^2-k$ 和 $a_0 \geq b_0$，我們知道 $a_1 < a_0$，故產生了一組解 (a_1,b_0) 滿足 $ab+1$ 整除 a^2+b^2 但其商不為平方數 (因為其商也是 k)，且 $a_1+b_0 < a_0+b_0$，這與我們的假設矛盾！

又若 $a_1=0$，則 $a_0a_1=b_0^2-k=0$，得到 k 是完全平方數，矛盾！所以我們知道 a_1 是負整數，帶回原式得

$$a_1^2+b_0^2-ka_1b_0-k \geq a_1^2+b_0^2+k-k>0.$$

仍然產生矛盾！ □

這邊要特別注意的是，做題目的時候要小心什麼時候才可以找到更小的合理解，因為有時候找到的解不一定還會滿足原本題目的條件，而驗證其合理性往往是最難的一步。

有時候我們會看到題目出現很多二次的方程式，解答往往是可將原本的項寫成一階一次遞迴式，其實這可從根與係數的關係看出：在例題中即為 $a+a'=kb$，由於當我們的根在「跳躍」時，k 值不變，所以容易可寫出 a,b 的遞迴式。

一個題外話，Vieta jumping 其實和代數幾何裡的 parameterization 有關，習題 7 給了一個簡單的例子。

例題 2.2: Romania MO 2004

試找出所有能寫成以下型式的正整數：

$$\frac{a^2+ab+b^2}{ab-1}$$

其中 a,b 為不全為 1 的正整數。

證明： 我們使用歸謬法證明他只能取值為 4 或 7：

首先當 $a=b$ 時易驗證原分式只能取值為 4。假設存在滿足 $ab-1$ 整除 a^2+ab+b^2 但其商不為 4 或 7 的數對，我們假設在這些數對的集合中 (a_0,b_0) $(a_0>b_0)$ 為滿足 $a+b$ 最小者 (若不只一組，則任取)。現在我們將原方程式改為 $a_0^2+a_0b_0+b_0^2=k(a_0b_0-1)$，其中 $k\neq 4$ 和 7。然後將他視作是一個關於 a 的二次方程，則他還會有另外一個根 a_1，且滿足：

$$\begin{cases} a_0+a_1=(k-1)b_0 & (1)\\ a_0a_1=b_0^2+k & (2)\end{cases}$$

綜合兩式我們知道 a_1 也是正整數。若又有 $a_1\leq b_0$，則 (a_1,b_0) 是滿足題意的解，但是 $a_1+b_0<a_0+b_0$，這與我們的假設矛盾！

因此也有 $a_1>b_0$，故我們假設 $a_0=b_0+u$ 且 $a_1=b_0+v$ $(u,v\geq 1)$，帶回方程組得

$$\begin{cases} u+v=(k-3)b_0 & (3)\\ (u+v)b_0+uv=k & (4)\end{cases}$$

將 (4) 式帶入 (3) 式解得 $b_0=1$，但這代回原分式只有 $k=7$，矛盾！

最後，$a=b=2$ 時原分式取值為 4，$a=2,b=1$ 時原分式取值為 7。 □

例題 2.3

證明以下的方程無正整數 (x,y,z) 解：$x^2+y^2+z^2=xyz+1$.

我們先假設有解 (x_0,y_0,z_0) $(x_0\geq y_0\geq z_0)$，並利用根與係數的關係得到：

$$\begin{cases} x_0+x_1=y_0z_0 & (1)\\ x_0x_1=y_0^2+z_0^2-1 & (2)\end{cases}$$

這時候會發現不管是由 (1) 式或 (2) 式下手，都得不到有用的結論。很討厭。不過如果我們願意把原本的方程視為二次方程，那何不利用其他二次方程的性質呢？

證明： 使用歸謬法：

假設原方程有解，並且 (x_0,y_0,z_0) $(x_0\geq y_0\geq z_0)$ 是滿足 $x+y+z$ 最小者，將其視為關於 x 的二次方程 $f(x)$，則必須有另一根 x_1，由假設我們知道 $x_1\geq x_0$。由

於原本的二次方程開口向上，且有 $x_1 \geq x_0 \geq y_0 \geq z_0$，所以我們知道 $f(y_0) \geq 0$，即 $y_0^2 - y_0^2 z_0 + y_0^2 + z_0^2 - 1 \geq 0$。再由 $y_0 \geq z_0$，而

$$y_0^2 - y_0^2 z_0 + y_0^2 + y_0^2 - 1 \geq y_0^2 - y_0^2 z_0 + y_0^2 + z_0^2 - 1.$$

也就是有 $y_0^2 - y_0^2 z_0 + y_0^2 + z_0^2 - 1 \geq 0$，我們就得到了 $z_0 < 3$。接下來只需帶入 $z_0 = 1, 2$ 找解即可！ □

Problem set

P1. Taiwan TST 2011

Let x and y be positive integers such that xy divides $x^2 + y^2 + 6$. Show that

$$\frac{x^2 + y^2 + 6}{xy}$$

is a cube.

P2. ISL 2002 N4

Is there a positive integer m such that the equation

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{abc} = \frac{m}{a+b+c}$$

has infinitely many solutions in positive integers a, b, c ?

P3. USA TST 2002

Find in explicit form all ordered pairs of positive integers (m, n) such that $mn - 1$ divides $m^2 + n^2$.

P4. Iran MO 1996

Assume that m and n are odd positive integers such that

$$m^2 - n^2 + 1 \mid n^2 - 1.$$

Prove that $m^2 - n^2 + 1$ is a perfect square and find all solutions.

P5. ISL 2009 N4

Find all positive integers n such that there exists a sequence of positive integers $a_1, a_2, \ldots, a_n$ satisfying:

$$a_{k+1} = \frac{a_k^2 + 1}{a_{k-1} + 1} - 1$$

for every k with $2 \leq k \leq n - 1$.

P6. ISL 2007 N6

Let k be a positive integer. Prove that the number $(4k^2 - 1)^2$ has a positive divisor of the form $8kn - 1$ if and only if k is even.

P7. Prove that the equation

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

has infinitely many rational solutions.

P8. Japan MO 2013

Let $n \geq 2$ be a positive integer. Find the minimum value of positive integer m for which there exist positive integers $a_1, a_2, \ldots, a_n$ such that :

(a) $a_1 < a_2 < \cdots < a_n = m$

(b) $\frac{a_1^2+a_2^2}{2}$, $\frac{a_2^2+a_3^2}{2}$, $\ldots$, $\frac{a_{n-1}^2+a_n^2}{2}$ are all square numbers.

P9. Germany MO 2003

Prove that there exist infinitely many pairs (a, b) of relatively prime positives integer such that

$$\frac{b^2-5}{a} \text{ and } \frac{a^2-5}{b}$$

are both positive integers.

P10. British MO 2007

Show that there are infinitely many pairs of positive integers (m, n) such that

$$\frac{m+1}{n} + \frac{n+1}{m}$$

is a positive integer.

P11. Find infinitely many triples (a, b, c) of positive integers such that a, b, c are in a arithmetic progression and such that $ab + 1, bc + 1, ca + 1$ are perfect squares.

P12. Markov's equation

Find all the solutions (x, y, z, k) of the equation $x^2 + y^2 + z^2 = kxyz$, where x, y, z, k are natural numbers.

P13. Mongolia MO 2000

Find all $n \in \mathbb{N}$ such that the following equations has natural solutions (x, y, z): $(x + y + z)^2 = nxyz$

P14. Consider the equation $(x + y + z + t)^2 = nxyzt$.

(a) Prove that if $n > 16$ then the equation has no solution (x, y, z, t) in $\mathbb{N}$.

(b) Find all perfect square n such that the equation has solution (x, y, z, t) in $\mathbb{N}$.

P15. RMM 2016

A cubic sequence is a sequence of integers given by $a_n = n^3 + bn^2 + cn + d$, where b, c and d are integer constants and n ranges over all integers, including negative integers.

(a) Show that there exists a cubic sequence such that the only terms of the sequence which are squares of integers are a_{2015} and a_{2016}.

(b) Determine the possible values of $a_{2015} \cdot a_{2016}$ for a cubic sequence satisfying the condition in part (a).

4.3 指數 Diophantine 方程

這類方程大概就是型如 $a^x - b^y = c$ 之類的東東，而由 Pólya-Størmer Theorem 我們知道給定 a, b, c 時只會有有限組解 (x, y)。通常解這類方程有幾種方法：

(1) 同餘 a, b 的質因數次方，或者同餘其他質數次方。這時可以得出 x, y 的形式。

(2) 由 (1) 找出形式 $x = cm + n$ 之後，再模 p^t，而這些質數次方必須讓 $\delta_{p^t}(a)$ 盡量小 (就是讓 $(p-1, a)$ 的比率盡量大)，或是讓 a 是原根。

(3) 假設你猜 x_0 是最大解，去模 a^{x_0+1}。

(4) 假設你猜 (x_0, y_0) 是最大解，改寫原方程變為 $a^{x_0}(a^u - 1) = b^{y_0}(b^v - 1)$，然後繼續模，直到導出例如左邊要被 a^{x_0+1} 整除這種矛盾。

例題 3.1: Taiwan TST 2011

找出以下方程的所有正整數 (m, n) 解：

$$3^m - 7^n = 2.$$

證明： 代數字可以猜測 $(m, n) = (2, 1)$ 是唯一解。假設還有更大解 $(m, n) = (2+u, 1+v)$，那麼

$$3^2(3^u - 1) = 7(7^v - 1).$$

由於 $9 \mid 7^v - 1$，因此 $3 \mid v$，得到 $19 \mid 7^3 - 1 \mid 7^v - 1$，故有

$$19 \mid 3^u - 1.$$

這要求 $18 \mid u$，但就會有 $37 \mid 3^{18} - 1 \mid 3^u - 1$。所以

$$37 \mid 7^v - 1.$$

這蘊含 $9 \mid v$，由此 $27 \mid 7^9 - 1 \mid 7^v - 1 \mid 3^2(3^u - 1)$，矛盾! (請思考每一步模的那些質數是怎麼取的) □

另外，如果在 $a^x - b^y = c$ 的 a, b 中有偶數就太棒了，你可以試著模 2 的冪次，並利用 Carmichael 函數中證明 $\lambda(2^n) = 2^{n-2}$ 的技巧得到一些東東。例如你要求 $2^x + 1 = 5^y$，去模 2^x 你就知道 y 一定要長成 $2^{x-2}t$ 這種形式。然後就會發現 y 成長得太快，根本就幾乎不會有 $2^x + 1 = 5^y$！

Problem set

P1. China MO 2005

Find all positive integers (a, b, c, d) such that

$$2^a 3^b - 5^c 7^d = 1.$$

P2. Find all positive integers (a, b, c, d) such that

$$2^a 3^b 7^c - 43^d = 1.$$

P3. Find the least number which can't be express in the form

$$2^x 3^y - 2^z 3^w$$

with x, y, z, w be nonnegative.

P4. Prove that the exponential equation

$$\prod_{i=1}^{k} {x_i}^{x_i} = z^z$$

has infinitely many solutions $(x_1, \ldots, x_k, z)$ for any given k.

P5. Let b, c are given positive integers. Does there always exist a positive integer a such that $(a, b) = 1$ and

$$|a^x - b^y| \geq c$$

for all positive integers x and y?

4.4 加性數論

密度 (density) 是加性數論研究中一個重要的問題。這之中最典型的大概就屬 Hilbert–Waring 定理：對任意正整數 k，總存在某個正整數 $g(k)$ 使得所有正整數都可以表示成不超過 $g(k)$ 個正整數的 k 次方之和。在數學競賽裡常常會有題目要求證明所有正整數都可以寫成數個某種類型的數之和，以下我們介紹一些定理及處理方法：

定理 4.4 (Fermat polygonal number theorem) 每個正整數都可以表示成不超過 n 個 n 角形數 (n-gonal number) 之和。

定理 4.5 (Lagrange's four-square theorem) 每個正整數都可以表示成四個整數的平方和。

運用四平方和定理，John H. Conway 和 W. A. Schneeberger 在 1939 年證明了不可思議的：

定理 4.6 (15-Theorem) 如果一個二次型 (quadratic form) 的對應矩陣為整值矩陣 (integral matrix)，並且可以透過變數取整數值而表示出 15 以內所有數 (事實上只要表示出 $1, 2, 3, 5, 6, 7, 10, 14, 15$)，那麼他必定可以透過變數取整數值而表示出所有正整數。

而在 2005 年，Manjul Bhargava 和 Jonathan Hanke 改進了他們的方法，證明了：

定理 4.7 (290-Theorem) 如果一個整係數的二次型可以透過變數取整數值而表示出 $1, 2, 3, 5, 6, 7, 10, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290$，那麼他必定可以透過變數取整數值而表示出所有正整數。

定義 4.1 給定集合 $A_1, \ldots, A_n$，定義他們的和集 (sumset) 為：

$$A_1 \oplus \cdots \oplus A_n = \{a_1 + \cdots + a_n \,|\, a_i \in A_i \,\forall\, i\}$$

重要性質——★ (Cauchy-Davenport Theorem) 給定域 $\mathbb{Z}/p\mathbb{Z}$ 中兩子集 A, B，那麼

$$|A \oplus B| \geq \max\{p, |A| + |B| - 1\}$$

定義 4.2 給定非負整數的集合 A，定義他的 Schnirelmann 密度為：

$$d(A) = \inf_{n \geq 1} \frac{A(n)}{n}.$$

其中 $A(n)$ 是 A 中不超過 n 的元素個數。

重要性質——★ (Mann's Theorem) 給定兩非負整數集合 A, B，那麼

$$d(A \oplus B) \geq \min\{1, d(A) + d(B)\}.$$

證明： 這也是競賽裡 call 了就嚇嚇叫的定理之一。筆者將證明改為引導式題目請讀者練習。在接下來所有的部份中，考慮的非負整數子集都是包含 0 的集合。而我們試圖探討 $d(A), d(B)$ 和 $d(A \oplus B)$ 的關係。

固定正整數 g，分別以 A_1, B_1 記 A, B 中不超過 g 的元素形成的集合。假設可以找得到某個常數 $\theta \in (0, 1]$ 使得：

$$A_1(m) + B_1(m) \geq \theta m, \quad \forall m = 1, 2, \ldots, g.$$

我們的目的是要找出新的非負整數子集 A_2, B_2 使得以上不等式對於 A_2, B_2 仍成立，並且這兩個集合仍包含 0，$B_2(g) < B_1(g)$，而 $A_2 \oplus B_2 \subseteq A_1 \oplus B_1$.

1. 假設 $B_1 \not\subseteq A_1$，證明可以藉由取 $A_2 = A_1 \cup B_1$, $B_2 = A_1 \cap B_1$ 來達成目的。

2. 假設 $B_1 \subseteq A_1$.

(a) 證明集合 $\{a \in A \,|\, \exists b \in B, a+b \notin A\}$ 非空，假設 a_0 是這個集合的最小元素，證明 $a_0 \neq 0$.

(b) 假設 $B_1(g) > 0$，證明如果存在整數 z 與 B_1 中的元素 b 滿足 $z - a_0 < b \leq z$，那麼對所有 $a \in A_1$ 滿足 $1 \leq a \leq z - b$ 者，總有 $a + b \in A_1$。利用這個結論證明 $A_1(z) \geq A_1(b) + A_1(z-b)$.

(c) 假設 $B_1(g) > 0$，證明如果存在 $y \leq g$ 使得 $A_1(y) < \theta y$，那麼 $y > a_0$.

(d) 假設 $B_1(g) > 0$，記 $B' = \{b \in B_1 \,|\, a_0 + b \notin A_1\}$, $A' = \{a_0 + b \,|\, b \in B', a_0 + b \leq g\}$。考慮 $A_2 = A_1 \cup A'$, $B_2 = B_1 \cap (B'^c)$，其中 B'^c 是 B' 在非負整數中的補集。證明這兩個集合仍包含 0，$B_2(g) < B_1(g)$，而 $A_2 \oplus B_2 \subseteq A_1 \oplus B_1$.

(e) 證明 $A_2(m) = A_1(m) + A'(m)$, $B_2(m) = B_1(m) - B'(m)$, $A'(m) = B'(m - a_0)$。由此推出當 $B'(m) = B'(m - a_0)$ 時會有 $A_2(m) + B_2(m) \geq \theta m$.

(f) 當 $B'(m) < B'(m - a_0)$ 時，先證明 $B_1(m) = B_1(m - a_0) \geq B'(m) = B'(m - a_0) > 0$，並藉由考慮 B_1 中滿足 $m - a_0 < b_0 \leq m$ 的最小整數 b_0，來推導出仍有 $A_2(m) + B_2(m) \geq \theta m$ (提示：此時將有 $B_1(m - a_0) = B_1(b_0 - 1)$，而可在 (b) 中取 $z = m$, $b = b_0$).

(g) 總結以上結果。

(h) 利用上述結論，對 $B_1(g)$ 進行數學歸納法，證明 $(A_1 \oplus B_1)(g) \geq \theta g$.

(i) 證明選取 $\theta = \min(1, d(A) + d(B))$ 的合法性。我們能對 $d(A \oplus B)$ 給出怎樣的結論？

3. 對於正整數 n，以 nA 簡記集合 $A \oplus \cdots \oplus A (n \text{ 次})$。假設非負整數子集 A 具有正的 Schnirelmann 密度，證明存在正整數 m 使得 $mA = \mathbb{N} \cup \{0\}$. □

例題 4.1

試證有無窮多個正整數不能寫成以下的表達形式：

$$x_1^3 + x_2^5 + x_3^7 + x_4^9 + x_5^{11}$$

其中 $x_1, x_2, x_3, x_4, x_5 \in \mathbb{N}$.

證明： 我們取夠大的數 N，那麼不超過 N 的 a 次方數最多有 $N^{\frac{1}{a}}$ 個，因此不超過 N 且能表示成 $x_1^3 + x_2^5 + x_3^7 + x_4^9 + x_5^{11}$ 的數至多有 $N^{\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{9}+\frac{1}{11}}$ 個。因此將 N 取趨向無限大就得到了我們的結論。 □

例題 4.2: Schur 定理

把 $M = \{1, 2, \cdots, n\}$ 分成 t 個不相交的子集 $M_1, \ldots, M_t$。證明如果 $n \geq \lfloor t!e \rfloor$，那麼至少存在一個集合 M_z 會包含滿足 $x_i - x_j = x_k$ 的三個元素 x_i, x_j, x_k.

證明：(這裡的是暴力證法，更優美的證法請參考正整數集上的 Ramsey 理論一章) 由 Tylor 展開式我們先得到遞迴關係 $S_t = tS_{t-1} + 1$，其中 $S_0 = 1$。
用歸謬法：假設沒有一組劃分裡存在 $a+b=c$，由鴿子先生的定理我們知道 M 中至少有 $\lfloor \frac{S_t}{t} \rfloor = S_{t-1} + 1$ 個數被分到某一劃分，假設叫做 $M_1 = \{x_1, \cdots, x_k\}$ 使得 $x_1 < \cdots < x_k$，其中 $k \geq \lfloor \frac{S_t}{t} \rfloor$。

考慮集合 $Y_1 = \{y_1^{(1)}, \ldots, y_{k-1}^{(1)}\}$，其中 $y_i^{(1)} = x_{i+1} - x_1$，我們有 $|Y_1| \geq S_{t-1}$，並且 Y_1 中元素都不在 M_1 中 (否則與歸謬假設矛盾)。因此在 Y_1 中的元素必須在 $M_2, \ldots, M_t$ 這 $t-1$ 個集合中。

簡單歸納一下，我們假設得到 $M_1, \ldots, M_i = \{y_{i-1,1}^{(i-1)}, \ldots, y_{i-1,S_{t-i}+1}^{(i-1)}\}$，那麼考慮集合 $Y_i = \{y_1^{(i)}, \ldots, y_{S_{t-i}}^{(i)}\}$，其中 $y_j^{(i)} = y_{i-1,j+1}^{(i-1)} - y_{i-1,1}^{(i-1)}$，知道有 $|Y_i| \geq S_{t-i}$，並且 Y_i 中元素都不在 $M_1, \cdots, M_i$ 中 (否則與歸謬假設矛盾)。因此在 Y_i 中的元素必須在 $M_{i+1}, \ldots, M_t$ 這 $t-i$ 個集合中，所以又可以找到 M_{i+1} 使其中至少有 $S_{t-i-1}+1$ 個 Y_i 中的元素。(這邊符號太多，我懶得檢查了，反正意思到就好)

最後，我們知道 M_t 中至少有兩個數 $y_{t-1,2}^{(t-1)} < y_{t-1,1}^{(t-1)}$，由於數 $y_{t-1,1}^{(t-1)} - y_{t-1,2}^{(t-1)}$ 必在 $M_1, \ldots, M_{t-1}$ 中 (假設在 M_s 中)，而這兩數又可以寫成 $y_{t-1,\square}^{(t-1)} = y_{s-1,\square}^{(s-1)} - y_{s-1,1}^{(s-1)}$ 的形式，這會導致 M_s 中有三數 $a+b=c$，與歸謬假設矛盾! □

加性數論裡的題目方法不外乎直接估計欲求數所有的密度，或者是用鴿籠原理不斷將範圍縮小，比方 Mann's theorem 就可以依此證明，要嘛就是神奇的構造。當然，你還有 Combinatorial Nullstellensatz 這種更強的定理可以選擇。

Problem set

P1. ELMO shortlist 2012 N3

Let $s(k)$ be the number of ways to express k as the sum of distinct 2012^{th} powers, where order does not matter. Show that for every real number c there exists an integer n such that $s(n) > cn$.

P2. ELMO 2014

Define a beautiful number to be an integer of the form a^n, where $a \in \{3, 4, 5, 6\}$ and n is a positive integer. Prove that each integer greater than 2 can be expressed as the sum of pairwise distinct beautiful numbers.

P3. Show that any integer can be expressed as a sum of two squares and a cube.

P4. Show that each integer can be written as the sum of five perfect cubes (not necessarily positive).

P5. ISL 2000 N6

Show that the set of positive integers which cannot be represented as a sum of distinct perfect squares is finite.

P6. Find the greatest positive integer n with the following property: there exist n non-negative integers $x_1, x_2, \ldots, x_n$, at least one different from zero, such that for any numbers $a_1, a_2, \ldots, a_n \in \{-1, 0, 1\}$, at least one different from zero, n^3 does not divide $a_1x_1 + a_2x_2 + \cdots + a_nx_n$.

P7. Erdős' theorem

A set A is called sum-free if there do not exist $a, b, c \in A$ (not necessarily distinct) such that $a + b = c$. Prove that every set A of n nonzero integers contains a sum-free subset of size greater than $\frac{n}{3}$.

P8. Van der Waerden's theorem

Prove that for any given positive integers r and k, there is some number $N(r, k)$ such that if the integers $\{1, 2, \ldots, N\}$ are colored, each with one of r different colors, then there are at least k integers in arithmetic progression all of the same color.

P9. ISL 1999 A4

Prove that the set of positive integers cannot be partitioned into three nonempty subsets such that for any two integers x, y taken from two different subsets, the number $x^2 - xy + y^2$ belongs to the third subset.

P10. ISL 1995 N7

Does there exist an integer $n > 1$ that satisfies the following condition? The set of positive integers can be partitioned into n nonempty subsets such that an arbitrary sum of $n - 1$ integers, one taken from each of any $n - 1$ of the subsets, lies in the remaining subset.

4.5 補充教材——Diophantine 分析

4.5.1 一般理論

Diophantine 逼近的核心思想就是以有裡數去逼近一個無理數。比方說大家都看過的：$355/113 \approx \pi$ 就是一個“好”的有理逼近，因為把 355/113 的分母換成比 113 還小的自然數時，都找不到分數比它更接近 π。而這部分的研究在 18 世紀數學家發展出連分數 (continued fractions) 的方法後開始有了許多成果。

而 Diophantine 逼近在一般 Diophantine 方程的研究上也有許多應用，另外還可以當做區分代數數與超越數的一個準則，因此在超越數論中占了很重要的地位。理論部分，筆者覺得大概要從 Dirichlet's approximation theorem 開始說起：

定理 4.8 (Dirichlet's Approximation Theorem) 對任意無理數 α，可找到無窮多個有理數 p/q 滿足

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

證明： 先給定 $Q \geq 2$，將區間 $[0,1)$ 分成 $[(i-1)/Q, i/Q)$，其中 $i = 1, 2, \ldots, Q$。考慮 $0, \{\alpha\}, \{2\alpha\}, \ldots, \{Q\alpha\}$，由鴿籠原理知道這些數中必有兩數落在我們分好的同一區間中，假設是 $\{i\alpha\}, \{j\alpha\}$，那麼

$$|(i\alpha - j\alpha) + (s_j - s_i)| < \frac{1}{Q}.$$

(其中 s_i, s_j 分別是 $\{i\alpha\}, \{j\alpha\}$ 的整數部分) 又因為 $i, j < Q$，除掉便得到

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qQ} < \frac{1}{q^2}.$$

對某個有理數 p/q，其中 $q < Q$。現在把 Q 加大到很大很大，還是要找到

$$\left|\alpha - \frac{p'}{q'}\right| < \frac{1}{q'Q'}.$$

又可再多出一組 p'/q'，一直重複就得到無窮多個了。 □

評論 4.1 這個定理有些神奇的用法，例如證明費馬二平方和定理 XD。有時候在數學競賽裡還會看到一些他的推廣，像是某些中國題之類。另外讀者有興趣可以證明高維版本：給定實數 $\alpha_1, \ldots, \alpha_d$ 以及正整數 N，那麼可以找到整數 $p_1, \ldots, p_d$, $1 \leq q \leq N$ 使得

$$\left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{qN^{\frac{1}{d}}}.$$

這個定理最終形式就是 Hurwitz's theorem，而且注意他們都是對所有無理數 α 都成立的估計，超強！不過其實數學家有興趣研究的是代數數的 Diophantine 逼近部分，因為代數數有很好的解析性質：它會是某個整係數多項式的根。好的定理是：

定理 4.9 給定代數數 α，僅存在有限多個有理數 p/q 滿足

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\kappa}.$$

另一個等價敘述是說，存在某個常數 $c = c(\alpha) > 0$，使得對所有有理數 p/q，都有

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^\kappa}.$$

其中 κ 的值一直被數學家下修 (以下 $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$)：

κ	contributor
$\kappa = n$	Liouville, 1844
$\kappa = (n+1)/2 + \epsilon$	Thue, 1909
$\kappa = n/s + s - 1 + \epsilon$	Siegel, 1921
$\kappa = \sqrt{2n} + \epsilon$	Dyson, Gel'fond, 1947
$\kappa = 2 + \epsilon$	Roth, 1955

值得注意的是指數 $2+\epsilon > 2$ 已經不能再改進了 (由 Dirichlet approximation theorem 可看出)，而這是很不可思議的事情，一個代數數的 approximation exponent 跟它的次數是無關的！由於 Roth 優秀的成果，他在 1958 年拿到了 Fields Medal。然後這個定理的過程實在很煩，在這邊我們不打算證明它。運用這個定理，在 1909 年挪威數學家 Axel Thue 證明了以下很厲害的事實：

定理 4.10 (Thue's Theorem) 若 $H(x,y)$ 是次數不小於 3 且齊次的整係數不可約多項式，那麼不定方程 $H(x,y) = c$ 僅有有限組整數解 (x,y)，其中 c 是給定的非 0 整數。

證明： 我們使用歸謬法: 假設有無限組整數解 (x,y)，那麼考慮 $|x_1|, |x_2|, \ldots$ 以及 $|y_1|, |y_2|, \ldots$ 這兩個無窮數列，其中必有一個數列的值無上界，不妨假設是 y。現在設 $c \neq 0$，我們先證原方程只有有限組整數解 $x, y > 0$：

設 $\theta_1, \ldots, \theta_n$ 是 $H(x/y, 1)$ 的所有複數根，那麼

$$H(x,y) = a_n(x - \theta_1 y)(x - \theta_2 y)\cdots(x - \theta_n y) = c.$$

由上式得到

$$|a_n||x - \theta_1 y||x - \theta_2 y|\cdots|x - \theta_n y| = |c|.$$

所以我們知道至少存在一個 k 使得

$$|x - \theta_k y| \leq \sqrt[n]{\left|\frac{c}{a_n}\right|} = c_1.$$

由於 $H(x,y)$ 不可約，所以 $\theta_1, \ldots, \theta_n$ 兩兩不同。因此，有正常數 c_2 使得對所有 $i \neq j$，有 $\theta_i - \theta_j > c_2$。並且當 $y > 2c_1/c_2$ 時，有

$$|x - \theta_j y| = |(\theta_k - \theta_j)y + (x - \theta_k y)| > c_2 y - c_1 > \frac{1}{2}c_2 y.$$

由此得

$$\prod_{j \neq k} |x - \theta_j y| > \left(\frac{1}{2}c_2 y\right)^{n-1}.$$

代回 $H(x,y)$ 的分解式得到

$$|x - \theta_k y| < \frac{c_3}{y^{n-1}}\,,\ c_3 = \frac{|c|}{|a_n|\left(\frac{1}{2}c_2\right)^{n-1}} > 0.$$

因此給出

$$\left|\frac{x}{y} - \theta_k\right| < \frac{c_3}{y^n}\,,\ \text{對某正常數 } c_3.$$

而此估計只能對有限多個 $y > 0$ 成立。因此 $H(x, y) = c$ 只有有限組整數解 $x, y > 0$。同樣的 $H(x, -y) = c$ 仍不可約，因此 $H(x, -y) = c$ 也只有有限組整數解 $x, -y > 0$，而 $H(x, 0) = c$ 顯然只有有限組整數解。

綜上 $H(x, y) = c$ 只有有限組整數解 (x, y)，這與歸謬假設矛盾！因此原定理必須成立。 □

而用 Thue-Siegel-Roth theorem 還可以證明更多的不定方程僅有有限組整數解，例如 Catalan's conjecture 的某些特例。然而，我們僅能證明有有限組整數解，卻不知道解的上界，這樣也無法肯定是否計算機已經找到了方程的所有解，實在是很可惜。

我們先把焦點放在另外的問題上。Hilbert 當年還提到了一個與代數數和超越數相關的命題：若 b 是無理數、a 是非 $0, 1$ 的代數數，那麼 a^b 是否一定為超越數？而這問題在 1934 年以及 1935 年分別被 Gel'fond 和 Schneider 獨立的證明了 (答案是肯定的)。此命題的一個等價敘述為：如果 α 和 β 是非零的代數數，且 $\log \alpha$ 和 $\log \beta$ 在 $\mathbb{Q}$ 上線性獨立 (linearly independent)，那麼在 $\mathbb{A}$ 上也是線性獨立的。(讀者可以證證看他們的等價性)

時間往後推移，1966 年 Baker 證明了上述命題的一般情況：如果 $\alpha_1, \ldots, \alpha_n$ 是非零的代數數，且 $\log \alpha_1, \ldots, \log \alpha_n$ 在 $\mathbb{Q}$ 上線性獨立，那麼在 $\mathbb{A}$ 上也是線性獨立的。同時他還把這方法推到「有效計算法」上，給出了某類 Diophantine 方程解的上界，而一旦知道了上界，從理論上講，我們就可以求出所有的解，只要把界內的數帶回去驗證即可。由於 Baker 那實在是強得太誇張的定理，國際數學家大會在 1970 年頒給他 Fields Medal。

有時候還會碰到聯立方程組，就是要求某些估計要同時成立，仍有好的結果：

定理 4.11 (Schmidt's Theorem) 設 $x_1, \ldots, x_n$ 是代數數，且 $1, x_1, \ldots, x_n$ 在 $\mathbb{Q}$ 上線性獨立，給定正數 ϵ，那麼僅有有限組有理數 $(p_1/q, \ldots, p_n/q)$ 滿足

$$\left| x_i - \frac{p_i}{q} \right| < \frac{1}{q^{1+\frac{1}{n}+\epsilon}}.$$

4.5.2 Pólya-Størmer 定理

在 AoPS 混過一段時間的讀者可能會認識以下結論：

定理 4.12 (Kobayashi's Theorem) 給定正整數數列 $\langle a_n \rangle$，定義集合 $\mathbb{P}(\langle a_n \rangle) = \{p \mid p \text{ 是質數, 存在 } i \text{ 使得 } p \mid a_i\}$。假設一給定無界的正整數數列 $\langle a_n \rangle$ 滿足 $\mathbb{P}(\langle a_n \rangle)$ 是有限集，則對任意 $t \neq 0$，$\mathbb{P}(\langle a_n + t \rangle)$ 都是無限集。

其中關於命名部分筆者認為是有些爭議的。雖然論壇中絕大部分的人都稱它為 Kobayashi's theorem，然而事實上早在 1918 年的一篇論文 G., Pólya. *Zur arithmetischen Untersuchung der Polynome.* Mathematische Zeitschrift (1918). Volume: 1, 143-148. 中 G.Pólya 就已證明了等價的定理 (另外維基百科是把這定理歸功於 C.Størmer)，而小林先生的結論直到 1981 年才發表在 Tokyo Journal of Mathematics 上。

定理 4.13 (Pólya-Størmer Theorem) 給定有限質數所生成的集合 $\langle S \rangle = \langle p_1, \ldots, p_r \rangle$。現在我們把 $\langle S \rangle$ 中的元素依序列出為 $a_1 < a_2 < \cdots$，則有 $\lim_{i \to \infty} a_{i+1} - a_i = \infty$。換句

話說，給定整數 c，則 $a_{i+1} - a_i = c$ 僅有有限組解 i。

證明： 命題要我們證明的其實就是：$p_1^{\alpha_1} \cdots p_r^{\alpha_r} - p_1^{\beta_1} \cdots p_r^{\beta_r} = c$ 僅有有限組非負整數解 $(\alpha_1, \ldots, \alpha_r, \beta_1 \ldots, \beta_r)$。

現在將 $(\alpha_1, \ldots, \alpha_r, \beta_1 \ldots, \beta_r)$ 對模 3 進行分類。於是可以把每一組方程式寫成：

$$(p_1^{\alpha_1'} \cdots p_r^{\alpha_r'})X^3 - (p_1^{\beta_1'} \cdots p_r^{\beta_r'})Y^3 = c.$$

其中 α', β' 分別是 α, β 模 3 的餘數。現在由於給定的質數集是有限的，這樣對應出來的方程式也是有限的，而每一個都可由 Thue's theorem 知道僅有有限組整數解。因此，命題成立。 □

這兩個定理很強，舉例來說，可以看到 Pólya-Størmer theorem 問的就是質因數集固定的數在自然數裡面的分布情況，而這定理宣稱了相鄰 B-光滑數之間的差必須趨近無窮大，但我們知道相鄰正整數的差永遠是 1，因此質數必須要有無窮多個才能構造出自然數！

關於光滑數的研究，會在第二部的 Diophantine 逼近一章作較深入的探討，筆者在裡面用 Baker 定理將上面的定理做了推廣。

4.5.3 Baker 定理

定理 4.14 (Baker's theorem) 令 $\alpha_1, \ldots, \alpha_n$ 是非零的代數數，次數與高 (指代數數 α 的極小多項式變成整係數多項式後係數絕對值最大者) 分別不超過 d 和 H。假設說有整數 $b_1, \ldots, b_n$，其中絕對值最大者為 T，滿足

$$0 < |b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| < e^{-\delta T}.$$

其中 $0 < \delta < 1$。那麼

$$T < (4^{n^2} \delta^{-1} d^{2n} \log H)^{(2n+1)^2}.$$

有一些改進，像是若 $H(x, y)$ 是次數不小於 3 且齊次的整係數不可約多項式，那 $H(x, y) = c$ 的解會滿足 $\max\{|x|, |y|\} < ac^b$，其中 a, b 是僅依賴 $H(x, y)$ 的可計算常數。如果讀者有興趣的話可以拿來作上一節的習題。以下介紹其在 Pell equation 上的應用。

研究 5.1

試用 Baker's theorem 求出滿足 $5^a - 3^b = 2$ 的正整數數對 (a, b) 的一個上界。

證明： 首先計算排除掉 $b = 1, \ldots, 7$ 的情況 (之後顯然要有 $b > a$)。讓兩邊除以 3^b，並取對數得到

$$0 < a \log 5 - b \log 3 = \log(\frac{2}{3^b} + 1). \tag{4.2}$$

我們最終的目的是要找到 $0 < \delta < 1$ 滿足 $\log(\frac{2}{3^b} + 1) < e^{-\delta b}$。為了估計 $\log(\cdot)$ 的值，考慮 Tylor 展開式：

$$\log(\frac{2}{3^b} + 1) = \frac{2}{3^b} - \frac{1}{2}\left(\frac{2}{3^b}\right)^2 + \frac{1}{3}\left(\frac{2}{3^b}\right)^3 - \frac{1}{4}\left(\frac{2}{3^b}\right)^4 + - \cdots \tag{4.3}$$

$$\leq \frac{2}{3^b} + \frac{1}{3}\left(\frac{2}{3^b}\right)^3 + \frac{1}{5}\left(\frac{2}{3^b}\right)^5 + \cdots \leq \frac{2}{3^b} + \left(\frac{2}{3^b}\right)^3 + \left(\frac{2}{3^b}\right)^5 + \cdots \tag{4.4}$$

$$= \frac{A}{1 - A^2} \leq A^{0.9}, \quad \text{其中 } A = \frac{2}{3^b} \tag{4.5}$$

$$\leq 2^{0.9} e^{-0.9b} \leq e^{-0.9b + 0.63} = e^{-0.9(b - 0.7)} < e^{-0.9(\frac{9}{10}b)} = e^{-0.81b}. \tag{4.6}$$

因此

$$0 < a \log 5 - b \log 3 = \log(\frac{2}{3^b} + 1) < e^{-0.81b}.$$

在這裡顯然有 $d = 1$, $H = 5$, $T = b$, $\delta = 0.81$。所以就得到方程式解的上界：

$$b = T < (4^4 (0.81)^{-1} \log 5)^{25} < 509^{25}.$$

雖然範圍還是大得驚人，不過至少已經能夠給出一個估計了！ □

我們現在來依序分析各個式子：

Step**1.** 首先是，為什麼一開始要計算排除掉 $b = 1, \ldots, 7$ 的情況？原因是這樣才能給出後面更緊的估計。例如看到 (4.5) 式，其成立的條件就必須是 $b \geq 2$，而如果還想把 0.9 用更大的數值取代 (可以看到這樣 δ 也會變大，造成最後能估計出更小的上界)，就必須再把 b 的初始值放大。還有另一個是 (4.6) 式，b 要夠大才能夠有 $b - 0.7 > (9/10)b$ (這邊同樣也是想讓 δ 變大)。

Step**2.** 再來我們看到 (4.2) 式，對這類型指數方程的處理方法很一般，就是除掉某數次方，然後直接得到 Baker's theorem 中絕對值裡的形式。但對其他的丟番圖方程，則是常使用到代數裡的 prime ideal theorem，將因式分解後再取對數。

Step**3.** 接下來是 (4.3),(4.4) 式，這邊沒什麼好說的。反正在分析裡面常常亂丟東西，倒也不用太擔心最後找不到在 $(0, 1)$ 區間裡的 δ 值。除非你是真的要研究某個方程的解，這時候中間估計就很重要了，只要你注意到 Baker's theorem 最後解的上界有多恐怖 ... 。

Step**4.** 最後提醒，最好先找出 T 是誰再去做估計，不然到後來你的 $e^{-\delta T}$ 可能會崩潰。好的，聽筆者廢話講那麼多還不如自己做一次，讀者可以隨便找一道指數 Diophantine 方程那節的題目來練習，相信一定能體會到更多東西。

接下來的這個研究完全翻譯自於論文 Liptai, Kálmán. *Lucas balancing numbers.* Acta Mathematica Universitatis Ostraviensis 14.1 (2006): 43-47. 如果有侵犯著作權請通知筆者，會馬上將這一段刪除。裡面採用的對數估計是 A. Baker 和 H. Wüstholz 在 1993 年做的改進版：

定理 4.15 (Baker-Wüstholz theorem) 給定 $\alpha_1, \ldots, \alpha_n$ 是非 0 和 1 的代數數以及整數 $b_1, \ldots, b_n$，令

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n.$$

我們令 $B = \max\{|b_1|, \ldots, |b_n|, e\}$, $A_i = \max\{H(\alpha_i), e\}$ $(i = 1, \ldots, n)$，並且假設代數數的次數不超過 d。如果 $\Lambda \neq 0$，那麼

$$\log |\Lambda| > -(16nd)^{2(n+2)} \log A_1 \cdots \log A_n \log B.$$

至今，Baker 定理的估計還一直在被下修，這使得我們能夠以計算機計算出越來越多的神奇的丟番圖方程的解數。

研究 5.2

如果對正整數 m，存在正整數 r 使得

$$1 + 2 + \cdots + (m-1) = (m+1) + (m+2) + \cdots + (m+r).$$

那麼我們稱 m 是一個 *Balancing number*。證明沒有 Lucas number 是 balancing number。

證明： 首先由 Pell 方程的基礎知識我們知道 balancing number y 是由下生成：

$$z + y\sqrt{8} = (3 + \sqrt{8})^m, \quad m = 1, 2, 3, \ldots \tag{4.7}$$

而 Lucas number y' 是由如下六個基本解所生成：

$$y' + x'\sqrt{5} = (3 + \sqrt{5})(9 + 4\sqrt{5})^n. \tag{4.8}$$
$$y' + x'\sqrt{5} = (7 + 3\sqrt{5})(9 + 4\sqrt{5})^n. \tag{4.9}$$
$$y' + x'\sqrt{5} = (18 + 8\sqrt{5})(9 + 4\sqrt{5})^n. \tag{4.10}$$
$$y' + x'\sqrt{5} = (1 + \sqrt{5})(9 + 4\sqrt{5})^n. \tag{4.11}$$
$$y' + x'\sqrt{5} = (4 + 2\sqrt{5})(9 + 4\sqrt{5})^n. \tag{4.12}$$
$$y' + x'\sqrt{5} = (11 + 5\sqrt{5})(9 + 4\sqrt{5})^n. \tag{4.13}$$

所要求的就是方程式 (3.7) 和方程式 (3.8∼13) 的公共解。現在只考慮 (3.7) 和 (3.8) 的公共解，也就是求出 (m, n) 滿足

$$\frac{(3 + \sqrt{8})^m}{\sqrt{8}} - \frac{(3 - \sqrt{8})^m}{\sqrt{8}} = (3 + \sqrt{5})(9 + 4\sqrt{5})^n + (3 - \sqrt{5})(9 - 4\sqrt{5})^n.$$

於是我們令

$$P = \frac{(3 + \sqrt{8})^m}{\sqrt{8}}, \quad Q = (3 + \sqrt{5})(9 + 4\sqrt{5})^n.$$

帶回去公共解的方程可以得到所要求為

$$P - 4P^{-1} = Q - \frac{1}{8}Q^{-1}.$$

亂估計知道

$$P - Q = 4P^{-1} - \frac{1}{8}Q^{-1} > 4(P^{-1} - Q^{-1}) = -4\frac{P-Q}{PQ}.$$

這代表 $P > Q$。然後又計算易知 $P > 90$, $P - Q < 4P^{-1}$，因此

$$\begin{aligned} 0 < \log\frac{P}{Q} &= -\log\left(1 - \frac{P-Q}{P}\right) < 4P^{-2} + 16P^{-4} \text{ (Tylor expansion)} \\ &< 4.16P^{-2} < \frac{0.00052}{(9+4\sqrt{5})^{2n}}. \end{aligned}$$

接著令

$$0 < \log\frac{P}{Q} = n\log(9+4\sqrt{5}) - m\log(3+\sqrt{8}) + \log(3+\sqrt{5})\sqrt{8} = \Lambda.$$

(故有 $4n > m$) 剩下就可以丟進估計了。取 $\alpha_1 = 9+4\sqrt{5}, \alpha_2 = 3+\sqrt{8}, \alpha_3 = (3+\sqrt{5})\sqrt{8}$，會有 $A_1 = 18, A_2 = 6, A_3 = 1024, B = 4n, d = 4$，由 Baker-Wüstholz theorem 有：

$$\log|\Lambda| > -(16\times 3\times 4)^{10}\log 18\log 6\log 1024\log 4n.$$

最後偷喵一下其他人長怎樣：

$$\begin{aligned} &\log\frac{P}{Q} < \log\left(\frac{0.00052}{(9+4\sqrt{5})^{2n}}\right) < -5.77n. \\ \Rightarrow\ &n < \frac{1}{5.77}(16\times 3\times 4)^{10}\log 18\log 6\log 1024\log 4n < 10^{24}\log 4n. \end{aligned}$$

這就得到了一個上界：$n < 10^{26}$。(3.7) 和其他方程的公共解也同理估一個上界，得證！ □

最後再提一個東西當做總結。關於丟番圖方程解數有限的問題，還有一個同樣很誇張的 Faltings' theorem：

定理 4.16 (Faltings' theorem) 虧格 (genus) 個數大於 1 的有理代數曲線上僅有有限個有理點。

比方說常見的圓錐 (二次) 曲線就是虧格個數為 0 的情況，這時無有理點或是有無窮多個有理點。至於虧格個數為 1 的情況則是無有理點或是全體有理點可有有限個有理點線性組合出。G.Faltings 理所當然的因為這個不可思議的定理 (原為 Mordell's conjecture) 的證明在 1986 年拿到了 Fields Medal。另外如果假設 abc 猜想成立，仍然可得到這個定理。

Chapter 5

正整數集上的 Ramsey 理論

這一章要介紹一些 Ramsey 理論，算是組合數論吧。1928 年，英國數學家 Frank Plumpton Ramsey 在倫敦數學學會上宣讀了一篇論文，正式宣告了一個數學理論的誕生之日，即是今日所謂的 Ramsey 理論。這個理論的中心思想是：給定一個結構，是否對任意我們想要的性質，都有辦法透過從結構中取出夠多元素而找到？當年 Ramsey 的論文即是在討論邊著色的超圖其子圖的任一完美子圖的單色性問題。

5.1 幾個經典結論

定理 5.1 (Ramsey 定理) 定義 $T^{(m)}$ 為集合 T 的所有 m 元子集構成的集合。給定正整數 n, k，那麼對於可數無窮集 $X^{(k)}$ 的任一個 n-染色，總存在一個無窮子集 A 使得 $A^{(k)}$ 是單色的。

上述定理是 Ramsey 定理的原始版本。今日我們常看到的通常是它的有限形式，比方說最有名的：世界上有六隻小貓，任兩隻都互相喜歡或沒感覺，那麼一定有遲鈍的三角戀。

■ **Schur's Theorem**

自最早 1892 年 Hilbert 的定理後，第二個提出 Ramsey 型定理的數學家大概是 Issai Schur。1916 年他發表研究了將近三年的論文 − 主題是有限域上的費馬最後猜想 − 並且證出了如下定理：

定理 5.2 (Schur 定理) 給定正整數 n，總存在正整數 $S(n)$，使得對於 $\{1, 2, \ldots, S(n)\}$ 的任一個 n-染色，方程式 $a + b = c$ 總有同色解。

證明： 我們知道存在一個正整數 $S(n)$ 使得對完全圖 $K_{S(n)}$ 的任一個 n-邊染色，總有同色三角形。現在將圖的頂點標號 $1, 2, \ldots, S(n)$，並且將邊 $e(ij)$ 塗上 $|i - j|$ 的顏色，任取圖中一同色三角形 ijk $(i < j < k)$ 出來，那麼 $(k - j) + (j - i) = (k - i)$ 為一組方程式 $a + b = c$ 的同色解。 □

要在定理中要求相異正整數 a, b, c 也是簡單的。大綱是：我們在原本的 n-染色再加

入新的 n 個顏色 (和原本一一對應) 變成 $2n$-染色，並在 $K_{S(2n)}$ 的邊 $e(ij)$ 塗上 $|i-j|$ 的顏色或新的 $|i-j|$ 的對應色，而這取決於 $[i/i-j]$ 是奇數或偶數。

Schur 定理宣稱了方程式 $a+b=c$ 同色解的存在性，我們自然會想把它推廣到更一般的形式：$a_1x_1+\cdots+a_nx_n=b$ 是否有同色解？例如 2012 年臺灣選訓一階的獨立研究題，證明 $x+2y=5z$ 可以藉由將正整數 5-染色而找不到同色解。

後來 Schur 指導了一名博士生 Rado 在他 1933 年的學位論文及之後的研究中，證明出一個更深刻的定理。首先定義名詞：如果對任意正整數 m，對於 $\mathbb{N}$ 的任一個 m-染色，方程式

$$a_1x_1+\cdots+a_nx_n=b.$$

總有同色解 $(x_1,\ldots,x_n)$，那麼稱此方程式為正則的 (regular)。例如 $a+b-c=0$ 就是正則的。

定理 5.3 (Rado's single equation theorem) 令 E 為方程式 $a_1x_1+\cdots+a_nx_n=0$。那麼 E 是正則的當且僅當某些 a_i 的和為 0。

接下來還可以談談 Rado 定理在高維齊次系統的推廣。2013 年暑假的數學營中，筆者原本提供了一道組合題當作獨立研究的預選題：「是否可將平面染有限種顏色，使得不存在同色正多邊形？」這題最後因為做不出來而沒選上。後來我考慮了它的弱化型式：「是否可將平面染有限種顏色，使得不存在同色正三邊形？」這時發現可以用複數將題目改成：「是否可將 $\mathbb{C}$ 有限染色，使得方程式 $x^2+y^2+z^2=xy+yz+zx$ 不存在同色解？」這時候就發現了，這其實是 Rado 定理在二次方程時的推廣。

類似的問題還有許多，諸如能否將 $\mathbb{N}$ 有限染色，使得方程式 $x^2+y^2=z^2$ 不存在同色解？等等，這些問題都是困難的。或者應該說，Rado 定理在高維情況下還是個猜想，基本上不用嘗試去解決類似的問題。不過有些方程式的確是可以用特殊的方法來做計算的，例如原本的同色正多邊形題，就是著名 Hales-Jewett 定理的一個推論。

■ Van der Waerden's Theorem

1920 年，Schur 又提出一個關於染色的猜想：正整數有限染色後，是否一定存在等差數列？這一直到 1926 年 Van der Waerden 從一位荷蘭學生那裡聽說後，才完全解決了它。隔年 Van der Waerden 在德國數學學會上發表此定理，造成數學界轟動，許多數學家深受此定理美感吸引，想要找到比原本更好的證明、以及提出另外一些推廣形式。這很快成為了數學家最喜愛的定理之一。

定理 5.4 (Van der Waerden 定理) 給定正整數 n,k，總存在正整數 $W(n,k)$ 使得對於 $\{1,\ldots,W(n,k)\}$ 的任一個 n-染色，存在長度為 k 的等差數列。

我們考慮 $n=2$ 的情況，假設已證出它成立。那麼容易推出命題中 $n=2$ 的無窮版本：對於 $\mathbb{N}$ 的任一個 2-染色，存在任意長的等差數列。事實上，如果能證明 $n=2$ 即可推到任意 n。因為可把原來 n 染色分兩小組，塗到 c_1 的正整數一組，塗到 $c_2,\ldots,c_n$ 的正整數一組，那麼有一組含很長的等差數列 $a_1,a_2,\ldots,a_t$，把這串等差數列和他對應到的

塗色 (組 c_1 或組 $c_2, \ldots, c_n$) 拿出來，再討論一次，持續這個過程，會得到對任意正整數 n-染色定含任意長的等差數列。

現在假設說對某個 k 不存在 $W(n,k)$ 了，那這代表對任一正整數 m，存在一種將 $\{1,\ldots,m\}$ n-染色的方法 C_m，使得沒有長度為 k 的等差數列。那麼在

$$C_1, C_2, \ldots$$

中，由於 1 只被染成 n 種顏色之一，所以由鴿籠原理我們知道有

$$C_1^{(1)}, C_2^{(2)}, \ldots$$

使得這些染色法中 1 都被塗到某色 i_1。然後在新的這個序列 $\langle C_i^{(1)} \rangle$ 中再找 2 被塗成同色 i_2 的子序列。持續這個過程，我們知道有

$$C_1^{(n)}, C_2^{(n)}, \ldots$$

使得這些染色法中 t 都被塗到某色 i_t $(1 \leq t \leq n)$。現在考慮新的染色法 C，他把正整數 t 塗到 i_t $(\forall t \in \mathbb{N})$，那麼這個染色法亦不包含長度為 k 的等差數列 (否則在某個染色法 $C_i^{(n)}$ 中就有了)。即是說，可把正整數有限染色而不包含長度為 k 的等差數列，這和無窮版本矛盾。

命題中宣稱可以找到任意長的等差數列，但這卻不代表存在無窮長的等差數列。而事實上也是有染色法可以推翻後者的，想想看吧。另外你可能注意到了，最後 2-染色這看起來較弱的版本，竟然能蘊含原本較強的結論。這種手法其實和證明 Ramsey number 是類似的，把某些顏色綁在一起看做一種新顏色，就可以一直歸納上去。

另外還有許多等差數列的相關問題。像是 2004 年的 Green-Tao 定理：存在任意長的質數等差數列。而如果偷用 Van der Waerden 定理還可以改成：對質數的任意有限染色，必存在任意長的等差數列。或是關於冪次數能否成等差的研究，最有名的大概是 1997 年 Darmon 和 Merel 證明的：三次以上的冪次數不存在三項的等差數列。而我們知道平方數裡卻有無窮多組三項等差數列，那麼是否可把他們有限染色使得不會有單色的這種數對呢？

■ The Density Theorem

Van der Waerden's theorem 斷言，把正整數有限染色後必定含有無窮長的等差數列，卻沒有告訴我們要多大的集合才會有這種性質。具體來說，對於什麼樣的正整數子集 T，什麼條件能保證其中含有無窮長的等差數列呢？兩名匈牙利數學家 P.Erdős 以及 P.Turán 曾提出猜想：

猜想 5.1 令 A 為正整數的一個子集，定義 $A(n) = A \cap \{1,\ldots,n\}$，以及其上密度：

$$\bar{d}(A) = \limsup_{n\to\infty} \frac{|A(n)|}{n}.$$

那麼如果正整數子集 T 有正的上密度，則 T 會含有無窮長的等差數列。

這個猜想被匈牙利青年數學家 E.Szemerédi 在 1973 年完全證明出來，他的成就被譽為組合數論裡的一大傑作。而 Erdős 則獎賞他 1000 美元的獎金 − 這是他曾付過的最高金額，也是他提出過為數眾多的懸賞難題的第二高金額。最高的是比上述更強的一個猜想：

猜想 5.2 令 T 為正整數的一個子集，那麼如果 T 的元素倒數和發散，則 T 會含有無窮長的等差數列。

在 Szemerédi 用組合方法證出密度定理的兩年後，1977 年 Harry Furstenberg 用了歷遍理論 (Ergodic Theory) 中的方法給出了完全不同的證法，事實上，他開創了一個全新的數學分支 − Ergodic Ramsey Theory。

Problem set

P1. Schur's theorem

Let n be a positive integer. Prove that there exists an integer N such that for any prime $p > N$, the congruence equation $x^n + y^n \equiv z^n \pmod{p}$ has a non-trivial solution.

