中国科学 : 数学　2020 年　第 50 卷　第 11 期 : 1525 ~ 1540
SCIENTIA SINICA Mathematica
创刊 70 周年特邀综述

同余数问题和 Goldfeld 猜想

田野[1,2,3,4]

1. 中国科学院数学与系统科学研究院, 北京 100190;
2. 中国科学院大学数学科学学院, 北京 100049;
3. 中国科学院晨兴数学中心, 北京 100190;
4. 中国科学院华罗庚数学重点实验室, 北京 100190
E-mail: ytian@math.ac.cn

收稿日期: 2020-08-05; 接受日期: 2020-09-28; 网络出版日期: 2020-11-03
国家自然科学基金 (批准号: 11688101 和 11531008) 资助项目

摘要　本文介绍同余数问题的最新进展, 特别地, 同余椭圆曲线 Goldfeld 猜想的进展.

关键词　同余数　L 函数　Goldfeld 猜想　Selmer 群的分布

MSC (2010) 主题分类　11G05, 11G40

1　同余数问题

本节用初等语言叙述同余数问题中的基本猜想及结果, 但这些猜想更为系统的背景以及这些结果的建立均涉及后面介绍的椭圆曲线深刻算术理论.

定义 1.1　一个正整数 n 称为同余数, 若它是一个有理直角三角形的面积, 即存在正有理数 a、b 和 c, 使得

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

根据史料记载, 对同余数的研究可追溯到公元 972 年的一份阿拉伯文稿. 人们很早就知道 5、6 和 7 都是同余数 (见 Fibonacci 1225 年的著作《平方数》), 相对应的直角三角形有边长

$$\left(\frac{3}{2},\frac{20}{3},\frac{41}{6}\right),\quad (3,4,5),\quad \left(\frac{35}{12},\frac{24}{5},\frac{337}{60}\right).$$

事实上, Euclid 在《几何原本》中给出了边长为无公因子整数的直角三角形 (称其为本原直角三角形) 的边长公式. 对任意互素正整数 $\alpha>\beta$ 使得 $2\nmid\alpha+\beta$, 则

$$\alpha^2-\beta^2,\quad 2\alpha\beta,\quad \alpha^2+\beta^2$$

英文引用格式: Tian Y. Congruent number problem and Goldfeld conjecture (in Chinese). Sci Sin Math, 2020, 50: 1525–1540, doi: 10.1360/SSM-2020-0244

是一个本原直角三角形的边长. 反之, 任何本原直角三角形的边长都由唯一的一对这样的 (α,β) 给出. 由此不难看出, 一个正整数 n 是同余数当且仅当存在这样的 (α,β) 及有理数 t 使得

$$\alpha\beta(\alpha^2-\beta^2)=nt^2.$$

取 $(\alpha,\beta)=(5,4),(2,1),(16,9)$, 我们就得到了上述对应于 5、6 和 7 的直角三角形.

Fibonacci 在《平方数》中还不加证明地断言 1 不是同余数, 这直到 400 年后 (1659 年) 才由 Fermat 发现无穷下降法给出了其证明. 回顾 Fermat 证明 $n=1,2,3$ 不是同余数的方法. 如不然, 则对某个正整数 t, 存在面积为 nt^2 的本原直角三角形, 即有互素的一奇一偶正整数 α 和 β 使得

$$\alpha\beta(\alpha^2-\beta^2)=nt^2.$$

考虑模 8 的剩余可知, 存在正整数 r、s、u 和 v 使得

$$\alpha=r^2,\quad \beta=ns^2,\quad \alpha+\beta=u^2,\quad \alpha-\beta=v^2.$$

这样, 容易看出

$$\left(\frac{u+v}{2},\frac{u-v}{2},r\right)$$

也是一个整边长直角三角形, 其面积为 $n(s/2)^2$, 但其斜边 $r=\sqrt{\alpha}<\alpha^2+\beta^2$. 除去边长的公因子, 我们得到一个比原来小的本原直角三角形, 它的面积形如 nt_1^2. 这样的过程无限进行下去就给出了矛盾 (没有无限严格下降的正整数序列). 同理可证模 8 余 3 的素数不是同余数. Fermat 发现的这个无穷下降法有相当深远的影响, 例如, 后面会看到 Mordell 在 1922 年建立的椭圆曲线上有理点形成一个有限生成交换群的这一重要定理就深受它的影响.

上面阐述的方法使得人们有如下更多同余数和非同余数的例子 (浅灰部分为非同余数):

$n \bmod 8$	1	2	3	5	6	7
n	1	2	3	5	6	7
	9	10	11	13	14	15
	17	18	19	21	22	23
	25	26	27	29	30	31
	33	34	35	37	38	39
	41	42	43	45	46	47
	⋯	⋯	⋯	⋯	⋯	⋯
	217	218	219	221	222	223
	⋯	⋯	⋯	⋯	⋯	⋯

这些数据使得人们猜测任意模 8 余 5、6 和 7 的正整数都是同余数 (参见文献 [1]), 而模 8 余 1、2 和 3 的正整数是同余数的概率为 0. 下面给出同余数研究中的关键问题, 其中最基本的问题如下:

基本问题 是否存在一个算法, 通过有限步能判断一个给定的正整数是否为同余数? 对同余数, 怎样找出所有对应的直角三角形.

由文献 [2] 知, 若假设椭圆曲线的 BSD 猜想成立, 则对一个无平方因子的正整数 n, 使得若 n 为奇数, 令 $a=1$, 否则令 $a=2$, 则 n 为同余数当且仅当三元二次型方程

$$\frac{n}{a}=2ax^2+y^2+8z^2,\quad x,y,z\in\mathbb{Z}$$

的整数解中 z 为奇数的解与 z 为偶数的解个数相同. 事实上, 由 Coates 和 Wiles [3] 在 Birch 和 Swinnerton-Dyer (BSD) 猜想方面的工作知, 上述论断的必要性方向成立 (从而 Tunnell 获得了非同余数的一个充分性条件, 例如, 我们由它可知 1、2 和 3 不是同余数). 这样如果假设 BSD 猜想成立, 上述问题的前半部分有肯定的解答. 在 Tunnell (基于 Coates-Wiles 和 Shimura-Waldspurger) 的工作后, 上述基本问题遗留部分可叙述如下:

基本猜想一 假设三元二次型方程

$$\frac{n}{a}=2ax^2+y^2+8z^2,\quad x,y,z\in\mathbb{Z}$$

的整数解中 z 为奇数的解与为偶数的解个数一样多, 则 n 为同余数, 进而存在一个有效算法在有限步找出它所对应的所有有理边长直角三角形.

上述猜想本质是 BSD 猜想. 对模 8 余 5、6 和 7 的正整数 n, 我们可知 $2ax^2+y^2+8z^2=n/a$ 无解, 从而 n 为同余数.

关于非同余数的分布有如下基本猜测: 模 8 余 1、2 和 3 的正整数是同余数的概率为 0. Goldfeld [4] 有如下一个更强的猜测 (这之所以更强是由于前面提到的 Coates-Wiles 的工作):

基本猜想二 (偶情形 Goldfeld 猜想) 对几乎所有 (按概率 100%) 的模 8 余 1、2 和 3 的无平方因子的正整数 n, 三元二次型方程

$$\frac{n}{a}=2ax^2+y^2+8z^2,\quad x,y,z\in\mathbb{Z}$$

的整数解中 z 为奇数的解与为偶数的解个数不等.

注意, 上面的基本猜想一已经猜测任意模 8 余 5、6 和 7 的正整数都是同余数. 我们稍后会看到 Goldfeld [4] 对模 8 余 5、6 和 7 的情形类似基本猜想二, 也有一个 "极小情形概率为 1" 的猜想 (参见猜想 2.8).

定理 1.2 [5,6] 对任意整数 $k\geqslant 1$, 在每个模 8 余 5、6 和 7 的剩余类中都存在无穷多恰有 k 个奇素因子的无平方因子同余数.

