DOI:10.19789/j.1004-9398.2024.06.001
文献引用:冷明睿,范永丰,蔡立.椭圆曲线14a2的一族二次扭[J].首都师范大学学报(自然科学版),2024,45(6):2-8. LENG M R,FAN Y F,CAI L. Quadratic twists of the elliptic curve 14a2[J]. Journal of Capital Normal University(Natural Science Edition),2024,45(6):2-8.

椭圆曲线14a2的一族二次扭*

冷明睿[1#]，范永丰[1#]，蔡　立[2#**]

(1. 首都师范大学数学科学学院，北京　100048；2. 首都师范大学交叉科学研究院，北京　100048)

摘要:本文考虑椭圆曲线14a2的一族二次扭。通过应用经典的2-下降法,证明了这一族中的所有曲线的2-Selmer群都同构于$(\mathbf{Z}/2\mathbf{Z})^2$。假设Shafarevich-Tate群有限,那么这些曲线的秩为1,Selmer $\mathbf{Z}_2$-余秩为1,且Shafarevich-Tate群的2-部分平凡。进而,根据Gross-Zagier公式和Tunnell-Saito定理,提出了一个问题:对于仅在2,7处分歧的四元数代数所对应的志村曲线,如何证明其上某个具体的Heegner点的非平凡性。

关键词:椭圆曲线;Selmer群;Heegner点
中图分类号:O156.2　　**文献标志码**:A

Quadratic twists of the elliptic curve 14a2*

LENG Mingrui[1#]，FAN Yongfeng[1#]，CAI Li[2#**]

(1. School of Mathematical Sciences，Capital Normal University，Beijing　100048；2. Academy for Multidisciplinary Studies，Capital Normal University，Beijing　100048)

Abstract: In this paper, we consider a quadratic twist family of the elliptic curve 14a2. Using the classical 2-descent method, we prove that all curves in this family have 2-Selmer group $(\mathbf{Z}/2\mathbf{Z})^2$. Assume the finiteness of the Shafarevich-Tate group, then these curves have rank 1, Selmer $\mathbf{Z}_2$-corank 1, and trivial 2-primary part of the Shafarevich-Tate group. According to the Gross-Zagier formula and the Tunnell-Saito theorem, we raise the question of how to prove the non-triviality of certain explicit Heegner points defined on Shimura curves associated to the quaternion algebra precisely ramified at 2 and 7.

Keywords: elliptic curve; Selmer group; Heegner point
CLC: O156.2　　**DC**: A

0　引　言

令E是一条定义在$\mathbf{Q}$上的椭圆曲线,并令$L(E,s)$是L-级数。Birch和Swinnerton-Dyer(BSD)猜想断言$E(\mathbf{Q})$的Mordell-Weil秩等于解析秩$r_{\mathrm{an}}(E/\mathbf{Q}) \coloneqq \mathrm{ord}_{s=1}L(E,s)$。广为人知的是,对于$r=0,1$,$r_{\mathrm{an}}(E/\mathbf{Q})=r \Rightarrow \mathrm{rank}_{\mathbf{Z}}E(\mathbf{Q})=r$,且Shafarevich-Tate群$Ш(E/\mathbf{Q})$是有限的。特别地,BSD猜想成立。这个结论基于Gross和Zagier[1]和Kolyvagin[2]所做的杰出工作。考虑p^∞-Selmer群

收稿日期:2024-07-10
*国家重点研发计划项目(2023YFA1009702);国家自然科学基金项目(12371012)
#所有作者按照姓氏笔画排序,贡献均等
**通信作者:caili@cnu.edu.cn

$S^{(p^\infty)}(E/\mathbf{Q})$的$\mathbf{Z}_p$-余秩,一个基本事实是对任何素数$p$,

$$\mathrm{rank}_{\mathbf{Z}} E(\mathbf{Q}) = r \text{ 且 } Ш(E/\mathbf{Q}) < \infty \Rightarrow \mathrm{corank}_{\mathbf{Z}_p} S^{(p^\infty)}(E/\mathbf{Q}) = r。$$

因此,对于$r = 0, 1$是否有

$$\mathrm{corank}_{\mathbf{Z}_p} S^{(p^\infty)}(E/\mathbf{Q}) = r \Rightarrow r_{\mathrm{an}}(E/\mathbf{Q}) = r?$$

上述蕴含关系通常被称作p-逆定理。

近年来,关于p-逆定理的研究取得了很大的进展,其主要技术手段是岩泽主猜想。当$r = 0$时,复乘椭圆曲线的情形最初由Rubin[3]对所有好约化的常态素数$p > 2$给出了证明。最近,此结论已经被Burungale和Tian[4]无条件地推广到所有的素数上;而对于非复乘情形,Skinner和Urban[5]在某些假设下对于常态的$p > 2$给出了证明;Wan[6]则在某些假设下对于好约化的超奇异素数$p > 2$做了证明。在$r = 1$时,首个一般性的p-逆定理的证明由Skinner[7]和Zhang[8]分别独立给出,在不同的假设下对非复乘椭圆曲线的常态的$p > 3$情形进行了证明。而对于复乘情形,Burungale和Tian[9]对常态的$p > 3$做了证明;Yu[10]对常态的$p = 2, 3$进行了证明。超奇异的$p > 3$情形被Burungale-Skinner-Tian所考虑。

