

椭圆曲线有理点扭子群的明显分类

邱德荣

清华大学高等研究中心 北京 100084
E-mail: dqiu@math.tsinghua.edu.cn

张贤科

清华大学数学科学系 北京 100084
E-mail: xianke@tsinghua.edu.cn

摘 要 本文给出了有理数域 \mathbb{Q} 上椭圆曲线 E 按其偶数阶循环扭子群 $E_{\text{tors}}(\mathbb{Q})$ 的分类, 并给出了 $E_{\text{tors}}(\mathbb{Q})$ 的生成元. 这些结果, 连同新近 Ono 在 $E_{\text{tors}}(\mathbb{Q})$ 非循环情形的结果, 完全解决了 E 含 2 阶有理点时的分类和参数化问题.

关键词 椭圆曲线; 有理点; 扭群

MR(2000) 主题分类 11G05, 14H52, 14K05

中图分类 O156.2, O175.25

Explicit Classification for Torsion Subgroups of Rational Points of Elliptic Curves

De Rong QIU

Center for Advanced Study, Tsinghua University, Beijing 100084, P. R. China
E-mail: dqiu@math.tsinghua.edu.cn

Xian Ke ZHANG

Department of Mathematical Sciences, Tsinghua University, Beijing 100084, P. R. China
E-mail: xianke@tsinghua.edu.cn

Abstract We study the classification of elliptic curves E over the rationals \mathbb{Q} according to the torsion subgroups $E_{\text{tors}}(\mathbb{Q})$. More precisely, we classify those elliptic curves with $E_{\text{tors}}(\mathbb{Q})$ being cyclic with even orders. We also give explicit formulas for generators of $E_{\text{tors}}(\mathbb{Q})$. These results, together with the recent results of K. Ono for the non-cyclic $E_{\text{tors}}(\mathbb{Q})$, completely solve the problem of the explicit classification and parameterization when E has a rational point of order 2.

Keywords Elliptic curve; Rational point; Torsion group

MR(2000) Subject Classification 11G05, 14H52, 14K05

Chinese Library Classification O156.2, O175.25

* 本文翻译并压缩于本刊英文版 (2002)18 卷 3 期 539–548 页

收稿日期: 1999-07-29; 修改日期: 2001-03-09; 接受日期: 2001-07-20

基金项目: 国家自然科学基金资助项目 (19771052); 教育部优秀年轻教师基金资助课题

1 引言和主要结果

设 E 是定义在 \mathbb{Q} 上的椭圆曲线. 由 Mordell-Weil 定理, Mordell-Weil 群 $E(\mathbb{Q})$ 是一个有限生成 Abel 群

$$E(\mathbb{Q}) \cong E_{\text{tors}}(\mathbb{Q}) \times \mathbb{Z}^r,$$

其中 $E(\mathbb{Q})$ 是 E 的 \mathbb{Q} -有理点群, $E_{\text{tors}}(\mathbb{Q})$ 是 $E(\mathbb{Q})$ 的扭子群 (即 $E(\mathbb{Q})$ 的有限阶点集), \mathbb{Z} 是有理整数集.

1977 年, Mazur 在文 [1, 2] 中决定了 $E_{\text{tors}}(\mathbb{Q})$ 的所有类型, 即证明了 \mathbb{Q} 上椭圆曲线 E 的扭子群 $E_{\text{tors}}(\mathbb{Q})$ 必同构于如下 15 个群之一

$$\mathbb{Z}/m\mathbb{Z}, \quad 1 \leq m \leq 10 \text{ 或 } m = 12; \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, \quad 1 \leq n \leq 4,$$

且每一个这样的群必为某个 E 的扭子群 $E_{\text{tors}}(\mathbb{Q})$ (见文 [3], 223 页).

1996 年, Ono 按 Mazur 的扭子群结构类型给出了非循环情形下椭圆曲线的一个分类判则和参数化, 即证明了如下定理 (见文 [4]):

定理^[4] 设 $E: y^2 = x(x+M)(x+N)$ 为椭圆曲线, M 和 N 为有理整数, 则

(i) $E_{\text{tors}}(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ 当且仅当以下某一对数为完全平方

$$M, N; \quad -M, -M+N; \quad -N, -N+M.$$

(ii) $E_{\text{tors}}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ 当且仅当

$$(1) \quad M = d^2 u^4, \quad N = d^2 v^4; \text{ 或}$$

$$(2) \quad -M = d^2 u^4, \quad -M+N = d^2 v^4; \text{ 或}$$

$$(3) \quad -N = d^2 u^4, \quad -N+M = d^2 v^4$$

对某正整数 d, u, v, w 成立, 且 $u^2 + v^2 = w^2$, $(u, v, w) = 1$.