定理 1.3 [7,8] 在每个模 8 余 5、6 和 7 的剩余类中, 同余数都有正密度.

定理 1.4 [9] 在模 8 余 1、2 和 3 的正整数中, 同余数出现的概率为 0.

定理 1.5 [10] 关于上述同余数的偶情形, Goldfeld 猜想成立.

注 1.6 对任意大于 2 的整数 m, $m(m^2-1)$ 都是一个同余数. 由此不难证明对每个模 8 余 1、2 和 3 的剩余类都存在无穷多个无平方因子的同余数.

2 椭圆曲线

本节以同余数问题引入椭圆曲线, 首先讲述 Mordell-Weil 群的有限生成性与 Fermat 无穷下降法的联系, 进而提出关于 L- 函数在中心点处 Taylor 展式的首项的 3 个基本问题, 最后给出本文主要概述的结果 (参见主定理 B).

从上面的讨论易知, n 是一个同余数当且仅当存在非零整数 α 和 β 及有理数 t 使得

$$nt^2=\alpha\beta(\alpha+\beta)(\alpha-\beta)\quad 或\quad n\left(\frac{t}{\beta^2}\right)^2=\frac{\alpha}{\beta}\left(\left(\frac{\alpha}{\beta}\right)^2-1\right),$$

从而当且仅当椭圆曲线

$$E^{(n)}: ny^2z=x^3-xz^2$$

存在使得 $y\neq 0$ 的有理数解 $[x:y:1]$. 注意, 曲线 $E^{(n)}$ 有另一个等价的定义方程 $y^2z=x^3-n^2xz^2$. 一般地, 有理数域 $\mathbb{Q}$ 上的椭圆曲线是指定义在有理数域上的亏格 1 的射影光滑代数曲线且带有一个有理点 O, 或等价地, 是射影平面上由如下方程定义的一条光滑曲线:

$$A: y^2z=x^3+axz^2+bz^3,\quad a,b\in\mathbb{Q}.$$

其上有理点的集合 $A(\mathbb{Q})$ 有 Abel 群的结构: 以 $O=[0:1:0]$ 为零元, 三点 P、Q 和 R 共线当且仅当 $P+Q+R=O$. 以同样的方式, A 上坐标为代数数的点形成一个交换群 $A(\overline{\mathbb{Q}})$. 特别地, $A(\overline{\mathbb{Q}})$ 上的满足 $2P=O$ 的点 P 构成一个 4 阶群 $A[2]=\{[x:y:1]\in A(\overline{\mathbb{Q}})\mid y=0\}\cup\{O\}$.

定理 2.1 [11] 令 $A/\mathbb{Q}$ 为定义在有理数域上的椭圆曲线, 则 $A(\mathbb{Q})$ 为一个有限生成的交换群.

记 $A(\mathbb{Q})$ 的秩为 $\operatorname{rank}A(\mathbb{Q})$, 也称为 A 的秩. 记 $A(\mathbb{Q})$ 的扭子群为 $A(\mathbb{Q})_{\mathrm{tor}}$.

命题 2.2 对椭圆曲线 $E^{(n)}: y^2=x^3-n^2x$, 有 $E^{(n)}(\mathbb{Q})_{\mathrm{tor}}=E^{(n)}[2]\cong(\mathbb{Z}/2\mathbb{Z})^2$.

推论 2.3 一个正整数 n 为同余数当且仅当 $E^{(n)}$ 的秩为正.

现在回顾用椭圆曲线语言描述的 Fermat 无穷下降法以及它在 Mordell 定理证明中所扮演的重要角色. 假设 A 为椭圆曲线且 $A[2]\subset A(\mathbb{Q})$, 不妨记它的方程为 $A: y^2=(x-c_1)(x-c_2)(x-c_3)$. 对 A 中任意一个满足 $x\neq c_i$ 的有理点 (x,y), 记

$$x-c_i=m_iy_i^2,\quad 1\leqslant i\leqslant 3$$

和 $m=(m_1,m_2,m_3)$, 其中 m_i 为 $x-c_i$ 的平方自由部分 (例如, $-\frac{3\cdot 125}{4\cdot 7}=(-3\cdot 5\cdot 7)\cdot(5/2\cdot 7)^2$), 则 $[y_1,y_2,y_3,1]$ 为 $\mathbb{P}^3$ 中如下定义的射影曲线 $C(m)$ 的一个有理点:

$$C(m): m_iy_i^2-m_jy_j^2=(c_j-c_i)t^2,\quad 其中\ 1\leqslant i<j\leqslant 3.$$

$C(m)$ 为 A 的一个 2 覆盖. 考虑如下集合 (也可看成 $(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^{3,N=1}$ 的子群):

$$\{(m_1,m_2,m_3)\mid m_i\ 无平方因子,\ m_1m_2m_3\ 为平方数, C(m)(\mathbb{Q})\neq\emptyset\},$$

则逐项相乘给出了该集合的乘法群结构. 由此, 有群同构:

$$\kappa: A(\mathbb{Q})/2A(\mathbb{Q})\xrightarrow{\sim}\{(m_1,m_2,m_3)\mid m_i\ 无平方因子,\ m_1m_2m_3\ 为平方数, C(m)(\mathbb{Q})\neq\emptyset\}.$$

为使 $C(m)$ 在局部域 $\mathbb{Q}_p$ 上有解, m_i 的素因子必须整除 $2\prod(c_i-c_j)$. 回到 Fermat 考虑的情形, $E^{(n)}: y^2=x^3-n^2x$, 此处 $n=1,2,3$. 考虑 $E^{(n)}(\mathbb{Q})$ 上的非扭点 $P_1=(n\alpha/\beta, n^2t/\beta^2)$, 其中 $(\alpha,\beta)=1, 2\nmid\alpha+\beta$. 考虑模 8 的剩余, 我们知道

$$\alpha=r^2,\quad \beta=ns^2,\quad \alpha+\beta=u^2,\quad \alpha-\beta=v^2,$$

从而 P_1 对应的 2- 覆盖有

$$(m_1,m_2,m_3)=\left(\frac{n\alpha}{\beta},\frac{n\alpha}{\beta}-n,\frac{n\alpha}{\beta}+n\right)=(1,1,1),$$

因而是平凡的. 故 $E^{(n)}(\mathbb{Q})/2E^{(n)}(\mathbb{Q})\cong E^{(n)}[2]$, 可知存在 $P_2\in A(\mathbb{Q})$ 使得 $P_1\in 2P_2+E^{(n)}[2]$ 但是 P_2 比 P_1 的 "高度" 更小, 这里 P_1 的高度可以认为是对应直角三角形的斜边 $\alpha^2+\beta^2$. 上述过程实际上给出了 Mordell 定理的证明的本质部分, 即对 $\mathbb{Q}$ 上椭圆曲线 A,

(1) $A(\mathbb{Q})/2A(\mathbb{Q})$ 是有限的;

(2) 存在一个正定二次的高度函数 $\widehat{h}: A(\mathbb{Q})\otimes_{\mathbb{Z}}\mathbb{R}\to\mathbb{R}$ 具有如下性质: 对任意常数 $C>0$, 满足 $\widehat{h}(P)<C$ 的点 $P\in A(\mathbb{Q})$ 个数有限.

对 $\mathbb{Q}$ 上椭圆曲线 A, 可以定义类似于 Riemann zeta 函数的一个解析不变量, 称为 A 的 L 函数, 记作 $L(A,s)$. 它定义为一个 Euler 乘积

$$L(A,s):=\prod_p L_p(A,s).$$

这里 p 取遍所有素数, 假设 Δ 为 A 的判别式, 不整除 2Δ 的素位 p 处的 Euler 因子

$$L_p(A,s)=(1-a_p(A)p^{-s}+p^{1-2s})^{-1},$$

其中若令 $\widetilde{A}$ 为 A 在 p 处的约化, 则 $a_p(A):=p+1-\#\widetilde{A}(\mathbb{F}_p)$. 对整除 2Δ 的坏素位处的局部 L 函数的定义参见文献 [12]. 例如, 对无平方因子正整数 n, 椭圆曲线 $E^{(n)}: y^2=x^3-n^2x$ 在所有坏素数 $p\mid 2n$ 处的 Euler 因子 $L_p(E^{(n)},s)=1$. 对于定义在数域上的椭圆曲线, 我们也类似地定义 L 函数.