P2. Determine if there exist a finite-coloring of positive integer such that one can find a function $f : \mathbb{N} \to \mathbb{N}$, such that $x + f(y)$ and $y + f(x)$ have the different colors for all $x, y \in \mathbb{N}$.

P3. Prove that the set of positive integers cannot be partitioned into three nonempty subsets such that for any two integers x, y taken from two different subsets, the number $x^2 - xy + y^2$ belongs to the third subset.

P4. KöMaL 2012

Show that the positive integers can be coloured with three colours in such a way that the equation $x + y = z^2$ has no solution (x, y, z) consisting of distinct numbers with the same colour.

P5. Let n be a positive integer. Determine the size of the largest subset of $\{-n, -n + 1, \ldots, n - 1, n\}$ which does not contain three elements a, b, c (not necessarily distinct) satisfying $a + b + c = 0$.

P6. Prove that every finite-coloring of positive integer contains an arithmetic progression of any given finite length, whose common difference is a perfect square.

P7. If for some coloring of $\mathbb{N}$ there is a solution to a certain equation with all its variable belonging to different color classes, we called it a *rainbow* solution. Show that for any 3-coloring of positive integer there is a rainbow $AP(3)$. And there is a coloring of $\mathbb{N}$

with infinitely many colors, with each color having positive density such that there is no rainbow $AP(3)$.

■ 補充習題— Roth 定理

因為這一章好像有點短所以筆者偷抄在《集合中的組合數學》的最後一個習題。我們可以考慮 Van der Waerdern 定理的密度問題 (Szemerédi 定理)：將正整數集染色後，如果有「足夠多」的正整數都被塗上某種顏色，是否可以找到任意長且被塗上這種顏色的單色等差數列？這個習題將帶領讀者證明上述問題的一個較弱版本，也為第二部加性數論一章先打一點基礎：

定理 5.5 對所有 $\delta > 0$，當 $n > \exp\exp(1200/\delta)$ 時，只要 $A \subseteq [n]$ 包含至少 δn 個元素，那麼 A 中就有長度為 3 的等差數列 (即 3 個數成等差數列)。

—預備知識—

離散 Fourier 分析是現今加性數論的主流方法，這是由數學家 Timothy Gowers 在 1998 年重新證明 Szemerédi 定理時所引入的，我們以下將介紹這個工具。

提醒讀者對正整數 n，將以 $[n]$ 簡記集合 $\{1, 2, \ldots, n\}$。而對於集合 A，將用 1_A 表示他的判斷函數，也就是說 $1_A(x) = 1$ 如果 $x \in A$，否則 $= 0$。以下為了節省符號，如非特別說明則所有的函數都是指從 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}$ 的函數，並引入 X_n 是 $\mathbb{Z}/n\mathbb{Z}$ 上的均勻隨機變數，並以 $\mathbb{E}$ 表示期望值。對於不熟悉機率的讀者，可以把這些東西就當成一種縮寫，而他們的意義就是說當 f 是一個從 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}$ 的函數時

$$\mathbb{E}[f(X_n)] = \frac{1}{n} \sum_{x \in \mathbb{Z}/n\mathbb{Z}} f(x).$$

最後我們以 $e_n(\cdot)$ 記從 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}$ 的函數

$$e_n(x) = \exp\left(2i\pi \frac{x}{n}\right) = \cos\left(\frac{x}{n}\right) + i \sin\left(\frac{x}{n}\right).$$

1. 證明當 $r \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ 時 $\mathbb{E}[e_n(rX_n)] = 0$，否則 $= n$.

2. 當 f 是一個函數時，定義 $\widehat{f}$ 如 $\widehat{f}(r) = n\mathbb{E}[f(X_n)e_n(-rX_n)]$ 是一個從 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}$ 的函數，這個過程稱為 Fourier 變換。證明 Fourier 反演：

$$f(x) = \sum_{r \in \mathbb{Z}/n\mathbb{Z}} \widehat{f}(r) e_n(rx), \ \forall\, x \in \mathbb{Z}/n\mathbb{Z}.$$

3. 證明 Parseval 恆等式

$$\sum_{r \in \mathbb{Z}/n\mathbb{Z}} |\widehat{f}(r)|^2 = n \sum_{r \in \mathbb{Z}/n\mathbb{Z}} |f(r)|^2.$$

4. 當 f, g 為兩個函數時，可以定義卷積 $f * g$ 為 $(f * g)(r) = n\mathbb{E}[f(X_n)g(r - X_n)]$ 仍然是一個從 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}$ 的函數。取三個函數 f, g, h，證明

(a) $f*g = g*f$, $(f*g)*h = f*(g*h)$.

(b) $f*(g+h) = f*g + f*h$.

(c) $\widehat{f*g} = \widehat{f}\cdot\widehat{g}$.

(d) $\mathbb{E}[(f*g)(X_n)] = \mathbb{E}[f(X_n)]\mathbb{E}[g(X_n)]$.

利用 (c) 證明對於 $\mathbb{Z}/n\mathbb{Z}$ 的任意子集 A 總有

$$\sum_{(x,d)\in(\mathbb{Z}/n\mathbb{Z})^2} 1_A(x)1_A(x+d)1_A(x+2d) = \frac{1}{n}\sum_{x\in\mathbb{Z}/n\mathbb{Z}} \widehat{1_A}(x)^2\widehat{1_A}(-2x).$$

5. 證明

$$f*g(r) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}^2} f(y)e_n(-yr)\sum_{x\in\mathbb{Z}/n\mathbb{Z}^2} g(x-y)e_n(-(x-y)r)$$

6. 對於 $\mathbb{Z}/n\mathbb{Z}$ 的兩個子集 A, B，記得定義 $A+B = \{a+b \mid a\in A, b\in B\}$。試找出 $A+B$ 和 $1_A * 1_B$ 的關係。

—第一部分—

給定 $\mathbb{Z}/n\mathbb{Z}$ 的一個有序子集 P，當它可以被看作是在 $\mathbb{Z}$ 上的等差數列時，我們說 P 是 $\mathbb{Z}$-等差的。例如說在 $\mathbb{Z}/7\mathbb{Z}$ 中，有序子集 $\{5,1,4\}$ 是一個等差數列，因為 $1-5 = 3 = 4-1$，然而它並不是 $\mathbb{Z}$-等差的。另一方面有序子集 $\{2,4,6\}$ 就同時是等差數列和 $\mathbb{Z}$-等差的。我們要證明以下性質：

宣稱 1 假設 $1 \geq \delta > 0$ 且 $n \geq 50/\delta^2$，那麼對所有包含至少 δn 個元素的 $A \subseteq \mathbb{Z}/n\mathbb{Z}$，只要對於所有 $r \in \mathbb{Z}/n\mathbb{Z}\setminus\{0\}$ 都有 $|\widehat{1_A}(r)| \leq \delta^2 n/100$，那麼以下敘述有至少一者為真。

(i) 在 A 中有長度為 3 的 $\mathbb{Z}$-等差數列。

(ii) 存在一個 $\mathbb{Z}$-等差數列 $P \in \mathbb{Z}/n\mathbb{Z}$，它的長度 $\geq \lfloor n/3\rfloor$，且滿足 $|A\cap P| \geq (\delta+\delta/6)|P|$.

1. 把 $\mathbb{Z}/n\mathbb{Z}$ 不相交地分成 3 個子集合 $I_1 = \{0,\ldots,\lfloor n/3\rfloor-1\}, I_2 = \{\lfloor n/3\rfloor,\ldots,\lfloor 2n/3\rfloor-1\}, I_3 = \{\lfloor 2n/3\rfloor,\ldots,n-1\}$，並令 $B = A\cap I_2$。以下假設條件 (ii) 不為真，證明有 $|B| \geq \delta n/5$.

2. 令 $N(A)$ 為 $y-x \equiv z-y \pmod n$ $(x,y,z)\in A\times B\times B$ 的解數。證明 $N(A)$ 只會算到 $\mathbb{Z}$-等差數列。

3. 由於在 $N(A)$ 的定義中沒有規定不能有 $x=y=z$，所以會把退化的 $\mathbb{Z}$-等差數列也算進去。我們可以用一個很粗略的估計：A 中至少有 $N(A)-|B| \geq N(A)-n$ 個長度為 3 的的 $\mathbb{Z}$-等差數列，因此為了證明條件 (i) 為真，只須證明 $N(A) > n$.

寫出

$$N(A) = \frac{1}{n} \sum_{r\in\mathbb{Z}/n\mathbb{Z}} \sum_{x\in A} \sum_{y\in B} \sum_{z\in B} e_n((2y-x-z)r)$$
$$= \frac{1}{n} \sum_{r\in\mathbb{Z}/n\mathbb{Z}} \widehat{1_A}(r) \cdot \widehat{1_B}(-2r) \cdot \widehat{1_B}(r).$$

4. 由 Cauchy 不等式證明

$$N(A) \geq \frac{1}{n}|A||B|^2 - \frac{1}{n} \max_{r\neq 0} |\widehat{1_A}(r)| \cdot \left(\sum_{r\neq 0} |\widehat{1_B}(-2r)|^2\right)^{1/2} \cdot \left(\sum_{r\neq 0} |\widehat{1_B}(r)|^2\right)^{1/2}.$$

5. 注意到當 s 固定時 $s \equiv -2r \pmod n$ 至多只有兩個解 r，證明 $\sum_{r\neq 0} |\widehat{1_B}(-2r)|^2 \leq 2\sum_{r\neq 0} |\widehat{1_B}(r)|^2$。並由宣稱中的敘述得到

$$N(A) \geq \frac{|A||B|^2}{n} - \frac{\delta^2}{50\sqrt{2}} \sum_{r\neq 0} |\widehat{1_B}(r)|^2.$$

6. 利用 Parseval 恆等式證明條件 (i) 為真。

—第二部分—

宣稱 2 如果 $n \geq 50$ 且 $\delta > 0$，那麼對所有包含至少 δn 個元素的 $A \subseteq \mathbb{Z}/n\mathbb{Z}$，以下敘述至少一者為真。

(i) 對所有 $r \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$，有 $|\widehat{1_A}(r)| \leq \delta^2 n/100$.

(ii) 在 $\mathbb{Z}/n\mathbb{Z}$ 中存在一個至少有 $\delta^2\sqrt{n}/5000$ 個元素的一個 $\mathbb{Z}$-等差有序子集 P，使得 $|A \cap P| \geq (\delta + \delta^2/800)|P|$.

給定 $n \geq 50$，並取一個包含至少 δn 個元素的 $A \subseteq \mathbb{Z}/n\mathbb{Z}$，假設敘述 (i) 是不成立的，那麼我們要敘述 (ii) 成立。由假設取某個 $r \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ 使得 $|\widehat{1_A}(r)| > \delta^2 n/100$.

1. 令 m 是小於等於 $n/(6\lceil\sqrt{n}\rceil)$ 的最大正整數，首先要找到 $\mathbb{Z}/n\mathbb{Z}$ 中一個長度為 $2m+1$ 且有夠好性質的等差數列。

   考慮數 $jr \pmod n$ $(j = 0, \ldots, \lceil\sqrt{n}\rceil)$，由鴿籠原理證明存在正整數 λ 使得

$$\lambda \leq \lceil\sqrt{n}\rceil, \quad |\lambda r \,(\mathrm{mod}\, n)| \leq \lceil\sqrt{n}\rceil.$$

2. 藉由考慮集合 $\{-m\lambda, -(m-1)\lambda, \ldots, -\lambda, 0, \lambda, \ldots, (m-1)\lambda, m\lambda\}$ 證明 $\mathbb{Z}/n\mathbb{Z}$ 中有一個長度為 $2m+1$ 的等差數列。令這個集合為 Q.

3. 證明對這個集合 Q，有 $\widehat{1_Q}(r) > |Q|/2$.

4. 令 f_A 是由 $f_A(x) = 1_A(x) - |A|/n$ 給出的函數，而 $h_{A,Q} = f_A * 1_Q$。證明

$$\mathbb{E}[|h_{A,Q}(X_n)|] \geq \frac{1}{n}|\widehat{f_A}(r)||\widehat{1_Q}(r)|, \quad \mathbb{E}[h_{A,Q}(X_n)] = 0.$$

5. 由前述證明

$$\mathbb{E}[h_{A,Q}(X_n) + |h_{A,Q}(X_n)|] \geq \frac{\delta^2}{200}|Q|.$$

因此可取到 $x \in \mathbb{Z}/n\mathbb{Z}$ 使得 $h_{A,Q}(x) \geq \frac{\delta^2}{400}|Q|$.

6. 藉由考慮除以 n 的餘數，可以把 $Q_x = \{x - q \mid q \in Q\}$ 當成是 $\mathbb{Z}/n\mathbb{Z}$ 的子集。由定義證明

$$h_{A,Q}(x) = |A \cap Q_x| - \frac{|A|}{n}|Q_x|.$$

7. 注意到 $|Q_x| = |Q|$，由上述證明

$$|A \cap Q_x| \geq \left(\delta + \frac{\delta^2}{400}\right)|Q|.$$

8. 藉由寫成

$$Q = \{-m\lambda \,(\mathrm{mod}\, n), \ldots, 0 \,(\mathrm{mod}\, n), \ldots, m\lambda \,(\mathrm{mod}\, n)\}$$

證明 Q 可以寫成兩個 $\mathbb{Z}$-等差數列的聯集；類似地證明 Q_x 可以寫成兩個 $\mathbb{Z}$-等差數列的聯集，並假設這兩個 $\mathbb{Z}$-等差數列叫做 P 和 P'.

9. 證明當 P 和 P' 其中一個集合只包含 $< \delta^2|Q_x|/800$ 個元素時，另一個集合將會滿足條件 (ii).

10. 我們於是假設 P 和 P' 都包含 $\geq \delta^2|Q_x|/800$ 個元素。證明對其中一者，比方說 P，會有

$$\frac{|A \cap P|}{|P|} \geq \frac{|A \cap Q_x|}{|Q_x|} \geq \delta + \frac{\delta^2}{400}.$$

利用 $n \geq 50$ 證明這個集合會滿足條件 (ii)。至此宣稱證畢。

—第三部分—

現在用上述兩個宣稱證明定理 5.5。對 $\delta > 0$，以 $H(\delta)$ 記命題「當 $n > \exp\exp(1200/\delta)$ 時，只要 $A \subseteq [n]$ 包含至少 δn 個元素，那麼 A 中就有長度為 3 的等差數列。」以下將使用的方法叫做 density increment argument，這個論述的想法是說，首先 $\delta \geq 1$ 時命題是顯然為真的，而如果進一步存在某個函數 f 使得有蘊含式 $H(f(\delta)) \Rightarrow H(\delta)$，並且對所有 $\delta > 0$ 將 f 迭代夠多次之後總會有 $f(\delta) \geq 1$ 時，那麼命題總是成立的！

在以上的兩個宣稱中，我們觀察到下列重要性質

- 總會把 A 放進某個 $\mathbb{Z}$-等差數列 P 中，使得 $A \cap P$ 在 P 中的密度變得更大 (也就是說 $|A \cap P|/|P| \geq |A|/n$)。

- 如果說可以在 $A \cap P$ 中取出一個「對於 P 為 $\mathbb{Z}$-等差數列」的 $\mathbb{Z}$-等差數列，那麼這個 $\mathbb{Z}$-等差數列對於 $\mathbb{Z}/n\mathbb{Z}$ 仍為一個 $\mathbb{Z}$-等差數列。

在定理 5.5 中我們要求 $A \subseteq [n]$，但其實可以考慮 $A_0 = \{a - 1 \mid a \in A\} \in \mathbb{Z}/n\mathbb{Z}$。試利用以上觀察到的兩個性質以及 density increment argument 證明定理 5.5。

評論 5.1 以上的兩個宣稱說明的是一個集合的 Fourier 係數與這個集合表現得像不像等差數列之間的關係，可以定義所謂的 Fourier 權重 $\|A\|_u$ 為

$$\|A\|_u = \max_{r \neq 0} |\widehat{1_A}(r)|.$$

會有許多 Fourier 權重和等差數列之間的關係式，另外預備知識的第 4, 6 小題告訴我們可以用這樣的方法來計算和集 $A + B$ 中等差數列的數量。

對於想多了解離散 Fourier 分析在加性數論上應用的讀者，可以參考這篇課程講義 (http://math.rice.edu/~kk43/cmcthesis.pdf)，另外對於較一般的討論可以閱讀文獻 T. Terence & V. Van. *Additive Combinatorics. Cambridge Studies in Advanced Mathematics. 105.* Cambridge University Press (2006). 和另一篇講義 (https://www.math.cmu.edu/~af1p/Teaching/AdditiveCombinatorics/Tao.pdf).

Chapter 6

遞迴

6.1 簡介

在數學上，遞迴 (Recursion)，是指在函式的定義中使用函式自身的方法，就是說，一種遞推地定義一個序列的方程式：序列的每一項是定義為前幾項的函數。競賽數學裡關於遞迴關係中的數論問題大概可以分為兩類：

- 遞迴關係中含有取最大公因數、開根號等等，感覺有東西會變少 (小) 的。
- 隱藏得很好，讓你不知道有好的遞迴式存在：題目通常出現平方後再開根號關係。
- 高次方的遞迴式。

它們處理的方式也都蠻固定的。第一種明顯就是要你對其中一個東西賦值，可能是某數質因數分解式中所有質數冪次總和啊、寫成分數形式後分子加分母的和之類的，然後進行無窮遞降法，這就多多練習抓感覺。至於第三種沒有什麼一般的方向可以抓，可以用例題 1.3 摸看看。最後是第二種，就是典型的 Vieta jumping 題，你把數列前幾項寫出來後，大概就會發現他有 2 階的齊次遞迴，例如：$a_1 = 1$, $a_{n+1} = 2a_n + \sqrt{3a_n^2 + 1}$. 證明每項都是整數。

今天我們要介紹的主要是整數遞迴數列中的整除關係。你明年可能碰到這樣的問題：試求出 Fibonacci sequence 第 2014 項的十位跟個位是多少。當算到某一項時，你好像發現了這個數列的末兩位數好像會循環！哼哼，這其實是有原因的，事實上：

定理 6.1 如果遞迴數列 $\langle a_n \rangle$ 的遞迴關係是

$$a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k}).$$

其中 f 是多項式。那麼對任意正整數 m，數列 $\langle a_n \pmod m \rangle$ 都是循環的。

證明： 我們觀察數列 $\langle a_n \pmod m \rangle$ 中的連續 k 項，由於在 $\bmod m$ 下只有有限種可能 (最多就 m^k 種)，因此由鴿籠原理知道必定有兩段連續 k 項是相等的，這個數列每一項都可由它前面的連續 k 項依同樣的規則決定，因此數列 $\langle a_n \pmod m \rangle$ 必是循環的。 □

評論 6.1 注意到這說明了 Fibonacci sequence 對模任意正整數是循環數列，又因為這個數列每一項都可由它前面 (或後面) 的連續兩項決定，且 $f_0 = 0$，所以對模任意正整數都有無窮多項是 0，也就是說對任意正整數 m，Fibonacci sequence 裡有無窮多項是 m 的倍數！

為方便研究，我們定義說：

定義 6.1 對於循環數列 $\langle a_n \rangle$，假設說正整數 T 使得

$$a_{n+T} = a_n$$

對所有 n 都成立 (事實上只要對足夠大的 n 成立就好，不過這邊感興趣的是對所有 n 都成立的情況)，那麼我們稱 T 為這個數列的**週期** (period)。並且稱這些 T 裡面最小的那個為**最小週期**。(在 Fibonacci sequence 中又稱做 **Pisano period**)

定義完之後會發現一件比較麻煩的事，我們在研究的週期不只一個，這時候搞不好這些週期還有各自的性質，可我們又不可能一一去研究。然而你想到數論問題裡面很多時候都會有最小週期整除週期的情況發生 (比如某數對 $\mathbb{Z}/p\mathbb{Z}$ 的 order)，會不會循環數列也有這種性質呢？

重要性質——★ 如果循環數列 $\langle a_n \rangle$ 的最小週期是 T，而 T' 是任一週期，那麼 $T \mid T'$。

證明： 由定義，必須要有

$$a_{n+T} = a_n \quad \text{以及} \quad a_{n+T'} = a_n \ \forall n.$$

又由輾轉相除法，我們可以找到整數 d, d' 使得 $dT + d'T' = \gcd(T, T')$。這時候會有

$$a_n = a_{n+T} = a_{n+2T} = \cdots = a_{n+dT} = \cdots = a_{n+dT+d'T'} = a_{n+\gcd(T,T')} \ \forall n.$$

然而我們已宣稱 T 是最小週期，因此 $\gcd(T, T') = T$，即 $T \mid T'$。 □

先讓我們回到一開始的問題：Fibonacci sequence 第 2014 項的十位跟個位是多少？由中國剩餘定理可以知道，事實上你只需分別求出第 2014 項 mod 4 和 mod 25 是多少就好了，因為很快就可以發現：其實 mod 100 的最小週期就是 mod 4 和 mod 25 的最小週期的最小公倍數吧！而且這命題還可以再加強一點：

定理 6.2 假設一數列 $\langle a_n \rangle$ 在模任何正整數下都是循環的，且計 mod x 下的最小週期是 $T(x)$。那麼當 $(m, n) = 1$ 時，$T(mn) = \text{lcm}[T(m), T(n)]$。

證明： 首先由定義有 $a_{x+\text{lcm}[T(m),T(n)]} \equiv a_x \pmod{m}$，對 mod n 也成立，因此 $T(mn) \mid \text{lcm}[T(m), T(n)]$。再來由於 $a_{x+T(mn)} \equiv a_x \pmod{mn}$ 對所有 x 都要成立，因此

$$a_{x+T(mn)} \equiv a_x \pmod{m}$$

$$a_{x+T(mn)} \equiv a_x \pmod{n}$$

這兩式對所有 x 都必須要成立。由重要性質就知道 $T(m), T(n) \mid T(mn)$，所以 $\operatorname{lcm}[T(m), T(n)] \mid T(mn)$。綜上 $T(mn) = \operatorname{lcm}[T(m), T(n)]$。 □

有了這個定理，如果說你想要研究某一遞迴數列在模 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 的最小週期時，實際上只要求出模 p^i 的週期就好了！

例題 1.1: Italy MO 2007

考慮以下給定的數列：$x_1 = 2$, $x_{n+1} = 2x_n^2 - 1$，對所有 $n \geq 1$。證明對所有 $n \geq 1$，n 和 x_n 都是互質的。

證明： 首先當 $n = 1$ 時結論是成立的。現在考慮 n 的任一質因數 p，我們想要證明的就是 p 和 x_n 互質，而 n 可以是 p 的任何一個倍數，因此自然會想到去分析 $\langle x_n \pmod p \rangle$ 的週期。

考慮數列 $\langle x_n \pmod p \rangle_{n=1}^{p-1}$。只要當中有任何一個數是 0 或 1，那麼我們知道 $x_{p-t} \bmod p$ 只能是 -1 或 1，此時結論成立。如果當中沒有任何一個數是 0 或 1，那麼這 $p-1$ 個數只能有 $p-2$ 種取值，因此有兩個數是一樣的，那麼顯見這時候產生了一個週期，一個週期中任一數又不能是 0 (否則變成 $0, -1, 1, 1, \ldots$)，此時結論亦成立。綜上得證。 □

例題 1.2: ISL 1998 Q1

整數數列 $\langle a_n \rangle$ 是由以下的遞迴關係所定義：

$$a_0 = 0,\ a_1 = 1,\ a_{n+2} = 2a_{n+1} + a_n.$$

試證 2^k 整除 a_n 當且僅當 2^k 整除 n。

證明： 我們先宣稱他和 Fibonacci 數列有相同的性質：(1) $a_{m+n} = a_{m-1}a_n + a_m a_{n+1}$、(2) 如果 $m \mid n$，那麼 $a_m \mid a_n$。其中 (1) 可以對 $m+n$ 做數學歸納法證明，或是用矩陣證。(2) 的話則是使用輾轉相除法。

分析一下題目要求證的：$v_2(a_n) = v_2(n)$，我們可能會希望用數學歸納法的想法證明。首先我們把這數列模 2 和模 4，易看出週期分別是 0, 1 和 0, 1, 2, 1，因此題目的結論在 $k = 1, 2$ 時是成立的。再來在 (1) 中帶入 $m = n$，得到 $a_{2n} = a_n(a_{n-1} + a_{n+1}) = 2a_n(a_{n-1} + a_n)$，所以 $v_2(a_{2n}) = v_2(2a_n(a_{n-1} + a_n)) = v_2(a_n) + 1$ (因為 $a_{n-1} + a_n$ 是奇數)，因此用數學歸納法就知道結論在 k 為任意正整數時都成立。 □

評論 6.2 這種利用恆等式去求出對某個質數的冪次在 2 階齊次遞迴中很常見，然後證明中所用的輾轉相除法還可以做出一般 2 階遞迴很多好用的整除或最大公因數等等的性質。如果想練習更多這類型的題目，可以參考 PEN。

例題 1.3: German TST 2009

數列 $\langle a_n \rangle$ 定義為：$a_1 = 1$ 且 $a_{n+1} = a_n^4 - a_n^3 + 2a_n^2 + 1$，對所有 $n \geq 1$。試證存在無窮多個質數 p 使得任一個 a_n 都不被 p 整除。

證明： 首先注意到我們可以用 $a_0 = 0$ 生出同樣的數列。然後看一下剛剛學的：這樣的數列 $\langle a_n \pmod p \rangle$ 必定是循環的。那麼你會發現，題目其實是要求證明無窮多個質數 p，使得 $\langle a_n \pmod p \rangle$ 的循環節裡不包含 0。

先觀察一下遞迴式，因為有一項係數是 2 跟其他人不一樣很奇怪，所以你可能會想移項成

$$a_{n+1} - a_n = (a_n^2 + 1)(a_n^2 - a_n + 1).$$

然後我們想證的是 $\langle a_n \pmod p \rangle$ 的循環節裡不包含 0，可是又已經有 $a_0 = 0$，所以我們知道要取的 p 一定不能讓循環節包含 a_0。這代表知道要取的 p 會讓 $\langle a_n \pmod p \rangle = \langle b_0, b_1, \ldots, \overline{c_1, \ldots, c_i} \pmod p \rangle$ (就是說 $\langle a_n \rangle$ 前幾項不在循環節裡)。為了讓數列循環，你可能會想到取 $p \mid a_{m+1} - a_m$。

現在要說明的是為什麼這樣的 p 為什麼會滿足題意：首先看出 $(a_{m+1}, a_m) = 1$，再來因為 $a_{m+1} \pmod p = a_m \pmod p$，因此由同樣的遞迴公式可以得到 $a_m \pmod p = a_{m+1} \pmod p = a_{m+2} \pmod p = \cdots$！而如果有某項 a_i 滿足 $a_i \pmod p = 0$，又因為 $a_0 \pmod p = 0$，這會代表 $\langle a_n \pmod p \rangle$ 的循環節裡包含 0，但我們知道循環節剛好是 $\overline{a_m}$，矛盾！因此這樣的 p 會滿足要求。

接著還要證明可以取到無窮多個 p。這是簡單的，因為假設 $q^s \mid\mid a_{m+1} - a_m$ (其中 q 為奇質數)，那麼帶入移項過後的遞迴式我們仍有 $q^s \mid\mid a_{k+1} - a_k \ \ \forall k \geq m$。而易計算 $v_2(a_{m+1} - a_m) = v_2\big((a_m^2+1)(a_m^2 - a_m + 1)\big) = 2$ (因為數列每項都是奇數)。且 $\langle a_{n+1} - a_n \pmod p \rangle$ 又是嚴格遞增的，因此 p 要有無窮多個。 □

Problem set

P1. ISL 2010 A5

Denote by $\mathbb{Q}^+$ the set of all positive rational numbers. Determine all functions $f : \mathbb{Q}^+ \to \mathbb{Q}^+$ which satisfy the following equation for all $x, y \in \mathbb{Q}^+$:

$$f\left(f(x)^2 y\right) = x^3 f(xy).$$

P2. ISL 2008 N3

Let $a_0, a_1, a_2, \ldots$ be a sequence of positive integers such that the greatest common divisor of any two consecutive terms is greater than the preceding term; in symbols, $\gcd(a_i, a_{i+1}) > a_{i-1}$. Prove that $a_n \geq 2^n$ for all $n \geq 0$.

P3. Let $P(x)$ be a nonzero polynomial with integer coefficients. Let $a_0 = 0$ and for $i \geq 0$ define $a_{i+1} = P(a_i)$. Show that $\gcd(a_m, a_n) = a_{\gcd(m,n)}$.

P4. ISL 2015 N4

Suppose that $a_0, a_1, \ldots$ and $b_0, b_1, \ldots$ are two sequences of positive integers such that $a_0, b_0 \geq 2$ and

$$a_{n+1} = \gcd(a_n, b_n) + 1, \qquad b_{n+1} = \operatorname{lcm}[a_n, b_n] - 1.$$

Show that the sequence a_n is eventually periodic; in other words, there exist integers $N \geq 0$ and $t > 0$ such that $a_{n+t} = a_n$ for all $n \geq N$.

P5. ISL 2015 N6

For any $m, n \in \mathbb{N}$ we write $f^n(m) = \underbrace{f(f(\cdots f}_{n \text{ times}}(m)\cdots))$. Suppose that f has the following two properties:

(a) If $m, n \in \mathbb{N}$, then $\frac{f^n(m)-m}{n} \in \mathbb{N}$;

(b) The set $\mathbb{N} \setminus \{f(n) \mid n \in \mathbb{N}\}$ is finite.

Prove that the sequence $f(1) - 1$, $f(2) - 2$, $f(3) - 3, \ldots$ is periodic.

P6. ELMO 2010 N4

Let r and s be positive integers. Define $a_0 = 0, a_1 = 1$, and $a_n = ra_{n-1} + sa_{n-2}$ for $n \geq 2$. Let $f_n = a_1 a_2 \cdots a_n$. Prove that $\dfrac{f_n}{f_k f_{n-k}}$ is an integer for all integers n and k such that $n > k > 0$.

P7. USAMO 1993

Let a and b be odd positive integers. Define the sequence $\langle f_n \rangle$ by putting $f_1 = a$, $f_2 = b$, and by letting f_n for $n \geq 3$ be the greatest odd divisor of $f_{n-1} + f_{n-2}$. Show that f_n is constant for sufficiently large n and determine the eventual value as a function of a and b.

P8. Brazil MO 2004

Consider the sequence $\langle a_n \rangle_{n=0}^{\infty}$ given by $a_0 = a_1 = a_2 = a_3 = 1$ and

$$a_n a_{n-4} = a_{n-1} a_{n-3} + a_{n-2}^2.$$

Prove that all its terms are integers.

P9. ISL 2014 N7

Let $c \geq 1$ be an integer. Define a sequence of positive integers by $a_1 = c$ and

$$a_{n+1} = a_n^3 - 4c \cdot a_n^2 + 5c^2 \cdot a_n + c$$

for all $n \geq 1$. Prove that for each integer $n \geq 2$ there exists a prime number p dividing a_n but none of the numbers $a_1, \ldots, a_{n-1}$.

P10. KöMaL 2013

Denote by u_n the n-th Fibonacci number ($u_1 = u_2 = 1$, $u_{n+}1 = u_n + u_{n-1}$). Prove that if $a, b, c > 1$ are integers such that a divides u_b, b divides u_c and c divides u_a, then 5 divides a, b and c, or 12 divides a, b and c.

P11. KöMaL 2000

A sequence of numbers is called of Fibonacci-type if each term, after the first two, is the sum of the previous two. Prove that the set of positive integers can be partitioned into the disjoint union of infinite Fibonacci-type sequences.

P12. Given a finite set S of positive integers, show that there exists a linear recursive sequence

$$a_1, a_2, a_3, \ldots$$

such that $\{n \mid a_n = 0\} = S$.

6.2 補充教材——體擴張

這個小節主要要介紹算 Fibonacci 數列模 p 的週期的方法，提醒讀者剛剛已經證明過想要研究某一遞迴數列在模 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 的最小週期時，實際上只要求出模 p^i 的週期就好了。在計算之前，我們先定義 $\phi = (1 + \sqrt{5})/2$, $\bar{\phi} = (1 - \sqrt{5})/2$，並先討論最簡單的情況：模 p 的週期。

首先你可能會迷惘，怎麼可能求的出週期呢？我們對 Fibonacci 數列就強力的了解就是它的封閉式，難道你要我真的用那個一般式去炸週期嗎，不好笑啊。所以現在要介紹一點抽象代數的結構：Field Extenstion 以及 Splitting Field。

Field 筆者在此假定各位至少知道它的定義 (可以做加減乘除的地方)，以及會把一些像同餘運算、指數原根二次剩餘等寫成 $\mathbb{F}_p$ 的形式表達了。首先介紹 Field Extenstion。

回顧數學的發展過程，人類依次引入了正整數、非負整數、有理數、實數、複數。在這過程中，基本都是因為「某個方程在現有的代數結構中找不到解，所以引入新的概念」。因為 $x + 1 = 2$ 無正整數解，所以引入負整數和 0；因為 $2x = 1$ 無整數解，所以引入有理數；因為 $x^2 = 2$ 無有理數解，所以引入根號；因為 $x^2 = -1$ 無實數解，所以引入複數。那麼，什麼叫做「引入新的代數結構」?

這其實純粹是個理想化數學的方法，因為現在找不到，所以我們加新東西進去讓它更完美。比如說從正整數再引入非負整數的過程中，我們讓方程式 $x + 1 = 2$ 有解了，但那個所謂的「解」，它所有的性質完全就和「正整數」這個結構無關，因為它並不是在這個結構下產生的。這造成了一個奇怪的現象，明明在想法上是「擴張」的概念，但如果要用嚴謹的數學式去定義時，我們卻必須先有那個「擴張後的結構」，才能說從原本的結構去生成擴張後的結構。(如果下面兩個定義看不懂其實你都可以不要管，可以直接從**定理 5.4** 看起，這之後的東東完全可以用二項式展開以及二次剩餘的基本性質做出來。)

定義 6.2 如果 $\mathbb{L}$ 是一個 field，並且 $\mathbb{K}$ 是 $\mathbb{L}$ 的一個 subfield (即 $\mathbb{K}$ 對 $\mathbb{L}$ 上定義的加法跟乘法封閉，且 $\mathbb{K}$ 中每個元素對加法跟乘法的逆都還是在 $\mathbb{K}$ 中)，則說 $\mathbb{L}$ 是 $\mathbb{K}$ 的 extension。

我們知道 field extenstion 也分很多種，比方集合 $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ 是 $\mathbb{Q}$ 的擴張，而擴張次數 $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ 是有限的。然而像集合 $\mathbb{R}$ 是 $\mathbb{Q}$ 的擴張，擴張次數 $[\mathbb{R} : \mathbb{Q}] = \mathbb{C}$ 卻是無限的。在數論中，我們真正感興趣的是所謂的代數擴張 (algebraic extension)，這是用在某個 field 上的多項式的根當做基底產生的擴張。比方 $\mathbb{Q}[\sqrt{2}]$ 就是一個代數擴張，因為多項式 $x^2 - 2 = 0$ 的係數都在 $\mathbb{Q}$ 中，然後 $\sqrt{2}$ 是 $x^2 - 2 = 0$ 的根。

定義 6.3 給定某個 field $\mathbb{K}$，以及一個係數都在那個 field 上的多項式 f，我們稱 f 對 $\mathbb{K}$ 的 splitting field 指的是 $\mathbb{K}$ 的一個最小 extension field $\mathbb{L}$，使得 f 在 $\mathbb{L}$ 中可以完全被分解成線性因式。

舉例來說，現在有一個 field，就是 $\mathbb{Q}$，然後有個係數都在 $\mathbb{Q}$ 上的多項式 $f(x) = x^3 - 2$，那麼 $f(x)$ 對 $\mathbb{Q}$ 的 splitting field 就是 $\mathbb{Q}[\sqrt[3]{2}, \omega]$，其中 ω 是三次單位根。有時候 splitting field 不唯一，但可以確定它們都是同構的。

現在重新回到 Fibonacci 數列模 p 的週期 (以下計 Fibonacci 數列模正整數 m 的週期為 $l(m)$)。我們證明以下定理：

定理 6.3 假設一質數 $p \equiv \pm 1 \pmod 5$，則 $l(p) \mid p - 1$。

證明： 由假設知道 $\mathbb{F}_p$ 中有個元素扮演了 $\sqrt{5}$ 的角色 (就是說 5 是模 p 的二次剩餘)，所以 $\phi, \bar{\phi}$ 都是 $\mathbb{F}_p$ 中的元素。由 Fermat 小定理有：

$$\phi^{p-1} = 1 \text{ 以及 } \bar{\phi}^{p-1} = 1.$$

因此 $F_{p-1} = \dfrac{1}{\sqrt{5}}\left(\phi^{p-1} - \bar{\phi}^{p-1}\right) = 0$。故又有

$$\begin{aligned} F_p &= \frac{1}{\sqrt{5}}\left(\phi^p - \bar{\phi}^p\right) = \frac{1}{\sqrt{5}}\left(\phi - \bar{\phi}\right) \\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = 1. \end{aligned}$$

綜上我們有

$$\begin{cases} F_{p-1} = 0 = F_0 \\ F_p = 1 = F_1. \end{cases}$$

故 $p - 1$ 是 Fibonacci sequence 模 p 的週期，由重要性質就知道 $l(p) \mid p - 1$。 □

定理 6.4 假設一質數 $p \equiv \pm 2 \pmod 5$，則 $l(p) \mid 2p + 2$，且 $(2p + 2)/l(p)$ 是奇數。

證明： 這時候 $\mathbb{F}_p$ 中就沒有 $\sqrt{5}$ 了，但我們還是要用通項公式計算啊，怎麼辦呢？所以考慮 $x^2 - 5$ 在 $\mathbb{F}_p$ 上的 splitting field:

$$\mathbb{F}_p[\sqrt{5}] = \left\{a + b\sqrt{5} \mid a, b \in \mathbb{F}_p\right\}.$$

(可以驗證有模逆等等)，而且此時 $5^{\frac{p-1}{2}} = -1$。計算可知

$$\begin{aligned}\phi^p &= \left(\frac{1+\sqrt{5}}{2}\right)^p = \left(\frac{1}{2}+\frac{\sqrt{5}}{2}\right)^p = \left(\frac{1}{2}\right)^p + \left(\frac{\sqrt{5}}{2}\right)^p \\ &= \left(\frac{1}{2}\right)^p \left(1+\sqrt{5}^p\right) = \frac{1}{2}\left(1+5^{\frac{p-1}{2}}\sqrt{5}\right) \\ &= \frac{1}{2}\left(1-\sqrt{5}\right) = \bar{\phi}.\end{aligned}$$

因此也有

$$(\bar{\phi})^p = \overline{(\phi^p)} = \bar{\bar{\phi}} = \phi.$$

綜合以上兩式，我們得到：

$$F_p = \frac{\phi^p - \bar{\phi}^p}{\sqrt{5}} = \frac{\bar{\phi}-\phi}{\sqrt{5}} = -1.$$
$$F_{p+1} = \frac{\phi^{p+1} - \bar{\phi}^{p+1}}{\sqrt{5}} = \frac{\phi\bar{\phi} - \bar{\phi}\phi}{\sqrt{5}} = 0.$$

這告訴我們 $F_p = -1$, $F_{p+1} = 0$, $F_{p+2} = -1$，所以 $F_{2p+1} = 1$, $F_{2p+2} = 0$, $F_{2p+3} = 1$，即有 $l(p) \mid 2p+2$。並且 $l(p) \nmid p+1$，所以 $(2p+2)/l(p)$ 是奇數。 □

我們發現雖然有一些漂亮的結果了，可惜還是解不出一般的週期。事實上可以證明若 n 是奇數，那麼 $l(n)$ 就是 ϕ 在 $\mathbb{Z}_n^\times[\sqrt{5}]$ 中的 order，而在抽象代數中要處理某數在 field 的 order 這類型的問題都是難的。不過既然知道它的結構其實和 order 有關，自然會聯想到：指數原根二次剩餘的一些性質能不能套用上來呢？

我們計算 Fibonacci 數列模 p^i 的週期時，會發現一個和指數性質完全一樣的結論：(讀者可以想想看，模正整數的週期會不會有像原根和 Carmichael 函數類似的結果呢)

定理 6.5 如果 k 是最大的正整數使得 $l(p^k) = l(p)$，那麼對所有 $k_0 > k$，有 $l(p^{k_0}) = p^{k_0-k}l(p)$.

證明是簡單的，可以用和證指數性質時的一樣方法：二項式展開再加上數學歸納法，只是有點煩所以在此略去，讀者請自行練習。

現在研究 Fibonacci 數列模正整數的週期已有許多成果，這邊礙於筆者能力以及篇幅只介紹了一小段，有興趣鑽研者可以自行 google。另外這種計算模正整數的週期亦可當作一種質數檢驗法。

Problem set

P1. Show that $\gcd(F_m, F_n) = F_{\gcd(m,n)}$ for all $m, n \in \mathbb{N}$. And conclude that no Fibonacci number can be factored into a product of two smaller Fibonacci numbers, each greater than 1.

P2. FKMO 2013

Two coprime positive integers a, b are given. Integer sequence $\langle a_n \rangle$, $\langle b_n \rangle$ satisties

$$(a + b\sqrt{2})^{2n} = a_n + b_n\sqrt{2}$$

Find all prime numbers p such that there exist positive integer $n \leq p$ satisfying $p \mid b_n$.

P3. The Lucas sequence $\langle L_n \rangle$ is given by $L_0 = 2$, $L_1 = 1$ and $L_{n+1} = L_n + L_{n-1}$ for $n \geq 1$. Prove that if a prime number p divides $L_{2k} - 2$ for $k \in \mathbb{N}$, then p also divides $L_{2k+1} - 1$.

P4. KöMaL 1997

Suppose that $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ are integer sequences such that $a_1 = b_1 = 0$, and

$$a_n = nb_n + a_1b_{n-1} + a_2b_{n-2} + \cdots + a_{n-1}b_1.$$

holds for $n \geq 1$. Prove that, for any prime number p, a_p is divisible by p.

P5. ISL 2003 N7

The sequence $a_0, a_1, a_2, \ldots$ is defined as follows: $a_0 = 2$, $a_{k+1} = 2a_k^2 - 1$ for $k \geq 0$. Prove that if an odd prime p divides a_n, then 2^{n+3} divides p.

P6. Prove that there exists a Fibonacci primitive root (remember?) modulo p iff $p \equiv 1$ or $9 \pmod{10}$ and $l(p) = p - 1$.

P7. Lucas–Lehmer primality test

Let $M_p = 2^p - 1$ be the Mersenne number. Define a sequence $\langle s_n \rangle$ for all $n \geq 0$ by

$$s_0 = 4, \quad s_{n+1} = s_n^2 - 2 \ \ \forall n \geq 0.$$

Then M_p is prime if and only if $s_{p-2} \equiv 0 \pmod{M_p}$.

