# Master's thesis in mathematics:
# Elliptic curves with large Selmer groups

Remke Kloosterman

23rd March 2001

# Contents

# Introduction & notation

It is well known that for an elliptic curve $E$, defined over $\mathbb{Q}$, the group of $\mathbb{Q}$-rational points $E(\mathbb{Q})$ is finitely generated ([Sil 1, chapter VIII]).

To describe this group, the first thing one can do, is to look for the points of finite order. This is easy: suppose $E$ is given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$ (for a curve defined over $\mathbb{Q}$ this is always possible) and let $P \neq O$ be a point of finite order, then either $y(P) = 0$ or $y(P)^2$ is an integer dividing $4A^3 + 27B^2$.

The second point of interest is the rank of the group. To find this, one considers $E(\mathbb{Q})/pE(\mathbb{Q})$ ($p \in \mathbb{Z}$, a prime number). An approach to determine this group would be the following: we have the exact sequence

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to H^1(G_{\mathbb{Q}}, E[p]) \to H^1(G_{\mathbb{Q}}, E)[p] \to 0.$$

We want to know the image of the first map, which equals the kernel of the second map. This is quite difficult with the techniques we have at this moment, but if we replace $\mathbb{Q}$ by an $\ell$-adic completion we have a much easier problem. Consider now the kernel of $H^1(G_{\mathbb{Q}}, E[p]) \to \prod_\ell H^1(G_{\mathbb{Q}_\ell}, E)$. This kernel contains at least the searched kernel, but can be much bigger.

We define the $p$-Selmer group $S^p(\mathbb{Q}, E)$ as the kernel of the map

$$H^1(G_{\mathbb{Q}}, E[p]) \to \prod_\ell H^1(G_{\mathbb{Q}_\ell}, E).$$

This is an $\mathbb{F}_p$-vector space.

The cokernel of the map $E(\mathbb{Q})/pE(\mathbb{Q}) \to S^p(\mathbb{Q}, E)$ is denoted by $Ш(E, \mathbb{Q})[p]$. In fact, this is the subgroup of elements of order $p$ in the so-called Shafarevich-Tate group.

Now we can ask the following questions:

1. Can the rank of an elliptic curve be arbitrarily large?
2. Can the $p$-part of the Shafarevich-Tate group be arbitrarily large?
3. Can the $p$-Selmer group be arbitrarily large?

It is widely conjectured that the rank can get arbitrarily large. This would mean that all $S^p$ can get simultaneously large. Conversely: assume that the Shafarevich-Tate group is finite (this is also widely conjectured). For proving that the rank can be arbitrarily large, it would be sufficient to ask that an infinite number of the $S^p$ can get simultaneously arbitrarily large.

Our main theorem will be

**Theorem 0.0.1.** *Suppose $p \in \{3, 5, 7, 13\}$, fix an integer $m$. Then there exists infinitely many non-isomorphic elliptic curves $E/\mathbb{Q}$ such that $dim_{\mathbb{F}_p} S^p(\mathbb{Q}, E) \geq m$.*

The proof depends heavily on the fact, that for the primes $p$ mentioned in the theorem, there exist infinitely many non-isomorphic elliptic curves with an isogeny of degree $p$ defined over $\mathbb{Q}$.

The first thing we do is to describe these curves and the isogenous ones. Then we will try to find large $S^p$'s. We use the following plan:

Suppose $\phi : E \to E'$ is an isogeny of degree $p$. One can associate to this a $\mathbb{F}_p$-vector space $S^\phi(\mathbb{Q}, E)$. We show that the dimension of $S^p(\mathbb{Q}, E)$ will be bigger than the dimension of $S^{\phi'}(\mathbb{Q}, E')$ minus 2. ($\phi'$ is the dual isogeny of $\phi$.) So if we want to find large $S^p$, we can do this by finding large $S^{\phi'}$. For this we use the following relation of Cassels

$$\frac{\#S^{\phi'}(\mathbb{Q}, E')}{\#S^\phi(\mathbb{Q}, E)} = \frac{\#E'(\mathbb{Q})[\phi']\Omega_E \prod c_{E,q}}{\#E(\mathbb{Q})[\phi]\Omega_{E'} \prod c_{E',q}}$$

(we will define these quantities later).

We will use families of elliptic curves with an isogeny of order $p$. In the families we consider, the quantities $\Omega_E/\Omega_{E'}$ and $\#E'(\mathbb{Q})[\phi']/\#E(\mathbb{Q})[\phi]$ are constant. So we have to play a bit with the $c_{E,q}$ and $c_{E',q}$.

From certain theorems one can deduce that, if the $E$ has certain properties this number $c_{E,q}$ depends only on $\text{ord}_q(\Delta)$, with $\Delta$ the discriminant of the curve. So we have to find a sub-family of curves such that the discriminant of $E$ has a large number of primes $\ell$ for which $\text{ord}_\ell(\Delta)$ is high and $\text{ord}_\ell(\Delta')$ is small.

