中国科学: 数学 2024 年 第 54 卷 第 8 期: 1157 ~ 1168
SCIENTIA SINICA Mathematica
数学问题专栏

与同余数相关的若干问题与猜想

秦厚荣

南京大学数学学院, 南京 210093
E-mail: hrqin@nju.edu.cn

收稿日期: 2024-03-29; 接受日期: 2024-05-20; 网络出版日期: 2024-07-24
国家自然科学基金 (批准号: 11971224 和 12231009) 资助项目

摘要 基于作者在同余数问题方面的研究结果, 本文提出一系列问题与猜想. 部分猜想给出了数值验证.

关键词 同余数问题 椭圆曲线 K_2 群 Shafarevich-Tate 群 问题与猜想

MSC (2020) 主题分类 11G05, 11G40, 11E20

1 引言

三条边长都是有理数的直角三角形的面积称为同余数. 同余数问题即判断一个给定的正整数是否是同余数. 著名的直角三角形莫过于勾三股四弦五, 这表明 6 是同余数. 假设直角三角形三条边长分别是有理数 a、b 和 c, 并且假设 c 是斜边长, 则这个直角三角形的面积是 $\frac{1}{2}ab$. 记 $\frac{1}{2}ab=\frac{s}{t}$, 其中 s 和 t 是正整数. 将原来的直角三角形的三条边长都延长 t 倍, 得到一个相似的直角三角形, 其面积是 st, 这说明研究同余数时只需要考虑正整数就可以, 而且以上讨论还说明, 只需要考虑没有平方因子的正整数.

同余数问题非常自然. 所以, 不少人相信古希腊时期这个问题已经有人考虑过. 法国国家图书馆存有一千年前阿拉伯世界关于同余数问题研究的一些原始档案. 那时候的学者们发现了最大是 10,374 的 34 个同余数的例子. 一般认为 5 是同余数是 Fibonacci 证明的. Fermat 证明了 1 (等价地, 一个平方数) 不是同余数, 为此创造了在现代数学中仍然十分有效的无穷递降法. 著名的 Fermat 大定理也可能是受到这个研究结果的启发提出来的. Dickson [7] 收集了较为丰富的同余数研究的历史资料.

同余数问题与椭圆曲线上有理点的存在性有着深刻的联系, 这个同样应该归功于 Fermat. 正是这个联系帮助人们看到了同余数问题的本质, 进而同余数的研究进入了现代数学的范畴.

要证明一个正整数 n 是同余数, 就是要求有理数 $a,b,c\in\mathbb{Q}$ 满足

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

英文引用格式: Qin H R. Conjectures and problems on congruent numbers (in Chinese). Sci Sin Math, 2024, 54: 1157–1168, doi: 10.1360/SSM-2024-0091

如果令

$$(x,y)=\left(\frac{1}{2}a(a-c),\frac{1}{2}a^2(c-a)\right),$$

则有

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

即 (x,y) 是椭圆曲线 $Y^2=X^3-n^2X$ 上的有理点. 这里 $y\neq 0$ 意味着这是 $Y^2=X^3-n^2X$ 上的一个无穷阶的点.

另外, 如果 $(x,y)\in\mathbb{Q}^2$ 是椭圆曲线 $Y^2=X^3-n^2X$ 上的有理点, 当 $y\neq 0$ 时, 公式

$$\left(\frac{x^2-n^2}{y}\right)^2+\left(\frac{2xn}{y}\right)^2=\left(\frac{x^2+n^2}{y}\right)^2,\quad \frac{1}{2}\left(\frac{x^2-n^2}{y}\right)\left(\frac{2xn}{y}\right)=n$$

说明 n 是同余数. 这样就有如下命题.

命题 1.1 假设 n 是没有平方因子的正整数, 则 n 是同余数的充分必要条件是椭圆曲线 E_n : $Y^2=X^3-n^2X$ 有 $y\neq 0$ 的有理点 (x,y).

著名的 BSD 猜想 (Birch and Swinnerton-Dyer conjecture)[2] 是千禧年七大数学问题之一, 这个猜想推测椭圆曲线有理点与其 L- 函数值有着深刻的联系.

假设 $E/\mathbb{Q}$ 是椭圆曲线, 而 p 为素数. 记

$$a_p=p+1-\#E(\mathbb{F}_p),$$

定义局部 L- 函数

$$L_p(T)=\begin{cases}1-a_pT+pT^2, & \text{当 } E \text{ 在 } p \text{ 处有好的约化时,}\\ 1-T, & \text{当 } E \text{ 在 } p \text{ 处有分裂的乘性约化时,}\\ 1+T, & \text{当 } E \text{ 在 } p \text{ 处有非分裂的乘性约化时,}\\ 1, & \text{当 } E \text{ 在 } p \text{ 处有加性约化时.}\end{cases}$$

定义 1.1 椭圆曲线 $E/\mathbb{Q}$ 的 L- 函数定义为

$$L(E,s)=\prod_p\frac{1}{L_p(p^{-s})},$$

其中 p 取遍所有素数.

BSD 猜想 假设 $E/\mathbb{Q}$ 是椭圆曲线, $E(\mathbb{Q})$ 表示它所有有理点构成的群 (Mordell-Weil 群),

$$r=\operatorname{rank}E(\mathbb{Q})$$

是该群的算术秩.