Chapter 7

整係數多項式

多項式的研究源於代數方程求解，是最古老數學問題之一，也是數學理論最豐富的一個領域。筆者覺得幾乎所有數論性質皆源自多項式與質數的關係，本章即是希望較廣泛的介紹多項式的各種性質。這一章習題大概是這篇文章最有水準的一批題目了。

這一章會用到一個我們在 Diophantine 方程一章的補充教材裡引入的記號：對一個整數數列 $\langle a_n\rangle_{n\in\mathbb{N}}$，以 $\mathbb{P}(\langle a_n\rangle)$ 記他的質因數集，也就是說 $\mathbb{P}(\langle a_n\rangle)=\{p \text{ 為質數} \mid \text{存在 } n\in\mathbb{N} \text{ 使得 } p \text{ 整除 } a_n\}$。當 f 是一個整係數多項式時，又以 $\mathbb{P}(f)$ 簡記 $\mathbb{P}(\langle f(n)\rangle)$

7.1 一些基本工具

■ Divisibility, Greatest Common Divisor

重要性質——★ 若 f 是整係數多項式，則對任意不相等的兩整數 a,b 都有

$$a-b \mid f(a)-f(b).$$

定理 7.1 (Bezout's Theorem) 在 $\mathbb{Q}[x]$ 上會有

$$(f_1(x),f_2(x),\ldots,f_n(x))=(\gcd(f_i(x))).$$

定理 7.2 (Chinese Remainder Theorem) 對於任意給定的兩兩互質的有理係數多項式 $Q_1,\ldots,Q_n$，以及任意有理係數多項式 $R_1,\ldots,R_n$，同餘式 $P\equiv R_i \pmod{Q_i}$ 在模 $Q_1\cdots Q_n$ 下總有唯一解。

■ Symmetric Polynomial

定義 7.1 給定 n 個變元 $x_1,\ldots,x_n$，定義

$$\sigma_k=\sum_{1\le i_1<\cdots<i_k\le n} x_{i_1}\cdots x_{i_k}$$

其中 $k=1,2,\ldots,n$。稱為關於 $x_1,\ldots,x_n$ 的基本對稱多項式 (elementary symmetric polynomials)。並且為方便定義 $\sigma_0=1$。

定理 7.3 (Fundamental Theorem of Symmetric Polynomials) R 是環。對任意對稱多項式 $F(x_1,\ldots,x_n)\in R[x_1,\ldots,x_n]$，總存在 n 元多項式 $f\in R[y_1,\ldots,y_n]$，使得

$$F(x_1,x_2,\ldots,x_n)=f(\sigma_1,\ldots,\sigma_n).$$

定理 7.4 (Newton's Identities) 給定 n 個變元 $x_1,\ldots,x_n$，定義 $S_k=x_1^k+\cdots+x_n^k$

1. $\sum_{i=0}^{n}(-1)^i S_{m-i}\sigma_i=0$，其中 $m\geq n$。
2. $m\sigma_m=\sum_{i=1}^{m}(-1)^{i+1}\sigma_{m-i}S_i$，其中 $m\leq n$。

■ Polynomial Interpolation

在數值分析這個數學分支中，多項式插值是指用多項式對一組給定數據進行插值的過程。換句話說就是，對於一組給定的數據，要尋找一個恰好通過這些數據點的多項式。有兩個基本的插值法：

定理 7.5 (Newton Interpolation) 給定 $n+1$ 個點 $(x_0,y_0),\ldots,(x_n,y_n)$，那麼

$$N(x)=\sum_{i=0}^{n}a_i\prod_{j=0}^{i-1}(x-x_j)$$

就會通過這些點。其中 a_i 可在解出 $a_0,\ldots,a_{i-1}$ 之後用 $N(x_i)$ 的值解出。

定理 7.6 (Lagrange Interpolation) 給定 $n+1$ 個點 $(x_0,y_0),\ldots,(x_n,y_n)$，那麼

$$P(x)=\sum_{i=0}^{n}\left[y_i\prod_{j\neq i}\frac{x-x_j}{x_i-x_j}\right]$$

就會通過這些點，並且次數為 n。

■ Polynomial Equation[選讀]

定理 7.7 (Cramer's Rule) 考慮 n 個變元 $(x_1,\ldots,x_n)$ 的 n 條式子的線性方程組，寫成矩陣 $Ax=b$，其中 A 是 $n\times n$ 方陣，x 和 b 都是行矩陣。那麼這個方程組有唯一解

$$x_i=\frac{\det(A_i)}{\det(A)},\ \ \forall i=1,\ldots,n.$$

其中 A_i 是把 A 的第 i 行以 b 代換之後的方陣。

定理 7.8 (Vandermonde matrix) 定義 $m\times n$ 階的 Vandermonde matrix 為：

$$V=\begin{bmatrix}1&\alpha_1&\alpha_1^2&\ldots&\alpha_1^{n-1}\\1&\alpha_2&\alpha_2^2&\ldots&\alpha_2^{n-1}\\\vdots&&&\ddots&\vdots\\1&\alpha_m&\alpha_m^2&\ldots&\alpha_m^{n-1}\end{bmatrix}$$

那麼 n 階方陣的行列式值可以寫成 $\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)$.

7.2 多項式模 m

7.2.1 算數性質

人類這種生物對於質數有一種病態的嚮往。好久好久以前，有人問：是否存在一個整係數多項式永遠都只產生質數？從此之後，相似的命題不斷推陳出新：有沒有整係數多項式 $f(x)$ 讓 $f(m!)$ 永遠都只產生質數？有沒有整係數多項式 $f(x_1, x_2, \ldots, x_n)$ 讓 $f(k, 2^k, \ldots, n^k)$ 永遠都只產生質數？有沒有二次整係數多項式 $f(x) = x^2 + x + m$ 讓 $f(0), \ldots, f(m-2)$ 都是質數？

在這個多項式產生質數問題爆炸的年代，為了解決上面的問題，我們必須先知道原命題的架構是什麼，以及它還能有什麼推論，以後才方便見招拆招。

定理 7.9 沒有非常數的整係數多項式 $f(x)$ 永遠都只產生質數。甚至，也找不到整係數多項式 $f(x)$，使得 x 夠大時都只產生質數。

證明： 使用歸謬法：假設存在整係數多項式 $f(x)$，使得存在整數 M，滿足對所有 $x \geq M$，$f(x)$ 都是質數。假設 $f(M) = p$，那麼我們考慮數 $f(M + pt)$, $t = 0, 1, \ldots$，顯見這裡面的任一個數都是 p 的倍數，但都要是質數，因此只有 $f(M + pt) = p$, $\forall t \geq 0$。但這是不可能的，因為這代表多項式 $g(x) \equiv f(x) - p$ 有無窮多個零點，矛盾。 □

證明過程中用到了性質：$a - b \mid f(a) - f(b)$。千萬不要小看它，在許多競賽題裡看到什麼質數啊、指數之類的性質時，它常常是你的好夥伴。我們還可以用它證明一個好的結論：

定理 7.10 (Schur's Theorem) 整係數多項式的質因數集是無限集。

證明： 使用歸謬法：假設存在整係數多項式 $f(x)$，使得其質因數集是有限集，設此多項式所有質因數為 $p_1, \ldots, p_n$。代任意數 a 進去得到 $f(a) = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$，那麼我們考慮數 $f(a + p_1^{\alpha_1+1} \cdots p_n^{\alpha_n+1} t)$, $t = 0, 1, \ldots$，由性質 $a - b \mid f(a) - f(b)$ 知必定要有 $p_1^{\alpha_1} \cdots p_n^{\alpha_n} \mid\mid f(a + p_1^{\alpha_1+1} \cdots p_n^{\alpha_n+1} t)$, $\forall t \geq 0$ (注意這個手法，很重要！)，然而我們說此多項式的所有質因數就是 $p_1, \ldots, p_n$，因此 $f(x)$ 對無窮多個點取同樣值，矛盾。 □

這真的是一個重要而且漂亮的定理。而用 Hensel's lemma 跟上面提過的性質還可以加強成：一個整係數多項式必在無窮多個局部域 (local field) $\mathbb{Q}_p$ 中有零點，請讀者自行練習。另外，你現在應該能解決提出的前兩個問題了，至於第三個，請不要去嘗試它 $\ldots$。

多項式的零點真的是超級無敵重要的性質，就競賽來說，基本上都是直接在問零點性質的問題，像是習題 1,4,7,21,22，還有 ISL 2012 N5。做類似題目時，用到的想法大概不出：

重要性質——★

- $p \mid f(a + pt) - f(a)$，然後代 a 是零點之類的。

- $f(x)$ 的零點個數有限 (最多就是次數)。
- 如果有某一代數數是 $f(x)$ 在無窮多個 $\mathbb{F}_p$ 的擴域的零點，那其就是 $f(x)$ 在複數域上的零點。並考慮基佬多項式 (將在代數數域一節介紹)。
- 一個整係數多項式必在無窮多個局部域 $\mathbb{Q}_p$ 中有零點。
- 一堆整係數多項式的質因數交集仍是無窮集 (例題 2.6)。

數學家希望了解這些讓給定的多項式 $f(x)$ 在 $\mathbb{F}_p$ 中有零點的那些 p。甚至，對於一般質數，能夠掌握 $f(x)$ 在 $\mathbb{F}_p$ 中的結構。這樣的野心實現了：

定理 7.11 (Frobenius Density Theorem) 給定首項係數為 1 且次數為 n 的不可約多項式 f，假設 f 在模 p 下的分解型 (decomposition type) 為 $n_1, \ldots, n_r$，那麼這樣的質數 p 的解析密度為

$$\frac{|\{\sigma \in \mathrm{Gal}(f) \mid \sigma \text{ 的 cycle pattern 為 } n_1, \ldots, n_r\}|}{|\mathrm{Gal}(f)|}$$

後來在 1922 年 Chebotarëv 還將此定理推廣到更強的境界。然而這同樣需要 Galois 理論以及大量代數數論的預備知識，所以這裡僅列出兩個較直接的推論供參考：

- 若 $f(x)$ 是 n 次式，那麼存在無窮多個質數 p 使得 $f(x)$ 在 $\mathbb{F}_p$ 中有 n 個零點。
- $f(x)$ 有一次因式當且僅當對所有足夠大的質數 p，$f(x)$ 在 $\mathbb{F}_p$ 中都有零點。

例題 2.1

令 $P(x)$ 是個整係數多項式，使得對所有正整數 n 總有 $P(n) > n$。定義數列 $\langle x_k \rangle$ 如下：$x_1 = 1$, $x_{i+1} = P(x_i)$ 對所有 $i \geq 1$。假設對所有正整數 m，這個數列都有某一項被 m 整除。試證 $P(x) = x + 1$.

證明： 任取整數 n，由題意我們知道存在 m 使得 $x_{n+1} - x_n \mid x_m$。

Case I. $m < n$ 對無窮多個 n 成立。
那麼由 $x_{n+1} - x_n \mid x_m < x_n$ 知道 $x_{n+1} < 2x_n$ 對無窮多個 n 成立，亦即 $P(x) < 2x$ 對無窮多個 x 成立，再加上對所有正整數 x 都有 $P(x) > x$，因此 $P(x) = x + c$ 對某個 c。再由於 $P^{[k]}(1) \equiv 1 \pmod{c}$ 對所有 k，因此只有 $c = 1$。

Case II. $m < n$ 對有限多個 n 成立。
那麼 $m \geq n$ 對無窮多個 n 成立。再由 $x_{n+1} - x_n \mid x_m - x_{m-1}, x_{m-1} - x_{m-2}, \ldots, x_{n+1} - x_n$ 得到 $x_{n+1} - x_n \mid x_n$，因此 $x_{n+1} < 2x_n$ 對無窮多個 n 成立，又回到 Case I.。 □

例題 2.2: Romania TST 2010

一個非常數的整係數多項式 $f(x)$ 滿足：對任一質數 p，總存在某質數 q 以及一個正整數 m 使得 $f(p)=q^m$。試證存在某個正整數 n 使得 $f(x)=x^n$。

證明： 我們分兩種情況：

Case I. $p=q$ 只對有限多個質數 p 成立。
現在假設 $f(p)=q^{m_1}, f(r)=s^{m_2}$，其中 $p\neq q, r\neq s$ 都是質數，並且 $q\neq s$ (注意這總是取得到的，因為多項式的質因數集是無窮集。)，然而由中國剩餘定理以及 Dirichlet 定理可取到質數 v 使得 $v\equiv p \pmod q$ 且 $v\equiv p \pmod q$，此時 $q\mid f(v)-f(p), s\mid f(v)-f(r)$，代表 $f(v)$ 不可能是質數的次方，矛盾！

Case II. $p=q$ 對無窮多個質數 p 成立。
那麼假設 $f(p_i)=p_i^{m_i}$，而 f 的次數是 d，領導係數為 a 是非零整數。那麼

$$a=\lim_{i\to\infty}\frac{f(p_i)}{p_i^d}=p_i^{m_i-d}.$$

因此存在某數 M 使得對所有 $i\geq M$，有 $m_i=d$。因此 $f(p_i)=p_i^d$ 對無窮多個 i 成立，即 $f(x)-x^d$ 有無窮多個零點，故 $f(x)=x^d$。 □

例題 2.3: 整值多項式判別法

令 $f(x)\in\mathbb{Q}[x]$ 的次數為 n。證明以下條件等價

1. 對所有 $x\in\mathbb{Z}$，都有 $f(x)\in\mathbb{Z}$。
2. 對連續的 $n+1$ 個正整數 x，都有 $f(x)\in\mathbb{Z}$。
3. 存在 $a_0,a_1,\ldots,a_n\in\mathbb{Z}$，使得
$$f(x)=a_n\binom{x}{n}+a_{n-1}\binom{x}{n-1}+\cdots+a_0\binom{x}{0}.$$

證明： 首先 (3)⇒(1) 和 (1)⇒(2) 是顯然的，因此我們只須證 (2)⇒(3)。
首先我們不失一般性設 $f(0),f(1),\ldots,f(n)$ 是整數 (否則使用線性變換 $x\to x-m$)。取 $a_0=f(0)$ 是整數，假設我們可取到 $a_0,\ldots,a_{k-1}$ 都是整數，則令

$$a_k=f(k)-\left(a_{k-1}\binom{k}{k-1}+a_{k-2}\binom{k}{k-2}+\cdots+a_0\binom{k}{0}\right)$$

也是整數。並且

$$g(x)=a_n\binom{x}{n}+a_{n-1}\binom{x}{n-1}+\cdots+a_0\binom{x}{0}$$

與 $f(x)$ 在 $0,1,\ldots,n$ 共 $n+1$ 個點的取值一樣，又次數都是 n，故 $f\equiv g$。 □

例題 2.4: USA TST 2010

令 f 是一個整係數多項式，滿足 $f(0)=0$ 以及

$$\gcd(f(0),f(1),f(2),\dots)=1.$$

證明存在無窮多個正整數 n 滿足以下：

$$\gcd(f(n)-f(0),f(n+1)-f(1),f(n+2)-f(2),\dots)=n.$$

證明： 首先我們用 Tylor expansion 展開 $f(n+x)-f(x)$ 會得到

$$f(n+x)-f(x)=\frac{1}{1!}f'(x)(n)+\frac{1}{2!}f''(x)(n)^2+\frac{1}{3!}f'''(x)(n)^3+\cdots.$$

我們希望的是 $f(n+x)-f(x)$ 整體只被 n 整除，因此先把 n 約去得

$$\frac{f(n+x)-f(x)}{n}=\frac{1}{1!}f'(x)+\frac{1}{2!}f''(x)(n)+\frac{1}{3!}f'''(x)(n)^2+\cdots.$$

現在希望的是他們無大於 1 的公因數。首先我們可以把質數分成兩類：與 n 不互質的以及與 n 互質的。現在對任一與 n 不互質的質數 p，有

$$\frac{f(n+x)-f(x)}{n}=\frac{1}{1!}f'(x)\pmod p.$$

我們希望至少有一個 x 使 $f'(x)$ 不被 p 整除，這顯然是取得到的：因為 $f'(x)$ 是個多項式，所以他有無窮個質因數，現在取一個大於它次數的質因數 q，那麼 $f'(x)\equiv 0 \pmod q$ 只有有限組解，否則 $f'(x)$ 的所有係數都被 q 整除，我們只須讓 q 跑遍 $f'(x)$ 所有大於它次數的質因數即可知存在某質數 r 使得 $f'(x)\equiv 0 \pmod r$ 無解，於是我們取 $n=r^t$。

再來對任一與 n 互質的質數 p，假設 $(f(n+x)-f(x))/n$ 全體都被 p 整除，那麼 $f(n+x)-f(x)$ 全體也都被 p 整除。但現在 $n=r^t$ 與 p 互質，再由 $p\mid f(ns+x)-f(x), f(ps'+x)-f(x)$ 對所有整數 s,s' 知道對所有整數 x 都有 $p\mid f(x+1)-f(x)$，這與 $p\mid 0=f(0)$ 加在一起就得到 $p\mid f(x)$ 對所有整數 x，與原題假設矛盾。故得證。 □

例題 2.5: 重要性質之一

給定非常數的整係數多項式 f，試證對任意正整數 N，總可找到質數 p 以及一個整數 c，使得 $p^N\mid f(c)$。

證明： 我們採用數學歸納法：當 $f(x)=ax+b$ 時，顯然對任意 N 我們只要取 $(p,a)=1$ 就必存在 c。假設 f 的次數 $<k$ 時命題成立。現在考慮 f 的次數為 k 時：

Case I. f 是可約的。
那麼由歸納假設我們知道命題成立。

Case II. f 是不可約的。
此時 f, f' 是互質的多項式 (因為 f 無重根)，所以存在整係數多項式 q, r 使得 $f(x)q(x) + f'(x)r(x) = d$ 是某個非 0 常數。此時我們知道讓 $p \mid f(c)$ 且 $p \mid f'(c)$ (對某個 c) 的質數 p 只能有有限多個。然而 $\mathbb{P}(f)$ 是個無窮集，所以在之中存在某質數 q 使得 $q \mid f(c)$ 但 $q \nmid f'(c)$ (對某個 c)，由 Hensel's lemma 我們可將次方弄到任意大。此時命題亦成立。 □

例題 2.6: 重要性質之二

若 $f_1, \ldots, f_n$ 是整係數多項式，則 $\mathbb{P}(f_1) \cap \cdots \cap \mathbb{P}(f_n)$ 是無窮集。

證明： 這個性質超級重要，但是沒有初等證明。不失一般性假設 $f_1, f_2, \ldots, f_n$ 全都不可約，分別取 $r_1, r_2, \ldots, r_n$ 是他們的根。由 primitive element theorem，擴張 $\mathbb{Q}[r_1, r_2, ..., r_n]$ 會有一個 primitive element ω，這代表存在有裡係數多項式 $g_1, g_2, \ldots, g_n$ 使得 $g_i(\omega) = r_i$。現在注意到 $f(g_i(x))$ 們會有一個非常數公因式 (例如 ω 的極小多項式，極小多項式將在代數數域一節介紹)，由 Schur 定理便得證。

想弄掉有裡係數只需要把他們共乘一個很大的整數就行了。 □

7.2.2 多項式函數

雖然現在才講好像有點晚了，不過我想各位應該不會太介意，上面我們常常用「取 $f(x) \in Q[x]$，而 $f(1) = \cdots$」之類的說法，其實這超不優。首先在 $\mathbb{Q}$ 上的多項式集合不該寫成 $\mathbb{Q}[x]$，而是必須寫成 $\mathbb{Q}[X]$，這是有歷史原因的可以自己去查查看，再來是大家都知道的不能寫 $f(x)$ 要寫 f。最後 $f(1) = \cdots$ 也是不對的，因為 $\mathbb{Q}[X]$ 裡的元素是「多項式」而不是「多項式函數」，你不能夠直接代值進去，我們必須要說「由多項式 f 可以自然對應到一個多項式函數 $\tilde{f}$，而它在 1 上面的取值是 $\cdots$」，最後這個多項式與多項式函數的對應很重要，因為在某些地方非零多項式可以自然應到零多項式函數。這些東西很麻煩，以後讀者念數學系抽象代數會學比較清楚，這篇文章既然是給高中生看的，這裡就不用太嚴謹隨便寫寫了。

一般來說研究某個 r 維向量空間 F^r 投影回原本域 F 所產生的結構時，我們常常會考慮 $F[x_1, \ldots, x_r]$ 中的多項式 f，其中 $f(a_1, \ldots, a_r)$ 表示依序把 f 中的 x_i 用 a_i 代換掉後所算出來的值。例如 $f(x, y) = x^2 + y^2$，那麼 $f : \mathbb{R}^2 \to \mathbb{R}$ 代表的就是把平面上的點依某種性質 (和原點的距離) 送到實數的一個函數。

照例，如果 $f(s) = g(s)$ 對所有定義域裡的元素 s 都成立，那麼將記為 $f = g$。今天我們希望能夠分類所有函數，一個簡單的想法是：如果作為多項式有 $f \neq g$，那麼當作 $F^r \to F$ 的函數時，仍有 $f \neq g$。這樣的判別法在某些情況下是成立的：

定理 7.12 如果 F 是無窮域，並且 $f \in F[x_1, \ldots, x_r]$ 是非 0 多項式，那麼可以從 F 中取出 r 個數 $a_1, \ldots, a_r$ 使得 $f(a_1, \ldots, a_r) \neq 0$。

證明： 數學歸納法。首先 $r = 1$ 顯然成立，因為 $f(x) = 0$ 的解數最多是 $\deg(f)$ 個。現在從 r 推到 $r+1$，由於 f 非 0，因此至少存在某個變數 x_{r+1} 使得 $f = c_0 + c_1 x_{r+1} + \cdots + c_k x_{r+1}^k$，其中 $c_j \in F[x_1, \ldots, x_r]$ 不全為 0 (假設 c_t 非 0)。由歸納假設存在 $(a_1, \ldots, a_r)$ 使得 $c_t \neq 0$，於是又可以取到某個 $x_{r+1} = a_{r+1} \in F$，使 $f(a_1, \ldots, a_r) \neq 0$。 □

在有限域的情況下這樣的準則失效了。因為 x^q 和 x 在 $\mathbb{F}_q$ 中是恆等函數，卻是不相等的多項式。但由於 Lagrange 定理在任意域中都會成立，所以你可能預料到了：

定理 7.13 如果 $f \in \mathbb{F}_q[x_1, \ldots, x_r]$，滿足 f 中每個變數 x_i 的次數都小於 q，那麼可以從 $\mathbb{F}_q$ 中取出 r 個數 $a_1, \ldots, a_r$ 使得 $f(a_1, \ldots, a_r) \neq 0$。

證明： 模仿上面定理。 □

現在對於任意 $f \in \mathbb{F}_q[x_1, \ldots, x_r]$，我們總是可以把裡面某個變數 x_i 大於等於 q 次的項用多項式除法 $x_i^k = (x_i^q - x_i)q_k(x_i) + r_k(x_i)$ 換掉，其中 $\deg(r_k) < q$。於是可以得到 $f(x_1, \ldots, x_r) = \sum f_i(x_1, \ldots, x_r)(x_i^q - x_i) + r(x_1, \ldots, x_r)$，其中 r 中每個變數 x_i 的次數都小於 q。注意到函數 $x_i^q - x_i$ 總是取值為 0，我們可以證明當 $S = \mathbb{F}_q^r$ 時，所有從 S 到 $\mathbb{F}_q$ 的函數均可以用 $\mathbb{F}_q[x_1, \ldots, x_r]$ 的元素表示出，因此就得到了

$$\mathbb{F}_q^S \simeq \mathbb{F}_q[x_1, \ldots, x_r]/(x_1^q - x_1, \ldots, x_r^q - x_r).$$

這個結論可以應用在證明 Chevalley-Waring Theorem。另外關於多變數多項式零點還有另一個很強的定理：Combinatorial Nullstellensatz，有興趣可以 google 或參考謝宇觀的講義。

重要性質——★ (Chevalley-Waring Theorem) 如有 r 個多項式 $\{f_i\} \in \mathbb{F}_q[x_1, \ldots, x_n]$ 並且 $n > \sum d_i$，其中 d_i 是 f_i 的總次數。那麼他們的公共零點個數被 $\mathrm{char}\, \mathbb{F}_q = p$ 整除。

證明： 我們考慮要如何計算一群多項式的公共零點個數，也就是說，尋找某個函數 g，使得

$$g(\mathbf{x}) = \begin{cases} 1 & , \quad \mathbf{x} \text{ 是多項式們的公共零點} \\ 0 & , \quad \text{其他情況} \end{cases}$$

這樣就可以變成改求

$$\sum_{\mathbf{x} \in \mathbb{F}_q^n} g(\mathbf{x}).$$

我們顯然會取 $g(\mathbf{x}) = (1 - f_1(\mathbf{x})^{q-1}) \cdots (1 - f_r(\mathbf{x})^{q-1})$。這時 g 的總次數小於 $n(q-1)$，因此必定有某個變數 x_i 使得 $\deg_{x_i}(g(\mathbf{x})) < q - 1$，利用性質：

$$\sum_{x \in \mathbb{F}_q} x^i = 0 \quad (\forall\, i < q - 1).$$

便證到了結論。 □

7.2.3 置換多項式

完全剩餘系的概念最早是 Gauss 在 1801 年發表的著作《Disquisitiones Arithmeticae》中被有系統的研究。而所謂的置換多項式 (permutation polynomial)，簡單來說就是能夠表示出完全剩餘系的多項式。

由整係數多項式的算數性質我們知道 $f(a+mt) \equiv f(a) \pmod{m}$ 總是成立的，這代表數列 $\langle f(x) \pmod{m} \rangle$ 是循環的，且 m 是其中一個週期。於是，自然會問：這週期裡面是否所有數都被表示出來了？所以定義：

定義 7.2 設 $f(x)$ 是一個整係數多項式，如果當 x 跑遍模 m 的完全剩餘系時，$f(x)$ 也會跑遍模 m 的完全剩餘系，那麼稱 $f(x)$ 是模 m 的置換多項式。

1863 年，Hermite 首度開創了對模為質數的置換多項式的研究，得出了一個判別準則。之後 Dickson 在 1896,1897 年將這個概念推廣到一般的 finite field 上面，對其進行更深入且一般的探討，甚至到二十世紀中期，一些基本工作都是由他本人完成的。一直到 50 年代之後，一些數學家搬來其他領域的核武開始對這方面的進攻，使得置換多項式被推廣到代數幾何、代數數論、組合之中，近年來研究的論文更是日漸蓬勃。事實上在數學競賽中也常會看到它的影子，筆者到現在已在 Turkey MO 2000, USA TST 2007, Putnam 2008, ISL 2010 N4, KöMaL 2010, Iran TST 2012, CGMO 2013, APMO 2014 看過多達八題！以下我們大略介紹模 m 的置換多項式。

首先由中國剩餘定理我們會發現多項式 $f(x)$ 是模 $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ 的置換多項式當且僅當 $f(x)$ 是模所有 $p_i^{\alpha_i}$ 的置換多項式。也就是說我們又可以只研究模為質數次方的情況了。接下來，又容易聯想到，Hensel's lemma 能否在這裡發揮作用呢？也就是說，在 $\mathbb{Z}/p^k\mathbb{Z}$ 上的置換多項式，和在 $\mathbb{Z}/p\mathbb{Z}$ 上置換多項式是否有一定程度的關聯？首先要注意到根本的：

定理 7.14 (Tylor's Theorem) 好用的展開式 (通常用 $x = a + tp^k$ 代入)：

$$f(x) = \frac{1}{0!}f(a) + \frac{1}{1!}f'(a)(x-a) + \frac{1}{2!}f''(a)(x-a)^2 + \frac{1}{3!}f'''(a)(x-a)^3 + \cdots .$$

引理 7.1 $f(x)$ 是 $\mathbb{Z}/p^k\mathbb{Z}$ 上的置換多項式當且僅當它是在 $\mathbb{Z}/p\mathbb{Z}$ 的置換多項式，並且 $f'(x) \equiv 0 \pmod{p}$ 無解。

證明： 首先如果 $f(x)$ 是在 $\mathbb{Z}/p\mathbb{Z}$ 的置換多項式，並且 $f'(x) \equiv 0 \pmod{p}$ 無解。那麼由 Hensel's lemma 我們可以知道對任意 $a \in \mathbb{Z}/p^k\mathbb{Z}$，$f(x) \equiv a \pmod{p^k}$ 總是有解的，這代表 $f(x)$ 是在 $\mathbb{Z}/p^k\mathbb{Z}$ 上的置換多項式。

再來如果 $f'(x) \equiv 0 \pmod{p}$ 有解 $x = a$，那麼由 Tylor expansion 知道 $f(a+p^{k-1}t) \equiv f(a) \pmod{p^k}$，這時 $f(x)$ 不是在 $\mathbb{Z}/p^k\mathbb{Z}$ 上的置換多項式。綜上。 □

上面這個引理根本強到爆，我們把問題直接化約成模為質數的置換多項式了。而由上一節的結論又可以再繼續化簡：稱 $f(x)$ 除以 $x^q - x$ 的餘式為 $f(x)$ 的簡化多項式，那

麼我們知道當且僅當其簡化多項式為 $\mathbb{F}_q$ 的置換多項式時，原多項式也是 $\mathbb{F}_q$ 的置換多項式。

以上說的都是理論的部分。但在計算上，我們能否給出一個置換多項式的實例呢？舉例來說，考慮置換：

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 3 & 0 & 4 & 2 \end{pmatrix}$$

我們能否找到一個多項式來表示它呢？會發現這是簡單的，可以利用 Lagrange Interpolation，以及模逆元的性質製造出整係數多項式 (在 $\mathbb{Z}/5\mathbb{Z}$ 中)：

$$f(x) = 1 \times \frac{(x-1)(x-2)(x-3)(x-4)}{(0-1)(0-2)(0-3)(0-4)} + 3 \times \frac{(x-0)(x-2)(x-3)(x-4)}{(1-0)(0-2)(0-3)(0-4)} + \cdots$$

而且從這裡可以看出，對於 $\mathbb{Z}/p\mathbb{Z}$ 的任一個置換 π，我們都找到一個多項式來表示它！

雖然這方法簡單又漂亮，但有一個問題：怎麼驗證 $f'(x) \equiv 0 \pmod{p}$ 有沒有解？也就是說，我們還不能確定能否構造出 $\mathbb{Z}/p^k\mathbb{Z}$ 的置換多項式。

1897 年，美國數學家 L.E.Dickson 提出了 Dickson polynomials，定義為：

$$D_n(x,\alpha) = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-k} \binom{n-k}{k} (-\alpha)^k x^{n-2k}.$$

定理 7.15 給定非零元 $a \in \mathbb{F}_q$，$q = p^m$。則 Dickson polynomials $D_n(x,a)$ 是在 $\mathbb{F}_q$ 上的置換多項式當且僅當 $(n, q^2-1) = 1$。而是在 $\mathbb{F}_q$ 上的正則置換多項式 (即 $D_n'(x,a) \equiv 0 \pmod{p}$ 無解) 當且僅當 $(n, p(q^2-1)) = 1$。

證明： 假設 $(n, q^2-1) = 1$，而 $D_n(b,a) = D_n(c,a)$。我們可在 $\mathbb{F}_q$ 的二次擴域 $\mathbb{F}_{q^2}$ 中取 β, γ 滿足 $\beta + a\beta^{-1} = b, \gamma + a\gamma^{-1} = c$。那麼會有

$$D_n(b,a) = D_n(\beta + a\beta^{-1}, \beta \cdot a\beta^{-1}) = (\beta)^n + (a\beta^{-1})^n = (\gamma)^n + (a\gamma^{-1})^n = D_n(c,a).$$

因此 $(\beta^n - \gamma^n)(\beta^n\gamma^n - a^n) = 0$，即 $\beta^n = \gamma^n$ 或 $\beta^n\gamma^n = a^n$。又因為 $(n, q^2-1) = 1$，因此 $\beta = \gamma$ 或 $\beta\gamma = a$ ，無論為何，總有 $b = c$，即 $D_n(x,a)$ 是在 $\mathbb{F}_q$ 上的置換多項式。

接下來證明正則置換多項式的部分。首先由 $D_n(x + a/x, a) = (x)^n + (a/x)^n$，兩邊對 x 微分得到

$$D_n'(x + \frac{a}{x}, a)(1 - \frac{a}{x^2}) = n(x)^{n-1} - n\frac{a^n}{x^{n+1}}.$$

這即是說

$$D_n'(x + \frac{a}{x}, a) = n\frac{(x^2)^n - a^n}{x^{n-1}(x^2-a)} = \frac{n}{x^{n-1}}h(x), \quad h(x) \in \mathbb{Z}[x].$$

如果 $D_n'(x,a)$ 在 $\mathbb{F}_p$ 中無零點，那麼有 $p \nmid n$，因此加上第一部分有 $(n, p(q^2-1)) = 1$。反過來，如果 $(n, p(q^2-1)) = 1$，但 $D_n'(x,a)$ 在 $\mathbb{F}_p$ 中有零點 k，在二次擴域 $\mathbb{F}_{q^2}$ 中取 β 使得 $\beta + a\beta^{-1} = k$。於是有 $h(\beta) = 0$。這代表 $(\beta^2 - a)h(\beta) = (\beta^2)^n - a^n = 0$，加上 $(n, q^2-1) = 1$ 就得到 $\beta^2 = a$。代回 $h(\beta) = na^{n-1} = 0$，只能有 $p \mid n$，矛盾。綜上。 □

現在讓我們以不一樣的眼光重新檢視這個理論。剛剛都是說，有沒有辦法給出一個置換多項式？那麼自然會問，給了一個多項式 $f(x)$ 之後，它會在哪些 finite field/ring 中是置換多項式？為方便我們定義集合：

$$P(f) = \{p \in \mathbb{P} \mid f(x)\text{是 } \mathbb{Z}/p\mathbb{Z} \text{ 的置換多項式}\}.$$
$$R(f) = \{p \in \mathbb{P} \mid f(x)\text{是 } \mathbb{Z}/p\mathbb{Z} \text{ 的正則置換多項式}\}.$$

那麼可以證明：

引理 7.2 若整係數多項式 f 是 $f_1, f_2, \ldots, f_n$ 的複合函數 (composition)，那麼

$$P(f) = P(f_1) \cap P(f_2) \cap \cdots \cap P(f_n).$$
$$R(f) = R(f_1) \cap R(f_2) \cap \cdots \cap R(f_n).$$

證明： 由數學歸納法，我們僅需證明 $f = f_2 \circ f_1$ 的情況。

首先由置換多項式以及複合運算的定義知道 f 是模 p 的置換多項式當且僅當 f_1 和 f_2 都是模 p 的置換多項式。第一式成立。

再來證第二式時須先承認第一式。由複合函數的微分知道 $f'(x) = f_2'(f_1(x)) \cdot f_1'(x)$，因此 $f'(x) \equiv 0 \pmod{p}$ 無解當且僅當 $f_1'(x) \equiv 0 \pmod{p}$ 和 $f_2'(x) \equiv 0 \pmod{p}$ 都無解，這就證完了第二式。 □

最後還有一個非常重要的置換多項式判別方法。1863 年，Hermite 證明了：

定理 7.16 (Hermite's Criterion) 給定有限域 $\mathbb{F}_q$，$f(x) \in \mathbb{F}_q[x]$，則 $f(x)$ 是 $\mathbb{F}_q$ 的置換多項式當且僅當下面兩個條件同時成立：

1. $f(x)$ 在 $\mathbb{F}_q$ 中恰有一個零點。
2. 對每個整數 $1 \le t \le q-2$，$(f(x))^t$ 的簡化次數小於等於 $q-2$。

值得提的是，條件 1. 可以改成 $(f(x))^{q-1}$ 的簡化次數等於 $q-1$。這判別法可以用類似和我們在指數教材最後一節中提過的方法證明，留給讀者當做練習。雖然他在實際計算上沒什麼用，不過就理論而言可是非常漂亮的，例如你現在可以看出如果 $d \mid q-1$，那不存在次數 d 的 $\mathbb{F}_q$ 的置換多項式。

以上講了幾個判別法，真正遇上多項式時可不可能有更快或更直接的方法計算出 $\mathbb{Z}/p^k\mathbb{Z}$ 的置換多項式？這當然是可行的，只是會很痛苦，比方 $f(x) = a_0 + a_1x + \cdots + a_dx^d$ 是 $\mathbb{Z}/3^k\mathbb{Z}$ 的置換多項式當且僅當：

1. $a_1 \not\equiv 0 \pmod{3}$.
2. $a_1 + a_3 + a_5 + \cdots \not\equiv 0 \pmod{3}$.
3. $a_2 + a_4 + a_6 + \cdots \equiv 0 \pmod{3}$.
4. $(a_1 + a_4 + a_7 + \cdots) + 2(a_2 + a_5 + a_8 + \cdots) \not\equiv 0 \pmod{3}$.

5. $(a_1+a_2+a_7+a_8\cdots)+2(a_4+a_5+a_{10}+a_{11}+\cdots)\not\equiv 0 \pmod 3$.

更多的討論可見論文。

以上是單變數置換多項式的討論。那麼後面自然會問有沒有多變數的置換多項式 $f(x_1,\ldots,x_n)$？一個合理的定義是：如果對任意 a，同餘方程 $f(x_1,\ldots,x_n)\equiv a \pmod m$ 恰有 m^{n-1} 組解，則稱 f 是置換多項式。然後由中國剩餘定理依舊有多項式 f 是模 $m=p_1^{\alpha_1}\cdots p_n^{\alpha_n}$ 的置換多項式當且僅當 f 是模所有 $p_i^{\alpha_i}$ 的置換多項式 (這其實沒那麼顯然，讀者可以練習看看)。接下來當然會聯想到我們能否跟上面一樣證明：f 是 $\mathbb{Z}/p^k\mathbb{Z}$ 上的置換多項式當且僅當它是在 $\mathbb{Z}/p\mathbb{Z}$ 的置換多項式，並且 $\partial f/\partial x_i\equiv 0 \pmod p$ 無公共解？

很可惜，問題就難在這裡，因為這是錯的，我們僅能證明 f 是 $\mathbb{Z}/p\mathbb{Z}$ 上的置換多項式且 $\partial f/\partial x_i\equiv 0 \pmod p$ 無公共解時，它一定是 $\mathbb{Z}/p^k\mathbb{Z}$ 上的置換多項式。然而其逆不真。也就是說我們無法從模 p^l 的置換多項式直接推出模 p^{l+1} 的置換多項式。一個簡單的例子是 $x^{p^2}+py^p$，它是模 p^2 的卻不是模 p^3 的置換多項式。

定義 7.3 令 $f_1,\ldots,f_m\in\mathbb{F}_q[x_1,\ldots,x_n]$, $1\le m\le n$ 是一群多項式，如果說對任意數對 $(a_1,\ldots,a_m)\in\mathbb{F}_q^m$，聯立方程

$$f_1(x_1,\ldots,x_n)=a_1,\ldots,f_m(x_1,\ldots,x_n)=a_m$$

都恰有 q^{n-m} 組解的話，那麼稱 $f_1,\ldots,f_m$ 是一組正交 (orthogonal) 多項式。

可以看出這其實是置換多項式的推廣，因為一組正交多項式中的任一子系統仍是正交多項式，退化來說任一多項式都會是置換多項式。而且當 $m<n$ 時用差值法還可以再讓正交組擴大，因此我們總是可以找到元素個數為 $m=n$ 的一組正交多項式。

接下來的推廣定理就是把我們上面提過的性質改為多變數的條件，就略去了。至於一般在整數剩餘類環上面的研究就比較少見，筆者僅看過四五篇論文在討論一些特別的情況。

Problem set

P1. A polynomial $P(x)$ has the property that for every $y\in\mathbb{Q}$ there exists $x\in\mathbb{Q}$ such that $P(x)=y$. Prove that P is a linear polynomial.

P2. Iran MO 2016

We call a function g special if $g(x)=a^{f(x)}$ (for all x) where a is a positive integer and f is polynomial with integer coefficients such that $f(n)>0$ for all positive integers n.

A function is called an exponential polynomial if it is obtained from the product or sum of special functions. For instance, $2^x3^{x^2+x-1}+5^{2x}$ is an exponential polynomial.

Prove that there does not exist a non-zero exponential polynomial $f(x)$ and a non-constant polynomial $P(x)$ with integer coefficients such that $P(n)|f(n)$ for all positive integers n.

P3. ISL 2006 N4

Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients and let k be a positive integer. Consider the polynomial

$$Q(x) = P(P(\cdots P(P(x))\cdots)) \quad (k \text{ times})$$

Prove that there are at most n integers such that $Q(t) = t$.

P4. ISL 2011 N6

Let $P(x)$ and $Q(x)$ be two polynomials with integer coefficients such that no non-constant polynomial with rational coefficients divides both $P(x)$ and $Q(x)$. Suppose that for every positive integer n the integers $P(n)$ and $Q(n)$ are positive, and $2^{Q(n)} - 1$ divides $3^{P(n)} - 1$. Prove that $Q(x)$ is a constant polynomial.

P5. ELMO 2013

For what polynomials $P(n)$ with integer coefficients can a positive integer be assigned to every lattice point in $\mathbb{R}^3$ so that for every integer $n \geq 1$, the sum of the n^3 integers assigned to any $n \times n \times n$ grid of lattice points is divisible by $P(n)$?

P6. Let $f(x)$ be an integer polynomial. For an integer a, consider the sequence of iterations $a_0 = a, a_{n+1} = f(a_n)$. Prove that if $a_n \to \infty$, and $f(x)$ isn't of the form Ax^d, then $\mathbb{P}(\langle a_n \rangle)$ is an infinite set.

P7. MOSP 2001

Let f be a polynomial with rational coefficients such that $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Prove that for any integers m, n, the number

$$\text{lcm}[1, 2, \ldots, \deg(f)] \cdot \frac{f(m) - f(n)}{m - n}$$

is an integer.

P8. Suppose $f(x)$ is an integer-valued polynomial with degree d such that $m - n \mid f(m) - f(n)$ for all pairs of integers (m, n) satisfying $0 \leq m < n \leq d$. Is it necessarily true that $m - n \mid f(m) - f(n)$ for all pairs of integers (m, n)?

P9. Iran TST 2011

Let p be a prime and k a positive integer such that $k \leq p$. We know that $f(x)$ is a polynomial in $\mathbb{Z}[x]$ such that for all $x \in \mathbb{Z}$ we have $p^k \mid f(x)$.

(a) Prove that there exist polynomials $A_0(x), \cdots, A_n(x)$ all in $\mathbb{Z}[x]$ such that

$$f(x) = \sum_{i=0}^{k} (x^p - x)^i p^{k-i} A_i(x)$$

(b) Find a counterexample for each $k > p$ and each prime p.

P10. USA TST 2009

Fix a prime number $p > 5$. Let a, b, c be integers no two of which have their difference divisible by p. Let i, j, k be nonnegative integers such that $i + j + k$ is divisible by $p - 1$. Suppose that for all integers x, the quantity

$$(x-a)(x-b)(x-c)[(x-a)^i(x-b)^j(x-c)^k - 1]$$

is divisible by p. Prove that each of i, j, k must be divisible by $p - 1$.

P11. USA TST 2008

Let n be a positive integer. Given an integer coefficient polynomial $f(x)$, define its *signature modulo* n to be the (ordered) sequence $f(1), f(2), \ldots, f(n)$ modulo n. Of the n^n such n-term sequences of integers modulo n, how many are the signature of some polynomial $f(x)$ if

(a) n is a positive integer not divisible by the square of a prime.

(b) n is a positive integer not divisible by the cube of a prime.

P12. Romania TST 2004

Let p be a prime number and $f(x) \in \mathbb{Z}[x]$ given by

$$f(x) = a_{p-1}x^{p-2} + a_{p-2}x^{p-3} + \cdots + a_2 x + a_1,$$

where $a_i = \left(\frac{i}{p}\right)$ is the Legendre symbol of i with respect to p.

(a) Prove that $f(x)$ is divisible with $(x-1)$, but not with $(x-1)^2$ iff $p \equiv 3 \pmod 4$.

(b) Prove that if $p \equiv 5 \pmod 8$ then $f(x)$ is divisible with $(x-1)^2$ but not with $(x-1)^3$.

P13. Find all polynomial $P(x) \in \mathbb{Z}[x]$ such that if $P(m) \mid P(n)$ then $m \mid n$.

P14. KöMaL 2011

Let $f(x) \in \mathbb{Z}[x]$ with degree n, and let $d_1, \ldots, d_n$ be pairwise distinct integers. Suppose that for infinitely many prime p there exists an integer k_p such that $f(k_p + d_1) \equiv \cdots \equiv f(k_p + d_n) \equiv 0 \pmod p$. Prove that there exists an integer k_0 such that $f(k_0 + d_1) = \cdots = f(k_0 + d_n) = 0$.

P15. CGMO 2013

Find the number of polynomials $f(x) = ax^3 + bx$ satisfying both following conditions:

(a) $a, b \in \{1, 2, \ldots, 2013\}$;

(b) the difference between any two of $f(1), f(2), \ldots, f(2013)$ is not a multiple of 2013.

P16. KöMaL 2010

For what primes p does there exist a cubic polynomial f with integer coefficients with the property that p does not divide the leading coefficient of f and $f(1), f(2), \ldots, f(p)$ give pairwise distinct remainders modulo p?

P17. Show that if $f(x) \in \mathbb{Z}[x]$ satisfying $\deg(f(x))$ is even. Then $P(f(x))$ is a finite set.

P18. Suppose $f(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ is of the form

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_r) + h(x_{r+1}, \ldots, x_n), \;\; 1 \leq r < n.$$

Prove that if and only if at least one of g and h is a permutation polynomial over $\mathbb{F}_p$ then f is a permutation polynomial over $\mathbb{F}_p$.