(iii) $E_{\text{tors}}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ 当且仅当 $M = (a^4 + 2a^3b)d^2$, $N = (b^4 + 2b^3a)d^2$, 且 $a/b \notin \{-2, -1/2, -1, 1, 0\}$ 对某互素的整数 a, b 和正整数 d 成立.

(iv) 其余情形: $E_{\text{tors}}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

本文将进一步考虑椭圆曲线按 Mazur 的扭子群结构类型的分类和参数化问题. 我们考虑 $E_{\text{tors}}(\mathbb{Q})$ 为偶数阶循环群的情形.

设 $E: y^2 = f(x)$ 为一椭圆曲线, $f(x) \in \mathbb{Q}[x]$. 记 $f(x)$ 的三个复根为 α, β, γ , 则 $P_1 = (\alpha, 0)$, $P_2 = (\beta, 0)$, $P_3 = (\gamma, 0)$ 恰为 E 的三个非平凡二阶点, 故 $E[2] = \{O, P_1, P_2, P_3\}$ 即为 E 的二阶点扭子群. 由 Mazur 定理知道, 扭子群 $E_{\text{tors}}(\mathbb{Q})$ 非循环当且仅当 $E_{\text{tors}}(\mathbb{Q}) \supset E[2]$, 即 $\alpha, \beta, \gamma \in \mathbb{Q}$. 由此可知 $E_{\text{tors}}(\mathbb{Q})$ 为循环群当且仅当 $f(x)$ 最多只有一个有理根. 故 $E_{\text{tors}}(\mathbb{Q})$ 是偶数阶循环群的充分必要条件为 E 恰有一个非平凡的二阶有理点, 即 $f(x)$ 恰有一个有理根. 我们以下即设如此. 在平移意义下, 可设 $f(x)$ 的此唯一有理根为 0, 故有 $f(x) = x(x-\alpha)(x-\beta)$.

因为 $\alpha+\beta$ 和 $\alpha\beta$ 均为有理数, 故可设 $\alpha = a+b\sqrt{D}$, $\beta = a-b\sqrt{D}$, 其中 $a, b \in \mathbb{Q}$, $b \neq 0$, D 为无平方因子整数. 还可进一步设 a, b 为有理整数且 $\gcd\{a, b\} = (a, b)$ 无平方因子. 事实上, 如果将 x, y 换为 $x/d^2, y/d^3$, 则 E 的方程 $E: y^2 = x(x-\alpha)(x-\beta)$ 化为 $E_d: y^2 = x(x-d^2\alpha)(x-d^2\beta)$. E 和 E_d 是 \mathbb{Q} -同构的, 故 $E(\mathbb{Q}) \cong E_d(\mathbb{Q})$, $E_{\text{tors}}(\mathbb{Q}) \cong E_{d\text{tors}}(\mathbb{Q})$.

本文的主要结果是:

定理 设 $E: y^2 = x(x+M)(x+N)$ 为一椭圆曲线, 其中 $M = m+n\sqrt{D}$, $N = m-n\sqrt{D}$, D 和 (m, n) 均为无平方因子整数, $D \neq 1$, $n \neq 0$ 和 m 均是有理整数, 则 E 的 \mathbb{Q} -有理点扭子群 $E_{\text{tors}}(\mathbb{Q})$ 分类如下

