2018-12-24

2019-01-22

何谓 abc 猜想?

北京大学数学科学学院
李文威

- 数论是以整数或相关数学结构为主题的研究. 问题往往极初等, 使用的工具和思想却无远弗届.
- 深刻的数论问题往往同时牵涉整数的
  - 乘法性质 (譬如因数分解, 素数),
  - 加法性质 (譬如拆分).

  例如 **Goldbach 猜想**: 任何 ≥ 4 的偶数可以写成两个素数之和.

以下将探究的个案是年代较近, 牵涉却极广的 **abc 猜想**.

相对初等的参考材料有:

E. Bombieri, W. Gubler, *Heights in Diophantine Geometry* (2006), Chapter 12.

M. Waldschmidt, *Lecture on the abc conjecture and some of its consequences* (2015).

abc 猜想初貌

若 N 为非零整数, 定义

$$\mathrm{rad}(N) := \prod_{\substack{p:\text{素数} \\ p|N}} p.$$

强 abc 猜想 (J. Oesterlé, D. W. Masser, ∼1986)

对于任意实数 $\epsilon > 0$, 存在常数 $C(\epsilon) > 0$ 使得当

- $a, b, c \in \mathbb{Z}_{\geq 1}$ 两两互素, 而且
- $a + b = c$ 时,

$$c < C(\epsilon)\mathrm{rad}(abc)^{1+\epsilon}.$$

互素条件是必要的. 今后简称为 **abc 猜想**.

David Masser

Joseph Oesterlé

图片取自 Oberwolfach Photo Collection

等价的表述

对于任意实数 $\epsilon > 0$, 存在常数 $C(\epsilon) > 0$ 使得: 若 $a, b, c \in \mathbb{Z} \setminus \{0\}$ 互素, $a + b + c = 0$, 则:

$$\max\{|a|, |b|, |c|\} < C(\epsilon)\mathrm{rad}(abc)^{1+\epsilon}.$$

1. 猜想中不能取 $\epsilon = 0$ (Stewart–Tijdeman).
2. 条件可以放松为特定的 ϵ, 例如 $\epsilon = 1$ 情形 (弱 abc 猜想).

除了大量数值计算的支持, 目前也已有对数版本的上界: 存在 $K > 0$ 满足

$$\log c < K \cdot \mathrm{rad}(abc)^{\frac{1}{3}+\epsilon}.$$

(Stewart–Yu, 2001)

abc 猜想的推论: Fermat 大定理

设 $x, y, z \in \mathbb{Z} \setminus \{0\}$ 互素, 满足 **Fermat 方程**

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

在 abc 猜想的等价表述中取 $(a, b, c) := (x^n, y^n, -z^n)$. 命 $M := \max\{|x|, |y|, |z|\}$, 容易检查 $M \geq 2$, 而且

$$\begin{aligned} M^n &< C(\epsilon)\mathrm{rad}\left(x^n y^n z^n\right)^{1+\epsilon} \\ &= C(\epsilon)\mathrm{rad}(xyz)^{1+\epsilon} \\ &\leq C(\epsilon)|xyz|^{1+\epsilon} \leq C(\epsilon)M^{3+3\epsilon}. \end{aligned}$$

对给定的 ϵ 和 $C(\epsilon)$, 上式表明 n 充分大时方程无解. □

注记

Fermat 大定理断言 $n \geq 3$ 时方程 $x^n + y^n = z^n$ 没有满足 $xyz \neq 0$ 的整数解; 这已由 R. Taylor 和 A. Wiles 通过**椭圆曲线**的模性证明 (1995).

abc 猜想的推论: Pillai 猜想

形如 a^b 的正整数 ($a \in \mathbb{Z}_{\geq 1}$, $b \in \mathbb{Z}_{\geq 2}$) 称为完全幂. 所有完全幂按大小排成数列

$$1, 4, 8, 9, 16, 25, 27, 32, \ldots$$

Pillai 猜想 (1945)

相邻两个完全幂的差趋近于 $+\infty$.