(1) 解析秩等于算术秩: $L(E,s)$ 在 $s=1$ 处零点的重数等于 r, 即 $L(E,s)$ 在 $s=1$ 处的 Taylor 展开为

$$L(E,s)=C_0(s-1)^r+C_1(s-1)^{r+1}+C_2(s-1)^{r+2}+\cdots,$$

其中 $C_0\neq 0$.

(2) 有等式关系

$$C_0=\frac{\Omega_E\cdot|Ш_E|\cdot\mathrm{Reg}(E)\cdot\prod c_p}{|E_{\mathrm{tors}}(\mathbb{Q})|^2},$$

这里 Ω_E 是极小 Néron 微分形式在 $E(\mathbb{R})$ 上的积分, $Ш_E$ 表示 $E/\mathbb{Q}$ 的沙群 (Shafarevich-Tate group), $\mathrm{Reg}(E)$ 为 $E/\mathbb{Q}$ 的正则子 (regulator), $E_{\mathrm{tors}}(\mathbb{Q})$ 是 $E(\mathbb{Q})$ 的挠部分, Tamagawa 数 $c_p=[E(\mathbb{Q}_p):E_0(\mathbb{Q}_p)]$, 其中 $E_0(\mathbb{Q}_p)$ 表示 $E(\mathbb{Q}_p)$ 模 p 后所有非奇异的点, $|G|$ 表示群 G 的阶.

下面的定理将椭圆曲线 $Y^2=X^3-n^2X$ 上的无穷阶有理点的存在性归结为 L- 函数在 1 点值的计算.

定理 1.1 [6] 假设 E 是定义在 $\mathbb{Q}$ 上的有复乘的椭圆曲线, 如果 $E(\mathbb{Q})$ 有无穷阶的有理点, 则 $L(E,1)=0$.

对于 $\mathbb{Q}$ 上没有复乘的椭圆曲线, Kolyvagin [12] 和 Kato [10] 也建立了上述定理.

有如下一个自然的推论: 如果 n 是同余数, 则 $L(E_n,1)=0$. 反过来, 如果假设 BSD 猜想成立, 则由 $L(E_n,1)=0$ 也可以推导出 n 是同余数.

关于 BSD 猜想, 目前人们已经证明了如下结论:

(1) $L(E,1)\neq 0$, 那么 $\mathrm{rank}E(\mathbb{Q})=0$;

(2) $L(E,1)=0$, 但是 $L'(E,1)\neq 0$, 则 $\mathrm{rank}E(\mathbb{Q})=1$.

关于同余数问题, 文献 [19] 证明了下面的定理:

定理 1.2 假设 n 是无平方因子的正奇数 (或者, 偶数). 如果 n 是同余数, 则

$$\#\{(x,y,z)\in\mathbb{Z}^3\mid n=x^2+2y^2+32z^2\}=\#\{(x,y,z)\in\mathbb{Z}^3\mid n=2x^2+4y^2+9z^2-4yz\}$$

(或者, $\#\{(x,y,z)\in\mathbb{Z}^3\mid \frac{n}{2}=x^2+4y^2+32z^2\}=\#\{(x,y,z)\in\mathbb{Z}^3\mid \frac{n}{2}=4x^2+4y^2+9z^2-4yz\}$).

反之, 假设 BSD 猜想对椭圆曲线 $Y^2=X^3-n^2X$ 成立, 则上述等式意味着 n 是同余数.

定理 1.3 (Tunnell 定理 [26]) 假设 n 是无平方因子的正奇数 (或者, 偶数). 如果 n 是同余数, 则

$$\#\{(x,y,z)\in\mathbb{Z}^3\mid n=x^2+2y^2+32z^2\}=\frac{1}{2}\#\{(x,y,z)\in\mathbb{Z}^3\mid n=x^2+2y^2+8z^2\}$$

(或者, $\#\{(x,y,z)\in\mathbb{Z}^3\mid \frac{n}{2}=x^2+4y^2+32z^2\}=\frac{1}{2}\#\{(x,y,z)\in\mathbb{Z}^3\mid \frac{n}{2}=x^2+4y^2+8z^2\}$).

反之, 假设 BSD 猜想对椭圆曲线 $Y^2=X^3-n^2X$ 成立, 则上述等式可以反推导出 n 是同余数.

比较定理 1.2 与 1.3. 虽然数值上对无平方因子的正奇数 n 有 (仅以定理 1.2 和 1.3 中第一个等式为例)

$$\begin{aligned}&\#\{(x,y,z)\in\mathbb{Z}^3\mid n=x^2+2y^2+32z^2\}-\#\{(x,y,z)\in\mathbb{Z}^3\mid n=2x^2+4y^2+9z^2-4yz\}\\&=2\bigg(\#\{(x,y,z)\in\mathbb{Z}^3\mid n=x^2+2y^2+32z^2\}-\frac{1}{2}\#\{(x,y,z)\in\mathbb{Z}^3\mid n=x^2+2y^2+8z^2\}\bigg),\end{aligned}$$

但是, 上面的等式对一般的 n 并不成立. 以前者为系数构造的模形式既是尖形式也是特征形式, 而后者为系数构造的模形式既不是尖形式也不是特征形式. 从这个意义上看, Tunnell 定理给出的是数值上的等式, 而定理 1.2 给出的是数论意义丰富的等式.

