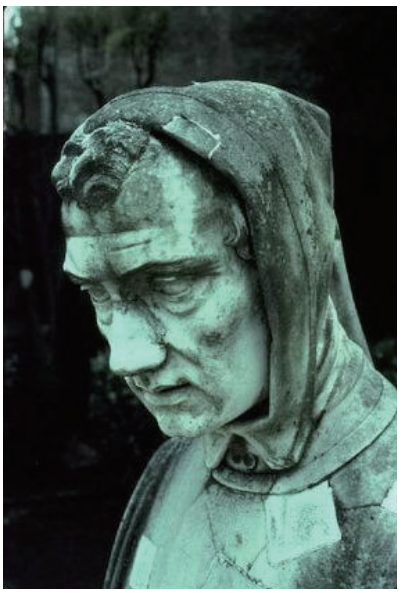
千禧年难题之
BSD 猜想——不定方程的有理解问题

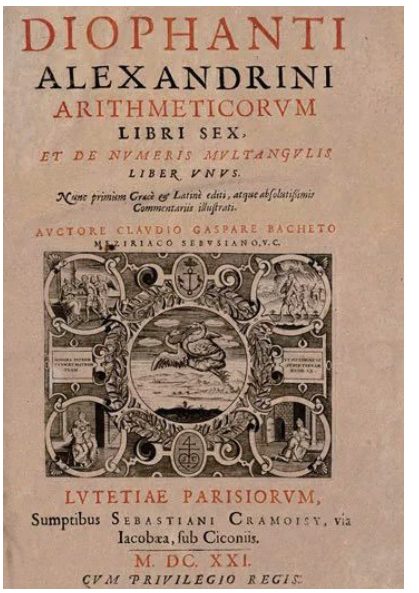
马英浩 / 文　袁新意 / 指导

千禧年大奖难题（Millennium Prize Problems），又称世界七大数学难题，是七个由克雷数学研究所（Clay Mathematics Institute, CMI）于 2000 年 5 月公布的数学猜想。BSD 猜想是其中之一，B 和 SD 分别是两位数学家姓氏的首字母，全称为贝赫与斯维纳通 - 戴尔猜想（Birch and Swinnerton-Dyer Conjecture），是数论领域的著名问题。为了描述某一种特殊不定方程（椭圆曲线）有理解的集合大小，BSD 猜想通过两个截然不同的思路给出两个不同的指标——代数秩和解析秩，并猜测它们相等。虽然猜想表述艰深晦涩，但却和课本上曾出现的一些流传几千年的数论知识一脉相承，是进入现代社会以来，真理的追求者对古老问题的进一步探索。

绵延千年的古老问题

数学是一个历史悠久的学科，而数论是数学的一个古老分支，至少有两千多年的历史。在这两千多年中，素数的分布问题和有理系数不定方程的有理解问题也一直困扰着人们。早在公元前 3 世纪，欧几里得就用反证法证明了素数有无穷多个，并寻求过勾股定理的通解。五六百年后，大约相当于中国的三国时期，丢番图（Diophantus）集中研究了有理系数多项式构成的不定方程，讨论了它们的有理数解。他所著的《算术》是人类第一本系统阐述代数方程的著作，讨论了很多相关问题，因而不定方程也被称为丢番图方程。在此后的近两千年，人们使用了各种方法试图解决这些问题，得到了一些成果，但也有很多局限性。近代以来，数学家们逐渐提出了更加复杂而深刻的办法，借用了很多其他数学





丢番图塑像和他的《算术》拉丁文译本（图片来源于网络）

分支的工具，一定程度上推进了有关问题的理解，但还有很多问题悬而未决。BSD 猜想就是一个不定方程问题的例子。

丢番图方程的例子有很多，小学奥数就有一次不定方程的例子，而二次不定方程的佩尔（Pell）方程理论就已经是高中竞赛的知识了。事实上，英国数学家约翰·佩尔和这个理论没有多大关系，该问题由古印度数学家婆罗摩笈多（Brahmagupta）提出，之后在费马再次提出后，直到 18 世纪才被拉格朗日最终解决。称其为佩尔方程是因为欧拉的误记。