- (I) $E_{\text{tors}}(\mathbb{Q}) \supset \mathbb{Z}/4\mathbb{Z}$ 当且仅当 $m = a^2 + b^2D$, $n = 2ab$, 其中 $a, b \in \mathbb{Z}$ 为非零互素整数.
- (II) $E_{\text{tors}}(\mathbb{Q}) = \mathbb{Z}/8\mathbb{Z}$ 当且仅当 $m = u^4 + v^2w^2D$, $n = 2u^2vw$, $2u^2 - v^2 = w^2D$, 其中 $u, v, w \in \mathbb{Z}$ 为非零整数.
- (III) $E_{\text{tors}}(\mathbb{Q}) \supset \mathbb{Z}/6\mathbb{Z}$ 当且仅当 $m = a^2 + 2ac + b^2D$, $n = 2b(a+c)$, $a^2 - b^2D = c^2$, 其中 $a, b, c \in \mathbb{Z}$ 为非零互素整数.
- (IV) $E_{\text{tors}}(\mathbb{Q}) = \mathbb{Z}/12\mathbb{Z}$ 当且仅当 $m = v^2 - u^2 + w^2D$, $n = 2vw$, $3(v^2 - w^2D)^4 - 4u^2(v^2 - w^2D)^2(v^2 + w^2D) - 16u^4v^2w^2D = 0$, 其中 $u, v, w \in \mathbb{Z}$ 是非零整数.
- (V) $E_{\text{tors}}(\mathbb{Q}) = \mathbb{Z}/10\mathbb{Z}$ 当且仅当 $m = 2s(s+u) - v^2$, $n = 2st$, $(s+u)^2 - v^2 = t^2D$, $(u-v)^2(u+v) = 4uvs$, 其中 $u, v, s, t \in \mathbb{Z}$ 是非零整数.

(VI) 其余情形: $E_{\text{tors}}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$.

进一步, 设 P_n 是 n 阶循环群 $E_{\text{tors}}(\mathbb{Q})$ 的一个生成元, 则 P_n 和 $2P_n$ 的 x -坐标 $x(P_n)$ 和 $x(2P_n)$ 依上述各情形分别取值如下:

- (I) $x(P_4) = a^2 - b^2D$; $x(2P_4) = 0$.
- (II) $x(P_8) = (v \pm u)(v \mp u)^3$; $x(2P_8) = (u^2 - v^2)^2$.
- (III) $x(P_6) = 5c^2 + 4ac$; $x(2P_6) = c^2$.
- (IV) $x(P_{12}) = (u \pm v)^2 - w^2D$; $x(2P_{12}) = u^2$.
- (V) $x(P_{10}) = 2v^2 + 4vs - u^2$; $x(2P_{10}) = u^2$.
- (VI) $x(P_2) = 0$.

2 定理的证明

引理 1 设 $E: y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ 为数域 K 上椭圆曲线, $\alpha, \beta, \gamma \in K$. 设点 $(x_0, y_0) \in E(K)$, 则 $(x_0, y_0) = 2(x_1, y_1)$ 对某点 $(x_1, y_1) \in E(K)$ 成立当且仅当 $x_0 - \alpha$, $x_0 - \beta$ 和 $x_0 - \gamma$ 都是 K 中平方元 (见文 [5], 85 页).

定理的证明 根据 Lutz-Nagell 定理, 任意有理扭点 $P \in E_{\text{tors}}(\mathbb{Q})$ 都是整点, 即坐标 $x(P)$, $y(P) \in \mathbb{Z}$ (见文 [5]). 且我们有如下倍点坐标公式 (见文 [3]):

$$x(2P) = ((x(P)^2 - MN)/2y(P))^2.$$

(I) 设 $E_{\text{tors}}(\mathbb{Q}) \supset \mathbb{Z}/4\mathbb{Z}$, 则 E 包含一个四阶有理点 P , 且 $2P = (0, 0)$. 由引理 1 知, M 和 N 都是数域 $K = \mathbb{Q}(\sqrt{D})$ 中的平方元. 进一步分析易知, M 和 N 实际上都是环 $\mathbb{Z}[\sqrt{D}]$ 中的平方元, 即有 $M = (a + b\sqrt{D})^2$, $N = (a - b\sqrt{D})^2$, $a, b \in \mathbb{Z}$, 从而 $m = a^2 + b^2D$, $n = 2ab$. 又 (m, n) 不含平方因子, 且 $n \neq 0$, 故 $(a, b) = 1$, $ab \neq 0$.

反之, 如果 (I) 中关于 M 和 N 的条件成立, 则 M 和 N 都是 K 中平方元, 于是根据引理 1 可得 $(0, 0) = 2P$, 对某个点 $P \in E(K)$ 成立, 从而由上述倍点坐标公式得 $x(P)^2 - MN = 0$, 于是 $x(P)^2 = MN = (a^2 - b^2D)^2$, 故 $x(P) = \pm(a^2 - b^2D)$, 将此代入 E 的方程中, 由 Lutz-Nagell 定理可得 E 的两个整点 P :

$$x(P) = (a^2 - b^2D), \quad y(P) = \pm 2a(a^2 - b^2D).$$

(E 不含有限阶有理点 P , 其 x -坐标为 $x(P) = -(a^2 - b^2D)$). 这些点 P 即是 $E_{\text{tors}}(\mathbb{Q})$ 中的四阶非平凡点.