椭圆曲线 A 的 L 函数收集了其局部信息 $\#\widetilde{A}(\mathbb{F}_p)$, 且 Euler 乘积在 $\Re(s)>3/2$ 时绝对收敛.

定理 2.4 [13–15] 设 A 是 $\mathbb{Q}$ 上椭圆曲线, 则其 L 函数 $L(A,s)$ 有全纯延拓至整个复平面且满足对称点为 $s=1$ 的函数方程

$$\Lambda(A,s):=N^{s/2}\cdot 2(2\pi)^{-s}\Gamma(s)L(A,s)=\epsilon(E)\Lambda(A,2-s),$$

其中 $N\in\mathbb{Z}_{\geqslant 1}$ 为 A 的导子, $\epsilon(A)\in\{\pm 1\}$ 为 $L(A,s)$ 的根数.

例 2.5 令 n 为一个无平方因子的正整数, 则 $E^{(n)}$ 的 L 函数的根数为

$$\epsilon(E^{(n)})=\begin{cases}+1, & \text{若 } n\equiv 1,2,3 \pmod 8,\\ -1, & \text{若 } n\equiv 5,6,7 \pmod 8.\end{cases}\tag{2.1}$$

对于椭圆曲线 A 的算术, 其 L 函数在对称中心 $s=1$ 处 Taylor 展式的首项系数尤为重要:

$$L(A,s)=a_r(s-1)^r+(\text{高次项}),\quad a_r\neq 0.$$

其中首项次数 r 记作 $\mathrm{ord}_{s=1}L(A,s)$. 我们关心首项 $a_r(s-1)^r$ 的如下问题:

(1) 它的算术意义. BSD 猜想断言首项次数 r 等于 $A(\mathbb{Q})$ 的秩, 而首项系数由包括 A 的 Mordell-Weil 群 $A(\mathbb{Q})$ 及 Shafarevich-Tate 群 $Ш(A/\mathbb{Q})$ 等算术不变量给出.

(2) 它在 A 的二次扭族中的变化行为. 关于首项次数 r 有 Goldfeld 猜想, 以及 a_r 的 "代数部分" 的分布和特殊值 $L(A,1)$ 的模性 (猜测参见猜想 2.9).

(3) 它和 "motivic" 对象的关系. 例如, 令 K 是一个虚二次数域, A_K 为 A 在 K 上的基变换, 当 A_K 的根数为 $+1$ 时, Waldspurger 公式联系了 $L(A_K,1)$ 和环面周期; 当根数为 -1 时, Gross-Zagier 公式联系了 $L'(A_K,1)$ 和 Heegner 点.

现在给出以上 (1) 和 (2) 中所涉及内容的细节 (关于 (3) 见第 3 和 4 节, 特别地见定理 4.7 和 3.9). 首先回顾 BSD 猜想. 椭圆曲线的 Shafarevich-Tate 群如下定义, 它被猜测是一个有限群:

$$Ш(A/\mathbb{Q}) := \ker\left(H^1(\mathbb{Q},A)\to\prod_v H^1(\mathbb{Q}_v,A)\right).$$

猜想 2.6 (BSD 猜想) 令 $A/\mathbb{Q}$ 为一条椭圆曲线, 则 $L(A,s)$ 的首项次数有

$$r := \mathrm{ord}_{s=1}L(A,s) = \mathrm{rank}_{\mathbb{Z}}A(\mathbb{Q}),$$

首项系数的代数部分 (称为 A 的解析 Sha)

$$\mathcal{L}(A) := \frac{L^{(r)}(A,1)}{r!\cdot R(A)\cdot\Omega(A)}\cdot\frac{(\#A(\mathbb{Q})_{\mathrm{tor}})^2}{\prod_\ell c_\ell(A)} = \#Ш(A/\mathbb{Q}),$$

其中 $R(A)$、$\Omega(A)$ 和 $c_\ell(A)$ 分别为 A 的正则子、周期和在素数 ℓ 处的 Tamagawa 数 (参见文献 [12]).

对一个素数 p, 若上述等式两边均为非零有理数且 p 进赋值相等, 则称 A 的 p 部分 BSD 猜想成立.

注 2.7 假设 BSD 猜想成立, 则存在一个有效算法来给出正则子的上界, 从而给出一个有效算法来计算 $A(\mathbb{Q})$ 的生成元 (参见文献 [16]).

关于 L 函数特殊值在二次扭族中的变化行为, 有如下猜想.

猜想 2.8 [4] 令 $A: y^2=x^3+ax+b$ 为 $\mathbb{Q}$ 上的椭圆曲线, 对无平方因子整数 n, 称

$$A^{(n)}: ny^2 = x^3+ax+b$$

为 A 的在 $\mathbb{Q}(\sqrt{n})$ 上的二次扭. 对整数 $r\geqslant 0$, Goldfeld 猜测如下:

$$\mathrm{Prob}\left(\mathop{\mathrm{ord}}_{s=1}L(A^{(n)},s)=r\right) = \begin{cases}\dfrac{1}{2}, & \text{若 } r=0,1,\\ 0, & \text{若 } r\geqslant 2.\end{cases}$$

关于 L 函数的首项系数在二次扭族中的分布, 我们有如下猜测.

猜想 2.9 (解析 Sha 的分布猜想) 令 $A/\mathbb{Q}$ 为一条椭圆曲线, 满足 $A[2]\subset A(\mathbb{Q})$ 且 A 没有定义在 $\mathbb{Q}$ 上的 4 阶循环子群, 则对 $r=0,1$ 和 $t\in\mathbb{Z}_{\geqslant 0}$, 有

$$\mathrm{Prob}(\mathrm{ord}_2(\mathcal{L}(A^{(n)}))=2t, \mathrm{ord}_{s=1}L(A^{(n)},s)=r \mid \epsilon(A^{(n)})=(-1)^r) = \pi_{r,t},$$

其中

$$\pi_{r,t} := \lim_{\substack{n\to\infty\\ n\equiv r \bmod 2}} \mathrm{Vol}(\{M\in X_r(n)\mid \#\mathrm{coker}(M)_{\mathrm{tor}}=2^{2t}\}),$$

这里 $X_r(n)$ 为如下的带有典范概率测度的 2- 进集合:

$$X_r(n) := \{M\in M_{n\times n}(\mathbb{Z}_2)\mid {}^tM=-M, \mathrm{corank}(M)=r\}.$$

注 2.10 这里, 赋予 $X_r(n)$ 以 2- 进拓扑, 记 d 为 $X_r(n)$ 的维数. 可知在 $X_r(n)$ 的 Borel σ- 代数上存在一个唯一的有界实值测度 μ (参见文献 [17]) 使得对任意的 $X_r(n)$ 的既开又闭子集 S, 有

$$\mu(S)=\lim_{m\to\infty}\frac{\#\{S\text{ 在 }M_{n\times n}(\mathbb{Z}_2/2^m\mathbb{Z}_2)\text{ 中的像}\}}{2^{md}}.$$

上述定理中的概率测度为 $\frac{1}{\mu(X_r(n))}\mu$.

本文主要概述主定理 (见定理 1.3 和 1.5) 如下.

主定理 A [10] 对于同余椭圆曲线 $E:y^2=x^3-x$, Goldfeld 猜想对 E 的二次扭族和 $r=0$ 成立.

