Zeta函數與超越不變量

于靖

數學研究的對象在一般的感覺裡是比較抽象的, 雖然它也有很實際的一面。我自己做數學, 主要是在研究數論。數論探討的是數, 在數學裡它是最古老的一支。但是, 它仍有許多沒有解決的難題。我今天的題目是 Zeta 函數與超越不變量, 就涉及了一些這樣的問題。

我們先從數開始。所謂的數, 在數學裡是指自然數、整數、有理數, 然後是實數。所以, 通常在中學的教科書裡, 畫有一個數線, 先描上原點O, 然後向右等距畫出所有自然數的點, 向左對稱地點出負整數點。再以等分點對應有理數。最後所有的實數點就會塡滿整條數線。

我們用 N 代表所有自然數集合, Z 代表所有整數的集合, Q 代表所有有理數的集合, R 代表所有實數集合。其包含關係如下:

$$N \subset Z \subset Q \subset R$$

數論裡面的難題往往可以很簡潔地描述。一個例子是所謂的費瑪 (Pierre de Fermat, 1601-1665) 問題。方程式

$$X^n + Y^n = Z^n, \quad XYZ \neq 0, \quad n > 2$$

沒有整數解。這個問題經過三個半世紀, 終於在1994年被 Princeton 大學的 A. Wiles 教授證明出來。這個問題的解決, 被認爲是本世紀在數學 (至少是純數學) 裡面最大的進展。

數論的特質之一就是你可以寫下很多這樣看起來很簡單, 中學生都可以了解的問題, 解答起來卻是非常困難。對數論有興趣的人, 往往會花很多的時間, 總其一生的精力, 試圖去證明或解決這樣的問題。

實數裡有一個很特別的數,

$$\pi = 3.14159265358979323846264338\cdots。$$

它不是有理數, 甚至不是任何整係數方程式的根, 這種數叫做超越數。π 在小學數學裡就開始教了, 但是它其實是一個不容易的觀念。我們說 π 是一個不變量, 不論你畫那一個圓, 圓周長和直徑的比例是不變的, 這個比例就是 π。如果你實際去算的話, 就會一直不斷地寫下小數點後面的數字來。然後你就會發現, 這些數目字其實是非常非常不規則。小學生碰到 π 的時候, 通常有一個疑惑, 就是 π 到底是多少。你如果只寫下有限個位數, 其實並不正確。正確的方式是要一直寫下去, 小數點右邊不能停下來。寫得愈多位數就愈接近眞正的 π。既然這些小數點後面的數目字出現得雜亂無章, 這樣子的一個數, 你怎麼去了解它呢?

所謂 π 是超越數的意思是說, 它不滿足任何一個代數方程式:

$$a_0+a_1\pi+\cdots+a_n\pi^n=0, \text{ 其中 } a_i \text{ 是整數。}$$

這是 Lindemann 在1882年證明的事。當時證明了這個定理被認爲是十九世紀最重要的數學成就之一。

我們爲什麼要去證明「π 不會是任何一個整係數代數方程式的根」這樣的事呢? 假如它滿足了某一個代數方程式, 找到這個方程式就能夠提供我們有關它的重要的資訊, 要了解它就容易多了。所以爲了要眞正了解這一個很實際的數, 就必須先確定它是否滿足某代數方程式。如果一個數滿足某個整係數代數方程式, 就稱爲代數數。否則就稱之爲超越數。但是在數學上不能因爲你找不到這樣一個方程式就說它沒有。因爲可能是有而你還沒找到。所以唯一能夠說它沒有的方式, 就是你必須去證明。眞正從邏輯上去證明, π 不滿足任何代數方程式。這是很困難的事, 是數學家經歷了兩百年才證明出來的一件事情。