虽然人们很快找到了一次和二次不定方程的通解，但更高次的不定方程人们几乎没有处理的有效手段。其中三次不定方程的有理解问题介于“可解”和“不可解”之间，因而一直广受数论学家的关注。

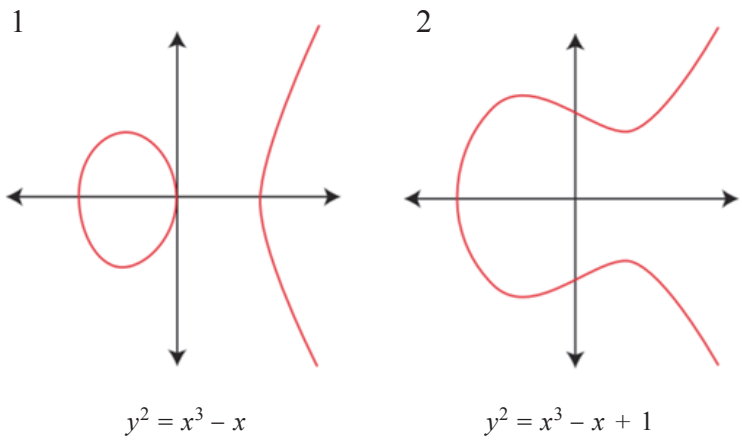
椭圆函数——一个三次不定方程

椭圆曲线起初并非是数论学家研究的对象。19 世纪，数学家们开始广泛研究各类特殊函数理论，其中就包括椭圆曲线。尽管最近几十年除了一些斯拉夫数学家，特殊函数理论鲜有人问津，以致于数学系相关的课程都很少，但在物理学或其他很多领域特殊函数还有很深远的影响。

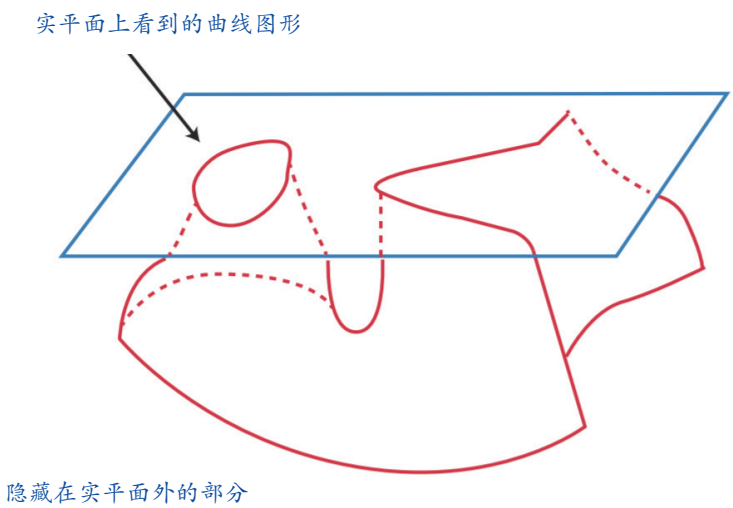
最初人们研究椭圆周长时，通过一定的积分变换技巧可以把椭圆弧长公式转换成下述积分：

$$\int_{\alpha}^{\beta} \frac{dx}{\sqrt{x^3+ax+b}}.$$

出于一些圆锥曲线的巧妙性质，该积分无法通过基本初等函数表示，但与



非退化的实数域上椭圆曲线



复数域上椭圆曲线示意图 [1]

魏尔斯特拉斯（Weierstrass）椭圆函数有一定的对应关系。其中分母的函数项平方即为形如 $y^2 = x^3 + ax + b$ 的方程，这被称为椭圆曲线。

最初人们研究的是定义在实数域和复数域上的椭圆曲线，特别是复变函数带来的几何直观。但在二次不定方程已被解决的年代，作为有着良好性质的三次不定方程，椭圆曲线似乎注定对数论产生深远的影响。

数论中历史悠久的“同余数”问题就可以归结为对椭圆曲线的研究。在公元 10 世纪以前，阿拉伯数学家就开始思考如何判断一个数是不是某个三条边

[1] 图片选自《浅说椭圆曲线》, 数学文化 (2013), 第 4 卷第 3 期 .