对给定的 $k \geq 1$, 我们希望证明 $x^p - y^q = k$ 的正整数解 (x^p, y^q) 有限, 其中 $p, q \in \mathbb{Z}_{\geq 2}$. 取 $d := \gcd(x^p, y^q, k)$ 和 $(a, b, c) := (x^p/d, -y^q/d, -k/d)$ (互素, $\sum = 0$).

- $\operatorname{rad}(abc) \leq xyk$.
- 代入 abc 猜想: $x^p/d \leq C(\epsilon)(xyk)^{1+\epsilon}$. 因为 $d \leq k$ 而 $y^q \leq x^p$,

$$x^p \leq C(\epsilon)k^{2+\epsilon}(xy)^{1+\epsilon} \leq C(\epsilon)k^{2+\epsilon}x^{\left(1+\frac{p}{q}\right)(1+\epsilon)}.$$

省略仅依赖 (ϵ, k) 的常数, 将先前的不等式简写为

$$x^p \ll_{\epsilon,k} x^{\left(1+\frac{p}{q}\right)(1+\epsilon)}.$$

- 若 $p \geq 3$, 则 $1+\frac{p}{q} \leq 1+\frac{p}{2} \leq \frac{5p}{6}$, 取 ϵ 充分小使得 $\left(1+\frac{p}{q}\right)(1+\epsilon) \leq \frac{6p}{7}$, 那么 $(x^p)^{1/7} \ll_{\epsilon,k} 1$. 仅有有限多个 x^p.
- 若 $p=2$, $q \geq 3$: 类似地, $1+\frac{p}{q} \leq 1+\frac{p}{3} \leq \frac{5p}{6}$. 同样推导上界.
- 若 $p=q=2$: 方程 $x^2-y^2=k$ 仅有有限多个正整数解 (x,y).

这就说明 abc 猜想蕴涵 Pillai 猜想. $\square$

类比: 多项式的 abc 猜想

设 K 特征为 0 的域 (不妨取 $\mathbb{C}$). 以多项式环 $K[X]$ 代替 $\mathbb{Z}$, 以有理函数域 $K(X)$ 代替 $\mathbb{Q}$.

- $K[X]$ 的代数性质和 $\mathbb{Z}$ 类似; 其上仍有唯一分解定理, 不可约首一多项式扮演素数的角色.
- 对于非常值多项式 $f \in K[X]$, 命

$$\operatorname{rad}(f) := \prod_{\substack{p \in K[X]:\text{不可约首一} \\ p \mid f}} p$$

$$= \text{以 } f \text{ 的根为单根的首一多项式.}$$

定理 (Mason–Stothers, 1981)

设 $a, b, c \in K[X]$ 非常值多项式, 两两互素并且 $a + b + c = 0$, 那么

$$\max\{\deg a, \deg b, \deg c\} \leq \deg \operatorname{rad}(abc) - 1.$$

可以设想为整数的 abc 猜想在多项式情形的类比.

证明. 对变元 X "形式地" 求导, 得到

$$\begin{pmatrix} 1 & 1 & 1 \\ \frac{a'}{a} & \frac{b'}{b} & \frac{c'}{c} \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = 0.$$

左式的秩为 2, 否则 $\frac{a'}{a} = \frac{b'}{b} = \frac{c'}{c}$ 将导致 a, b, c 有公因式. 记

$$\deg(f/g) := \deg f - \deg g, \quad (\log f)' := \frac{f'}{f} = \sum_{p:\text{首一不可约}} n_p \cdot \frac{p'}{p}$$

其中 n_p 是 p 整除 f 的次数. 线性代数表明 $\exists\, \lambda \in K(X)$ 使得

$$\lambda\,(a, b, c) = \left((\log c)' - (\log b)', (\log a)' - (\log c)', (\log b)' - (\log a)'\right).$$

对 $\heartsuit \in \{a, b, c\}$, 上式蕴涵 $\deg \lambda + \deg \heartsuit \leq -1$. 另一方面,

$$\begin{aligned} \operatorname{rad}(abc) \cdot \text{右式} \in K[X]^3 &\implies \operatorname{rad}(abc)\lambda \cdot (a, b, c) \in K[X]^3 \\ &\overset{a,b,c\text{ 互素}}{\implies} \operatorname{rad}(abc)\lambda \in K[X] \implies \deg \operatorname{rad}(abc) \geq -\deg \lambda. \end{aligned}$$

证毕. □

Mason–Stothers 定理蕴涵多项式版本的 Fermat 大定理.

