Is there a simple test for determining whether an elliptic curve has an infinite number of rational solutions?

椭圆曲线的有理数解

陈亦飞

中国科学院数学与系统科学研究院, 北京 100190

E-mail: yifeichen@amss.ac.cn

2016-08-23 收稿, 2016-11-08 修回, 2016-11-09 接受, 2016-11-24 网络版发表

摘要 椭圆曲线的研究历史悠久, 其中一个基本问题就是对于一条椭圆曲线, 找出其所有的有理数解. 对椭圆曲线有理数解的研究也不断推动着数论中众多领域的发展. 例如, 椭圆曲线理论在证明费马大定理中起到了关键作用. 1922年, 莫德尔证明椭圆曲线的有理数解构成一个有限生成交换群. 从而, 椭圆曲线有无穷多解等价于这个群的秩大于0. 与此相关的最著名的当属七大千禧年问题之一的贝赫(Birch)和斯维纳通-戴尔(Swinnerton-Dyer)猜想(BSD猜想): 椭圆曲线的秩和哈斯-韦伊(Hasse-Weil) L 函数在 $s=1$ 处的阶相等. BSD猜想为判断椭圆曲线是否有无穷多有理数解提供了一个途径. 然而, 要证明这个猜想十分困难, 数学家们仍在为此努力着.

关键词 椭圆曲线, BSD 猜想, 椭圆曲线的秩

1 介绍

解方程是数学的核心问题之一. 而解方程又包含三个基本问题: 一是方程是否有解? 二是有多少解? 三是能否给出求解公式. 不同研究领域的数学家关心不同类型的方程或解. 数论学家关心代数方程的整数解(丢番图问题)或有理数解. 微分方程学家关心微分方程的实数解. 几何学家一般关心方程的实数解或复数解. 当方程或方程组的解不易求出时, 数学家关心方程解集的整体性质, 一般称为几何对象: 拓扑学家关心拓扑流形, 即连续函数方程定义的解集; 微分几何学家关心微分流形, 即微分方程定义的解集; 代数几何学家关心代数簇, 即代数方程定义的解集. 人类对自然界的认识逐步深入, 最早理解的就是自然数、整数和有理数. 所以, 关心方程的整数解或有理数解是非常自然的. 本文中讨论的曲线其定义方程系数均为有理数.

给定一条平面直线 $y=ax+b$, 其中系数 a, b 是有理数, 很容易判断它有无穷个有理数解, 即集合 $\{(x_0, y_0) \mid x_0, y_0 \text{ 都是有理数} \mid y_0 = ax_0 + b\}$ 是一个无限

集合. 平面2次曲线 C 的一般方程可以写成 $ax^2+bxy+cy^2+dx+ey+f=0$, 其中系数 a, b, c, d, e, f 全是有理数, 且 a, b, c 不同时为0. 如果把 C 看成是实平面上的曲线, 由解析几何的知识, 曲线 C 可能是椭圆、双曲线、抛物线或者两条直线. 我们把两条直线的情形称为退化的或者奇异的, 其他的情形称为光滑的或者非奇异的. 我们一般讨论占大多数的光滑情形. 有的光滑2次曲线没有有理点, 比如 $x^2+y^2+1=0$. 如果一条2次曲线上有一个有理数点, 则它有无穷个有理数解. 大致的想法是先在 C 上找到一个有理数点 O , 然后通过投影的方式参数化2次曲线 C 上所有的有理数点. 如图1, 在直线 L 上任取有理点 Q , 连接直线 OQ 和2次曲线 C 相交于一点 P . 不难证明 P 也是有理数点, 而且 C 上的所有有理数点可以用这种方式得到(图1).