均为有理数的直角三角形的面积，并试图给出判别方法[2]。近代椭圆曲线理论出现以后，这个孤立的古老的问题变成了一个更深刻的现代理论的例子，尽管至今仍然悬而未决[3]。具体而言，假设 n 是一个同余数，也就是说，它可以写成一个三条边均为有理数的直角三角形的面积。设这个三角形的直角边为 a、b，斜边为 c，我们就可以得到如下方程组：

$$a^2 + b^2 = c^2, \quad \frac{1}{2}ab = n.$$

如果令 $x = n(a + c)/b$，且 $y = 2n^2(a + c)/b^2$，则可以将原方程化为如下的二元三次不定方程，也就是椭圆曲线的形式：

$$y^2 = x^3 - n^2x.$$

在椭圆曲线的 BSD 猜想成立的假设下，图内尔（Tunnell）[4] 证明了一切除以 8 余 5、6、7 的数都是同余数，并给出了正整数是同余数的充要条件。

很多历史悠久的数论问题和更高次的丢番图问题，都可以转化为椭圆曲线这个三次不定方程的问题，这一普遍性和它的解集的一个深刻结构深深地吸引着很多研究者。

解集的表示

写出不定方程的所有有理解不是一件容易的事。对于一次和二次方程，一个可行的做法是使用分析的语言将解集写成一个离散参数空间，并让参数取所有的整数。然而三次方程没有那么多解，因而解集常常并不构成某个参数空间。一个可行的做法是给出一些“原始解”，通过一定的运算方式，可以从“原始解”生成集合中所有的元素。

费马或许是第一个用几何作图寻找新解的人。

$$y^2 = x^3 + ax + b \qquad (a, b \in \mathbb{Z})$$
$$\Delta = 4a^3+27b^2 \neq 0$$

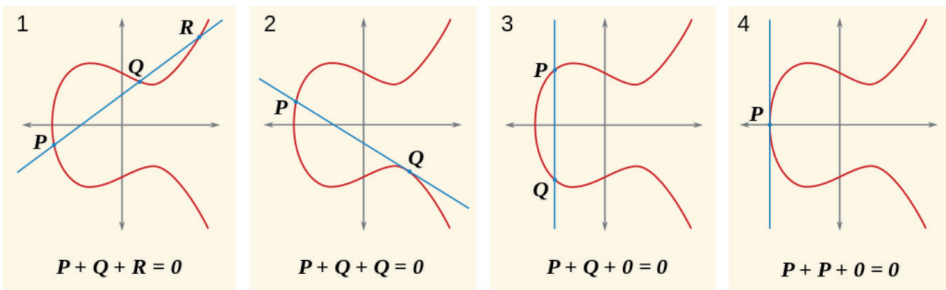
对于上述的整系数的椭圆曲线，费马指出，在已知原方程一些解的情况下，可以通过切割线这种作图方式，生成该方程新的有理解：两个有理坐标的点确定的直线方程系数是有理数，跟有理系数多项式方程联立以后，经过因式分解可以得到第三个交点的坐标，显然第三个点也是有理点。之后魏尔斯特拉斯为

[2] A. Weil, Basic Number Theory, Birkhaüser, Boston, 1984. 第一章第七节

[3] 维基百科 congruent numbers https://en.wikipedia.org/wiki/Congruent_number

[4] 参见 J. Tunnell, A classical diophantine problem and modular forms of weight 3/2, Invent. Math. 72 (1983), 323–334.

