ACTA ARITHMETICA
LXXVIII.3 (1997)

Computation of the Selmer groups of certain parametrized elliptic curves

by

S. Schmitt (Saarbrücken)

In their article [S-T], Roel J. Stroeker and Jaap Top considered elliptic curves over $\mathbb{Q}$ defined by the equation

$$E_p: \quad y^2 = (x+p)(x^2+p^2),$$

where $p \in \mathbb{P}$ is a prime number. They determined the Selmer groups corresponding to certain 2-isogenies and the sign of the functional equation of these curves. Moreover, they gave a method for computing the Mordell–Weil group $E_p(\mathbb{Q})$ in some cases.

The aim of this note is to generalize their method to curves over $\mathbb{Q}$ defined by the equation

$$E_z: \quad y^2 = (x+z)(x^2+z^2)$$

with arbitrary $z \in \mathbb{Q}^*$. Whereas the methods are analogous to those of R. J. Stroeker and J. Top, the results obtained here are quite different. We shall develop an algorithm for computing the Selmer groups corresponding to 2-isogenies of these curves. This algorithm is based on four theorems, which constitute the main results of Section 2 and describe the Selmer groups of these curves. We also generalize the procedure for finding generators of the Mordell–Weil groups of these curves. This procedure terminates if the Tate–Shafarevich groups are trivial, which is certainly not so in general. Stroeker and Top were able to prove that the Tate–Shafarevich group is nontrivial in a special case of a prime $k = p \equiv 9 \bmod 16$ and $\left(\frac{1+\sqrt{-1}}{p}\right) = 1$ (see [S-T]), but I could not generalize their method.

I wish to thank Professor H. G. Zimmer for suggesting this topic to me and for his advice, especially for his hint on the structure of the torsion groups.

1. On the curves $E_z: y^2 = (x+z)(x^2+z^2)$. We start with an elliptic curve

$$E_z: \quad y^2 = (x+z)(x^2+z^2)$$

with $z \in \mathbb{Q}$. If $z = 0$, then the given curve E_0 is singular, so we shall assume that $z \in \mathbb{Q}^*$.

The transformation $x = x' - z$, $y = y'$ yields another model, isomorphic to E_z over $\mathbb{Q}$:

$$E'_z: \quad y'^2 = x'^3 - 2zx'^2 + 2z^2x'.$$

The discriminant of this curve is $\Delta_z = -2^8 z^6 \neq 0$, $z \in \mathbb{Q}^*$.

For $z_1 \neq z_2$, both from $\mathbb{Q}^*$, E_{z_1} and E_{z_2} are isomorphic over $\mathbb{Q}(\sqrt{z_2/z_1})$. That means that these curves are twists of each other. Therefore, I can confine myself to considering a smaller class of elliptic curves, namely those E_z with squarefree z.

It is therefore sufficient to consider elliptic curves of the form

$$E_k: \quad y^2 = x^3 - 2kx^2 + 2k^2x \tag{1}$$

with $k = \pm p_1 \dots p_\kappa$, where $p_i \in \mathbb{P}$ are distinct primes and $\kappa \in \mathbb{N}_0$. For $\kappa = 0$, we have $k = \pm 1$.

The curves E_k have the discriminant $\Delta_k = -2^8 k^6$ and the Tate value $c_{k,4} = -32k^2$.

For $k = \pm p_1 \dots p_\kappa$, we conclude that (see [Ta])

$$E_k \quad \text{has} \quad \begin{cases} \text{good reduction } (\mathrm{mod}\ l) & \text{for } l \in \mathbb{P},\ l \notin \{2, p_1, \dots, p_\kappa\}, \\ \text{additive reduction } (\mathrm{mod}\ l) & \text{for } l \in \{2, p_1, \dots, p_\kappa\}. \end{cases}$$

All curves E_k contain the point $P = (0,0)$ in $E_k(\mathbb{Q})$ as a torsion point of order 2. $E_k(\mathbb{Q})$ has no other points of order 2, because otherwise the equation $x^2 - 2kx + 2k^2 = 0$ would have a solution in $\mathbb{Q}$. Furthermore, $E_k(\mathbb{Q})$ has no point of order 4, a fact which follows from the duplication formula applied to $P = (0,0)$.

For the exact determination of the torsion group of $E_k/\mathbb{Q}$, we use the reduction theorem in [Fo, II, §2, p. 44], for the number field $\mathbb{Q}$:

THEOREM 1.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ by a p-minimal Weierstrass equation for a given prime $p \in \mathbb{P}$. Then the order of the torsion group of $E/\mathbb{Q}$ satisfies the following divisibility relation*:

1. *If E has good reduction* $\bmod p$, *then*

$$|E_{\mathrm{tor}}(\mathbb{Q})| \,\big|\, |\widetilde{E}(\mathbb{Z}/p\mathbb{Z})| \cdot p^{2t}.$$

2. *If E has additive reduction* $\bmod p$, *then*

$$|E_{\mathrm{tor}}(\mathbb{Q})| \,\big|\, |E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)| \cdot p^{2+2t}.$$

Here

$$t = \begin{cases} 0 & \text{for } p > 2, \\ 1 & \text{for } p = 2, \end{cases}$$

$\widetilde{E}$ is the reduction of E mod p and $E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \widetilde{P} \in \widetilde{E}(\mathbb{Z}/p\mathbb{Z})$ is nonsingular$\}$.

We use this general theorem, because we neither know the number of prime factors of k nor the primes dividing k. As these are the primes where k has additive reduction, we have to apply the divisibility relation for additive reduction modulo p. By this theorem, applied to the primes 3 and 5, we conclude that the torsion group of $E_k/\mathbb{Q}$ is

$$E_{k,\mathrm{tors}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.$$

Therefore, the Mordell–Weil group of the curve E_k is

$$E_k(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^r,$$

with $r = \mathrm{rk}(E_k(\mathbb{Q}))$ the rank of E_k over $\mathbb{Q}$.