值得注意的是,上述结果对于$p = 2$情形仅提供了极为少量的信息,特别是对于非复乘椭圆曲线,这是目前岩泽主猜想难以处理的情形。

但幸运的是,对于此种情形下一些二次扭族,有一个替代的方法可用来计算r_{an},即Birch引理[11-13]。此引理给出了Heegner点非平凡性一个判定条件,结合Gross-Zagier公式[1]即可得$r_{\mathrm{an}} = 1$。原始的Birch引理所考虑的Heegner点是定义在紧化的模曲线

$$X_0(N) := \Gamma_0(N)\backslash\mathcal{H} \cup \{\text{尖点}\}$$

上的。这里$\Gamma_0(N)$是水平N的Hecke同余子群,$\mathcal{H}$是上半平面。令E是定义在$\mathbf{Q}$上的导子为N的一条椭圆曲线。假设$K = \mathbf{Q}(\sqrt{-\ell})$,这里$\ell$是满足$\ell > 3, \ell \equiv 3 (\mathrm{mod}4)$的素数,并且假设$(E, K)$满足Heegner假设,即每一个$N$的素因子都在$K$中分裂。那么,存在一个理想$\mathcal{N} \subset \mathcal{O}_K$使得$\mathcal{O}_K/\mathcal{N} = \mathbf{Z}/N\mathbf{Z}$。因此,有一个复乘点$P := (\mathbf{C}/\mathcal{O}_K \to \mathbf{C}/\mathcal{N}^{-1}) \in X_0(N)(H_K)$,这里$H_K$是$K$的希尔伯特类域。令$f: X_0(N) \to E$是$E$的一个模参数化。定义

$$y_K := \sum_{\tau \in \mathrm{Gal}(H_K/K)} f(P^\tau) \in E(K),$$

那么,Birch证明了如果$f([0]) \notin 2E(\mathbf{Q})$以及$f([\infty]) = O$,其中$[0]$和$[\infty]$分别是0和无穷远处的尖点,那么$y_K$是$E(K)$上的无限阶点。

Birch引理已经被推广到更多情形。Tian[14]、Coates等[12]和Cai等[15]利用不同于Birch所取水平的模曲线上的Heegner点,分别为$X_0(32)$、$X_0(36)$以及$X_0(49)$构造了具体的二次扭族。

然而,对于一些椭圆曲线,无论水平如何选择,在模曲线上定义的Heegner点总是映射到挠点。要处理这个问题,一个引人注目的结果是Yuan等[16]的一般化的Gross-Zager公式,将L-级数的导数与一般志村曲线上定义的Heegner点的高度联系起来。

本文构造了一个Cremona标签为14a2的椭圆曲线的二次扭族。

定理0.1　令E = 14a2,ℓ是一个满足$\ell \equiv 3 (\mathrm{mod}4)$的素数,并且2,7在$\mathbf{Q}(\sqrt{-\ell})$中惯性。

(1)椭圆曲线$E^{(-\ell)}(\mathbf{Q})$的2-Selmer群$S^{(2)}(E^{(-\ell)}/\mathbf{Q}) = (\mathbf{Z}/2\mathbf{Z})^2$。若进一步假设Shafarevich-Tate群$Ш(E^{(-\ell)}/\mathbf{Q})$有限,那么$\mathrm{rank}_{\mathbf{Z}} E^{(-\ell)}(\mathbf{Q}) = 1$,Shafarevich-Tate群$Ш(E^{(-\ell)}/\mathbf{Q})[2]$的2-部分平凡,以及Selmer 2-余秩$\mathrm{corank}_{\mathbf{Z}_2} S^{(2^\infty)}(E^{(-\ell)}/\mathbf{Q}) = 1$。

(2)可用于构造$E(\mathbf{Q}(\sqrt{-\ell}))$上的非挠点的Heegner点只能定义在与仅在2,7处分歧的不定四元数代数所对应的志村曲线上,参见命题2.1。

下面使用经典的2-下降法作为证明(1)的主要工具[17]。在第2节中,将Heegner点的平凡性归结为p-进群表示论中的一个分歧律问题,接着使用Tunnell-Saito定理[18-19]证明(2)。最后,给出了一个精确的Heegner点[20],其是非平凡的当且仅当L-函数的导数中心值是非零的。在本文结束前,提出了一个问题,即如何证明此Heegner点的非平凡性,参见问题2.3。

1　经典2-下降法

首先回顾如下基本事实。

定理1.1[17,定理X.4.2]　设$f: E/K \to E'/K$是定义在域K上的椭圆曲线的同源映射,那么有正合序列

$$0 \to E'(K)/f(E(K)) \to S^{(f)}(E/K) \to Ш(E/K)[f] \to 0。$$

这里 $S^{(f)}(E/K)$ 是 f-Selmer 群,$Ш(E/K)[f]$ 是 Shafarevich-Tate 群的 f-部分。

现在,令 E 和 ℓ 同定理 0.1,考虑 $E = 14a2$ 的简化魏尔斯特拉斯形式

$$E: y^2 = x^3 - 46\,035x - 3\,116\,178,$$

通过变量代换将其有理 2-挠点移动到 $(0,0)$,可以写出 $E^{(-\ell)}$ 确切的表达式

$$E^{(-\ell)}: y^2 = x^3 + 2\cdot 3^2\cdot 13\cdot \ell x^2 - 3^4\cdot 7^3\cdot \ell^2 x。 \quad (1)$$

为了应用 2 -下降法,还需要考虑另外一条曲线

$$E'^{(-\ell)}: y^2 = x^3 - 2^2\cdot 3^2\cdot 13\cdot \ell x^2 + 2^{11}\cdot 3^4\cdot \ell^2 x,$$

这样就有次数为 2 的同源映射 $\phi: E^{(-\ell)} \to E'^{(-\ell)}$ 和其对偶同源映射 $\hat{\phi}: E'^{(-\ell)} \to E^{(-\ell)}$ 满足 $\hat{\phi}\circ\phi = [2]$,具体形式为

$$\phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(-3^4\cdot 7^3\cdot \ell^2 - x^2)}{x^2}\right), \quad (2)$$

$$\hat{\phi}(x,y) = \left(\frac{y^2}{4x^2}, \frac{y(2^{11}\cdot 3^4\cdot \ell^2 - x^2)}{8x^2}\right)。 \quad (3)$$