这样的解集定义了一种运算——对于 P 和 Q，两点所在直线交图像于第三点 R，R 关于 x 轴的反射 R' 则被定义成 $P+Q$。之后或许是丹麦数学家尤尔（Juel）第一个发现，如果把无穷远点作为集合的“单位元”并把反射的元素定义为“逆元”，那么这样的运算对于解集封闭，还显然具有交换律，并且竟然具有结合律[5,6]。在这个意义下，对抽象代数稍有了解的读者不难发现，椭圆曲线的实数解构成一个群，而有理解竟然是这个群的子群！这样的奇妙性质让椭圆曲线吸引了很多数学家的目光。



椭圆曲线解集的加法结构[7]

庞加莱在 1901 年的论文中系统总结了前人关于椭圆曲线有理点的理论，并指出对于每个椭圆曲线，只需要得到有限个有理解，再通过切线、割线操作序列的无穷组合，就可以完全表示出有理解的解集。也就是说，这个解集在之前定义的“切割线”运算之下是一个有限生成交换群。事实上，像生成全体多项式这样的对象，我们都需要选取所有的 x^k，用无穷个基底才能生成，但庞加莱认为，生成一个椭圆曲线的所有有理解，用有限个解就够了。这个猜想在 1922 年才被英国数学家莫德尔（Mordell）证明，此后这有限个能生成全部解的“原始解”（生成元）有怎样的性质，或者说究竟多少个解才能生成所有的解，就成了一个很重要的问题。

$$\mathbb{Z}^r \oplus \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_k}$$

有限生成交换群的结构

有些“原始解”在和自己不断操作以后会回到自己，就像除以 3 的余数是

[5] C. Juel, *Ueber die Parameterbestimmung von Punkten auf Curven zweiter und dritter Ordnung. Eine geometrische Einleitung in die Theorie der logarithmischen und elliptischen Funktionen,* Math. Ann. 47 (1896), 72–104.

[6] Who first identified the group structure of an elliptic curve? https://hsm.stackexchange.com/questions/5171/who-first-identified-the-group-structure-of-an-elliptic-curve

[7] 图片选自《浅说椭圆曲线》, 数学文化 (2013), 第 4 卷第 3 期 .

集合 {0,1,2}，1+1+1 在除以三的意义下等于 0；而有的“原始解”不断操作则永远不会重复，就像整数 1 不论加多少次都回不到自身。抽象代数告诉我们，一个椭圆曲线有理解解集作为一个有限生成交换群，可以被视为一个有限群（第一类解）直和 $\mathbb{Z}$ 的某个方次（第二类解）。而这个方次 r 被称为该椭圆曲线的代数秩，r 越大生成全部解所需的“原始解”越多。知道了 r 的大小以后，构造椭圆曲线的所有有理解就简单很多。

有趣的数值现象

对于一个难以探求整体解的不定方程问题，我们常常会考虑它的某种“局部性质”：如果原方程的有理解被视为“整体解”，那么方程在模（mod）素数 p 意义下的解就可视为“局部解”。在模素数 p 的意义下，椭圆曲线的解 (x, y) 至多有 p^2 种可能，记模素数 p 的局部解个数为 N_p。数论学家们期待，由于“局部整体原理”（local-global principle），局部解的数量跟整体解的数量存在某种的对应联系。事实上，整体解显然是局部解。

在以往，这样的计算十分困难，幸运的是，剑桥大学的 EDSAC 在 1949 年正式投入使用，这是世界上第一台实际运行的存储程序式电子计算机。更加幸运的是，本文的主角之一，数论学家斯维讷通 - 戴尔知道如何使用它。

人类第一台实际运行的存储程序式电子计算机 EDSAC，占地面积 20 平方米

面对这样一个庞然大物，在 20 世纪 50 年代末期，他和另一位主角，数论学家贝赫（Birch）着手准备计算一系列特殊的（带复乘的）椭圆曲线的代数秩，和每个方程对全部小于 1000 的素数的解的数量 N_p。