The global L-series of $E_k/\mathbb{Q}$ is

$$L(s, E_k|\mathbb{Q}) = \prod_{l \in \mathbb{P}\setminus\{2,p_1,\ldots,p_\kappa\}} \frac{1}{1 + (A_l - (l+1))l^{-s} + l^{1-2s}},$$

where $A_l = \sharp\widetilde{E}_k(\mathbb{Z}/l\mathbb{Z})$ denotes the number of points on the reduced elliptic curve $\widetilde{E}_k$ of $E_k \pmod{l}$.

The conductor of these curves is given in the following proposition.

Proposition 1.1. *For $k = \pm 2^\alpha p_1 \ldots p_\kappa$ with $\alpha \in \{0,1\}$ and $p_i \in \mathbb{P}\setminus\{2\}$, $i = 1, \ldots, \kappa$, $\kappa \in \mathbb{N}_0$, the conductor of $E_k/\mathbb{Q}$ is*

$$N_k = 2^7 p_1^2 \ldots p_\kappa^2.$$

Specifically, for $\kappa = 0$ and hence $k = \pm 2^\alpha$, one has $N_k = 2^7$.

With [MF IV] one has the following theorem:

Theorem 1.2. *Let $k = vp_1 \ldots p_\kappa$ with $v \in \{\pm 1, \pm 2\}$ and $p_1, \ldots, p_\kappa \in \mathbb{P}\setminus\{2\}$, $\kappa > 0$ and put*

$$w = \pm v \quad \text{according as} \quad p_1 \ldots p_\kappa \equiv \pm 1 \pmod 4.$$

For $n \in \mathbb{Z}$, define the character

$$\chi = \chi_{p_1 \ldots p_\kappa}(n) := \left(\frac{n}{p_1 \ldots p_\kappa}\right)$$

by the Jacobi symbol with $\chi(n) = 0$ if $\gcd(n, p_1 \ldots p_\kappa) > 1$. Then

$$L(s, E_k|\mathbb{Q}) = L_\chi(s, E_w|\mathbb{Q}),$$

where $L_\chi(s, E_w|\mathbb{Q})$ is the L-series of $E_w/\mathbb{Q}$ twisted by χ.

For $k = \pm 1, \pm 2$, E_k has conductor $N_k = 2^7$. Ogg [Og] determined all elliptic curves over $\mathbb{Q}$ with 2-power conductor. Honda and Miyawaki [H-M] gave a complete table of all modular forms of weight 2 for $\Gamma_0(N)$ with N

a power of 2. From these results, it follows that the 4 curves E_1, E_{-1}, E_2, E_{-2} are modular.

The above relation between the L-series of the curves E_k implies the following fact proved by induction on the number of different prime factors in k on the basis of Proposition 17 in [Ko], p. 127.

PROPOSITION 1.2. *All curves E_k are modular.*

The global L-series of E_k (for every integer k) is known to satisfy the functional equation (cf. [B-S])

$$\left(\frac{\sqrt{N_k}}{2\pi}\right)^s \Gamma(s)L(s,E_k|\mathbb{Q}) = \varepsilon_k\left(\frac{\sqrt{N_k}}{2\pi}\right)^{2-s} \Gamma(2-s)L(2-s,E_k|\mathbb{Q}),$$

where Γ is the usual Gamma function and $\varepsilon_k \in \{\pm 1\}$.

Table 1 from [MF IV] lists elliptic curves over $\mathbb{Q}$ with conductor $128 = 2^7$. The curves $E_{\pm 1}$ and $E_{\pm 2}$ are isomorphic to the following curves in [MF IV]:

$$E_{-1} \cong 128A, \quad E_1 \cong 128C,$$
$$E_{-2} \cong 128F, \quad E_2 \cong 128G.$$

Then with [B-S], one establishes the following theorem:

THEOREM 1.3. *For $k = vp_1 \dots p_\kappa$ with $v \in \{\pm 1, \pm 2\}$ and $p_i \in \mathbb{P}\backslash\{2\}$, the sign of the functional equation of E_k is*:

$p_1 \dots p_\kappa \pmod 8$	$\varepsilon_{p_1 \dots p_\kappa}$	$\varepsilon_{-p_1 \dots p_\kappa}$	$\varepsilon_{2p_1 \dots p_\kappa}$	$\varepsilon_{-2p_1 \dots p_\kappa}$
1	-1	1	1	1
3	1	-1	1	1
5	1	-1	-1	-1
7	-1	1	-1	-1

The conjecture of Birch and Swinnerton-Dyer implies that ε_k is related to the rank r of E_k over $\mathbb{Q}$ by $\varepsilon_k = (-1)^r$. Hence, by this conjecture, one can find the parity of the rank of E_k.

2. Selmer groups corresponding to 2-isogenies

2.1. *Basic facts.* A procedure for finding the rank of an elliptic curve over $\mathbb{Q}$ with a torsion point of order 2 was developed by Tate (see [Si-Ta] or [S-T]). It is based on the classical Selmer– and Tate–Shafarevich groups. I shall apply this procedure to the curves E_k.