定理 1.2 的证明首次给出了来自二次型的、权为 3/2 的尖形式到权为 2 的尖形式的 Shimura 提升的方法. 关键点是发现了三元二次型表奇素数的平方与相关的四元二次型表这个奇素数之间存在着深刻的联系:

$$\begin{aligned}&\#\{(x,y,z)\in\mathbb{Z}^3\mid p^2=2x^2+4y^2+9z^2-4yz\}\\&=\#\{(x,y,z,w)\in\mathbb{Z}^4\mid p=2x^2+3y^2+3z^2+4w^2+2yz\},\end{aligned}$$

具体证明参见文献 [19].

假设 BSD 猜想成立, 则模 8 余 5, 6, 7 的无平方因子的正整数都是同余数. Tian[23,24] 在这方面有杰出的成果.

根据 Goldfeld 猜想, 模 8 余 1, 2, 3 的每一类中几乎所有的无平方因子的正整数都是非同余数, 由 Smith[22]、Burungale 和 Tian[4,5] 的工作知道这一结论成立. 但是, 需要特别指出, 模 8 余 1, 2, 3 的每一类中都有无穷多个同余数. 用 K_2R 表示环 R 的 Milnor 群, $r_{2^i}(G)$ 表示有限交换群 G 的 2^i- 秩. 基于定理 1.2, 在模 8 余 1, 2, 3 的情形, 文献 [19] 分别给出了如下结果:

定理 1.4 (1) 设 $p\equiv 1 \pmod 8$ 为奇素数, 记 $F=\mathbb{Q}(\sqrt{p})$, O_F 为其整元环. 如果 p 是同余数, 则 $r_8(K_2O_F)=1$. 所以, 如果 $r_8(K_2O_F)=0$, 则 p 是非同余数.

(2) 如果 $p\equiv 1 \pmod{16}$ 且 $h(-p)\not\equiv h(-2p) \pmod{16}$, 则 $2p$ 是非同余数.

(3) 如果 $p\equiv 1 \pmod 8$, $q\equiv 3 \pmod 8$ 且 $h(-pq)\not\equiv h(-p) \pmod 8$, 则 pq 是非同余数.

如何在模 8 余 1, 2, 3 这 3 种情形刻画同余数呢? 下文提出了一系列猜想, 推测在上述 3 种情形下同余数的状况.

本文中讨论的猜想有的是第一次提出, 有的在本文作者的其他论文中已经呈现. 其中部分猜想可以看作 Cohen-Lenstra 探索 (heuristic) 法的类比.

2 猜想与问题

本节介绍作者在同余数问题研究中产生的一系列猜想与问题. 为了叙述这些猜想与问题, 需要回顾相关知识与研究结果 (参见文献 [4,5,7,8,11,13–25,27]). 一些经典结果, 将不给出处地直接引用.

设 K 是数域, M_K 是 K 上全体不等价赋值构成的集合. 设 E 和 E' 是定义在 K 上的椭圆曲线, 而 $\phi: E/K\to E'/K$ 是一个同源映射.

定义 2.1 E/K 的 ϕ-Selmer 群是由下式定义的 $H^1(G_{\bar{K}/K}, E[\phi])$ 的子群:

$$S^{(\phi)}(E/K)=\ker\left\{H^1(G_K,E[\phi])\to\prod_{v\in M_K}H^1(G_{K_v},E)\right\},$$

其中 $E[\phi]$ 表示 ϕ 的核.

定义 2.2 沙群 $Ш_{E/K}$ (或者 $Ш_E$) 的定义如下:

$$Ш_{E/K}=\ker\left\{H^1(G_K,E)\to\prod_{v\in M_K}H^1(G_{K_v},E)\right\}.$$

定理 2.1 假设 $\phi: E/K\to E'/K$ 是定义在 K 上的同源, 则

(1) 有正合列

$$0\to E'(K)/\phi(E(K))\to S^{(\phi)}(E/K)\to Ш_{E/K}[\phi]\to 0;$$

(2) Selmer 群 $S^{(\phi)}(E/K)$ 有限.

注 2.1 如果取 $E=E'=E_n$, $\phi=[2]$, 则

$$0\to E(\mathbb{Q})/2E(\mathbb{Q})\to S^{(2)}(E/\mathbb{Q})\to Ш_{E/\mathbb{Q}}[2]\to 0$$

是正合的.

记 $s(n)$ 为满足

$$|S^{(2)}(E/\mathbb{Q})| = 2^{2+s(n)}$$

的整数, 其中 $S^{(2)}(E/\mathbb{Q})$ 为同余椭圆曲线 E 的 2-Selmer 群. 非负整数 $s(n)$ 称之为同余椭圆曲线 E 的 2-Selmer 秩. 用 $r(n)$ 表示 $E_n(\mathbb{Q})$ 的算术秩. 则有明显的不等式

$$0 \leqslant r(n) \leqslant s(n).$$

因此, 对于无平方因子的正整数 n, 如果 $s(n) = 0$, 则 n 是非同余数.