一個有理數如果以十進位數展開, 寫出的數目字就會相當規則。也許某位數以後都是0, 也就是只有有限的位數。不然的話, 它所出現的數目字就會是循環的, 也就是說往小數點右方繼續展開下去會有週期的現象。π 是一個超越數, 就表示在它的小數展開裡, 數目字出現得相當複雜、相當不規則。一個基本的問題是: 我們如何掌握或描述一個數的「複雜程度」。這個問題到今天還沒有完全解決。我們仍然沒有一個滿意的方法, 把所有的數按複雜程度去分類。像 π 這個數, 它不滿足任何代數方程式, 你只能一步一步的去接近它, 近似它。這其實已經不是容易的事了。1950 年代電腦剛誕生在 Princeton 時, 數學家就用電腦來計算 π, 可以近似到小數點之後兩仟位。現在用最新的超級電腦, 可以算到幾十億位。從兩仟位到幾十億位, 這中間不只是電腦硬體的進步, 計算方法更有大幅的改進。計算方法的改進就是數學, 也就是說你必須找到更好的數學方法去作數值近似。從古希臘、祖沖之、牛頓到現代, 數學家仍持續不斷的在找尋更好的數學方法去近似 π。

從 π 再回到最基本的數: 整數。在整數中間作除法, 就引進了有理數。令 Q 是所有的有理數所成的集合, 在這集合裡就可以做加、減、乘、除四則運算。這樣的一個結構, 我們叫做體。所有實數 R 也構成一個體, 比 Q 更大的體。複數 C 又構成一個更大的體。

爲了要深入探討像 Q 這樣一個體, 數學家引進了特別的工具來輔助研究。Zeta函數就是這樣的一種工具

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\quad \mathrm{Re}(s)>1.$$

這是上世紀中 Riemann 所寫下的 Riemann Zeta 函數, 是一個無窮級數。其中 s 表示一個複數變數, 在複數平面上跑, 原先的數線是複數平面上的 x-軸, y-軸表示虛數軸, 其上的點對應所謂的純虛數。這個 Zeta 函數級數裡的每一項是 $\frac{1}{n^s}$ 的形式, n 是正整數。

引進這種特殊的函數, 似乎是很唐突的事, 不知從何處冒出來, 但是這一步對於整個數學的發展卻是相當關鍵的。在 Riemann

之前, 已經有很多跡象出現。早他一百年, Euler 就發現了以下的公式, 對於偶數 m

$$\zeta(m)=\sum_{n=0}^{\infty}\frac{1}{n^m}=\frac{-(2\pi\sqrt{-1})^m}{2m!}B_m.$$

把偶數 m 代進 s, 就是 Zeta 函數在 m 的取值, 左邊的 B_m 是一個有理數的數列, 稱爲 Bernoulli 數, 它們可以很容易的從指數函數 e^z 的冪級數展開算出來:

$$\frac{z}{e^z-1}=\sum_{m=0}^{\infty}B_m\frac{z^m}{m!}.$$

$B_0=1, B_1=-1/2, B_2=1/6, B_3=0,$
$B_4=1/30, B_5=0,\ldots$

Euler發現的這個公式到底有什麼意思呢? 首先, 這個式子是出人意之外的, Zeta 函數和超越不變量 π 分別出現在等式的兩邊。π 原來是從圓周長來的, 因而表示圓和 Zeta 函數是有關聯的, 也表示指數函數和 Zeta 函數是有關聯的。π 在數學裡之所以非常重要, 就是因爲它會在許多令人意外的關鍵場合很漂亮地出現。Euler這個式子背後其實隱藏著許多豐富的現象。

由 Euler 的公式我們知道 $\zeta(2)$ 是 π^2 乘上一個特別的有理數, $\zeta(4)$ 是 π^4 乘上一特別的有理數, 等等。因此我們完全清楚了 $\zeta(2),\zeta(4),\ldots$, 因爲 π 是超越數, 這些函數值當然也是超越數。

如果令變數 s 趨近於1, $\zeta(s)$ 的值會趨近無窮大, 但是只要複數 s 的實部大於1, 級數和都會收斂, 除了 $2,4,6,\ldots$ 等偶數點的取值, 當然也可以讓 Zeta 函數在 $3,5,7,\ldots$ 等大於 1 的奇數上取值, 可是這就發生問題了, 不僅 Euler 不知道 $\zeta(3),\zeta(5),\ldots$, 直到今天我們仍然幾乎什麼都不知道。唯一知道的事是1978年法國數學家 R. Apery 證明出 $\zeta(3)$ 不是有理數。連 $\zeta(5)$ 是不是有理數都還不知道。