平面1次和2次曲线的有理数解清楚以后, 人们自然考虑平面3次曲线. 我们通常假设这个3次曲线上有一个有理数点. 光滑的有理系数平面3次曲线经过适当的坐标变换可写成标准形式或者魏尔斯特拉斯(Weierstrass)形式

引用格式: 陈亦飞. 椭圆曲线的有理数解. 科学通报, 2016, 61: 3638–3643

Chen Y F. Rational solutions of an elliptic curve (in Chinese). Chin Sci Bull, 2016, 61: 3638–3643, doi: 10.1360/N972016-00926

$$y^2 = x^3 + ax + b,$$

其中系数 a, b 是整数, 且判别式 $\Delta = -16(4a^3 + 27b^2) \neq 0$. 这样的曲线称为椭圆曲线. 判别式不为0等价于3次曲线是光滑的. 椭圆曲线的有理数解是本文的主要内容. 接下来我们会通过例子介绍椭圆曲线的有理数解可能有限也可能无穷. 值得一提的是1983年, 法尔廷斯(Faltings)证明了次数大于3的光滑平面曲线只有有限个有理数解.

椭圆曲线理论有广泛的应用, 比如密码学^[1,2]和大数分解^[3]等. 本文将介绍椭圆曲线有理数解的基本结构以及秩的概念. 然后介绍BSD猜想与椭圆曲线秩的深刻联系. 最后介绍与椭圆曲线理论密切相关的费马大定理和同余数问题.

2 椭圆曲线的秩

我们定义的椭圆曲线如图2所示.

从函数图像上看, 椭圆曲线似乎和椭圆没有直接的关系. 事实上, “椭圆曲线”这个名字来自于计算椭圆的周长时, 需要计算以下类型的积分

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

其中分母的函数 $y = \sqrt{x^3 + ax + b}$ 两边平方即是椭圆

图1 平面2次曲线的投影

Figure 1 Projection of a plane conic

图2 椭圆曲线的例子

Figure 2 Examples of elliptic curves

曲线的方程. 这类积分一般无法用初等函数的表达式计算出来.

我们可以把椭圆曲线 E 看成一条射影曲线, 由齐次方程

$$y^2z = x^3 + axz^2 + bz^3$$

定义. 我们称点 $(0,1,0)$ 为射影平面中的无穷远点 ∞ . 记

$$E(\mathbb{Q}) = \{(x, y), \text{ 且 } x, y \in \mathbb{Q} \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$$

其中 a, b 是整数, $\mathbb{Q}$ 是有理数集合.

基本问题: 给定一条椭圆曲线 E , 如何确定集合 $E(\mathbb{Q})$?

例1 令 E 是由方程 $y^2 = x^3 - x$ 定义的椭圆曲线. 令 $y=0$, 我们得到3个整数点 $(0,0)$, $(1,0)$ 和 $(-1,0)$. 则 $E(\mathbb{Q})$ 至少包含这3个点和无穷远点 ∞ . 事实上, 由费马(Fermat)的无穷递降方法可以证明(见文献[4]第II章)

$$E(\mathbb{Q}) = \{(0,0), (1,0), (-1,0), \infty\}.$$

椭圆曲线的有理数集 $E(\mathbb{Q})$ 不仅是一个集合, 还有一个自然的群结构. 群是一种代数结构, 它具有高度对称性. 群 $(S, +)$ 是一个集合 S 上有一个二元结合运算 $+$, 且集合 S 中存在一个单位元又称为零元 e , 使得每个 S 中的元素 a 都存在唯一逆元 b , 满足 $a+b=e$. 通常的例子有整数 $\mathbb{Z}$ 和通常的加法 $+$, 单位元是0, 每个整数 n 的逆元为 $-n$. 又比如二进制数 $\mathbb{Z}_2 = \{0,1\}$, 和二进制的加法, 单位元是0, 由于 $1+1=0$, 所以1的逆元就是1本身. 群的概念是法国天才数学家伽罗瓦(Galois, 1811~1832)在证明一元五次方程没有根式解时引入的. 群的出现极大推动了代数乃至整个数学的发展. 由此可见, 解方程是数学发展的源动力之一.