定义 2.3 假设 $n \in \mathbb{N}$ 无平方因子, n' 是 n 的奇数部分, 且 $n' = p_1 \cdots p_m$ 是其素因子分解. 设 $A = A(n) = (a_{ij})$ 为 $m \times m$ 阶矩阵, 系数满足

$$a_{ij} = \left[\frac{p_j}{p_i}\right], \quad \text{当 } i \neq j \text{ 时},$$

而 $a_{ii} = [\frac{n'/p_i}{p_i}]$, 其中 $[\dot{:}]$ 是取值在 $\mathbb{F}_2$ 上的 Legendre 符号. 再设 $D_u = \mathrm{diag}([\frac{u}{p_i}])$, 其中 $u \in \{-1, \pm 2\}$. Monsky 矩阵 M_o 和 M_e 分别定义为

$$M_o := \begin{pmatrix} A + D_2 & D_2 \\ D_2 & A + D_{-2} \end{pmatrix},$$

$$M_e := \begin{pmatrix} D_2 & A + D_2 \\ A^{\mathrm{T}} + D_2 & D_{-1} \end{pmatrix}.$$

上面所有矩阵都定义在 $\mathbb{F}_2$ 上.

Monsky (参见文献 [8, 附录]) 证明了以下 $s(n)$ 的公式:

$$s(n) = \begin{cases} 2m - \mathrm{rank}_{\mathbb{F}_2}(M_o), & \text{若 } (2, n) = 1, \\ 2m - \mathrm{rank}_{\mathbb{F}_2}(M_e), & \text{若 } (2, n) = 2, \end{cases} \tag{2.1}$$

$$s(n) = \begin{cases} \text{偶数}, & \text{如果 } n \equiv 1, 2, 3 \pmod 8, \\ \text{奇数}. & \text{如果 } n \equiv 5, 6, 7 \pmod 8. \end{cases} \tag{2.2}$$

对于同余椭圆曲线, 假设 BSD 猜想成立, 则有

(1) $L(E_n, 1) \neq 0$ 当且仅当 $E_n(\mathbb{Q})$ 是有限的, 当且仅当 n 是非同余数;

(2) 当 $E_n(\mathbb{Q})$ 有限时, 有如下等式:

$$L(E_n, 1) = \frac{\Omega_{E_n} \cdot |Ш_{E_n}| \cdot \prod c_p}{|E_n(\mathbb{Q})|^2}.$$

下面按照模 8 余 1, 2, 3 的情形来讨论.

(I) 模 8 余 1 的情形

考虑两个二次型 $f(x, y, z) = x^2 + 2y^2 + 32z^2$ 和 $g(x, y, z) = 2x^2 + 4y^2 + 9z^2 - 4yz$. 一个重要的事实是, 它们在同一个种 (genus) 里, 并且是这个类数为 2 的种里的 2 个代表元. 记

$$r_f(n) = \#\{(x, y, z) \mid x, y, z \in \mathbb{Z}, n = f(x, y, z)\},$$
$$r_g(n) = \#\{(x, y, z) \mid x, y, z \in \mathbb{Z}, n = g(x, y, z)\}.$$

作为定理 1.2 的推论, 有如下结果:

推论 2.1 假设 n 为无平方因子的奇数, 如果 $r_f(n) \neq r_g(n)$, 则解析沙群的阶由如下公式给出:

$$|Ш_{E_n}| = \left(\frac{r_f(n) - r_g(n)}{2\sigma_0(n)}\right)^2,$$

这里 $\sigma_0(n)$ 表示 n 的正因子的个数. 假设 BSD 猜想成立, 则上式右边的值给出沙群的阶.

为了减少过多记号的引入, 本文用同样的记号 Ш 来表示解析沙群与算术沙群. 当然, 假设 BSD 猜想成立, 这两个群是一样的.

猜想 2.1 在所有 $p \equiv 1 \pmod 8$ 的素数构成的集合中, 满足 $r_4(K_2O_F) = 1$ 的素数构成的子集合具有密度 $\frac{1}{2}$, 满足 $r_8(K_2O_F) = 1$ 的素数构成的子集合具有密度 $\frac{1}{4}$. 一般地, 当 $n \geqslant 1$ 时, 满足 $r_{2^{n+1}}(K_2O_F) = 1$ 的素数构成的子集合具有密度 $\frac{1}{2^n}$, 这里 O_F 是 $F = \mathbb{Q}(\sqrt{p})$ 的整元环.

表 1 的数据分别显示了前 1,000 个和前 10,000 个模 8 余 1 的素数 $r_{2^n} = r_{2^n}(K_2O_F)$ 的分布情形.

当 $n = 1$ 时, 上述猜想成立. 事实上, 根据文献 [1,17] 中结果, 当 $p \equiv 1 \pmod 8$ 时, $r_4(K_2O_F) = 1$ 等价于 $p = x^2 + 32y^2$, 这样由 Chebotarev 密度定理就可以推导出在 $p \equiv 1 \pmod 8$ 的素数构成的集合中满足 $r_4(K_2O_F) = 1$ 的素数构成的子集合具有密度 $\frac{1}{2}$. 换而言之, 在 $p \equiv 1 \pmod 8$ 的素数构成的集合中非同余数的密度大于等于 $\frac{1}{2}$. 如果上述猜想对 $n = 2$ 时成立的, 利用定理 1.4, 我们推导出非同余数的密度大于等于 $\frac{3}{4}$.

引入记号

$$P = \{p, 素数 \mid p \equiv 1 \pmod 8\},$$
$$P(4^n) = \{p \in P \mid 4^n \parallel \#Ш_{E_p}\}.$$

猜想 2.2 对于任意算术级数 A, 如果 $A \cap P$ 是无限集合, 则 $A \cap P$ 中同余数是具有 0 密度的无限子集.