主定理 B 对同余椭圆曲线 $E:y^2=x^3-x$, 有

B_0: 解析 Sha 分布猜想对 E 的二次扭族和 $r=t=0$ 成立, 即

$$\mathrm{Prob}(\mathrm{ord}_2(\mathcal{L}(E^{(n)}))=0,\mathrm{ord}_{s=1}L(A^{(n)},s)=0\mid\epsilon(E^{(n)})=1)=\pi_{0,0},$$

B_1: 对 $r=1$ 和 $t=0$ 有

$$\mathrm{Prob}(\mathrm{ord}_2(\mathcal{L}(E^{(n)}))=0,\mathrm{ord}_{s=1}L(A^{(n)},s)=1\mid\epsilon(E^{(n)})=-1)\geqslant\frac{2}{3}\pi_{1,0}.$$

3 椭圆曲线的基本算术理论

现在解释在上述 Goldfeld 猜想及解析 Sha 分布的结果中所涉及的思想方法. 我们从同余数椭圆曲线二次扭族的偶 Goldfeld 猜想开始. 令 n 为一个无平方因子正整数, 令 $a=1$, 若 n 为奇数; 令 $a=2$, 若 n 为偶数. 定义

$$\begin{aligned}\mathcal{L}(n):=&\#\left\{(x,y,z)\in\mathbb{Z}^3\;\middle|\;2ax^2+y^2+8z^2=\frac{n}{a},2\mid z\right\}\\&-\#\left\{(x,y,z)\in\mathbb{Z}^3\;\middle|\;2ax^2+y^2+8z^2=\frac{n}{a},2\nmid z\right\}.\end{aligned}$$

重述定理 1.5 (主定理 A 的等价形式) 如下:

主定理 A′ 在所有满足 $n\equiv1,2,3\ (\mathrm{mod}\ 8)$ 的无平方因子正整数中, 那些使得 $\mathcal{L}(n)\neq0$ 的 n 的密度为 1, 即

$$\mathrm{Prob}(\mathcal{L}(n)\neq0\mid n\equiv1,2,3\ (\mathrm{mod}\ 8)\text{ 无平方因子正整数})=1.$$

证明 由定理 3.6–3.8 可得. □

上述定理的证明基于椭圆曲线的算术, 其中 Selmer 群是一个基本对象.

3.1 Selmer 群

假设 $A[2]\subset A(\mathbb{Q})$, 沿用上一小节的记号, 定义

$$\mathrm{Sel}_2(A/\mathbb{Q}):=\{(m_1,m_2,m_3)\mid m_i\text{ 平方自由},m_1m_2m_3\text{ 为平方数},C(m)(\mathbb{Q}_v)\neq\emptyset,\forall v\},$$

则该集合有限 (因为 m_i 只能被 $2\prod(c_i-c_j)$ 的素因子整除). 故有如下 2- 递降过程:

$$\kappa:A(\mathbb{Q})\twoheadrightarrow A(\mathbb{Q})/2A(\mathbb{Q})\hookrightarrow\mathrm{Sel}_2(A/\mathbb{Q}).$$

记 $Ш(A/\mathbb{Q})[2]$ 为上述映射的商. 可知若 $\mathrm{Sel}_2(A/\mathbb{Q})/\kappa(A(\mathbb{Q})_{\mathrm{tor}})=0$, 则 A 的秩为 0.

猜想 3.1 $\dim_{\mathbb{F}_2} Ш(A/\mathbb{Q})[2]$ 为偶数. 特别地, 若 $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/\mathbb{Q})/\kappa(A(\mathbb{Q})_{\mathrm{tor}})$ 为奇数, 则 A 的秩为正.

对同余椭圆曲线 $E^{(n)}$, 有

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^{(n)}/\mathbb{Q})/\kappa(E^{(n)}(\mathbb{Q})_{\mathrm{tor}}) \begin{cases} \text{是偶数}, & \text{若 } n \equiv 1,2,3 \pmod 8, \\ \text{是奇数}, & \text{若 } n \equiv 5,6,7 \pmod 8. \end{cases}$$

因此, 由上述猜想可以得到任意模 8 余 5、6 和 7 的正整数都是同余数.

问题 3.2 当 $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/\mathbb{Q})/\kappa(A(\mathbb{Q})_{\mathrm{tor}}) = 1$ 时, 如何构造一个 $A(\mathbb{Q})$ 中的非挠元素并且证明 A 的秩为 1?

注 3.3 [7] 假设 $n = p_1 \cdots p_{2k+1}$ 无平方因子, 其中 p_i 为模 8 余 5 的满足对任意 $i \neq j$ 都有 $(\frac{p_i}{p_j}) = -1$ 成立的素数, 则 $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^{(n)}/\mathbb{Q})/\kappa(E^{(n)}(\mathbb{Q})_{\mathrm{tor}}) = 1$ 且 n 是同余数.

基于 Heath-Brown、Swinnerton-Dyer 和 Kane 的工作, 有如下描述 Selmer 群在二次扭族中变化行为的定理:

定理 3.4 [18–20] 假设 $A/\mathbb{Q}$ 为一条满足 $A[2] \subset A(\mathbb{Q})$ 的椭圆曲线, 且 A 没有 4 阶循环子群, 那么对任意自然数 d, 均有

$$\mathrm{Prob}(\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A^{(n)}/\mathbb{Q})/\kappa(A^{(n)}(\mathbb{Q})_{\mathrm{tor}}) = d) = \frac{2^d}{\prod_{j=1}^{d}(2^j-1)\prod_{j=0}^{\infty}(1+2^{-j})}.$$

一般 Selmer 群的定义需要 Galois 上同调. 对一条椭圆曲线 $A/\mathbb{Q}$ 和一个素数方幂 p^n, 有 Kummer 映射

$$\kappa : A(\mathbb{Q})/p^nA(\mathbb{Q}) \hookrightarrow H^1(\mathbb{Q}, A[p^n]), \quad P \mapsto \left(\sigma \mapsto (\sigma - 1)\left(\frac{P}{p^n}\right)\right).$$

类似地, 有局部 Kummer 映射 $\kappa_v : A(\mathbb{Q}_v)/p^nA(\mathbb{Q}_v) \hookrightarrow H^1(\mathbb{Q}_v, A[p^n])$. 有如下的交换图表成立:

$$\begin{array}{ccc} A(\mathbb{Q})/p^nA(\mathbb{Q}) & \xrightarrow{\kappa} & H^1(\mathbb{Q}, A[p^n]) \\ \downarrow & & \downarrow \\ \prod_v A(\mathbb{Q}_v)/p^nA(\mathbb{Q}_v) & \xrightarrow{\prod_v \kappa_v} & \prod_v H^1(\mathbb{Q}_v, A[p^n]). \end{array}$$

定义 A 的 p^n-Selmer 群为

$$\mathrm{Sel}_{p^n}(A/\mathbb{Q}) := \ker\left(H^1(\mathbb{Q}, A[p^n]) \to \prod_v \frac{H^1(\mathbb{Q}_v, A[p^n])}{\Im(\kappa_v)}\right).$$

可知 $\mathrm{Sel}_{p^n}(A/\mathbb{Q})$ 为一个有限交换群, 且满足如下的短正合列:

$$0 \to A(\mathbb{Q})/p^nA(\mathbb{Q}) \xrightarrow{\kappa} \mathrm{Sel}_{p^n}(A/\mathbb{Q}) \to Ш(A/\mathbb{Q})[p^n] \to 0.$$

类似地, 定义 A 的 p^∞-Selmer 群为

$$\mathrm{Sel}_{p^\infty}(A/\mathbb{Q}) := \ker\left(H^1(\mathbb{Q}, A[p^\infty]) \to \prod_v \frac{H^1(\mathbb{Q}_v, A[p^\infty])}{\Im(A(\mathbb{Q}_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(\mathbb{Q}_v, A[p^\infty]))}\right).$$

它是余有限生成 $\mathbb{Z}_p$ 模, 带有辛结构, 且满足如下正合列:

$$0 \to A(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(A/\mathbb{Q}) \to Ш(A/\mathbb{Q})[p^\infty] \to 0.$$

Bhargava-Kane-Lenstra-Poonen-Rains 提出如下猜想 (BKLPR 猜想).