在复数域上, 计算重数的意义下, 一条直线与椭圆曲线相交3个点. 且容易证明(牛顿首先明确证明): 如果这3个点中有2个是有理数点, 则第3个点也是有理数点. 在 $E(\mathbb{Q})$ 中可以定义如下加法, 任取 $P, Q \in E(\mathbb{Q})$, 通过 P, Q 做直线与椭圆曲线交于点 R ; 如果 $P=Q$, 则取过点 P 的切线与椭圆曲线交于点 R . 由前面的讨论知 $R \in E(\mathbb{Q})$. 定义 $P+Q$ 为 R 关于 x 轴的对称点. 取如图3所示.

可以证明, 在图3加法定义下, $E(\mathbb{Q})$ 是一个交换群, 即 $P+Q=Q+P$, 无穷远点 ∞ 是单位元.

以下是庞加莱在1901年的猜想, 1922年被莫德尔证明.

图3 椭圆曲线 $y^2=x^3-x+1$ 与它的加法Figure 3 addition law of the elliptic curve $y^2=x^3-x+1$

莫德尔定理(Mordell, 1922) 交换群 $E(\mathbb{Q})$ 是有限生成的. 即存在有限个点 $P_1, P_2, \dots, P_t \in E(\mathbb{Q})$, 使得对 $E(\mathbb{Q})$ 中的每个点 P , 都存在整数 $n_1, n_2, \dots, n_t$, $P = n_1 P_1 + n_2 P_2 + \dots + n_t P_t$.

由莫德尔定理和有限生成交换群结构定理知,

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus T,$$

其中 r 是一个非负整数, 称为椭圆曲线的秩, 记作 $\text{rank}(E)$, 子群 T 称为 $E(\mathbb{Q})$ 的扭子群. 扭子群 T 中的元素阶都是有限的.

群中元素 g 的阶定义为最小的正整数 n , 使得 $ng=e$. 如果这个正整数不存在, 则 g 的阶定义为无穷. 比如, 整数群 $\mathbb{Z}$ 中元素1的阶为无穷, 而二进制数 $\mathbb{Z}_2$ 中元素1的阶为2. 回到例1中的椭圆曲线 $y^2=x^3-x$, 点 $P=(1,0)$ 的切线平行于 y 轴(如图2). 按椭圆曲线加法的定义 $2P=P+P=\infty$. 所以点 P 的阶是2. 在图3中, 椭圆曲线 $y^2=x^3-x+1$ 上点 $P=\left(-\frac{11}{9}, \frac{17}{27}\right)$ 的阶为无穷. 这一点虽然不易从椭圆曲线加法的定义中看出, 但我们可以通过下面的纳格-卢茨(Nagell-Lutz)定理得到. 这同时说明了椭圆曲线 $y^2=x^3-x+1$ 有无穷个有理数解.

清楚了椭圆曲线有理解的群结构后, 只需要确定椭圆曲线的秩 r 和扭子群 T , 则 $E(\mathbb{Q})$ 就完全确定了.

定理 椭圆曲线 E 有无穷多有理数解等价于 $\text{rank}(E)>0$.

目前对椭圆曲线的扭子群已经研究得很清楚了.

定理(纳格-卢茨^[5,6]) 令 E 是椭圆曲线 $y^2=x^3+ax+b, a, b \in \mathbb{Z}$. 如果点 $(x, y) \in T$, 且 $(x, y) \neq \infty$, 则

- (1) x, y 是整数;
- (2) $y=0$ 或者 $y^2 \mid 4a^3 + 27b^2$.

我们现在回过头来看例1中的椭圆曲线 $y^2=x^3-x$. 由纳格-卢茨定理, 非平凡的有限阶有理数点 (x, y) , 满足 $y \in \{0, \pm 1, \pm 2\}$. 所以, 我们逐个验算后能找出所有有限阶有理数点是 $\{(-1, 0), (0, 0), (1, 0), \infty\}$.

梅热定理(Mazur, 椭圆曲线扭子群结构定理) 椭圆曲线 E 的扭子群 T 是下列15种群中的一种

- (1) $\mathbb{Z}_n, 1 \leq n \leq 10$, 或 $n=12$;
- (2) $\mathbb{Z}_{2m} \oplus \mathbb{Z}_2, 1 \leq m \leq 4$.