特别地, P 中同余数是具有 0 密度的无限子集. 这是大家早就相信但是难以证明的结论.

下面从沙群的角度来引入一个猜想. 当 $n = 0$ 时,

$$P(1) = P(4^0) = \{p \in P \mid \#Ш_{E_p} 为奇数\}.$$

我们知道, $p \in P(1)$ 当且仅当 p 是同余数.

猜想 2.3 (1) 集合 $P(1)$ 有无限多个元素并且有渐近公式

$$\#\{p \in P(1) \mid p \leqslant x\} \sim cx^{\frac{3}{4}}(\log x)^{-\frac{5}{8}},$$

这里 $0.2 < c < 0.21$ 是一个常数. 特别地, $P(1)$ 在 P 中是具有 0 密度的无限子集.

(2) 对于任意整数 $n \geqslant 1$, $P(4^n)$ 在 P 中的密度为 $\frac{1}{2^n}$.

本文作者推测如下问题的答案是肯定的.

问题 2.1 (1) 集合 $P(1)$ 有无限多个元素, 其对应的椭圆曲线的沙群是平凡的吗?

(2) 进一步地, 集合 $P(1)$ 中对应的椭圆曲线的沙群非平凡的子集在 $P(1)$ 中是 0 密度吗? 如果不是 0 密度, 这个密度是多少?

表 1 猜想 2.1 的数值结果

	$r_{2^2}=1$	$r_{2^3}=1$	$r_{2^4}=1$	$r_{2^5}=1$	$r_{2^6}=1$	$r_{2^7}=1$	$r_{2^8}=1$	$r_{2^9}=1$	$r_{2^{10}}=1$	$r_{2^{11}}=1$	$r_{2^{12}}=1$	$r_{2^{13}}=1$	$r_{2^{14}}=1$	$r_{2^{15}}=1$
1,000	494	252	127	57	29	16	12	8	3	0	1	1	0	0
10,000	4,960	2,464	1,217	611	315	165	81	44	25	16	5	2	1	1

表 2 是猜想 2.3(2) 的一些数值结果: 第 2 和 3 行分别是前 1,000 个和前 10,000 个模 8 余 1 的素数满足 $4^m \parallel \#Ш$ 的分布数据, 为了方便起见, 这里将 $Ш_{E_p}$ 简记为 Ш.

前面用 r_{2^n} 表示 $r_{2^n}(K_2O_F)$. 对于一个正整数 n, 记 δ_{2^n} 为满足 $r_{2^n}=1$ 和 $r_{2^{n+1}}=0$ 的素数个数. 下面的表 3 和 1 实际是同一组数据, 是表 1 的另外一种统计方法.

表 2 和 3 分别是关于沙群和 K_2 群的. 可是, 让人意外的是第 2 和 3 列的数值结果完全一致, 这意味着 Birch-Tate 猜想和 BSD 猜想存在着紧密联系.

Birch-Tate 猜想 设 F 是全实数域, ζ_F 为该域的 Dedekind ζ 函数, $w_2(F)$ 表示 $F(\sqrt{F})$ 中单位根的个数. 那么

$$\#K_2O_F = w_2(F)\cdot|\zeta_F(-1)|.$$

注 2.2 Mazur-Wiles 和 Wiles 在 Iwasawa 主猜想方面的工作可以推导出 Birch-Tate 猜想的奇部分成立. 文献 [3] 表明, 对 Abel 数域, 这个猜想的偶部分也成立.

现在来解释前面的现象. 实际上, 根据文献 [19] 的结果, 有如下定理:

定理 2.2 设 $p\equiv 1\,(\mathrm{mod}\ 8)$ 为素数, $F=\mathbb{Q}(\sqrt{p})$, E_p 为方程 $Y^2=X^3-p^2X$ 定义的椭圆曲线. 则

(1) $8\parallel\#(K_2O_F)$ 当且仅当

$$4\parallel\#Ш(E_p),$$

这里 $Ш(E_p)$ 表示解析沙群, 下同;

(2) $16\parallel\#(K_2O_F)$ 当且仅当

$$16\parallel\#Ш(E_p);$$

(3) $32\mid\#(K_2O_F)$ 当且仅当

$$64\mid\#Ш(E_p),$$

或者 E_p 的 Mordell-Weil 群的算术秩等于 2.

问题 2.2 对算术沙群证明上述定理中的 (1)–(3).

定理 2.3 设 $p\equiv 1\,(\mathrm{mod}\ 8)$ 为素数, $F=\mathbb{Q}(\sqrt{p})$, E_p 为方程 $Y^2=X^3-p^2X$ 定义的椭圆曲线. 则

(1) 8 正好整除 $w_2(F)\cdot\zeta_F(-1)$ 当且仅当 4 正好整除

$$\frac{L(E,1)(\#E(\mathbb{Q})_{\mathrm{tor}})^2}{\Omega_E R_E\prod_{p|N}c_p};$$

表 2 猜想 2.3(2) 的数值结果

$p\equiv 1(8)$	$4\,\|\|\,\#Ш$	$4^2\,\|\|\,\#Ш$	$4^3\,\|\|\,\#Ш$	$4^4\,\|\|\,\#Ш$	$4^5\,\|\|\,\#Ш$	$4^6\,\|\|\,\#Ш$	$r_f=r_g$
1,000	506	242	114	20	0	0	118
10,000	5,040	2,496	1,186	461	66	1	750