For the elliptic curve over $\mathbb{Q}$

$$E_k: \quad y^2 = x^3 - 2kx^2 + 2k^2x, \tag{2}$$

with $k = \pm p_1 \dots p_\kappa$ as above and its 2-isogenous curve

$$E'_k: \quad Y^2 = X^3 + 4kX^2 - 4k^2X. \tag{3}$$

I denote by ψ the corresponding 2-isogeny and by ψ' its dual isogeny:

$$\psi : E_k \to E'_k, \qquad (x,y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(2k^2-x^2)}{x^2}\right),$$

and

$$\psi' : E'_k \to E_k, \qquad (X,Y) \mapsto \left(\frac{Y^2}{4X^2}, \frac{Y(-4k^2-X^2)}{8X^2}\right).$$

The Selmer groups corresponding to the 2-isogenies ψ' and ψ of these curves are

$$\begin{aligned} S_k[\psi'] = \{1\cdot\mathbb{Q}^{*2}, 2\cdot\mathbb{Q}^{*2}\} \\ \cup \Big\{ d\cdot\mathbb{Q}^{*2} : d \,|\, 2k^2, n^2 = dm^4 - 2km^2e^2 + \frac{2k^2}{d}e^4 \text{ has solutions} \\ n,m \neq 0, e \neq 0 \text{ in } \mathbb{R} \text{ and (mutually prime) solutions in } \mathbb{Z}_p \\ \text{for all } p \in \mathbb{P} \Big\} \end{aligned}$$

and

$$\begin{aligned} S_k[\psi] = \{\pm 1\cdot\mathbb{Q}^{*2}\} \\ \cup \Big\{ d\cdot\mathbb{Q}^{*2} : d \,|\, -4k^2, n^2 = dm^4 + 4km^2e^2 - \frac{4k^2}{d}e^4 \text{ has solutions} \\ n,m \neq 0, e \neq 0 \text{ in } \mathbb{R} \text{ and (mutually prime) solutions in } \mathbb{Z}_p \\ \text{for all } p \in \mathbb{P} \Big\}. \end{aligned}$$

One has a map $\delta : E_k(\mathbb{Q}) \to S_k[\psi']$ with

$$\begin{aligned} \mathcal{O} \mapsto 1\cdot\mathbb{Q}^{*2}, \qquad (0,0) \mapsto 2k^2\cdot\mathbb{Q}^{*2} = 2\cdot\mathbb{Q}^{*2}, \\ (x,y) \mapsto x\cdot\mathbb{Q}^{*2} \qquad \text{for } (x,y) \notin \{\mathcal{O},(0,0)\} \end{aligned}$$

with

$$\operatorname{Ker}\delta = \psi' E'_k(\mathbb{Q}).$$

In an analogous way one can treat the isogenous curve E'_k. The cokernels of the following left hand side injections are called the *Tate–Shafarevich groups* $Ш_k[\psi']$ of E_k resp. $Ш_k[\psi]$ of E'_k:

$$\begin{aligned} 0 \to E_k(\mathbb{Q})/\psi' E'_k(\mathbb{Q}) \to S_k[\psi'] \to Ш_k[\psi'] \to 0, \\ 0 \to E'_k(\mathbb{Q})/\psi E_k(\mathbb{Q}) \to S_k[\psi] \to Ш_k[\psi] \to 0. \end{aligned}$$

For the rank of the elliptic curves one obtains the formula

$$\begin{aligned}(4)\qquad \operatorname{rk}(E_k'(\mathbb{Q})) &= \operatorname{rk}(E_k(\mathbb{Q}))\\ &= \dim_{\mathbb{F}_2}(S_k[\psi']) - \dim_{\mathbb{F}_2}(Ш_k[\psi'])\\ &\quad + \dim_{\mathbb{F}_2}(S_k[\psi]) - \dim_{\mathbb{F}_2}(Ш_k[\psi]) - 2.\end{aligned}$$

For the primes p not dividing the discriminants $\Delta_k' = 2^{13}k^6$ of E_k' resp. $\Delta_k = -2^8k^6$ of E_k, the corresponding equations

$$n^2 = dm^4 - 2km^2e^2 + \frac{2k^2}{d}e^4$$

resp.

$$n^2 = dm^4 + 4km^2e^2 - \frac{4k^2}{d}e^4$$

define curves of genus 1 over $\mathbb{F}_p$. By the Hasse theorem, which estimates the number of points of elliptic curves over finite fields, these curves have a $\mathbb{F}_p$-rational point for $p > 3$. For $p = 3$, one sees by straightforward calculation that these curves have a $\mathbb{F}_3$-rational point. By Hensel's lemma (see e.g. [We]), these points can be lifted to solutions of the above equations in $\mathbb{Z}_p$.

For computing the Selmer groups, it suffices therefore to consider the primes $2, p_1, \ldots, p_\kappa$ and ∞.

For $d < 0$, the equation corresponding to the group $S_k[\psi']$ has no solution in $\mathbb{R}$. It follows that $d \cdot \mathbb{Q}^{*2}$ is not in $S_k[\psi']$ for negative d. For $d > 0$, the equation corresponding to $S_k[\psi']$ is solvable in $\mathbb{R}$, and the same is true in this case for the equations corresponding to $S_k[\psi]$.

Hence it remains to look for solutions in $\mathbb{Z}_p$ for the primes $p = 2$, $p_1, \ldots, p_\kappa$ only.

Obviously, $\{1 \cdot \mathbb{Q}^{*2}, 2 \cdot \mathbb{Q}^{*2}\}$ resp. $\{\pm 1 \cdot \mathbb{Q}^{*2}\}$ always lie in $S_k[\psi']$ resp. $S_k[\psi]$. From this observation it follows that

$$\begin{aligned}(5)\qquad \{1 \cdot \mathbb{Q}^{*2}, 2 \cdot \mathbb{Q}^{*2}\} \subset S_k[\psi'] \subset \{1 \cdot \mathbb{Q}^{*2}, 2 \cdot \mathbb{Q}^{*2}\}\\ \cup \{p_{i_1} \ldots p_{i_l} \cdot \mathbb{Q}^{*2}, 2p_{i_1} \ldots p_{i_l} \cdot \mathbb{Q}^{*2} :\\ 1 \le l \le \kappa,\ 1 \le i_1 < \ldots < i_l \le \kappa\}\end{aligned}$$

and

$$\begin{aligned}(6)\qquad \{\pm 1 \cdot \mathbb{Q}^{*2}\} \subset S_k[\psi] \subset \{\pm 1 \cdot \mathbb{Q}^{*2}, \pm 2 \cdot \mathbb{Q}^{*2}\}\\ \cup \{\pm p_{i_1} \ldots p_{i_l} \cdot \mathbb{Q}^{*2}, \pm 2p_{i_1} \ldots p_{i_l} \cdot \mathbb{Q}^{*2} :\\ 1 \le l \le \kappa,\ 1 \le i_1 < \ldots < i_l \le \kappa\}.\end{aligned}$$