例1中椭圆曲线 $y^2=x^3-x$ 的有理数解集的群结构是 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

相对于 $E(\mathbb{Q})$ 的扭子群, 人们对 $\text{rank}(E)$ 的认识还不够清楚. 目前没有算法确定椭圆曲线的秩, 也不清楚哪些整数能成为椭圆曲线的秩. 关于椭圆曲线的秩有以下猜想.

秩分布猜想(Rank Distribution Conjecture) 秩大于1的椭圆曲线密度为0, 秩0和秩1的椭圆曲线分布相同.

秩分布猜想通俗地讲就是秩0和秩1的椭圆曲线各占一半, 秩取其他值的椭圆曲线很少. 关于这个猜想 目前知道的最好结果是巴尔加瓦(Bhargava)和香卡(Shankar)于2015年发表在 Ann Math 上:

定理(巴尔加瓦-香卡^[7]) 至少5/8的椭圆曲线秩为0或1.

3 BSD猜想

本节我们介绍椭圆曲线领域最重要的猜想——BSD猜想. 它为计算椭圆曲线的秩提供了一个方向.

为了叙述这个猜想, 我们需要做一些准备. 首先对椭圆曲线做模 p 约化, 这是数论中一种重要的技巧. 通常把整数 $\mathbb{Z}$ 的问题约化到有限域 $\mathbb{Z}_p$. 令 E 是由方程 $y^2=x^3+ax+b, a, b \in \mathbb{Z}$, 定义的椭圆曲线. 对任意不整除判别式的素数 p , 即 $p \nmid \Delta = -16(4a^3+27b^2)$, 我们可以将椭圆曲线 E 约化成有限域 $\mathbb{Z}_p$ 上的椭圆曲线 E_p , E_p 在 $\mathbb{Z}_p$ 上的定义方程为 $y^2=x^3+\tilde{a}x+\tilde{b}$, 其中 $\tilde{a}, \tilde{b}$ 分别是整数 a, b 模 p 的余数.

例2, 令 E 是椭圆曲线 $y^2=x^3-5x+2$, 其判别式 $\Delta=-2^3 \cdot 7^2$. 则素数 $3 \nmid \Delta$, 且有限域 $\mathbb{Z}_3$ 上的椭圆曲线 E_3 由方程 $y^2=x^3+x+2$ 定义.

令 $E(\mathbb{Z}_p) = \{(x, y) \in E_p, x, y \in \mathbb{Z}_p\} \cup \{\infty\}$. 由于 $\mathbb{Z}_p$ 是有限域, 所以集合 $E(\mathbb{Z}_p)$ 是个有限集合.

存在一个自然的模 p 约化的群同态, $E(\mathbb{Q}) \rightarrow E(\mathbb{Z}_p)$, $P \mapsto \tilde{P}$. 具体的定义如下:

$$P = \left(\frac{a_1}{b_1}, \frac{a_2}{b_2} \right) \mapsto \tilde{P} = \begin{cases} \left(\frac{\tilde{a}_1}{\tilde{b}_1}, \frac{\tilde{a}_2}{\tilde{b}_2} \right), & \text{如果 } p \nmid b_i, i=1,2, \\ \infty, & \text{其他,} \end{cases}$$

其中 a_i, b_i 是整数, $\tilde{a}_i, \tilde{b}_i$ 分别是 a_i, b_i 模 p 的余数.

贝赫和斯维纳通-戴尔的想法是 $E(\mathbb{Q})$ 越大, 当素数 p 变大时, $E(\mathbb{Z}_p)$ 也相应地变大.

椭圆曲线的哈斯-韦伊(Hasse-Weil) L -函数是一个关于 s 的单变元复函数:

$$L(E, s) = \prod_{p \mid \Delta} \left(1 - \frac{1 + p - N_p}{p^s} + \frac{p}{p^{2s}} \right)^{-1} \times \prod_{p \nmid \Delta} l_p(E, s)^{-1},$$

其中 N_p 是有限集合 $E(\mathbb{Z}_p)$ 的元素个数, $l_p(E, s)$ 是 p^{-s} 的一个多项式, 且 $l_p(E, 1) \neq 0$ [8].