Apery 能夠證明 $\zeta(3)$ 不是有理數是因爲他得到另一個算式

$$\zeta(3)=\sum_{n=1}^{\infty}\frac{1}{n^3}=\frac{5}{2}\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^3\begin{pmatrix}2n\\ n\end{pmatrix}}$$

等式中間的級數及右邊的級數各給了一個方式去近似 $\zeta(3)$, 所不同的是以右邊的級數去近似速度上會快很多。能夠多快的去逼近一個實數是一個關鍵, 涉及了一個基本現象: 如果能寫下一個數列“不太慢”的去近似一個數而不碰到那個數, 那個數就必然不是有理數。原來用來定義 $\zeta(m)$ 的級數, 缺點就是收斂的太慢, 取近似值時速度也太慢。當初 Euler 研究他的公式就是先去作數值計算 $\zeta(2),\zeta(4),\ldots$, 他發現級數走得太慢, 因此想找出更好的線索。經過幾年努力他猜到了公式, 然後又經過十餘年才證明出他的公式。

對於一個我們有興趣的數, 像 π, 很重要的問題是能找到多快的方法去近似它。前面談過近幾十年來 π 的近似值計算, 所以能算出幾十億位除了電腦進步外, 就是因爲數學家還一直在努力找更好更快的方法去近似 π。這裡所涉及的深奧數學, 不只關係到一個數是否是有理數, 也關係到一個數是否是超越數。早在上世紀 Liouville 就已發現, 如果我們能夠足夠快的去近似一個數而不碰到那個數, 則那個數就應該是超越數。問題是這兒所

謂速度足夠快到底要多快, 須要精確的研究。速度是跟用以近似的有理數的分母以及誤差相關。這個問題經過百年研究到1956年倫敦大學的 Roth 才完全解決。他的工作隨後就獲得了國際數學會的 Fields 獎。

如同自然界的許多現象, 數學現象往往也可以推得很廣, 可以有很多的變化, 並以很多不的形式呈現。與上述求近似值類似的一個現象是去考慮空間。數與空間都是數學裡研究的基本對象。中央研究院已故周煒良院士有一個很有名的定理, 是說在複數射影空間裡, 解析子空間一定也是代數子空間。代數子空間就好比是代數數, 是可以由一組多項式來描述的。解析子空間就像是實數, 放在射影空間中受到了限制, 就必須是代數子空間。根據陳省身院士的說法, 周院士的這個定理, 當初部分的靈感就是來自「有理數逼近實數時, 如果速度受限, 能被逼近的數就必須是代數數這個事實」。陳院士與周院士年輕時曾經一起在德國做研究, 知曉這個周定理與數論中有理數近似代數數的關聯典故。兩年前陳院士在美國數學會紀念周院士的文章裡, 還特別寫出了這個故事。

再回到 Zeta 函數。我們可以把 Riemann Zeta 函數看成定義在複數平面上的解析函數。原本的定義級數只有在 s 的實部大於1才收斂, 但是藉著所謂解析延拓, 我們可以讓它生長在整個複數平面上。然後, 這個函數就會有一種對稱性, 並滿足一個函數方程式。

$$\Lambda(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s),$$
$$\Lambda(s) = \Lambda(1-s).$$

這裡對稱性是說函數 $\Lambda(s)$ 在 s 與1-s 的取值完全一樣。在實數 $s=1/2$ 作垂線, 把複數平面分爲兩半, 則 $\Lambda(s)$ 在左右兩個半平面是完全對稱的。回到 Zeta 函數, 這個對稱性告訴了我們 Zeta 函數在負整數點的取值。在負偶數, Zeta 函數值是0; 在負奇數 Zeta 函數的取值是把 Euler 公式中 π 的乘冪扔掉後所剩下的有理數。

由於 Zeta 函數很對稱, 它的零根也應是對稱的。這個對稱性就產生了一個數學上最重要的問題, Riemann猜想: Zeta 函數所有的零根, 除了負偶數外, 都正好落在實部等於 1/2 的 x-軸垂直線上。這個 Riemann 猜想可以導出很多有用的結果, 從有關質數的分佈到理論計算機科學上的重要結果。很多數學家甚至認爲, 繼 Fermat 問題解決之後, Riemann 猜想是廿一世紀數學研究致力的最大目標。