7.3 一點抽象代數 選讀

有時候我們要研究的多項式可能不是模質數，而是在模合數的情況下玩，你會發現許多意想不到的事情發生了：$(3)(2x) = 0$ (in $\mathbb{Z}/6\mathbb{Z}[x]$)，也就是存在 zero-divisor。

這其實不難理解，因為在模質數下產生的是個域，因此也會是 integral domain，但在一般情況下我們有的只是普通的環而已。而接下來主要要研究的就是 $R[x]$ 裡面的 units, nilpotent 以及 zero-divisors。在開始之前，我們先研究這些元素在 R 裡面的性質。首先注意到：$u \in R$ 是個 unit 當且僅當 $(u) = R$。如果我們將此觀點反過來看，或許可以掌握 non-units 的性質：

定理 7.17 環 R 中全體極大理想 (maximal ideal) 的聯集等於 non-units 的集合。

證明： 注意到我們已知 unit 不可能在任一真理想 (proper ideal) 裡，因此也不在極大理想裡，所以全體極大理想的聯集被包含在 non-units 的集合中。

另一方面，如果元素 u 不在極大理想的聯集裡，那麼他也不在任一個極大理想裡，這代表理想 (u) 不在任一極大理想裡，因此只能是 (0) 或 R (用 Zorn's lemma 可知任一真理想都在某個極大理想裡)。 □

以上定理給出了極大理想的聯集的性質，那麼自然會問其交集的性質。注意到極大理想必是素理想 (prime ideal)，而我們能針對更小的集合給出限制：

定理 7.18 環 R 中全體素理想交集等於 nilradical。

證明： 首先對任意 $u \in \mathrm{nil}(R)$，可找到正整數 n 使得 $u^n = 0$。因此對任意素理想 P 均有 $u^n \in P$，故也有 $u \in P$。因此 $\mathrm{nil}(R)$ 在全體素理想交集中。

另一隻手，如果 $u \notin \mathrm{nil}(R)$，那麼我們考慮所有不含任意 u^t 的理想的集合，在 inclusion 下它是 poset，由 Zorn's lemma 有極大元素 M，我們宣稱 M 必要是素理想 (因

為極大理想必是素理想，所以合理猜測在 inclusion 下的極大元素可能也是素理想)。假如說 $ab \in M$ 但 $a, b \notin M$，這造成 $M + (a)$, $M + (b)$ 是比 M 更大的集合，因此他們必定含有某些 u^{t_1}, u^{t_2}，但這造成 $u^{t_1+t_2} \in (M + (a))(M + (b)) \subseteq (M + (ab)) = M$，矛盾，因此 M 是素理想，這就證明了另一個方向的包含。 □

一般來說，所有極大理想的交集叫做 Jacobson radical。在 R 是 integral domain 的情況下，可以證明 $J(R[x]) = \text{nil}(R[x])$。

7.3.1 $R[x]$ 中的 units

雖然以上兩個定理在 $R = \mathbb{Z}/m\mathbb{Z}$ 是顯然的，不過當我們要在 $R[x]$ 裡面做事時，僅用初等的模運算實在是麻煩。開始分類 $R[x]$ 中元素的性質後，就可以看見他們的威力了。

首先我們要找出 $R[x]$ 中的 units。假設 $f = a_0 + a_1x + \cdots + a_nx^n$ 是個 unit，我們自然會想把它放進某個素理想 P 裡面看 (在整係數多項式的情況就等於是把它模某個質數)，於是考慮 natural mapping $\phi_P : R[x] \to (R/P)[x]$。由於在 $R[x]$ 中有某個 g 使得 $fg = 1$，因此 $\phi_P(f)\phi_P(g) = \phi_P(fg) = \phi_P(1) = 1$，這代表 f 在任意素理想中仍是一個 unit。但是注意到因為 P 是素理想，所以 $(R/P)[x]$ 是 integral domain，這表示 f 在 $(R/P)[x]$ 中的次數為 0，因此 $a_i \in P$ 對所有 $i > 0$。而這是對所有素理想都成立的，因此 a_i 在素理想的交集裡，就是說它是 nilpotent。同時，a_0 不能在任一素理想中，因此不在任意極大理想裡，故是 unit。

我們已知 unit 一定要長成 $f = a_0 + a_1x + \cdots + a_nx^n$，$a_0$ 是 unit，a_i 是 nilpotent 對所有 $i > 0$ 這樣。反過來說長這樣的一定是 unit 嗎？容易注意到我們應該會希望有：u 是 unit，n 是 nilpotent，則 $u + n$ 是 unit 這樣的事發生。而這顯然是成立的！因為我們可以用 $(u + n)^{-1} = u^{-1} - u^{-2}n + u^{-3}n^2 + - \cdots$，而 n^t 從某時開始會恆為 0。因此得到了：

定理 7.19 對 $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$，當且僅當 a_0 是 unit，a_i 是 nilpotent 對所有 $i > 0$ 時，f 是 unit。

7.3.2 $R[x]$ 中的 nilpotent

定理 7.20 對 $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$，當且僅當 a_i 是 nilpotent 對所有 i 時，f 是 nilpotent。

證明完全是從分類 unit 的方式照抄過來。最後注意到 $R = \mathbb{Z}/m\mathbb{Z}$ 中的 units 就是和 m 互質的那些數，而當 $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 時，nilpotent 就是 $p_1^{\beta_1} \cdots p_k^{\beta_k}$，其中 $\beta_i \leq \alpha_i$。

7.3.3 $R[x]$ 中的 zero-divisors

最後我們來進行 zero-divisor 的分類。如果 f 是個 zero-divisor，這代表找得到另外的 $g \in R[x]$ 使得 $fg = 0$。這樣的性質看起來似乎沒有什麼好用的規則，但事實上以下的

定理告訴你很強的：

定理 7.21 對 $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$，當且僅當存在 $a \in R$ 使得 $af = 0$ 時，f 是個 zero-divisor。

證明： 假設 $g = b_0 + b_1x + \cdots + b_mx^m$ 使得 $fg = 0$，並且是在所有使 $fg' = 0$ 中滿足次數最小的那個 g。注意到 $a_nb_m = 0$，因此多項式 a_ng 的次數比 g 小，而又滿足 $f(a_ng) = 0$，因此只能有 $a_ng = 0$。重複以上過程，我們發現 $a_ig = 0$ 對所有 i。特別地，$a_ib_m = 0$ 對所有 i，因此 $b_mf = 0$。 □

7.3.4 多項式的根

方程式的起點就在於根的存在性以及表示方法。由 local-global principle，要處理一個整係數多項式的數論性質時，我們會想看這個多項式對質數冪次 p^m 的性質，從各個局部域推知其整體性。最簡單的，我們先處理模 p 下的結構。

比方說 $8x^2 + 1$ 在模 5 下，我們知道它其實和 $3x^2 + 1$ 模 5 沒什麼兩樣。而且知道當我們為了表示代 $x = -\infty, \ldots, 0, 1, 2, \ldots, \infty$ 進去所產生的數時，實際上僅需要代 $x = 0, 1, 2, 3, 4$ 這五個數。這是一個好現象！我們能夠將無窮個情況化約到有限個，而且為了計算 $f(x) \pmod p$ 的值，僅需考慮 $x \pmod p$ 的值！

性質 7.1 以下多項式均在 $F[x]$ 中，且非 0。

(1) $F[x]$ 中沒有 zero-divisor，即是說任兩個非零元乘起來仍是非零元。

(2) 餘數除法成立。就是說對任意 $f(x), g(x)$，一定找得到 $q(x), r(x)$ 使得 $g(x) = f(x)q(x) + r(x)$，其中 $r(x) = 0$ 或 $\deg(r(x)) < \deg(f(x))$。

(3) (Bezout's theorem) 如果 $d(x)$ 是 $f(x), g(x)$ 的最大公因式，那存在 $h(x), s(x)$ 使得 $d(x) = f(x)h(x) + g(x)s(x)$。

(4) 唯一分解性。對於任一 $f(x)$，一定可以將他寫作

$$f(x) = cp_1(x)^{n_1}p_2(x)^{n_1} \cdots p_k(x)^{n_k}.$$

其中 $c \in F$, p_i 是領導係數為 1 的多項式。並且這種表法唯一。

可以看出來，其實條件 (2), (3), (4) 就是在分別說 $F[x]$ 是 ED, PID 以及 UFD。

跟在複數域上的多項式一樣，接下來我們想處理重根的問題。首先要注意到一件非常重要的事：多項式不一定在 $\mathbb{F}_p[x]$ 中可以完全分解成線性因式的乘積 (套用抽象代數的術語來說，就是 $\mathbb{F}_p$ 並非是個 algebraically closed field)。這是一個嚴重的問題，為什麼呢？

舉例來說，方程 $(x^2 + 1)^2 = 0$ 可被約成 $(x + i)^2(x - i)^2 = 0$，因此他有兩個二重根：i 和 $-i$。但是注意到這兩個根是在 $\mathbb{C}$ 中才有定義的！所以我們理所當然得不會說 $\mathbb{R}[x]$ 中的多項式 $(x^2 + 1)^2$ 有重根。這造成了麻煩的結果：一個多項式在某個域中無重根，但在

它的擴域裡卻有！我們有沒有辦法找到一個方法一次判別出多項式重根在某個域裡的存在性呢？一般來說是不可能的，你僅能知道多項式在其代數閉包內是否有重根，無法知道它在特定的域裡面是否有。因此下面我們要來研究代數閉包的性質。開始研究前，先整理出我們想要問的兩大問題：

(1) 有沒有可能一個多項式在某個域裡有不同分解方式，其中一個有重根另一個卻沒有？

(2) 有沒有可能存在一個定義在 F 中的多項式，不管對於 F 的任一個擴域 E，都沒辦法在 E 中完全分解成線性因式的乘積？

(1) 是個超嚴重的問題，不過幸好之前提到的唯一分解定理已解決這種窘境，有重根就是有重根，沒有就是沒有。(2) 的話，想像一下如果有個多項式不管在哪個域都有一個不可約因式叫做 $(x^2+1)^2$，你一定很想說 x^2+1 當然會在某個地方有個根，這時候 $(x^2+1)^2$ 就有重根啊！

定理 7.22 對任意域 F，$F[x]$ 中的任一多項式 $f(x)$ 必在 F 的某個擴域 E 中有根。

證明： 直接考慮 $E = F[x]/(f(x))$。由於 $F \cap (f(x)) = \phi$，因此可以將 F embed 進 E 中，而顯見此時 $f(x)$ 在 E 中有根。 □

你會發現對 $F[x]$ 中的任一次數為 n 的多項式 $f(x)$，僅需用這個定理找 $n-1$ 次擴域，我們就能將 $f(x)$ 完全分解成線性因式，這樣就可以討論重根的問題了！(題外話：引用 Zorn's lemma，可以證明對任意 F，都找得到擴域 F'，使得 $F[x]$ 中的任一多項式都能在 $F'[x]$ 完全中分解成線性因式) 首先回想起微積分裡面對於多項式的微分好像有很好用的性質，因此延續它的定義 (當然只是形式上的，因為現在不是連續函數了)，我們考慮：

定義 7.4 多項式 $f(x)$ 的 (algebraic) derivation $f'(x)$ 為：

$$\text{若 } f(x) = \sum_{i=0}^{n} a_i x^i \text{，則 } f'(x) = \sum_{i=0}^{n} i a_i x^{i-1}.$$

則此運算同樣的保有性質：

(1) $(f(x)+g(x))' = f'(x) + g'(x)$。

(2) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$。

定理 7.23 設 $f(x), g(x) \in F[x]$，E 是 F 的任一個擴域，則 $f(x), g(x)$ 在 $F[x]$ 中互質等價於在 $E[x]$ 中互質。

證明： 首先如果在 $E[x]$ 中互質，那顯然在 $F[x]$ 中也互質。現在如果在 $F[x]$ 中互質，這代表會有 $A(x), B(x) \in F[x]$ 使得 $f(x)A(x) + g(x)B(x) = 1_F = 1_E$ (Bezout's theorem)，如果 $f(x), g(x)$ 在 $E[x]$ 中不互質，代表有一個 $h(x) \in G[x]$ 使得 $h(x) \mid f(x), g(x)$，然而這代表 $h(x) \mid f(x)A(x) + g(x)B(x) = 1_E$，矛盾。 □

定理 7.24 (重根判別法) 設 $f(x) \in F[x]$，E 是 F 的任一個擴域，$c \in E$。那麼：

(1) c 是 $f(x)$ 的重根等價於 $f(c) = f'(c) = 0$。

(2) $f(x)$ 在 F 的任一擴域都沒有重根等價於 $f(x), f'(x)$ 在 $F[x]$ 中互質。

證明：

(1) 這其實跟在一般複數域上沒什麼兩樣，就不證了。

(2) 如果 d 是 $f(x)$ 在 E' 的重根，其中 E' 是 F 的擴張。那麼由 (1) 有 $f(d) = f'(d) = 0_{E'}$，這代表 $x-d$ 是 $f(x), f'(x)$ 在 $E'[x]$ 中的公因式 (因式定理)，因此他們在 $E'[x]$ 中不互質，也就會在 $F[x]$ 中不互質。反之，如果 $f(x), f'(x)$ 在 $F[x]$ 中不互質，那麼它們的公因式在 F 的某個擴張 E'' 中會有根 α，於是 $f(\alpha) = f'(\alpha) = 0_{E''}$，代表在這個擴張中 α 是重根。 □

好的，總算圓滿處理掉重根的問題了。最後小補充，我們知道有個重要的東西叫做判別式 (discriminant)，它可以用來判別複數域上一個多項式到底有沒有重根，現在問題來了，我們能不能擴張它的有效範圍，來判斷在 $\mathbb{F}_p[x]$ 中的多項式是否在 $\mathbb{F}_p$ 的某個擴域中有重根？或者等價的講，判斷在 $\mathbb{F}_p[x]$ 中分解是否會有平方因式？而我們自然會希望可以證明對領導係數為 1 的多項式有：

定理 7.25 多項式 $f(x)$ 在 $\mathbb{F}_p$ 的某擴域有重根等價於 $\mathrm{Disc}(f) = 0$ (in $\mathbb{F}_p$)。

證明： 有 $\mathrm{Disc}(f) \equiv \prod (x_i - x_j)^2$，再加上 $\mathbb{F}_p$ 的任一擴域都是 integral domain。 □

很容易理解：$\Delta = 0$ 代表在有裡數域上有平方因式，其中 0 是有裡數域加法單位元；那同樣地 $\Delta \equiv 0 \pmod{p}$ 也應代表在 $\mathbb{F}_p$ 有會有平方因式。舉個實例，整係數多項式 $x^3 + 3x^2 - 36x - 20$ 的判別式 $\Delta = 88560 \equiv 0 \pmod{3}$，而他在 $\mathbb{F}_3[x]$ 中可分解為 $(x+1)^2(x-2)$，有平方因式 (甚至還不小心是重根)！另外這當然對 resultant 也是對的。

上面陳述的是關於零點的一些性質。至此，我們討論完 $f \in \mathbb{F}_p[x]$ 的情況了。至於多項式去模 p^m 的情況，要扯到 p-adic number 去，因為很難所以就此打住。而在競賽題中基本上可以用 Hensel's lemma 解決。

7.4 環與體

7.4.1 代數數域

這小節講的基本就是 $\mathbb{Q}$ 的擴域。裡面的命題其實都可以直接改作一般多項式環的情況，不過現在姑且讓我們就數學史的發展方向，從熟悉的代數體系談起。

公元前 480 年左右雅典興起，成了世界的貿易首都及文化中心。因為當時奴隸占國家人口大多數，勞動力並無缺乏，這就在有閒階級中產生了一種強烈的欲望，要求有某種形式的文化，能為政治或社會帶來幫助，一批職業教師滿足了這樣的要求，這些人被

大家稱為哲人。他們和 Pythagorus 學派不同，並沒有形成一種哲學的特徵或是共同的學說。他們在數學上最主要的貢獻就是對現在我們耳熟能詳的尺規三大作圖難題的研究：

(1) 三等分角問題。我們都知道能夠以尺規平分一個角，那麼能否把它繼續三等分呢? 這主要是人們在作正多邊形時為了平分圓弧所延伸出來的研究。

(2) 立方體體積加倍問題。這源自於建築學上的需要，在神話中，鼠疫蔓延了 Delos 島，一個先知得到神的諭示，必須將 Apolo 祭壇的體積加倍神才會平息憤怒，由於建築師不知道該怎麼做，所以去請教哲學家 Plato，Plato 就告訴他們其實神真正的旨意是要讓希臘人為不重視幾何學而感到羞愧。

(3) 化圓為方問題。這是基於人們對用正多邊形去逼近圓所得到的啟示：正多邊形可以切成許多三角形再重拼回正方形，那麼圓不也應該要這樣嗎? 而這問題後來又因為 Hippocrates 證明出月牙定理：用畢氏定理將直角三角形面積換成另外兩月牙形面積之和，讓數學家燃起希望。

2000 多年來不計其數的數學家投入畢生心力為了解決這三大難題，但都無一例外的失敗了，於是人們開始懷疑這些問題的可能性。1637 年 Descartes 創立了解析幾何學，使尺規作圖的標準可以有代數式的量化，他們本質上就是關於線性或二次方程的研究。而到了 1837 年，法國數學家 Wantzel 用簡單的 field extenstion 概念證明了能尺規作圖的充要條件其實是與多項式的次數相關，因而解決了三等分角以及立方體體積加倍問題。直到 1882 年德國數學家 Lindemann 證明了 π 的超越性 (transcendental)，才使尺規三大作圖難題徹底宣告結束。

那麼，尺規作圖到底跟什麼多項式的次數有關呢，而所謂的「超越性」又是指什麼？我們有以下的定義：

定義 7.5 令 α 是個複數，如果他是某個整係數多項式 $f(x)$ 的根，那麼稱他為代數數 (algebraic number)，否則稱為超越數。

比方說 $\sqrt{2}$ 是 $x^2-2=0$ 的根，因此 $\sqrt{2}$ 是代數數。為了更深入研究這些數的性質，注意到假設說今天有個多項式叫 $(x^2-2)(x^2-3)$，我們知道 $\sqrt{2}$ 是它的根，可是跟 (x^2-3) 明顯是完全無關的！為了排除多餘的條件，自然會想說：代數數 α 滿足的不可約整係數多項式應該才是我們要的，而且那個多項式的其他複數根和 α 一定有什麼基情，於是定義：

定義 7.6 令 α 是個代數數，我們稱 α 的極小多項式 (minimal polynomial) 是滿足以 α 為根、領導係數為 1、並且次數最小的有理係數多項式 $f(x)$。並稱 $f(x)$ 的任一根 β 是 α 的共軛 (conjugate)。

由於極小和基佬的發音很像，所以以下採用基佬多項式這個信達雅的名稱。由基佬關係，可以證明共軛分類可將全體代數數分成等價類 (equivalent class)，並有以下很有用的性質：

性質 7.2 代數數 α 的極小多項式唯一，並且設 $f(x)$ 是他的極小多項式。如果有理係數多項式 $g(x)$ 以 α 為根，則在 $\mathbb{Q}[x]$ 上會有 $f(x) \mid g(x)$。

證明： 由輾轉相除法和次數最小性即得。 □

然而這個性質卻告訴我們：共軛在有裡數域上是不可能被分辨的。要是我們想要只研究其中一個數，那又該怎麼辦呢？所以自然會想定義以下：

定義 7.7 假設 F 是個域，L 是它的擴域，且 a 為 L 中的元素。我們以 $F[a]$ 表示包含 F 以及 a 的最小的環；以 $F(a)$ 表示包含 F 以及 a 的最小的域。

值得注意的是，當 a 是 F 上的代數數時，我們會有 $F[a] = F(a)$。現在的問題是，選定了代數數 α，那要如何決定 $\mathbb{Q}[\alpha]$ 這個集合到底是什麼呢？首先可以想見它和 α 的極小多項式一定有關係，並且不難看出，如果極小多項式是 $f(x) = a_n x^n + \cdots + a_1 x + a_0$，那麼應該要有

$$\mathbb{Q}[\alpha] = \{q_n \alpha^{n-1} + \cdots + q_1 \alpha + q_0 \mid q_n, \ldots, q_0 \in \mathbb{Q}\}.$$

這證明也是簡單的。而同時也宣稱了 $1, \alpha, \ldots, \alpha^{n-1}$ 就是一組基底。另外，還有重要的：$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f(x))$。

嗯，我們之前好像提過任意 F，都找得到擴域 F'，使得 $F[x]$ 中的任一多項式都能在 $F'[x]$ 完全中分解成線性因式。這代表對 $\mathbb{Q}$，我們找得到它一個擴域記作 $\mathbb{A}$，使得任一代數數都在 $\mathbb{A}$ 中，這個域叫做 $\mathbb{Q}$ 上的代數數域 (algebraic number field over $\mathbb{Q}$)。這邊給出不用抽象代數的證法：

性質 7.3 全體代數數形成一個域。

證明： 我們假設 α, β 是兩個代數數，分成以下情形：

- $-\alpha$：設 $f(x)$ 是以 α 為根的整係數多項式，則 $\pm f(-x)$ 之一就是以 $-\alpha$ 為根的整係數多項式。
- $1/\alpha$：假設 $\sum_{i=0}^{n} a_i x^i$ 以 α 為根，則 $\sum_{i=0}^{n} a_{n-i} x^i$ 以 $1/\alpha$ 為根。
- $\alpha + \beta$：設 $f(x)$ 是以 α 為根的整係數多項式，$g(x)$ 是以 β 為根的整係數多項式，且 $f(x)$ 的所有根是 $\alpha_1, \ldots, \alpha_n$，$g(x)$ 的所有根是 $\beta_1, \ldots, \beta_m$，考慮

$$F(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - (\alpha_i + \beta_j)).$$

- $\alpha\beta$：同樣的想法，考慮

$$F(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - \alpha_i \beta_j). \qquad \square$$

最後再提一個擴域的性質。如果 L 是 F 的代數擴張，F 是 E 的代數擴張，那麼當然可以把 L 看成是 E 的代數擴張，於是自然會想問 $[L : F], [F : E], [L : E]$ 這三者之間的關係。

定理 7.26 $[L:E]=[L:F]\cdot[F:E]$.

例題 4.1: APMO 2005

試證對任意無理數 a，總可找到無理數 b 和 b'，使得 $a+b, ab'$ 是有理數，而 $a+b', ab$ 是無理數。

證明： 我們考慮 a 的極小多項式 $f(x)$：

Case I. $\deg f=2$。
假設 f 的另一根是 c，那麼我們取 $b,b'\neq c$ 使得 $a+b$ 和 ab' 都是有理數，易知此時 b,b' 滿足要求。

Case II. $\deg f>2$，或 f 根本不存在。
那麼我們任取 b,b' 使得 $a+b$ 和 ab' 都是有理數，易知此時 b,b' 滿足要求。 □

例題 4.2: Brazil MO 2006

令 $f(x)\in\mathbb{Q}[x]$ 是個不可約多項式，假設說他有兩個根的乘積為 1。試證 f 的次數是偶數。

證明： 假設這兩根是 α,β。首先因為 $f(x)$ 不可約，因此易知 $f(x)$ 同時是 α 和 β 的極小多項式 (這兩數會是共軛的)。現在我們假設 $f(x)=(x-\theta_1)\cdots(x-\theta_n)$，考慮

$$g(x)=(x-\frac{1}{\theta_1})\cdots(x-\frac{1}{\theta_n})$$

我們知道 $g(x)$ 也是以 α,β 為根、領導係數為 1 的有理係數多項式，且因為 $\deg g=\deg f$，因此 $g(x)$ 也是 α 和 β 的極小多項式，所以 $f(x)\equiv g(x)$。也就是說對 $f(x)$ 的任一根 z，$1/z$ 也會是他的根。所以 f 的次數是偶數。 □

例題 4.3: Iran MO 2006

考慮以下兩個命題：

1. $P(x),R(x)$ 是兩個有理係數多項式，且 $P(x)$ 不是零多項式，也不可約。試證存在一個非零多項式 $Q(x)\in\mathbb{Z}[x]$ 使得 $P(x)\mid Q(R(x))$。
2. $P(x),R(x)$ 是兩個整係數多項式，$P(x)$ 的領導係數為 1。試證存在一個領導係數為 1 的多項式 $Q(x)\in\mathbb{Z}[x]$ 使得 $P(x)\mid Q(R(x))$。

證明： 呵呵。

1. 我們假設 $P(x)=0$ 的根是 $\epsilon_1,\ldots,\epsilon_n$，而 $R(\epsilon_i)=\theta_i$。則顯然 θ_i 仍是代數數，所以他們有極小多項式。令 $Q(x)$ 是他們極小多項式的公倍式，顯然滿足要求。

2. 令 $Q(x)=(x-\theta_1)\cdots(x-\theta_n)$，由於 $P(x),Q(x)$ 都是整係數多項式，且 $P(x)$ 領導係數為 1，而 $Q(x)$ 的各項係數可以 ϵ 的基本對稱多項式表示出，所以也都是整數，此時 $Q(x)$ 滿足要求。 □

7.4.2 在 $\mathbb{Q}[x]$ 中的不可約多項式

多項式分解性的重要性相信大家都了解，我們從最基礎的代數結構 $\mathbb{Q}[x]$ 談起。一般來說要證明一個多項式不可約可以從以下幾點著手：

- 從根的關係下手。
  - 通常是將根代回去取模，用三角不等式在複數平面上限制住根的範圍。
  - 較高級的，我們可以考慮看看根的 minimal polynomial。
- 由代數基本定理作限制。
  - 由 n 次複係數多項式恰好有 n 個複數根，去定義新的式子。
  - 用勘根定理：若實數 a,b 滿足 $f(a)f(b)<0$，則 f 在 (a,b) 中有根。

除了這些之外目前也沒有什麼好的算法了。更多可以參閱 V.V.Prasolov 所著的 Polynomials.

給不熟悉抽象代數的讀者：以下的證明中當我們說 natural mapping $\phi_p:\mathbb{Z}[x]\to\mathbb{Z}/p\mathbb{Z}[x]$ 時，指的是將整係數多項式的係數都模 p，例如 $\phi_5(x^2+12x+123)=x^2+2x+3$.

定理 7.27 (Gauss's Lemma) 一個整係數多項式在 $\mathbb{Q}[x]$ 能分解等價於在 $\mathbb{Z}[x]$ 中能分解。也就是說若 $P\in\mathbb{Z}[x]$，且 $P=FG$，其中 $F,G\in\mathbb{Q}[x]$，那麼存在 $q\in\mathbb{Q}$ 使得 $qF\in\mathbb{Z}[x]$, $q^{-1}G\in\mathbb{Z}[x]$。

證明： 過程中我們僅需用到 $\mathbb{Q}$ 是 $\mathbb{Z}$ 的 quotient field 這個條件。令 $P=a_nx^n+\cdots+a_1x+a_0=FG$，其中 $F,G\in\mathbb{Q}[x]$。假設 q 跟 r 是使得 qF 以及 rG 都是整係數多項式的最小正整數，而 $qF=q_kx^k+\cdots+q_1x+q_0$、$rG=r_lx^l+\cdots+r_1x+r_0$。所以有 $(qr)P=(qF)(rG)$。假設 p 是 q 的一個質因數，考慮 natural mapping $\phi_p:\mathbb{Z}[x]\to\mathbb{Z}/p\mathbb{Z}[x]$，得到 $0=\phi_p((qr)P)=\phi_p(qF)\phi_p(rG)$。由於 $\mathbb{Z}/p\mathbb{Z}[x]$ 是 integral domain，因此 $\phi_p(qF),\phi_p(rG)$ 中有一者為 0。不可能是 $\phi_p(qF)$，否則違反 q 的最小性，所以寫成 $(qr/p)P=(qF)(rG/p)$，重複這個過程即得 P 的整係數分解式。 □

定理 7.28 (Extended Eisenstein's Criterion) 整係數多項式 $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 滿足：

$$(1)\ p \mid a_0, a_1, \ldots, a_k \qquad (2)\ p \nmid a_{k+1} \qquad (3)\ p^2 \nmid a_0.$$

那麼 $P(x)$ 有次數高於 k 的不可約因式。

證明： 對 $\deg(P(x))$ 使用數學歸納法。假設 $P(x) = Q(x)R(x)$。考慮 natural mapping $\phi_p : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$，得到 $\phi_p(P(x)) = \phi_p(Q(x))\phi_p(R(x))$，由於 $p^2 \nmid a_0$，因此 $\phi_p(Q(x))$, $\phi_p(R(x))$ 中至少一者常數項非 0，假設是 $\phi_p(R(x))$。而 $\phi_p(P(x))$ 的最低項次數為 $k+1$，這要求 $\phi_p(Q(x))$ 的最低項次數為 $k+1$，因此 $Q(x)$ 也滿足原本給出的三個條件。 □

定理 7.29 (Perron's Criterion) 令整係數多項式 $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 滿足 $a_0 \neq 0$ 以及

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|.$$

那麼 $P(x)$ 是不可約的。

定理 7.30 (Hilbert's Irreducibility Theorem) 假設多變數有理係數多項式 $P_1, \ldots, P_n \in \mathbb{Q}[x_1, \ldots, x_s, y_1, \ldots, y_l]$ 全都不可約。那麼存在無窮多個 (事實上原本只宣稱必存在一個) 有理數點 $\mathbf{y} = (y_1, \ldots, y_l)$ 使得多項式 $P_1[x_1, \ldots, x_s, \mathbf{y}], \ldots, P_n[x_1, \ldots, x_s, \mathbf{y}]$ 全都不可約。

後面兩個定理的證明需要知道 Rouché's theorem，所以就不提了。要注意 Hilbert's Theorem 是個強到爆的東西，我們甚至能宣稱存在整數向量 $\mathbf{y}$ 滿足條件。另外讀者可以想想看為什麼可以從存在一個推到存在無窮多個。

注意到前兩個定理證明的本質是一樣的，這個方法是說假設某多項式在 $R[x]$ 中可約，那麼考慮由 $\phi : R[x] \to (R/P)[x]$ 的 natural homomorphism，如果在後面的 integral domain 不可約，那前面也不行。也就是說，我們由一個局部的性質 (在模某個質數不可約)，掌握了整體的資訊 (在有裡數域不可約)。自然會問說：這方法能不能拿來用在判別不可約多項式？

可惜的是 local-global principle 在這裡不適用了。事實上可以證明：

定理 7.31 多項式 $x^4 + 1$ 在 $\mathbb{Z}[x]$ 不可約，但在所有 $\mathbb{F}_p[x]$ 中都可約。

證明： 分成以下情況：

I. -1 是模 p 的二次剩餘，此時 $p \equiv 1 \pmod 4$。
約成 $(x^4 + 1) = (x^2 + i)(x^2 - i)$.

II. 2 是模 p 的二次剩餘，此時 $p \equiv \pm 1 \pmod 8$。
約成 $(x^4 + 1) = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$.

III. -2 是模 p 的二次剩餘，此時 $p \equiv 1, 3 \pmod 8$。
約成 $(x^4 + 1) = (x^2 + \sqrt{2}ix - 1)(x^2 - \sqrt{2}ix - 1)$. □

而我們還可以用 Hilbert's Irreducibility Theorem 找出一整類局部可約但整體不可約的多項式：$x^4+2ax^2+b^2$。更一般的，可以證明對任意合數 n，總是找得到次數為 n 且在 $\mathbb{F}_p$ 中都可約但在 $\mathbb{Q}$ 中不可約的多項式。而多項式次數為質數時，若在 $\mathbb{Q}$ 中不可約，則必在無窮多個 $\mathbb{F}_p$ 中不可約 (Chebotarëv Density Theorem 的推論)。

例題 4.4: Japan MO 1999

試證明多項式

$$f(x)=(x^2+1^2)(x^2+2^2)\cdots(x^2+n^2)+1$$

在 $\mathbb{Z}[x]$ 中不可約。

證明： 假設可分解成 $f=QR$，那麼我們知道 $Q(ai)R(ai)=1\ \forall a=\pm1,\ldots,\pm n$。由於 Q,R 都是整係數多項式，再由 $|Q(ai)R(ai)|=1$ 可以知道 $Q(ai)=1,-1,i,-i$，不論是哪種情形，總有 $R(ai)=\overline{Q(ai)}$，也就是說 $R(x)=\overline{Q(x)}$ 有 $2n$ 個根，因此 $R(x)$ 以及 $Q(x)$ 的偶次項全部相等。然而從 $f=QR$ 比較兩邊常數項就得到矛盾。 □

例題 4.5: Iran TST 2007

是否存在一個無窮數列 $a_0,a_1,\cdots\in\mathbb{N}$，使得對任意 $i\neq j$，都有 $(a_i,a_j)=1$。並且對任意正整數 n，多項式 $f_n(x)=a_0+a_1x+\cdots+a_nx^n$ 都是不可約的？

證明： 由於題目要求一個無窮且兩兩互質的正整數數列，所以我們知道像 Perron's criterion、Eisenstein's criterion 等等都沒辦法用。現在回歸最原始的想法，我們要怎麼證明一個多項式不可約? 最基本的當然是先分解掉領導係數和常數項，把所有可能的因數及次數組合都配出來，再用待定係數法做，因此為方便，我們應該會希望 $\langle a_i\rangle$ 中全是質數。我們取 $a_n>a_0+a_1+\cdots+a_{n-1}$。假設 $f_n(x)$ 可約，那麼必有 $f_n(x)=(a_nx^u+\cdots\pm1)(x^v+\cdots\mp a_0)$ 或是 $(x^u+\cdots\pm1)(a_nx^v+\cdots\mp a_0)$，會發現不論如何某個因式裡所有根乘積必定大於等於 1 ，所以 $f_n(x)$ 也必有根的長度大於等於 1，但這會和我們取 $\langle a_i\rangle$ 的條件矛盾。 □

例題 4.6: Romania TST 2010

令 p 為一質數，且 $n_1, \ldots, n_p$ 是一堆自然數。證明多項式

$$\frac{x^{n_1} + x^{n_2} + \cdots + x^{n_p} - p}{x^{\gcd(n_1, n_2, \ldots, n_p)} - 1}$$

在有理數域中不可約。

證明： 我們假設可約，由於你發現原式給你 p 是質數，所以最後一定是拆成 $(ax^u + \cdots \pm 1)(bx^v + \cdots \mp p)$ 的形式，其中 $b < p$ (否則原分式 $= p$)。從後式看會發現一定有根的長度大於 1 ，而從前式看也一定有根的長度小於等於 1 。然而比方代 $n_1 = 4, n_2 = 2$ 會發現從有根的長度大於 1 這方面下手可能導不出矛盾，所以應該是從有根的長度小於等於 1 導矛盾。

現在假設可約，那麼有根的長度小於等於 1，假設 α 是 $(x^{n_1} + x^{n_2} + \cdots + x^{n_p} - p)/(x^{\gcd(n_1, n_2, \ldots, n_p)} - 1)$ 的根。那麼 $p = |\alpha^{n_1} + \cdots + \alpha^{n_p}| \leq |\alpha|^{n_1} + \cdots + |\alpha|^{n_p}$，由於等號必須成立，故只有 $|\alpha| = 1$ 且 α^{n_i} 全部同向，然而 $p = \alpha^{n_1} + \cdots + \alpha^{n_p}$，故只有 $\alpha^{n_i} = 1$ 對所有 i，然而這代表 α 只能是 $x^{\gcd(n_1, n_2, \ldots, n_p)} - 1$ 的根，所以已被約去，矛盾！ □

7.4.3 分圓多項式

有些讀者想看分圓多項式可能是因為知道它可以用來證明 Dirichlet 定理的一個特例：形如 $an + 1$ 的質數有無窮多個；也可能是因為想看 Zsigmondy 定理的證明。但還是要給各位潑冷水，說實話筆者覺得這沒什麼意義。首先 Dirichlet 定理的特例只需要知道指數的一些性質還有 Schur 定理 (整係數多項式的質因數集是無限集) 就可以簡單做出來了，再來 Zsigmondy 的初等證明僅僅就只是個證明，沒什麼啟發的點，不過確實對熟悉指數處理有點幫助就是了。筆者覺得這篇 (https://www.quora.com/Why-are-cyclotomic-polynomials-important-What-are-their-applications) 解釋得不錯，不過需要不少數學成熟度才能體會。

這一寫節因為已經有挺詳盡的講義：Cyclotomic Polynomials in Olympiad Number Theory，所以我就不自己編了。僅再提幾點：

1. 若 ξ_m 是 m 次本原根，則 ξ_m 的 minimal polynomial 就是 $\Phi_m(x)$。
2. **(Gauss's formula)** 若 n 是大於 3 且無平方因數 (square-free) 的奇數，那麼

   $$4\Phi_n(x) = A_n^2(x) - (-1)^{\frac{n-1}{2}} n x^2 B_n^2(x)$$

   其中 $A_n(x)$ 和 $B_n(x)$ 都是整係數多項式，且 $A_n(x)$ 的次數是 $\phi(n)/2$，$B_n(x)$ 的次數是 $\phi(n)/2 - 2$。
3. **(Lucas's formula)** 若 n 是大於 3 且無平方因數的奇數，那麼

   $$\Phi_n(x) = A_n^2(x) - (-1)^{\frac{n-1}{2}} n x B_n^2(x)$$

   其中 $A_n(x)$ 和 $B_n(x)$ 都是整係數多項式，且 $A_n(x)$ 的次數是 $\phi(n)/2$，$B_n(x)$ 的次數是 $\phi(n)/2 - 1$。

然後有個有趣的問題，在大約公元前 300 年時，Euclid 證明了質數有無限多個，他用的神構造到現在還是數學中最經典的證明之一：假設質數只有有限個 $p_1, \ldots, p_n$，那麼數 $p_1 p_2 \cdots p_n + 1$ 不能被任何一個質數整除，矛盾！

這個證明還可以推廣到許多情況，比方說要證明型如 $4k+1$ 的質數有無限多個：假設只有有限個 $p_1, \ldots, p_n$，那麼考慮數 $4(p_1 p_2 \cdots p_n)^2 + 1$，顯然他是個奇數，又如果質數 q 整除他，那麼 -1 是模 q 的二次剩餘，但 q 不能是 $p_1, \ldots, p_n$ 中的任何一個，矛盾！

其實這些證明本質上都是先做出一個整係數多項式，然後取他在某點的值，證明整除這多項式值的質數會滿足我們的要求。於是問題出現：比方說我們能否找出某多項式，使得有無窮多個 $5k+2$ 型的質數整除他呢?

首先我們必須對要求做出嚴格的定義。先由分圓多項式的性質我們可以知道，任何整除 $\Phi_n(x)$ 的質數不是 n 的因數就是 $nk+1$ 型的質數，而又由前面提過的：對任意多項式 $\mathbb{P}(f) \cap \mathbb{P}(g)$ 都是無窮集，我們知道對多項式 f 和整數 a 必定有無窮多個形如 $ak+1$ 型的質數是他的質因數。因此會有合理的定義：

定義 7.8 給定正整數 a, l，如果整係數多項式 f 的任意質因數 p 要嘛是 $\equiv 1 \pmod{a}$，要嘛是 $\equiv l \pmod{a}$ (而且這種質因數要有無窮多個)，除此之外只有有限個例外。則我們說一個 f 是個對模 a 餘 l 的 *Euclidean polynomial*。

定理 7.32 (Schur-Murty Theorem) 存在模 a 餘 l 的 Euclidean polynomial 當且僅當 $l^2 \equiv 1 \pmod{a}$。

Problem set

P1. Prove that the minimal polynomial of an algebraic number can't have multiple-roots.

P2. Let $f(x)$ be a a polynomial with rational coefficients, and n an arbitrary integer. Prove that there exist polynomials $g(x), h(x) \in \mathbb{Q}[x]$ such that $f(x)g(x) = h(x^n)$.

P3. Let $f \in \mathbb{Q}[x]$ irreducible and $g \in \mathbb{Q}[x]$, then prove that every irreducible factor of $f(g(x)) \in \mathbb{Q}[x]$ has degree divisible by $\deg f$.

P4. Prove that the polynomial $f(x) = (x-a_1)^2(x-a_2)^2 \cdots (x-a_n)^2 + 1$ is irreducible, where a_i are pairwise distinct.

P5. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients, such that $|a_0|$ is prime and

$$|a_0| > |a_1| + |a_2| + \cdots + |a_n|.$$

Show that $f(x)$ is irreducible.

P6. Let p be prime. Show that $f(x) = x^{p-1} + 2x^{p-2} + 3x^{p-3} + \cdots + (p-1)x + p$ is irreducible.

P7. Iran MO 2005

Let $P(x) \in \mathbb{Q}[x]$ be an irreducible polynomial with odd degree, and $Q(x), R(x) \in \mathbb{Q}[x]$ such that $P(x) \mid Q(x)^2 + Q(x)R(x) + R(x)^2$. Prove that $P(x)^2 \mid Q(x)^2 + Q(x)R(x) + R(x)^2$.

P8. Romania TST 2003

Let $f(x) \in \mathbb{Z}[x]$ be an irreducible monic polynomial with integer coefficients. Suppose that $|f(0)|$ is not a perfect square. Show that $f(x^2)$ is also irreducible.

P9. Turkey MO 2006

Find all the triangles such that its side lenghts, area and its angles' measures (in degrees) are rational.

P10. Iran MO 2003

Let $f_1, f_2, \ldots, f_n$ be polynomials with integer coefficients. Show that there exists a reducible polynomial $g(x) \in \mathbb{Z}[x]$ such that $f_i(x)+g(x)$ is irreducible for $i = 1, 2, \ldots, n$.

P11. Show that there exists infinitely many positive integers n such that the largest prime divisor of $2^n - 1$ is less than $2^{\frac{n}{2013}} - 1$.

P12. Suppose that all zeros of a monic polynomial $P(x)$ with integer coefficients are of module 1. Prove that all its zeros are actually roots of unity, i.e. $P(x) \mid (x^n-1)^k$ for some natural n, k.

7.5 簡易解析方法

從解析方法的角度來看，多項式成長的速率實在是太慢了，也因此他會限制出許多性質。首先回顧一下 Euler 證明質數有無限多的方法：

證明： 假設質數只有有限多個 $p_1, \ldots, p_n$，由於所有正整數都可由質數次方乘積表示出，所以

$$\sum_{k=1}^{m} \frac{1}{k} < \prod_{i=1}^{n} \sum_{j=1}^{\infty} \frac{1}{p_i^j} = \prod_{i=1}^{n} \frac{1}{1 - 1/p_i}$$

但是左式發散，右式卻收斂，矛盾！ □

可以看出證明的關鍵在於「所有數都可由質數次方乘積表示出」以及「公比小於 1 的幾何幾數收斂」。將同樣的證明搬到多項式我們可以證明：

定理 7.33 假設 $\langle a_n \rangle$ 是個嚴格遞增的整數數列，使得存在整係數多項式 f 讓不等式 $a_n \leq f(n)$ 對所有正整數 n 都成立。那麼數列 $\langle a_n \rangle$ 的質因數集是無窮集。

證明： 假設質因數只有有限多個 $p_1, \ldots, p_N$，那麼

$$\sum_{k=1}^{\infty} \frac{1}{a_k} = \sum_{\alpha_1, \ldots, \alpha_N} \frac{1}{p_1^{\alpha_1} \ldots p_N^{\alpha_N}}$$

顯然右式收斂，但從這邊還看不出左式會不會發散。不過我們發現右式就算多幾個次方也還是收斂，所以我們引入數 $m = \dfrac{1}{\deg f + 1}$，寫作

$$\sum_{k=1}^{\infty} \frac{1}{(f(k))^m} \leq \sum_{k=1}^{\infty} \frac{1}{a_k^m} = \sum_{\alpha_1,\ldots,\alpha_N} \frac{1}{p_1^{m\alpha_1} \cdots p_N^{m\alpha_N}}$$

這時就有右式收斂，但左式卻發散！

事實上我們能證明更強的條件：只要 $\langle a_n \rangle$ 是個嚴格遞增的正整數數列，且對於任意正整數 k，它的成長速率都比 $2^{\sqrt[k]{n}}$ 還要慢，那麼它的質因數集是無窮集。注意顯然多項式的成長速率滿足要求。

假設可以僅用 $p_1, \ldots, p_k$ 表示出所有項，現在令 $N(n)$ 是所有能寫成 $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 的不超過 n 的正整數個數。我們必須要有：

$$\sum_{i=1}^{k} \alpha_i \log p_i \leq \log n.$$

因此得到 $\alpha_i \leq \log n / \log p_i \leq \log_2 n$，對所有 i。但這代表 $N(n) \leq (\log_2 n)^k$，代入 $n = a_n$ 得到矛盾。 □

例題 5.1

令 $f, g \in \mathbb{Z}[x]$ 是兩個非常數多項式，使得有無窮多個正整數 n 讓 $f(n) \mid g(n)$。試證 f 可在 $\mathbb{Q}[x]$ 中整除 g。

證明： 先由輾轉相除法得到 $g = fq + r$，其中 q, r 都是有理係數多項式，且 $\deg r < \deg f$。再來乘上某定整數 N 使得 Nq, Nr 都是整係數多項式，再由 $f(n) \mid g(n)$ 得到

$$N\frac{r(n)}{f(n)} \in \mathbb{N}, \ \forall\, n.$$

然而 $\deg r < \deg f$，因此

$$\lim_{n\to\infty} N\frac{r(n)}{f(n)} = 0.$$

所以當 n 足夠大時必有 $r(n) = 0$，故 r 的零點有無限個，這只有 $r \equiv 0$。 □

例題 5.2: Problems From the Book

令 $f \in \mathbb{Z}[x]$ 是一個次數為 k 的多項式，使得對於所有足夠大的正整數 n，總有 $\sqrt[k]{f(n)} \in \mathbb{Z}$。試證存在整數 a, b 使得 $f(x) = (ax + b)^k$。

證明：把題目給我們的條件寫下：存在某個整數數列 $\langle x_i \rangle$，使得 $f(n) = x_n^k$，而我們想要證的就是 $x_n = an + b$。因此我們預期 $x_{n+1} - x_n$ 會收斂到某個數 (就是 a 會是整數)。首先假設 $f(n) = a_k x^k + \cdots + a_1 x + a_0$，我們易證明

$$\lim_{n\to\infty} \frac{x_{n+1}}{x_n} = 1 \ , \ \lim_{n\to\infty} \frac{n}{x_n} = c_1.$$

對某個常數 c_1。因此由 $f(n+1) - f(n) = x_{n+1}^k - x_n^k$ 得到

$$\lim_{n\to\infty} (x_{n+1} - x_n) = \lim_{n\to\infty} \frac{f(n+1) - f(n)}{\sum x_{n+1}^i x_n^{k-i}} = c_2.$$

對某個常數 c_2。又因為 $\langle x_i \rangle$ 是整數數列，所以當 n 足夠大時必有 $x_{n+1} - x_n = c$，對某個整數常數 c。因此對所有 $n \geq M$，有 $x_n = an + b$，對某兩個整數常數 a, b。所以多項式 $g(x) \equiv f(x) - (ax + b)^k$ 有無窮多個零點，故 $f(n) \equiv (an + b)^k$。 □

此外還可用 Hilbert's Irreducibility Theorem 給出更漂亮的解：考慮多項式 $g(x, y) = f(x) - y^k$，把它分解到所有因式都不可約，考慮因式中關於 y 是二次以上和零次的式子，那麼存在 $\mathbf{x}$ 使得這些因式都不可約，當然也沒有根。而只能有有限個一次因式，因此在這無窮多個 $\mathbf{x}$ 中，存在無窮多個讓某個因式都是 0，代回 $g(x, y) = f(x) - y^k$ 便得到要求的結論。

評論 7.1 由上面兩題可以看出主要的步驟是：

1. 把題目給的所有關係用好的代數式表達出來。
2. 假設題目給你的是數列 $\langle y_i \rangle$，求出式子中會有哪個相對應變動的數列 $\langle x_i \rangle$。
3. 估計數列 $\langle x_i \rangle$ 發散或收斂。

在進入以下的習題前先幫各位做好心理建設，以下的題目對高中生來說該是這一整篇講義裡面整體平均最難的題目，8,9,10,11 那幾題從難度來說大概可以到 ISL N100 以上吧。還有裡面的想法可能會與這一章第二小節多項式模 m 有關。

Problem set

P1. USAMO 1995

Suppose $q_0, q_1, q_2, \ldots$ is an infinite sequence of integers satisfying the following two conditions:

(a) $m - n$ divides $q_m - q_n$ for $m > n \geq 0$.

(b) There is a polynomial P such that $|q_n| < P(n)$ for all $n \geq 0$.

P2. Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that

$$|x^{f(y)} - y^{f(x)}| < f(x)f(y).$$

holds for all $x, y \in \mathbb{N}$.

P3. Bulgaria MO 1995

For any positive integer n, let $P(n)$ be the greatest prime divisor of n. Prove that there are infinitely many positive integers n with

$$P(n) < P(n+1) < P(n+2).$$

P4. USAMO 2006

For integral m, let $P(m)$ be the greatest prime divisor of m. By convention, we say $P(\pm 1) = 1$ and $P(0) = \infty$. Find all polynomials f with integer coefficients such that the sequence $\{P(f(n^2)) - 2n\}_{n\geq 0}$ is bounded above.

P5. Iran TST 2007

Find all monic polynomials $f(x)$ in $\mathbb{Z}[x]$ such that $f(\mathbb{Z})$ is closed under multiplication.

P6. Iran TST 2014

Find all polynomials P with integer coefficients that $P(\mathbb{Z}) = \{p(a) \mid a \in \mathbb{Z}\}$ has a eometric progression.

P7. ISL 2012 A4

Let f and g be two nonzero polynomials with integer coefficients and $\deg f > \deg g$. Suppose that for infinitely many primes p the polynomial $pf + g$ has a rational root. Prove that f has a rational root.

P8. Prove that if $f, g \in \mathbb{Z}[x]$ are coprime polynomials then there are infinitely many positive integers n such that $nf + g$ is irreducible in $\mathbb{Z}[x]$.

P9. Let $f(x) \in \mathbb{Q}[x]$ of degree higher than 1. Prove that the set $\cap_{i=1}^{\infty} f^{[i]}(\mathbb{Q})$ has at most finitely many elements.

P10. Suppose $f(x), g(x) \in \mathbb{Q}[x]$ are polynomials such that $f(\mathbb{Q}) = g(\mathbb{Q})$. Prove that there exist rational numbers a, b such that $f(x) = g(ax + b)$.

P11. Let f, g two real polynomials such that for any real x, if $f(x)$ is integer, so is $g(x)$. Prove that there are integers m, n such that $g(x) \equiv mf(x) + n$.

P12. Iran MO 2011

Let $P(x)$ be a nonzero polynomial with integer coefficients. Prove that there exists infinitely many prime numbers q such that for some natural number n, $q \mid 2^n + P(n)$.

P13. China MO 2011

Let m, n be positive integer numbers. Prove that there exist infinite many couples of positive integer nubmers (a, b) such that

$$a + b \mid am^a + bn^b, \quad (a, b) = 1.$$

P14. China TST 2010

Given positive integer k, prove that there exists a positive integer N depending only on k such that for any integer $n \geq N$, $\binom{n}{k}$ has at least k different prime divisors.

P15. ARO 2008 Generalized

Find all positive integer n such there exists integers $b_1, \ldots, b_n$ satisfying the number $(x+b_1)\cdots(x+b_n)$ is a perfect power for infinitely many x.