推论

设 $u, v, w \in K[X]$ 互素, 非常值, 并且满足 $u^n + v^n = w^n$, 其中 $n \in \mathbb{Z}_{\geq 1}$, 则 $n < 3$.

证明: 我们有

$$\begin{aligned} n \max\{\deg u, \deg v, \deg w\} &\leq \deg \operatorname{rad}(u^n v^n (-w^n)) - 1 \\ &= \deg \operatorname{rad}(uvw) - 1. \end{aligned}$$

若 $n \geq 3$ 则左式 $\geq \deg(uvw) \geq \deg \operatorname{rad}(uvw)$, 矛盾. $\square$

数学之外

- 数论学家 D. Goldfeld 认为 abc 猜想是不定方程的研究中最重要的未解问题.
- 尽管 abc 猜想的表述简单, 其威力之大不免使人惊且疑.
- 假若我们相信数学中存在某种 “困难度守恒律”, 则 abc 猜想大概不会有容易[1]的证明.
- 尽管如此, 研究 abc 猜想的种种等价形式和相关的工具, 对于推进 (和学习) 数学有实实在在的帮助.

[1]至少得比 Taylor–Wiles 对 Fermat 大定理的证明容易.

abc 猜想简史

1. Masser 和 Oesterlé 的 abc 猜想主要源于对椭圆曲线的 Szpiro 猜想的思考.

   J. Oesterlé, *Nouvelles approches du "théorème" de Fermat*, Astérisque, Séminaire Bourbaki, Exp 694.

2. 多项式情形起源更早 (W. Stothers, 1981; R. C. Mason, 1984).

椭圆曲线是一类特殊的平面曲线, 带有指定的 "零点". 何谓代数曲线? 代数几何提供了一套完整理论, 简单起见, 这里只论平面代数曲线.

平面代数曲线

- 域 K 上的**平面代数曲线**是由多项式方程描绘的几何对象:

$$f(X,Y)=0,\quad f\in K[X,Y].$$

- 几何上, 更容易操作的对象是射影平面

$$\mathbf{P}^2 := \left\{\ell\subset K^3 : \text{一维子空间}\right\} = \left\{(X:Y:Z) : \text{不全为零}\right\}$$

其中 $(X:Y:Z)$ 代表向量 (X,Y,Z) 张出的直线.
平面借由 $(X,Y)\mapsto(X:Y:1)$ 嵌入 $\mathbf{P}^2$. 所以

$$\mathbf{P}^2 = \underbrace{\text{平面}}_{\text{“仿射部分”}} \sqcup \underbrace{\left\{(x:y:0) : x,y\in K,\ \text{不全为零}\right\}}_{\text{“无穷远点”}}.$$

- 平面曲线 $f(X,Y)=0$ 自然地延拓为 $\mathbf{P}^2$ 中的**射影曲线**, 由齐次多项式方程 $Z^{\deg f} f\left(\frac{X}{Z},\frac{Y}{Z}\right)=0$ 定义.
- 曲线光滑 $\iff$ 处处有良定义的切线 (用 ∇f 确定).