由定理 1.1,得到

$$0 \to \frac{E'^{(-\ell)}(\mathbf{Q})}{\phi(E^{(-\ell)}(\mathbf{Q}))} \to S^{(\phi)}(E^{(-\ell)}/\mathbf{Q}) \to Ш(E^{(-\ell)}/\mathbf{Q})[\phi] \to 0, \quad (4)$$

$$0 \to \frac{E^{(-\ell)}(\mathbf{Q})}{\hat{\phi}(E'^{(-\ell)}(\mathbf{Q}))} \to S^{(\hat{\phi})}(E'^{(-\ell)}/\mathbf{Q}) \to Ш(E'^{(-\ell)}/\mathbf{Q})[\hat{\phi}] \to 0。 \quad (5)$$

令 $C_d/\mathbf{Q}$ 和 $C'_d/\mathbf{Q}$ 分别是 $E^{(-\ell)}/\mathbf{Q}$ 和 $E'^{(-\ell)}/\mathbf{Q}$ 所对应的齐性空间。具体由方程

$$C_d: dw^2 = d^2 - 2^2\cdot 3^2\cdot 13\cdot d\ell z^2 + 2^{11}\cdot 3^4\cdot \ell^2 z^4,$$

$$C'_d: dw^2 = d^2 + 2\cdot 3^2\cdot 13\cdot d\ell z^2 - 3^4\cdot 7^3\cdot \ell^2 z^4$$

给出。令 S 是所有的使得 $E^{(-\ell)}$ 和 $E'^{(-\ell)}$ 具有坏约化的有限素位,再加上无穷素位所构成的集合。可以验证

$$S = \{2, 3, 7, \ell, \infty\}。$$

此外,令

$$\mathbf{Q}(S,2) = \left\{b \in \mathbf{Q}^\times/(\mathbf{Q}^\times)^2 \mid \mathrm{ord}_v(b) \equiv 0 (\mathrm{mod}2),\ \forall v \notin S\right\}。$$

注意到 ϕ-Selmer 群满足

$$S^{(\phi)}(E^{(-\ell)}/\mathbf{Q}) \cong \left\{d \in \mathbf{Q}(S,2) \mid C_d(\mathbf{Q}_v) \neq \varnothing,\ \forall v \in S\right\},$$

以及类似的

$$S^{(\hat{\phi})}(E'^{(-\ell)}/\mathbf{Q}) \cong \left\{d \in \mathbf{Q}(S,2) \mid C'_d(\mathbf{Q}_v) \neq \varnothing,\ \forall v \in S\right\}。$$

更进一步,还可以给出式(4)和(5)中映射 δ 和 δ' 的具体表达,由下列式子给出

$$\delta: O \mapsto 1, \quad (0,0) \mapsto 2^{11}\cdot 3^4\cdot \ell^2, \quad (X,Y) \mapsto X;$$

$$\delta': O \mapsto 1, \quad (0,0) \mapsto -3^4\cdot 7^3\cdot \ell^2, \quad (X,Y) \mapsto X。$$

命题 1.2 如上文所述将 $S^{(\phi)}(E^{(-\ell)}/\mathbf{Q})$ 和 $S^{(\hat{\phi})}(E'^{(-\ell)}/\mathbf{Q})$ 等同于 $\mathbf{Q}^\times/(\mathbf{Q}^\times)^2$ 的子群,那么有:

(1) $S^{(\phi)}(E^{(-\ell)}/\mathbf{Q}) = \langle 2, \ell\rangle \cong (\mathbf{Z}/2\mathbf{Z})^2$;

(2) $S^{(\hat{\phi})}(E'^{(-\ell)}/\mathbf{Q}) = \langle -7\rangle \cong \mathbf{Z}/2\mathbf{Z}$。

根据上文的讨论,只需要对于所有的 $d \in \mathbf{Q}(S,2)$ 和 $v \in S$ 确定 C_d 和 C'_d 在 $\mathbf{Q}_v$ 上的可解性即可。因此,下面的证明在很大程度上依赖于 Hensel 引理。

证明 首先证明(1)。

对于 $d = -1$ 有

$$C_{-1}: -w^2 = 1 + 2^2\cdot 3^2\cdot 13\cdot \ell z^2 + 2^{11}\cdot 3^4\cdot \ell^2 z^4 > 0,$$

所以,$C_{-1}(R) = \varnothing$。因此,$-1 \notin S^{(\phi)}(E^{(-\ell)}/\mathbf{Q})$。

对于 $d = \pm 2$ 有

$$\delta(0,0) = 2^{11}\cdot 3^4\cdot \ell^2 \equiv 2\left(\mathrm{mod}(\mathbf{Q}^\times)^2\right)。$$

因此,$2 \in S^{(\phi)}(E^{(-\ell)}/\mathbf{Q})$,以及 $-2 \notin S^{(\phi)}(E^{(-\ell)}/\mathbf{Q})$。

对于 $d = 3k, 3 \nmid k$ 有

$$C_{3k}: 3kw^2 = (3k)^2 - 2^2\cdot 3^3\cdot 13\cdot \ell k z^2 + 2^{11}\cdot 3^4\cdot \ell^2 z^4。$$

注意到 $\mathrm{ord}_3(3kw^2)$ 是奇数,而上式等号右边的 3-进赋值是偶数。所以,$C_{3k}(\mathbf{Q}_3) = \varnothing$。因此,$3k \notin S^{(\phi)}(E^{(-\ell)}/\mathbf{Q})$。

对于 $d = 7k, 7 \nmid k$ 有

$$C_{7k}: 7kw^2 = (7k)^2 - 2^2\cdot 3^2\cdot 7\cdot 13\cdot \ell k z^2 + 2^{11}\cdot 3^4\cdot \ell^2 z^4。$$

注意到 $\mathrm{ord}_7(7kw^2)$ 是奇数,而上式等号右边的 7-进赋值是偶数。所以,$C_{7k}(\mathbf{Q}_7) = \varnothing$。因此,$7k \notin S^{(\phi)}(E^{(-\ell)}/\mathbf{Q})$。