Riemann Zeta 函數既然是很重要而牽連甚廣的函數, 與它性質相近的函數當然也是很有意思的。於是數學家考慮廣義的 Zeta 函數, 這些函數都生長在複數平面上, 都有對稱性而滿足適當的函數方程式。對每一個這種 Zeta 函數也都可以作 Riemann 猜想, 而它們在整數點的取值也應該都是很微妙的不變量。雖然對任何一個這種 Zeta 函數我們並沒有更多知識, 但是考慮這些函數仍然可以發揮很大的作用。Wiles 解決 Fermat 問題時就用到廣義的 Zeta 函數。

解決 Fermat 問題, 要用反證法: 假定有解, 然後找出矛盾。首先假定有非零整數 a, b, c 使

$$a^l + b^l = c^l$$

其中 l 是固定奇質數。依 Frey 的建議, 再考慮方程式

$$y^2 = x(x-a^l)(x+b^l)$$

對任何與 abc 互質的質數 p, 考慮二元同餘方程式

$$y^2 = x(x-a^l)(x+b^l)(\bmod p)$$

解出同餘解的個數爲 $p-a_p$。然後從數列 $\{a_p\}_p$依一定方式擴充到一個數列$\{a_n\}_{n=1}^{\infty}$, 再作函數

$$\mathcal{S}_{abc}(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

這個 Zeta 函數也有一種對稱性, 它滿足函數方程式:

$$\Lambda(s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s)\mathcal{S}_{abc}(s),$$
$$\Lambda(s) = \pm\Lambda(2-s),$$

其中 N 是一個與 a,b,c 有關的正整數。從這個 $\mathcal{S}_{abc}(s)$, 根據 Ribet 的理論, 可以跳到另一個 Zeta 函數, 滿足同型的函數方程式。但是 N 可以降下來, 一直到降到2爲止。然後從這種複變函數理論裡, 可以導出滿足上述方程式的這種 Zeta 函數只有零函數。因此這種函數不可能存在。因而, 一開始始作俑者的 Fermat 方程式整數解 a,b,c 必定原來就是不能存在的!

Zeta 函數 $\zeta_{abc}(s)$ 在這兒是作爲一個相當複雜的工具。有點像在中學幾何裡面畫輔助線, 要走很遠的路, 寫很長的論文, 證明很多細節, 最後才導出矛盾。

我個人特別有興趣的是另外一種 Zeta 函數, 來自所謂的有限體。體是一個集合, 對裡面的元素你可以做加、減、乘、除。這個集合可以只有有限個元素, 就叫做有限體。一個有限體的元素個數一定是一個質數 p 的乘冪 q。這個時候, 這個體就是所謂的特徵 p 的體, 裡面任何一個元素把它自己加了 p 次以後就變成零了。也就是說, 在它的世界裡面你是走不遠的, 你走了 p 步就一定走回原點。這樣的一個世界雖然怪, 其實是有用的。在現代理論計算機科學裡面, 很多地方就是可以用到有限體, 例如涉及網路安全的密碼學。

一個有限體只是一個有限的集合, 看起來很簡單。我們把這個體的元素來做係數, 然後再加上一個變元 t。這樣以加、減、乘運算得到集合稱爲多項式環 $A = F_q[t]$。裡面的元素就是多項式, 係數在有限體裡: $\sum_{i=0}^{n} c_i t^i$, $i \in F_q$。這樣子寫多項式的時候, 可以把它看成像整數的十進位展開, 係數就是一種 digits。這些多項式運算起來就像原來的整數, 雖然走了 p 步就一定走回原點。在原來的數的世界裡面, 當然沒有這樣的性質。可是另外一方面, 它的加乘等很多性質是跟整數很像的。所以這些多項式其實是一種不同世界裡的整數。