椭圆曲线

椭圆曲线的初等定义: 由 **Weierstrass 方程**

$$\text{仿射部分：} Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

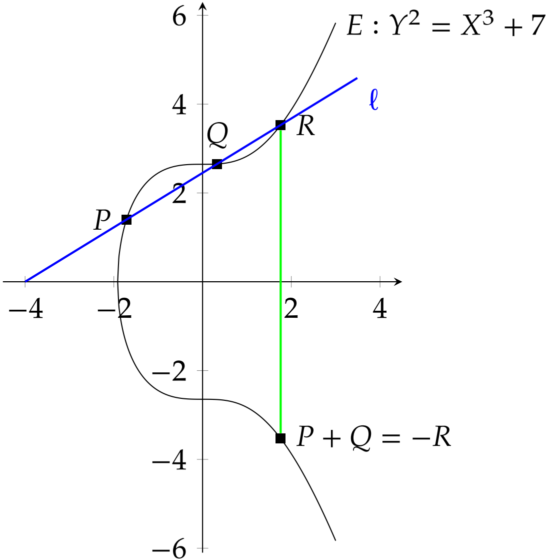
$$\text{射影版本：} Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

确定的平面射影曲线 E, 要求光滑. 指定无穷远点 $(0:1:0) \in \mathbf{P}^2$ 为其 “零点”.

平面代数曲线可以在不同坐标下表示. 精确到以下变换, E 的 Weierstrass 方程唯一: 令 $r, s, t, u \in K$, 设 u 可逆, 容许的变换是

$$X = u^2X' + r, \quad Y = u^3Y' + su^2X' + t.$$

顺带一提: (1) 椭圆曲线有不依赖坐标的内禀几何定义. (2) 椭圆曲线具有加法结构 (群), 以 $(0:1:0)$ 为零元.



椭圆曲线 $E : Y^2 = X^3 + 7$ 的实数部分及其加法结构示意图

从 Weierstrass 方程的系数计算

$$\begin{gathered}
b_2 := a_1^2 + 4a_2, \quad b_4 := a_1a_3 + 2a_4, \quad b_6 := a_3^2 + 4a_6, \\
b_8 := a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2, \\
c_4 := b_2^2 - 24b_4, \quad c_6 := -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\
j := c_4^3/\Delta.
\end{gathered}$$

- 精确到同构, 不变量 $j(E)$ 完整分类了域 K 上的椭圆曲线.
- Δ 可逆 $\iff$ Weierstrass 方程定义光滑代数曲线.
- 坐标变换 $(X, Y) \rightsquigarrow (X', Y')$ 下

$$u^4c_4' = c_4, \quad u^{12}\Delta' = \Delta.$$

曲线的 $\bmod p$ 约化

以下只考虑 $K := \mathbb{Q}$ 上的椭圆曲线 E.
利用坐标变换, 可以取到极小 Weierstrass 方程:

- 系数 $a_1, \ldots, a_6 \in \mathbb{Z}$,
- 对每个素数 p, 它在 Δ 中的幂次尽可能小.

极小判别式 $|\Delta_E|$ 只依赖于 E 的同构类.
将极小 Weierstrass 方程 $\bmod p$, 就得到有限域 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ 上的射影平面曲线 E_p, 无关各种资料的选取.

- 若 E_p 仍是椭圆曲线 ($\iff p \nmid \Delta$), 则称 E 在 p 处有**好约化**.
- 坏约化情形按 E_p 的奇点性质 (结点/尖点) 分为**乘性**与**加性**两种约化.

椭圆曲线的导子

仍考虑 $\mathbb{Q}$ 上的椭圆曲线 E. 另一个重要不变量是 E 的**导子**

$$N_E := \prod_{p:\text{素数}} p^{f_p} \in \mathbb{Z}_{\geq 1},$$

$$f_p = \begin{cases} 0, & \text{好约化} \\ 1, & \text{乘性约化} \\ \geq 2, & \text{加性约化}. \end{cases}$$

指数 f_p 的确切定义涉及**分歧理论**, 最简单的描述或许是透过 E 的 Tate 模.

广义 Szpiro 猜想的陈述

以极小 Weierstrass 方程对 $\mathbb{Q}$ 上的椭圆曲线 E 定义 Δ_E, $c_4(E)$ 等等.