(II) 设 $E_{\text{tors}}(\mathbb{Q}) = \mathbb{Z}/8\mathbb{Z}$ 且 P 是 E 的一个 8 阶有理点, 则 $2P$ 即为 E 的 4 阶有理点, 于是由 (I) 知道 $m = a^2 + b^2D$, $n = 2ab$, 且 $x(2P) = a^2 - b^2D$. 从而由引理 1 可得 $x(2p) = a^2 - b^2D$, $x(2P) + M = 2a^2 + 2ab\sqrt{D}$, $x(2P) + N = 2a^2 - 2ab\sqrt{D}$ 都是域 K 中的平方元, 故由倍点坐标公式及 $x(P)$, $y(P)$, $x(2P)$, MN , a 和 b 都是有理整数这些事实, 可得

- (i) $a^2 - b^2D = c^2$;
- (ii) $2a^2 + 2ab\sqrt{D} = (s + t\sqrt{D})^2$, 其中 $c, s, t \in \mathbb{Z}$. 由此得到:
- (iii) $s^2 = a(a + c)$;
- (iv) $t^2D = a(a - c)$.

由于 $(a, b) = 1$ 且 D 不含平方因子, 故由 (i) 得 $(a, c) = 1$, 从而 $(a, a + c) = 1$, 于是根据 (iii) 可知 $a = u^2$, $a + c = v^2$, $u, v \in \mathbb{Z}$ 且 $(u, v) = 1$. 又由 (iv) 可得 $2u^2 - v^2 = w^2D$, $w \in \mathbb{Z}$. 再由 (i) 式我们即可得到 $b = vw$, 从而有 $m = u^4 + v^2w^2D$, $n = 2u^2vw$, $2u^2 - v^2 = w^2D$, $u, v, w \in \mathbb{Z}$ 且均非零.

反之, 设椭圆曲线 E 满足所给条件, 则 E 显然也满足情形 (I) 的条件, 这样 E 就包含一个 4 阶 \mathbb{Q} -有理点 P_4 且 $x(P_4) = (u^2 - v^2)^2$. 容易验证 P_4 的坐标满足引理 1 (对于数域 $K = \mathbb{Q}(\sqrt{D})$), 从而有 $P_4 = 2P$, 其中 $P \in E(K)$, 且显然 P 为 E 的 8 阶点. 于是由倍点坐标公式, 得 $x(2P) = x(P_4) = (u^2 - v^2)^2 = ((x^2 - MN)/2y)^2$, 即有 $4y^2(u^2 - v^2)^2 = (x^2 - MN)^2$ (这里 $x = x(P)$, $y = y(P)$).

将 m, n 的关系式代入上述方程及 E 的方程可得如下关于 x 的方程

$$x^4 - 4(u^2 - v^2)^2x^3 - 2(u^2 - v^2)^2(5u^4 + 6u^2v^2 - 3v^4)x^2 - 4(u^2 - v^2)^6x + (u^2 - v^2)^8 = 0,$$

即 $(x - (u^2 - v^2)^2)^4 = 16u^4(u^2 - v^2)^2x^2$.

由此可得它的有理整解为

$$x = (v \pm u)(v \mp u)^3.$$

将此 x 的值代入 E 的方程即可解出 y (显然为有理整数), 从而可得 E 的 8 阶 \mathbb{Q} -有理点 P_8 , 且 $x(P_8) = (v \pm u)(v \mp u)^3$. 这就证明了 (II).