哈斯证明了哈斯-韦伊 L -函数 $L(E, s)$ 当 s 的实部 >1.5 时绝对收敛, 怀尔斯(Wiles)等证明 $L(E, s)$ 可全纯延拓到整个复平面上. 将函数 $L(E, s)$ 在 $s=1$ 处做泰勒展开, 得到

$$L(E, s) = c \cdot (s-1)^r + \text{高次项}, \text{ 其中 } c \neq 0.$$

非负整数 r 是 L -函数 $L(E, s)$ 在 $s=1$ 的阶, 称为椭圆曲线 E 的解析秩(analytic rank), 记为 $\text{rank}_{\text{an}}(E)$.

BSD猜想 对每个椭圆曲线 E , $\text{rank}(E) = \text{rank}_{\text{an}}(E)$.

在假设BSD猜想成立的情况下, $L(E, 1) = 0$ 当且仅当椭圆曲线 E 有无穷个有理数解.

BSD猜想于20世纪60年代提出. 许多数学家致力于这个猜想. 2000年, 美国克雷数学研究所宣布BSD猜想为新千禧年七大数学难题之一, 并为首位证明此猜想的数学家提供百万美元奖金. 它是一个非常困难的猜想, 目前人们对这个猜想知道的不多. 关于BSD猜想的介绍文章很多, 可以参考怀尔斯在千禧年问题中对BSD猜想的介绍 [9].

定理 (科利华金(Kolyvagin) [10, 11], 格罗斯(Gross)-乍基亚(Zagier) [12])

- (1) $\text{rank}_{\text{an}}(E) = 0$, 则 $\text{rank } E = 0$;
- (2) $\text{rank}_{\text{an}}(E) = 1$, 则 $\text{rank } E = 1$.

例1中的椭圆曲线 $E: y^2 = x^3 - x$, 之前用了费马的无限递降方法说明 $E(\mathbb{Q})$ 是有限集. 现在可以利用上述定理说明. 事实上, 由计算机软件计算出 $L(E, 1) = 0.65551438857302295 \dots \neq 0$. 所以 $\text{rank}_{\text{an}}(E) = 0$. 由上面定理(1)得, $\text{rank } E = 0$. 从而 $E(\mathbb{Q})$ 是有限集.

4 费马大定理

费马曾经在丢番图的书中批注如下“结论”, 后来称为费马猜想.

费马猜想 方程 $x^n + y^n = z^n, n > 2, xyz \neq 0$, 没有整数解 (x, y, z) . 当 $n=1$ 或 2 时, 很容易找到无穷个整数解. 与平面曲线有理数解和次数的关系类似, 当 $n > 2$ 时, 方程展现出非常不同的算术性质.

费马本人证明了 $n=4$ 的情形, 并声称自己找到了一般情形的解法. 此后的几百年里, 许多著名数学家致力于解决这个猜想, 但他们都失败了. 直到1995年, 被怀尔斯(Wiles) [13]彻底解决.

椭圆曲线理论在解决费马猜想中起到了关键作用. 事实上, 如果 (a, b, c) 是方程 $x^n + y^n = z^n$ 的一组非平凡解, 则费雷(Frey)曲线 $y^2 = x(x+a^n)(x-b^n)$ 是一条椭圆曲线(虽然不是标准形式). 1990年里贝特(Ribet)证明该曲线不能是模曲线. 而另一方面, 怀尔斯于1995年证明谷山-志村猜想(Taniyama-Shimura conjecture), 推出任何费雷曲线都是模曲线. 从而得到矛盾, 也就证明了费马方程无非平凡整数解.

5 同余数问题

同余数问题是一个经典的数学问题, 暂未彻底解决. 但这个问题与椭圆曲线有无穷个有理数解关系紧密.

给定正整数 n , 是否存在三条边都是有理数的直角三角形, 并且面积恰好是 n ? 如果存在这样的三角形, 就称 n 是同余数. 即对于整数 n , 如果存在正有理数 $x, y, z = \sqrt{x^2 + y^2}$, 使得 $n = \frac{xy}{2}$, 则 n 是同余数.