In order to decide for a number $d \in \mathbb{Q}^*$, whether or not $d \cdot \mathbb{Q}^{*2}$ is in $S_k[\psi']$ resp. $S_k[\psi]$, I shall first assume that d is a squarefree integer and then I shall test the numbers da^2 with $a \in \mathbb{Z}\backslash\{0\}$ such that $da^2 \mid 2k^2$ resp. $da^2 \mid -4k^2$.

In determining the Selmer groups, I need some special Legendre symbols. In this subsection, p is always a prime different from 2. I shall consider the three cases $p \equiv 1 \pmod 8$, $p \equiv 5 \pmod 8$ and $p \equiv 7 \pmod 8$.

If $p \equiv 1 \pmod 8$, then the elements $(1 \pm \sqrt{-1}), (-1 \pm \sqrt{-1}), (1 \pm \sqrt{2})$ and $(-1 \pm \sqrt{2})$ define residue classes $\bmod p$. We have the following relations:

$$\left(\frac{1+\sqrt{-1}}{p}\right) = \left(\frac{1-\sqrt{-1}}{p}\right) = \left(\frac{-1+\sqrt{-1}}{p}\right) = \left(\frac{-1-\sqrt{-1}}{p}\right) \tag{7}$$

and

$$\left(\frac{1+\sqrt{2}}{p}\right) = \left(\frac{1-\sqrt{2}}{p}\right) = \left(\frac{-1+\sqrt{2}}{p}\right) = \left(\frac{-1-\sqrt{2}}{p}\right). \tag{8}$$

Let $w \in \mathbb{Z}$ denote a primitive root modulo p. Since $p \equiv 1 \pmod 8$, the relation

$$w^{(p-1)/8} \equiv \sqrt[4]{-1} \pmod p,$$

defines some 4th root $\sqrt[4]{-1} \bmod p$. From the identity

$$[\sqrt{2}(1+\sqrt{-1})]^2 = 2(2\sqrt{-1}) = 4\sqrt{-1}$$

we now derive the equation

$$\sqrt{2}(1+\sqrt{-1}) = \pm 2\sqrt[4]{-1}.$$

Hence we have

$$\begin{aligned}\left(\frac{1+\sqrt{-1}}{p}\right)\left(\frac{1+\sqrt{2}}{p}\right) &= \left(\frac{1+\sqrt{2}(1+\sqrt{-1})+\sqrt{-1}}{p}\right)\\ &= \left(\frac{(1 \pm \sqrt[4]{-1})^2}{p}\right) = 1,\end{aligned}$$

and conclude that

$$\left(\frac{1+\sqrt{-1}}{p}\right) = \left(\frac{1+\sqrt{2}}{p}\right).$$

For computing these Legendre symbols, it thus suffices to determine the value of one of them, e.g. of $\left(\frac{1+\sqrt{-1}}{p}\right)$. We remark that because of the relations (7) and (8) it does not matter which root of -1 or $2 \bmod p$ is used to compute the symbols.

The remaining cases $p \equiv 5 \pmod 8$ and $p \equiv 7 \pmod 8$ lead to different results:

For $p \equiv 5 \pmod 8$, the values $1 \pm \sqrt{-1}$ and $-1 \pm \sqrt{-1}$ define residue classes $\bmod p$. We obtain the relations

$$\left(\frac{1+\sqrt{-1}}{p}\right) = -\left(\frac{1-\sqrt{-1}}{p}\right), \qquad \left(\frac{-1+\sqrt{-1}}{p}\right) = -\left(\frac{-1-\sqrt{-1}}{p}\right).$$

Therefore, one of the symbols in each equality attains the value 1. Hence for determining the Selmer groups, it does not matter which sign of the roots $\pm\sqrt{-1} \bmod p$ is chosen so that, by a suitable choice of the sign, one can always ensure that $\left(\frac{1+\sqrt{-1}}{p}\right) = 1$, say.

For $p \equiv 7 \pmod 8$ one derives similar results. Here the values $1 \pm \sqrt{2}$ and $-1 \pm \sqrt{2}$ define residue classes $\bmod p$, and we obtain the relations

$$\left(\frac{1+\sqrt{2}}{p}\right) = -\left(\frac{1-\sqrt{2}}{p}\right), \qquad \left(\frac{-1+\sqrt{2}}{p}\right) = -\left(\frac{-1-\sqrt{2}}{p}\right).$$

As in the case $p \equiv 5 \pmod 8$, I can take one of $\pm\sqrt{2} \bmod p$ to ensure that $\left(\frac{1+\sqrt{2}}{p}\right) = 1$, say.

2.2. *Determination of the Selmer groups.* For determining the Selmer groups for general k, I distinguish the two cases $k = \pm 2p_1 \dots p_\kappa$ and $k = \pm p_1 \dots p_\kappa$ for distinct primes $p_1, \dots, p_\kappa \in \mathbb{P}\backslash\{2\}$ and $\kappa \in \mathbb{N}_0$. Here $\kappa = 0$ means that $k = \pm 2$ or ± 1, respectively.