表 3 表 1 的另一种统计方法

	δ_2	δ_{2^2}	δ_{2^3}	δ_{2^4}	δ_{2^5}	δ_{2^6}	δ_{2^7}	δ_{2^8}	δ_{2^9}	$\delta_{2^{10}}$	$\delta_{2^{11}}$	$\delta_{2^{12}}$	$\delta_{2^{13}}$	$\delta_{2^{14}}$	$\delta_{2^{15}}$
1,000	506	242	125	70	28	13	4	4	5	0	2	0	1	0	0
10,000	5,040	2,496	1,247	606	296	150	84	37	19	9	11	3	1	0	1

(2) 16 正好整除 $w_2(F)\cdot\zeta_F(-1)$ 当且仅当 16 正好整除

$$\frac{L(E,1)(\#E(\mathbb{Q})_{\rm tor})^2}{\Omega_E R_E\prod_{p|N}c_p};$$

(3) 32 整除 $w_2(F)\cdot\zeta_F(-1)$ 当且仅当 64 整除

$$\frac{L(E,1)(\#E(\mathbb{Q})_{\rm tor})^2}{\Omega_E R_E\prod_{p|N}c_p},$$

或者 E_p 的 Mordell-Weil 群的算术秩等于 2.

下面考虑 Mordell-Weil 群的算术秩.

猜想 2.4 用 $P(t,s)$ 表示满足下面条件的全体无平方因子的正整数 n 构成的集合:

(1) n 恰有 t 个不同的奇素因子;

(2) $n\equiv 1\pmod 8$;

(3) $s(n)=s$.

而 $P(t,s,r)$ 表示 $P(t,s)$ 中满足 $r(n)=r$ 的所有 n 构成的子集.

那么 $P(t,s,0)$ 在 $P(t,s)$ 中的密度是 1, 并且对于任意偶数 $0\leqslant r\leqslant s(n)$, 都有

$$\#P(t,s,r)=\infty.$$

例 2.1 考虑形如 $n=pq$ 且满足 $p\equiv q\equiv 1\pmod 8$ 和 $(\frac{p}{q})=1$ 的正整数, $n=pq$, $p\equiv q\equiv 1\pmod 8$, $(\frac{p}{q})=1$, 此时, $M_o=0$, 所以 $s(n)=4$.

(1) $n=17\cdot 257: r=0$;

(2) $n=17\cdot 89: r=2$;

(3) $n=409\cdot 809: r=4$.

(II) 模 8 余 2 的情形

与前面类似, 二次型 $s=s(x,y,z)=x^2+4y^2+32z^2$ 和 $t=t(x,y,z)=4x^2+4y^2+9z^2-4yz$ 是类数为 2 的同一个种里的 2 个代表元. 记

$$r_s(n)=\#\{(x,y,z)\in\mathbb{Z}^3\mid n=s(x,y,z)\},$$
$$r_t(n)=\#\{(x,y,z)\in\mathbb{Z}^3\mid n=t(x,y,z)\}.$$

下面的结果也是定理 1.2 的推论.

推论 2.2 假设 $n\equiv 2\pmod 8$ 为无平方因子的正整数, 如果 $r_s(n/2)\neq r_t(n/2)$, 则解析沙群的阶由

$$|Ш_{E_n}|=\left(\frac{r_s(n/2)-r_t(n/2)}{2\sigma_0(n/2)}\right)^2$$

给出. 假设 BSD 猜想成立, 上述公式也给出了沙群的阶.

如果 $n=2p\equiv 2\pmod 8$, 其中 p 为奇素数, 则有如下 3 种情形:

$$p\equiv 5\pmod 8,\quad p\equiv 9\pmod{16},\quad p\equiv 1\pmod{16}.$$

定理 2.4 [7] (1) (Genocchi, 1855) 设素数 $p\equiv 5\pmod 8$, 则 $2p$ 不是同余数.

(2) (Bastien, 1915) 设素数 $p\equiv 9\pmod{16}$, 则 $2p$ 不是同余数.

但是 Bastien 之后一百多年, $p\equiv 1 \pmod{16}$ 情形哪怕是猜想的结论也没有出现. 在文献 [19] 给出同余数新的判别法后, 本文作者证明了如下结果:

定理 2.5 设 $p\equiv 1 \pmod{16}$ 是素数. 如果 $h(-p)\not\equiv h(-2p) \pmod{16}$, 则 $2p$ 不是同余数.

接下来解释为什么之前没有 $p\equiv 1 \pmod{16}$ 情形的结果. 对于 $p\equiv 1 \pmod{16}$, 有

$$16 \mid r_s(p)-r_t(p).$$

如果 $r_s(p)\neq r_t(p)$, 并假设 BSD 猜想成立, 则得 $16\mid \#Ш_{E_{2p}}$, 而之前所有同余数 (非同余数) 方面的结果都是 $\#Ш_{E_{2p}}$ 偶部分至多是 4. 因为以前的方法处理不了 $16\mid \#Ш_{E_{2p}}$ 的情形.