7.6 補充教材——多項式的最大質因數

這部份引入的是多項式的最大質因數，主要方法其實是上一節的延續，但是因為有許多困難的東西我也不會證明，只能作簡略的介紹。大意是想讓大家知道一些數學定理的發展歷史，當然你也可以用等一下講的結論去作上一小節的題目，就會知道高等數學的強大在哪了 $\cdots$。

我們知道多項式實在是數論的根源，有些關於多項式取值的問題也因而產生。比方說一次多項式 $ax+b$ 會不會取質數值？如果會，那能不能取無窮多個質數值？這部分在 1837 年被 Dirichlet 解決了：只要 $(a,b)=1$，那算數數列 $\langle an+b\rangle$ 就包含無窮多個質數，而事實上裡面每個等差數列的質數密度都是相等的。這真的是個很酷的定理。

之後，自然會問，那二次以上的整係數多項式會不會取無窮多個質數值呢？首先當然有幾個必要條件：

(1) 多項式 $f(x)$ 的領導係數為正 (其實可以不用，如果把 $-p$ 也算質數的話)。

(2) $f(x)$ 在 $\mathbb{Z}[x]$ 上不可約。

(3) $\gcd(f(1), f(2), \ldots) = 1$ (其實僅需檢驗從 $f(0)$ 到 $f(d)$，其中 d 是次數)。

而這些條件就夠了嗎？不知道，這正是鼎鼎大名的猜想 (Bunyakovsky conjecture)。另外還有一些推廣形式：$f_1(x), \ldots, f_n(x)$ 都是不可約的整係數多項式，而且不存在質數 p 使得對所有正整數 m 都有 $p \mid f_1(m)\cdots f_n(m)$，那存在整數 n 代進去後這些多項式同時是質數 (Schinzel's hypothesis H)。

因為二次以上的命題太難了，數學家決定研究最簡單的形式：n^2+1 能否取無窮多個質數值？經過了 101 年的努力，到現在還是沒解決，不過多少還是有了一些很酷的成果 (筆者常常在想，其實有時候這些解決這些問題本身已經不重要了。重點是為了解決他們，一直會有許多很強大的方法出現，解掉某些特例。然後我們卻可以從弱化型式中看出更多命題背後的結構！)。以下挑了幾題研究研究：

Problem.(ISL 2011 N2) 考慮多項式 $P(x) = (x+d_1)(x+d_2)\cdots(x+d_9)$，其中 d_i 兩兩相異。試證存在一個正整數 N，使得對所有 $x \geq N$，$P(x)$ 都被某個大於 20 的質數整除。

Problem.(ISL 2008 N6) 試證存在無窮多個整數 n 使得 n^2+1 的最大質因數比 $2n+\sqrt{2n}$ 還大。

Problem. 是否存在整數 $k>3$ 使得 $(1+1^2)(1+2^2)\cdots(1+k^2)$ 是個完全平方數？

Problem.(ISL 2009 N7) 如果 a,b 是兩個大於 1 的相異正整數，證明存在正整數 n 使得 $(a^n-1)(b^n-1)$ 不是完全平方數。

要注意，此處不一定會提供完整的證明，這裡只是為了介紹一些理論才討論這幾題的，它們是筆者覺得較漂亮也比較多背景的題目，希望讀者先至少把三題競賽題想過後再繼續往下看。

研究 6.1: ISL 2011 N2

考慮多項式 $P(x)=(x+d_1)(x+d_2)\cdots(x+d_9)$，其中 d_i 兩兩相異。試證存在一個正整數 N，使得對所有 $x\geq N$，$P(x)$ 都被某個大於 20 的質數整除。

證明： 使用歸謬法，假設說存在某組 $(d_1,\ldots,d_9)$ 使得會有無窮多個 x 讓 $P(x)$ 只被小於 20 的質數整除 (這些 x 依序為 $x_1,x_2,\ldots$)。設小於 20 的質數為 $p_1,\ldots,p_8$。我們知道當 $n\to\infty$ 時，會有 $v_{p_i}(x_n+d_j)\to\infty$ (對所有 j，都可找到 i)，由鴿籠原理，裡面有兩個 d_j 會對應到同一個 p_i，假設是 d_{j_1} 以及 d_{j_2}，即

$$\text{當 } n\to\infty \text{ 時, } \ v_{p_i}(x_n+d_{j_1})\to\infty, \ \ v_{p_i}(x_n+d_{j_2})\to\infty.$$

但是相減會有 $v_{p_i}(d_{j_1}-d_{j_2})\to\infty$，這是不可能的。 □

這個解法主要的想法就是，第一步先發現 20 以內只有 8 個質數，那麼接著自然會想到鴿籠原理，但是重點就在於抽屜的取法。另外官方解亦給出了 N 的上界，方法是不失一般性假設 d_i 全正，用類似上面的方法估計 $v_{p_i}(x_n+d_j)$ 的成長速率，最後得到 $N\leq d^8$，其中 $d=\max\{d_1,\ldots,d_9\}$。後來在 AoPS 的網站上還有位網友回應說，這題其實是 Kobayashi's theorem 的直接推論。但正如在 Diophantine 方程一章的補充教材提到過的，關於命名部分筆者認為有些爭議。比較好的是以下定理：

定理 7.34 (Pólya-Størmer Theorem) 給定有限質數所生成的集合 $\langle S\rangle=\langle p_1,\cdots,p_r\rangle$。現在我們把 $\langle S\rangle$ 中的元素依序列出為 $a_1<a_2<\cdots$，則有 $\lim_{i\to\infty}a_{i+1}-a_i=\infty$。換句話說，給定整數 c，則 $a_{i+1}-a_i=c$ 僅有有限組解 i。

請讀者用此定理來證證看 ISL 2011 N2。另外，這命題還可以再加強成：若整係數多項式 $f(x)$ 至少有兩個相異根，那麼 $\lim\limits_{x\to\infty}P(f(x))=\infty$，這裡 $P(m)$ 表示 m 的最大質因數。不過要用到較深的 prime ideal theorem，此處略去。

注意到，原本 shortlist 的題目是要求我們對最大質因數估計其下界，那麼現在自然會想要問能否也估計出其上界：

性質 7.4 對於所有 $\epsilon > 0$，以及 $k \geq 2$，總存在無窮多個正整數 n 使得

$$P((n+1)\cdots(n+k)) < n^{\epsilon}.$$

先分析題目，會發現我們可以把所有質數分為兩類：小於等於 k 的和大於 k 的，容易估計前者在乘積中最少出現幾次，而後者最多也只能整除乘積中的某一項。假設 q 是某個質數，且 $q \mid n+i$，我們自然會希望 q 整除 $n+i$ 的次方越高越好，因為這樣就壓縮到 $n+i$ 又長出一個大於 q 的質因數的可能性。

現在令 $p_1 < p_2 < \cdots < p_s$ 是所有小於等於 k 的質數，我們可以表示出：

$$i = p_1^{\alpha_1(i)} \cdots p_s^{\alpha_s(i)} \quad (i = 1, 2, \ldots, k).$$

現在希望 $n+i$ 被小於等於 k 的質數整除越多次越好，為了讓 $n+1, \ldots, n+k$ 中每個數都滿足需求，可能會取 $\mathrm{lcm}[1, 2, \ldots, k] \mid n$，這時候便可以對每個 $n+i$ 拆成 $n+i = i(n/i+1)$。但注意到今天要找的 n 是無界的，所以 n/i 可以任意跑，我們必須給出 $n/i+1$ 的一般分解式才行。

證明： 把所有夠大的質數放進互斥集合 $\Theta_1, \ldots, \Theta_k$ 中，使得：

$$\prod_{p \in \Theta_i} \left(1 - \frac{1}{p}\right) < \frac{\epsilon}{2} \quad (i = 1, 2, \ldots, k).$$

這總是做得到的，因為：

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \to 0 \quad \text{as} \quad x \to \infty.$$

並且令 $Q_i = \prod_{p \in \Theta_i} p$。注意到這些 Q 之間兩兩互質，於是我們可以用中國剩餘定理對 $j = 1, \ldots, s$ 都構造數 L_j：

$$L_j \equiv \alpha_j(i) \pmod{Q_i} \quad (\forall\, i = 1, 2, \ldots, k).$$

現在令 $n = \prod_{j=1}^{s} p_j^{L_j}$，那麼我們可以得到 $n + i = i(u_i^{Q_i} + 1)$ 對所有 i，其中

$$u_i = \prod_{j=1}^{s} p_j^{(L_j - \alpha_j(i))/Q_i}.$$

由於 Q_i 都是奇數，所以當我們令 $X = -u_i$ 時，便可以用分圓多項式做出分解：

$$u_i^{Q_i} + 1 = -\prod_{d \mid Q_i} \Phi_d(X).$$

這已經完全符合剛剛分析時所要做出的條件了，於是現在僅需用分圓多項式的性質估計每個因式的最大質因數成長速率：

$$\begin{aligned} \max_{d \mid Q_i} \{\Phi_d(X)\} &\leq \max_{d \mid Q_i} \{||X| + 1|^{\phi(d)}\} = (u_i + 1)^{\phi(Q_i)} \\ &= (O(u_i))^{\phi(Q_i)} = (O(n))^{\phi(Q_i)/Q} = (O(n))^{\epsilon/2}. \end{aligned}$$

提醒大家當有個函數 f 時，$O(f)$ 表示一個取絕對值後小於等於 $|f|$ 的某個固定常數倍的項。 □

研究 6.2: ISL 2008 N6/論文題

1. 試證存在無窮多個整數 n 使得 n^2+1 的最大質因數比 $2n+\sqrt{2n}$ 還大。
2. 是否存在整數 $k>3$ 使得 $(1+1^2)(1+2^2)\cdots(1+k^2)$ 是個完全平方數？

第 1. 題的背景顯然是 Euler's conjecture：存在無窮多個整數 n 使得 n^2+1 是質數。如果猜想成立，那此命題也馬上得證了。

我們自然會想用學過的性質來解決它。記得在上一題分析時說過，對所有至少兩個相異根的 $f(x)$，都會有 $\lim_{x\to\infty} P(f(x))=\infty$，而此題要求出的就是 $P(f(x))$ 的成長速率。

1973 年，蘇聯數學家 C. B. Kotov 用 Baker's theorem 證明了：只要不可約整係數多項式 $f(x)$ 的次數大於等於 2，那麼必定有

$$P(f(x))>c_f\log\log x,\ \ \forall x>x(f).$$

其中 $c_f, x(f)$ 是依賴多項式的常數 (其實他只證了次數大於等於 4 的情況，次數為 2,3 則分別被 Schinzel 和 Sprindžuk 解決)。也就是說，任意多項式的最大質因數成長速率至少是 $\log\log x$ (因此又給出了 ISL 2011 N2 的證明)！

然而這個結果還無法解決我們一開始的問題。現在把眼光放低一點，反正題目只要我們證明“有無窮多個 n 使得 n^2+1 的最大質因數好大”，因此我們僅須找到一種對無窮多個 n 成立的多項式最大質因數估計即可。1967 年 C.Hooley 證明了：如果 D 不是完全平方數，那麼 n^2-D 的最大質因數可以超過 $n^{1.1}$ 無窮多次。而在 1986 年 J.M.Deshouillers 和 H.Iwaniec 改進了他的方法，證明了 n^2-D 的最大質因數可以超過 $n^{1.2}$ 無窮多次。至此，原本的命題得到了證明。

另外為了解決 Bunyakovsky conjecture，一個研究是說當不可約整係數多項式 G 的次數大於等於 2 時，G 的值域中是否有無窮多個數在 P_r 中 (其中 P_r 是質因數個數 (重複計算) 小於等於 r 的數的集合)？為方便，先定義 g 是 G 的次數。這問題是 Rademacher 在 1924 年首先研究的，他證明了 G 的值域中有無窮多個數在 P_{4g-1} 中，經過了一堆數學家的研究，在 1968 年 Richert 證明了 G 的值域中有無窮多個數在 P_{g+1} 中。

接下來要進入論文題：雖然乍看之下和 ISL 沒什麼關聯，但其實是有的。對於乘積 $(1+1^2)\cdots(1+k^2)$，理所當然的，我們想套用上面的結論：n^2+1 的最大質因數會超過 $n^{1.2}$ 無窮多次。現在假設找到 $1\sim k$ 裡面使得 n^2+1 的最大質因數超過 $n^{1.2}$ 的最大的數 n，且最大質因數為 p。那麼可以知道 $p\,||\,n^2+1$，因此如果要是完全平方數，那一定要找到 m 使得 $p\mid m^2+1$，且此時要有 $p\mid m^2-n^2=(m+n)(m-n)$，因此 $m+n\geq p$，即 $m\geq p-n>n^{1.2}-n$。這給我們一個啟示：如果能知道 n^2+1 的最大質因數超過 $n^{1.2}$ 的那些 n 的分布密度，那麼或許可以估計一些東西以證明出矛盾，證明原式絕對不是完全平方數。

可惜事情沒那麼好混，我們並不知道他們的分布密度。所以你可能會開始想，或許單一 $(1+k^2)$ 的質因數與乘積 $(1+1^2)\cdots(1+k^2)$ 的質因數結構或是估計並不能放在一

起計算。1877 年 2 月 14 日，一位非凡的數學家誕生了，他的名子叫 Edmund Landau。1909 年，他出版了 ⟨⟨Handbuch der Lehre von der Verteilung der Primzahlen⟩⟩，是首度對解析數論有系統論述的著作，並且推廣了 (其實最早由 Paul Bachmann 在 1892 年就引入) 函數分析中超級重要的概念：Big O notation。

定義 7.9 (Big O notation) 令 $f, g : \mathbb{R} \to \mathbb{R}$ 是兩個函數，當且僅當存在某個正實數 M 使得存在 x_0 滿足 $|f(x)| < M|g(x)|,\ \forall x > x_0$ 時，我們記做 $f(x) = O(g(x))$.

這在分析學中估計誤差項時是非常好用的工具，如我們第一題已經先偷用了。另外一般為了表示不同的成長速率，我們會把 $f = O(g)$ 記作 $f \ll g$。回到原本的問題，Landau 在書中的第 27 節證明了：乘積 $(1+1^2)\cdots(1+x^2)$ 的最大質因數成長速率會超過任何 x 的常數倍 (於是也把 ISL 的命題加強了)。

證明： 以 P_x 表示 $(1+1^2)(1+2^2)\cdots(1+x^2)$ 的最大質因數。假設存在正數 M 使得會有無窮多個 x 滿足 $P_x \le Mx$。對任一這樣的 x，我們計算 $(1+1^2)(1+2^2)\cdots(1+x^2)$ 的任一質因數 p 的最大次方：

Case I. $p = 2$。
那麼我們知道不可能有 $2^2 \mid 1+y^2$，因此

$$v_2\left((1+1^2)(1+2^2)\cdots(1+x^2)\right) \le (x+1)/2.$$

Case II. $p \equiv 1 \pmod 4$。
假設 $p^m \mid 1+y^2$，顯然在 $1 \le y \le p^m$ 時會有兩個解，因此

$$v_p\left((1+1^2)(1+2^2)\cdots(1+x^2)\right) \le \sum_{p \le Mx} 2\left(\left[\frac{x}{p^m}\right]+1\right).$$

另外當 $p \equiv 3 \pmod 4$ 時由二次剩餘基本性質不可能有 $p \mid 1+y^2$。接著，我們開始分析在乘積 $(1+1^2)(1+2^2)\cdots(1+x^2)$ 中每個質數對他的貢獻。注意到必須要有 $p^m \le 1+x^2$ 才會計算到 p 貢獻了 m 次，因此我們對 p 最大就是加到 $\log(1+x^2)/\log p$ 冪次。並且，我們求和的質數 p 小於等於乘積的最大質因數，因此也不超過 Mx。最後還需要知道質數定理以及 Dirichlet 定理：

(1) 以 $\pi(x)$ 記小於等於 x 的質數個數，那麼 $\pi(x) = O\left(\dfrac{x}{\log x}\right)$。

(2) 當 m, l 互質時，$\displaystyle\sum_{\substack{p \equiv l \pmod m \\ p \le x}} \frac{\log p}{p} = \frac{1}{\phi(m)}\log x + O(1)$。

分析完求和條件後，現在開始估計：

$$\begin{aligned}
\log\prod_{n=1}^{x}(1+n^2) &= \sum_{n=1}^{x}\log(1+n^2)\\
&\le 2\cdot\frac{x+1}{2}+\sum_{\substack{p\equiv 1\ (\mathrm{mod}4)\\ p\le Mx}}\log p\left(\left(\frac{2x}{p}+2\right)+\left(\frac{2x}{p^2}+2\right)+\cdots\right)\\
&= O(x)+\sum_{\substack{p\equiv 1\ (\mathrm{mod}4)\\ p\le Mx}}\log p\left(\left(\frac{2x}{p}+2\right)+\cdots\right)+O(\sum_{\substack{p\equiv 1\ (\mathrm{mod}4)\\ p\le Mx}}\log p\cdot\frac{\log(1+x^2)}{\log p})\\
&= O(x)+2x\sum_{\substack{p\equiv 1\ (\mathrm{mod}4)\\ p\le Mx}}\frac{\log p}{p-1}+O\left(\log x\cdot\pi(Mx)\right)\\
&< O(x)+2x\sum_{\substack{p\equiv 1\ (\mathrm{mod}4)\\ p\le Mx}}\frac{5}{4}\cdot\frac{\log p}{p}+O\left(\log x\cdot\frac{x}{\log x}\right)\\
&< \frac{5}{8}x\log x+O(x).
\end{aligned}$$

這件事對無窮多個 x 要成立。但那是不可能的，因為隨便估一下就知道

$$\sum_{n=1}^{x}\log(1+n^2)>2\sum_{n=1}^{x}\log n>2\log x^{(x/2)}=x\log x.$$

這就產生了矛盾。故原命題成立。 □

並且，利用類似的方法我們同樣可以證明對所有整數 a，$(a+1^2)(a+2^2)\cdots(a+x^2)$ 的最大質因數成長速率依舊比 x 的任何常數倍還快。而在 1922 年，Negall 更將命題推廣到多項式代連續整數進去的值相乘，直接估計出了其最大質因數的成長速率 (關於這點，筆者查不到文獻，此處是 Erdős 所宣稱)：

定理 7.35 (Nagell's theorem) 令 $f(x)$ 是一個整係數多項式，且不能在 $\mathbb{Q}[x]$ 上完全分解成線性因式的乘積，以 P_x 表示 $f(1)f(2)\cdots f(x)$ 的最大質因數，那麼對足夠大的 x 都有 $P_x>cx\log x$.

好的，讓我們回去看原命題，其實我們已經可以證明讓 $(1+1^2)(1+2^2)\cdots(1+x^2)$ 為完全平方數的 x 是有限的了！僅需取 x 夠大，讓 $(1+1^2)(1+2^2)\cdots(1+x^2)$ 的最大質因數 p 超過 $2x+1$，這時你會發現 $v_p\left((1+1^2)(1+2^2)\cdots(1+x^2)\right)=1$，於是當然它不可能是完全平方數。至於要估計出一個確切的上界，必需把分析過程中出現的常數都寫出來。有興趣者可以參考論文 J. Cilleruelo, *Squares in* $(1^2+1)\cdots(n^2+1)$, J. Number Theory 128 (2008), 2488-2491. 作者只用到初等方法。不過筆者這裡用的手段和裡面的內容有點小差異。

研究 6.3: ISL 2009 N7

若 a, b 是兩個大於 1 的相異正整數，證明存在正整數 n 使得 $(a^n - 1)(b^n - 1)$ 不是完全平方數。

最後一題讓我們來玩玩不同的東西。剛剛都是討論某個數的最大質因數，如果改看全部的質因數那會發生什麼事呢？1985 年，Joseph Osterlé 及 David Massor 在研究代數幾何時提出了猜想：

猜想 7.1 (The abc conjecture) 對所有正常數 ϵ，總存在常數 $M(\epsilon)$ 使得對所有滿足 $a + b = c$ 的互質整數 a, b, c，都有

$$\max\{|a|, |b|, |c|\} < M(\epsilon) \cdot \mathrm{rad}(abc)^{1+\epsilon}.$$

其中 $\mathrm{rad}(N)$ 是正整數 N 的所有質因數相乘。

不久後數學家就發現這個東西實在太強了，許多 Diophantine 方程都可以用此宣稱解數有限，因此被大師 Goldfeld 譽為「Diophantine 分析中最重要的猜想」。幾年前日本數學家望月新一宣稱已攻破此猜想，不過直到筆者重新整理講義的今天—2017 年 2 月—還是沒幾個人能看得懂他的論文。

先來對這個猜想作一些附註。首先是：為什麼不能取 $\epsilon = 0$ 呢？仔細注意不等式兩邊，左邊顯然跑很快，但是較大的右邊卻只能取到全體質因數相乘，也就是說如果不小心有 $abc = t^k$ 之類的，那麼要有 $\max\{|a|, |b|, |c|\} \ll t$，這樣右式很容易就被蓋掉了！用此想法可以證明：

性質 7.5 不能取 $\epsilon = 0$，因為 $\liminf_{\epsilon \to 0} M(\epsilon) = +\infty$.

證明： 考慮 Pell 方程 $x^2 - 2y^2 = 1$ 的解 (x_n, y_n)，由 $x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n$ 給出。用數學歸納法可以證明 $2^{m+1} \mid y_{2^m}$。當把 abc 猜想用在方程 $1 + 2y_n^2 = x_n^2$ $(n = 2^m)$ 時，可以得到

$$\begin{aligned} x_n^2 &\le M(\epsilon) \cdot \mathrm{rad}(2x_n y_n)^{1+\epsilon} \le M(\epsilon)(2x_n \frac{y_n}{2^{m+1}})^{1+\epsilon} \\ &= M(\epsilon)(x_n \frac{y_n}{2^m})^{1+\epsilon} < M(\epsilon)\frac{x_n^{2(1+\epsilon)}}{2^{m(1+\epsilon)}}. \end{aligned}$$

固定 n，把 ϵ 趨近 0 就得到結論。 □

Erdős 和 Woods 曾經猜測：存在某個常數 k，我們可以僅用 $x + 1, \ldots, x + k$ 的質因數來決定任意正整數 x。數學家 Langevin 在 1992 年發現這個東西只是 abc 猜想的一個小推論而已：

證明： 我們證明只可能存在有限組正整數 $n < m$ 滿足

$$\mathrm{rad}(n + i) = \mathrm{rad}(m + i) \quad \text{for } i = 1, 2, 3, 4.$$

事實上，如果此式要成立，那我們來看方程式 $(n+1)-1=n$，可以得到

$$n < n+1 \ll \mathrm{rad}(n(n+1))^{1+\epsilon} = \mathrm{rad}(n)^{1+\epsilon}\mathrm{rad}(n+1)^{1+\epsilon}.$$

類似的式子對 m 也會成立。現在 $0 < m-n = (m+i)-(n+i)$，因此 $m-n$ 總是被 $\mathrm{rad}(m+i)$ $(i=1,2,3,4)$ 給整除。並注意到 $\gcd(m+i, m+j) \le j-i = O(1)$，因此

$$\mathrm{lcm}[\mathrm{rad}(m+1), \ldots, \mathrm{rad}(m+4)] \gg \mathrm{rad}(m+1)\cdots\mathrm{rad}(m+4).$$

既然 $m-n$ 是全部 $\mathrm{rad}(m+i)$ 的公倍數，就可以給出

$$\mathrm{rad}(m+1)\cdots\mathrm{rad}(m+4) \ll m-n \le m+1 \ll \mathrm{rad}(m+1)^{1+\epsilon}\mathrm{rad}(m+2)^{1+\epsilon},$$
$$\mathrm{rad}(m+3)\mathrm{rad}(m+4) \ll \mathrm{rad}(m+1)^{\epsilon}\mathrm{rad}(m+2)^{\epsilon}.$$

這邊大家應該已經看出來要爆了，最後再取到 $\epsilon = 1/3$ 就會有

$$\begin{aligned} m < m+3 &< \mathrm{rad}(m+3)^{1+\epsilon}\mathrm{rad}(m+4)^{1+\epsilon} \\ &\ll (\mathrm{rad}(m+1)\mathrm{rad}(m+2))^{\epsilon(1+\epsilon)} \\ &\le ((m+1)(m+2))^{\epsilon(1+\epsilon)} \ll m^{8/9}. \end{aligned}$$

所以 $m = O(1)$。我們就可以再把 k 往上取，把所有例外弄掉。 □

這告訴我們可以用 x 附近的數的質因數來決定任意正整數 x。現在回到原本的 ISL 題，運用 Lifting the Exponent Lemma 可以把它轉化成：如果對所有質數 p 都有 $\delta_p(a) = \delta_p(b)$，那麼 $a = b$。你可能想要從代數數論的角度來解釋，但相信我，這種類型的命題基本上都會變成很難的猜想，請放棄這條路 (但在這裡你或許可以上 AoPS 查關鍵詞：A masterpiece)。

性質 7.6 假設 abc 猜想成立，那麼我們可以用 x 對質數的 order 來決定這個正整數。也就是說，如果 $\mathrm{rad}(a^n-1) = \mathrm{rad}(b^n-1)$ 對所有正整數 n 都成立，那麼 $a = b$。

證明： 假設 $b > a > 1$ 是給定的整數，並且滿足等式。考慮方程式 $(b^n-1)+1 = b^n$，由 abc 猜想可以有

$$b^n \ll \mathrm{rad}(b^n-1)^{1+\epsilon} = \mathrm{rad}(a^n-1)^{1+\epsilon} \ll a^{n(1+\epsilon)}.$$

因為 $b > a$，所以 $\log b > \log a$。現在取 ϵ 夠小，使得 $c_0 = \log b - (1+\epsilon)\log a > 0$，那麼對這個 ϵ 就會有

$$e^{n\log b} \ll e^{(1+\epsilon)n\log a},$$

代表 $e^{c_0 n} \ll 1$，也就是 $n \ll 1$。 □

評論 7.2 這裡用了一個大猜想來證明 ISL 的題目，不知道考試時到底該不該給分。

顯然用 abc 猜想可以估計出更多和冪次數有關的 Diophantine 方程，例如 Fermat 猜想之類的，在那方面的進展就讓我們略去。

假設說今天有個整係數的齊次多項式 $F(x,y)$，你想要估計它的成長速率 (單變數是 trivial)，很快會發現沒那麼容易，因為即使有一個變數跑很大，可能還是可以調整另一個讓他減下來，而關鍵似乎就在 $F(x/y,1)$ 這個單變數多項式的根上。首先記 $H = H(m,n) = \max\{|m|,|n|\}$，注意到當複數 $\alpha \neq \beta$ 給定時，可以估計出 $(m-\alpha n)-(m-\beta n) = (\alpha-\beta)n$，以及 $\beta(m-\alpha n)-\alpha(m-\beta n) = (\beta-\alpha)m$，因此 $\max\{m-\alpha n, m-\beta n\} \gg H$。並由 Thue-Siegel-Roth theorem 可以知道：

$$|F(m,n)| \gg n^{\deg(F)} \prod_{\theta:\ F(\theta,1)=0} \left|\theta - \frac{m}{n}\right| \gg H^{\deg(F)-2-\epsilon}.$$

而文獻 [?] 帶我們走得更遠：

定理 7.36 假設 abc 猜想成立，而 $f(x,y) \in \mathbb{Z}[x,y]$ 是個齊次且無重根的多項式，那麼

$$\mathrm{rad}(f(m,n)) \gg_{f,\epsilon} \max\{|m|,|n|\}^{\deg(F)-2-\epsilon}.$$

其中 $\epsilon > 0$ 是給定的常數，而 m,n 是互質的整數。

在開始證明之前，可能有人聽過多項式中的 abc 猜想：Mason's theorem，我們現在需要一個比他再強一些的引理：

引理 7.3 假設 $f(x,y) \in \mathbb{Z}[x,y]$ 是齊次且無重根的多項式，那麼可以找出另外三個齊次且無公因式的多項式 $a(x,y), b(x,y), c(x,y) \in \mathbb{Z}[x,y]$，次數均為 D。$a(x,y)b(x,y)c(x,y)$ 的根 (重根僅算一次) 有 $D+2$ 個，且包含 $f(x,y)$ 的所有根，最後還滿足 $a+b=c$。

證明： (定理的證明) 對 $f(x,y)$，用引理可以找到 $a(x,y), b(x,y), c(x,y)$，把他們相乘後不可約的因子拿出來看，可以得到形如 $f(x,y)g(x,y)$ 的東西，次數為 $D+2$。

令 $d = \gcd(a(m,n), b(m,n))$，其中 $(m,n)=1$。那麼因為 $d \mid \mathrm{res}(a,b)$，且 $a(x,y), b(x,y)$ 無公因式，所以 d 有界。考慮 $a(m,n)/d + b(m,n)/d = c(m,n)/d$ 可以得到：

$$\max\{|a(m,n)|,|b(m,n)|\}^{1-\epsilon} \ll \mathrm{rad}(abc) \ll \mathrm{rad}(fg) \leq \mathrm{rad}(f(m,n))g(m,n).$$

現在令 $H = H(m,n) = \max\{|m|,|n|\}$，注意到 α 給定時 $|m-\alpha n| \ll H$，因此 $g(m,n) \ll H^{D+2-\deg(F)}$。然後剛剛說了 $\max\{m-\alpha n, m-\beta n\} \gg H$，因此 $\max\{a(m,n), b(m,n)\} \gg H^D$。代回式子便得到了**定理 6.27**。 □

另外做一點附註，$\deg(F)-2-\epsilon$ 已經是最好的估計了，也就是說總是找得到無窮多組互質的 m,n 滿足 $\mathrm{rad}(f(m,n)) \ll_f \max\{|m|,|n|\}^{\deg(F)-2}$，大意是用 Hensel's lemma 取一個好的質數 p 讓 p 很大次方整除 $f(m,n)$ 再估計。如果說今天考慮單變數次數為 d 的多項式 $g(x) \in \mathbb{Z}[x]$，那麼我們可以考慮相對應的 $f(x,y) = y^{d+1}g(x/y)$，這告訴我們 $g(x) = f(x,1)$，所以有 (然後你發現 ISL 2011 N2 又證完了)：

定理 7.37 假設 abc 猜想成立，而 $g(x) \in \mathbb{Z}[x]$ 是個無重根的多項式，那麼

$$\mathrm{rad}(g(m)) \gg_{g,\epsilon} |m|^{\deg(g)-1-\epsilon}.$$

其中 $\epsilon > 0$ 是給定的常數。

至此看來 abc 猜想似乎很強，但不能給出一個好的界，而僅能宣稱夠大時會怎樣。假設 $p_1, \ldots, p_k$ 是一堆質數，寫作 $L = \log|\log p_1^{a_1} \cdots p_k^{a_k}|$，那麼 Baker's theorem 給出了估計

$$L \geq -(16k)^{2(k+2)}(\log A)\prod \log p_i.$$

其中 A 是 $a_1, \ldots, a_k$ 中最大者。而事實上可以發現 abc 猜想給出了

$$L \gg (\log A)\prod \log p_i.$$

所以 Baker's theorem 和 abc 猜想在某種意義下是等價的。而用這樣的想法，Stewart 和 Yu 在 2001 年證明出 abc 猜想較弱的形式：$\max\{|a|,|b|,|c|\} < \exp(M(\epsilon)\mathrm{rad}(abc)^{\frac{1}{3}+\epsilon})$.

Problem set

P1. Assume that the abc conjecture is true. Prove that if $g(x) \in \mathbb{Z}[x]$ has no repeated roots and a prime power q^k divides $g(m)$, then $q \ll |m|^{(1+\epsilon)/(k+1)}$.

P2. Assume that the abc conjecture is true. Let p_i be the i-th powerful number, then $p_{n+2} - p_n \to \infty$ as $n \to \infty$. But there are infinitely many n such that $p_{n+1} - p_n = 1$.

Chapter 8

終章——總整理

這一章是前面稍微整理過的，這裡的每個性質大概都很重要，如果下面提到的某個想法還不熟，也許該回去前面複習一下。還有也加了一些前面沒有的章節和題目，順序也沒跟前面一樣。這裡的題因為幾乎沒有更新大概都比較舊。

8.1 指數與原根

(1) 若兩正整數 a 和 m 互質，且 $a^k \equiv 1 \pmod{m}$，則 $\delta_m(a) \mid k$。

(2) 若兩正整數 a 和 m 互質，且 $\delta_m(a) = d$，則 $\delta_m(a^k) = \dfrac{d}{\gcd(d,k)}$。

(3) 若 p 為一奇質數，且 $a \neq \pm 1$ 不被 p 整除，設 $\delta_p(a) = d$，k_0 是使得 $a^d \equiv 1 \pmod{p^{k_0}}$ 成立的最大的正整數，則

$$\delta_{p^k}(a) = \begin{cases} d & , \quad k \leq k_0 \\ dp^{k-k_0} & , \quad k > k_0 \end{cases}$$

(4) 當且僅當 $m = 2, 4, p^k, 2p^k$ 時模 m 有原根。

(5) 原根可以生成簡化剩餘系。

(6) (The Carmichael Function)

$$\lambda(m) = \begin{cases} \phi(m) & , \quad m = 2, 4, p^k, 2p^k \ (p\text{為奇質數}) \\ 2^{k-2} & , \quad m = 2^k \ (k \geq 3) \\ \operatorname{lcm}[\lambda(p_1^{k_1}), \cdots, \lambda(p_t^{k_t})] & , \quad m = p_1^{k_1} \cdots p_t^{k_t} \end{cases}$$

(7) (Hensel's Lemma) 設 $f(x)$ 為一整係數多項式，且令 m, k 為兩正整數使得 $m \leq k$。若整數 r 使得

$$f(r) \equiv 0 \pmod{p^k} \text{ 且 } f'(r) \not\equiv 0 \pmod{p}$$

那麼存在整數 s 使得

$$f(s) \equiv 0 \pmod{p^{k+m}} \text{ 且 } r \equiv s \pmod{p^k}$$

而且 s 在模 p^{k+m} 下是唯一的，可以寫成 $s = r + tp^k$。

P1. (Romania TST 2008) 令 $m, n \geq 3$ 是兩個奇數。試證 $2^m - 1 \nmid 3^n - 1$.

P2. 證明對任意正整數 m, d，存在正整數 x 使得 $\delta_m(x) = d$ 當且僅當 $d \mid \lambda(m)$。

P3. 令 p 是質數。給定 $a_1, \ldots, a_n$ 是 n 個兩兩相異且不超過 $p-1$ 的正整數，滿足

$$p \mid a_1^k + \cdots + a_n^k, \quad \forall k = 1, \ldots, p-1.$$

試求出 $\{a_1, \ldots, a_n\}$。

P4. 給定整數 a 以及質數 p。試證指數同餘方程 $a^k \equiv 1 \pmod{p^k}$ 僅有有限組整數解 k。

P5. 試求出所有正整數數對 (a, b, c) 滿足：$(2^a - 1)(3^b - 1) = c!$。

P6. 令 $N > 1$ 是奇數。證明不可能會有 $a^{N-1} \equiv -1 \pmod{N}$。

P7. 令 $k \geq 2$ 是整數。證明有無窮多個合數 n 使得對所有與 n 互質的整數 a，總有 $n \mid a^{n-k} - 1$。

P8. (USA TST 2003) 試求出所有質數數對 (p, q, r) 使得

$$p \mid q^r + 1, \quad q \mid r^p + 1, \quad r \mid p^q + 1.$$

P9. (China TST 2004) 給定正整數 u。試證方程 $n! = u^a - u^b$ 僅有有限多組正整數解 (n, a, b)。

P10. (IMToT 2011) 對所有 $n > 1$，證明 $1^1 + 3^3 + 5^5 + \cdots + (2^n - 1)^{2^n - 1}$ 被 2^n 整除，但不被 2^{n+1} 整除。

8.2 型式 $x^n - y^n$, $x^n + y^n$

(1) $\gcd(x^m - y^m, x^n - y^n) = x^{\gcd(m,n)} - y^{\gcd(m,n)}$。

(2) $\gcd(x^m + y^m, x^n + y^n) = x^{\gcd(m,n)} + y^{\gcd(m,n)}$ (當 m, n 都是奇數)。

(3) 如果有 $p^N \mid\mid x - c$，多模一次寫成 $x \equiv c + tp^N \pmod{p^{N+1}}$.

(3) Lifting the Exponent Lemma。

(4) (Zsigmondy's theorem)

(a) 若 $a > b \geq 1$，且 a, b 互質，那麼 $a^n - b^n$ 至少有個質因數 p，使得對所有 $k < n$，p 不整除 $a^k - b^k$。除了例外：1. $2^6 - 1^6$ 以及 2. $n = 2$，且 $a + b$ 是 2 的冪次。

(b) 若 $a > b \geq 1$，且 a, b 互質，那麼 $a^n + b^n$ 至少有個質因數 p，使得對所有 $k < n$，p 不整除 $a^k + b^k$。除了例外：$2^3 + 1^3$。

P1. 證明對所有互質的正整數 $a > b$，以及 $n = 2^\alpha n_1 > 2$，總有 $n^{\tau(n)/2} \mid \phi(a^n - b^n)$ 以及 $\frac{1}{2}(2^{\alpha+2}n)^{\tau(n_1)/2} \mid \phi(a^n + b^n)$。

P2. 若自然數 x, y, p, n, k 滿足 $x^n + y^n = p^k$，且 n 是大於 1 的奇數，p 是奇質數，試證 n 是 p 的冪次。

P3. 給定整數 $a \geq 4$，證明存在無窮多個無平方因數的整數 n，使得 n 整除 $a^n - 1$。

P4. 給定實數 $x_1, \ldots, x_n$，假設對任意正整數 k 都有 $x_1^k + \cdots + x_n^k$ 是整數，證明 $x_1, \ldots, x_n$ 都是整數。

P5. (China MO 2011) 給定兩個自然數 m, n。試證存在無窮多組正整數數對 (a, b) 滿足

$$a + b \mid am^a + bn^b, \quad (a, b) = 1.$$

P6. (ISL 2012 N6) 給定兩個自然數 x, y。試證若對所有的正整數 n，都有 $2^n y + 1$ 整除 $x^{2^n} - 1$，則 $x = 1$。

P7. 若合數 n 滿足 $2^n \equiv 2 \pmod{n}$，則稱 n 是一個偽質數。試證對任意正整數 $k > 1$，總有無窮多個偽質數恰好是 k 個不同質數相乘。

P8. 證明對任意給的六個正整數 a, b, c, d, e, f，只要 $a^i + b^i + c^i - d^i - e^i - f^i, i = 1, 2, \ldots, 6$ 都被某個質數 p 整除，那麼對所有正整數 n，$a^n + b^n + c^n - d^n - e^n - f^n$ 都會被那個質數 p 整除。

8.3 Diophantine 方程

(1) A Collection of Algebraic Identities。

(2) (Thue's Theorem) 若 $H(x, y)$ 是次數不小於 3 且齊次的整係數多項式，那麼僅當 $H(x, y) = q_n(ax + by)^n$ 或是 $q_n(ax^2 + bxy + cy^2)^{\frac{n}{2}}$ 時 (其中 q_n 是有理數)，不定方程 $H(x, y) = d \neq 0$ 才可能有無限多組整數解 (x, y)。

(3) 指數不定方程大概就是型如 $a^x - b^y = c$ 之類的東東，而由 Pólya-Størmer Theorem 我們知道給定 a, b, c 時只會有有限組解 (x, y)。通常解這類方程有幾種方法:

(a) 同餘 a, b 的質因數次方，或者同餘其他質數次方。這時可以得出 x, y 的形式。

(b) 由 (1) 找出形式 $x = cm + n$ 之後，再模 p^t，而這些質數次方必須讓 $\delta_{p^t}(a)$ 盡量小 (就是讓 $(p-1, a)$ 的比率盡量大)，或是讓 a 是原根。

(c) 假設你猜 (x_0, y_0) 是最大解，改寫原方程變為 $a^{x_0}(a^u - 1) = b^{y_0}(b^v - 1)$，然後繼續模，直到導出例如左邊要被 a^{x_0+1} 這種矛盾。

P1. 求出 $2^a 3^b 7^c - 43^d = 1$ 的所有正整數解 (a, b, c, d)。

P2. 求出不能以 $2^x 3^y - 2^z 3^w$ 表示的最小正整數，其中 x, y, z, w 都是非負整數。

8.4 二次型

(1) 基本 Pell 方程：若 z_0 是 $\mathbb{Z}[\sqrt{d}]$ 的基本解。則對所有 $z \in \mathbb{Z}[\sqrt{d}]$ 滿足 $N(z) = 1$ 者，必有某整數 n 及適當正負號使 $z = \pm z_0^n$。

(2) 廣義 Pell 方程：若 z_0 是 $\mathbb{Z}[\sqrt{d}]$ 的基本解。則存在有限個數 $z_1, z_2, \ldots, z_m \in \mathbb{Z}[\sqrt{d}]$，使得對所有 $z \in \mathbb{Z}[\sqrt{d}]$ 滿足 $N(z) = a$ 者，必有某整數 n, i 及適當正負號使 $z = \pm z_i z_0^n$。

(3) 若已知有理係數二次方程上的一個有理點，則上面所有有理點都可以用 Vieta jumping 找出。

(4) (Thue's Lemma) 給定整數 a，則可找到整數 $0 < x, y < \sqrt{p}$ 使得 $ax \equiv y \pmod{p}$。並用 Thue's Lemma 證明型如 $x^2 + ny^2$ 的質數。

(5) 表示論。15,290-theorem 以及 Hasse-Minkowski local-global principle。

P1. (Fermat's theorem) 試證沒有大於 1 的三角數是四次方數。

P2. 在幾何學裡，海倫三角形是指邊長和面積都是整數的三角形。試求出所有以連續正整數為邊長的海倫三角形。

P3. (Romania MO 2004) 試求出所有可表示成

$$\frac{a^2 + ab + b^2}{ab - 1}$$

的正整數，其中 a, b 是不等於 1 的正整數。

P4. (ISL 2002 N4) 試問是否存在正整數 m 使得方程

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{abc} = \frac{m}{a + b + c}$$

有無窮多組正整數解 a, b, c？

P5. (Markoff-Hurwitz equation) 考慮方程

$$x_1^2 + \cdots + x_n^2 = a x_1 \cdots x_n$$

其中 $n \geq 3$。試證當 $a > n$ 時無解，$a = n$ 時所有解可由 $(1, \cdots, 1)$ 生成。

P6. 試證所有在 $(0, 1)$ 區間中且分母是奇數的有理數都可寫成

$$\frac{xyz}{x^2 + y^2 + z^2}.$$

的型式，其中 x, y, z 是適當的整數。

P7. 試求出最小的正整數 n，使得存在全不為 -1 的整數 $a_1, \ldots, a_n$，滿足所有的質數都可以寫成 $x^2 + a_i y^2$ 的型式，其中 x, y, i 是適當的正整數。

P8. (Thue's Lemma 的應用)

(a) 證明所有 $4k+1$ 型的質數可以寫成 x^2+y^2。

(b) 證明所有 $8k+1,+3$ 型的質數可以寫成 x^2+2y^2。

(c) 證明所有 $7k+1,+2,+4$ 型的奇質數可以寫成 x^2+7y^2。

(d) (KöMaL ??) 令 n 是正整數，證明方程式 $x^2+xy+y^2=n$ 如果有有理數解那也有整數解。

(e) (KöMaL ??) 證明方程 $x^3-x+9=5y^2$ 沒有整數解。

(f) (Iran MO 2013) 假設 p 是質數，證明 p 可表成 $2x^2+3y^2$ 當且僅當 $p\equiv 5,11 \pmod{24}$。

難**P8.** 考慮二次型：$ax^2+by^2+cz^2+dt^2$，其中 x,y,z,t 都是非負整數。證明當 $(a,b,c,d)=(1,1,2,2)$ 時此二次型能表示所有正整數。你或許會用到四平方和定理。一般地，Ramanujan 證明了不計次序共有 54 組這樣的 (a,b,c,d)。另外如果允許恰有一個正整數不被表達，那共有 88 組。

難**P9.** 試證明不能寫成四個全不為 0 的平方數之和的正整數其自然密度為 0。

8.5 積性函數

(1) 要處理對 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 成立的性質時，只看 $p_i^{\alpha_i}$。

(2) 若 f 是積性函數，則他的和函數亦為積性函數。

(3) 所有質數的倒數和發散 $\Rightarrow$ 很多積性函數會和某東西比例發散。

(4) (Mőbius inversion formula) 設 F 是數論函數 f 的和函數，則

$$f(n)=\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right).$$

P1. (AMM, Problem 5357) 對正整數 n，計 $f(n)$ 為把 n 表示成兩個互質正整數乘積的方法數，次序不計。並令 $v(n)=(-1)^{\omega(n)}$，其中 $\omega(n)$ 是 n 的不同質因數個數。證明

$$\sum_{n=1}^{\infty}\frac{v(n)\left(f(n)\right)^3}{n^2}=\frac{7}{8}.$$

P2. (P. Erdős) 證明對任意正整數 k，方程式 $\phi(x)=k!$ 總有解。

P3. (Iran MO 2012) 證明對所有 $n\in\mathbb{N}$，總存在自然數 $a_1<a_2<\cdots<a_n$ 使得 $\phi(a_1)>\phi(a_2)>\cdots>\phi(a_n)$.

P4. (China TST 2012) 對於給定的正整數 n，如果 $\tau(m)<\tau(n)$ 對所有 $m<n$ 都成立，那麼稱 n 是“好數”。試證對所有正整數 k 都只有有限多個好數不被 k 整除。

P5. (Romania TST 2010) 給定正整數 a。證明有無窮多個正整數 m 滿足 $\tau(am) < \tau(am+1)$。

P6. (Taiwan TST 2011) 試問由以下定義的數列：$a_1 = (2011)!$, $a_i = \phi(a_{i+1})$。是否是個無窮整數數列？

難**P7.** 給定正實數 $b > a > 0$，試證一定存在正整數 n 滿足

$$b > \frac{\phi(n+2)}{\phi(n)} > a.$$

難**P8.** 數學家 Sylvester 引入了一類正整數叫作貓咪數 (admissible numbers)，定義為：如果小於等於 m 且與 m 互質的的所有正整數是模 $\phi(m)$ 的完全剩餘系，那麼稱 m 是貓咪數。貓有無窮多隻。證明既是合數又是貓咪數的整數一定被 3 整除。甚至，證明只能是 15。

8.6 整係數多項式

(1) 若 f 是整係數多項式，則對任意不相等的兩整數 a, b 都有 $a - b \mid f(a) - f(b)$.

(2) 若 $f_1, \ldots, f_n$ 是整係數多項式，則 $\mathbb{P}(f_1) \cap \cdots \cap \mathbb{P}(f_n)$ 是無窮集。

(3) 令 $p_1, p_2, \ldots$ 是 $\mathbb{P}(f)$ 由小排到大的所有元素，那麼存在 M 滿足對所有 $i \geq M$，$f(x)$ 在局部域 $\mathbb{Q}_{p_i}$ 中都有零點。

(4) (Bezout's Theorem) 對任意有理係數多項式 f, g，總存在有理係數多項式 u, v，使得

$$f(x)u(x) + g(x)v(x) = \gcd(f(x), g(x)).$$

(5) (整值多項式判別法) 令 $f(x) \in \mathbb{Q}[x]$ 且次數為 n。則以下條件等價：

(a) 對所有 $x \in \mathbb{Z}$，有 $f(x) \in \mathbb{Z}$.

(b) 對 $n+1$ 個連續整數 x，有 $f(x) \in \mathbb{Z}$.

(c) 存在 $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ 使得

$$f(x) = a_n \binom{x}{n} + a_{n-1} \binom{x}{n-1} + \cdots + a_0 \binom{x}{0}.$$

(6) α 的基佬多項式整除所有以 α 為根的多項式。

(7) $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ 是 α 的極小多項式的次數，並且擴張次數具有可積性。

(8) (Gauss's Lemma) 一個整係數多項式在 $\mathbb{Q}$ 能分解等價於在 $\mathbb{Z}$ 中能分解。

(9) (Lagrange's Theorem) 設 $\deg(f(x)) = d$，則在任一個包含其係數的域中，$f(x)$ 的零點至多有 d 個。

(10) (Tylor's Theorem) 好用的展開式 (通常用 $x = a + tp^k$ 代入):

$$f(x) = \frac{1}{0!}f(a) + \frac{1}{1!}f'(a)(x-a) + \frac{1}{2!}f''(a)(x-a)^2 + \frac{1}{3!}f'''(a)(x-a)^3 + \cdots.$$

P1. 試求出所有整係數多項式 f 滿足：對所有互質的正整數 a, b，數列 $\langle f(an+b)\rangle_{n=1}^{\infty}$ 包含無窮多個值不同的項，並且這些項兩兩互質。

P2. (KöMaL 2009) 對於給定的整係數多項式 $\{p_1(x), \ldots, p_n(x)\}$，如果存在整係數多項式 $q_1(x), \ldots, q_n(x)$ 滿足 $q_1(x)p_1(x) + \cdots + q_n(x)p_n(x) = \gcd(p_1(x), \ldots, p_n(x))$，那麼稱 $\{p_1(x), \ldots, p_n(x)\}$ 是一組歐幾里德算法組。假設對於給定的整係數多項式 $\{f_1(x), \ldots, f_n(x)\}$，任意兩個都會形成一組歐幾里德算法組，證明 $\{f_1(x), \ldots, f_n(x)\}$ 本身就是一組歐幾里德算法組。

P3. 令 $f(x)$ 是整係數多項式。對於給定的整數 a，考慮如下生成的數列: $a_0 = a$, $a_{n+1} = f(a_n)$。試證如果 $a_n \to \infty$，而且 $f(x)$ 不是長成 Ax^d 這副死樣，那麼 $\mathbb{P}(\langle a_n\rangle)$ 是無窮集。

P4. (ISL 2012 N5) 令 n 是整數，定義 $\mathrm{rad}(n)$ 為 n 所有不同的質因數的乘積，且為方便定義 $\mathrm{rad}(0) = 0$, $\mathrm{rad}(\pm 1) = 1$。試找出所有係數全為非負整數的多項式 $f(x)$ 滿足對所有正整數 n，都有 $\mathrm{rad}(f(n))$ 整除 $\mathrm{rad}(f(n^{\mathrm{rad}(n)}))$。

P5. 求出所有多項式 $P(x) \in \mathbb{Z}[x]$ 使得若 $P(m) \mid P(n)$，那麼 $m \mid n$。

P6. (ISL 2011 N6) 令 $P(x)$ 和 $Q(x)$ 是互質的兩整係數多項式。假設對任意正整數 n，$P(n)$ 和 $Q(n)$ 都是正的，並且 $2^{Q(n)} - 1$ 整除 $3^{P(n)} - 1$。試證 $Q(x)$ 是常數多項式。

P7. 令 $f \in \mathbb{Z}[x]$ 是次數為 k 的多項式，使得對所有自然數 n，總有 $\sqrt[k]{f(n)} \in \mathbb{Z}$。試證存在整數 a, b 使得 $f(x) = (ax+b)^k$。

P8. (Romania TST 2003) 令 $f(x)$ 是領導係數為 1 的整係數不可約多項式。假設 $|f(0)|$ 不是平方數。證明 $f(x^2)$ 依然不可約。

P9. (Iran MO 2003) 令 $f_1, f_2, \ldots, f_n$ 是一堆整係數多項式。試證存在可約的多項式 $g(x) \in \mathbb{Z}[x]$ 使得 $f_i(x) + g(x)$ 全都不可約。

P10. (Iran TST 2011) 令 p 是質數而 k 是正整數使得 $k \le p$。已知 $f(x)$ 是整係數多項式滿足對所有 $x \in \mathbb{Z}$ 都有 $p^k \mid f(x)$.

(a) 試證存在整係數多項式 $A_0(x), \ldots, A_n(x)$ 使得

$$f(x) = \sum_{i=0}^{k} (x^p - x)^i p^{k-i} A_i(x).$$

(b) 試對所有 $k > p$ 以及每個 p 都找出反例。

P11. (USA TST 2008) 令 n 是正整數。對於給定的整係數多項式 $f(x)$，定義他的模 n 指標是指有序數列 $f(1), f(2), \ldots, f(n)$ 模 n 後的結果。在所有 n^n 個模 n 的 n 項整數數列中，有多少個是某多項式的 $f(x)$ 的模 n 指標，當

(a) n 是無平方因數的正整數?

(b) n 是無立方因數的正整數?