按照哈塞（Hasse）定理，椭圆曲线在模每个素数 p 的局部解个数 N_p 跟 p 相差不大，因此他们在计算时考虑 N_p 除以 p 和代数秩 r 的关系，并发现了如下的公式：

$$\prod_{p\le X}\frac{N_p}{p}\approx C\log(X)^r \qquad \text{as } X\to\infty$$

BSD 猜想的原始版本，其中 C 为大于零的常数

式子左边的累乘衡量了方程在模素数 p 意义下的局部解数量，等式右边则是关于整体解的解集大小的衡量指标——代数秩 r 的函数。计算结果简洁地展示了他们的关系，这也是 BSD 猜想的“原始版本”。时至今日，利用计算机辅助证明能够猜出这样精妙的公式的例子也很少见，因此，在计算机刚刚诞生的年代，这样出人意料而天马行空的公式最初引起了很多学者的质疑，其中甚至包括本文主角之一贝赫的博士生导师卡塞尔（Cassels），但随着越来越多的数值结果和其他证据的出现，数论学家们不得不接受这样的猜想。

然而，这个形式的美感或许还不够强，尽管很可能是正确的。有的椭圆曲线对应的序列收敛比较慢，或收敛之前有些跃迁，这些情形之下计算极限就不能很好的反应这个性质。在数论学家志村五郎（Shimura）的提议和同事达文波特（Davenport）的帮助下，贝赫得以用 L 函数重新书写这个猜想[8]。L

英国数论学家 Swinnerton-Dyer

[8] How did Birch and Swinnerton Dyer arrive at their conjecture? https://mathoverflow.net/questions/66561/how-did-birch-and-swinnerton-dyer-arrive-at-their-conjecture

函数在当时还没有引起数论学家的高度重视，但在之后现代数论的发展中则受到了广泛关注。

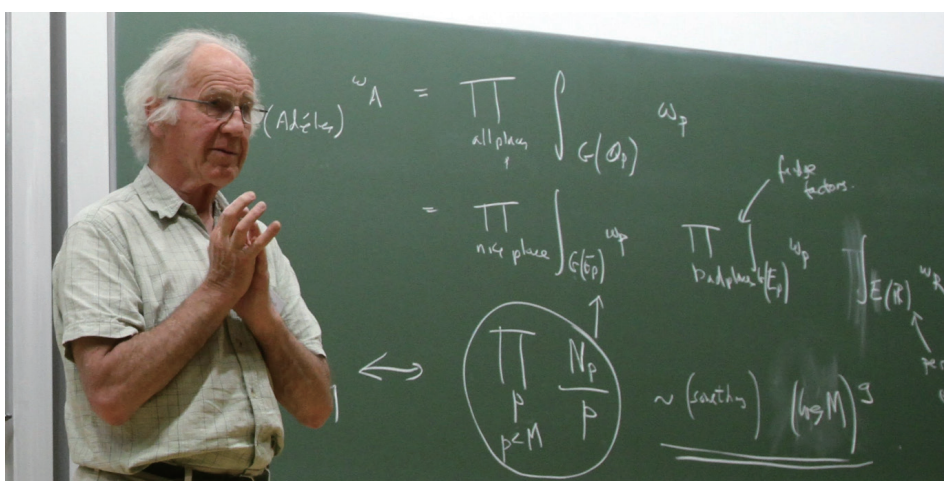
BSD 猜想的正式版本

猜想提出者之一，英国数论学家斯维讷通 - 戴尔曾调侃，一开始没想到用 L 函数表示原始版本，是由于法国数学家韦伊（Weil）在很早就把 L 函数推向了数学的中心位置，导致很多数学家反而“唯恐避之不及”。但在同事布扎尔德（Buzzard）看来，对后世影响深远的朗兰兹纲领（1967，Langlands program）当时尚未提出，L 函数在有限维伽罗瓦（Galois）表示和自守表示等对象中表现出的深刻性并没有得到足够的揭示，原始版本没有使用 L 函数是很正常的。

$$L(C,s) := \prod_{p \nmid 2\Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

椭圆曲线 C 对应的 L 函数，a_p 表示素数 p 减去方程 C 模 p 的解的个数，Δ 是判别式

著名的黎曼猜想中的 zeta 函数就是 L 函数的一个例子。而对于任意的椭圆曲线 C 我们都可以定义一个 L 函数 $L(C, s)$，作为一个关于 p^{-s} 的多项式的连乘——乘积中丢掉有限项可以被判别式整除的素数对应的多项式。取对数后容易证明，乘积在 s 的实部大于 1.5 时绝对收敛。鉴于每项乘积都是多项式，是一种解析函数，累乘的结果是某个右半平面上的解析函数。BSD 猜想的正式版本则是把原始版本关于“局部解”一侧的极限式转化为延拓到 $s = 1$ 处的幂级数展开，并类似地建立跟“整体解”解集大小的关联。