猜想 3.5 [17] 椭圆曲线 A 按照高度排序, 对给定的 r 和有限辛 p- 群 G, 有如下概率的分布:

$$\begin{aligned}&\mathrm{Prob}(\mathrm{Sel}_{p^\infty}(A/\mathbb{Q})\cong(\mathbb{Q}_p/\mathbb{Z}_p)^r\oplus G)\\&=\frac{(\#G)^{1-r}}{\#\,\mathrm{Aut}(G)}\times\begin{cases}\dfrac{1}{2}\displaystyle\prod_{i=r+1}^{\infty}(1-p^{1-2i}), & \text{若 } r=0,1,\\ 0, & \text{若 } r\geqslant 2,\end{cases}\end{aligned}$$

这里 $\mathrm{Aut}(G)$ 为保持辛结构的自同构群.

在二次扭族中, 可以猜测 $\mathrm{Sel}_{2^\infty}(A/\mathbb{Q})$ 的分布也遵从上述对所有椭圆曲线的分布行为的某种修正. 特别地, 当 $A[2]\subset A(\mathbb{Q})$ 且没有定义在 $\mathbb{Q}$ 上的 4 阶循环子群时, 两种分布是一致的 (见下面定理 3.6).

现在概述主定理 A′ 的证明, 其主要通过如下定理得到:

定理 3.6 [8,9] 假设 $A/\mathbb{Q}$ 为一条椭圆曲线且满足如下条件:

- 所有 A 的 2- 挠点都是有理的;
- A 没有定义在 $\mathbb{Q}$ 上的 4 阶循环子群,

则在 A 的满足根数为 $+1$ (或 -1) 的二次扭族 $\{A^{(n)}\}$ 中, 满足 $\mathrm{corank}_{\mathbb{Z}_2}\mathrm{Sel}_{2^\infty}(A^{(n)}/\mathbb{Q})=0$ (或 $=1$) 的子集的密度为 1, 即对 $r=0,1$,

$$\mathrm{Prob}(\mathrm{corank}_{\mathbb{Z}_2}\mathrm{Sel}_{2^\infty}(A^{(n)}/\mathbb{Q})=r\mid\epsilon(A^{(n)})=(-1)^r)=1.$$

更进一步地, 对任意整数 $r\geqslant 0$ 和任意辛 2- 群 G, 有

$$\begin{aligned}&\mathrm{Prob}(\mathrm{Sel}_{2^\infty}(A/\mathbb{Q})\cong(\mathbb{Q}_2/\mathbb{Z}_2)^r\oplus G)\\&=\frac{(\#G)^{1-r}}{\#\,\mathrm{Aut}(G)}\times\begin{cases}\dfrac{1}{2}\displaystyle\prod_{i=r+1}^{\infty}(1-2^{1-2i}), & \text{若 } r=0,1,\\ 0, & \text{若 } r\geqslant 2.\end{cases}\end{aligned}$$

定理 3.7 [21] 1) 令 $A/\mathbb{Q}$ 为一条带复乘的 (with complex multiplication, CM) 椭圆曲线, p 为任意一个素数, 则

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(A/\mathbb{Q})=0\quad\text{当且仅当}\quad L(A,1)\neq 0.$$

更一般地, 令

- $f\in S_k(\Gamma_1(N))$ 为一个 CM 特征模形式, k 为偶数;
- p 为任意素数;
- F 为 f 的系数域;
- λ 为一个 F 的位于 p 之上的素位;
- $V_{F_\lambda}(f)$ 为 f 对应的 λ- 进 Galois 表示,

则

$$H^1_f\left(\mathbb{Q},V_{F_\lambda}(f)\left(\frac{k}{2}\right)\right)=0\quad\text{当且仅当}\quad L\left(f,\frac{k}{2}\right)\neq 0,$$

其中 H^1_f 为 Bloch-Kato Selmer 群 (参见文献 [22]).

基于 Waldspurger-Shimura 的工作, Tunnell 有如下结果 (Qin 在脚注 2) 中给出了新证明):

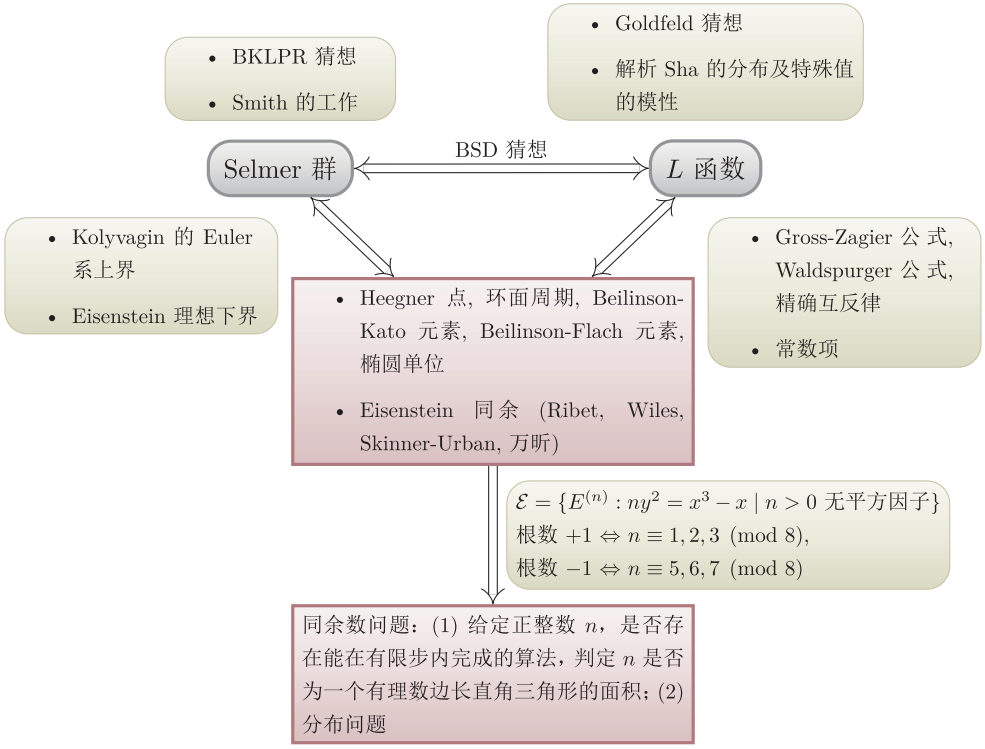
1) Ashay B, Tian Y. A rank zero p converse to a theorem of Gross-Zagier, Kolyvagain and Rubin II. Preprint
2) Qin H R. Congruent numbers, quadratic forms and K_2. Preprint

定理 3.8 [23] $L(E^{(n)},1)\neq 0$ 当且仅当 $\mathcal{L}(n)\neq 0$. 更精确地, 存在权为 3/2 的模形式 $\sum_{n=1}^{\infty}a_nq^n\in S_{3/2}(128,\chi_1)$ 和 $\sum_{n=1}^{\infty}b_nq^n\in S_{3/2}(128,\chi_2)$, 使得对所有的平方自由的 $n\in\mathbb{Z}_{\geqslant 0}$, 有

$$\mathcal{L}(n)=\begin{cases}a_n,\\ b_{n/2},\end{cases}\quad \text{以及}\quad \frac{L(E^{(n)},1)}{\Omega/\sqrt{n}}=\begin{cases}\dfrac{a_n^2}{16}, & \text{若 } n\equiv 1,3 \pmod 8,\\ \dfrac{b_{n/2}^2}{8}, & \text{若 } n\equiv 2 \pmod 8,\end{cases}$$

其中 $\Omega=\int_1^{\infty}\frac{dx}{\sqrt{x^3-x}}$.

为了研究关于 L 函数的 Goldfeld 猜想, 我们基于 Selmer 群的分布 (例如, Smith 的工作), 然后通过 BSD 猜想上的结果过渡到 L 函数的分布行为. 而 BSD 方面的结果是由椭圆单位和 Beilinson-Flach 元素的研究得到. 一般地, 关于椭圆曲线的算术, 有如下图表.