P12. 給定整數 a, b，試證存在 $f(x) \in \mathbb{Z}[x]$ 使得對任意 n，$f(n)$ 的質因數都型如 $ak + b$ 當且僅當 $b = 1$。

難**P13.** 給定正整數 $a > b > 1$，試證對任意 $n > 6$，總有 $P(a^n - b^n) > n$，其中 $P(\cdot)$ 表示最大質因數。更甚，證明 $\lim_{n\to\infty} P(a^n - b^n)/n = \infty$。

8.7 二項式係數

(1) (Lucas's Theorem) 設 p 為一質數，給定兩數 $m < n$，假設他們在 p 進位下分別寫成 $n = (\overline{n_t n_{t-1} \cdots n_0})_p$ 以及 $m = (\overline{m_s m_{s-1} \cdots m_0})_p$，那麼

$$\binom{n}{m} \equiv \prod_{i=0}^{t} \binom{n_i}{m_i} \pmod{p}$$

這裡 $\binom{0}{0} = 1$ 且當 $n_i < m_i$ 時 $\binom{n_i}{m_i} = 0$。

(2) (Kummer's Theorem) 設 p 為一質數，給定兩數 $m < n$，假設 $(n - m) + m$ 此運算在 p 進位下共進了 t 位，則 $p^t \mid\mid \binom{n}{m}$。

(3) 一堆 Wolstenholme's Theorem。

(4) 模逆以及 $\binom{p}{k} \equiv \dfrac{p \cdot (-1)^{k-1}}{k} \pmod{p^2}$。

(5) 二項式係數寫成階乘形式後，可以直接算出某一質因數的冪次。或是用組合恆等式湊出某固定形式後，再看其他東西。

(6) 看到題目要證明 mod p^N，可以瘋狂頭尾配把 mod p^N 消到 mod p。

P1. 求出 $0 \le k \le n$ 時，$\binom{n}{k}$ 裡有幾個數是奇數。

P2. (USA TST 2002) 令 p 是大於 5 的質數，對於給定的整數 x，定義：

$$f_p(x) = \sum_{k=1}^{p-1} \frac{1}{(px + k)^2}.$$

試證對任意 x, y，$f_p(x) - f_p(y)$ 的分子被 p^3 整除。

P3. 試證

$$\frac{1}{1^3}+\frac{1}{2^3}+\cdots+\frac{1}{(p-1)^3}$$

的分子被 p^2 整除。

P4. Pascal 三角很神奇的，任一列大概都不會全互質。證明對任意 $\varepsilon>0$，總存在 $N(\varepsilon)$，使得對所有正整數 $n>N(\varepsilon)$ 以及 $k_1,\ldots,k_{100}<\varepsilon\sqrt{n}$，這 100 個數

$$\binom{2n}{n+k_1},\binom{2n}{n+k_2},\ldots,\binom{2n}{n+k_{100}}$$

有一個大於 1 的公因數。

P5. (ISL 2011 N7) 令 p 為一奇質數。對所有正整數 a 定義

$$S_a=\frac{a}{1}+\frac{a^2}{2}+\cdots+\frac{a^{p-1}}{p-1}.$$

令 m 和 n 是兩個整數使得

$$S_3+S_4-3S_2=\frac{m}{n}.$$

證明 p 整除 m.

P6. 證明如果 $0\le i\le p-1<n$，且 $q=\lfloor\frac{n-1}{p-1}\rfloor$，那麼

$$\sum_{m\equiv j\pmod p}(-1)^m\binom{n}{m}\equiv 0\pmod{p^q}.$$

8.8 函數方程

(1) 競賽數論中函數方程基本上都可以化歸成較特殊的題目：給定 $g(n)\mid f(n)$ 的條件。

(a) 通常我們會從質數下手，先選定會讓 $f(n)$ 變質數的 n 開始討論，或者是先找出 $g(n)$ 在某些特殊 n 值的函數值。

(b) 接著把 $f(n)$ 直接模 $g(n)$，然後被整除得要恆大於其因式，再來開始證明 $g(n)$ 增長的比 $f(n)\pmod{g(n)}$ 還快，就可以把你不期待的解刪去。

P1. (Iran MO 2008) 試求出所有 $f\in\mathbb{Z}[x]$，使得對任意 $a,b,c\in\mathbb{N}$ 都有 $a+b+c\mid f(a)+f(b)+f(c)$.

P2. (ISL 2004 N3 Generalized) 給定正整數 d,e，試確定所有函數 $f:\mathbb{N}\to\mathbb{N}$ 滿足對所有正整數 m,n 都有：

$$(f(m))^d+f(n)\mid(m^d+n)^e.$$

P3. (ISL 2009 N3) 已知某個非常函數 $f:\mathbb{Z}\to\mathbb{Z}$ 滿足對任意 $a\neq b$，都有 $a-b$ 整除 $f(a)-f(b)$，證明 $\mathbb{P}(f)$ 是無窮集。

P4. (ISL 2011 N3) 令 n 是正整數。試確定所有函數 $f:\mathbb{Z}\to\mathbb{Z}$ 使得對任意互異的整數 x,y，$f(x)-f(y)$ 都整除 x^n-y^n。當：

(a) n 是奇數。

(b) n 是偶數。

P5. (ISL 2010 N5) 試求出所有函數 $g:\mathbb{N}\to\mathbb{N}$ 使得對所有正整數 n,m，

$$(g(m)+n)(g(n)+m)$$

總是完全平方數。

P6. (ISL 2015 N7) 一個函數 $f:\mathbb{N}\to\mathbb{N}$ 被稱為 k-好的，如果

$$\gcd(f(m)+n,f(n)+m)\le k$$

對所有 $m\neq n$ 總成立。求出所有 k 使得存在 k-好函數。

P7. (USA TSTST 2012) 令函數 $f:\mathbb{N}\to\mathbb{N}$ 滿足以下條件:

(a) 當 m,n 互質時，$f(m),f(n)$ 也互質。

(b) 對所有 n，有 $n\le f(n)\le n+2012$。

試證對任意自然數 n 及質數 p，如果 $p\mid f(n)$ 那麼也有 $p\mid n$。

8.9 遞迴

(1) 多項式的遞迴關係會讓數列數列 $\langle a_n \pmod m\rangle$ 是循環的 $\Rightarrow$ 看最小週期。

(2) 最小週期可整除任一週期，並且具有可積性。

(3) 在 splitting field 裡處理模。並注意二項式展開。

(4) 很多二階遞迴具有意想不到的算數性質，例如輾轉相除法等。

(5) 把題目要證的先刮起來不看，剩下的東西也有可能會有自己的遞迴。

P1. (ELMO 2010 N4) 令 r 和 s 是兩個正整數。定義一個二階遞迴：$a_0=0$, $a_1=1$, $a_n=ra_{n-1}+sa_{n-2}$。令 $f_n=a_1a_2\cdots a_n$。證明對任意正整數 $n>k>0$，$\dfrac{f_n}{f_kf_{n-k}}$ 都會是整數。

P2. (FKMO 2013) 給定兩互質的正整數 a,b。定義數列 $\langle a_n\rangle,\langle b_n\rangle$ 如下：

$$(a+b\sqrt{2})^{2n}=a_n+b_n\sqrt{2}.$$

求出所有質數 p，使得存在正整數 $n\le p$ 滿足 $p\mid b_n$。

P3. (KöMaL 1997) 假設 $a_1, a_2, \ldots$ 和 $b_1, b_2, \ldots$ 是兩個整數數列且滿足 $a_1 = b_1 = 0$,

$$a_n = nb_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_{n-1} b_1.$$

證明對任意質數 p，a_p 總是被 p 給整除。

P4. 試證 $2^n \mid \binom{2n}{0} + \binom{2n}{2} 3 + \binom{2n}{4} 3^2 + \cdots + \binom{2n}{2n} 3^n$.

P5. $\langle L_n \rangle$ 是盧卡斯數列。證明如果質數 p 整除 $L_{2k} - 2$，那麼 p 也會整除 $L_{2k+1} - 1$。

P6. 證明模 p 下存在廢剝吶棄原根當且僅當 $p \equiv 1$ 或 $9 \pmod{10}$，而且 $l(p) = p - 1$。

P7. (ISL 2003 N7) 數列 $a_0, a_1, a_2, \ldots$ 定義如下: $a_0 = 2$, $a_{k+1} = 2a_k^2 - 1$。證明如果奇質數 p 整除 a_n，那麼 2^{n+3} 會整除 $p^2 - 1$。

Part II

第二部

簡介

這一部是初等解析方法，主要目的是希望帶領讀者一瞥數論中的一些經典結論，也同時補充之前講義提到卻沒有加以證明的部分。內文採用引導式題目的方式一步步建立一些結果，在每一部分中各個小題都是有關連的，但是每一個章節之間彼此是獨立的，但強烈建議讀者從第一章數論函數開始，因為是最基本的。

另外為了版面整潔，除了人名外其餘數學名詞都會翻譯成中文。我們要求讀者寫出「嚴謹」的數學證明，並且使用的性質都必須能夠自己證明出來，當然，如果在解題過程中發現一題太難，可以先跳過並直接承認該題結論，之後再重新做過。

最後，因為以前沒有記參考文獻的習慣，而且這一部內容大半都是看論文後編出來的，所以遺失了很多題目來源。筆者僅記得編題時閱讀過的書與網路講義：

[1] Gerald Tenenbaum & Michel Mendes France, *The Prime Numbers and Their Distribution (Student Mathematical Library, Vol. 6)*, American Mathematical Society (May 5, 2000).

[2] Gerald Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory (Cambridge Studies in Advanced Mathematics)*, Cambridge University Press; 1 edition (June 30, 1995).

[3] Ivan Niven & Herbert S. Zuckerman & Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, Wiley; 5 edition (January 1991).

[4] Jean-marie De Koninck & Florian Luca, *Analytic Number Theory: Exploring the Anatomy of Integers (Graduate Studies in Mathematics)*, American Mathematical Society (May 2, 2012).

[5] Terence Tao & Van H. Vu, *Additive Combinatorics (Cambridge Studies in Advanced Mathematics)*, Cambridge University Press; 1 edition (December 21, 2009).

[6] http://people.reed.edu/∼jerry/361/lectures/lec11.pdf

[7] http://www.dms.umontreal.ca/∼koukoulo/documents/notes/sievemethods.pdf

這邊也要和遺失了題目來源的那些作者道歉，如果讀者知道來源文章麻煩請通知筆者。

Chapter 9

數論函數

- 卷積 convolution
- 整環 integral domain
- 環 ring
- 收斂座標 abscissa of convergence

所謂的數論函數指的是定義域為整數而值域為複數的函數，比方常見的有質因數個數函數 ω、Euler 函數 ϕ、因數和函數 τ 等等。最重要的數論函數是積性和加性函數，在此之上會定義所謂的 Dirichlet 卷積，而得到一個交換環。事實上可以證明他是一個整環。

研究一些數論函數的大小常常可以帶給我們有趣的結論。比方說以 $d(n)$ 計正整數 n 的因數個數，那麼如果 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 是他的質因數分解，可以得到 $d(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1)$. 當我們對質數的成長速率有基本認識後，可以簡單地推得 $d(n) = n^{o(1)}$. 這邊馬上有個應用：欲研究方程 $x^3+y^3 = n$ 的解數，注意到 $x^3+y^3 = (x+y)(x^2-xy+y^2)$，並且由 $x + y$, $x^2 - xy + y^2$ 可以決定出 x, y，至多只有常數倍的誤差，因此方程至多有 $n^{o(1)}$ 個解。

另外一個在解析數論中很基本的問題是要研究由數論函數 f 所決定的 $\sum_{n \le x} f(n)$ 的成長速率。例如質數定理等價於

$$\sum_{n \le x} \Lambda(n) = x + o(x).$$

其中 Λ 表示 Mangoldt 函數。而 Riemann 猜想則是等價於上式的較強形式

$$\sum_{n \le x} \Lambda(n) = x + O(x^{1/2+o(1)}).$$

一般處理級數和的方法有 Euler-Maclaurin 求和公式，或是 Stieltjes 積分等。在本文中不要求讀者有這兩個預備知識，不過會後者的話許多問題便顯得輕鬆多了。

我們從一個簡單的例子開始：假設數論函數 f 是因數和函數 τ，那麼

$$\begin{aligned}\sum_{n\le x}\tau(n) &= \sum_{n\le x}\sum_{d\mid n}1 = \sum_{d\le x}\sum_{n\le x,d\mid n}1\\ &= \sum_{d\le x}\sum_{n\le x,d\mid n}\frac{x}{d}+O(1)\\ &= x\log x+O(x).\end{aligned}$$

這是一個平凡的估計。而 Dirichlet 雙曲線法帶我們走的更精確些：

$$\sum_{n\le x}\tau(n) = x\log x+(2\gamma-1)x+O(\sqrt{x}).$$

運用這個手法還可以求 $f(n)=\tau(n^2+1)$ 等等的情況。到後來 Erdős 終於把結果一般化：假設 P 是一個從定義域和值域都是正整數的不可約多項式，那麼

$$\sum_{n\le x}\tau(P(n))\asymp x\log x.$$

而取 $P(X)=X^2+X+1$，可以出成以下題目：對任意正整數 n，證明存在 n 個兩兩互質的正整數 $k_1,\dots,k_n$ 使得 $k_1\cdots k_n-1$ 是兩個相鄰正整數的乘積。

這個章節旨在建立一些基本結果，以及讓讀者熟悉基本的處理方式。在開始前我們先介紹解析數論中常用的符號。假設存在兩個函數 f,g 對於足夠大的實數都有定義，而且 g 可以寫成 f 和另外一個有界函數的乘積的話，將寫作 $g=O(f)$，這代表函數 g 的成長速率不能超過 f 的成長速率。另一方面，如果 g 可以寫成 f 和另外一個在無窮大時值趨近於 0 的函數乘積的話，將寫作 $g=o(f)$。最後，如果 g 可以寫成 f 和另外一個在無窮大時值趨近於 1 的函數乘積的話，將寫作 $g\sim f$，並且說 f 和 g 等價。為方便我們還可以以 $f\gg g$ 表示 $g=O(f)$，而 $f\ll g$ 表示 $f=O(g)$，並且當 $f\gg g, f\ll g$ 兩式同時成立時，會記 $f\asymp g$，可以看出這代表兩個函數的數量級是相等的。對於實數 x，$[x]$ 指的是小於等於 x 的最大整數，而估計式 $[x]=x+O(1)$ 是非常有用的，以下將會看到。

■ 預備知識 ■

1. 級數問題中常見所謂的 Abel 求和公式：假設 (a_k) 是複數數列，而 $f:[1,+\infty)\to\mathbb{C}$ 是一個 $\mathcal{C}^1$ 函數，對所有實數 $x\ge 1$，我們定義 $A(x)=\sum_{n\le x}a_n$。證明：

$$\sum_{n\le x}a_nf(n) = A(x)f(x)-\int_1^x A(t)f'(t)\,dt.$$

2. 在級數問題中，另外用來估計和的還有積分測試：假設 f 是定義在 $[1,+\infty)$ 的恆正函數，而且 $\lim_{x\to+\infty}f(x)=0$。對正整數 n，定義：

$$s_n=\sum_{k=1}^{n}f(k),\quad t_n=\int_1^n f(x)\,dx,\quad d_n=s_n-t_n.$$

那麼：

(a) $0 < f(n+1) \le d_{n+1} \le d_n \le f(1)$.

(b) $\lim_{n\to+\infty} d_n$ 存在。

(c) s_n 收斂當且僅當 t_n 收斂。

(d) $0 \le d_k - \lim_{n\to+\infty} d_n \le f(k)$, $\forall k \in \mathbb{N}$.

■ 第一部分 ■

定義 $\pi(x)$ 為小於等於 x 的質數個數，在這個部分要探討的是 $\pi(x)$ 的性質，我們將試圖給出質數定理的弱化版本。從現在開始，以 $\Lambda(n)$ 表示 Mangoldt 函數，定義為：

$$\Lambda(n) = \begin{cases} \log p & , \ \exists v \in \mathbb{N},\ n = p^v \\ 0 & , \ \text{其他情況} \end{cases}$$

以及和 $\psi(x) = \sum_{d\le x} \Lambda(d)$。而僅在這個部分中，定義函數 $B(x)$ 如 $B(x) = \log([x]!)$.

1. 證明 $B(n) = \sum_{d\le n} \Lambda(d)[n/d]$.

   接下來考慮函數 $\Upsilon(x) = [x] - 2[x/2]$, $\forall x > 0$，以及 $B_2(x) = B(x) - 2B(x/2)$.

2. 證明 $B_2(x) = x\log 2 + O(\log x)$.

3. 證明 $\Upsilon(x)$ 是週期為 2 的函數，接著求出它在區間 $[0,2)$ 的值，並利用這結果證明 $\psi(x) - \psi(x/2) \le B_2(x) \le \psi(x)$.

4. 證明 $x\log 2 + O(\log x) < \psi(x) < x\log 4 + O((\log x)^2)$.

5. 將 $\psi(x)$ 寫成 $\sum_{p^v\le x} \log p$，證明

$$\psi(x) = \sum_{p\le x} \left[\frac{\log x}{\log p}\right] \log p.$$

   然後證明 $\pi(x) = \psi(x)/\log x + O(\sqrt{x}/\log x)$ (提示：考慮 $p \le \sqrt{x}$ 及 $\sqrt{x} < p \le x$)。

6. 總結以上結果為 Chebyshev 的質數估計：

$$(\log 2 + o(1))\frac{x}{\log x} \le \pi(x) \le (\log 4 + o(1))\frac{x}{\log x}.$$

7. 試利用函數 $\Upsilon(x) = [x] - [x/2] - [x/3] - [x/5] + [x/30]$ 改良上下界，並推論出以下定理：對任意正整數 n，總存在正數 x_0 使得對於所有整數 $x \ge x_0$，區間 $[x, 2x]$ 中都至少有 n 個質數。

8. 利用上述結論證明找到常數 c_1, c_2, n_0 使得 $c_1 n\log n < p_n < c_2 n\log n$ 對所有正整數 $n \ge n_0$ 都成立，其中 p_n 是第 n 個質數。

■ 第二部分 ■

當一個函數的定義域為全體正整數 (或是整數) 時稱它為數論函數。一般數學上研究的數論函數有兩種常見的性質：若對所有互質的正整數 m, n 恆有 $f(mn) = f(m)f(n)$，則稱 f 是積；若是滿足 $f(mn) = f(m) + f(n)$ 則稱 f 是加性的。例如 Euler 函數 $\phi(n)$ 是積性的，而計算相異質數個數的函數 $\omega(n) = \sum_{p|n} 1$ 則是加性的。

當有兩個數論函數 f, g 時，可考慮它們的 Dirichlet 卷積：$(f*g)(n) = \sum_{d|n} f(d)g(n/d)$.

1. 證明以下關於卷積的性質：

   (a) 全體數論函數在加法和卷積下構成交換環。

   (b) Mőbius 反演公式：$g = 1 * f \Leftrightarrow f = \mu * g$.

   (c) 兩個積性函數的卷積仍為積性函數。

對一個數論函數 f，稱 $F(s) = \sum_{n=1}^{+\infty} f(n)/n^s$ 是它的 Dirichlet 級數，在這個部分僅考慮 s 為實數的情況。我們知道如果存在實數 s 使得 $F(s)$ 絕對收斂，那麼對於所有 $s' > s$，$F(s')$ 都會絕對收斂。定義 $\alpha_f = \inf\{s \,|\, F(s)\text{絕對收斂}\}$，稱為函數 f 的收斂座標。另外重要的函數是 Riemann 函數 $\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$，此處僅討論 s 為大於 1 的實數。以下題目需要級數收斂的知識。

2. 假設
$$F(s) = \sum_{n=1}^{+\infty} \frac{f(n)}{n^s}, \quad G(s) = \sum_{n=1}^{+\infty} \frac{g(n)}{n^s}$$
收斂座標存在且都等於 α，而且存在某個發散實數數列 $\alpha \le s_1 < s_2 < \cdots$ 使得 $F(s_k) = G(s_k)\ \forall k \in \mathbb{N}$。考慮 $h(n) = f(n) - g(n)$，如果 x 是最小使得 $h(x) \neq 0$ 的正整數，證明會得到矛盾。以上結果說明了什麼？

3. 如果 f 是積性的，且收斂座標 α_f 存在，證明當 $s > \alpha_f$ 時有等式
$$\sum_{n=1}^{+\infty} \frac{f(n)}{n^s} = \prod_{p\text{ 為質數}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\right).$$

4. 假設 $F(s) = \sum_{n=1}^{+\infty} f(n)/n^s$ 和 $G(s) = \sum_{n=1}^{+\infty} g(n)/n^s$ 的收斂座標都存在且分別等於 α_f, α_g，證明對所有 $s > \max\{\alpha_f, \alpha_g\}$，有等式
$$\sum_{n=1}^{+\infty} \frac{f(n)}{n^s} \sum_{n=1}^{+\infty} \frac{g(n)}{n^s} = \sum_{n=1}^{+\infty} \frac{h(n)}{n^s}.$$
其中 $h = f * g$.

5. Wintner 定理：假設 f 是數論函數，定義它的平均為 $M_x(f) = 1/x \sum_{n\le x} f(n)$。證明如果 $g = \mu * f$ 且 $\sum_{n=1}^{+\infty} g(n)/n$ 絕對收斂，那麼 $\lim_{x\to+\infty} M_x(f) = \sum_{n=1}^{+\infty} g(n)/n$.

6. 利用 Mőbius 函數 $\mu(n)$ 和 Riemann 函數 $\zeta(s)$ 求出任取正整數則取到無平方因數的整數的機率。

7. 建立關係式 (也要找出收斂座標的下界)：

$$\sum_{n=1}^{+\infty}\frac{\mu(n)}{n^s}=\frac{1}{\zeta(s)},\quad \sum_{n=1}^{+\infty}\frac{\phi(n)}{n^s}=\frac{\zeta(s-1)}{\zeta(s)}.$$

■ 第三部分 ■

為了估計一些常見數論函數的界，我們將在這個部分給出一些基本結果。

1. 記得 $\sum_{d|n}\Lambda(d)[n/d]=\log n!=n\log n-n+O(\log n)$，證明 $\sum_{d\leq x}\Lambda(d)/d=\log x+O(1)$.

2. 推導出 $\sum_{p\leq x}\log p/p=\log x+O(1)$.

3. 利用上式證明存在常數 a 使得 $\sum_{p\leq x}1/p=\log\log x+a+O(\frac{1}{\log x})$.

4. 再由 $e^{-1/p}(1-1/p)^{-1}=1+O(1/p^2)$ 證明存在常數 b 使得

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1}=b\log x+O(1).$$

從而它的倒數關係式成立：

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right)=\frac{1}{b\log x}\left(1+O\left(\frac{1}{\log x}\right)\right).$$

同時說明

$$\prod_{p\leq x}\left(1+\frac{1}{p}\right)=\frac{1}{\zeta(2)}\left(b\log x+O(1)\right).$$

■ 第四部分 ■

以下將給出 Euler ϕ 函數的一些性質來說明如何利用以上的估計式推論出不平凡的結果，注意本部分中每小題間並無太多關聯性。

1. 證明 $\phi(n)\gg n/\log\log n$.

2. 利用等式 $\phi=\mu*\mathrm{Id}$ 以及函數 $A(x)=\sum_{n\leq x}\phi(n)/n$ 證明

$$\sum_{n\leq x}\phi(n)=\frac{1}{2\zeta(2)}x^2+O\left(x\log x\right).$$

3. 欲研究集合 $(n/\phi(n))_{n\in\mathbb{N}}$ 的性質。證明

$$\sum_{p\text{ 是質數}}\log\left(1+\frac{1}{p-1}\right)$$

發散。注意到當 $p\to+\infty$ 時級數中的項 $\to 0$，我們可以對這個集合下怎樣的結論？

4. 考慮 Dirichlet 級數，證明

$$\sum_{n\le x}\frac{n}{\phi(n)}=\left(\prod_{p\text{是質數}}\left(1+\frac{1}{p(p-1)}\right)+o(1)\right)x.$$

並由此得出

$$\sum_{n\le x}\frac{1}{\phi(n)}=\left(\prod_{p\text{是質數}}\left(1+\frac{1}{p(p-1)}\right)+o(1)\right)\log x.$$

■ 第五部分 ■

中國數學家張益唐於 2013 年 4 月 17 日在數學年刊上發表了以下結果：

$$\liminf_{n\to+\infty}(p_{n+1}-p_n)<7\times10^7.$$

震驚了數學界，這是關於相鄰質數的上界所給出的一個估計。在這個部分裡，我們則是要對相鄰質數的下界做出限制，最後要證明的結果為 Erdős 在 1934 年做出的：存在正常數 c_1 使得對無窮多個正整數 n 有

$$p_{n+1}-p_n>\frac{c_1\log p_n\log\log p_n}{(\log\log\log p_n)^2}.$$

1. 試問從質數定理可以得到這樣的結果嗎？

2. 本題需要用到下一章介紹的 Brun 篩法，讀者可以暫時承認這個結果，之後再回來證明。令 m 是任意大於 1 的正整數，對正整數對 (x,y) 滿足 $1\le x<y<m$，以 N 記集合 $\{p\text{是質數}\mid p+1\text{不被任何質數}q\in[x,y]\text{所整除}\}$ 的大小，那麼

$$N<\frac{c_3m\log x}{\log m\log y}.$$

其中 c_3 是不取決於 m,x,y 的絕對常數。

3. 記 N_0 為不超過 $p_n\log p_n$ 的正整數中，最大質因數小於 $p_n^{1/20\log\log p_n}$ 者的個數。並記 N_1 為其中質因數個數不多於 $10\log\log p_n$ 者的個數，而 N_2 為其中質因數個數多於 $10\log\log p_n$ 者的個數，注意到有 $N_0=N_1+N_2$。

   (a) 直接估計得 $N_1=o(p_n/(\log p_n)^2)$.

   (b) 記 d 為因數個數函數，證明如果 n 是屬於 N_2 對應到集合的正整數，那麼 $d(n)>2^{10\log\log p_n}>(\log p_n)^5$。藉由估計 $\sum_{k\le x}d(k)$ 來證明 $N_2=o(p_n/(\log p_n)^2)$. 因此 $N_0=o(p_n/(\log p_n)^2)$.

4. 證明存在常數 c_4 使得 $\{p\text{是質數}\mid p\le c_4p_n\log p_n/(\log\log p_n)^2, p+1\text{不被任何質數}q\in[\log p_n,p_n^{1/20\log\log p_n}]\text{所整除}\}$ 的大小少於 $p_n/4\log p_n$.

接下來考慮以下集合

$$\begin{aligned} Q &= \{p \text{ 是質數} \mid 1 < p \le \log p_n\} \\ R &= \{p \text{ 是質數} \mid \log p_n < p \le p_n^{1/20 \log\log p_n}\} \\ S &= \{p \text{ 是質數} \mid p_n^{1/20 \log\log p_n} < p \le p_n/2\} \\ T &= \{p \text{ 是質數} \mid p_n/2 < p \le p_n\} \end{aligned}$$

而 A 是 $\{k \text{ 是正整數} \mid k \le p_n \log p_n, k \text{ 的所有質因數都在 } R \text{ 中}\}$ 和 $\{p \text{ 是質數} \mid p_n/2 < p \le c_4 p_n \log p_n/(\log\log p_n)^2, \text{ 對所有 } r \in R, p \text{ 不同餘於 } -1 \text{ 模 } r\}$ 的聯集。

5. 由上證明 $|A| \le |T|$.

因此，可以由中國剩餘定裡找到正整數 $z < p_1 \cdots p_n$ 滿足：

$$\begin{cases} z \equiv 0 \pmod{q} \\ z \equiv 1 \pmod{r} \\ z \equiv 0 \pmod{s} \\ z \equiv a_i \pmod{t_i} \end{cases}$$

其中 $(\text{mod } q)$ 表示該同餘式對於所有 $q \in Q$ 都成立，而 R, S 同理。最後 $\{a_1, \ldots, a_{|A|}\} = A$, $\{t_1, \ldots, t_{|T|}\} = T$.

6. 取 b 為小於 $c_4 p_n \log p_n/(\log\log p_n)^2$ 的某個正整數，證明 $z+b$ 和 $p_1 \cdots p_n$ 一定不互質。

7. (a) 令 x 為正實數，證明小於等於 x 的所有質數乘積小於等於 4^x.

   (b) 取 $x = \frac{1}{2}\log p_n$。由前幾題得到以下性質：存在正常數 c_5 使得可以找到全都小於 p_n 的連續 $K = c_5 \log p_n \log\log p_n/(\log\log\log p_n)^2$ 個正整數，他們都至少有一個小於 $\frac{1}{2}\log p_n$ 的質因數。因此我們知道存在 $K - \frac{1}{2}\log p_n > \frac{1}{2}K$ 個連續的正合數。

   (c) 由此推出 Erdős 的結果。

Chapter 10

分布密度

- 和集 sum set
- 篩法 sieve
- 緊緻 compact
- 階 order
- 測度 measure
- 連通 connected

給定一個正整數的集合 A，是否可能定義他在自然數集中的密度呢？進一步地，是否能在子集和子集間定義加法乘法等等的運算，使得他們滿除夠好的性質呢？這些問題，特別是在 $\mathbb{F}_p$ 上的運算，是組合數論最根本要處理的對象。在第一部分裡我們定義了 Schnirelmann 密度並證明 $d(A \oplus B) \geq \min\{d(A) + d(B), 1\}$，這個結果在有限體 $\mathbb{F}_p$ 上的版本又被稱作 Cauchy-Davenport 定理，最後在 1964 年，數學家 Kemperman 成功將他一般化：如果 G 是一個帶有 Haar 測度 μ 的緊緻連通群，那麼對於任意緊緻子集 A, B，總有 $\mu(AB) \geq \min\{\mu(A) + \mu(B), 1\}$.

我們還可以考慮一個集合在自然數集中的分布情況，這便是解析數論中篩法的範疇了。數論中所謂的篩法指的是這樣的一個過程：先給定一個正整數子集 A，接著對每個質數 p 都給出一個集合 A_p，裡面的元素都滿足某種特定的性質，而目的是估計出 $A \setminus (\cup A_p)$ 的大小。例如國中時大家都學過的 Eratosthenes 的質數篩法就是取 $A = \mathbb{N}$, $A_p = \{n \,|\, p \text{ 整除 } n\}$。

但是多數的數論問題研究的是同餘式之間的關係，Eratosthenes 的質數篩法顯然是不足的，我們需要考慮更一般的方法：給定正整數子集 $\mathcal{A}$，以及質數子集 $\mathcal{P}$，還有某個正實數 y。目的是要估計集合 $\mathcal{A}$ 中有多少元素不被小於等於 y 的質數所整除，也就是說要估計集合 $\mathcal{S}(\mathcal{A}, \mathcal{P}, y) = \{a \in \mathcal{A} \,|\, p \in \mathcal{P}, \gcd(a, p) > 1 \Rightarrow p > y\}$ 的大小。為了達成這個目標，對每個正整數 d，都定義如下的集合：$\mathcal{A}_d = \{a \in \mathcal{A} \,|\, d \text{ 整除 } a\}$，如果集合 $\mathcal{A}$ 裡的數在自然數中分布的夠均勻，那麼我們可以期待 $|\mathcal{A}_d| = |\mathcal{A}|/d$，但這並不總是如此，所以我們會寫成

$$|\mathcal{A}_d| = |\mathcal{A}| \cdot \frac{\rho(d)}{d} + R_d.$$

其中 $\rho(d)/d$ 表示取到集合 $\mathcal{A}_d$ 裡元素的機率，而 R_d 是誤差項。一般來說會要求 ρ 是個積性函數，因為當 m, n 互質時一個 $\mathcal{A}$ 裡的數能被正整數 m 整除和被正整數 n 整除應為兩個獨立事件。

現在可以合理的猜測大約會有

$$|\mathcal{S}(\mathcal{A},\mathcal{P},y)| \approx |\mathcal{A}| \cdot \prod_{p\in\mathcal{P},\, p\le y}\left(1-\frac{\rho(p)}{p}\right).$$

這是一個粗略的估計。由此想法出發可以有 Brun 組合篩法、Selberg 篩法、大篩法、小篩法等等，以及他們的各種形式。中國解析數論學家陳景潤在 1966 年證明了大偶數必可表為一個質數及一個不超過二個質數的乘積之和，又於 1978 年證明了存在無窮多個不超過二個質數乘積的正整數，減掉 2 後會是一個質數，這些都是篩法的重大里程碑。從第二個部分後我們將研究兩個篩法的一些應用。

■ 第一部分 ■

在這個部分裡要研究的是一個整數子集的密度，與自然密度不同，我們考慮如下的定義：一個非負整數子集 A 的 Schnirelmann 密度 $d(A)$ 為

$$d(A) = \inf_{n\ge 1}\frac{A(n)}{n}.$$

其中 $A(n)$ 為 A 中不超過 n 的正整數個數。而兩個非負整數子集 A, B 的和集 $A\oplus B$ 定義為 $A\oplus B = \{a+b \,|\, a\in A, b\in B\}$. 在接下來所有的部份中，考慮的非負整數子集都是包含 0 的集合。而我們試圖探討 $d(A), d(B)$ 和 $d(A\oplus B)$ 的關係。

固定正整數 g，分別以 A_1, B_1 記 A, B 中不超過 g 的元素形成的集合。假設可以找得到某個常數 $\theta\in(0,1]$ 使得：

$$A_1(m) + B_1(m) \ge \theta m, \quad \forall m = 1,2,\ldots,g.$$

我們的目的是要找出新的非負整數子集 A_2, B_2 使得以上不等式對於 A_2, B_2 仍成立，並且這兩個集合仍包含 0，$B_2(g) < B_1(g)$，而 $A_2\oplus B_2 \subseteq A_1\oplus B_1$.

1. 假設 $B_1 \not\subseteq A_1$，證明可以藉由取 $A_2 = A_1\cup B_1$, $B_2 = A_1\cap B_1$ 來達成目的。

2. 假設 $B_1\subseteq A_1$.

   (a) 證明集合 $\{a\in A \,|\, \exists b\in B,\, a+b\notin A\}$ 非空，假設 a_0 是這個集合的最小元素，證明 $a_0\neq 0$.

   (b) 假設 $B_1(g) > 0$，證明如果存在整數 z 與 B_1 中的元素 b 滿足 $z-a_0 < b \le z$，那麼對所有 $a\in A_1$ 滿足 $1\le a\le z-b$ 者，總有 $a+b\in A_1$。利用這個結論證明 $A_1(z)\ge A_1(b)+A_1(z-b)$.

   (c) 假設 $B_1(g)>0$，證明如果存在 $y\le g$ 使得 $A_1(y) < \theta y$，那麼 $y > a_0$.

   (d) 假設 $B_1(g)>0$，記 $B' = \{b\in B_1 \,|\, a_0+b\notin A_1\}$, $A' = \{a_0+b \,|\, b\in B',\, a_0+b\le g\}$。考慮 $A_2 = A_1\cup A'$, $B_2 = B_1\cap (B'^c)$，其中 B'^c 是 B' 在非負整數中的補集。證明這兩個集合仍包含 0，$B_2(g) < B_1(g)$，而 $A_2\oplus B_2\subseteq A_1\oplus B_1$.

(e) 證明 $A_2(m) = A_1(m) + A'(m)$, $B_2(m) = B_1(m) - B'(m)$, $A'(m) = B'(m - a_0)$。由此推出當 $B'(m) = B'(m - a_0)$ 時會有 $A_2(m) + B_2(m) \geq \theta m$.

(f) 當 $B'(m) < B'(m - a_0)$ 時，先證明 $B_1(m) = B_1(m - a_0) \geq B'(m) = B'(m - a_0) > 0$，並藉由考慮 B_1 中滿足 $m - a_0 < b_0 \leq m$ 的最小整數 b_0，來推導出仍有 $A_2(m) + B_2(m) \geq \theta m$ (提示：此時將有 $B_1(m - a_0) = B_1(b_0 - 1)$，而可在 (b) 中取 $z = m, b = b_0$).

(g) 總結以上結果。

(h) 利用上述結論，對 $B_1(g)$ 進行數學歸納法，證明 $(A_1 \oplus B_1)(g) \geq \theta g$.

(i) 證明選取 $\theta = \min(1, d(A) + d(B))$ 的合法性。我們能對 $d(A \oplus B)$ 給出怎樣的結論？

3. 對於正整數 n，以 nA 簡記集合 $A \oplus \cdots \oplus A(n \text{ 次})$。假設非負整數子集 A 具有正的 Schnirelmann 密度，證明存在正整數 m 使得 $mA = \mathbb{N} \cup \{0\}$.

■ 第二部分 ■

Gallagher 篩法是處理指數問題的重要工具之一：假設 B 是有限的正整數子集，T 是由質數及質數次方組成的有限集合。假設存在一個函數 $u(t)$ 使得 $|B \pmod t| \leq u(t)$ 對所有自然數 t 都成立，其中 $B \pmod t$ 指的是 B 中元素 $\bmod t$ 後形成的集合。

1. 引入 $Z(B, t, r)$ 表示 $|\{b \mid b \in B, b \equiv r \pmod t\}|$。證明以下等式列：

$$\frac{|B|^2}{u(t)} \leq \sum_{r \pmod t} (Z(B,t,r))^2 = \sum_{r \pmod t} \sum_{b,b' \equiv r \pmod t} 1 = |B| + \sum_{\substack{b \equiv b' \pmod t \\ b \neq b'}} 1.$$

2. 假設 $X \geq \max\{|b| \mid b \in B\}$，在上式中乘上 $\Lambda(t)$ 證明：

$$|B|^2 \sum_{t \in T} \frac{\Lambda(t)}{u(t)} \leq |B| \sum_{t \in T} \Lambda(t) + \log(2X)(|B|^2 - |B|).$$

由此說明在怎樣的條件下可以對集合 B 的大小給出怎樣的限制。

接下來考慮它的應用，以下以 $\delta_m(a)$ 記和 m 互質的整數 a 在模 m 下的階，記得重要的性質：若 p 為一奇質數，且 $a \neq \pm 1$ 不被 p 整除，設 $\delta_p(a) = d$，k_0 是使得 $a^d \equiv 1 \pmod{p^{k_0}}$ 成立的最大的正整數，則

$$\delta_{p^k}(a) = \begin{cases} d & , \quad k \leq k_0 \\ dp^{k-k_0} & , \quad k > k_0. \end{cases}$$

3. 這一小題要證明如下的定理：假設正整數 a, b 滿足對所有質數次方 q 都存在正整數 v_q 使得 $b \equiv a^{v_q} \pmod q$，那麼存在正整數 v 使得 $b = a^v$.

(a) 給定正整數 k,t，對正整數 G 定義 $S(G)=\{q=p^v \mid p$ 是質數, $k \mid \delta_q(t), \delta_q(t) \le G\}$。利用 Mőbius 反演公式證明 $\sum_{\delta_q(t)=g}\Lambda(q) \sim \phi(g)\log a$ $(g \to +\infty)$，並再由此推論出

$$\sum_{q\in S(G)} \Lambda(q) \gg G^2 \quad (G \to +\infty).$$

(b) 取 $B=\{n \le x \mid n=a^ib^j$ 對某兩個非負整數 $i,j\}$, $T=\{q \mid q$ 是質數次方, $\delta_q(a) \le y\}$，其中 x 是正整數，y 是一個 x 的函數。證明對任意 x，總可以找到 y 使得在 Gallagher 篩法中可估計出 $|B| \ll \log x$.

(c) 假設對所有正整數 m,n 總有 $a^m \ne b^n$，證明 $|B| \gg (\log x)^2$。由此推出存在正整數 i,j 使得 $a^i=b^j$.

(d) 取互質的正整數 i_0,j_0 使得 $a^{i_0}=b^{j_0}$，由此推得存在正整數 v 使得 $b=a^v$.

4. 假設正整數 $a,b \ne 1$ 滿足對所有正整數 n 都有 $a^n-1 \mid b^n-1$，證明存在正整數 v 使得 $b=a^v$.

5. 假設正整數 a,b 滿足對所有正整數 n 都有 $(a^n-1)(b^n-1)$ 是完全平方數，證明 $a=b$.

■ 第三部分 ■

以下繼續使用引文的符號 $\mathcal{S}(\mathcal{A},\mathcal{P},y)=\{a \in \mathcal{A} \mid p \in \mathcal{P}, \gcd(a,p)>1 \Rightarrow p>y\}$.

1. 考慮以下兩個數論裡的經典問題：

   - 給定正整數 m，我們想計算區間 $(m^2,(m+1)^2)$ 中有多少質數。考慮集合 $\mathcal{A}=\{n \in (m^2,(m+1)^2)\}$，$y=m+1$，$\mathcal{P}=\{$全體質數$\}$.
   - 給定正整數 x，我們想計算有多少形如 n^2+1 的質數，其中 $n \le x$。考慮集合 $\mathcal{A}=\{n^2+1 \mid n \le x\}$，$y=\sqrt{x^2+1} \sim x$，$\mathcal{P}=\{$全體質數$\}$.

   探討各個情況中 $\mathcal{A},\mathcal{P},y$ 選取的合理性 (注意第二個例子中 $|\mathcal{S}(\mathcal{A},\mathcal{P},y)|$ 並不直接是我們要算的數目，而在大多數情況都只能得到要算的數目的一個上界)，並且分別求出 $\mathcal{A}_d,\rho(d)$。最後給出 $|R_d|$ 的一個上界。

以下要討論 Brun 組合篩法的應用。在本文中我們都會取 $\mathcal{P}=\{$全體質數$\}$，而為方便以 $P(y)$ 表示所有小於等於 y 的質數乘積，$V(y)$ 表示 $\prod_{p\in\mathcal{P},\,p\le y}\left(1-\frac{\rho(p)}{p}\right)$.

2. 由排容原理可以得到等式

$$|\mathcal{S}(\mathcal{A},\mathcal{P},y)| = |\mathcal{A}| + \sum_{j\ge 1}(-1)^j \sum_{p_1<\cdots<p_j\le y} |\mathcal{A}_{p_1\cdots p_j}|.$$

試由此證明 Eratosthenes 篩法：

$$\sum_{\substack{d|P(y)\\ \omega(d)\le 2h+1}} \mu(d)|\mathcal{A}_d| \le |\mathcal{S}(\mathcal{A},\mathcal{P},y)| \le \sum_{\substack{d|P(y)\\ \omega(d)\le 2h}} \mu(d)|\mathcal{A}_d|.$$

其中 h 是任一正整數，而 $\omega(d)$ 表示正整數 d 的正因數個數。

3. 由上述不等式式得到

$$|\mathcal{S}(\mathcal{A},\mathcal{P},y)| = \sum_{\substack{d|P(y)\\ \omega(d)<r}} \mu(d)|\mathcal{A}_d| + O\left(\sum_{\substack{d|P(y)\\ \omega(d)=r}} |\mathcal{A}_d|\right).$$

接下來利用 $|\mathcal{A}_d| = |\mathcal{A}| \cdot \frac{\rho(d)}{d} + R_d$ 以及表達式 $V(y)$ 繼續證明出

$$|\mathcal{S}(\mathcal{A},\mathcal{P},y)| = |\mathcal{A}| \cdot V(y) + O\left(|\mathcal{A}| \cdot \sum_{\substack{d|P(y)\\ \omega(d)=r}} \frac{\rho(d)}{d} + \sum_{\substack{d|P(y)\\ \omega(d)\le r}} |R_d|\right).$$

4. 為方便暫時用 $g(d)$ 表示 $\rho(d)/d$。證明

$$\sum_{\substack{d|P(y)\\ \omega(d)=r}} g(d) = \frac{1}{r!}(\sum_{p<y} g(p))^r.$$

利用 Stirling 公式以及

$$\sum_{p<y} g(p) \le \sum_{p<y} \log\frac{1}{1-g(p)} = -\log V(y)$$

證明當 $r > 3.6\log|V(y)|$ 時會有估計式

$$|\mathcal{S}(\mathcal{A},\mathcal{P},y)| = |\mathcal{A}| \cdot V(y)\left(1 + O\left(\frac{1}{\sqrt{r}}\right)\right) + O\left(\sum_{\substack{d|P(y)\\ \omega(d)\le r}} |R_d|\right).$$

以上類似的結果及其變形是 Brun 的組合篩法。

利用將區間 $[1,y]$ 分割成更多小區間，然後在每個區間上對 $|\mathcal{S}(\mathcal{A},\mathcal{P},y)|$ 都做出限制，我們可以證明以下結果 (這裡直接承認其正確性)：

定理 10.1 (Brun 組合篩法) 假設存在某個值域為非負整數的數論積性函數 ρ，以及兩個正常數 κ, A 使得

$$\text{(i)}\quad |A_d| = |\mathcal{A}_d| \cdot \frac{\rho(d)}{d} + R_d \qquad (d \mid P(y)), \tag{10.1}$$

$$\text{(ii)}\quad \prod_{\eta \le p \le \xi} \left(1 - \frac{\rho(p)}{p}\right)^{-1} < \left(\frac{\log \xi}{\log \eta}\right)^{\kappa} \left(1 + \frac{A}{\log \eta}\right) \qquad (2 \le \eta \le \xi). \tag{10.2}$$

那麼可以有以下估計式 (其中大 O 符號不依賴於 $|\mathcal{A}|, y, u \ge 1$)：

$$|\mathcal{S}(\mathcal{A}, \mathcal{P}, y)| = |\mathcal{A}| \prod_{p \in \mathcal{P},\, p \le y} \left(1 - \frac{\rho(p)}{p}\right) \left(1 + O(u^{-\frac{u}{2}})\right) + O\left(\sum_{\substack{d \mid P(y) \\ d \le y^u}} |R_d|\right).$$

首先研究這個篩法在孿生質數問題上的應用，在這裡要證明的是 Brun 定理：構成孿生質數對的那些質數倒數和收斂，就此，我們仍然未知是否有無窮多對孿生質數對。先引進 $\mathcal{J}(x) = |\{n \le x \,|\, n, n+2 \text{都是質數}\}|$.

5. 考慮集合 $\mathcal{A} = \{n(n+2) \,|\, \le x\}$，$\mathcal{P} = \{\text{全體質數}\}$。證明對任意正實數 y 總有 $\mathcal{J}(x) \le \pi(y) + |\mathcal{S}(\mathcal{A}, \mathcal{P}, y)|$.

6. 取 $y = x^{\frac{1}{4}}, u = 1$，證明 $\mathcal{J}(x) \ll \frac{x}{(\log x)^2}$.

7. 利用等式
$$\mathcal{J}(n) - \mathcal{J}(n-1) = \begin{cases} 1 & , \text{ 如果 } n \text{ 和 } n+2 \text{ 都是質數} \\ 0 & , \text{ 其他情況} \end{cases}$$
證明 $\sum_{p, p+2 \text{都是質數}} \frac{1}{p}$ 收斂。

最後的目的是要研究 Goldbach 猜想。到這個部分結束之前，將以 $\mathfrak{T}(N)$ 表示集合 $\{p \,|\, N - p \text{是質數}\}$ 的大小，可以看做是將正整數 N 寫成兩個質數和的方法個數。

8. 考慮集合 $\mathcal{A} = \{m(N-m) \,|\, m \le N\}$，$y = N^{\frac{1}{3}}$，$\mathcal{P} = \{\text{全體質數}\}$。證明 $\mathfrak{T}(N) \le |\mathcal{S}(\mathcal{A}, \mathcal{P}, y)| + 2N^{\frac{1}{3}}$.

9. 在這個情況下該如何取函數 ρ？而對 R_d 的大小能給出什麼上界？利用結果及上述定理證明
$$\mathfrak{T}(N) \ll \frac{N}{(\log N)^2} \prod_{p \mid N} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right).$$

10. 假設 $\mathcal{Q}$ 是由 $0, 1$ 以及所有能寫成兩質數和的正整數所形成的集合，而以 $\mathcal{Q}(x)$ 表示集合 $\mathcal{Q} \cap \{1, 2, \ldots, x\}$。證明
$$\left(\sum_{n \le x} \mathfrak{T}(n)\right)^2 \le \left(\sum_{n \le x} \mathfrak{T}(n)^2\right) \times |\mathcal{Q}(x)|.$$

11. 假設 $x \geq 4$，證明會有
$$\sum_{n \leq x} \mathfrak{T}(n) \gg \frac{x^2}{(\log x)^2}.$$

12. 證明
$$\sum_{n \leq x} \mathfrak{T}(n)^2 \ll \frac{x^3}{(\log x)^4}.$$

13. 利用以上結果證明 $\mathcal{Q}$ 有正的 Schnirelmann 密度，因而存在正整數 c 使得 $c\mathcal{Q} = \mathbb{N} \cup \{0\}$。

14. 對於任一正整數 $m \geq 2$，已知 $m - 2 \in c\mathcal{Q}$，證明 m 可以寫成至多 $2c$ 個質數之和。

最後做一個註解。以上的 Mann 定理 (第一部分所證明)，也可以用在證明 Waring 問題：對任意正整數 k，總存在正整數 $g(k)$ 使得所有正整數均可以寫為至多 $g(k)$ 個 k 次方數之和。這個證明稍微複雜，用到的想法是第 13 章將介紹的三角和，只是詳細的過程不在本文介紹的性質內。而數學家 Erdős 運用 Mann 定理則宣稱了他證明了以下性質：對任意正整數 k，總存在正整數 $e(k)$ 使得所有正整數均可以寫為至多 $e(k)$ 個質數的 k 次方之和或差。這實在太誇張了。

Chapter 11

Diophantine 逼近

本章到第二部分為止取自巴黎高等師範學院考題 (http://concours-maths-cpge.fr/)。

- 純量積 scalar product
- 基本解 the fundamental unit
- 連分數 continued fractions
- 代數數 algebraic number
- 超越數 transcendental number
- 光滑數 smooth number

所謂的 Diophantine 逼近是為了解 Diophantine 方程所發展出的方法，一個經典的例子就是以有裡數去逼近一個無理數。比方說大家都看過的：$355/113 \approx \pi$ 就是一個“好”的有理逼近，因為把 355/113 的分母換成比 113 還小的自然數時，都找不到分數比它更接近 π。而這部分的研究在 18 世紀數學家發展出連分數的方法後開始有了許多成果。

其後，該領域的主要注意力轉向對有理逼近的誤差進行估計、度量，以給出儘可能精確的上下界。當處理的數分別為有理數、代數數、超越數時，其最佳逼近誤差下界的階是不同的。基於這種思想，Liouville 在 1844 年建立了有關代數數逼近的一個基本結論，並由此具體地構造出了一個超越數，證明了它的超越性。由此可見，Diophantine 逼近與數論的另一分支——超越數論緊密相關。而除了上述最經典的單個實數的有理逼近問題，該領域還包括多個實數的聯立逼近、非齊次逼近、實數的代數數逼近、還有第七章節將會介紹的均勻分布等方面。

定理 11.1 (Thue-Siegel-Roth 界) 給定代數數 α，僅存在有限多個有理數 p/q 滿足

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\kappa}.$$

另一個等價敘述是說，存在某個常數 $c = c(\alpha) > 0$，使得對所有有理數 p/q，都有

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^\kappa}.$$

其中 κ 的值一直被數學家下修 (以下 $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$)：

κ	contributor
$\kappa = n$	Liouville, 1844
$\kappa = (n+1)/2 + \epsilon$	Thue, 1909
$\kappa = n/s + s - 1 + \epsilon$	Siegel, 1921
$\kappa = \sqrt{2n} + \epsilon$	Dyson, Gel'fond, 1947
$\kappa = 2 + \epsilon$	Roth, 1955

■ 第一部分 ■

在接下來所有的問題中，我們以 $\{\theta\} = \theta - [\theta]$ 記實數 θ 的小數部份。而在第一部份中，以 $||\theta||$ 記 $\min(\{\theta\}, 1 - \{\theta\})$.