广义 Szpiro 猜想 (1983)

设 $\epsilon > 0$, 那么存在仅依赖于 ϵ 的常数 $B(\epsilon) > 0$ 使得对所有 $\mathbb{Q}$ 上的椭圆曲线 E, 我们有

$$\max\left\{|\Delta_E|, |c_4(E)|^3\right\} \leq B(\epsilon) N_E^{6+\epsilon}.$$

事实: 初等数论 $\leftrightarrow$ 代数几何

abc 猜想 $\iff$ 广义 Szpiro 猜想.

以下勾勒 $\Longleftarrow$ 的论证.

基本工具是 $\mathbb{Q}$ 上的 **Frey 椭圆曲线**

$$E : Y^2 = X(X+a)(X-b), \quad a,b,c \in \mathbb{Z} \setminus \{0\} \text{ 互素}, \; c := a+b.$$

$$N_E = 2^{f_2} \prod_{\substack{p \mid abc \\ p \neq 2}} p,$$

其中依照 E 在 $p = 2$ 处的约化

$$f_2 = \begin{cases} 0, & \text{好约化} \\ 1, & \text{乘性约化} \\ \geq 2, & \text{加性约化} \end{cases}$$

1. $16 \nmid abc$: 已然是极小 Weierstrass 方程. 事实:

$$\Delta_E = 16(abc)^2, \quad c_4(E) = 16(a^2+ab+b^2), \quad 2^{f_2} \mid \Delta_E.$$

2. $16 \mid abc$: 需要稍微复杂的论证. 以下略去.

选定 $\epsilon > 0$. 设 $a, b, c \in \mathbb{Z}_{\geq 1}$ 互素, $a + b = c$. 考虑相应的 Frey 曲线 E. 简单起见假设 $16 \nmid abc$. 广义 Szpiro 猜想蕴涵

$$\max\left\{16^3\left|a^2 + ab + b^2\right|^3, 16|abc|^2\right\} \leq B(\epsilon) N_E^{6+\epsilon}.$$

1. 易见存在常数 $A > 0$ 使得 $|c|^6 = \left((a+b)^2\right)^3 \leq A \cdot$ 左式.
2. 另一方面 $16 \nmid abc \implies 16^3 \nmid \Delta_E = 16(abc)^2$, 已知此时 $2^{f_2} \mid \Delta_E$, 故

$$\begin{aligned} N_E = 2^{f_2} \prod_{p \neq 2, p \mid abc} p &< 16^3 \prod_{p \neq 2, p \mid abc} p \\ &< 2^{11} \mathrm{rad}(abc). \end{aligned}$$

于是广义 Szpiro 猜想蕴涵 abc 猜想成立. □

Lucien Szpiro

图片取自 Oberwolfach Photo Collection

除了应用于 abc 猜想, Frey 曲线也是 Taylor 和 Wiles 证明 Fermat 大定理的工具之一. 设 $a, b, c \in \mathbb{Z} \setminus \{0\}$, 设 $p \geq 5$ 是素数.

$$a^p + b^p = c^p$$
$$E : Y^2 = X(X - a^p)(X + b^p) \quad \text{(仿射部分)}$$

那么椭圆曲线 E 将与谷山–志村–Weil 的**模性**猜想矛盾.
这一观察可以上溯至 Y. Hellegouarch (1971—1975) 和 G. Frey (1986).

函数域

域 $\mathbb{C}$ 上的光滑射影曲线 $\overset{\text{范畴等价}}{\approx}$ 紧 Riemann 曲面:= 1 维连通复流形.

- 紧 Riemann 曲面 C 的**函数域**$:= \{f : C \to \mathbb{C} \sqcup \{\infty\} : \text{亚纯函数}\}$.
- 19 世纪数学家的洞见: Riemann 曲面的函数域和 $\mathbb{Q}$ 的有限扩张 (称为**数域**) 及其代数整数环有许多类比.
- 另一方面, 以任意域 K 替代 $\mathbb{C}$, 代数几何的工具可以对 K 上的所有代数曲线 C 定义函数域.
  特别地, 可取 K 为 q 个元素的有限域 $\mathbb{F}_q$, 其中 q 是素数的幂.