下面证明主定理 B. 由于还不能直接证明 2 部分 BSD 公式, 因此定理 B_0 的建立利用了环面周期.

主定理 $\mathbf{B_0}$ 在所有模 8 余 1、2 和 3 的正整数中,

$$\mathrm{Prob}(2^{-\mu(n)}\mathcal{L}(n)\text{ 是奇数})=\pi_{0,0}=\prod_{n=1}^{\infty}(1+2^{-n})^{-1}=0.4194\cdots,$$

其中 $\pi_{0,0}$ 如猜想 2.9 所示. 特别地,

$$\mathrm{Prob}(\mathcal{L}(n)\neq 0\mid n\equiv 1,2,3 \pmod 8)\geqslant\pi_{0,0}.$$

证明 由定理 3.10、3.4 和 3.11 可得. □

在该证明中, 一个关键步骤是应用环面周期的 Waldspurger 公式. 下面给出 Waldspurger 公式的一个简单应用, 其方法也是后面用归纳法证明定理 3.10 的初始步骤.

定理 3.9 假设 p 为模 8 余 3 的一个素数, 则

$$\mathcal{L}(E^{(p)}) \in 1+2\mathbb{Z},$$

其中 $\mathcal{L}(E^{(n)}) = 2^{-\mu(n)}\mathcal{L}(n)$.

证明概要如下. 考虑定义在 $\mathbb{Q}$ 上只在 2 和 ∞ 处分歧的四元数代数 $\mathbb{B}$. 记 $K=\mathbb{Q}(\sqrt{-p})$. 令 R 为 B 的一个阶使得其判别式等于 32 且存在嵌入 $\mathcal{O}_K \to R$, 则上述嵌入诱导了映射 $\mathrm{Pic}(\mathcal{O}_K) \to X_R := B^\times \backslash \widehat{B}^\times / \widehat{R}^\times$. 记 f 为文献 [24] 中的 $\mathbb{Z}$ 本原的测试向量, 则 Waldspurger 公式将 L 函数 $L(E_K,1)$ 与周期 $P_K(f)=\sum_{t\in \mathrm{Pic}(\mathcal{O}_K)} f(t)$ 联系起来:

$$P_K(f) = \pm \mu_K \mathcal{L}(E)\mathcal{L}(E^{(p)}),$$

其中 $\mu_K = [\mathcal{O}_K^\times : \mathbb{Z}^\times]$. 另一方面可以知道 f 在 $\mathrm{Pic}(\mathcal{O}_K)$ 的像上取值为奇数, 故 $\mathcal{L}(p)$ 为奇数.

对任意平方自由正整数 n, 定义

$$G(n) = \sum_{\substack{n=d_0d_1\cdots d_r \\ d_0\equiv 1 \pmod 8}} \prod_i g(d_i) \pmod 2 \in \mathbb{F}_2.$$

更一般地, 有如下结论:

定理 3.10 [7] 假设 $n \equiv 1,2,3 \pmod 8$ 为一个无平方因子的正整数, 则

$$2^{-\mu(n)}\mathcal{L}(n) \equiv G(n) \pmod 2,$$

这里 $\mu(n)$ 为 n 的素因子个数加 1.

上述定理的证明通过归纳法得到, 该方法首先在文献 [5] 中引入, 后来在文献 [7] 中推广. 之后 Smith 证明了如下定理:

定理 3.11 对任意一个模 8 余 1、2 和 3 的正整数 n,

$$G(n) \equiv 1 \pmod 2 \quad \Leftrightarrow \quad \mathrm{Sel}_2(E^{(n)}/\mathbb{Q})/E^{(n)}(\mathbb{Q})[2] = 0.$$

从而结合前述 Heath-Brown 等的定理 3.4, 可知定理 3.1 成立. 结合 Rubin 的定理 [21] 有如下推论:

推论 3.12 对任意一个模 8 余 1、2 和 3 的正整数 n, 当 $2^{-\mu(n)}\mathcal{L}(n)$ 是奇数或 $\mathrm{Sel}_2(E^{(n)})/E^{(n)}[2] = 0$ 时, $E^{(n)}$ 对应的 BSD 公式成立, 即

$$\frac{L(E^{(n)},1)}{\Omega_{E^{(n)}}} = \frac{\#Ш(E^{(n)}/\mathbb{Q})\cdot \prod c_\ell}{\#E^{(n)}(\mathbb{Q})^2_{\mathrm{tor}}}.$$

4 复乘理论和 Heegner 点

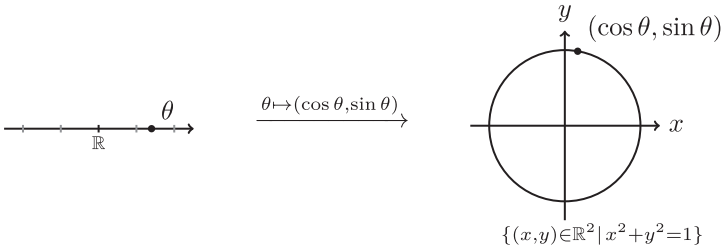
前面考虑了非同余数的分布. 事实上, 同余数的构造等同于椭圆曲线上的有理点构造. 基于复乘理论的 Heegner 点提供了一种系统的机制来构造有理点.

定理 4.1 [25] 任意素数 $p \equiv 5,7 \pmod 8$ 和任意满足 $2p \equiv 6 \pmod 8$ 的素数 p 都是同余数.

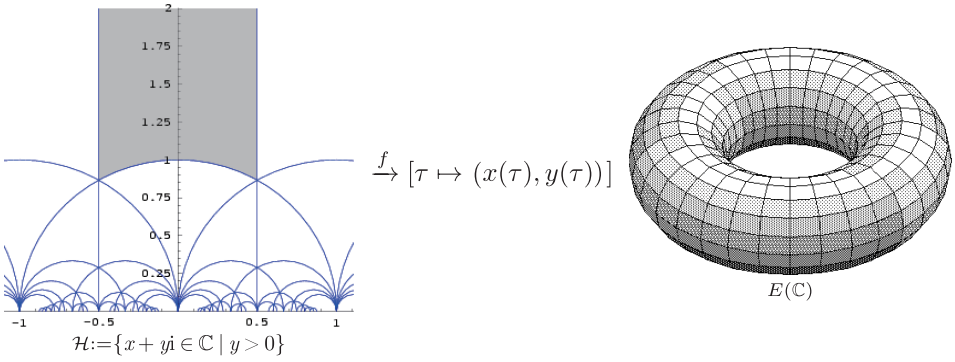
例 4.2 素数 $157 \equiv 5 \pmod 8$ 为同余数, 但是 "最小的" 面积为 157 的有理直角三角形的两直角边为

$$\frac{411340519227716149383203}{21666555693714761309610} \quad 和 \quad \frac{6803298487826435051217540}{411340519227716149383203}.$$

Heegner 是怎样得到这样的突破的? 回顾单位圆周 $x^2+y^2=1$ 可以有实直线参数化:



更进一步, 若 θ 为 π 的有理倍, 则 $\cos\theta$ 和 $\sin\theta$ 都是代数数. 类似地, $E: y^2=x^3-x$ 也有这样的性质 (模性), 即它由上半平面参数化:



为了给出参数化 $f: \mathcal{H} \to E(\mathbb{C})$, 回顾 $\mathcal{H}$ 上的经典的 j- 函数, 定义为

$$j(\tau) = 1728\frac{g_2^3(\tau)}{g_2^3(\tau) - 27g_3^2(\tau)},$$

其中

$$g_2(\tau) = 60\sum_{(m,n)\neq(0,0)} \frac{1}{(m+n\tau)^4}, \quad g_3(\tau) = 140\sum_{(m,n)\neq(0,0)} \frac{1}{(m+n\tau)^6}.$$

事实 4.3 j- 函数具有模性: $j(\frac{a\tau+b}{c\tau+d}) = j(\tau)$ 对任意 $\tau \in \mathcal{H}$ 和任意

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

成立.