如果我们令

$$X = \frac{n(x+z)}{y}, \quad Y = \frac{2n^2(x+z)}{y^2},$$

得椭圆曲线方程

$$Y^2 = X^3 - n^2X.$$

事实上, 人们证明了:

定理 n 是同余数等价于上面的椭圆曲线有无限多个有理数解.

滕内尔定理(Tunell's Theorem) 给了同余数问题部分解答; 在假设BSD猜想正确的前提下, BSD猜想给了同余数问题一个完整解答.

滕内尔定理 给定一个无平方因子正整数 n , 定义

$$A_n = \# \{ (x, y, z), x, y, z \in \mathbb{Z} \mid n = 2x^2 + y^2 + 32z^2 \}$$

$$B_n = \# \{ (x, y, z), x, y, z \in \mathbb{Z} \mid n = 2x^2 + y^2 + 8z^2 \}$$

$$C_n = \# \{ (x, y, z), x, y, z \in \mathbb{Z} \mid n = 8x^2 + 2y^2 + 64z^2 \}$$

$$D_n = \# \{ (x, y, z), x, y, z \in \mathbb{Z} \mid n = 8x^2 + 2y^2 + 16z^2 \}$$

假如 n 是同余数, 如果 n 是奇数, 则 $2A_n = B_n$; 如果 n 是偶数, 则 $2C_n = D_n$. 反过来, 如果假设 BSD 猜想对椭圆曲线 $y^2 = x^3 - n^2x$ 成立, 则上面的等式是 n 为同余数的充分条件.

蒙斯基(Monsky)的定理告诉我们如何判断一个

素数是否是同余数.

定理(蒙斯基, 1990) 如果 $p \equiv 3(\bmod 8)$, 则 p 不是同余数, 但 $2p$ 是同余数; 如果 $p \equiv 5(\bmod 8)$, 则 p 是同余数; 如果 $p \equiv 7(\bmod 8)$, 则 p 和 $2p$ 都是同余数.

中国科学院数学与系统科学研究院的田野研究员在同余数问题上取得了如下重要进展:

定理(田野^[14], 2014) 任意给定正整数 k , 在模 8 余 5, 6, 7 的类中有无限多个无平方因子的同余数, 这些同余数恰好是 k 个素因子的乘积.

致谢 田野研究员给予本文一些技术细节的解释. 感谢审稿人的宝贵修改意见.

参考文献

- 1 Miller V S. Use of elliptic curves in cryptography, in Advances in cryptology-CRYPTO'85. Lect Notes in Comp Sci 218, Berlin: Springer-Verlag, 1986. 417–426
- 2 Koblitz N. Elliptic curve cryptosystems. Math Comp, 1987, 177: 203–209
- 3 Lenstra H W. Factoring integers with elliptic curves. Ann Math, 1987, 3: 649–673
- 4 Wiles A. Number Theory, An Approach Through History. Boston: Birkhäuser, 1984
- 5 Nagell T. Solution de quelque problèmes dans la théorie arithmétique des cubiques planes du premier genre. Vid Akad Skrifter Oslo I, 1935, 1: 1–25
- 6 Lutz E. Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p -adic. J Reine Angew Math, 1937, 238–247
- 7 Bhargava M, Shankar A. Ternary cubic forms having bounded invariants and the existence of a positive proportion of elliptic curves having rank 0. Ann Math, 2015, 2: 587–621
- 8 Tate J T. The arithmetic of elliptic curves. Invent Math, 1974, 179–206
- 9 Wiles A. The Birch and Swinnerton-Dyer conjecture. In: Carlson J, Jaffe, Arthur, Wiles, Andrew. The Millennium Prize Problems. Am Math Soc, 2006, 31–44
- 10 Kolyvagin V A. Finiteness of $E(\mathbb{Q})$ and $\text{III}(E, \mathbb{Q})$ for a subclass of Weil curves. Izv Akad Nauk SSSR Ser Mat, 1988, 3: 522–540, 670–671
- 11 Kolyvagin V A. Euler systems. Cartier P, et al, eds. In: The Grothendieck Festschrift (vol II). Prog In Math, 87. Boston: Birkhäuser, 1990, 435–483
- 12 Gross B H, Zagier D B. Heegner points and derivatives of L-series. Invent Math 84, 1986, 2: 225–320
- 13 Wiles A. Modular elliptic curves and Fermat's last theorem. Ann Math, 1995, 3: 443–551
- 14 Tian Y. Congruent numbers and Heegner points. Camb J Math, 2014, 2: 117–161

