同余数

John Coates

译者：张起帆，校者：胥鸣伟

John Coates，剑桥大学教授。

数论是研究隐含在整数和有理数中奥秘的数学分支（有理数指的是两个整数的比），而同余数问题则是数论中，或许还是整个数学中，最古老的一个尚未解决的重大问题。从有文字记载的历史来说，这个问题至少可以追溯到一千多年前。我们称三条边的长都是有理数的直角三角形为**有理直角三角形**，而称一个正整数 N 为**同余数**，是说 N 是一个有理直角三角形的面积。如果用任意一个整数的平方去乘同余数 N，则得到另一个同余数，因此我们只需考察那些没有平方因子的正整数 N（即 N 不被大于 1 的平方数整除）。简单地说，同余数问题就是确定那些无平方因子的正整数是不是同余数。人们早就知道：一个正整数 N 是同余数当且仅当在椭圆曲线 $y^2 = x^3 - N^2x$ 上有一个点 (x, y)，其坐标 x, y 为有理数且 $y \neq 0$。直到 17 世纪，数学家们才用写出相应有理直角三角形的巧妙方法构造出同余数的数表。例如：$5, 6$ 和 7 都被确认是同余数，因为它们分别是三边为 $(40/6, 9/6, 41/6)$, $(3, 4, 5)$ 和 $(288/60, 175/60, 337/60)$ 的直角三角形的面积。关于同余数的第一个重要的理论结果是 Fermat 建立的，他在 17 世纪证明了 1 不是同余数。正如我们在后面将更为详细解释的那样，Fermat 的发现，更确切地说，从它以后关于同余数的每一个所证明的主要新结果都最终导致了对关于 Diophantus 方程的某些最深刻的问题的研究的重大进展。在 20 世纪 60 年代初所发现的著名的 Birch 和 Swinnerton-Dyer 猜想（BSD 猜想）[2] 增进了人们对于同余数问题的兴趣，并且回过头来，人们终于认识到同余数问题才是这个猜想的最古老也是最实际的例子。特别地，BSD 猜想预言每个具有以下形状

$$8n+5,\ 8n+6,\ 8n+7 \quad (n = 0, 1, 2, \cdots) \tag{1}$$

的整数应该是同余数［但注意，并非所有同余数都有此形状，例如边长为 $(225/30, 272/30, 353/30)$ 的直角三角形面积为 34］。关于 (1) 式所描述的整数的这个简单的一般性断言，其证明似乎仍然超越了当今数论的认知范围。然而，田野在 PNAS 上的文章 [1] 朝着这个方向取得了激动人心的进展，首次证明了存在很多形状 (1) 的具有大量素因子的同余数。特别地，文中证明对每个正整数 $k \geqslant 1$，存在无穷多个无平方因子的同余数，它具有形状 $8n+5, 8n+6, 8n+7$，且恰好有 k 个素因子，文中还明确告诉我们怎么构造它们。

Fermat 注意到他对 1 不是同余数的证明也能导出不存在有理数 x 和 y，使得 $xy \neq 0$ 和 $x^4 + y^4 = 1$。很可能就是这个事实引导他提出断言（常称 Fermat Last Theorem，即 Fermat 大定理）：对任何整数 $n \geqslant 3$，没有有理数 x 和 y 满足 $xy \neq 0$ 及方程 $x^n + y^n = 1$。对这第二个结论，他所宣称的证明至今没有发现任何证据。对它的第一个证明则是在代数数论和自守形式理论的一系列长足发展以后，由 Wiles 于 1994 年给出的 [3]；前面提到的这些理论的发展贯穿了整个 19 世纪和 20 世纪，而这些理论的根源至少部分可追溯到 Fermat 大定理和同余数问题。在一个不同的方向上，Mordell 于 1922 年推广了 Fermat 关于 1 不是同余数的证明方法 [4]，证明了对每一条由有理系数方程定义的椭圆曲线（以后就简称椭圆曲线），曲线上坐标为有理数的点构成的阿贝尔群是有限生成的。这个优美的结果是现代算术几何的起点。Heegner 是第一个证明了存在无穷多个无平方因子的同余数的人：在他的那篇现在已著名的发表于 1952 年的文章 [5] 中，证明了每个形如 $8n+5$ 的素数均为同余数。Heegner 的文章的重要性在 BSD 猜想被发现后的 20 世纪 60 年代后期才被人们认识到。我们在此不加详细解释地回想一下：那个（未加证明的）BSD 猜想预言是说，椭圆曲线 E 上存在无限个坐标为有理数的点当且仅当它的复 L-级数 $L(E,s)$ 在复平面的 $s=1$ 处取 0 值，这里 $L(E,s)$ 的定义是根据 E，对于所有素数做一个自然的欧拉乘积，这个做法受到我们所熟知的 Riemann 的 zeta 函数的欧拉乘积的启示。事实上，人们已知（见 [6, 7]），如果 $L(E,s)$ 在 $s=1$ 处不取 0 值，则 E 上只有有限个有理点，而且这个结果可以用来证明存在大量非同余数（见 [8, 9]）。但证明存在大量同余数却完全是不同的一回事。Heegner 的原始论文一点也没有涉及同余数的相关椭圆曲线的复 L-级数，然而，Birch 意识到 Heegner 方法的某种变形可以用来构造一大类椭圆曲线上的有理点（他称之为 Heegner 点），而且似乎恰当这个曲线的复 L-级数在 $s=1$ 处是单零点时，这些点是无限阶的。进而，他和 Stephens 进一步发现了一些令人信服的数值证据，表明这些 Heegner 点（准确地说，是在 Neron 和 Tate 的意义下这些点的高度）与 $L(E,s)$ 在 $s=1$