(III) 设 $E(\mathbb{Q})_{\text{tors}} \supset \mathbb{Z}/6\mathbb{Z}$, 则 E 包含一个 3 阶 \mathbb{Q} -有理点 P . 显然 $x(2P) = x(P) \neq 0$, 于是由倍点坐标公式可得 $x(2P) = u^2 = x(P)$, $u \in \mathbb{Z}$. 根据三阶扭点的性质 (见文 [6], 40 页), 我们知道 $x = x(P)$ 必满足

$$3x^4 + 4(M + N)x^3 + 6MNx^2 - M^2N^2 = 0.$$

这是一个关于变量 M, N 和 x 的四次齐次多项式方程, 可用 Nigel Boston 参数变换 (见文 [4], 109 页): $M/x = (1 + t)^2 - 1$, $N/x = (1 + 1/t)^2 - 1$, 其中 t 为参数. 仔细分析可知 $t \in \mathbb{Q}(\sqrt{D}) - \mathbb{Q}$. 设 $t = (a + b\sqrt{D})/c$, $(a, b, c) = 1$, $bc \neq 0$, $a, b, c \in \mathbb{Z}$. 将 $t, M/x, N/x$ 代入 E 的方程, 可得

$$(2 + a/c + ac/(a^2 - b^2D))(b/c - bc/(a^2 - b^2D)) = 0.$$

如果 $2 + a/c + ac/(a^2 - b^2D) = 0$, 则

$$2 + t + 1/t = (b/c - bc/(a^2 - b^2D))\sqrt{D}.$$

将此代入 E 的方程, 得

$$(y/x)^2/x = (b/c - bc/(a^2 - b^2D))^2 D.$$

这是不可能的 (因为 $x = u^2$ 且 D 不含平方因子), 故必有 $b/c - bc/(a^2 - b^2D) = 0$. 由此即得 $a^2 - b^2D = c^2$ (因为 $b \neq 0$), 故 $1/t = (a - b\sqrt{D})/c$, 从而得

$$m = x(a^2 + 2ac + b^2D)/c^2, \quad n = 2xb(a + c)/c^2.$$

容易验证 $(a^2 + 2ac + b^2D, 2b(a + c), c^2)$ 无平方因子. 由此即可推出 $x = c^2$, 因此

$$m = a^2 + 2ac + b^2D, \quad n = 2b(a + c), \quad a^2 - b^2D = c^2.$$

反之, 设椭圆曲线 E 满足 (III) 中所给条件, 则易得到 E 的一个三阶 \mathbb{Q} -有理点 P_3 , 且 $x(P_3) = c^2, |y(P_3)| = 2|a + c|c^2$.

实际上, 在此条件下, E 的每个三阶 \mathbb{Q} -有理点 P_3 均满足 $x(P_3) = c^2$. 于是 $P_3 + P_0 = P_6$ 即是 E 的一个非平凡六阶 \mathbb{Q} -有理点, 其中 $P_0 = (0, 0)$ 是二阶点. 进一步根据椭圆曲线加法坐标计算公式^[3] 可得 $x(P_6) = 5c^2 + 4ac$. 这就证明了 (III).

(IV) 设 $E_{\text{tors}}(\mathbb{Q}) = \mathbb{Z}/12\mathbb{Z}$, 则 E 包含一个阶为 12 的 \mathbb{Q} -有理点 P . 于是 $2P$ 是六阶有理点. 类似于前述用 (I) 的结果证明 (II) 的方法, 我们运用 (III) 的结果可得

$$m = v^2 - u^2 + w^2D, \quad n = 2vw;$$

且有

$$(4.1) \quad b(a + c) = vw;$$

$$(4.2) \quad 5c^2 + 4ac = u^2;$$

$$(4.3) \quad a^2 - b^2D = c^2;$$

$$(4.4) \quad 4c(a + c) + (a + c)^2 + b^2D = v^2 + w^2D,$$

其中 a, b, c 如 (III) 所述, 且 $u, v, w \in \mathbb{Z}$ 均为非零整数.

根据这些公式, 经过极为繁杂的计算, 即得到如下等式

$$3(v^2 - w^2D)^4 - 4u^2(v^2 - w^2D)^2(v^2 + w^2D) - 16u^4v^2w^2D = 0.$$

反之, 设椭圆曲线 E 满足 (IV) 中所给条件, 则经仔细分析可验证 E 满足 (III) 中条件, 从而 E 含有一个六阶 \mathbb{Q} -有理点 P_6 , 且 $x(P_6) = 5c^2 + 4ac = u^2$. 进一步易验证 P_6 满足引理 1 的条件, 从而 $P_6 = 2P$, 对某个点 $P \in E(K), K = \mathbb{Q}(\sqrt{D})$, 于是 P 是 12 阶点, 根据倍点坐标公式, E 的方程及所给条件, 可得 $x = x(P)$ 的如下方程

$$x^4 - 4u^2x^3 - hx^2 - 4u^2ex + e^2 = 0,$$

其中

$$h = 2((v^2 - w^2D)^2 + 2u^2(v^2 + w^2D) - 3u^4), \quad e = (v^2 - w^2D)^2 + u^4 - 2u^2(v^2 + w^2D).$$