For the sake of simplicity, I introduce the following notation. For fixed $p_{i_1}, \dots, p_{i_l}$ with $1 \le l \le \kappa$, $1 \le i_1 < \dots < i_l \le \kappa$ we put

$$p_1 \widetilde{\dots} p_\kappa := \frac{p_1 \dots p_\kappa}{p_{i_1} \dots p_{i_l}}.$$

Here we have $p_1 \widetilde{\dots} p_\kappa = 1$ if $p_{i_1} \dots p_{i_l} = p_1 \dots p_\kappa$ or if $\kappa = 0$.

The main theorems are the following:

THEOREM 2.1. *For $k = \pm 2p_1 \dots p_\kappa$ with primes $p_1, \dots, p_\kappa \in \mathbb{P}\backslash\{2\}$,*

$$\begin{aligned} S_k[\psi'] = {} & \{1 \cdot \mathbb{Q}^{*2}, 2 \cdot \mathbb{Q}^{*2}\} \\ & \cup \Bigg\{ p_{i_1} \dots p_{i_l} \cdot \mathbb{Q}^{*2}, 2p_{i_1} \dots p_{i_l} \cdot \mathbb{Q}^{*2} : 1 \le l \le \kappa,\ 1 \le i_1 < \dots < i_l \le \kappa, \\ & \quad \forall i \in \{i_1, \dots, i_l\} : p_i \equiv 1, 5 \pmod 8 \\ & \quad \wedge \left[\forall i \in \{i_1, \dots, i_l\} : p_i \equiv 1 \pmod 8 \Rightarrow \left(\frac{p_1 \widetilde{\dots} p_\kappa (1+\sqrt{-1})}{p_i} \right) = 1 \right] \\ & \quad \wedge \left[\forall j \notin \{i_1, \dots, i_l\} : \left(\frac{p_{i_1} \dots p_{i_l}}{p_j} \right) = 1 \vee \left(\frac{2p_{i_1} \dots p_{i_l}}{p_j} \right) = 1 \right] \Bigg\}. \end{aligned}$$

Its $\mathbb{F}_2$-dimension satisfies $\dim_{\mathbb{F}_2} S_k[\psi'] \le \kappa + 1$.

THEOREM 2.2. *For $k = \pm 2p_1 \dots p_\kappa$ with primes $p_1, \dots, p_\kappa \in \mathbb{P}\backslash\{2\}$,*

$$\begin{aligned} S_k[\psi] = {} & \{\pm 1 \cdot \mathbb{Q}^{*2}\} \\ & \cup \Bigg\{ \pm p_{i_1} \dots p_{i_l} \cdot \mathbb{Q}^{*2} : 1 \le l \le \kappa,\ 1 \le i_1 < \dots < i_l \le \kappa, \\ & \quad \forall i \in \{i_1, \dots, i_l\} : p_i \equiv 1, 7 \pmod 8 \\ & \quad \wedge \left[\forall i \in \{i_1, \dots, i_l\} : p_i \equiv 1 \pmod 8 \Rightarrow \left(\frac{p_1 \widetilde{\dots} p_\kappa (1+\sqrt{-1})}{p_i} \right) = 1 \right] \\ & \quad \wedge \left[\forall j \notin \{i_1, \dots, i_l\} : \left(\frac{p_{i_1} \dots p_{i_l}}{p_j} \right) = 1 \vee \left(\frac{-p_{i_1} \dots p_{i_l}}{p_j} \right) = 1 \right] \Bigg\}. \end{aligned}$$

Its $\mathbb{F}_2$-dimension satisfies $\dim_{\mathbb{F}_2} S_k[\psi] \le \kappa + 1$.

THEOREM 2.3. *For $k = \pm p_1 \dots p_\kappa$ with primes $p_1, \dots, p_\kappa \in \mathbb{P}\backslash\{2\}$,*
$S_k[\psi'] = \{1 \cdot \mathbb{Q}^{*2}, 2 \cdot \mathbb{Q}^{*2}\}$

$$\cup \Bigg\{ p_{i_1} \dots p_{i_l} \cdot \mathbb{Q}^{*2}, 2p_{i_1} \dots p_{i_l} \cdot \mathbb{Q}^{*2} : 1 \le l \le \kappa,\ 1 \le i_1 < \ldots < i_l \le \kappa,$$

$$\forall i \in \{i_1, \dots, i_l\} : p_i \equiv 1, 5 \pmod 8$$

$$\wedge \left[\forall i \in \{i_1, \dots, i_l\} : p_i \equiv 1 \pmod 8 \Rightarrow \left(\frac{p_1 \widetilde{\dots} p_\kappa (1+\sqrt{-1})}{p_i} \right) = 1 \right]$$

$$\wedge \left[\forall j \notin \{i_1, \dots, i_l\} : \left(\frac{p_{i_1} \dots p_{i_l}}{p_j} \right) = 1 \vee \left(\frac{2p_{i_1} \dots p_{i_l}}{p_j} \right) = 1 \right]$$

$$\wedge [p_{i_1} \dots p_{i_l} \equiv 5 \pmod 8 \Rightarrow k \equiv 3, 7 \pmod 8] \Bigg\}.$$

Its $\mathbb{F}_2$-dimension satisfies $\dim_{\mathbb{F}_2} S_k[\psi'] \le \kappa + 1$.