英国数论学家 Birch

志村五郎和达文波特曾向贝赫指出，L 函数在 $s = 1$ 处的幂级数展开可以很好地表示他所计算的椭圆曲线（即带复乘的椭圆曲线）的信息。然而当时大家对 L 函数知之甚少——Hasse 曾在 1958 年猜想，L 函数可以解析延拓到整个复平面[9]（复变函数的知识告诉我们这样的解析延拓如果存在则唯一），但在BSD猜想诞生的年代，人们尚没有证明这一点。L 函数一旦不能解析延拓，$s = 1$ 处的零点重数就没有定义，然而大胆的 Birch 却敢于这样猜测，并决心用 L 函数重写 BSD 猜想。直到三十多年后人们加深了对 L 函数的了解，BSD 猜想的陈述才具有意义。上世纪 90 年代，怀尔斯（Wiles）及其学生泰勒（Taylor）证明了谷山 - 志村 - 韦伊猜想（Taniyama-Shimura-Weil conjecture）的半稳定情形，即椭圆曲线与数论中的重要对象“模形式”一一对应，这使得人们确认 L 函数在整个复平面上的解析延拓，并将 L 函数写成某个关于 $s = 1$ 中心对称的函数方程的形式[10,11]。此后的 2001 年，布勒伊（Breuil）、康莱德（Conrad）、戴蒙德（Diamond）和泰勒共同推广了该证明，从而证明了谷山 - 志村 - 韦伊猜想的一般情形[12]。当然人们熟知怀尔斯和泰勒的工作通常是因为它顺便证明了费马大定理。

$$ord_{s=1}(L(E,s)) = rank_{\mathbb{Z}}(E(K))$$

BSD 猜想的正式版本，E 表示椭圆曲线

美国数论学家戈尔德菲尔德（Goldfeld）通过类似素数定理的估计手法，证明了 BSD 猜想的“原始版本”中极限所趋近的真实值，不论是否等于代数秩，都一定是椭圆曲线对应的 L 函数在 $s = 1$ 处重根的个数，也即 L 函数在 $s = 1$ 处做幂级数展开后，第一个系数非零项的 $(s-1)^k$ 的幂次 k。这个数被称为“解析秩”，而 BSD 猜想的正式版本就是“解析秩等于代数秩”。事实上原始版本的结论更加深刻，因为它除了正式版本的结论外，还蕴含了 L 函数的黎曼假设——即 L 函数解析延拓后的零点实部都等于对称中心。

到此，BSD 猜想的内容就全部露出水面。椭圆曲线（一种三次不定方程）整体解集的代数秩（表征有限生成交换群的生成元多少）和解析秩（用 L 函数在对称中心的重根数量表征模每个素数 p 的局部解 N_p 的信息）相等。对一个古老的不定方程有理解问题的新探索，让人发现了各种奇妙的数学对象，衍生出一系列数学工具，并似乎有某种内在的联系，这实在是让人叹为观止！

[9] A. Weil, *Collected Papers,* Vol. II, Springer-Verlag, New York, 1979.

[10] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. 141 (1995), 553–572.

[11] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. 142 (1995), 443– 551.

[12] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over Q: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), 843–939.