对于 $d = \pm\ell$ 有

$$C_\ell: \ell w^2 = \ell^2 - 2^2\cdot 3^2\cdot 13\cdot \ell^2 z^2 + 2^{11}\cdot 3^4\cdot \ell^2 z^4,$$

断言 $C_\ell(\mathbf{Q}_v)$ 对所有的 $v \in S$ 非空。为了简单起见,做变量替换 $(w \mapsto \ell w, z \mapsto z/6)$ 得到

$$\ell w^2 = 1 - 13z^2 + 2^7 z^4。 \quad (6)$$

若 $v = 2$ 有

$$\ell w^2 \equiv 1 + 3z^2 (\mathrm{mod}8)。$$

固定 $w = 2$,那么因为 2 在 $\mathbf{Q}(\sqrt{-\ell})$ 中惯性,$-\ell \equiv 5(\mathrm{mod}8)$,所以有 $z^2 \equiv 1(\mathrm{mod}8)$。由 Hensel 引理,方程在 $\mathbf{Z}_2$ 中可解。

若$v=3$有

$$\ell w^2\equiv 1+2z^2+2z^4(\mathrm{mod}3)。$$

如果$\ell\equiv 1(\mathrm{mod}3)$,那么固定$z=0$,否则$\ell\equiv 2(\mathrm{mod}3)$,那么固定$z=1$。在这2种情形下,$w=1$都是一个单根。因此,式(6)在$\mathbf{Z}_3$中可解。

若$v=7$,固定$z=1$,有

$$\ell w^2\equiv 4(\mathrm{mod}7)。$$

因为7在$\mathbf{Q}\left(\sqrt{-\ell}\right)$中惯性,得到$\left(\frac{-\ell}{7}\right)=-1$。所以,

$$\left(\frac{\ell}{7}\right)=\left(\frac{-\ell}{7}\right)\left(\frac{-1}{7}\right)=(-1)(-1)^{(7-1)/2}=1,$$

于是ℓ是模7的二次剩余。因此,式(6)在$\mathbf{Z}_7$中可解。

若$v=\ell$,有

$$1-13z^2+2^7z^4\equiv 0(\mathrm{mod}\ell),$$

将上式视作关于z^2的二次方程。判别式是$\Delta=(-13)^2-4\cdot 2^7=-7^3$。由二次互反律,有

$$\left(\frac{-7^3}{\ell}\right)=\left(\frac{-1}{\ell}\right)\left(\frac{7}{\ell}\right)=(-1)^{(\ell-1)/2}(-1)^{(7-1)(\ell-1)/4}\left(\frac{\ell}{7}\right)=1,\tag{7}$$

所以,$z^2=\left(13\pm\sqrt{\Delta}\right)/2^8\in F_\ell$。有

$$\left(\frac{13+\sqrt{\Delta}}{\ell}\right)\left(\frac{13-\sqrt{\Delta}}{\ell}\right)=\left(\frac{2^9}{\ell}\right)=\left(\frac{2}{\ell}\right)=(-1)^{(\ell^2-1)/8}=-1。\tag{8}$$

因此,$13\pm\sqrt{\Delta}$中必有一个为模ℓ的二次剩余,这样找到一个单根。因此式(6)在$\mathbf{Z}_\ell$中可解。

若$v=\infty$,那么显然$(w,z)=\left(\sqrt{\ell},0\right)$是$C_\ell$的解,因此,$\ell\in S^{(\phi)}\left(E^{(-\ell)}/\mathbf{Q}\right)$,以及$-\ell\notin S^{(\phi)}\left(E^{(-\ell)}/\mathbf{Q}\right)$。这样便完成了对(1)的证明。现在来证明(2)。

对于$d=-7$有

$$\delta(0,0)=-3^4\cdot 7^3\cdot\ell^2\equiv -7\left(\mathrm{mod}\left(\mathbf{Q}^\times\right)^2\right),$$

因此,$-7\in S^{(\phi)}\left(E'^{(-\ell)}/\mathbf{Q}\right)$。

对于$d=-1,7$有

$$C_7'\colon 7w^2=7^2+2\cdot 3^2\cdot 7\cdot 13\cdot\ell z^2-3^4\cdot 7^3\cdot\ell^2z^4,$$

将C_7'简化为

$$w^2=7+2\cdot 13\cdot\ell z^2-7^2\cdot\ell^2z^4。$$

如果$\mathrm{ord}_\ell(z)\geqslant 0$,那么模$\ell$约化得到

$$w^2\equiv 7(\mathrm{mod}\ell)。$$

然而,在式(7)中,看到7不是模ℓ的二次剩余。如果$\mathrm{ord}_\ell(z)<0$,那么通过变量替换$w=w'z,z=1/(7\ell z')$得到

$$w^2=-1+2\cdot 13\cdot\ell z'^2+7^3\cdot\ell^2z'^4,$$

且$\mathrm{ord}_\ell(z')\geqslant 0$。同样模$\ell$约化,得到

$$w^2\equiv -1(\mathrm{mod}\ell)。$$

然而,因为$\ell\equiv 3(\mathrm{mod}4)$,这不可能发生。因此得到$C_7'(\mathbf{Q}_\ell)=\varnothing$,所以$-1,7\notin S^{(\phi)}\left(E'^{(-\ell)}/\mathbf{Q}\right)$。

对于$d=2k,2\nmid k$有

$$C_{2k}'\colon 2kw^2=(2k)^2+2^2\cdot 3^2\cdot 13\cdot\ell kz^2-3^4\cdot 7^3\cdot\ell^2z^4。$$

注意到$\mathrm{ord}_2(2kw^2)$是奇数,而上式等号右边的2-进赋值是偶数。所以,$C_{2k}'(\mathbf{Q}_2)=\varnothing$。因此,$2k\notin S^{(\phi)}\left(E'^{(-\ell)}/\mathbf{Q}\right)$。