1. (a) 假設 θ 和 Q 是兩個實數，我們考慮接下來的兩個集合：

$$A = \{q \in (0, Q) \cap \mathbb{N} \,|\, ||q\theta|| \leq Q^{-1}\}.$$

$$B = \{q \in (0, Q) \cap \mathbb{N} \,|\, ||q\theta|| < Q^{-1}\}.$$

試問 A 可以是空集合嗎？而 B 呢？

(b) 關於未知數為 $q \in \mathbb{N}$ 的不等式 $q||q\theta|| < 1$，我們可以對它的解數下怎樣的結論？

2. 假設 θ 是一個無理數。

(a) 證明存在整數無窮數列 (p_n) 和 (q_n) 滿足以下條件：

i. $q_1 = 1$ 且 (q_n) 嚴格遞增。

ii. 對所有正整數 n，有 $||q_n\theta|| = |q_n\theta - p_n|$.

iii. 數列 $(||q_n\theta||)$ 是嚴格遞減的。

iv. 對所有正整數 n 和所有正整數 q 滿足 $0 < q < q_{n+1}$，總有 $||q\theta|| \geq ||q_n\theta||$.

而由以上四條性質所定義出來的數列 (p_n) 和 (q_n) 是唯一的嗎？

(b) 如果 θ 是一個有理數，應該如何修改以上性質？

3. 假設 θ 是一個無理數，而數列 (p_n) 和 (q_n) 是在 (2) 中構造的數列。

(a) 證明以下性質：

i. 對所有正整數 n，有 $|\theta - \frac{p_n}{q_n}| \leq (q_n q_{n+1})^{-1}$.

ii. 如果 $0 < \theta < 1$，那麼不等式 $0 \leq p_n \leq q_n$ 對所有正整數 n 都成立。

(b) 試研究 $(q_n\theta - p_n)(q_{n+1}\theta - p_{n+1})$ 的正負號。

(c) 從 (b) 小題的結論找出 $q_{n+1}p_n - q_n p_{n+1}$ 和 $q_{n+1}||q_n\theta|| + q_n||q_{n+1}\theta||$ 的值。

(d) 證明對所有正整數 $n \leq 2$，都存在正整數 a_n 滿足：

i. $q_{n+1} = a_n q_n + q_{n-1}$ 以及 $p_{n+1} = a_n p_n + p_{n-1}$.

ii. 計算 $|q_{n-1}\theta - p_{n-1}| - |q_{n+1}\theta - p_{n+1}|$.

4. 假設 θ 是一個在 $(0,1)$ 區間的無理數，而數列 (u_n), (v_n) 和 (α_n) 是由以下方式構造的數列：

(a) $u_0 = v_1 = 1$, $u_1 = v_0 = 0$.

(b) 假設對於所有 $0 \le k \le n$，u_k 和 v_k 都已構造好，那麼定義

$$\alpha_n = \left[\frac{|v_{n-1}\theta - u_{n-1}|}{|v_n\theta - u_n|}\right].$$

(c) $u_{n+1} = \alpha_n u_n + u_{n-1}$, $v_{n+1} = \alpha_n v_n + v_{n-1}$.

試藉由分別討論 $0 < \theta < \frac{1}{2}$ 和 $\frac{1}{2} < \theta < 1$ 的情形，以及 3.(d).ii. 不等式的幫助，比較數列 (u_n), (v_n) 和 (p_n), (q_n)。

計算 $v_{n+1}u_n - v_n u_{n+1}$ 的值，並和 3.(c) 的結果作比較。

■ 第二部分 ■

下面以 $S^{n-1} = \{x = (x_1, \ldots, x_n) \in \mathbb{R}^n \,|\, x_1^2 + \cdots + x_n^2 = 1\}$ 記 n 維空間的單位球面，然後 $x \cdot y = \sum_{k=1}^n x_k y_k$ 表示向量 $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ 的純量積，並以 $|x| = (x \cdot x)^{\frac{1}{2}}$ 代表向量的長度。

1. 對正整數 n，實數 C 以及正實數 s，記

$$D(n, s, C) = \{\omega \in S^{n-1} \,|\, \forall k \in \mathbb{Z}^n \setminus \{0\},\ |\omega \cdot k| \ge C|k|^{-s}\}.$$

(a) 當 $n = 2$ 時：試提出集合 $O_k = \{\omega \in S^1 \,|\, |\omega \cdot k| < C|k|^{-s}\}$ 的幾何解釋，並由此推出對所有 $s > 1$，總存在正常數 $C(s)$ 使得對所有 $0 \le C \le C(s)$，集合 $D(2, s, C)$ 都是非空的 (提示：研究 $\sup_{A \ge 0} \sum_{k \in \mathbb{Z}^2 \setminus \{0\}, |k| \le A} |k|^{-s-1}$ 的值)。

(b) 當 $n \ge 3$ 時：證明對所有 $s > n - 1$，總存在正常數 $C(s)$ 使得對所有 $0 \le C \le C(s)$，集合 $D(n, s, C)$ 都是非空的。

我們說 θ 是一個次數為 d 的代數數當且僅當它是某個次數為 d 且不可約的有理係數多項式的根。

2. 假設無理實數 θ 是一個次數為 d 的代數數，證明存在正數 A 使得對所有 $p \in \mathbb{Z}$ 和 $q \in \mathbb{Z} \setminus \{0\}$ 都有

$$\left|\theta - \frac{p}{q}\right| \ge \frac{A}{|q|^d}.$$

(提示：假設 P 是以 θ 為根的不可約的有理係數多項式，考慮 $P(p/q)$ 的值並使用 Rolle 定理。)

3. 用 2. 的結論，試利用某個無窮級數和構造出非代數數的實數。

4. 試問對所有 C，集合 $D(2,1,C)$ 總是空的嗎？

5. 接下來的部分要證明 Minkowski 定理：假設 S 是 $\mathbb{R}^n$ 中的凸集，在 $-\mathrm{Id}_{\mathbb{R}^n}$ 的作用下是不變的，而且體積大於 2^n，那麼它至少包含除了原點以外的另一個格子點，也就是座標為整數的點。

   (a) 假設 S' 是一個 $\mathbb{R}^n$ 中體積大於 1 的點集，證明可以找到 S' 中兩點 v_1, v_2 使得 $v_1 - v_2 \in \mathbb{Z}^n$. (提示：可以僅處理 S' 是有界的情況，而此時考慮平移 $S' + \alpha$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$, $\max(\alpha_1, \ldots, \alpha_n) \le p$, 其中 p 是正整數。)

   (b) 利用以上結論證明 Minkowski 定理。

6. 最後我們想證明如果 $s < 1$，那麼對所有正實數 C，集合 $D(2,s,C)$ 都是空的。
   現在固定 $\omega = (\omega_1, \omega_2) \in S_1$，且 $\omega_2 \neq 0$。假設 α, Z 是兩個大於 1 的正實數，考慮集合：
   $$R(Z,\alpha) = \{k = (k_1,k_2) \in \mathbb{R}^2 \,|\, |k_1| \le \alpha Z,\ \left|\frac{\omega_1}{\omega_2}k_1 + k_2\right| \le Z^{-1}\}.$$

   (a) 給出 $R(Z,\alpha)$ 的幾何解釋，並計算它的面積。

   (b) 推導出如果 $s < 1$，那麼對所有正實數 C，集合 $D(2,s,C)$ 都是空的。

7. 證明對 $n \ge 3$，如果 $s < n-1$，那麼對所有正實數 C，集合 $D(n,s,C)$ 都是空的。

■ 第三部分 ■

這個部分要研究的是 Pell 方程解的性質。所謂的 Pell 方程指的是關於 (x,y) 的整係數方程式 $ax^2 - by^2 = c$，而簡單的運算告訴我們這其實只須研究 $a = 1$ 且 $b > 0, c \neq 0$ 且 b 也不是平方數的情況。在前幾個問題中，我們討論 $x^2 - dy^2 = 1$ 的正整數對解。

1. 假設 d 是一個非平方數的正整數，利用第一部分第 (3) 小題 (a) 的結果證明：存在正整數 $k < 1 + 2\sqrt{d}$ 使得 $x^2 - dy^2 = k$ 有無窮多組正整數對解 (x,y).

2. 如果 (x_1,y_1) 和 (x_2,y_2) 是上一題的兩組解，滿足 $k \mid x_1 - x_2$ 且 $k \mid y_1 - y_2$，那麼
   $$x = \frac{x_1x_2 - dy_1y_2}{k}, \qquad y = \frac{x_1y_2 - y_1x_2}{k}$$
   就會是 $x^2 - dy^2 = 1$ 的一組整數對解 (x,y)。由此證明 $x^2 - dy^2 = 1$ 有無窮多對正整數對解。

3. 現在我們想討論這些解的性質。定義 $\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} \mid (x,y) \in \mathbb{Z}^2\}$，在這個集合定義函數 $\overline{x + y\sqrt{d}} = x - y\sqrt{d}$ 以及 $N(x + y\sqrt{d}) = x^2 - dy^2$。證明 $\mathbb{Z}[\sqrt{d}]$ 是一個環，而對於 $z_1 = x_1 + y_1\sqrt{d}, z_2 = x_2 + y_2\sqrt{d}$ 總有 $\overline{z_1z_2} = \overline{z_1}\cdot\overline{z_2}$ 和 $N(z_1z_2) = N(z_1)N(z_2)$.

4. 證明存在 $z_0 = x_0 + y_0\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ 滿足

(a) $(x_0, y_0) \in \mathbb{N}^2$.

(b) $N(z_0) = 1$.

(c) 對所有 $z = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ 滿足 $(x, y) \in \mathbb{N}^2$, $N(z) = 1$ 者，都有 $x_0 < x$ 且 $y_0 < y$.

我們稱 z_0 為 Pell 方程 $x^2 - dy^2 = 1$ 的基本解，或是 $\mathbb{Z}[\sqrt{d}]$ 的基本解。

5. 利用 $z_0 > 1$ 以及函數 N，證明如果 (x, y) 是 $x^2 - dy^2 = 1$ 的一組正整數對解，那麼存在正整數 n 使得 $x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^n$。也就是說所有解都被基本解生成。

6. 現在開始研究一般 Pell 方程

$$x^2 - dy^2 = C \tag{11.1}$$

其中 d 是一個非平方的正整數而 C 為非零整數。證明如果 (x, y) 是方程 (3) 的整數解，且 $z_0 = x_0 + y_0\sqrt{d}$ 是 $x^2 - dy^2 = 1$ 的基本解，那麼對任意正整數 n，滿足 $x_n + y_n\sqrt{d} = (x + y\sqrt{d})(x_0 + y_0\sqrt{d})^n$ 的整數對 (x_n, y_n) 都會是方程 (3) 的整數解。

7. 利用上題，證明如果在 $\mathbb{Z}^2$ 上定義等價關係：$(u, v) \sim (u', v')$ 當且僅當

$$u'' = \frac{uu' - dvv'}{C}, \quad v'' = \frac{uv' - vu'}{C}$$

都是整數。那麼對所有整數對 (x, y)，(x, y) 是方程 (3) 的整數對解當且僅當任意與他在同一個等價類的整數對也是方程 (3) 的整數對解。

8. 由此得出：若 z_0 是 $\mathbb{Z}[\sqrt{d}]$ 的基本解。則存在有限個數 $z_1, z_2, \ldots, z_m \in \mathbb{Z}[\sqrt{d}]$，使得對所有 $z \in \mathbb{Z}[\sqrt{d}]$ 滿足 $N(z) = C$ 者，必有某整數 n, i 及適當正負號使 $z = \pm z_i z_0^n$。這些數 $z_1, z_2, \ldots, z_m$ 仍被稱為基本解。這個結論很重要。

9. 利用上上題定義的等價關係證明如果 $z = x + y\sqrt{d}$ 是方程 (3) 的一組基本解，而 $z_0 = x_0 + y_0\sqrt{d}$ 是 $\mathbb{Z}[\sqrt{d}]$ 的基本解，那麼我們可以給出限制：

$$0 \le |x| \le \frac{y_0}{\sqrt{2(x_0 + 1)}}\sqrt{|C|}, \quad 0 < |y| \le \sqrt{\frac{1}{2}(x_0 + 1)}\sqrt{|C|}.$$

(可以依序討論 C 的正負號。)

10. 如果 D 是一個模 4 同餘 0 或 1 的非平方正整數。證明解 $x^2 - Dy^2 = 1$ 和解 $x^2 - Dy^2 = 4$ 是一樣的。

■ 第四部分 ■

這個部分前 5 題取自筆者的專題研究，目的在於研究一些光滑數的性質。給定正整數 y，我們說正整數 n 是一個 y-光滑數當且僅當 n 的所有質因數都不超過 y，注意到 1 也是光滑數。以下給定一個正整數 $y \ge 2$，並考慮所有 y-光滑數形成的集合 $\{a_1, a_2, \ldots\}$，其中元素由小排到大。我們承認以下定理：

定理 11.2 (Baker's theorem) 令 $\alpha_1, \ldots, \alpha_n$ 是非零的代數數，次數與高 (指代數數 α 的極小多項式變成整係數多項式後係數絕對值最大者) 分別不超過 d 和 H。假設說有整數 $b_1, \ldots, b_n$，其中絕對值最大者為 T，滿足

$$0 < |b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| < e^{-\delta T}.$$

其中 $0 < \delta < 1$。那麼

$$T < (4^{n^2} \delta^{-1} d^{2n} \log H)^{(2n+1)^2}.$$

1. 利用 Baker 不等式證明對所有 $n \geq 2$ 總有

$$a_{n+1} - a_n \geq \frac{\exp\left(-(16r)^{2(r+2)}\Pi\right) a_n}{(\log 2a_n)^{(16r)^{2(r+2)}\Pi}}$$

其中 $r = \pi(y)$ 且 $\Pi = \prod_{2<p\leq y} \log p$.

2. 證明以 (a, b) 為未知數的 y-光滑數方程式 $a - b = k$ 的解數

$$\leq \frac{\left(\log k + \theta(y) + (16r)^{2(r+2)}\Pi\right)^r}{r!(\log 2)\Pi} \exp\left(\frac{(16r)^{2r+5}}{8}(\log 2)\Pi\right).$$

當 $k \to +\infty$，這個數目 $\asymp (\log k)^r$.

3. 假設 $f : \mathbb{N} \to \mathbb{N}$ 是嚴格遞增函數，且存在 $\epsilon > 0$ 使得 $f(n) \leq \exp(n^{\frac{1}{2r+\epsilon}})$。證明存在無窮多個正整數 k 使得以 (a, b) 為未知數的 y-光滑數方程式 $a - b = f(k)$ 無解。

4. 如果 x 是正實數，記 $\Psi(x, y)$ 為小於等於 x 的 y-光滑數的個數。藉由一個幾何論證給出 $\Psi(x, y)$ 的上下界，並推得

$$\exp\left(\left(n\pi(y)! \prod_{p\leq y} \log p\right)^{\frac{1}{\pi(y)}} - \theta(y)\right) \leq a_n \leq \exp\left(\left(n\pi(y)! \prod_{p\leq y} \log p\right)^{\frac{1}{\pi(y)}}\right).$$

5. 對一個正整數數列 $(u_n)_{n\in\mathbb{N}}$，以 $\mathbb{P}((u_n))$ 記他的質因數集，也就是說 $\mathbb{P}((u_n)) = \{p$ 為質數 $\mid$ 存在 $n \in \mathbb{N}$ 使得 p 整除 $a_n\}$。

假設 $(u_n)_{n\in\mathbb{N}}$ 是使得 $\mathbb{P}((u_n))$ 是有限集的一個嚴格遞增的正整數數列。現取一函數 $f : \mathbb{N} \to \mathbb{Z}$，假設它滿足：$\forall \epsilon > 0$，不等式 $0 < |f(n)| \leq \exp(n^\epsilon)$ 對無窮多個 n 成立。證明 $\mathbb{P}((u_n + f(n)))$ 是無限集。

6. 定義數論函數 $\mho$：如果 $n = \prod_i p_i^{\alpha_i}$ 是 n 的質因數分解式，那麼 $\mho(n) = \sum_{i:\ p_i > 10^{100}} \alpha_i$。試求出所有從 $\mathbb{N}$ 到 $\mathbb{N}$ 且滿足

$$\mho(f(a) - f(b)) \leq \mho(a - b) \text{ 對所有正整數 } a > b$$

的嚴格遞增函數 f.

做幾個註解。第 2. 小題中 $k=1$ 的情況又被稱作 Størmer 問題，這是由挪威數學家 Carl Størmer 在 1897 年首先研究的，他的方法需要解 $3^{\pi(y)}-2^{\pi(y)}$ 個 Pell 方程，後來 Lehmer D. H. 於 1964 年給出了只需解 $2^{\pi(y)}-1$ 個 Pell 方程的一個較簡單的手法。由後者的想法出發，筆者證明了方程 $a-b=k$ 的最大解滿足

$$b \leq \frac{k}{2}\exp\left[\left(\frac{p_{\pi(y)}^3}{c_2(y,k)}+1\right)\left(1+2\log\prod_{p\leq y}p\right)\prod_{p\leq y}p\right].$$

其中 $c_2(y,k)$ 是取決於 y,k 的可計算常數。而如果 $c_2(y,k)\asymp 1$，我們將得到一個比第 1. 小題給出的界要好得多的結果，但問題在於如何給出 $c_2(y,k)$ 的下界。另外第 5. 小題中 f 為常數函數又被稱為 Kobayashi 定理，在原始論文中作者給出的是用代數數論的作法。

Chapter 12

Dirichlet 特徵

本章到第三部分為止取自巴黎高等師範學院考題。

- 群 group
- 特徵 character
- 延拓 extend
- 原根 primitive root
- 群表示 group representation
- 單射 injective
- 體 field
- 同態映射 homomorphism

在交換環 $\mathbb{Z}/N\mathbb{Z}$ 的可逆元上的一個完全積性函數 χ 稱為一個 Dirichlet 特徵，可以自然地把它延拓成定義域為正整數的一個週期函數，而進一步考慮如第一章節所介紹的 Dirichlet L-級數：

$$L(s,\chi)=\sum_{n=1}^{+\infty}\frac{\chi(n)}{n^s}.$$

這些是 Dirichlet 在 1831 年為了證明他著名的算術定裡所引入的。

可以看出 Dirichlet 特徵是群表示的一個特殊例子，所以可以考慮正交關係，Fourier 級數等等作為分析的工具。而正如在群表示理論中所學到的，知道 Dirichlet 特徵的數目，或是其他一些性質，可以幫助了解 $\mathbb{Z}/N\mathbb{Z}$ 的結構，這在第四、五部分將會看到。

■ 預備知識 ■

1. 使用如下的 Abel 求和公式：假設 (u_k) 及 (v_k) 是兩個複數數列，我們以 U_n 表示 (u_k) 的前 n 項和，那麼：

$$\sum_{k=1}^{n}u_kv_k=U_nv_n+\sum_{k=1}^{n-1}U_k(v_k-v_{k+1}).$$

2. Mőbius 反演公式。假設 H 是一個值域在複數裡的數論積性函數。另有兩個函數 $F,G:[1,+\infty)\to\mathbb{C}$ 滿足

$$G(x)=\sum_{1\le k\le x}F\big(\frac{x}{k}\big)H(k)\quad\forall x\in[1,+\infty).$$

那麼他們也滿足以下關係：

$$F(x)=\sum_{1\le k\le x}\mu(k)G\big(\frac{x}{k}\big)H(k)\quad\forall x\in[1,+\infty).$$

■ 第一部分 ■

從現在開始到第三部分為止，N 是一個給定的正整數，在接下來的問題中是不會改變的。以 $G(N)$ 表示環 $\mathbb{Z}/N\mathbb{Z}$ 中可逆元所形成的乘法群。

假設 G 是一個有限且可交換的乘法群，我們稱從 G 打到乘法群 $\mathbb{C}^\times$ 的同態映射為一個特徵。假設 χ 和 χ' 為 G 上的兩個特徵，我們定義他們的乘積為 $\chi\chi'(g)=\chi(g)\chi'(g)$ $\forall g\in G$，那麼這仍為一個特徵。接下來以 ε 記所有元素都打到 1 的特徵 (又稱為平凡特徵)，$\widehat{G}$ 為 G 中所有特徵所形成的集合 (可知其為一個群)，而 $\widehat{\widehat{G}}$ 為 $\widehat{G}$ 中所有特徵所形成的集合。最後記 $\overline{\chi}$ 為 $\overline{\chi}(g)=\overline{\chi(g)}$ $\forall g\in G$ 的那個特徵。

對所有 $z\in G$，考慮 $\phi_x\in\widehat{\widehat{G}}$，定義為 $\phi_x:\widehat{G}\to\mathbb{C}^\times$, $\phi_x(\chi)=\chi(x)$。我們的目的是要證明映射 $G\to\widehat{\widehat{G}}$, $x\mapsto\phi_x$ 是單射的。

1. 記 $\langle x\rangle$ 是以 x 生成的群。假設 $x\in G$, $x\neq 1$，證明存在某個 $\langle x\rangle$ 上的特徵 χ 使得 $\chi(x)\neq 1$.

2. 假設 F 是由所有這個特徵 χ 所能延拓定義到的子群所形成的集合 (即是說子群 $H\in F$ 當且僅當 $\langle x\rangle\subseteq H$, 且 $\chi_H|_{\langle x\rangle}=\chi$)，證明 F 中存在元素個數最多的子群 G'。接下來假設 $G'\neq G$，那麼任取 $y\in G\backslash G'$，藉由考慮最小的正整數 n 使得 $y^n\in G$ (我們先討論這個 n 存在的情況)，證明 χ 能延拓定義到包含 y, G' 的子群上，導出矛盾。

3. 證明即使上述的 n 不存在，仍能導出矛盾。至此，我們知道有 $G'=G$.

4. 假設 $\chi'\in G, x\in G$，考慮以下兩個和：

$$\sum_{\chi\in\widehat{G}}\chi(x)\ \text{與}\ \sum_{\chi\in\widehat{G}}\chi\chi'(x).$$

藉由選取足夠好的 χ' 證明以下公式：

$$\sum_{\chi\in\widehat{G}}\chi(x)=\begin{cases}0 & ,\ \text{如果}\, x\neq 1\\ |\widehat{G}| & ,\ \text{如果}\, x=1.\end{cases}$$

$$\sum_{x\in G}\chi(x)=\begin{cases}0 & ,\ \text{如果}\,\chi\neq\varepsilon\\ |G| & ,\ \text{如果}\,\chi=\varepsilon.\end{cases}$$

5. 考慮 $\sum_{x,\chi}\chi(x)$，證明 $|G|=|\widehat{G}|$。現在我們可以對映射 $G\to\widehat{\widehat{G}}$ 得到什麼樣的結論？

■ 第二部分 ■

從現在開始，特徵都是指 $G(N)$ 上的特徵，而我們試圖將他們的定義延拓到整數集上。

1. 假設 χ 是一個非平凡特徵，證明可以定義：
$$\chi(m) = \begin{cases} \chi(m \pmod N) & , \text{ 如果 } m, N \text{ 互質} \\ 0 & , \text{ 如果 } m, N \text{ 不互質}. \end{cases}$$
並且在這個定義下，還會有 $\chi(ab) = \chi(a)\chi(b)$ 對所有整數 a, b. (對於平凡特徵，我們會定義為 $\varepsilon(n) = 1$，對所有整數 n，注意其特殊性。)

2. 假設 χ 是一個非平凡特徵，證明
$$\sum_{n\geq 1} \frac{\chi(n)}{n} \text{ 與 } \sum_{n\geq 1} \frac{\chi(n)\log n}{n}$$
都是收斂的，並分別記 $L(\chi)$ 與 $L_1(\chi)$ 為收斂值。

接下來到這個部分結束前，符號 χ 表示一個非平凡且值域在實數裡的特徵。

3. 假設 $f(n) = \sum_{d|n} \chi(d)$。證明當 n, m 互質時有 $f(mn) = f(m)f(n)$。由此而得出 $f(n) \geq 0$ 對所有正整數 n，並且 n 是平方數時還有 $f(n) \geq 1$.
假設對所有正實數 x 定義 $g(x) = \sum_{n\leq x} \frac{f(n)}{\sqrt{n}}$，那麼 $g(x)$ 在 $+\infty$ 的附近會有怎樣的成長趨勢？

4. 嚴謹地證明以下等式：
$$g(x) = \sum_{d'\leq x} \frac{1}{\sqrt{d'}} \sum_{\sqrt{x}<d\leq \frac{x}{d'}} \frac{\chi(d)}{\sqrt{d}} + \sum_{d\leq\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{d'\leq \frac{x}{d}} \frac{1}{\sqrt{d'}}.$$
接下來藉由估計當中這兩個和的下界，證明 $g(x) - 2\sqrt{x}L(\chi)$ 是有界的。

5. 證明在這情況下 $L(\chi)$ 是非零的。

■ 第三部分 ■

在這個部分中，χ 將表示非平凡的特徵 (值域在複數裡)。記得估計式 $\sum_{p\leq x} \log p/p = \log x + O(1)$.

1. 令 $G(x) = \sum_{n\leq x} \frac{x}{n}\chi(n)$. 證明 $G(x) - xL(\chi)$ 是有界的。現在進一步假設 $L(\chi) \neq 0$，利用 Mőbius 反演證明 $G(x) = \sum_{n\leq x} \frac{\mu(n)\chi(n)}{n}$ 也是有界的。

2. 另一方面，假設 $L(\chi) = 0$，那麼令 $G_1(x) = \sum_{n\leq x} \left(\frac{x}{n}\log\frac{x}{n}\right)\chi(n)$. 證明 $G_1(x) = -xL_1(\chi) + O(\log x)$. 和上一小題一樣，證明函數
$$x \mapsto L_1(\chi) \sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} + \log x$$
也是有界的。

3. 利用以上的結論來證明以下等式：

$$L_1(\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n}=\sum_{p\le x}\frac{\chi(p)\log p}{p}+O(1).$$

並由此推得

$$\sum_{p\le x}\frac{\chi(p)\log p}{p}=\begin{cases}O(1) & ,\ \text{如果 } L(\chi)\neq 0\\ -\log x+O(1) & ,\ \text{如果 } L(\chi)=0.\end{cases}$$

4. 記 T 為使得 $L(\chi)=0$ 的非平凡的特徵的個數，藉由考慮和

$$\sum_{\chi\in G(N)}\sum_{p\le x}\frac{\chi(p)\log p}{p}$$

來證明出估計

$$|G(N)|\sum_{\substack{p\le x\\ p\equiv 1 \pmod N}}\frac{\log p}{p}=(1-T)\log x+O(1).$$

由此可以得到 $T\le 1$.

5. 分別考慮 χ 的值域為實數及複數的情況，證明 T 等於零。

6. 假設 l 是一個和 N 互質的整數，考慮和

$$\sum_{\chi\in G(N)}\sum_{p\le x}\overline{\chi}(l)\frac{\chi(p)\log p}{p}$$

證明同餘 l 模 N 的質數有無窮多個。

■ 第四部分 ■

接下來的目的是要研究在環 $\mathbb{Z}/N\mathbb{Z}$ 中指數方程式 $a_1x_1^{k_1}+\cdots+a_rx_r^{k_r}=b$ 的解數。為了簡化問題，我們在一開始只研究 $N=p$ 是一個質數的情形，這時候以 $\mathbb{F}_p$ 簡記 $\mathbb{Z}/N\mathbb{Z}$，注意他是一個體。以下將以 $N(\text{方程式})$ 表示某一方程式在 $\mathbb{F}_p$ 的解數。

1. 求出 $|\widehat{(\mathbb{F}_p^\times)}|$.

2. 對於模 p 的特徵 χ，可以引入 Gauss 和定義為：

$$G(n,\chi)=\sum_{t=0}^{p-1}\chi(t)e^{2i\pi\frac{tn}{p}},\quad n\text{為整數.}$$

以 $\tau(\chi)$ 簡記 $G(1,\chi)$。證明 $\tau(\varepsilon)=0$ 以及當 $\chi\neq\varepsilon$ 時會有 $\tau(\chi)\tau(\overline{\chi})=\chi(-1)p$.

3. 證明當 $\chi\neq\varepsilon$ 時有 $\tau(\overline{\chi})=\chi(-1)\overline{\tau(\chi)}$，所以 $|\tau(\chi)|=\sqrt{p}$.

4. 承認原根的存在性，證明 $N(x^k=b)=N(x^{\gcd(k,p-1)}=b)$。之後到第 8. 題為止都假設對所有 i 有 $k_i\mid p-1$，試在做完第 8. 題後佐證這個假設的合理性。

5. 如果 $k \mid p-1$，證明 $\sum_{\chi^k=\varepsilon} \chi(b) = N(x^k = b)$.

6. 證明

$$N(a_1x_1^{k_1} + \cdots + a_rx_r^{k_r} = b) = \sum_{\vec{\chi}:\chi_i^{k_i}=\varepsilon} \chi_1(a_1^{-1}) \cdots \chi_r(a_r^{-1}) \sum_{\vec{b}:\sum b_i=b} \chi_1(b_1) \cdots \chi_r(b_r).$$

為簡化，引入 Jacobi 和：假設 $\chi_1, \ldots, \chi_r$ 是模 p 的 r 個特徵，那麼他們的 Jacobi 和定義為

$$J_0(\chi_1, \ldots, \chi_r) = \sum_{\vec{b}:\sum b_i=0} \chi_1(b_1) \cdots \chi_r(b_r),$$

$$J(\chi_1, \ldots, \chi_r) = \sum_{\vec{b}:\sum b_i=1} \chi_1(b_1) \cdots \chi_r(b_r).$$

利用這個寫法簡化出 $N(a_1x_1^{k_1} + \cdots + a_nx_n^{k_n} = b) =$

$$\sum_{\vec{\chi}:\chi_i^{k_i}=\varepsilon} \chi_1(a_1^{-1}) \cdots \chi_r(a_r^{-1}) \cdot \begin{cases} J_0(\chi_1, \ldots, \chi_r) & , \text{ 如果 } b = 0 \\ (\chi_1 \cdots \chi_r)(b) J(\chi_1, \ldots, \chi_r) & , \text{ 如果 } b \neq 0. \end{cases}$$

7. 建立以下表格

$\vec{\chi}$	$J(\vec{\chi})$	$\lvert J(\vec{\chi})\rvert$	$J_0(\vec{\chi})$	$\lvert J_0(\vec{\chi})\rvert$
$\vec{\varepsilon}$	p^{r-1}	p^{r-1}	p^{r-1}	p^{r-1}
$\prod_i \chi_i \neq \varepsilon$	$\dfrac{\tau(\chi_1)\cdots\tau(\chi_r)}{\tau(\chi_1\cdots\chi_r)}$	$p^{\frac{r-1}{2}}$	0	0
$\prod_i \chi_i = \varepsilon$	$-\dfrac{\tau(\chi_1)\cdots\tau(\chi_r)}{p}$	$p^{\frac{r}{2}-1}$	$(p-1)\dfrac{\tau(\chi_1)\cdots\tau(\chi_r)}{p}$	$(p-1)p^{\frac{r}{2}-1}$

如果某些 $\chi_i = \varepsilon$ 但不全為 ε，此時 $J_0(\vec{\chi}) = ?\, J(\vec{\chi}) = ?$

8. 證明

$$\lvert N(a_1x_1^{k_1} + \cdots + a_rx_r^{k_r} = b) - p^{r-1}\rvert \leq \begin{cases} M_0(p-1)p^{\frac{r}{2}-1} & , \text{ 如果 } b = 0 \\ M_0p^{\frac{r}{2}-1} + M_1p^{\frac{r-1}{2}} & , \text{ 如果 } b \neq 0 \end{cases}$$

其中 $M_0 = \lvert\{\vec{\chi} : \prod_i \chi_i = \varepsilon\}\rvert, M_1 = \lvert\{\vec{\chi} : \prod_i \chi_i \neq \varepsilon\}\rvert$，並且每一個 χ_i 都不等於 ε.

9. (此時不再有 $k_i \mid p-1$) 假設方程式 $a_1x_1^{k_1} + \cdots + a_rx_r^{k_r} = b$ 在模 p 下有解，且存在 i 使得 $\gcd(k_i, p) = 1$，證明對任意正整數 n，方程式 $a_1x_1^{k_1} + \cdots + a_rx_r^{k_r} = b$ 在模 p^n 下都有解。

10. 假設 $n_1, \ldots, n_t$ 是兩兩互質的正整數，且對任意 i 方程式 $a_1x_1^{k_1} + \cdots + a_rx_r^{k_r} = b$ 在模 n_i 下都有解，證明模 $n_1 \ldots n_t$ 下也有解。至此完成在一般模合數下解的研究。

11. 最後我們給出兩個應用：考慮方程式 $x^2 + y^2 = 1$，證明

$$N(x^2 + y^2 = 1) = p - \left(\frac{-1}{p}\right).$$

12. 利用 8. 證明對所有質數 $p > 11$，以及整數 r，同餘方程式 $x^2 + y^5 \equiv r \pmod{p}$ 總有解 (x, y).

做一下註解。第 7. 及第 8. 小題的結果稱作 Weil 定理，是以法國數學家 André Weil 命名的定理。Gauss 和以及 Jacobi 和原本都是為了解橢圓曲線上有理點 (或者是有限體上整點) 的個數所發展的工具，想要知道一些橢圓曲線相關性質的讀者可以參考 Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography (Discrete Mathematics and Its Applications).* Chapman and Hall/CRC; 2 edition. 該書只包含初等方法。筆者認為較適合高中生或大一學生看。

Chapter 13

N 次剩餘

- 三角和 trigonometric sum
- 導出 (特徵) induce
- 自同態 endomorphism
- 代數重數 algebraic multiplicity
- 本原特徵 primitive character
- 二次剩餘 quadratic residue
- 特徵值 eigenvalue

解析數論中一個很重要的問題是：假設給定實數數列 $(a_n)_{n\in\mathbb{N}}$，那麼要如何估計 (三角和)

$$\sum_{n=N}^{M} e^{2i\pi k a_n}$$

的大小？讓我們考慮以下幾個例子：

1. 給定正整數 m, N，證明方程式 $f(x_1,\dots,x_n) = N \pmod m$ 的解數是

$$\frac{1}{m}\sum_{x_1=0}^{m-1}\cdots\sum_{x_n=0}^{m-1}\sum_{a=0}^{m-1} e^{2i\pi a(f(x_1,\dots,x_n)-N)/m}.$$

2. 給定兩個整數數列 $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}$，證明方程式

$$f(x_1,\dots,x_n) = N, \quad \forall r \le n, \quad a_r \le b_r$$

的解數是

$$\sum_{a_1\le x_1\le b_1}\cdots\sum_{a_n\le x_n\le b_n}\int_0^1 e^{2i\pi a(f(x_1,\dots,x_n)-N)x}\,\mathrm{d}x.$$

寫出 Fermat 猜想，以及 Goldbach 猜想所對應出來的式子。

由於 Dirichlet 特徵又和 n 次單位根緊密相關，所以可以想見有時候也要學會估計像 Gauss 和等等的式子。三角和在解析數論中扮演舉足輕重的地位，例如給定整係數多項式 P，藉由估計特徵和，我們可以估計在 $P(1),\dots,P(x)$ 中 y-光滑數的個數；更一般地，我們可以研究在有限體上 Diophantine 問題的解數，特別是在高次剩餘及原根上的應用，我們將在下面看到。

■ 第一部分 ■

這個部分的目的在於證明所謂的 Pólya-Vinogradov 不等式：如果 q 是正整數，且 χ 為模 q 的一個非平凡特徵，定義域為全體整數 (見上一章節第二部份第 1 題)，那麼

$$\sup_{(N,M)\in\mathbb{N}^2}\left|\sum_{N\le n\le M}\chi(n)\right|\le 2\sqrt{q}\log q.$$

這個不等式可以推導出許多重要的結論，當然也有許多改進。以下會介紹他在計算二次剩餘甚至高次剩餘，還有模質數的原根的估計上的應用。

在這個部分裡 q 是一個給定的正整數。對一個模 q 的特徵 χ，如果對於所有 q 的因數 m，以及模 m 的特徵 χ'，都可以找到 a 使得 (I) a 與 q 互質, (II) a 模 m 餘 1, (III) $\chi(a)\neq\chi'(a)$，則我們說 χ 是一個本原特徵。否則 χ 則稱為非本原特徵，而我們知道此時存在 q 的因數 m，以及模 m 的特徵 χ'，使得對所有與 q 互質且模 m 餘 1 的整數 a 都有 $\chi(a)=\chi'(a)$，這時說 χ 被 χ' 所導出。例如以下的例子中模 6 的特徵 χ 就是被模 3 的特徵 χ' 所導出的：

$$\chi'(m)=\begin{cases}1 & , \quad m\equiv 1 \pmod 3\\ i & , \quad m\equiv 2 \pmod 3\\ 0 & , \quad m\equiv 0 \pmod 3\end{cases}\Rightarrow\ \chi(m)=\begin{cases}1 & , \quad m\equiv 1 \pmod 6\\ i & , \quad m\equiv 5 \pmod 6\\ 0 & , \quad m\equiv 0,2,3,4 \pmod 6\end{cases}$$

1. 假設 χ 是 q 的一個非本原特徵，證明存在 q 的因數 m，以及模 m 的本原特徵 χ'，使得 χ 被 χ' 所導出。

2. 對於模 q 的特徵 χ，可以引入 Gauss 和定義為：

$$G(n,\chi)=\sum_{t=0}^{q-1}\chi(t)e^{2i\pi\frac{tn}{q}},\quad n\text{為整數.}$$

仍然以 $\tau(\chi)$ 簡記 $G(1,\chi)$。證明當 χ 為本原特徵時會有 $|\tau(\chi)|=\sqrt{p}$. (提示：用兩種不同的方法表示 $\tau(\chi)\overline{\tau(\chi)}$，或是改進一下上一章節第四部份第 2.3 題的證明)

3. 假設 χ 為特徵，n 是整數。利用離散 Fourier 定理或是直接計算得到

$$\chi(n)=\frac{1}{\tau(\overline{\chi})}\sum_{k=0}^{q-1}\overline{\chi}(k)e^{2i\pi kn/q}.$$

4. 現在開始要證明 Pólya-Vinogradov 不等式。一開始假設 χ 為一個非平凡的本原特徵，利用前上兩題的結論證明對所有整數對 (N,M) 有

$$\left|\sum_{N\le n\le M}\chi(n)\right|\le\sqrt{q}\sum_{k=1}^{q-1}\frac{1}{\sin(\frac{k\pi}{q})}.$$

5. 考慮 Riemann 和以及利用不等式：對所有 $x \in [0, \pi/2]$, $\sin(\pi x) > 2x$。證明此時

$$\left| \sum_{N \le n \le M} \chi(n) \right| \le \sqrt{q} \log q.$$

6. 現在討論 χ 為非本原特徵的情況。取 q 的因數 m，以及模 m 的本原特徵 χ'，使得 χ 被 χ' 所導出，再記 $q = mr$。證明

$$\sum_{N \le n \le M} \chi(n) = \sum_{\substack{N \le n \le M \\ (n,r)=1}} \chi'(n) = \sum_{N \le n \le M} \sum_{d \mid (n,r)} \mu(d) \chi'(n) = \sum_{d \mid r} \mu(d) \sum_{\frac{M}{d} \le d \le \frac{N}{d}} \chi'(dm).$$

(提示：對第一個等號，看看什麼時候有 $\chi(n) = 0$，而什麼時候有 $\chi(n) = \chi'(n)$。)

7. 結束剩下的證明。

注意到處理二次剩餘所定義的 Legendre's 符號也是一個 Dirichlet 特徵，而在高次剩餘的情況下則是推廣了特徵的定義，藉由計算一般的情形，我們可以學習二次剩餘的性質。作為一個直接的結論：假設 p 是一個質數，記 $N_{\min}(p)$ 為模 p 的最小二次非剩餘，那麼 $N_{\min}(p) = O(\sqrt{p} \log p)$。而對於正整數 x，在任意長度為 x 的區間內模 p 的二次剩餘共有 $\frac{1}{2}x + O(\sqrt{p} \log p)$ 個，事實上大 O 符號前的常數可以被寫出來，留做練習。

另外筆者在指數教材中一文提到過，$N_{\min}(p) = O(p^{\frac{1}{2\sqrt{e}}} (\log p)^2)$，還有如果以 H 表示模 p 下連續二次 (非) 剩餘的最長長度，那麼 $H = O(p^{1/4} \log p)$。這兩個性質其實都是數學家 Burgess 將 Pólya-Vinogradov 不等式改進之後得到的結果。

接下來可以考慮該不等式在高次剩餘上的應用。假設 p 是一個質數，而 k 是 $p-1$ 的因數，且 $N < M$ 是兩個正整數。記在區間 $[N, M]$ 內的 k 次剩餘的數目為 $f_k(x)$，其中 $x = M - N$.

8. 取 $\chi_0, \dots, \chi_{k-1}$ 是使得 $\chi^k = \varepsilon$ 的那些特徵，證明

$$\frac{1}{k} \sum_{i=0}^{k-1} \sum_{a=N}^{M} \chi_i(a) = f_k(x).$$

9. 得到 $f_k(N, M) = x/k + O(\sqrt{p} \log p)$.

最後要估計模 p 的最小原根。令 $\beth_p$ 是原根的判斷函數，也就是說 $\beth_p(n) = 1$ 如果 n 是模 p 的原根，否則 $= 0$。我們希望用特徵表示這個函數。注意到一個數 n 不是原根，當且僅當他不是任何 v 次剩餘，其中 v 是 $p-1$ 的質因數。

10. 取 v 是 $p-1$ 的質因數。證明

$$\frac{1}{v} \sum_{\chi^v = \varepsilon} \chi(n) = \begin{cases} 1 & , \ a \text{ 是 } v \text{ 次剩餘} \\ 0 & , \ a \text{ 不是 } v \text{ 次剩餘} \end{cases}$$

11. 由上得到

$$\beth_p(n) = \prod_{v|p-1}\left(1 - \frac{1}{v}\sum_{\chi^v=\varepsilon}\chi(n)\right) = \sum_{d|\mathrm{rad}(p-1)}\frac{\mu(d)}{d}\sum_{\chi^d=\varepsilon}\chi(n).$$

其中 $\mathrm{rad}(x)$ 表示正整數 x 所有質因數的乘積。

12. 在取和時分開 $\chi=\varepsilon$ 和 $\chi\neq\varepsilon$，證明在區間 $[N, N+x]$ 中模 p 的原根個數為

$$\frac{\phi(p-1)}{p}x + O(2^{\omega(p-1)+1}\sqrt{p}\log p).$$

其中 $\omega(x)$ 表示正整數 x 的質因數個數。

13. 取 $\epsilon>0$。證明 $2^{\omega(p-1)+1}\sqrt{p}\log p\frac{p}{\phi(p-1)} \ll p^{1/2+\epsilon}$。令 $g(p)$ 為模 p 的最小原根，現在可以對他給出怎樣的上界？

■ 第二部分 ■

上一章節所介紹的 Dirichlet 特徵還有一個經典例子就是證明二次互反率：假設 p 和 q 是兩個相異的奇質數，那麼

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

在這個部分中，取 $\chi = \left(\frac{\cdot}{q}\right)$ 為模 q 的一個特徵，並考慮他的 Gauss 和 $\tau(\chi)$.

1. 回憶 Euler 判別法：$\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} \pmod q$.

2. 對整數 n，證明 Fourier 級數

$$\chi(n)\tau(\chi) = \sum_{k=1}^{q-1}\chi(m)e^{\frac{2i\pi kn}{q}}.$$

3. 導出 $\tau(\chi)^2 = (-1)^{q-1}q$.

4. 利用 $(a+b)^q = a^q + b^q$ (在 $\mathbb{F}_q$ 中)，證明在 $\mathbb{F}_q$ 中有等式

$$\tau(\chi)^p = \left(\frac{p}{q}\right)\tau(\chi).$$

5. 證明二次互反率。

■ 第三部分 ■

我們再次回到計算光滑數個數 $\Psi(x,y)$ 的問題。考慮 Dickman 函數 ρ：有初始條件 $\rho(u)=1$ 對所有 $u\in[0,1]$，而且滿足微分方程

$$u\rho'(u) + \rho(u-1) = 0, \quad (u\geq 1).$$

1. (a) 證明以上初始條件及微分方程定義出唯一的從 $[0,+\infty)$ 到 $\mathbb{R}$ 的函數 ρ.

   (b) 證明 $\rho \in \mathcal{C}^\infty$.

   (c) 證明對所有 $u \geq 1$，$u\rho(u) = \int_{u-1}^{u} \rho$。並得出 ρ 恆正，嚴格遞減至 0.

   (d) 證明 $\rho(u) \leq \frac{1}{\Gamma(u+1)}$ $(u \geq 0)$，其中 Γ 是 Euler Gamma 函數。

我們的目的是證明出 Dickman 定理：$\Psi(x, x^{\frac{1}{u}}) \sim x\rho(u)$, $(x \to +\infty)$。為此，考慮以下宣稱：$H(N) =$「Dickman 定理對於 $u \in [N, N+1]$ 為真。」

2. 證明 $H(0)$ 為真。

3. 當 $u \in [1,2]$ 時計算 $\rho(u)$ 以及 $\Psi(x, x^{\frac{1}{u}})$，證明 $H(1)$ 為真。

4. 取正整數 $N \geq 2$ 使得 $H(0), \ldots, H(N-1)$ 都為真。

   (a) 證明 Buchstab de Brujin 恆等式

   $$\Psi(x,y) = 1 + \sum_{p \leq y} \Psi\left(\frac{x}{p}, p\right).$$

   (b) 取 $u \in [N, N+1]$。藉由寫出

   $$\Psi(x, x^{\frac{1}{u}}) = \Psi(x, x^{\frac{1}{N}}) - \sum_{x^{1/u} < p \leq x^{1/N}} \Psi\left(\frac{x}{p}, p\right).$$

   證明 $H(N)$ 為真。

5. 讓我們考慮用這個定理來估計 $N_{\min}(p)$，模 p 的最小二次非剩餘。注意到一個正整數 n 如果是 $N_{\min}(p) - 1$-光滑的，那麼他也是模 p 的二次剩餘。藉由 Pólya-Vinogradov 不等式證明

   $$N_{\min}(p) = O\left(p^{\frac{1}{2\sqrt{e}}} (\log p)^{\frac{2}{\sqrt{e}}}\right).$$

6. 可以對高次剩餘得到什麼樣的結論？

■ 第四部分 ■

在這個部分中取 n 為 > 1 的奇數，令 $\zeta = \exp\left(\frac{2i\pi}{n}\right)$。取 V 是所有從 $\mathbb{Z}/n\mathbb{Z}$ 打到 $\mathbb{C}$ 的函數所形成的 n 維 $\mathbb{C}$-向量空間。並考慮其上的自同態線性映射 θ 定義為：

$$\theta(f) = \left\{ \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{C} \\ x & \mapsto & \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y)\zeta^{xy} \end{array} \right.$$

最後令 $\tau_n = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \zeta^{x^2}$.

1. 證明恆等式

   $$\theta \circ \theta(f)(x) = nf(-x), \quad \forall (f,x) \in V \times \mathbb{Z}/n\mathbb{Z}.$$

   並對角化 $\theta \circ \theta$.

2. 證明 θ 的秩為 τ_n，且 $|\tau_n| = \sqrt{n}$.

3. 假設 a, b, c, d 分別是 θ 關於特徵值 $\sqrt{n}, -\sqrt{n}, i\sqrt{n}, -i\sqrt{n}$ 的代數重數。證明

$$a + b = \frac{n+1}{2},\ c + d = \frac{n-1}{2},\ (a-b)^2 + (c-d)^2 = 1.$$

4. 計算 $\det(\theta)$，由此得出 a, b, c, d.