处的一阶导数有简单关系，而且它们都与 BSD 猜想相容。一件当年曾震惊整个数论界的历史事件是 Gross 和 Zagier 证明了 Birch 和 Stephens 的这一猜想 [10]。之后不久，Kolyvagin 发现了同等卓越的方法 [7]，它用这些 Heegner 点证明了对那些满足 $L(E,s)$ 在 $s=1$ 处的零点阶最多是 1 的椭圆曲线 E 的 BSD 猜想的大部分断言。

然而，所有这些将 Heegner 点和 L-函数相关联方面的后继发展都绕开了原始的同余数问题。一方面，对超过两个奇素因子且具有形状 (1) 的整数 N，没有人能看出怎样把 Heegner 的存在性证明推广到曲线 $y^2=x^3-N^2x$。另一方面，人们也不知道如何对一大类 (1) 形的合数 N 证明曲线的 L-级数有单零点。直到今天才最终由田野看出怎样把 Heegner 的讨论自然地推广到合数 N [1]，这一推广是通过把对涉及的 L-函数的深刻想法与 Heegner 的原始构造进行精妙结合完成的。有趣的是田野对 L-函数的使用依赖于两个完全不同的支持 BSD 猜想的部分已知结果。第一个是张寿武和他的学生们在 [11] 中建立的 Gross-Zagier 公式的重要推广（原始的 Gross-Zagier 公式不适用于同余数椭圆曲线上的 Heegner 点，因为某些分歧条件在这种情形不再成立）。第二个是赵春来关于同余数椭圆曲线的结果，不过不是 (1) 形的 N，而是 N 或为 $k\geqslant 1$ 个不同的 $8n+1$ 形素数之积或为这样的积的两倍。对这样的 N 所对应的椭圆曲线，L-函数 $L(E,s)$ 通常不会在 $s=1$ 处取 0 并已知 $M(E)=L(E,1)/\Omega$ 是有理数，其中 Ω 表示 E 的最小正实周期。BSD 猜想预言，对这些 N，有理数 $M(E)$ 一定被 2^{2k-1} 整除。赵春来在 [12, 13] 中找到了这个事实的巧妙证明。这个可除性在田野的工作中起了至关重要的作用。田和赵都对 N 的奇素因子个数做归纳，值得注意的是在他们各自的证明中有某种明显的平行，确切地说，田野使用了依附于 N 的因子的 Heegner 点的平均，赵春来使用了关于 N 的因子的 $M(E)$ 值的平均。

综上所述，田野的工作是这个古老问题的历史中的一个重要里程碑，并且就像过去总会出现的那样，将它推广到所有椭圆曲线似乎也只是时间问题。

参考文献

[1] Y. Tian, Congruent numbers with many prime factors, Proc Natl Acad Sci USA.

[2] B. Birch, P. Swinnerton-Dyer, Notes on elliptic curves II, Crelle 218 (1965), 79−108.

[3] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann of Math 141 (1995), 443−551.

[4] L. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degree, Math Proc Camb Phil Soc 21 (1922), 179−192.

[5] K. Heegner, Diophantische analysis und modulfunktionen, Math Z 56 (1952), 227−253.

[6] J. Coates, A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, Invent Math 39 (1977), 233−251.

[7] V. Kolyvagin, Euler systems, in The Grothendieck Festschrift, Vol. II, Progr Math 87 (1990), 435−483, Birkhauser Boston.

[8] C. Zhao, A criterion for elliptic curves with lowest 2-power in $L(1)$, Math Proc Camb Phil Soc 121 (1997), 385−400.

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

[10] B. Gross, D. Zagier, Heegner points and derivatives of L-series, Invent Math 84 (1986), 225−320.

[11] X. Yuan, S. Zhang, W. Zhang, The Gross-Zagier formula of Shimura curves, Annals Math Studies 184 (2012).

[12] C. Zhao, A criterion for elliptic curves with second lowest 2-power in $L(1)$, Math Proc Camb Phil Soc 131 (2001), 385−404.

[13] C. Zhao, A criterion for elliptic curves with lowest 2-power in $L(1)$ (II), Math Proc Camb Phil Soc 134 (2003), 407−420.

编者按：本文译自 John Coates 在 *Proc. Natl Acad Sci USA* 上的文章 Congruent numbers 的修订版本。