对于$d=3k,3\nmid k$有

$$C_{3k}'\colon 3w^2=3^2+2\cdot 3^3\cdot 13\cdot\ell z^2-3^4\cdot 7^3\cdot\ell^2z^4。$$

注意到$\mathrm{ord}_3(3kw^2)$是奇数,而上式等号右边的3-进赋值是偶数。所以,$C_{3k}'(\mathbf{Q}_3)=\varnothing$。因此,$3k\notin S^{(\phi)}\left(E'^{(-\ell)}/\mathbf{Q}\right)$。

对于$d=\pm\ell$有

$$C_\ell'\colon \ell w^2=\ell^2+2\cdot 3^2\cdot 13\cdot\ell^2z^2-3^4\cdot 7^3\cdot\ell^2z^4。$$

做变量替换$z'=3z,w'=w/\ell$得到

$$\ell w'^2=1-2\cdot 13\cdot z'^2-7^3z'^4,$$

通过比较上面等式2边ℓ-赋值,看到$z'\in\mathbf{Z}_\ell^\times$。所以,

$$1-2\cdot 13\cdot z'^2-7^3z'^4\equiv 0(\mathrm{mod}\ell)。$$

将上式视作关于z^2的二次方程,那么得到判别式$\Delta=(-2\cdot 13)^2-\left(-4\cdot 7^3\right)=2^{11}$,正如已经在式(8)中看到的那样,这不是模$\ell$的二次剩余。所以,$C_\ell'(\mathbf{Q}_\ell)=\varnothing$,并且$\ell\notin S^{(\phi)}\left(E^{(-\ell)}/\mathbf{Q}\right)$。同理可证$-\ell$情形。这便证明了(2)。

接下来,计算$E^{(-\ell)}$的挠子群。

命题1.3　$E_{\mathrm{tor}}^{(-\ell)}(\mathbf{Q})\cong\mathbf{Z}/2\mathbf{Z}$。

证明　显然,$(0,0)$是$E^{(-\ell)}(\mathbf{Q})$唯一的2阶挠点,所以

$$2|\#E_{\mathrm{tor}}^{(-\ell)}(\mathbf{Q})。$$

注意到$\#\tilde{E}(F_5)=6$与ℓ的选取无关,所以$\#E_{\mathrm{tor}}^{(-\ell)}(\mathbf{Q})|6$。最后,假设$P$是一个3阶挠点。令$x(P)=x\in\mathbf{Z}$是$P$的$x$-坐标,那么有

$$x(2P)=\frac{x^4+2\cdot 3^4\cdot 7^3\cdot\ell^2x^2+3^8\cdot 7^6\cdot\ell^4}{2^2\cdot x^3+2^3\cdot 3^2\cdot 13\cdot\ell x^2-2^2\cdot 3^4\cdot 7^3\cdot\ell^2x}。$$

因为P是三阶挠点,那么便得到$x(2P)=x$。这给出方程

$$x^4+2^3\cdot 3\cdot 13\cdot\ell x^3-2\cdot 3^4\cdot 7^3\cdot\ell^2x^2-3^7\cdot 7^6\cdot\ell^4=0。\tag{9}$$

事实上,$3\cdot 7^2\cdot\ell$和$-3^2\cdot 7^2\cdot\ell$是(9)仅有的2个解。然而,将其代入到式(1),在等式右边得到一个

非完全平方数,这与 Nagell-Lutz 定理矛盾。因此,$E_{\mathrm{tor}}^{(-\ell)}(\mathbf{Q})\cong\mathbf{Z}/2\mathbf{Z}$。

现在证明定理 0.1(1)。由定理1.1,得到下述正合序列:

$$0\to\frac{E'^{(-\ell)}(\mathbf{Q})}{\phi\left(E^{(-\ell)}(\mathbf{Q})\right)}\to S^{(\phi)}\left(E^{(-\ell)}/\mathbf{Q}\right)\to Ш\left(E^{(-\ell)}/\mathbf{Q}\right)[\phi]\to 0, \tag{10}$$

$$0\to\frac{E^{(-\ell)}(\mathbf{Q})}{2E^{(-\ell)}(\mathbf{Q})}\to S^{(2)}\left(E^{(-\ell)}/\mathbf{Q}\right)\to Ш\left(E^{(-\ell)}/\mathbf{Q}\right)[2]\to 0, \tag{11}$$

$$0\to\frac{E^{(-\ell)}(\mathbf{Q})}{\hat{\phi}\left(E'^{(-\ell)}(\mathbf{Q})\right)}\to S^{(\hat{\phi})}\left(E'^{(-\ell)}/\mathbf{Q}\right)\to Ш\left(E'^{(-\ell)}/\mathbf{Q}\right)[\hat{\phi}]\to 0, \tag{12}$$

$$0\to\frac{E'^{(-\ell)}(\mathbf{Q})[\hat{\phi}]}{\phi\left(E^{(-\ell)}(\mathbf{Q})[2]\right)}\to\frac{E'^{(-\ell)}(\mathbf{Q})}{\phi\left(E^{(-\ell)}(\mathbf{Q})\right)}\to\frac{E^{(-\ell)}(\mathbf{Q})}{2E^{(-\ell)}(\mathbf{Q})}\to\frac{E^{(-\ell)}(\mathbf{Q})}{\hat{\phi}\left(E'^{(-\ell)}(\mathbf{Q})\right)}\to 0。 \tag{13}$$