再看前面 7 个模 16 余 1 的素数. $17, 97, 113, 193, 241, 257, 337, \ldots$, 其中仅有 $2\cdot 241$ 是非同余数, 这是一个非常令人困惑的现象. 因为, 我们应该相信, 在所有 $p\equiv 1 \pmod{16}$ 的素数集合中, $2p$ 是同余数的子集是 0 密度. 可是, 这里居然大部分都是同余数. 其实这是数据样本小的原因, 随着选取的范围不断扩大, $2p$ 是同余数的 p 会越来越稀疏.

考虑当 $p\equiv 1 \pmod{16}$ 为素数时, 如何计数 $2p$ 这样的同余数. 先引入记号

$$Q=\{p, 素数 \mid p\equiv 1 \pmod{16}\},$$
$$Q(4^n)=\{p\in Q \mid 4^n \parallel \#Ш_{E_{2p}}\}.$$

当 $n=0$ 时,

$$Q(1)=Q(4^0)=\{p\in Q \mid \#Ш_{E_{2p}} 为奇数\}.$$

我们知道, $p\in Q(1)$ 当且仅当 $2p$ 是同余数.

猜想 2.5 (1) 集合 $Q(1)$ 有无限多个元素并且有渐近公式

$$\#\{p\in Q(1)\mid p\leqslant x\}\sim cx^{\frac{3}{4}}(\log x)^{-\frac{5}{8}},$$

这里 $0.16<c<0.17$ 是一个常数. 特别地, $Q(1)$ 在 Q 中是具有 0 密度的无限子集.

(2) 对于任意整数 $n\geqslant 1$, $Q(4^{n+1})$ 在 Q 中的密度为 $\frac{1}{2^n}$.

表 4 给出了猜想 2.5(2) 的一些计算结果. 如表 2, 这里将 $Ш_{E_{2p}}$ 简记为 Ш.

问题 2.3 (1) 集合 $Q(1)$ 有无限多个元素, 其对应的椭圆曲线的沙群是平凡的吗?

(2) 进一步地, 集合 $Q(1)$ 中对应的椭圆曲线的沙群平凡的子集在 $Q(1)$ 中是 0 密度吗? 如果不是 0 密度, 这个密度是多少?

与前面一样, 推测 (1) 的答案是肯定的.

Pizer [15] 给出了下列结果:

$$h(-p)+h(-2p)\equiv \frac{p-1}{2} \pmod{8}. \tag{2.3}$$

假设 (2.3) 是 $h(-p)$ 和 $h(-2p)$ 之间模 8 唯一的关系. 在模 16 意义下, $(h(-p), h(-2p))$ 共有 8 种可能的取值:

$$X=\{(0,0),(0,8),(4,4),(4,12),(8,0),(8,8),(12,4),(12,12)\},$$

表 4 猜想 2.5(2) 的数值结果

$p\equiv 1 \pmod{16}$	$16\parallel \#Ш$	$64\parallel \#Ш$	$256\parallel \#Ш$	$1024\parallel \#Ш$	$4096\parallel \#Ш$	$r_s(p)=r_t(p)$
1,000	507	196	34	0	0	263
10,000	4,982	2,356	888	164	2	1,608

其中 4 个满足 $h(-p) \not\equiv h(-2p) \pmod{16}$.

猜想 2.6 设 $S = \{p \in Q \mid h(-p) \not\equiv h(-2p) \pmod{16}\}$, 则 S 在 Q 中的密度为 $\frac{1}{2}$. 表 5 是数值依据.

猜想 2.6 可以由下面的猜想推导出:

猜想 2.7 任取 $(a,b) \in X$, 令

$$S_{(a,b)} = \{p \in Q \mid (h(-p), h(-2p)) \equiv (a,b) \pmod{16}\},$$

则 $S_{(a,b)}$ 在 Q 中的密度为 $\frac{1}{8}$.

猜想 2.8 用 $Q(t,s)$ 表示满足下面条件的全体无平方因子的正整数构成的集合:

(1) n 恰有 t 个不同的奇素因子;

(2) $n \equiv 2 \pmod{8}$;

(3) $s(n) = s$.

而 $Q(t,s,r)$ 表示 $Q(t,s)$ 中满足 $r(n) = r$ 的所有 n 构成的子集.

那么 $Q(t,s,0)$ 在 $Q(t,s)$ 中的密度是 1, 并且对于任意偶数 $0 \leqslant r \leqslant s(n)$, 都有

$$\#Q(t,s,r) = \infty.$$

例 2.2 考虑形如 $n = 2pq$ 且满足 $p \equiv q \equiv 1 \pmod{8}$, $(\frac{p}{q}) = 1$ 的正整数, $n = 2pq$, $p \equiv q \equiv 1 \pmod{8}$, $(\frac{p}{q}) = 1$, 此时, $M_e = 0$, 所以, $s(n) = 4$.

(1) $n = 2 \cdot 17 \cdot 137$: $r = 0$.

(2) $n = 2 \cdot 17 \cdot 281$: $r = 2$.

(3) $n = 2 \cdot 17 \cdot 1361$: $r = 4$.

(III) 模 8 余 3 的情形

下面是一个经典的结果.

命题 2.1 [7] (Genocchi, 1855) 设 $p \equiv 3 \pmod{8}$ 是素数, 则 p 是非同余数.