特别地, 取

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

则有 $j(\tau+1)=j(\tau)$. 因此, j 有如下的关于 $q=\mathrm{e}^{2\pi\mathrm{i}\tau}$ 的形式 Laurent 展开:

$$j(\tau)=\frac{1}{q}+744+196884q+21493760q^2+864299970q^3+\cdots.$$

事实 4.4 存在函数 $x(\tau),y(\tau)\in\mathbb{Q}(j(\tau),j(32\tau))$ 使得

$$y(\tau)^2=x(\tau)^3-x(\tau),$$

即 $(x(\tau),y(\tau))$ 是曲线 $E:y^2=x^3-x$ 上的点.

由此, 我们获得了 E 的由上半平面 $\mathcal{H}$ 给出的模参数化:

$$f:\mathcal{H}\to E(\mathbb{C}),\quad \tau\mapsto(x(\tau),y(\tau)).$$

事实 4.5 若 $\alpha\in\mathcal{H}$ 为一个二次代数数 (或二次代数整数), 则 $j(\alpha)$ 为代数数 (或代数整数).

例 4.6 j 在 $\tau=(1+\sqrt{-163})/2$ 处的取值为整数 -640320^3, 从而可以得到

$$\mathrm{e}^{\pi\sqrt{163}}=640320^3+743.99999999999925007\cdots$$

与一个整数十分接近.

Heegner 选择了合适的二次代数数 $\tau\in\mathcal{H}$, 从而得到了 E 上的一个定义在 $\mathbb{Q}(\sqrt{-n})$ 的某个交换扩张 H 上的代数点 $f(\tau)$. 对该点的所有 Galois 共轭 $f(\tau)^\sigma$, $\sigma\in\mathrm{Gal}(H/\mathbb{Q}(\sqrt{-n}))$ 求和可以得到 E 的一个定义在 $\mathbb{Q}(\sqrt{-n})$ 上的点, 称为 Heenger 点. 通过如下双射:

$$y^2=x^3-x\leftrightarrow -ny^2=x^3-x,\quad (x,y)\mapsto\left(x,\frac{y}{\sqrt{-n}}\right),$$

它也给出了 $E^{(n)}:ny^2=x^3-x$ 上的一个点. 可以证明当 $n\equiv5,6,7\ (\mathrm{mod}\ 8)$ 为一个奇素数时, 这个点为无限阶点.

定理 4.7 假设 p 为一个模 8 余 7 的素数, 则 $\mathrm{ord}_{s=1}L(E^{(p)},s)=1=\mathrm{rank}_{\mathbb{Z}}E^{(p)}(\mathbb{Q})$, 且其对应的 BSD 公式 2 部分成立.

上述定理的证明主要利用 Gross-Zagier 公式和 Heegner 点的非平凡性. 令 $K=\mathbb{Q}(\sqrt{-p})$, 则由模参数化 $f:X_0(32)\to E$ 和复乘理论可以构造出 $E(H_K)$ 中的一个点 $f(P)$, 其中 $P:=\{\mathbb{C}/\mathcal{O}_K\to\mathbb{C}/\mathcal{N}^{-1}\}$, 这里 $\mathcal{N}$ 为 $\mathcal{O}_K$ 的范数是 32 的整理想. 由 Atkin-Lehner 理论知, 对任意 $t\in\mathrm{Pic}(\mathcal{O}_K)$, 有

$$f(P)^{\sigma_t}+\overline{f(P)^{\sigma_t}}=f([0]),$$

其中 $\bar{\cdot}$ 为复共轭. 考虑

$$y_K:=\mathrm{Tr}_{H_K/K}f(P).$$

故有 $y_K+\overline{y}_K=\#\mathrm{Pic}(\mathcal{O}_K)f([0])$. 特别地, 当 $f([0])\notin2E(\mathbb{Q})$ 且 K 的类数为奇时, 可知 y_K 为无限阶点. Gross-Zagier 公式将 y_K 的高度与 $L'(E_K,1)$ 联系起来, 故由 y_K 的非平凡性可知 $\mathrm{ord}_{s=1}L(E^{(p)},s)=1$. 事实上, 一方面由 2 递降过程可知 $Ш(E^{(p)}/\mathbb{Q})[2]=0$; 另一方面, 解析 Sha 也是奇数, 这由 Heegner 点的上述 2 不可除性和如下 Gross-Zagier 公式得到:

$$\widehat{h}_K(y_K)=4\cdot\frac{L'(E_K,1)}{\Omega(E^{(p)})\Omega(E)}.$$

问题 4.8 当 n 为带有多个素因子的无平方因子整数时, 上述证明过程并不能直接用来判断 Heegner 点的非平凡性. 我们怎样来扩充 Heegner 的结果使得可以用来处理多个素因子情形?

定理 4.9 [7, 26, 27] 令 $n = p_1 \cdots p_k \equiv 5 \pmod 8$ 为一个无平方因子的正整数, 且满足 $p_i \equiv 1 \pmod 4$ 为素数, 且 $\mathbb{Q}(\sqrt{-n})$ 的类群没有 4 阶元, 则对椭圆曲线 $E^{(n)} : ny^2 = x^3 - x$, 有

(1) $\operatorname{ord}_{s=1} L(E^{(n)}, s) = 1 = \operatorname{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q})$;

(2) BSD 猜想对 $E^{(n)}$ 成立:

$$\frac{L'(E^{(n)}, 1)}{R \cdot \Omega} = \frac{\#Ш(E^{(n)}/\mathbb{Q}) \cdot \prod_\ell c_\ell(E^{(n)})}{(\#E^{(n)}(\mathbb{Q})_{\mathrm{tor}})^2}.$$

注 4.10 特别地, 定理 4.9 验证了 Monsky 在文献 [28, 第 23 页, 注 (3)] 中提出的猜想.

例 4.11 $6205 = 5 \times 17 \times 73 \equiv 5 \pmod 8$ 为同余数, 其中

$$(a, b, c) = \left(\frac{116581702045380}{2128879226717}, \frac{2128879226717}{9394174218}, \frac{46625756333848086607779 61}{19999062344860618182306} \right).$$

上述结果的证明的关键是证明 Heegner 点的非平凡性, 这依赖于

- Heegner 的推导方法;
- Gross-Zagier 公式和 Waldspurger 公式;
- 对素因子个数的归纳 [5, 7] (Heegner 的结果为归纳的第 1 步).

对模 8 余 5、6 和 7 的无平方因子整数 n, 上面的方法可给出对应 Heegner 点 2 不可除 (从而非平凡) 的一个充分判断条件 (参见文献 [7]). 类似于 $n \equiv 1, 2, 3 \pmod 8$ 的情形, Smith [8, 9] 证明了满足上述充分条件的 n 使得 Selmer 群达到极小, 按模 8 余 5、6 和 7 只占比例 $\frac{3}{4}$、$\frac{1}{2}$ 和 $\frac{3}{4}$. 特别地, 我们证明了定理 B_1, 从而定理 1.3 成立.

主定理 $\mathbf{B}_1'$ [7, 8] 令 $E^{(n)} : ny^2 = x^3 - x$, 则关于解析 Sha 的分布有

$$\mathrm{Prob}\left(\begin{smallmatrix} \operatorname{ord}_2(\mathcal{L}(E^{(n)}))=0 \\ \operatorname{ord}_{s=1} L(E^{(n)}, s)=1 \end{smallmatrix} \middle| \, n \equiv 5, 6, 7 \pmod 8 \text{ 为无平方因子的正整数} \right) \geqslant \frac{2}{3}\pi_{1,0}.$$

特别地, 弱奇 Goldfeld 猜想成立:

$$\mathrm{Prob}\left(\operatorname*{ord}_{s=1} L(E^{(n)}, s) = 1 \mid n \equiv 5, 6, 7 \pmod 8 \text{ 为无平方因子的正整数} \right) > \frac{1}{2}.$$

5 二次扭族的一般问题

除了同余数椭圆曲线, 二次扭族还有一个重要的例子是与镶嵌数相关的椭圆曲线.