THEOREM 2.4. *For $k = \pm p_1 \dots p_\kappa$ with primes $p_1, \dots, p_\kappa \in \mathbb{P}\backslash\{2\}$,*
$S_k[\psi] = \{\pm 1 \cdot \mathbb{Q}^{*2}\}$

$$\cup \Bigg\{ \pm p_{i_1} \dots p_{i_l} \cdot \mathbb{Q}^{*2} : 1 \le l \le \kappa,\ 1 \le i_1 < \ldots < i_l \le \kappa,$$

$$\forall i \in \{i_1, \dots, i_l\} : p_i \equiv 1, 7 \pmod 8$$

$$\wedge \left[\forall i \in \{i_1, \dots, i_l\} : p_i \equiv 1 \pmod 8 \Rightarrow \left(\frac{p_1 \widetilde{\dots} p_\kappa (1+\sqrt{-1})}{p_i} \right) = 1 \right]$$

$$\wedge \left[\forall j \notin \{i_1, \dots, i_l\} : \left(\frac{p_{i_1} \dots p_{i_l}}{p_j} \right) = 1 \vee \left(\frac{-p_{i_1} \dots p_{i_l}}{p_j} \right) = 1 \right] \Bigg\}$$

$$\cup \Bigg\{ \pm 2p_{i_1} \dots p_{i_l} \cdot \mathbb{Q}^{*2} : 0 \le l \le \kappa,\ 1 \le i_1 < \ldots < i_l \le \kappa,$$

$$\forall i \in \{i_1, \dots, i_l\} : p_i \equiv 1, 7 \pmod 8$$

$$\wedge \left[\forall i \in \{i_1, \dots, i_l\} : p_i \equiv 1 \pmod 8 \Rightarrow \left(\frac{p_1 \widetilde{\dots} p_\kappa (1+\sqrt{-1})}{p_i} \right) = 1 \right]$$

$$\wedge \left[\forall j \notin \{i_1, \dots, i_l\} : \left(\frac{2p_{i_1} \dots p_{i_l}}{p_j} \right) = 1 \vee \left(\frac{-2p_{i_1} \dots p_{i_l}}{p_j} \right) = 1 \right]$$

$$\wedge k \equiv 1, 5 \pmod 8 \Bigg\}.$$

Its $\mathbb{F}_2$-dimension satisfies $\dim_{\mathbb{F}_2} S_k[\psi] \le \kappa + 2$. Here $l = 0$ means that $\pm 2p_{i_1} \dots p_{i_l} \cdot \mathbb{Q}^{*2}$ is $\pm 2 \cdot \mathbb{Q}^{*2}$ and that $\{i_1, \dots, i_l\}$ is the empty set.

I shall only prove Theorem 2.1. The other theorems are proven by similar arguments (see [Sc]).

Proof of Theorem 2.1. Our task is to decide, for a given $d = p_{i_1} \dots p_{i_l}$, whether or not $d \cdot \mathbb{Q}^{*2}$ resp. $2d \cdot \mathbb{Q}^{*2}$ is in the corresponding Selmer group. To this end I must consider all rational numbers whose squarefree part is equal to d resp. $2d$. Of course, the numbers we have to consider must be integers and must divide $2k^2$ or $-4k^2$. In this situation we need an appropriate notation:

For fixed $p_{i_1}, \dots, p_{i_l}$ with $1 \le l \le \kappa$, $1 \le i_1 < \dots < i_l \le \kappa$, I introduce the power products

$$p_1^{\alpha_1} \dots p_\kappa^{\alpha_\kappa} \quad \text{and} \quad p_1^{\beta_1} \dots p_\kappa^{\beta_\kappa}$$

with

$$\alpha_j = \begin{cases} 0 \text{ or } 2 & \text{if } j \notin \{i_1, \dots, i_l\}, \\ 0 & \text{if } j \in \{i_1, \dots, i_l\}, \end{cases}$$

and

$$\beta_j = \begin{cases} 2 - \alpha_j & \text{if } j \notin \{i_1, \dots, i_l\}, \\ 0 & \text{if } j \in \{i_1, \dots, i_l\}. \end{cases}$$

The numbers $p_1^{\alpha_1} \dots p_\kappa^{\alpha_\kappa}$ and $p_1^{\beta_1} \dots p_\kappa^{\beta_\kappa}$ are squares, because $\alpha_j, \beta_j \in \{0, 2\}$ for all j. They also satisfy

$$(p_1^{\alpha_1/2} \dots p_\kappa^{\alpha_\kappa/2}) \cdot (p_1^{\beta_1/2} \dots p_\kappa^{\beta_\kappa/2}) = p_1 \widetilde{\dots} p_\kappa.$$

I will consider the Selmer groups for even numbers k of the form $k = 2vp_1 \dots p_\kappa$ with $p_1, \dots, p_\kappa \in \mathbb{P} \backslash \{2\}$ and $v \in \{\pm 1\}$. The equation of the elliptic curve E_k is then

$$E_k : \quad y^2 = x^3 - 4vp_1 \dots p_\kappa x^2 + 8p_1^2 \dots p_\kappa^2 x.$$

For the Selmer group, I have the inclusion (5).

Ad $S_k[\psi']$: Choose $d = p_{i_1} \dots p_{i_l}$ for $1 \le l \le \kappa$, $1 \le i_1 < \dots < i_l \le \kappa$. Then, since d and $4d$ divide $8p_1^2 \dots p_\kappa^2$, the equations

$$\begin{aligned} (9) \quad n^2 &= p_{i_1} \dots p_{i_l} p_1^{\alpha_1} \dots p_\kappa^{\alpha_\kappa} m^4 - 4vp_1 \dots p_\kappa m^2 e^2 \\ &\quad + 8p_{i_1} \dots p_{i_l} p_1^{\beta_1} \dots p_\kappa^{\beta_\kappa} e^4 \\ &= p_{i_1} \dots p_{i_l} [p_1^{\alpha_1} \dots p_\kappa^{\alpha_\kappa} m^4 - 4vp_1 \widetilde{\dots} p_\kappa m^2 e^2 + 8p_1^{\beta_1} \dots p_\kappa^{\beta_\kappa} e^4] \\ &= p_{i_1} \dots p_{i_l} [(p_1^{\alpha_1/2} \dots p_\kappa^{\alpha_\kappa/2} m^2 - 2vp_1^{\beta_1/2} \dots p_\kappa^{\beta_\kappa/2} e^2)^2 \\ &\quad + 4p_1^{\beta_1} \dots p_\kappa^{\beta_\kappa} e^4] \end{aligned}$$