5. 證明

$$\tau_n = \begin{cases} \sqrt{n} & , \quad n \equiv 1 \pmod 4 \\ i\sqrt{n} & , \quad n \equiv 3 \pmod 4 \end{cases}$$

6. 設 p 為奇質數，取 $\chi = \left(\frac{\cdot}{p}\right)$ 為模 p 的一個特徵。證明 $\tau(\chi) = \tau_p$.

現在我們有了 Gauss 和的公式。可以考慮證明以下定理：如果 p 為模 4 餘 3 的質數，那麼在 $[1, (p-1)/2]$ 中的二次剩餘個數會比二次非剩餘個數多。首先可以寫出

$$\sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^t = i\sqrt{p}.$$

藉由在兩邊同乘 $\frac{1}{\sqrt{p}n}\left(\frac{n}{p}\right)$ 並取虛數部分得到

$$\frac{1}{n}\left(\frac{n}{p}\right) = \frac{1}{\sqrt{p}} \sum_{h=0}^{p-1} \left(\frac{h}{p}\right) \frac{\sin(2\pi nh/p)}{n}.$$

7. 記得 Fourier 級數裡的一個恆等式

$$\sum_{m=1}^{+\infty} \frac{\sin((2m-1)\theta)}{2m-1} = \begin{cases} \pi/4 & , \quad 0 < \theta < \pi \\ -\pi/4 & , \quad \pi < \theta < 2\pi \end{cases}$$

證明 (在過程中交換求和順序)

$$\sum_{m=1}^{+\infty} \frac{1}{2m-1} \left(\frac{2m-1}{p}\right) = \frac{\pi E}{2\sqrt{p}}.$$

其中 $E = \sum_{t=0}^{(p-1)/2} \left(\frac{t}{p}\right)$.

8. 記得對所有 $s > 1$ 有 Dirichlet 級數

$$\sum_{m=1}^{+\infty} \frac{1}{(2m-1)^s} \left(\frac{2m-1}{p}\right) = \prod_{q \text{ 為質數}} \left(1 - \frac{1}{q^s}\left(\frac{q}{p}\right)\right)^{-1}.$$

證明左式在 $s \geq 1$ 均勻收斂，由此推得連續性。因此 $E > 0$.

■ 第五部分 ■

給定質數 p 以及由 ± 1 組成的向量 $\vec{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n)$，我們希望求出以下集合的大小。

$$A_{\vec{\varepsilon}} = \{k \in \mathbb{F}_p \mid \left(\frac{k+1}{p}\right) = \varepsilon_1, \ldots, \left(\frac{k+n}{p}\right) = \varepsilon_n\}.$$

1. 取 $n=2$。證明

$$|A_{(+1,+1)}| = \frac{1}{4}\sum_{x\in\mathbb{F}_p}\left(1-\left(\frac{x}{p}\right)\right)\left(1-\left(\frac{x+1}{p}\right)\right).$$

2. 利用 Euler 判別法計算上述和。

3. 取 $n=3$，求所有 $|A_{\vec{\varepsilon}}|$.

4. 當 n 繼續變大時，上述的方法無法有效計算一般項。請學過代數幾何的讀者由 Weil 界證明

$$|A_{\vec{\varepsilon}}| = \frac{p}{2^n} + O_{p\to+\infty}(\sqrt{p}).$$

特別地，對所有正整數 N，只要 p 夠大，在模 p 下都會有連續的 N 個二次非剩餘。

Chapter 14

Mellin 變換

本章取自巴黎高等師範學院考題。

- Mellin 變換 Mellin transformation
- 均勻連續 uniformly continuous
- 分段連續 piecewise continuous

■ 預備知識 ■

給定實數 a，以 Π_a (以及 $\overline{\Pi_a}$) 記複數平面上實數部分大於 a (大於等於 a) 的複數所形成的集合。並且回憶如果 a 是正實數，且 $z = x + iy$ 為複數的話，

$$a^z = e^{z \log a} = a^x(\cos(y \log a) + \sin(y \log a)).$$

所謂的 Mellin 變換是指以下的過程：給定函數 F，那麼定義

$$M_F(s) = \int_1^\infty F(s)x^{-s-1}\mathrm{d}x.$$

這個部分要證明：假設 F 恆正，遞增，而且 $F(x) \underset{x\to\infty}{=} O(x^a)$，那麼 M_F 在 Π_a 上會有定義。如果進一步假設存在一個正實數 l 使得函數

$$s \mapsto M_F(s) - \frac{l}{x-a}$$

可以連續延拓到 $\overline{\Pi_a}$ 的話，那麼 $F(x) \underset{x\to\infty}{\sim} lx^a$.

也就是說，如果對於 M_F 有足夠的認識的話，就可以給出 F 的成長速率。利用這個定理，可以證明質數定理：$\pi(x) \sim x/\log x$，以及估計許多數列的成長速率。當然 Mellin 變換也在數學的許多分支上有重要的應用。

以下以 B (以及 L) 記所有從 $\mathbb{R}$ 到 $\mathbb{C}$ 且分段連續的有界函數 (分段連續的 L^1 函數) 的集合。以下題目需要分析的一些知識。注意以下積分都要求證明其存在性，並且作分部積分和代數變換時也要證明操作是合法的。

1. 假設 $f : \mathbb{R}^+ \to \mathbb{C}$ (非負實數到複數) 的分段連續函數，我們以 E_f 記所有使得

$$t \mapsto f(t)e^{-zt}$$

為 L^1 函數的複數 z 所形成的集合。而對於 $z \in E_f$，記積分

$$L_f(z) = \int_0^\infty f(t)e^{-zt}.$$

(a) 假設 $a \in \mathbb{R}$ 且函數 e_a 定義為

$$e_a : t \in \mathbb{R}^+ \mapsto e^{at}.$$

求出 E_{e_a}。並且對 $z \in E_{e_a}$ 計算 $L_{e_a}(z)$.

(b) 取 f 為從 $\mathbb{R}^+$ 到 $\mathbb{C}$ 且分段連續的函數。假設存在實數 a 使得

$$t \in \mathbb{R} \mapsto e^{-at} f(t)$$

在 $\mathbb{R}^+$ 上有界。證明 E_f 包含 Π_a.

2. 取 $f \in L$.

(a) 證明，對實數 ξ，以下積分的存在性

$$\widehat{f}(\xi) = \int_{-\infty}^{+\infty} f(x)e^{-i\xi x}\,\mathrm{d}x.$$

(b) 對 $\lambda > 0$，函數 f_λ 的定義為

$$f_\lambda : x \in \mathbb{R} \mapsto f(x/\lambda).$$

對實數 ξ, 試以 $\widehat{f}$ 來表示 $\widehat{f_\lambda}(\xi)$.

3. 函數 K 的定義為

$$\forall x \in \mathbb{R}, \quad K(x) = \max\{1 - |x|, 0\}.$$

(a) 對實數 ξ, 計算 $\widehat{K}(\xi)$.

(b) 證明函數 $H = \widehat{K} \in L$，且值域為非負實數，並且 $c = \int_{\mathbb{R}} H > 0$.

4. 取 $f \in B$ 且 $g \in L$.

(a) 證明對所有實數 x，函數 $t \in \mathbb{R} \mapsto f(x-t)g(t)$ 都在 L 中。對實數 x，定義函數 f, g 的卷積為

$$(f * g)(x) = \int_{-\infty}^{+\infty} f(x-t)g(t)\,\mathrm{d}t.$$

(b) 假設當 x 趨近無限大時 $f(x)$ 會收斂到一個複數 l，證明

$$(f * g)(x) \underset{x \to +\infty}{\longrightarrow} l \int_{-\infty}^{+\infty} g.$$

而接下來我們將證明一部分的逆命題。

5. 假設 $g \in L$。證明對所有 $\delta > 0$ 總有

$$\int_{|x|>\delta} \lambda g(\lambda x) \underset{\lambda \to +\infty}{\longrightarrow} 0.$$

6. 繼續沿用第 2.3 題的符號。對於正實數 λ，我們記

$$H^\lambda = \widehat{K_\lambda}.$$

在這個問題中。我們假設有兩個正實數 a, l，還有 B 中的一個值域為非負實數的函數 f，滿足

(i) 函數 $t \in \mathbb{R} \mapsto e^{at} f(t)$ 在 $\mathbb{R}^+$ 上遞增。

(ii) 對於任意正實數 λ 總有

$$(f * H^\lambda)(x) \underset{x \to +\infty}{\longrightarrow} cl.$$

目的是要證明當 x 趨近無限大時 $f(x)$ 會收斂到複數 l。接下來給定非負實數 x 以及正實數 δ。

(a) 證明

$$(f * H^\lambda)(x + \delta) \geq f(x) e^{-2a\delta} \int_{-\delta}^{\delta} H^\lambda.$$

(b) 證明

$$(f * H^\lambda)(x - \delta) \leq f(x) e^{2a\delta} \int_{-\delta}^{\delta} H^\lambda + ||f||_{\infty,\mathbb{R}} \int_{|u| \geq \delta} H^\lambda.$$

其中 $||f||_{\infty,\mathbb{R}} = \sup_{t \in \mathbb{R}} |f(t)|$.

(c) 總結以上結果。

以上是利用 Fourier 變換以及 Laplace 變換所得到的結論。

數學上有所謂的 Abelian 定理以及 Tauberian 定理，他們給出了計算級數和的一些方法。更廣義的說如果今天有個發散級數 $\sum a_n$，那麼是否有可能賦予他一個值呢？數學家們曾經覺得這只會導致出許多矛盾，但時至今日，這已演變成完整且嚴謹的一個理論。今天這裡要介紹一個 Tauberian 定理，當然，不會牽涉到發散級數：取 $g : \mathbb{R}^+ \to \mathbb{R}^+$ 為一個分段連續且遞增的函數，而假設有兩個正實數 a, l 滿足

(i) 函數 $\phi : x \in \mathbb{R}^+ \mapsto g(x) e^{-ax}$ 在 $\mathbb{R}^+$ 上有界。注意到由 1.*b*) 小題 L_g 會在 Π_a 上有定義。

(ii) 函數

$$z \in \Pi_a \mapsto L_g(z) - \frac{l}{z - a}$$

可以連續延拓成定義在 $\overline{\Pi}_a$ 上的函數 G.

目的是要證明 $g(x) \underset{x \to +\infty}{\sim} l e^{ax}$。以下取 ϵ, λ 是兩個正實數，而 x 是一個實數。

7. 假設 y 是實數，證明

$$\int_0^{+\infty} \phi(t) e^{-(\epsilon + iy)t} \, \mathrm{d}t = l \int_0^{+\infty} e^{-(\epsilon + iy)t} \, \mathrm{d}t + G(a + \epsilon + iy).$$

8. 證明

$$\int_0^{+\infty} e^{-\epsilon t}\phi(t)H^\lambda(x-t)\,\mathrm{d}t = l\int_0^{+\infty} e^{-\epsilon t}H^\lambda(x-t)\,\mathrm{d}t + \int_0^{+\infty} G(a+\epsilon+iy)K_\lambda(y)e^{ixy}\,\mathrm{d}t.$$

(注意到此題會交換兩個積分的順序，需要證明。)

9. 證明

$$\int_0^{+\infty} \phi(t)H^\lambda(x-t)\,\mathrm{d}t = l\int_{-\infty}^{x} H^\lambda + \int_0^{+\infty} G(a+iy)K_\lambda(y)e^{ixy}\,\mathrm{d}t.$$

10. 證明 Riemann-Lesbegue 引理：假設 $f \in L$，那麼

$$\widehat{f}(\xi) = \int_{-\infty}^{+\infty} f(x)e^{-i\xi x}\mathrm{d}x \underset{\xi\to\pm\infty}{\longrightarrow} 0.$$

(提示：先考慮 f 是階梯函數且只在有限長度的區間內取值不為 0，接著對於一般函數，可考慮用階梯函數去均勻逼近。)

11. 利用以上結果證明 $g(x) \underset{x\to+\infty}{\sim} le^{ax}$.

12. 進一步的，總結以上為此定理：

定理 14.1 有三個正實數 a, k, l，而 $u : \mathbb{R}^+ \to \mathbb{R}^+$ 為一個分段連續且遞增的函數，滿足

(i) 對所有 $x \geq 1$，有 $u(x) \leq kx^a$。這個不等式蘊含了以下函數是有定義的

$$s \in \Pi_a \mapsto \int_1^{+\infty} u(x)x^{-s-1}x.$$

(ii) 存在連續函數 $V : \overline{\Pi_a} \to \mathbb{C}$ 使得

$$\forall s \in \Pi_a, \quad \int_1^{+\infty} u(x)x^{-s-1}\,x = \frac{l}{s-a} + V(s).$$

那麼 $u(x) \underset{x\to+\infty}{\sim} lx^a$.

■ 第一部分 ■

假設有 $q \geq 2$ 個全部都大於等於 2 的正整數 $m_1, \ldots, m_q$，以及 q 個正實數 $r_1, \ldots, r_q$ 滿足 $\kappa = \sum_{i=1}^q r_i > 1$。我們考慮以下定義的數列：

$$a_0 = 1 \qquad \text{且} \qquad \forall n \geq 1, \quad a_n = \sum_{j=1}^{q} r_j a_{[n/m_j]}.$$

其中 $[\bullet]$ 是 Gauss 函數。目的是要研究 a_n 的成長速率。

1. 作為一個例子，考慮

$$q = 2, \quad r_1 = 2, \quad r_2 = 3, \quad m_1 = 3, \quad m_2 = 9.$$

試給出 a_n 的一般式。

2. 對於複數 s，定義

$$\Phi(s) = \sum_{j=1}^{q} r_j m_j^{-s}.$$

證明存在唯一正實數 α 使得 $\Phi(\alpha) = 1$.

3. 證明存在正常數 C 使得對所有正整數 n 都有 $a_n \leq Cn^{\alpha}$.

4. 利用 $1 + [n/m] \geq (n+1)/m$ 證明所有非負整數 n 都有 $a_n \geq (n+1)^{\alpha}$.

5. (a) 對於 $s \in \Pi_a$，證明 $|\Phi(s)| < 1$.

   (b) 證明存在非 0 的實數 y 使得 $\Phi(\alpha + iy) = 1$ 當且僅當對所有 $k \neq l$ 都有 $\log(m_l)/\log(m_k)$ 是無理數。此時我們說假設 (H) 為真。

接下來考慮函數 A，定義為 $A : x \in \mathbb{R}^+ \mapsto a_{[x]}$。這在一般做數列的問題中是常見的手法，因為我們可以得到一個分段連續函數，因此有許多分析的工具可使用。

6. (a) 當 $x \in [0, 1)$ 時，$A(x)$ 為何？

   (b) 對所有 $x \geq 1$，證明

$$A(x) = \sum_{j=1}^{q} r_j A\left(\frac{x}{m_j}\right).$$

7. 假設 $s \in \Pi_a$，證明 $x \in [1, +\infty) \mapsto x^{-s-1}A(x)$ 是 L^1 函數。在以下問題中，將以 M 表示函數

$$s \in \Pi_a \mapsto \int_1^{+\infty} x^{-s-1} A(x) \mathrm{d}x.$$

8. 假設 $s \in \Pi_a$，證明 $s(1 - \Phi(s))M(s) = \kappa - \Phi(s)$.

9. 如果假設 (H) 為真。

   (a) 證明 M 可連續延拓到 $\overline{\Pi_a} \setminus \{\alpha\}$.

   (b) 證明存在 $\rho > 0$ 使得

$$s \mapsto M(s) - \frac{\rho}{s - \alpha}$$

   可連續延拓到 $\overline{\Pi_a}$。以 $m_1, \ldots, m_q, r_1, \ldots, r_q$ 表示 ρ.

10. 如果假設 (H) 為真。試用預備知識中的 Tauberian 定理給出 a_n 的等價式。

11. 如果 $q = 3, r_1 = r_2 = r_3 = 1, m_1 = 2, m_2 = 3, m_3 = 6$，給出 a_n 的等價式。

Chapter 15

均勻分布

- 遍歷理論 ergodic theory
- 密集 dense
- 緊緻 compact
- 測度 measure
- 對射 bijection

遍歷假設是統計物理中最重要的假設之一，假想在一個實驗中可以測量某個物理量 A，當每隔固定一小段時間就測量這個量一次時，我們可以定義 A 的時間平均；另一方面，如果可以在同樣的條件同樣的環境下不停重複這個實驗，那就可以定義 A 的空間平均。所謂的遍歷假設就是說時間平均以及空間平均會是相同的。在一般物理系統中，尤其在統計力學範疇裡，均採用此為基本的假設，而遍歷理論就是為了證明這個假設所產生的一個數學分支，目前研究具有不變測度的動力系統及其相關問題。

對 $[0,1)$ 的一個子區間 I，以 $\mu(I)$ 記其長度。對於實數 θ，以 $\{\theta\} = \theta - [\theta]$ 記他的小數部份。如果 $u = (u_n)_{n\in\mathbb{N}}$ 是一個實數數列，而 n 是一個正整數，記

$$N_n(u, I) = |\{k \in \{1, \dots, n\} \mid \{u_k\} \in I\}|.$$

假設對於任意 $[0,1)$ 的一個子區間 I，總有

$$\lim_{n\to+\infty} \frac{N_n(u, I)}{n} = \mu(I)$$

我們便說數列 u 在模 1 下均勻分布。這個概念是 Hermann Weyl 在 1916 年引入的，而在這個章節裡就是要探討均勻分布的一些性質。

■ 預備知識 ■

在約 1926-1927 年，量子力學奠基者之一的 Paul Dirac 發現如果能夠在實數上定義滿足

$$\delta(x) = 0 \text{ 對所有 } x \neq 0, \quad \delta(0) \neq +\infty,$$
$$\int_{\mathbb{R}} f(x)\delta(x)\,\mathrm{d}x = f(0) \text{ 對所有夠好的函數 } f$$

的函數 δ 時，那麼許多物理理論的描述都將變得更加簡略而許多計算也將變得容易。

從以前數學的角度來看這樣的函數不嚴謹的，首先 $+\infty$ 並不在一般常用的實數系裡，因此沒有一個函數能夠取值為 $+\infty$；其次第二式的積分在 Riemann 的觀點下來看也是不可能的，因為當 f 是分段連續函數時 $f\delta$ 在實數上的積分必定為 0！

Dirac 並不是第一個有這樣想法的科學家，事實上 Joseph Fourier 和 Augustin-Louis Cauchy 在這之前研究了一些積分定理就發現這種函數的重要性，只是 Dirac 將函數 δ 作為一種方便的記號在《量子力學原理》中引入，故該函數今天以他命名。

現代數學家將 Dirac 函數視為一種逼近過程來理解，將於下文解釋，與此同時我們會介紹一個在分析學上非常重要的手法：如何將一個很隨便的函數變成 $\mathcal{C}^\infty$ 函數。本預備知識的許多內容其實對於在 $\mathbb{R}^d$ 且於更廣義測度上有意義的函數都是對的，但是筆者認為這超過大二的範圍了，所以以下只會介紹從 $\mathbb{R}$ 到 $\mathbb{R}$ 的函數的性質，而考慮的積分都是 Riemann 積分。

以下固定 f 是從 $\mathbb{R}$ 到 $\mathbb{R}$ 的一個連續函數。這裡先提醒讀者下述取的函數 $(u_n)_{n\in\mathbb{N}}$ 會滿足性質，做題目時可能會用到：

(a) 所有 u_n 都是可積函數，並且

$$\sup_{n\in\mathbb{N}}\int_{\mathbb{R}}|u_n|<\infty.$$

(b)

$$\int_{\mathbb{R}}u_n\underset{n\to+\infty}{\longrightarrow}1.$$

(c) 對所有 $r>0$ 總有

$$\int_{|x|\geq r}u_n(x)\,\mathrm{d}x\underset{n\to+\infty}{\longrightarrow}0.$$

1. 令 u 是由 $u(x)=\exp(-1/x)$ 如果 $x>0$，否則 $=0$ 所定義的從 $\mathbb{R}$ 到 $\mathbb{R}$ 的函數。證明 u 是 $\mathcal{C}^\infty$ 函數。

2. 對所有正整數 n，可以定義從 $\mathbb{R}$ 到 $\mathbb{R}$ 的函數 u_n 如 $u_n(x)=c_nu(1/n-x)u(1/n+x)$，其中 c_n 是使得 $\int_{\mathbb{R}}u_n=1$ 的常數。證明卷積

$$(f*u_n)(x)=\int_{\mathbb{R}}f(x-t)u_n(t)\,\mathrm{d}t$$

存在。

3. 證明對任意正整數 n，$f*u_n$ 是 $\mathcal{C}^\infty$ 函數，並且 $(f*u_n)^{(k)}=f*(u_n)^{(k)}$.

4. 證明在所有 $\mathbb{R}$ 的緊緻集上 $f*u_n$ 會均勻收斂至 f.

5. 此題假設 f 是一個 $\mathcal{C}^p$ 函數，而 k 是不超過 p 的非負整數。證明在所有 $\mathbb{R}$ 的緊緻集上 $(f*u_n)^{(k)}$ 會均勻收斂至 $f^{(k)}$.

■ 第一部分 ■

1. 承認以下版本的 Fourier 逼近：假設 f 是從 $\mathbb{R}$ 到 $\mathbb{C}$ 的 1-週期連續函數，那麼對所有 $\epsilon > 0$，總存在某個形如
$$t \in \mathbb{R} \mapsto \sum_{j=-d}^{d} a_j e^{2i\pi jt}$$
的函數 p，其中 a_j 為複數。使得對所有實數 t 總有 $|f(t) - p(t)| < \epsilon$.

   證明 Weyl 準則：假設 $(u_n)_{n\in\mathbb{N}}$ 是 $[0,1)$ 中的一個數列，那麼他均勻分布當且僅當對所有正整數 j 都有
$$\lim_{n\to+\infty} \frac{1}{n} \sum_{k=1}^{n} e^{2i\pi j u_k} = 0.$$
   (提示：先考慮 f 是階梯函數，接著對於一般函數，可用階梯函數去均勻逼近。)

2. 證明如果 α 是個無理數，那麼 $(n\alpha)_{n\in\mathbb{N}}$ 在模 1 下均勻分布。

3. 找到一個全為有理數的模 1 均勻分布數列。

4. 證明 $((\frac{1}{2}(1+\sqrt{5}))^n)_{n\in\mathbb{N}}$ 在模 1 下並不均勻分布。由此可以看出並不是隨便一個無規則的數列都是模 1 下均勻分布的，而事實上均勻分布的例子也是不容易找到的。

5. (a) 證明 $\theta = \log 2/\log 10$ 是個無理數。

   (b) 假設 r 包含於 1 到 9 中，而 k 是個正整數。證明 2^k 的首位數字為 r 當且僅當
$$\frac{\log(r)}{\log(10)} \leq \{k\theta\} < \frac{\log(r+1)}{\log(10)}.$$

   (c) 利用 $v_r(n)$ 記 1 到 n 中使得 2^k 的首位數字為 r 的正整數 k 的個數，證明並找出 $(v_r(n)/n)_{n\in\mathbb{N}}$ 的極限。我們可以對 $(2^n$ 的首位數字$)_{n\in\mathbb{N}}$ 這麼集合下怎樣的結論？

6. 假設 $(u_n)_{n\in\mathbb{N}}$ 是 $[0,1)$ 中的一個數列。證明 $(u_n)_{n\in\mathbb{N}}$ 在 $[0,1)$ 上密集當且僅當存在 $\mathbb{N}$ 的對射函數 σ 使得 $(u_{\sigma(n)})_{n\in\mathbb{N}}$ 模 1 均勻分布。

■ 第二部分 ■

在這個部分中固定一個從 $[1,+\infty)$ 到 $\mathbb{R}$ 的 $\mathcal{C}^1$ 函數 f.

1. 令 k 是正整數。證明
$$|e^{2i\pi f(k)} - \int_k^{k+1} e^{2i\pi f}| \leq 2\pi \int_k^{k+1} |f(t) - f(k)|\,\mathrm{d}t \leq 2\pi \int_k^{k+1} |f'|.$$

2. 假設 $\lim_{x\to+\infty} f'(x) = 0$.

   (a) 證明如果 u 是一個在無窮大處值會趨近於 0 的連續函數，那麼
$$\lim_{x\to+\infty} \frac{1}{x} \int_1^{x+1} u \to 0.$$

(b) 證明 $e^{2i\pi f(k)} - \int_k^{k+1} e^{2i\pi f} \underset{k\to\infty}{\to} 0$ 以及

$$\frac{1}{n}\left(\sum_{k=1}^{n} e^{2i\pi f(k)} - \int_1^{n+1} e^{2i\pi f}\right) \underset{n\to\infty}{\longrightarrow} 0.$$

(c) 證明 $(f(n))_{n\in\mathbb{N}}$ 模 1 下均勻分布當且僅當對所有對所有正整數 j 都有

$$\int_1^{n+1} e^{2ij\pi f} \underset{n\to\infty}{=} o(n).$$

3. (a) 藉由直接積分，給出

$$\frac{1}{n}\left|\int_1^{n+1} (1 + 2i\pi x f'(x)) e^{2i\pi f(x)}\right| \underset{n\to\infty}{\longrightarrow} 1.$$

(b) 假設存在實數 a 使得 $xf'(x) \underset{x\to\infty}{\to} a$。找出下式在 $n \to +\infty$ 的極限：

$$\frac{1}{n}\int_1^{n+1} (xf'(x) - a) e^{2i\pi f(x)}\,\mathrm{d}x.$$

再來是下式在 $n \to +\infty$ 的極限：

$$\frac{1}{n}\left|\int_1^{n+1} e^{2i\pi f}\right|.$$

試問 $(f(n))_{n\in\mathbb{N}}$ 在模 1 下是否均勻分布？

4. 取 u, v 是兩個實數滿足 $u < v$，λ 是正實數，而 φ 是從 $[u, v]$ 到 $\mathbb{R}$ 的 $\mathcal{C}^2$ 函數。假設 φ' 是在 $[u, v]$ 上的單調函數，而且對所有 $t \in [u, v]$ 都有 $|\varphi'(t)| > \lambda$.

(a) 證明

$$\int_u^v e^{i\varphi} = \left[\frac{e^{i\varphi}}{i\varphi'}\right]_u^v + \int_u^v \frac{\varphi''}{i(\varphi')^2} e^{i\varphi}.$$

(b) 由此找到絕對常數 C 使得

$$\left|\int_u^v e^{i\varphi}\right| \le \frac{C}{\lambda}.$$

(c) 利用預備知識的結果看出上述不等式對 $\mathcal{C}^1$ 函數仍成立 (注意這個手法在分析學中是重要的)。

5. 導出 Féjer 準則：如果 f' 在無窮大附近單調，而且

$$f'(x) \underset{x\to+\infty}{\longrightarrow} 0, \quad xf'(x) \underset{x\to+\infty}{\longrightarrow} +\infty.$$

那麼 $(f(n))_{n\in\mathbb{N}}$ 在模 1 下均勻分布。

6. 令 $\alpha \in (0, 1)$，λ 是正實數，對所有 $x \ge 1$：

$$f_\alpha(x) = x^\alpha, \quad g_\lambda(x) = (\log x)^\lambda.$$

試問 $(f_\alpha(n))_{n\in\mathbb{N}}$ 及 $(g_\lambda(n))_{n\in\mathbb{N}}$ 是否在模 1 下均勻分布？

■ 第三部分 ■

對於兩個實數 a,b，以 $\delta_{a,b}$ 記 0 (如果 $a \neq b$)，或 1 (如果 $a = b$)。假設 F 是個從 $\mathbb{Z}$ 到 $\mathbb{C}$ 的函數，我們說 F 是正定型當且僅當對所有 $\mathbb{Z}$ 的有限子集 A，以及任意複數集 $(z_k)_{k\in A}$ 總有

$$\sum_{(k,l)\in A^2} F(k-l)z_k\overline{z_l} \in \mathbb{R}^+.$$

1. 取 r 是實數，定義 F_r 如下

$$F_r(k) = \delta_{0,k} + r, \ \ \forall k \in \mathbb{Z}.$$

證明 F_r 為正定型當且僅當 r 非負。

2. 在這個問題中 u 是從 $\mathbb{Z}$ 到 $\mathbb{C}$ 的有界函數，並且在 $\mathbb{Z}\backslash\mathbb{N}$ 上為零。而 φ 是從 $\mathbb{N}$ 到 $\mathbb{N}$ 的嚴格遞增函數。

假設存在從 $\mathbb{Z}$ 到 $\mathbb{C}$ 的函數 U 使得對所有整數 k 必有

$$\frac{1}{\varphi(n)}\sum_{m=1}^{\varphi(n)} u(m+k)\overline{u(m)} \underset{n\to+\infty}{\longrightarrow} U(k).$$

(a) 假設 k,l 是兩個整數，證明

$$\frac{1}{\varphi(n)}\sum_{m=1}^{\varphi(n)} u(m+k)\overline{u(m+l)} \underset{n\to+\infty}{\longrightarrow} U(k-l).$$

(b) 證明 U 是正定型。

3. 在這個問題中 f 是從 $\mathbb{N}$ 到 $\mathbb{C}$ 上單位圓的函數，使得對所有整數 k 必有

$$\frac{1}{n}\sum_{m=1}^{n} f(m+k)\overline{f(m)} \underset{n\to+\infty}{\longrightarrow} 0.$$

我們想要用歸謬法證明下式，因此假設他是錯的：

$$\frac{1}{n}\sum_{m=1}^{n} f(m) \underset{n\to+\infty}{\longrightarrow} 0.$$

(a) 證明存在從 $\mathbb{N}$ 到 $\mathbb{N}$ 的嚴格遞增函數 φ 以及一個非零複數 c 使得

$$\frac{1}{\varphi(n)}\sum_{m=1}^{\varphi(n)} f(m) \underset{n\to+\infty}{\longrightarrow} c.$$

由此定義一個從 $\mathbb{Z}$ 到 $\mathbb{C}$ 的函數 g 如下：

$$g(n) = \begin{cases} 0 & , \text{ 如果 } n \leq 0 \\ n-c & , \text{ 如果 } n > 0. \end{cases}$$

(b) 令 k 是整數，求證

$$\frac{1}{\varphi(n)}\sum_{m=1}^{\varphi(n)} g(m+k)\overline{g(m)} \underset{n\to+\infty}{\longrightarrow} \delta_{0,k} - |c|^2.$$

(c) 總結。

4. 試證 Van der Corput 定理：如果 $(u_n)_{n\in\mathbb{N}}$ 是一個實數數列，滿足對所有的正整數 k 都有 $(u_{n+k}-u_n)_{n\in\mathbb{N}}$ 模 1 均匀分布，那麼 $(u_n)_{n\in\mathbb{N}}$ 本身也模 1 均匀分布。

5. 最後是 Van der Corput 定理的一個應用。

(a) 數學歸納法證明如果 P 是個實係數的非零多項式，而領導係數是個無理數，那麼 $(P(n))_{n\in\mathbb{N}}$ 模 1 均匀分布。

(b) 假設 $(u_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}}$ 是兩個實數數列，而 d 是正整數，滿足

i. 對所有正整數 n，$u_{n+d}-u_n$ 是整數。

ii. 對所有正整數 $j\le d$，$(v_{(n-1)d+j})_{n\in\mathbb{N}}$ 模 1 均匀分布。

證明 $(u_n+v_n)_{n\in\mathbb{N}}$ 模 1 均匀分布。

(c) 證明如果 P 是個實係數的非零多項式，而至少有一個係數是無理數，那麼 $(P(n))_{n\in\mathbb{N}}$ 模 1 均匀分布。

Chapter 16

加性數論

- 同構 isomorphism
- 雙線性型 bilinear form
- 譜 spectrum
- 陪集 coset
- 秩 rank
- 精細 (拓撲) fine
- Fourier 權重 Fourier bias

■ 預備知識 ■

回憶以前所定義過的：G 為一個交換群，群上的關係為加法 $+$. 對於 G 的兩個子集 A, B 定義他們的和集為 $A+B=\{a+b \mid a\in A, b\in B\}$。稱從 G 打到乘法群 $\mathbb{C}^\times$ 的同態映射為一個特徵。$\widehat{G}$ 為 G 中所有特徵所形成的群，又稱為 G 的對偶群。

以下為節省符號，引入 X 是有限交換群 G 上的均勻隨機變數，Y 是 $\widehat{G}$ 上的均勻隨機變數，並以 $\mathbb{P}$ 表示機率，$\mathbb{E}$ 表示期望值，而 $\mathbb{V}$ 為變異數。對於 G 的一個子集 A，1_A 是指 A 的判斷函數，也就是說 $1_A(x)=1$ 如果 $x\in A$，否則 $=0$.

1. 此題欲證 Chernoff 不等式：假設 $X_1,\dots,X_n$ 是相互獨立的實數隨機變數，而且對所有 i 都有 $|X_i-\mathbb{E}[X_i]|\le 1$。記 $X=X_1+\cdots+X_n$，那麼對所有正實數 λ 總有

$$\mathbb{P}\left(|X-\mathbb{E}[X]|\ge\lambda\sigma\right)\le 2\max\left(e^{-\lambda^2/4}, e^{-\lambda\sigma/2}\right).$$

   其中 $\sigma=\sqrt{\mathbb{V}[X]}$.

   (a) 引理：假設 X 是一個實數隨機變數，滿足 $\mathbb{E}[X]=0$ 且 $|X|\le 1$。那麼對所有 $t\in[-1,1]$ 總有 $\mathbb{E}[e^{tX}]\le\exp\left(t^2\mathbb{V}[X]\right)$.

   (b) 說明為了證明 Chernoff 不等式，只須證明

$$\mathbb{P}\left(X\ge\lambda\sigma\right)\le e^{-t\lambda\sigma/2}.$$

   其中 $t=\min(1,\lambda/2\sigma)$.

   (c) 結束剩下的證明。

2. 證明同構 $G \cong \widehat{G}$，注意 G 是有限群。

3. 證明可以在所有從 G 到 $\mathbb{C}$ 的函數所形成的向量空間上定義內積

$$\langle\ ,\ \rangle : (f,g) \in (\mathbb{C}^G)^2 \mapsto \mathbb{E}[f(X)\overline{g(X)}].$$

4. 證明在此內積下 $\widehat{G}$ 的元素兩兩正交，且有

$$\sum_{\gamma\in\widehat{G}} \gamma = |G|1_{\{0\}}.$$

5. 假設 f 是一個 G 到 $\mathbb{C}$ 的函數，定義 $\widehat{f}$ 如 $\widehat{f}(\gamma) = \mathbb{E}[f(X)\overline{\gamma(X)}]$ 是從 $\widehat{G}$ 到 $\mathbb{C}$ 的函數，這個過程稱為 Fourier 變換。證明 Fourier 反演：

$$f(x) = \sum_{\gamma\in\widehat{G}} \widehat{f}(\gamma)\gamma(x),\ \forall\, x \in G.$$

6. 類似地可以在 $\mathbb{C}^{\widehat{G}}$ 上定義內積

$$\langle\ ,\ \rangle : (f,g) \in (\mathbb{C}^{\widehat{G}})^2 \mapsto |G| \cdot \mathbb{E}[f(Y)\overline{g(Y)}].$$

證明對任意 $(f,g) \in (\mathbb{C}^G)^2$，有 $\langle f,g\rangle = \langle \widehat{f}, \widehat{g}\rangle$。特別地 $\mathbb{E}[|f(X)|^2] = |G| \cdot \mathbb{E}[|\widehat{f}(Y)|^2]$.

7. 對 $(f,g) \in (\mathbb{C}^G)^2$，還可以定義卷積 $f * g \in \mathbb{C}^G$ 為 $(f*g)(x) = \mathbb{E}[f(Y)g(x-Y)]$。取三個從 G 到 $\mathbb{C}$ 的函數 f,g,h，證明

   (a) $f*g = g*f$, $(f*g)*h = f*(g*h)$.

   (b) $f*(g+h) = f*g + f*h$.

   (c) $\widehat{f*g} = \widehat{f}\cdot\widehat{g}$.

   (d) $\mathbb{E}[(f*g)(X)] = \mathbb{E}[f(X)]\mathbb{E}[g(X)]$.

   利用 (c) 證明對於 G 的任意子集 A 總有

$$\sum_{(x,d)\in G^2} 1_A(x)1_A(x+d)1_A(x+2d) = |G|^2 \sum_{\gamma\in\widehat{G}} \widehat{1_A}(\gamma)^2\widehat{1_A}(\gamma^{-2}).$$

8. 對於 G 的兩個子集 A,B，找出 $A+B$ 和 $1_A * 1_B$ 的關係。

■ 第一部分 ■

定義所謂的 Bohr 集如下：假設 G 是有限交換群，而 $\Gamma \subseteq \widehat{G}$，且 $\delta \geq 0$，那麼定義

$$\mathrm{Bohr}_G(\Gamma,\delta) = \{x \in G \mid |\gamma(x) - 1| \leq \delta,\ \forall\gamma \in \Gamma\}.$$

稱為秩為 $|\Gamma|$ 而半徑為 δ 的 Bohr 集。

筆者在此做個註解，有些書中定義 Bohr 集的方式是不同的。例如陶哲軒和 Van H. Vu 的書裡是先定義 G 上的雙線性型，再由複數的幅角定義。但是在 G 為有限群時這兩者顯然是等價的 (預備知識第 1. 題)，而事實上 Bohr 集是在 G 上最精細的可緊緻化拓撲，所有的定義都是等價的。

另外對於實數 θ，以 $||\theta||_{\mathbb{R}/\mathbb{Z}}$ 表示 θ 與離他最近的整數的距離，$\mathrm{e}(\theta) = \exp(2i\pi\theta)$.

1. 在這題 $G = \mathbb{F}_p^n$.
   (a) 在 G 上定義標準內積。證明 $\widehat{G} = \{x \in G \mapsto \mathrm{e}((r \cdot x)/p) \mid r \in G\}$.
   (b) 由此證明 $\mathrm{Bohr}_G(\Gamma, \delta)$ 包含 Γ 的" 正交空間"，所以 $\mathrm{Bohr}_G(\Gamma, \delta)$ 包含一個維度 $n - |\Gamma|$ 的子空間。

2. 在這題 $G = \mathbb{Z}/N\mathbb{Z}$.
   (a) 假設 $x_1, \ldots, x_k$ 是 G 中的元素，證明存在 $d \in G$ 使得對所有 i 都有 $||dx_k/N||_{\mathbb{R}/\mathbb{Z}} \leq N^{-1/k}$.
   (b) 證明對任意實數 θ 都有 $4||\theta||_{\mathbb{R}/\mathbb{Z}} \leq |\mathrm{e}(\theta) - 1| \leq 2\pi||\theta||_{\mathbb{R}/\mathbb{Z}}$.
   (c) 進一步假設 N 是質數。給定 $\Gamma \subseteq \widehat{G}$，且 $\delta \geq 0$。藉由將 Γ 寫成 $\Gamma = \{x \mapsto \mathrm{e}((r_i x)/N) \mid r_1, \ldots, r_k \in G\}$，且取 d 為以 $r_1, \ldots, r_k$ 及第 (a) 小題定義出來者，證明 $\mathrm{Bohr}_G(\Gamma, \delta)$ 包含某個型如 $\{-Md, \ldots, -d, 0, d \ldots, Md\}$ 的等差數列，而且這個等差數列的長度 $\geq \frac{1}{2\pi}\delta N^{1/|\Gamma|}$.

對於 G 的子集 A，以及非負實數 δ，定義 δ-譜為

$$\mathrm{Spec}_\delta(A) = \{\gamma \in \widehat{G} \mid |\widehat{1_A}(\gamma)| \geq \delta|A|/|G|\}.$$

3. 利用 $\mathbb{E}[\widehat{1_A}(Y)]$ 及 Markov 不等式證明 $|\mathrm{Spec}_\delta(A)| \leq \delta^{-2}|G|/|A|$.

4. 假設 A 為 G 的子集，目的是證明 Bogolyubov 引理：存在 Γ' 包含至多 α^{-2} 個元素使得 $\mathrm{Bohr}_G(\Gamma', \sqrt{2}) \subseteq 2A - 2A$，其中 $2A - 2A = A + A - A - A$.
   (a) 證明
   $$1_A * 1_A * 1_{-A} * 1_{-A}(x) = \sum_{\gamma \in \widehat{G}} |\widehat{1_A}(\gamma)|^4 \gamma(x) = \sum_{\gamma \in \widehat{G}} |\widehat{1_A}(\gamma)|^4 \mathrm{Re}(\gamma(x)).$$
   (b) 以下記 $|A| = \alpha|G|$。取 $\Gamma = \mathrm{Spec}_{\alpha^{1/2}}(A)$，利用 Parseval 恆等式證明 $|\Gamma| \leq \alpha^{-2}$.
   (c) 藉由給出 $\mathrm{Bohr}_G(\Gamma, \sqrt{2})$ 的幾何意義，並再注意到 $\widehat{1_A}(1)^4 = \alpha^4$，證明 Bogolyubov 引理。
   (d) 如果 A 是 $G = \mathbb{F}_p^n$ 含有 αp^n 個元素的子集，那麼 $2A - 2A$ 中包含維度 $n - 1/\alpha^2$ 的子空間。
   (e) 如果 N 是一個質數，且 A 是 $G = \mathbb{Z}/N\mathbb{Z}$ 含有 $\alpha|G|$ 個元素的子集，則 $2A - 2A$ 中包含長度 $\geq \frac{\sqrt{2}}{2\pi}N^{\alpha^2}$ 的等差數列。

5. 以下要研究 $3A = A + A + A$ 的性質。

   (a) 給 f 是從 G 到 $[0,1]$ 的一個函數，記 $\alpha = \mathbb{E}[f(X)]$。取 $\Gamma = \{\gamma \in \widehat{G} \mid |\widehat{f}(\gamma)| \geq \epsilon\alpha/2\}$，證明 Γ 包含至少 $1/4\alpha\epsilon^2$ 個元素，且

   $$|f * f * f(x+t) - f * f * f(x)| < \epsilon\alpha^2, \quad \forall (x,t) \in G \times \mathrm{Bohr}_G(\Gamma, \epsilon).$$

   (b) 假設 A 是 G 中含有 $\alpha|G|$ 個元素的子集，藉由考慮 $\mathbb{E}[1_A * 1_A * 1_A(X)]$，證明存在 $x_0 \in G$ 使得 $1_A * 1_A * 1_A(x_0) \geq \alpha^3$，由此推得 $x_0 + \mathrm{Bohr}_G(\Gamma, \alpha) \subseteq A + A + A$.

   (c) 如果 A 是 $G = \mathbb{F}_p^n$ 含有 αp^n 個元素的子集，那麼 $3A$ 中包含維度 $n - 4/\alpha^3$ 的射影子空間。

   (d) 如果 N 是一個質數，且 A 是 $G = \mathbb{Z}/N\mathbb{Z}$ 含有 $\alpha|G|$ 個元素的子集，則 $A+A+A$ 中包含長度 $\geq \frac{1}{2\pi}\alpha N^{\alpha^3/4}$ 的等差數列。

■ 第二部分 ■

假設 G 是有限交換群，對於他的一個子集 A 我們希望找到一種方式來度量他表現得像不像等差數列，因此可以定義所謂的 Fourier 權重 $\|A\|_u$ 為

$$\|A\|_u = \max_{\gamma \text{為非平凡特徵}} |\widehat{1_A}(\gamma)|.$$

我們將會在第 3. 小題看到這個定義的合理性。以下對於 G 的任一子集 A，以 $\mathbb{P}_G(A)$ 記 $|A|/|G|$.

1. 證明 $\|A\|_u = 0$ 當且僅當 $A = G$ 或 ϕ.

2. 證明等式鍊 (其中 $x \in G$ 為任一元素)

   $$\|A\|_u = \|-A\|_u = \|G \backslash A\|_u = \|A + x\|_u$$

3. 證明 $\|A\|_u \leq |A|/|G|$，等號成立當且僅當 A 包含在 G 的某個子群的陪集裡。

4. 證明如果 $A \cap B = \phi$，那麼有三角不等式

   $$\|A\|_u - \|B\|_u \leq \|A \cup B\|_u \leq \|A\|_u + \|B\|_u$$

5. 證明

   $$\|A\|_u \geq \frac{\mathbb{P}_G(A)(1 - \mathbb{P}_G(A))}{|G| - 1}.$$

如果今天有一群子集，當他們表現的全都像是等差數列時，那麼他們的和集可能就很小，因為許多項加起來都是一樣的；相反地，如果他們表現的都不像等差數列時和集應該就會很大。因此我們會有一個引理：

6. 假設 $n \geq 3$ 而 $A_1, \ldots, A_n$ 是 G 的子集。藉由考慮 $1_{A_1} * \cdots * 1_{A_n}$ 的 Fourier 變換以及考慮函數 Re (實數部分)，證明對任意 $x \in G$ 總有

$$\left| \frac{1}{|G|^{n-1}} |\{(a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n \,|\, x = a_1 + \cdots + a_n\}| - \mathbb{P}_G(A_1) \cdots \mathbb{P}_G(A_n) \right| \leq \|A_1\|_u \cdots \|A_{n-2}\|_u \sqrt{\mathbb{P}_G(A_{n-1})} \sqrt{\mathbb{P}_G(A_n)}.$$

特別當我們有

$$\|A_1\|_u \cdots \|A_{n-2}\|_u < \mathbb{P}_G(A_1) \cdots \mathbb{P}_G(A_{n-2}) \sqrt{\mathbb{P}_G(A_{n-1})} \sqrt{\mathbb{P}_G(A_n)}$$

時 $A_1 + \cdots + A_n = G$.

7. p 為大於等於 3 的質數，取 $G = \mathbb{F}_p$ 而 $A = \{x^2 \mid x \in G\}$.

   (a) 設 $x \in G$。計算

   $$\left| \sum_{a \in G} \mathrm{e}(-\frac{xa^2}{p}) \right|^2.$$

   (b) 證明 $\widehat{1_A}(a \mapsto \mathrm{e}(ax/p)) \leq \frac{1}{2p} + \frac{1}{2\sqrt{p}}$。因此有 $\|A\|_u$ 的上界。

   (c) 由此證明 $3A = G$.

8. 最後要研究的是在 A 中 4 項等差數列的個數。設 $0 < \delta < 1$，而 p 是模 4 餘 3 的一個質數。取 $G_p = \mathbb{F}_p$ 並定義

   $$A_p(\delta) = \{x \mid x^2 \equiv y \,(\mathrm{mod}\, p),\ |y| \leq \delta p/2\}.$$

   (a) 證明 $\mathbb{P}_{G_p}(A_p(\delta)) = (2[\delta p/2] + 1)/p$.

   (b) 任取 $\gamma \in \widehat{G_p}$，並取 $\xi \in G_p$ 使得 $\gamma = x \in G_p \mapsto \mathrm{e}(x\xi/p)$。由定義寫出

   $$\begin{aligned} \widehat{1_{A_p(\delta)}}(\gamma) &= \frac{1}{p} \sum_{x \in \mathbb{F}_p} 1_{A_p(\delta)}(x)\, \mathrm{e}\left(\frac{-x\xi}{p}\right) \\ &= \frac{1}{p} \sum_{x \in \mathbb{F}_p} \left(\frac{1}{p} \sum_{|b| \leq \delta p/2} \sum_{r \in \mathbb{F}_p} \mathrm{e}\left(\frac{r(x^2 - b)}{p}\right) \right) \mathrm{e}\left(\frac{-x\xi}{p}\right) \\ &= \frac{1}{p^2} \sum_{r \in \mathbb{F}_p} \left(\sum_{x \in \mathbb{F}_p} \mathrm{e}\left(\frac{r(x^2 - b)}{p}\right) \right) \left(\sum_{|b| \leq \delta p/2} \mathrm{e}\left(\frac{-br}{p}\right) \right). \end{aligned}$$

   (c) 證明

   $$\left| \sum_{x \in \mathbb{F}_p} \mathrm{e}\left(\frac{r(x^2 - b)}{p}\right) \right| \leq \sqrt{p}.$$

   (d) 利用第一部分第 2. 小題 (b) 的結果證明

   $$\left| \sum_{|b| \leq \delta p/2} \mathrm{e}\left(\frac{-br}{p}\right) \right| \leq \frac{1}{2 \cdot ||r/p||_{\mathbb{R}/\mathbb{Z}}}.$$

(e) 總結為 $\|A_p(\delta)\|_u = O_\delta\left(\frac{\log p}{\sqrt{p}}\right)$.

9. 我們要證明 Soundararajan 定理：設 $0 < \delta < 1$ 表示一個密度，那麼對所有夠大且模 4 餘 3 的質數 p，$A_p(\delta)$ 都包含至少 $\delta^3 p^2/(2 \cdot 7^3)$ 個 4 項的等差數列。

(a) 注意到 x_1, x_2, x_3 成等差數列當且僅當 $x_1 - 2x_2 + x_3 = 0$，藉由在第 6. 小題中選取夠好的 A_1, A_2, A_3 證明對所有夠大的 p，$A_p(\delta/7)$ 中至少包含 $\delta^3 p^2/(2 \cdot 7^3)$ 個 3 項的等差數列。

(b) 利用恆等式

$$a^2 - 3(a+d)^2 + 3(a+2d)^2 - (a+3d)^2 = 0.$$

證明如果 $A_p(\delta/7)$ 包含 $\{a, a+d, a+2d\}$，那麼 $A_p(\delta)$ 包含 $\{a, a+d, a+2d, a+3d\}$，總結。

Part III

習題解答

沒有那種東西，這只是你的妄想。

-by 江泓