经计算, 并结合 E 所满足的条件, 上述方程可化为

$$((x - u^2)^2 - (2u^2(v^2 + w^2D) - (v^2 - w^2D)^2))^2 = 4(v^2 - w^2D)^2x^2.$$

这样, 就有

$$(x - u^2)^2 - (2u^2(v^2 + w^2D) - (v^2 - w^2D)^2) = 2(v^2 - w^2D)x$$

或

$$(x - u^2)^2 - (2u^2(v^2 + w^2D) - (v^2 - w^2D)^2) = -2(v^2 - w^2D)x.$$

注意到 D 无平方因子, 从而可得整解 $x = (u \pm v)^2 - w^2D$. 由此可得 $y = y(P) \in \mathbb{Z}$. 因此 E 含有 12 阶非平凡 \mathbb{Q} -有理点 P_{12} , 且 $x(P_{12}) = (u \pm v)^2 - w^2D$. (IV) 得证.

(V) 设 $E_{\text{tors}}(\mathbb{Q}) = \mathbb{Z}/10\mathbb{Z}$, 且 P 是 E 的一个非平凡 5 阶 \mathbb{Q} -有理点, 易知 $x(4P) = x(P)$ 且 $x(2P) \neq x(P)$, 由倍点坐标公式, 得

$$x(2P) = \left(\frac{x(P)^2 - MN}{2y(P)} \right)^2, \quad x(P) = x(4P) = \left(\frac{x(2P)^2 - MN}{2y(2P)} \right)^2.$$

于是由 Lutz-Nagell 定理, 可得 $x(P) = u^2$, $x(2P) = v^2$, $u, v \in \mathbb{Z}$ 均非零, 且 $u^2 \neq v^2$, 代入上述公式, 得

$$[v^4 - (m^2 - n^2D)]^2 = 4u^2v^2(v^4 + 2mv^2 + m^2 - n^2D).$$

由此可得

$$(v^2 + m)^2 - n^2D = c^2, \quad v^4 - (m^2 - n^2D) = 2uvc,$$

$c \in \mathbb{Z}$, 且 $2v|c$. 于是 $c = 2vs$, $s \in \mathbb{Z}$, 代入上述两个等式中, 即可得出

$$m = 2s(s + u) - v^2, \quad n = 2st, \quad (s + u)^2 - v^2 = t^2D.$$

再代入 E 的方程中, 即可得 $(u - v)^2(u + v) = 4uvs$, 或 $(u + v)^2(u - v) = -4uvs$. 适当选取 u, v 的符号, 即得 $(u - v)^2(u + v) = 4uvs$.

反之, 设 E 满足 (V) 中条件, 则由该条件容易得到 E 的一个 5 阶非平凡 \mathbb{Q} -有理点 P_5 , 且

$$x(P_5) = u^2, \quad |y(P_5)| = |u(u^2 - v^2 + 2us)|.$$

于是 $P_{10} = P_0 + P_5$ 即是 E 的一个非平凡 10 阶 \mathbb{Q} -有理点, 且由椭圆曲线加法坐标计算公式^[3], 可得

$$x(P_{10}) = 2v^2 + 4vs - u^2.$$

(V) 得证. 这就完成了定理的证明.

参 考 文 献

- [1] Mazur B., Modular curves and the Eisenstein ideal, *IHES Publ. Math.*, 1977, **47**: 33–186.
- [2] Mazur B., Rational points on modular curves, *Modular functions of one Variable V.*, *Lecture Notes in Math.*, New York: Springer-Verlag, 1977, **601**: 107–148.
- [3] Silverman J., *The arithmetic of elliptic curves*, New York: Springer-Verlag, 1986.
- [4] Ono K., Euler's concordant forms, *Acta Arithmetica*, 1996, **LXX VIII**(2): 101–123.
- [5] Knapp A., *Elliptic curves*, Princeton: Princeton Univ. Press, 1992.
- [6] Silverman J., Tate J., *Rational points on elliptic curves*, New York: Springer-Verlag, 1992.