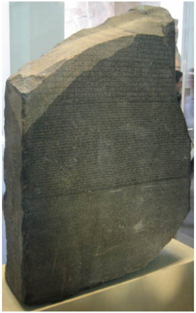
例: 域 K 上的射影直线

$$\mathbf{P}^1 := \{\ell \subset K^2 : \text{一维子空间}\}$$

以 $K(t)$ 为其函数域 (t: 变元).

A. Weil 设想的 **Rosetta 石碑**: 铭刻三种语言

$$\begin{tikzcd} & \text{数域} \arrow[dl, dash, dashed] \arrow[dr, dash, dashed] & \\ \text{函数域}_{/\mathbb{F}_q} \arrow[rr, dash, dashed] \arrow[d, leftrightarrow] & & \text{函数域}_{/\mathbb{C}} \arrow[d, leftrightarrow] \\ \text{曲线 } C_{/\mathbb{F}_q} & & \text{曲线 } C_{/\mathbb{C}} \end{tikzcd}$$



函数域上可资运用的工具更多. 多项式版本的 abc 定理 (Mason–Stothers) 便是一例, 其证明用到 $\mathbb{Q}$ 所欠缺的求导运算.

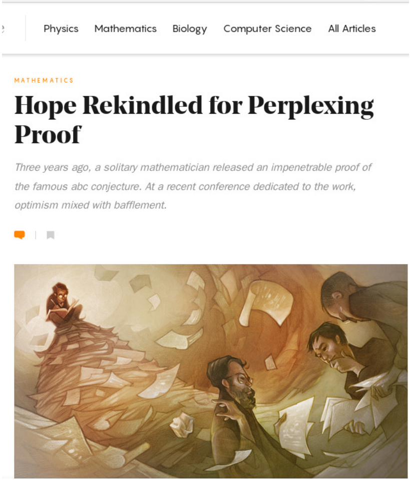
André Weil (1906—1998) 在 1940 年写给他妹妹 Simone Weil (1909—1943) 的一封信中解释了这一类比.

1922 年的 Weil 兄妹 (取自 A. Weil, *The Apprenticeship of a Mathematician*, 1992 年 Birkhäuser 出版)

近期动向

- 望月新一在 2012 年 8 月底公布了系列长文 *Inter-universal Teichmüller theory I—IV*, 声称证明了 abc 猜想.
- 基于他对远交换几何[2]的长年研究.
- 他的理论称为**宇宙际 Teichüller 理论** (IUTT), Ivan Fesenko 又称其为 "算术形变理论". 论文的第四部分实际导向关于不定方程的一些几何学估计[3], 蕴涵广义 Szpiro 猜想.

[2]Anabelian geometry, 由 Grothendieck 提出.
[3]确切地说: 双曲曲线的 Vojta 不等式


Physics Mathematics Biology Computer Science All Articles

MATHEMATICS

Hope Rekindled for Perplexing Proof

Three years ago, a solitary mathematician released an impenetrable proof of the famous abc conjecture. At a recent conference dedicated to the work, optimism mixed with bafflement.

2015 年底牛津大学举办关于 IUTT 的研讨会. 图片截自 Quanta Magazine 的报道: `https://www.quantamagazine.org/hope-rekindled-for-abc-proof-20151221`

1. 2018 年, P. Scholze 和 J. Stix 针对文章的一个核心断言提出了质疑 (*Why abc is still a conjecture*, August 2018), 认为难以修正.
2. 望月新一阵营并不买账. 见 Ivan Fesenko 斯文扫地的反击: *About certain aspects of the study and dissemination of Shinichi Mochizuki's IUT theory*.
3. 其它方面的进展: 可参考 H. Pasten 的文章 arXiv:1705.09251

有道是:

"战斗正未有穷期" — 

望赐教！

更新于 2019-11-26