一个平方自由的正整数 n 称为镶嵌数 (tiling number), 若存在正整数 k 使得等边三角形可以被分割成 nk^2 个全等三角形. 可以证明不等于 1、2、3 和 6 的无平方因子的整数 n 为镶嵌数当且仅当

$$E : y^2 = x(x-1)(x+3)$$

的两个二次扭 $E^{(\pm n)}$ 中有一个的秩为正.

定理 5.1 [3] 令 $n = p_1 \cdots p_k \equiv 7 \pmod{24}$ 为一个无平方因子的正整数, 其中 $p_i \equiv 1 \pmod 3$ 为素数, 且满足 $\mathbb{Q}(\sqrt{-n})$ 的类群没有 4 阶元, 则对椭圆曲线 $E^{(\pm n)} : \pm ny^2 = x(x-1)(x+3)$, 有

(1) $\operatorname{ord}_{s=1} L(E^{(\pm n)}, s) = 0 = \operatorname{rank}_{\mathbb{Z}} E^{(\pm n)}(\mathbb{Q})$, 特别地, n 不是一个镶嵌数;

(2) 若 $p = 2$ 或 p 为普通好约化, 则 $E^{(\pm n)}$ 的 BSD 猜想的 p 部分成立.

3) Feng K Q, Liu Q Y, Pan J Z, et al. The tiling number problem. Preprint

定理 5.2 [4] 令 $n=p_1\cdots p_k\equiv -1 \pmod{24}$ 为一个无平方因子的正整数, 其中 $p_i\equiv \pm 1 \pmod{24}$ 为素数且满足 $\mathbb{Q}(\sqrt{-n})$ 的类群没有 4 阶元, 则对椭圆曲线 $E^{(\pm n)}: \pm ny^2=x(x-1)(x+3)$, 有

(1) $\mathrm{ord}_{s=1} L(E^{(\pm n)},s)=1=\mathrm{rank}_{\mathbb{Z}} E^{(\pm n)}(\mathbb{Q})$, 特别地, n 是一个镶嵌数;

(2) 若 $p=2$ 或 p 为普通好约化, 则 $E^{(\pm n)}$ 的 BSD 猜想的 p 部分成立.

我们已经讨论了两条椭圆曲线的二次扭族:

• 同余数椭圆曲线 (congruent number elliptic curve, CNEC): $ny^2=x(x-1)(x+1)$, 带有 CM 但不存在有理 $\mathbb{Z}/4\mathbb{Z}$ 同源;

• 镶嵌数椭圆曲线 (tiling number elliptic curve, TNEC): $ny^2=x(x-1)(x+3)$ 不带 CM 但存在有理 $\mathbb{Z}/4\mathbb{Z}$ 同源.

这两族椭圆曲线对本文所涉及的所有问题来说是典型的. 给定一条椭圆曲线的二次扭族 $\mathcal{E}$, 我们有如下期待:

• 在有限步之内决定给定椭圆曲线 $E\in\mathcal{E}$ 是否有无穷阶点, 即 $\mathrm{rank}\, E(\mathbb{Q})>0$? (Tunnell 类型的结果对一般二次扭族都成立, 从而假设 BSD 猜想成立, 应该存在一个算法.)

• 当 E 遍历 $\mathcal{E}$ 时, 理解关于如下不变量:

$$\mathrm{Sel}_p(E/\mathbb{Q}),\quad \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}),\quad \mathrm{ord}_{s=1} L(E,s),\quad \mathcal{L}(E)$$

的分布问题. 特别地, $p=2$.

为了推广上述关于 CNEC 的结果, 需要新的想法, 特别是对 TNEC.

参考文献

1 Alter R, Curtz T B, Kubota K K. Remarks and results on congruent numbers. In: Proceedings of the Third Southeastern Conference on Combinatorics, Graph Theory and Computing. Boca Raton: Florida Atlantic University, 1972, 27–35

2 Tunnell J B. A classical Diophantine problem and modular forms of weight 3/2. Invent Math, 1983, 72: 323–334

3 Coates J, Wiles A. On the conjecture of Birch and Swinnerton-Dyer. Invent Math, 1977, 39: 223–251

4 Goldfeld D. Conjectures on elliptic curves over quadratic fields. In: Number Theory, Carbondale 1979 (Proceedings of the Southern Illinois Number Theory Conference Carbondale, March 30 and 31, 1979). Lecture Notes in Mathematics, vol. 751. Berlin: Springer, 1979, 108–118

5 Tian Y. Congruent numbers and Heegner points. Cambridge J Math, 2014, 2: 117–161

6 Tian Y. Congruent numbers with many prime factors. Proc Natl Acad Sci USA, 2012, 109: 21256–21258

7 Tian Y, Yuan X, Zhang S. Genus periods, genus points and congruent number problem. Asian J Math, 2017, 21: 721–774

8 Smith A. The congruent numbers have positive natural density. arXiv:1603.08479, 2016

9 Smith A. 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. arXiv:1702.02325, 2017

10 Burungale A, Tian Y. p-converse to a theorem of Gross-Zagier, Kolyvagin and Rubin. Invent Math, 2020, 220: 211–253

11 Mordell L J. On the rational solutions of the indeterminate equations of the third and fourth degrees. Proc Cambridge Philos Soc, 1922, 21: 179–192

12 Silverman H. The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, vol. 106. New York: Springer-Verlag, 2011

13 Wiles A. Modular elliptic curves and Fermat's last theorem. Ann of Math (2), 1995, 141: 443–551

14 Taylor R, Wiles A. Ring-theoretic properties of certain Hecke algebras. Ann of Math (2), 1995, 141: 553–572

15 Breuil C, Conrad B, Diamond F, et al. On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises. J Amer Math Soc, 2001, 14: 843–939

16 Manin J I. Cyclotomic fields and modular curves. Russian Math Surveys, 1971, 26: 7–78

4) He W, Hu Y R, Tian Y. Tiling number problem and Heegner points. Under preparation

17 Bhargava M, Kane D, Lenstra H, et al. Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves. Cambridge J Math, 2015, 3: 275–321
18 Kane D. On the ranks of the 2-Selmer groups of twists of a given elliptic curve. Algebra Number Theory, 2013, 7: 1253–1279
19 Heath-Brown D R. The size of Selmer groups for the congruent number problem, II. Invent Math, 1994, 118: 331–370
20 Swinnerton-Dyer P. The effect of twisting on the 2-Selmer group. Math Proc Cambridge Philos Soc, 2008, 145: 513–526
21 Rubin K. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. Invent Math, 1991, 103: 25–68
22 Bloch S, Kato K. L-functions and Tamagawa numbers of motives. In: The Grothendieck Festschrift, vol. I. Progress in Mathematics, vol. 86. Boston: Birkhäuser, 333–400
23 Tunnell J B. A classical Diophantine problem and modular forms of weight 3/2. Invent Math, 1983, 72: 323–334
24 Cai L, Shu J, Tian Y. Explicit Gross-Zagier and Waldspurger formulae. Algebra Number Theory, 2014, 8: 2523–2572
25 Heegner K. Diophantische analysis und modulfunktionen. Math Z, 1952, 56: 227–253
26 田野. 同余数问题与椭圆曲线. 中国科学: 数学, 2019, 49: 1313–1336
27 Li Y, Liu Y, Tian Y. On the Birch and Swinnerton-Dyer conjecture for CM elliptic curves over $\mathbb{Q}$. arXiv:1605.01481, 2016
28 Monsky P. Mock Heegner points and congruent numbers. Math Z, 1990, 204: 45–67

Congruent number problem and Goldfeld conjecture

Ye Tian

Abstract We introduce recent progress on the congruent number problem, in particular, on Goldfeld conjecture for congruent elliptic curves.

Keywords **congruent number, L function, Goldfeld conjecture, distribution of Selmer groups**

MSC(2010) **11G05, 11G40**

doi: 10.1360/SSM-2020-0244