從整數做除法可以得到分數。從多項式做除法也可以得到有理式, 或叫它有理函數。這些有理函數所成集合可以做加減乘除, 因此構成一個體, 就是所謂的函數體 $K = F_q(t)$, 相當於原來的有理數體。我們把有理數體放到實數體裡填充成一條數線, 在這裡也可以把函數體放入一條函數線。當然這裡

的線已經不是通常的直線。它的點對應的是一種冪級數, 以 $\frac{1}{t}$ 爲變元的冪級數。寫成

$$c_nt^n+\cdots+c_0+\frac{c_{-1}}{t}+\frac{c_{-2}}{t^2}+\cdots,\quad c_i\in F_q。$$

它的左半邊爲多項式, i 走到某個 n 爲止, 右半邊的級數, i 從 $-1,-2,-3,-4,\ldots$, 可以一直走下去。這個無窮係數序列 c_i, 就像一個實數的無窮多個 digits。所有這些冪級數構成一個體 $F_q((\frac{1}{t}))$。

在六十年前, 美國 Carlitz 引進了下面的 zeta 函數, 對正整數 m:

$$\zeta_c(m)=\sum_{\substack{a\in A\\ a\ monic}}\frac{1}{a^m}\in F_q((\frac{1}{t}))$$

如同作 Riemann Zeta 函數, 把多項式當成整數, 然後把它倒過來取它的乘冪。原來祇取正整數做, 現在就取那些首項係數是1的多項式來做級數的項。整個無窮級數加起來之後, 它的極限值仍然會在體 $F_q((\frac{1}{t}))$ 裡。

這些值 $\zeta_C(m)$ 是很有意思的。Carlitz 發現了以下的現象: 當 m 是 $q-1$ 的倍數的時候, 可以得到一個公式, 很像 Euler 原來對 Riemann Zeta 函數所得到的公式

$$\zeta_C(m)=\frac{\widetilde{\pi}^m\widetilde{B}_m}{\Gamma_{m+1}}$$

其中 Γ_m 是多項式的階乘, 定義是先定 $D_0=1, D_i=(t^{q^i}-t^{q^{i-1}})\cdots(t^{q^i}-t)$ 若 $i\geq 1$, 然後寫下 m 的 q 進位展開 $\sum_{i=0}^{\infty}m_iq^i$, 再定 $\Gamma_{m+1}=\prod_{i=0}^{\infty}D_i^{m_i}$。Bernoulli-Carlitz數 $\widetilde{B}_m$ 是有理函數的序列, 它的定義是從 Taylor 展開式得來:

$$\frac{z}{\exp_c(z)}=\sum_{n=0}^{\infty}\widetilde{B}_n\frac{z^n}{\Gamma_{n+1}}$$

其中$\exp_c(z)$是 Carlitz 指數函數$\exp_c(z)=\sum_{i=0}^{\infty}\frac{z^{q_i}}{D_i}$。這個 Carlitz 指數函數也是一種週期函數, $\widetilde{\pi}$ 就是它的基本的期, 是一個像圓周率乘上 $2\sqrt{-1}$ 那樣的不變量。

公式裡有一個 $\widetilde{\pi}$、有理函數 $\widetilde{B}_m$、以及階乘多項式 Γ_{m+1}。在原來 Euler 的公式裡面, m 必須是偶數, 因爲整數裡面只有兩種符號 (sign):+1,−1。在有限體 F_q 的世界裡面卻有 $q-1$ 種符號, 有限體裡每一個非零元素都對應一個符號。公式要成立 m 就必須是符號個數的倍數。所以在 Euler 的公式裡 m 是2的倍數, 而在 Carlitz 的公式裡 m 是 $q-1$ 的倍數。

就像圓周率 π, $\widetilde{\pi}$ 也應是所謂的超越數。也就是說, 它不會滿足任何一個多項方程式:

$$a_0+a_0\widetilde{\pi}+\cdots+a_n\widetilde{\pi}^n=0$$

方程式的係數 a_i 是在多項式環 A 裡。因爲這裡的 A, 就扮演了原來的整數集合的角色。$\widetilde{\pi}$ 的超越性是 Carlitz 的學生 Wade 證明的。把 $\widetilde{\pi}$ 除以 t^q-t 的 $q-1$ 次根就得到一個 $F_q((\frac{1}{t}))$ 裡的超越數。這裡的超越數表面上看起來夠奇怪。但是從另一角度來看, 卻有更好的性質。