关于 Shafarevich-Tate 群,有

$$0\to Ш\left(E^{(-\ell)}/\mathbf{Q}\right)[\phi]\to Ш\left(E^{(-\ell)}/\mathbf{Q}\right)[2]\xrightarrow{\phi} Ш\left(E'^{(-\ell)}/\mathbf{Q}\right)[\hat{\phi}], \tag{14}$$

$$0\to Ш\left(E'^{(-\ell)}/\mathbf{Q}\right)[\hat{\phi}]\to Ш\left(E'^{(-\ell)}/\mathbf{Q}\right)[2]\xrightarrow{\hat{\phi}} Ш\left(E^{(-\ell)}/\mathbf{Q}\right)[\phi]。 \tag{15}$$

由式(10)、(12)和(13),分别得到

$$\dim_{F_2}S^{(\phi)}\left(E^{(-\ell)}/\mathbf{Q}\right)=\dim_{F_2}\frac{E'^{(-\ell)}(\mathbf{Q})}{\phi\left(E^{(-\ell)}(\mathbf{Q})\right)}+\dim_{F_2}Ш\left(E^{(-\ell)}/\mathbf{Q}\right)[\phi],$$

$$\dim_{F_2}S^{(\hat{\phi})}\left(E'^{(-\ell)}/\mathbf{Q}\right)=\dim_{F_2}\frac{E^{(-\ell)}(\mathbf{Q})}{\hat{\phi}\left(E'^{(-\ell)}(\mathbf{Q})\right)}+\dim_{F_2}Ш\left(E'^{(-\ell)}/\mathbf{Q}\right)[\hat{\phi}],$$

及

$$\dim_{F_2}\frac{E'^{(-\ell)}(\mathbf{Q})[\hat{\phi}]}{\phi\left(E^{(-\ell)}(\mathbf{Q})[2]\right)}+\dim_{F_2}\frac{E^{(-\ell)}(\mathbf{Q})}{2E^{(-\ell)}(\mathbf{Q})}=\dim_{F_2}\frac{E'^{(-\ell)}(\mathbf{Q})}{\phi\left(E^{(-\ell)}(\mathbf{Q})\right)}+\dim_{F_2}\frac{E^{(-\ell)}(\mathbf{Q})}{\hat{\phi}\left(E'^{(-\ell)}(\mathbf{Q})\right)}。$$

因此,

$$\dim_{F_2}\frac{E^{(-\ell)}(\mathbf{Q})}{2E^{(-\ell)}(\mathbf{Q})}=\dim_{F_2}S^{(\phi)}\left(E^{(-\ell)}/\mathbf{Q}\right)+\dim_{F_2}S^{(\hat{\phi})}\left(E'^{(-\ell)}/\mathbf{Q}\right)。$$

可以具体计算得到

$$\dim_{F_2}\frac{E'^{(-\ell)}(\mathbf{Q})[\hat{\phi}]}{\phi\left(E^{(-\ell)}(\mathbf{Q})[2]\right)}=1。$$

注意到

$$(0,0)\in\frac{E^{(-\ell)}(\mathbf{Q})}{\hat{\phi}\left(E'^{(-\ell)}(\mathbf{Q})\right)},$$

因此,由式(12),$Ш\left(E'^{(-\ell)}/\mathbf{Q}\right)[\hat{\phi}]=0$。由式(14),有 $Ш\left(E^{(-\ell)}/\mathbf{Q}\right)[2]=Ш\left(E^{(-\ell)}/\mathbf{Q}\right)[\phi]$。那么将上面的到的结果带入到式(16),得到

$$\mathrm{rank}_{\mathbf{Z}}E^{(-\ell)}(\mathbf{Q})=1-\dim_{F_2}Ш\left(E^{(-\ell)}/\mathbf{Q}\right)[2],$$

因此,由式(11),得到

$$\dim_{F_2}S^{(2)}\left(E^{(-\ell)}/\mathbf{Q}\right)=2。$$

若假设 $Ш\left(E^{(-\ell)}/\mathbf{Q}\right)$ 有限,由文献[17]中的定理4.14,可以得到 $Ш\left(E^{(-\ell)}/\mathbf{Q}\right)[2]=0$,$\mathrm{rank}_{\mathbf{Z}}E^{(-\ell)}(\mathbf{Q})=1$。

令 p 是一个素数。定义 p^{∞}-Selmer 群为

$$S^{(p^{\infty})}(E/\mathbf{Q}):=\varinjlim S^{(p^n)}(E/\mathbf{Q})\cong\left(\mathbf{Q}_p/\mathbf{Z}_p\right)^r\oplus A,$$

这里 A 是一个有限阿贝尔 p-群。此外,$S^{(p^{\infty})}(E/\mathbf{Q})$ 的 $\mathbf{Z}_p$-余秩定义为 r。定义 Selmer 秩为

$$r_q(E/\mathbf{Q}):=\dim_{F_q}S^{(q)}(E/\mathbf{Q})-\dim_{F_q}E(\mathbf{Q})[q]。$$

则有 $r_p(E/\mathbf{Q})\geqslant r_{p^2}(E/\mathbf{Q})\geqslant\cdots\geqslant\mathrm{rank}_{\mathbf{Z}}(E/\mathbf{Q})$,

$$\lim_{n\to\infty}r_{p^n}(E/\mathbf{Q})=\mathrm{corank}_{\mathbf{Z}_p}S^{(p^{\infty})}(E/\mathbf{Q})。$$

由式(11),有 $S^{(2)}\left(E^{(-\ell)}/\mathbf{Q}\right)\cong(\mathbf{Z}/2\mathbf{Z})^2$。所以,

$$1=r_2\left(E^{(-\ell)}/\mathbf{Q}\right)\geqslant\mathrm{corank}_{\mathbf{Z}_2}S^{(2^{\infty})}\left(E^{(-\ell)}/\mathbf{Q}\right)\geqslant\mathrm{rank}_{\mathbf{Z}}\left(E^{(-\ell)}/\mathbf{Q}\right)=1。$$