and

$$\begin{aligned} (10) \quad n^2 &= 4p_{i_1} \dots p_{i_l} p_1^{\alpha_1} \dots p_\kappa^{\alpha_\kappa} m^4 - 4vp_1 \dots p_\kappa m^2 e^2 \\ &\quad + 2p_{i_1} \dots p_{i_l} p_1^{\beta_1} \dots p_\kappa^{\beta_\kappa} e^4 \end{aligned}$$

have to be solved for m, n, e in $\mathbb{Z}_2$ and $\mathbb{Z}_q$ for all q in $\{p_1, \dots, p_\kappa\}$ and for any $\alpha_1, \dots, \alpha_\kappa$ as above. The equation (10) leads to a contradiction in $\mathbb{Z}_2$: From $2 \,|\, n$, it follows that $4 \,|\, n^2$. As the solutions m, n, e must be relatively prime integers and as $2 \nmid p_{i_1} \dots p_{i_l} p_1^{\beta_1} \dots p_\kappa^{\beta_\kappa} e^4$, the equation (10) implies the contradiction

$$0 \equiv n^2 \equiv 2 \pmod 4.$$

Therefore, (10) has no solution in $\mathbb{Z}_2$.

Now I have to solve (9) in $\mathbb{Z}_2$ and in $\mathbb{Z}_q$ with $q \in \{p_1, \dots, p_\kappa\}$. Here I distinguish the two cases $q \in \{p_{i_1}, \dots, p_{i_l}\}$ and $q \notin \{p_{i_1}, \dots, p_{i_l}\}$.

In $\mathbb{Z}_{p_i}$ for $i \in \{i_1, \dots, i_l\}$: By Hensel's lemma, the last equation in (9) is soluble in $\mathbb{Z}_{p_i}$ if and only if the following conditions are satisfied:

1. $\left(\dfrac{-1}{p_i}\right) = 1 \Leftrightarrow p_i \equiv 1, 5 \pmod 8$ and
2. $\left(\dfrac{-2v\widetilde{p_1 \dots p_\kappa}(-1+\sqrt{-1})}{p_i}\right) = 1.$

For $p_i \equiv 5 \pmod 8$ the Legendre symbol $\left(\frac{-1+\sqrt{-1}}{p_i}\right)$ takes both values ± 1, depending on the choice of the root $\sqrt{-1}$, so the last condition can always be satisfied by a suitable choice of $\sqrt{-1}$ for $p_i \equiv 5 \pmod 8$.

For $p_i \equiv 1 \pmod 8$, the equation $\left(\frac{-2v}{p_i}\right) = 1$ holds, and hence condition 2 is equivalent to

2a. $p_i \equiv 1 \pmod 8 \Rightarrow \left(\dfrac{\widetilde{p_1 \dots p_\kappa}(1+\sqrt{-1})}{p_i}\right) = 1.$

In $\mathbb{Z}_{p_j}$ for $j \notin \{i_1, \dots, i_l\}$: Again by Hensel's lemma, the first equation in (9) is soluble in $\mathbb{Z}_{p_j}$ if one of the following conditions is fulfilled, depending on the choice of the α_j:

$$\left(\frac{p_{i_1} \dots p_{i_l}}{p_j}\right) = 1 \vee \left(\frac{2p_{i_1} \dots p_{i_l}}{p_j}\right) = 1.$$

Remark. To prove that $d \in S_k[\psi']$, one needs only one choice of $\alpha_1, \dots, \alpha_\kappa$, so that the accompanying equation (9) has a solution in $\mathbb{Z}_q$ for $q \in \{2, p_1, \dots, p_\kappa\}$. But the existence of solutions in $\mathbb{Z}_2$ and $\mathbb{Z}_{p_i}$ for $i \in \{i_1, \dots, i_l\}$ is independent of $\alpha_1, \dots, \alpha_\kappa$, so we can choose the α_j in an appropriate way that the above conditions are fulfilled, without changing the other results.

In $\mathbb{Z}_2$, the first equation in (9) has a solution if and only if $n^2 \equiv 1 \pmod 8$. It follows from the above conditions for solutions in $\mathbb{Z}_{p_i}$ that $p_{i_1} \dots p_{i_l} \equiv 1, 5 \pmod 8$.

If $p_{i_1} \dots p_{i_l} \equiv 1 \pmod 8$, then $m = 1$, $e = 2$ gives $n^2 \equiv 1 \pmod 8$, so that there is a solution in $\mathbb{Z}_2$.

If $p_{i_1} \dots p_{i_l} \equiv 5 \pmod 8$, then $m = 1, e = 1$ gives $n^2 \equiv 1 \pmod 8$, so that there is a solution in $\mathbb{Z}_2$.

On combining the above results we have proved Theorem 2.1. ∎

Altogether, one derives from the rank equation (4) the coarse estimates:

PROPOSITION 2.1. *For even k, one has* $\mathrm{rk}(E_k(\mathbb{Q})) \le 2\kappa$. *If k is odd, one has* $\mathrm{rk}(E_k(\mathbb{Q})) \le 2\kappa + 1$.