相关进展

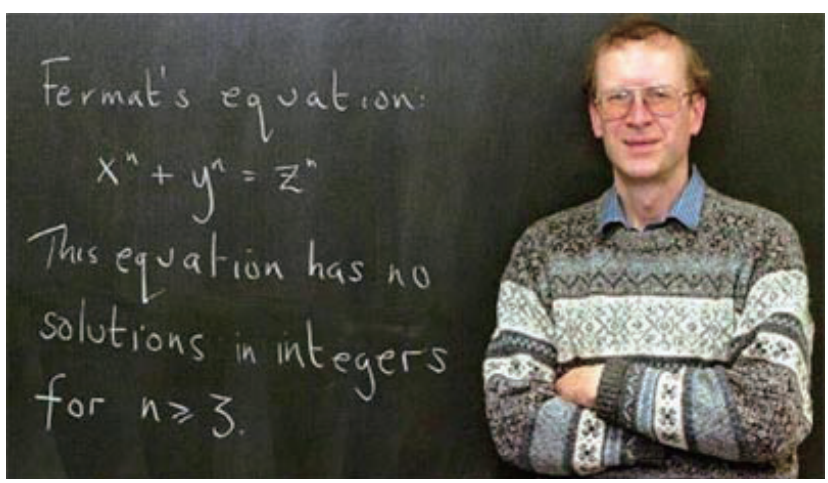
当然 BSD 猜想的故事并没有就此结束，数论的故事总是不断精彩。

第一个突破源于 1977 年，著名的数论学家科茨（Coates）和他的得意门生怀尔斯证明了 BSD 猜想对带复乘的椭圆曲线而言，解析秩为 0 时代数秩也为 0。

此后格罗斯（Gross）和扎吉尔（Zagier）在 1986 及科里瓦金（Kolyvagin）在 1989 年的工作共同证明了：BSD 猜想在解析秩小于等于 1 的情况下成立。此前贝赫总结德国电子工程师兼业余数学家黑格纳（Heegner）生前工作时，给出了椭圆曲线的一个解，但一直不知道如果作为解集的有限个生成元，是否贡献了代数秩。而格罗斯和扎吉尔给出了判定解是否是无挠（贡献了代数秩）的 Gross-Zagier 公式。公式将 L 函数在 $s = 1$ 处的导数跟衡量解复杂性的指标“高度”相结合，从而证明了 BSD 猜想在解析秩小于等于 1 时成立。

然而问题似乎遇到了瓶颈，尽管过去三十年人们在推广 Gross-Zagier 公式等方面取得了很多突破，然而对如何证明秩等于 2 这个猜想的特殊情况大家都还一筹莫展。

当然，上世纪 90 年代怀尔斯证明费马大定理时，数学家们顺便证明了 L 函数一定存在解析延拓函数方程，从而证明了 BSD 猜想的正式版本对任何椭圆曲线都有意义，这是了不起的突破。或许也正是如此，在克雷研究所评选千禧年数学问题时，人们将这个新时代寻找古老不定方程有理解的新探索确定为七个百万美金猜想之一。



英国数学家怀尔斯

虽然有理数域上的 BSD 猜想再无重大突破，将其类比到函数域却取得了一些进展。有理数集对加减乘除四则运算封闭，因此构成一个域，而函数域是他的一个类比：给定某个素数 p，一切整数除以 p 的余数只有 p 种可能，结合一点初等数论的知识不难验证这是一个有限域，这个域上的多项式 $\mathbb{F}_p[t]$ 对加

减乘三则运算封闭，从而构成了一个环，类比整数的唯一分解定理，有多项式的唯一分解定理。类似有理数，如果允许多项式环中的元素做除法，构成的分式函数就会形成一个函数域$\mathbb{F}_p[t]$。

有理数域上多项式方程有理解问题通常可以类比到函数域上方程求解的问题。例如费马大定理，可以类比到关于多项式$x(t)$，$y(t)$和$z(t)$的方程$x^n(t) + y^n(t) = z^n(t)$只有平凡解。探讨一个问题会对另一个域上的对应问题产生启发，因而人们也会研究函数域上的对应问题，来寻找解决数论问题的灵感。事实上，函数域虽然放弃了对有理方程的分析手段，但是可以对方程两边同时对t求导得到新的方程，还可以采用代数几何的研究方法，因此常常更加简单。例如黎曼猜想和数论中著名的ABC猜想的函数域上的版本都已经被证明。当然BSD猜想的函数域版本都没有彻底解决也说明这个猜想的难度。