这证明了定理0.1(1)。

2 志村曲线上的Heegner点

令 B 是 $\mathbf{Q}$ 上在同构意义下唯一的四元数代数。设有限素位集合 $\Sigma(B)$ 是由 B 的分歧素位所构成,即 $B_v:=B\otimes_{\mathbf{Q}}\mathbf{Q}_v$ 是一个可除代数当且仅当 $v\in\Sigma(B)$。令 U 是 $\hat{B}^{\times}$ 的一个紧开子群,其中 $\hat{B}:=B\otimes_{\mathbf{Q}}\hat{\mathbf{Q}}$。假设 $\#\Sigma(B)$ 是偶数。那么,存在一个相应的 $\mathbf{Q}$ 上的紧致化志村曲线 X_U,其复点通过

$$X_U(\mathbb{C})\cong B^{\times}\backslash\mathcal{H}^{\pm}\times\hat{B}^{\times}/U\cup\{\text{尖点}\}$$

形成一个紧黎曼面。

令 $E/\mathbf{Q}$ 是一条椭圆曲线并且设 $f:X_U\to E$ 是 $\mathbf{Q}$ 上的非常值态射,且将文献[16]中定义的 X_U 的正规化 Hodge 类 ξ_U 映到 E 的单位元。将 f 称作一个 E 通过 X_U 的模参数化。设 K 是一个虚二次域。

固定一个嵌入 $K\hookrightarrow B$,再令 $z\in H$ 是唯一的被 $K^\times$ 经由 $B^\times$ 作用固定的点。设 $P=[z,1]_U$ 是 $(z,1)\in H^\pm\times\hat{B}^\times$ 在 $X_U(\mathbf{C})$ 中的像。复乘理论保证了 P 事实上在 $X_U(K^{ab})$ 中,其中 K^{ab} 是 K 的极大阿贝尔扩张。那么,$f(P)$ 在 $E(K^{ab})\otimes_{\mathbf{Z}}\mathbf{Q}$ 上是有良好定义的点。定义

$$P_K(f)=\sum_{\tau\in\mathrm{Gal}(K^{ab}/K)}f(P^\tau)\in E(K)\otimes_{\mathbf{Z}}\mathbf{Q}。$$

如下命题本质上是来自于 Tunnell-Saito 定理[18-19]。

命题 2.1　令 $E=$ 14a2, ℓ 是与定理 0.1 中满足相同条件的素数,$K=\mathbf{Q}(\sqrt{-\ell})$。设 B 是一个四元数代数满足 $\Sigma(B)\neq 2,7$, U, X_U, f 同上,那么 $P_K(f)=0$。

证明　证明的框架参考 Yuan 等[16]所述。对于 $\hat{B}^\times$ 的 2 个紧开子群 $U_1\subset U_2$,存在一个自然的满同态 $X_{U_1}\to X_{U_2}$。定义

$$\pi=\mathrm{Hom}^0_\xi(X,E):=\varinjlim_U\mathrm{Hom}^0_{\xi_U}(X_U,E),$$

其中 $\mathrm{Hom}^0_{\xi_U}(X_U,E)$ 是由 $\mathrm{Hom}_{\mathbf{Q}}(X_U,E)\otimes_{\mathbf{Z}}\mathbf{Q}$ 中的将 ξ_U 映到单位元的同态组成的空间。显然,$f\in\pi$。进一步定义

$$P(\pi):=\mathrm{Hom}_{K^\times}(\pi,E(K)\otimes_{\mathbf{Z}}\mathbf{Q}),$$

显然,$f\mapsto P_K(f)$ 是 $\mathcal{P}(\pi)$ 中的元素。由文献[16]中的定理3.4可知,$\pi\otimes_{\mathbf{Q}}\mathbf{C}=\otimes_v\pi_{v,\mathbf{C}}$,其中 $\pi_{v,\mathbf{C}}$ 是 $B_v^\times$ 的一个不可约的可容许的 $\mathbf{C}$-表示。令

$$\mathcal{P}(\pi_v):=\mathrm{Hom}_{K_v^\times}(\pi_{v,\mathbf{C}},\mathbf{C})。$$

如果对某些素位 v, $\mathcal{P}(\pi_v)=0$,那么 $\mathcal{P}(\pi)=0$,于是问题约化到局部情形。

设 $N=14$ 是 E 的导子。如果 $v\nmid N$,那么 π_v 到 $GL_2(\mathbf{Q}_v)$ 的 Jacquet-Langlands 对应 σ 是一个主序列表示,因此,B_v 必定是分歧的[20,引理3.1(1)]。如果 $v|N$,由于 N 无平方因子,σ 的导子是奇数,因此,B_v 必定是非分裂的[20,引理3.1(4)]。根据 Tunnell-Saito 定理[18-19],如果 $\Sigma(B)\neq 2,7$,那么对某些 v,得到 $\mathcal{P}(\pi_v)=0$,这表明 $P_K(f)=0$。

故此,为了寻找所研究曲线的二次扭族上非平凡的 Heegner 点,B 的唯一可能的选择只能是恰好仅在 2,7 处分歧的四元数代数。作为文献[20]中定理1.5的特殊情形,现在对所研究的二次扭族给出精确 Gross-Zagier 公式。

定理 2.2[20]　令 $E=$ 14a2, ℓ 是与定理 0.1 中满足相同条件的素数,$K=\mathbf{Q}(\sqrt{-\ell})$。令 B 是 $\mathbf{Q}$ 上的唯一满足 $\Sigma(B)=2,7$ 的四元数代数。固定一个嵌入 $K\hookrightarrow B$。令 $R\subset B$ 是判别式为 14 且在 $K^\times$-共轭意义下唯一的满足 $R\cap K=O_K$ 的序模(order)。设 $U=\hat{R}^\times\subset\hat{B}^\times$。设 X_U 是 $\mathbf{Q}$ 上对应于 B 的水平为 U 的志村曲线,并设模参数化 $f\colon X_U\to E$ 如上文所述。那么,f 存在并且在差一个标量乘法的意义下唯一,并且有

$$L'(E_K,1)=\frac{8\pi^2(\phi,\phi)_{U_0(14)}}{\sqrt{\ell}}\cdot\frac{\hat{h}_K(P_K(f))}{\deg f},$$