陈亦飞

2000 年毕业于北京师范大学数学系, 获学士学位. 2003 年毕业于中国科学院数学与系统科学研究院, 获硕士学位. 2009 年毕业于美国 Johns Hopkins University, 获博士学位. 现任中国科学院数学与系统科学研究院副研究员, 中国数学会副秘书长, 研究领域为代数几何. 2011 年起, 主持国家自然科学基金 1 项, 参与国家自然科学基金重点项目 1 项, 国家自然科学基金创新群体项目 1 项. 2013 年访问英国剑桥大学 7 个月. 2015 年访问日本东京大学 7 个月.

Rational solutions of an elliptic curve

CHEN YiFei

Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China

The study of elliptic curves is long standing. A fundamental problem for an elliptic curve is to find all rational solutions. The problem has played and continues to play a fundamental role in the development of many areas of number theory. The theory of elliptic curves was crucial in the proof of Fermat's Last Theorem. In this paper, we introduce rational solutions of lines and conics first. A natural problem of rational solutions of plane cubic arises, which is the problem of rational solutions of an elliptic curve in most cases. There is a natural addition on the rational solutions of an elliptic curve. So the set of rational solutions of an elliptic curve forms an abelian group. In 1922, Mordell proved that the set of rational solutions of an elliptic curve was a finitely generated abelian group, which confirmed a conjecture of Poincaré in 1901. By the fundamental structure theorem of finitely generated abelian group, the group of rational solutions of an elliptic curve is completely determined by its rank and torsion subgroup. The rank of the rational solutions of an elliptic curve is called the rank of the elliptic curve, which is an import invariant of an elliptic curve. Therefore, an elliptic curve having infinitely many rational solutions is equivalent to the rank of elliptic curve being positive. After many efforts, people are clear about the torsion subgroup of the rational solutions of an elliptic curve. However, people know a little about the rank of an elliptic curve. There are many conjectures of the rank of elliptic curves. One of them says most elliptic curves has rank 0 or 1. Birch and Swinnerton-Dyer reduce an elliptic curve over rational numbers to the elliptic curve over a finite field. The advantage of an elliptic curve over a finite field is that its solutions are finite. Then Birch and Swinnerton-Dyer define Hasse-Weil L -function $L(E,s)$ regarding of solutions of the elliptic curve over the finite field. The Hasse-Weil L -function $L(E,s)$ has good analytic properties and is somehow computable. Birch and Swinnerton-Dyer conjecture that the rank of an elliptic curve E and the order of $s=1$ of the Hasse-Weil L -function $L(E,s)$ are equal. The BSD conjecture offers an approach to determine whether an elliptic curve has infinitely many rational solutions. However, the conjecture is extremely difficult, and it was chosen as one of the seven Millennium Prize Problems listed by Clay Mathematics Institute, which has offered a \$1,000,000 prize for the first correct proof. We will introduce current progress of the conjecture. In the end, we introduce Fermat's Last Theorem and congruent numbers. These two problems are closely related to the theory of elliptic curves. Fermat's Last Theorem was complete solved by Wiles in 1995. The problem of congruent numbers is not clear so far. We will introduce the recent important progress of the problem by Chinese mathematician Ye Tian. Besides, important and useful applications of elliptic curves have been found in many fields, such as cryptography, factoring large integers, and primality proving.

Elliptic curves, the Birch and Swinnerton-Dyer conjecture, rank of an elliptic curve

doi: 10.1360/N972016-00926