二十年前, 法國數學家 Christol-Cobham 發現: 在 $F_q((\frac{1}{t}))$ 這個世界裡面, 數的複雜性可以有比較好的描述。譬如:

$$c_nt^n+\cdots+c_0+\frac{c_{-1}}{t}+\frac{c_{-2}}{t^2}+\cdots,\quad c_i\in F_q,$$

它是否滿足代數方程式的充要條件正好是看係數序列 c_i 是不是可以由一個有限 Automata 來辨識。有限 Automata 其實就是最簡單的電腦, 只有有限個 state。前面說過到今天我們仍然沒有一個滿意的方法, 把通

常的數按複雜程度去分類。但是對 $F_q((\frac{1}{t}))$ 裡的數的複雜程度, 卻可以翻譯成電腦科學的話去描述。電腦科學中不同的計算複雜階層, 從有限 Automata 到 Turing machine 正好可以用來呈現 $F_q((\frac{1}{t}))$ 裡的數的複雜程度。

回到我們研究的問題上。對於 Carlitz 的這些 zeta 值 $\zeta_C(m)$, 我們想要了解。這裡有一個特別有意思的現象, q 可以是任何質數的乘冪, 最小可以是2。當 q 是2的時候, $q-1$ 就是1。因而 $F_q((\frac{1}{t}))$ 的世界是一個沒有 sign 的世界。每一個數乘上 -1 都是自己, -1 等於1。在這個沒有 sign 的世界, 就有一個簡單的結論, 任何整數都是 $q-1$ 的倍數。於是 Carlitz 公式清楚的告訴了我們所有的 $\zeta_C(m)$。一般情形下 q 不是2, 當 m 不是 $q-1$ 的倍數的時候, 我們仍然有興趣這些 zeta 值。就像原來古典數論裡 Euler 的問題, 要了解 $\zeta(3), \zeta(5), \ldots$。

在1991年, Anderson-Thakur 與我合作解決了上述的的問題。對於任意 q 我們都得到 $\zeta_C(m)$ 的完整了解。這裡 m 只要是正整數, 即使 m 不是 $q-1$ 的倍數, 我們也能清楚的知道 $\zeta_C(m)$, 並且證明它是超越數。不只是如此, 我們更知道, 在 m 不是 $q-1$ 的倍數的時候, $\zeta_C(m)$ 和 $\tilde{\pi}^m$ 之間的比例一定也是超越數。這是一個出乎意料之外的進展。在 $F_q((\frac{1}{t}))$ 這個比較怪的世界裡面, Euler的問題竟然完全解決了。這是三百年來古典數論想做而不能夠做到的事情。很多數學家曾經問過以下的問題: 當 m 是奇數時, $\zeta(m)$ 和 π^m 之間的比例是否是有理數? 因爲當 m 是偶數時 Euler 的公式說 $\zeta(m)$ 和 π^m 之間的比例確是有理數。我們得到的結果顯示答案可能是否定的。不僅 $\zeta(m)$ 和 π^m 之間的比例不應該是有理數, 它甚至不可能是代數數。當然, 我們的證明是在一個不同的世界, 對不同種的 zeta 值。因此邏輯上並沒有回答上面的問題, 只是給了一點啓示。也就是說, 合理的猜想應是: Riemann Zeta 函數在整數點的取值會產生無窮多個超越不變量。π 是裡面最簡單的一個, 其它 $\zeta(3), \zeta(5), \ldots$, 會得到一串無窮多個代數上不相關的超越不變量。

有一次在 Princeton, Fields 獎得主 Bombieri 與 Deligne 跟我談起這個 Zeta 函數值的工作。他們認爲: 證明當 m 是奇數時 $\zeta_C(m)$ 和 $\tilde{\pi}^m$ 之間的比例也是超越數, 是極漂亮的事。這兩個值本應該是沒有關係的, 但是在過去, 沒有人能舉出任何道理來說明它們沒有關係。我們所做的工作, 讓他們可以完全相信這個 Riemann Zeta 函數值的問題有朝一日也可以解決。