其中 $U_0(14)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in GL_2(\hat{\mathbf{Z}})\,\middle|\,c\in 14\hat{\mathbf{Z}}\right\}$, $(\cdot,\cdot)_{U_0(14)}$ 是相对于上半平面 H 的测度 $\mathrm{d}x\mathrm{d}y/y^2$ 的 Petersson 配对,ϕ 是对应于 E 的 $GL_2(\mathbb{A}_{\mathbf{Q}})$ 上权为 2 的希尔伯特全纯新形式,$\hat{h}_K$ 是 K 上的 Néron-Tate 高度,$\deg f$ 是模参数化 f 的次数。

证明　遵循文献[20]定理1.5中定义的记号。f 的存在唯一性可由文献[20]中的命题3.7得到。如同命题 2.1 的证明,有 $\pi_A=\pi$ 的中心特征平凡,$\chi=1$,以及 $\Sigma(B)=2,7$。因此文献[20]中定理1.5的条件(1)、(2)是满足的。阿贝尔簇 $A=E$ 是一条椭圆曲线,所以 $A^\vee=A$,则容易有如下验证:

(1) $D=D_K=-\ell, d=1$;

(2) $c=c_1=1, \Sigma=\Sigma_D=\varnothing$;

(3) 由于 $\mathrm{Pic}(\mathbf{Z})=0, \kappa_{c_1}=1$,于是有 $u_1=[\mathcal{O}_K^\times:\mathbf{Z}^\times]=1$;

(4) $f_1=f_2=f$,于是 $\left\langle P^0_\chi(f_1),P^0_{\chi^{-1}}(f_2)\right\rangle_{K,L}=\hat{h}_K(P_K(f))$,以及 $(f_1,f_2)_{R^\times}=\deg f$。

注意到

$$L'(E_K,1)=L(E,1)L'(E^{(-\ell)},1),$$

一个事实是 $L(E,1)\neq 0$。由定理 0.1, $E^{(-\ell)}(\mathbf{Q})$ 的秩是 1。假设 BSD 猜想是正确的,那么可以得到 $L'(E_K,1)\neq 0$,于是 $P_K(f)$ 是 $E(K)$ 中的非挠点。自然地提出如下问题。

问题 2.3　(不假设 BSD 猜想)如何证明 $P_K(f)$ 是 $E(K)$ 上的无限阶点?

志谢　感谢 Ashay Burungale 教授对论文的建议和指导。

参 考 文 献

[1] GROSS B, ZAGIER D. Heegner points and derivatives of *L*-series [J]. Inventiones Mathematicae, 1986, 84(2): 225-320.

[2] KOLYVAGIN V. Euler systems [J]. The Grothendieck Festschrift, 1990, 2: 435-483.

[3] RUBIN K. The "main conjectures" of Iwasawa theory for imaginary quadratic fields [J]. Inventiones Mathematicae, 1991, 103(1): 25-68.

[4] BURUNGALE A, TIAN Y. A rank zero p-converse to a theorem of Gross-Zagier, Kolyvagin and Rubin [EB/OL]. [2024-07-19]. https://arxiv.org/abs/2104.06732.

[5] SKINNER C, URBAN E. The Iwasawa main conjectures for GL_2 [J]. Inventiones Mathematicae, 2014, 195(1): 1-277.

[6] WAN X. Iwasawa main conjecture for supersingular elliptic curves and BSD conjecture [EB/OL]. [2024-07-19]. https://arxiv.org/abs/1411.6352.

[7] SKINNER C. A converse to a theorem of Gross, Zagier and Kolyvagin [J]. Annals of Mathematics, 2020, 191(2): 329-354.

[8] ZHANG W. Selmer groups and the indivisibility of Heegner points [J]. Cambridge Journal of Mathematics, 2014, 2(2): 191-253.

[9] BURUNGALE A, TIAN Y. p-converse to a theorem of Gross-Zagier, Kolyvagin and Rubin [J]. Inventiones Mathematicae, 2020, 220: 211-253.

[10] YU Q. *p*-converse to a theorem of Gross-Zagier, Kolyvagin, and Rubin for small primes [D]. Pasadena: California Institute of Technology, 2021.

[11] BIRCH B. Elliptic curves and modular functions [J]. Symposia mathematica, 1970, 4: 27-32.

[12] COATES J, LI Y, TIAN Y, et al. Quadratic twists of elliptic curves [J]. Proceedings of the London Mathematical Society, 2015, 110(2): 357-394.

[13] OUYANG Y, ZHANG S. Birch's lemma over global function fields [J]. Proceedings of the London Mathematical Society, 2017, 145: 577-584.

[14] TIAN Y. Congruent numbers and Heegner points [J]. Cambridge Journal of Mathematics, 2014, 2(1): 117-161.

[15] CAI L, CHEN Y, LIU Y. Heegner points on modular curves [J]. Transactions of the American Mathematical Society, 2018, 370(5): 3721-3743.

[16] YUAN X, ZHANG S, ZHANG W. The Gross-Zagier formula on Shimura curves [M]. Princeton: Princeton University Press, 2013.

[17] SILVERMAN J. The arithmetic of elliptic curves [M]. New York: Springer, 2009.

[18] SAITO H. On Tunnell's formula for characters of GL(2) [J]. Compositio Mathematica, 1993, 85(1): 99-108.

[19] TUNNELL J. Local ε-factors and characters of GL(2) [J]. American Journal of Mathematics, 1983, 105(6): 1277-1307.

[20] CAI L, SHU J, TIAN Y. Explicit Gross-Zagier and Waldspurger formulae [J]. Algebra & Number Theory, 2014, 8(10): 2523-2572.

(责任编辑:马田田)