Remark. The Selmer groups $S_k[\psi']$ and $S_k[\psi]$ can become arbitrarily large, a fact which can be shown in the following way. If we take $k = \pm 2p_1 \dots p_\kappa$ with primes $p_i \equiv 5 \pmod 8$, then the three conditions in Theorem 2.1 are satisfied for all products $p_{i_1} \dots p_{i_l}$. Hence the corresponding Selmer group is

$$S_k[\psi'] \cong (\mathbb{Z}/2\mathbb{Z})^{\kappa+1}.$$

If we have $k = \pm 2p_1 \dots p_\kappa$ with $p_i \equiv 7 \pmod 8$, then the three conditions in Theorem 2.2 are satisfied for all $p_{i_1} \dots p_{i_l}$, so we get

$$S_k[\psi] \cong (\mathbb{Z}/2\mathbb{Z})^{\kappa+1}.$$

One can also see that if $k = \pm p_1 \dots p_\kappa$ with $p_i \equiv 5 \pmod 8$, then

$$S_k[\psi'] \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^{\kappa} & \text{if } k > 0, \\ (\mathbb{Z}/2\mathbb{Z})^{\kappa+1} & \text{if } k < 0. \end{cases}$$

By looking at the last theorem, if $k = \pm p_1 \dots p_\kappa$ with $p_i \equiv 7 \pmod 8$, we get

$$S_k[\psi] \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^{\kappa+1} & \text{if } k \equiv 7 \pmod 8, \\ (\mathbb{Z}/2\mathbb{Z})^{\kappa+2} & \text{if } k \equiv 1 \pmod 8. \end{cases}$$

Based on the above theorems, I developed an algorithm for computing the Selmer groups for arbitrary $z \in \mathbb{Q}^*$. After prime factorization and determination of the squarefree part of z, it obtains a squarefree integer k and uses the theorems to compute the Selmer groups for $E_k \cong E_z$.

From the theory of Selmer groups corresponding to 2-isogenies, one cannot determine but only estimate the rank of elliptic curves. For an exact determination of the rank, one has to compute points of infinite order in the Mordell–Weil group. This can be done in an analogous way as described in [S-T]. I generalized their results to arbitrary rational k in [Sc]. The main idea of this method is to look further at the equations which have to be solved for computing the Selmer groups. Those equations can be "reduced" in such a way that solutions of the new equations normally have smaller absolute value than those of the old equations.

If, for a given k, the rank of the curve E_k over $\mathbb{Q}$ is greater than 0, then one can find points in $E_k(\mathbb{Q})$ by testing all those possible equations. These are only finitely many, and their number depends on the different

prime factors of k. However, one has to take into account the relation of these equations to the Tate–Shafarevich group. If an equation for $d \cdot \mathbb{Q}^{*2}$ in the definition of the Selmer group (see Section 2.1) is everywhere locally soluble, but has no solution in $\mathbb{Q}$, then $d \cdot \mathbb{Q}^{*2}$ is in the corresponding Tate–Shafarevich group. Hence the equations which have to be solved are also everywhere locally soluble, but not globally in $\mathbb{Q}$. If such a situation occurs, one is often unable to see whether the equation has no global solution, that is, that the Tate–Shafarevich group is nontrivial, or one has to search longer for a global solution. Stroeker and Top were able to prove that the Tate–Shafarevich group is nontrivial in a special case (see [S-T]), which I could not generalize.

By considering these equations, one determines a certain set of points of infinite order in $E_k(\mathbb{Q})$. The generating points of $E_k(\mathbb{Q})$ are then identified in this set by estimating the heights as described in [Zi] and searching for generators in a certain range as explained in Proposition 7.2 of [Si]. The estimation of the heights for the curves E_k is

$$-\frac{1}{2}\log|k| - \frac{49}{12}\log 2 \le \widehat{h}(P) - h(P) \le \frac{1}{2}\log|k| + 2\log 2$$

where $\widehat{h}$ is the Néron–Tate height and h is the Weil height on E_k.

References

[MF IV] B. J. Birch and W. Kuyk, *Modular Functions of One Variable IV*, Lecture Notes in Math. 476, Springer, 1975.

[B-S] B. J. Birch and H. P. F. Swinnerton-Dyer, *Elliptic curves and modular functions*, in: Modular Functions of One Variable IV, Antwerpen 1972, Lecture Notes in Math. 476, Springer, 1975, 2–32.

[Fo] H. G. Folz, *Ein Beschränktheitssatz für die Torsion von* 2*-defizienten elliptischen Kurven über algebraischen Zahlkörpern*, Dissertation, Universität des Saarlandes, 1985.

[H-M] T. Honda and I. Miyawaki, *Zeta-functions of elliptic curves of* 2*-power conductor*, J. Math. Soc. Japan 26 (1974), 362–373.

[Ko] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, New York, 1984.

[Og] A. Ogg, *Abelian curves over* 2*-power conductor*, to appear.

[Sc] S. Schmitt, *Berechnung der Mordell–Weil Gruppe parametrisierter elliptischer Kurven*, Diplomarbeit, Universität des Saarlandes, 1995.

[Si] J. H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. 55 (1990), 723–743.

[Si-Ta] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer, 1985.

[S-T] R. J. Stroeker and J. Top, *On the equation* $Y^2 = (X + p)(X^2 + p^2)$, Rocky Mountain J. Math. 27 (1994), 1135–1161.

[Ta] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in: Modular Functions of One Variable IV, Antwerpen 1972, Lecture Notes in Math. 476, Springer, 1975, 33–52.

[We] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, 1963.

[Zi] H. G. Zimmer, *A limit formula for the canonical height of an elliptic curve and its application to height computations*, in: Number Theory, R. Mollin (ed.), Proc. First Conf. Canad. Number Theory Assoc., Banff, 1988, de Gruyter, 1990, 641–659.

Fachbereich Mathematik
Universität des Saarlandes
Bau 27, Zimmer 429
D-66041 Saarbrücken, Germany
E-mail: susanne@math.uni-sb.de

Received on 24.10.1995
and in revised form on 27.8.1996 (2883)