文献 [19] 证明了下面的结果:

定理 2.6 (1) 设 $p \equiv 1$, $q \equiv 3 \pmod{8}$ 是两个素数. 如果 $h(-pq) \not\equiv h(-p) \pmod{8}$, 则 pq 不是同余数.

(2) 设 $p \equiv 5$, $q \equiv 7 \pmod{8}$ 是两个素数. 如果 $(\frac{q}{p}) = -1$, 或者 $(\frac{q}{p}) = 1$, $h(-pq) \equiv 4 \pmod{8}$, 则 pq 不是同余数.

对于模 8 余 3 的情形, 可以提出类似的猜想. 但是由于有命题 2.1, 我们需要考虑两个素因子乘积, 参考定理 2.6.

猜想 2.9 取定一个素数 p, 则在所有形如 $pq \equiv 3 \pmod{8}$ 的整数中, 有无穷多个同余数, 而且渐近公式也具有猜想 2.5 同样的形式.

对沙群也有类似的猜想.

表 5 猜想 2.6 的数值结果

$p \equiv 1 \pmod{16}$	$h(-p) \equiv h(-2p) \pmod{16}$
1,000	493
10,000	5,018

猜想 2.10 用 $R(t,s)$ 表示满足下面条件的全体无平方因子的正整数构成的集合:

(1) n 恰有 t 个不同的奇素因子;

(2) $n\equiv 3 \pmod 8$;

(3) $s(n)=s$.

而 $R(t,s,r)$ 表示 $R(t,s)$ 中满足 $r(n)=r$ 的 n 构成的子集.

那么 $R(t,s,0)$ 在 $R(t,s)$ 中的密度是 1, 并且对于任意偶数 $0\leqslant r\leqslant s(n)$, 都有

$$\#R(t,s,r)=\infty.$$

致谢 感谢审稿人仔细阅读本文并提出了很好的修改意见.

参考文献

1 Barrucand P, Cohn H. Note on primes of type x^2+32y^2, class number, and residuacity. J Reine Angew Math, 1969, 238: 67–70

2 Birch B J, Swinnerton-Dyer H P F. Notes on elliptic curves. II. J Reine Angew Math, 1965, 218: 79–108

3 Burns D, de Jeu R, Gangl H, et al. Hyperbolic tessellations and generators of K_3 for imaginary quadratic fields. Forum Math Sigma, 2021, 9: e40

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

5 Burungale A A, Tian Y. The even parity Goldfeld conjecture: Congruent number elliptic curves. J Number Theory, 2022, 230: 161–195

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

7 Dickson L E. History of the Theory of Numbers, Vol. II: Diophantine Analysis. New York: Chelsea Publishing, 1966

8 Heath-Brown D R. The size of Selmer groups for the congruent number problem, II. Invent Math, 1994, 118: 331–370

9 Kaplansky I. The forms $x+32y^2$ and $x+64y^2$. Proc Amer Math Soc, 2003, 131: 2299–2300

10 Kato K. p-adic Hodge theory and values of zeta functions of modular forms. Astérisque, 2004, 295: 117–290

11 Koblitz N. Introduction to Elliptic Curves and Modular Forms, 2nd ed. Graduate Texts in Mathematics, vol. 97. New York: Springer-Verlag, 1993

12 Kolyvagin V A. Euler systems. In: The Grothendieck Festschrift, vol. II. Boston: Birkhäuser, 1990, 435–483

13 Li J N, Ouyang Y, Xu Y. Abelian p-ramification groups and new Cohen-Lenstra heuristics (in Chinese). Sci Sin Math, 2021, 51: 1635–1654 [李加宁, 欧阳毅, 许跃. Abel p- 分歧扭子群和新 Cohen-Lenstra 猜想. 中国科学: 数学, 2021, 51: 1635–1654]

14 Li J N, Ouyang Y, Xu Y. On abelian 2-ramification torsion modules of quadratic fields. Sci China Math, 2022, 65: 2459–2482

15 Pizer A. On the 2-part of the class number of imaginary quadratic number fields. J Number Theory, 1976, 8: 184–192

16 Qin H R. The 2-Sylow subgroups of the tame kernel of imaginary quadratic fields. Acta Arith, 1995, 69: 153–169

17 Qin H R. The 4-rank of K_2O_F for real quadratic fields F. Acta Arith, 1995, 72: 323–333

18 Qin H R. Tame kernels and Tate kernels of quadratic number fields. J Reine Angew Math, 2001, 530: 105–144

19 Qin H R. Congruent numbers, quadratic forms and K_2. Math Ann, 2022, 383: 1647–1686

20 Shimura G. On modular forms of half integral weight. Ann of Math (2), 1973, 97: 440–481

21 Silverman J H. The Arithmetic of Elliptic Curves, 2nd ed. Graduate Texts in Mathematics, vol. 106. Dordrecht: Springer, 2009

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

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

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

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

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

27 Waldspurger J L. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. J Math Pures Appl (9), 1981, 60: 375–484

Conjectures and problems on congruent numbers

Hourong Qin

Abstract This paper proposes a series of conjectures and problems on congruent numbers based on the author's research findings on the subject. Numerical verification is also provided to support some of these conjectures.

Keywords **congruent number problem, elliptic curve, K_2 group, Shafarevich-Tate group, conjectures and problems**

MSC(2020) **11G05, 11G40, 11E20**

doi: 10.1360/SSM-2024-0091