π 來自於圓。$\tilde{\pi}$ 也來自一種對稱結構。在數學的術語裡, 對稱結構其實是有一個群在作用。例如圓, 你可以讓整數加法群作用, 也就是說, 圓可以轉整數倍的角度。因此, 把這個觀念推廣就可以以所謂的交換代數群來取代圓的觀念。從這幾句話, 數學家大概用了百年的時間去發展。現代的高等數論的核心就在這裡。我們可以想像 $\tilde{\pi}$ 來自於函數體的圓, 是不同世界裡另一種圓。這種圓上不是整數在作用, 而是多項式在作用。從古典的圓推廣到多項式在作用的對稱結構更是走了一大步, 經過 Carlitz 引進 Carlitz 模到 Drinfield

在三十多年前所發展出的 Drinfield 模理論。這一大步對於數論以及算術幾何有很大的影響, 因此 Drinfield 也是 Fields 獎得主。

要去證明 π 或 $\tilde{\pi}$ 是超越數, 對稱結構扮演相當關鍵的角色。所謂指數函數, 就是用來參數化圓或 Carlitz 模的函數, 它們可以把整數或多項式的非線性作用轉化爲線性作用。指數函數總是週期函數, $2\pi\sqrt{-1}$ 或 $\tilde{\pi}$ 就是它們的基本週期。我們能證明 π 或 $\tilde{\pi}$ 是超越數, 也就是因爲它們是有理對稱結構的週期。爲什麼能證明當 m 是奇數時 $\zeta_C(m)$ 和 $\tilde{\pi}^m$ 之間的比例也是超越數, 則是因爲它們是不同的有理對稱結構的週期。這裡的一個靈感來自 Hilbert 第七問題。

在 1900 年的時候, 德國領導數學家 Hilbert 在世界數學大會上曾經給了一個演講, 列出了二十三個二十世紀的主要數學問題。其中第七問題是說: 如果 $a \neq 0, 1$ 與 b 都是代數數, 而 b 不是有理數, a^b 是否是超越數? 這個當時被認爲極困難的問題, 在 1934年的時候就被俄國 Gelfond 證明了。他發現: 任何兩個代數數的對數, 如果他們的比例不是有理數, 就必須是超越數。這些比例不可能是非有理的代數數。譬如說, 它不可能是 $\sqrt{2}, \sqrt{3}, \ldots,$ 不可能滿足任何代數方程式而不是有理數。它祇能滿足一次的方程式, 或者任何代數方程式都不滿足。在30年代很多人就猜想這個基本的現象可以推廣到不只是兩個對數, 而是任意有限個代數數的對數。從這個猜想可以導出很多的重要結果。因此1966年 Baker 解決它之後就得到 Fields 獎。

這個有關代數數對數的重要基本現象, 即使走到有限體上函數體的不同世界仍然存在。那就是我的發現。佈於函數體的對稱結構 Drinfield 模有它的指數函數, 也有它的對數函數, 包括高維的對數向量。週期則可以看成廣義的代數數對數。這中間, 雖然表面上看起來是完全不同的世界, 但是追根究底到了關鍵的地方, 是有異曲同工之妙。Anderson-Thakur 證明了 $\zeta_C(m)$ 是某種 m 維 Drinfield 模上代數向量的對數。當 m 是奇數時,$\zeta_C(m)$ 和 $\tilde{\pi}^m$ 之間的比例不是有理函數, 所以根據我的定理它是超越數。在古典數的世界裡, 我們猜想 Riemann Zeta 函數值 $\zeta(m)$ 和 π^m 也是某種對稱結構的代數向量的對數, 這種對稱結構稱爲 Motives。可是因爲瞭解不夠, 目前無法證明任何事。

一旦走進函數體的世界, 就可以做相當多事情。我只能舉出其中一小部份。在函數體的世界, 不只是可以從直線的有理函數體出發, 其實還可以從任意曲線的函數體出發。所以我們可以有一整套全新的現象衍生出來。

—本文作者爲中央研究院數學所研究員—