BSD猜想的函数域版本是说，考虑椭圆曲线$y^2(t) = x^3(t) + a(t)x(t) + b(t)$，其中$a$、$b$、$x$、$y$是函数域$\mathbb{F}_p[t]$中的元素。也可以证明解构成了有限生成交换群，并定义解集的代数秩r。同样的也可以考虑所有的不可约首一多项式$p(t)$对应的局部解并类比定义L函数。这样的L函数是在$s = 1$处零点重数仍然被定义为解析秩。美国数学家泰特（Tate）首先考虑了函数域上的BSD猜想，并指出对于函数域上的猜想版本，代数秩小于等于解析秩，同时两者相等当且仅当Tate-Shafarevich群是有限群。

尾声

虽然过去几十年我们有了不同寻常的进展，数论学家们对寻找一般的代数曲线方程的有理解依然没什么好的办法。以致于怀尔斯在给BSD猜想的介绍中写道“希望BSD猜想的证明能够提供对一般性问题的洞察见解”[13]。

尽管人们对BSD猜想的证明寄予厚望，但这也只是数论的一小步，在自然面前，还有很多未知等待人类探索。即使BSD猜想被解决，在此基础上通过解析秩来计算代数秩也是很不容易的一件事；而且得到代数秩以后寻找足够数量的生成元也并不轻松。至于解集中看似简单的有限群（不贡献代数秩）的部分，虽然被美国数学家梅热（Mazur）解决，但是在更一般的阿贝尔簇（椭圆曲线的高维推广）上的“有理解”是否有类似性质的“挠（torsion）猜想”几十年来依然困扰着人们。

当然，对于更复杂高次的不定方程，人们并非毫无建树。Mordell曾猜想由于次数过高带来很强的约束，很多高次不定方程只有至多有限个解。这个猜想困扰人类六十多年后，在1983年由一位青年才俊——时年29岁的德国数学家法尔廷斯（Faltings）证明，他随后因此获得菲尔兹奖。而对于其他高次不定方程，有时可以尝试从中寻找椭圆曲线，并在椭圆曲线上寻找不平凡的解。

[13] 参见 A. Wiles, *The Birch and Swinnerton-Dyer Conjecture*. (2006)

例如 26 岁就当上哈佛大学教授的埃尔奇斯（Elkies）给出了如下式子[14]：

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

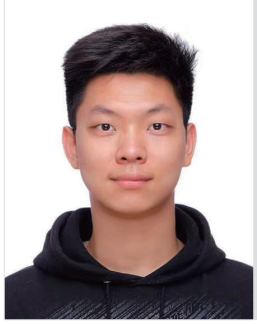
从而反驳了欧拉在 1769 年关于该方程只有平凡有理解的猜想。甚至由于这个解贡献了代数秩，原方程有无穷多解。

在伟大的真理面前，人类似乎已经努力地发展出各种深刻而晦涩的工具，取得了非凡的进展。但即便 BSD 猜想得以证明，人类还有很长的路要走。

屈原曾经说过，“路漫漫其修远兮，吾将上下而求索”。正是有一代又一代的数学家前仆后继，思考艰深的问题，一点点探求真理，人类才能逐渐了解到隐藏在整数背后的秘密，走向未知的远方。时至今日，斯维讷通 - 戴尔已然仙逝，贝赫也将近九旬，就连怀尔斯和法尔廷斯都年近古稀。随着时间的流逝，老一辈数学家们的传奇将会暂时告一段落，而新的传奇，将由各位年轻人来书写。

[14] N. Elkies, On $A^4 + B^4 + C^4 = D^4$, Math. Comput. 51 (1988), 825–835.

致谢：北京国际数学研究中心的多位老师同学对本文亦有帮助，谨向他们表达感谢。



作者简介：

马英浩，北京国际数学研究中心访问学生，目前正在攻读美国卡内基•梅隆大学音乐科技硕士项目，本科毕业于北京大学数学科学学院。

指导老师：

袁新意，2003 年毕业于北京大学，2008 年获得哥伦比亚大学博士学位，现任北京国际数学研究中心教授，研究领域是数论和算术几何。