Also we will prove

**Theorem 0.0.2.** *Fix an integer $m$. Then there exist infinitely many non-isomorphic elliptic curves $E/\mathbb{Q}$ such that $dim_{\mathbb{F}_2} S^2(\mathbb{Q}, E) \geq m$ and $dim_{\mathbb{F}_3} S^3(\mathbb{Q}, E) \geq m$.*

By a similar techniques we will prove that

**Theorem 0.0.3.** *For every $m$ there exists infinitely many couples $(E, K)$, where $K$ is an quadratic extension of $\mathbb{Q}$ and $E/K$ an elliptic curve, such that*

$$\dim S^{11}(K, E) \geq m.$$

We want also to get large $p$-parts of the Shafarevich-Tate group. An idea of finding curves with this property would be finding curves with an big $S^p$ and small $S^q$, for some $q$. We will try this in an example with $p = 3$ and $q = 2$.

We will make an attempt to prove that this can be done for the $S^2$ and the $S^5$. We find criteria when a curve with a rational 5-torsion has a large $Ш(\mathbb{Q}, E)[5]$. This criteria involves only quadratic reprocity in a cubic extension of $\mathbb{Q}$ and hence is a pure number theoretical problem.

# Notation

If $\phi : G \to H$ is a homomorphism we denote with $G[\phi]$ the kernel of $\phi$.

With $G_K$ we denote the absolute Galois group of $K$ and with $G_{L/K}$ we denote the Galois group of the extension $L/K$, provided that this extension is Galois.

$p, \ell$ are assumed to be prime numbers. $\mathcal{O}_K$ is the ring of integers of a number field $K$. $\mathfrak{p}, \mathfrak{q}$ are prime ideals of $\mathcal{O}_K$. $v$ is a normalized valuation on a field $K$.

Sometimes we don't distinguish the prime $\mathfrak{p}$ and the associated normalized valuation $v$.

# Chapter 1

# Isogenies

In this chapter we want to describe curves $E/\mathbb{Q}$ with an isogeny $\phi : E \to E'$ defined over $\mathbb{Q}$ of degree $p$. The easiest way to obtain this, is to divide out the subgroup generated by a rational point of order $p$. This is only possible for $p = 2, 3, 5$ and $7$. Mazur([Maz]) proved that the torsion part $E_{\text{tors}}(\mathbb{Q})$ can be $\mathbb{Z}/N\mathbb{Z}$ for $1 \leq N \leq 10$ and $N = 12$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ for $1 \leq N \leq 4$.

We will also give curves with an isogeny of degree 13.

## 1.1 Points of order $p$

Take an arbitrary field $K$. The following two propositions are from [Sil 1, Exer. 8.13].

**Proposition 1.1.1.** *Let $E/K$ be an elliptic curve with a point $O \neq P \in E(K)$ not of order 2, then $E$ is isomorphic over $K$ to one of the following curves ($u, w \in K$):*

1. *$y^2 + uy + wxy = x^3$ if $P$ has order 3,*
2. *$y^2 + uy + wxy = x^3 + wx^2$ otherwise.*

*Proof.* Suppose $E/K$ has an equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and $P \in E(K)$ not of order 2.

First we translate this point $P$ to $(0, 0)$, so we may assume that $a_6 = 0$.

Suppose $a_3 = 0$, then $[-1](0, 0) = (0, 0)$ ([Sil 1, III.2.3 (GLA)]) and $(0, 0)$ will be a point of order 2. This proves that $a_3 \neq 0$.

So we can map $(x, y)$ to $(x, a_4/a_3x + y)$, which maps $(0, 0)$ to $(0, 0)$. The coefficient of $x$ will be $a_4 - a_4 = 0$ and we have an equation of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2$.

Suppose $P$ has order 3; this happens precisely when $(0, -a_3) = [-1](0, 0) = [2](0, 0) = (a_2, a_1a_2 - a_3)$. So $(0, 0)$ is a point of order 3 if and only if $a_2 = 0$.

Suppose $P$ is not of order 2 or 3, then $a_2 \neq 0$ and we can map $(x, y)$ to $((a_2/a_3)^2x, (a_2/a_3)^3y)$ then the new $a_2$ and $a_3$ will be equal (see [Sil 1, Table 1.3]). □

**Proposition 1.1.2.** *Suppose $E/K$ has a point of order $n \in \{4, 5, 6, 7\}$ in $E(K)$, then $E/K$ is isomorphic to a curve of the form*

$$\begin{array}{ll}
n = 4 & y^2 + xy + dy = x^3 + dx^2 \\
n = 5 & y^2 + (d+1)xy + dy = x^3 + dx^2 \\
n = 6 & y^2 + dxy + (d-1)(2-d)y = x^3 + (d-1)(2-d)x^2 \\
n = 7 & y^2 + (-d^2 + d + 1)xy + (d^2 - d^3)y = x^3 + (d^2 - d^3)x^2
\end{array}$$

*and for every $d \in K$ these curves have a point of order $n$ in $E(K)$, provided that for that $d$, we have $\Delta(E) \neq 0$.*

*Proof.* By the previous proposition, we may assume that $E$ is given by $y^2 + uxy + wy = x^3 + wx^2$ and $(0,0)$ is a point of order $n$.

Suppose $P \in E(K)\backslash E(K)[2]$, then precisely one other point exists with the same $x$-coordinate and by [Sil 1, III.2.3 (GLA)] that other point is $-P$. (If $P$ has order two, no other point exists with that $x$-coordinate.)

If we want to find a point $P$ of order $n$, $n$ an odd prime number, it is necessary and sufficient to ask for a $P \neq O$ such that $x([(n-1)/2]P) = x([(n+1)/2]P)$. If $n$ is even, it is necessary to ask that $[n/2]P = [-n/2]P$.

The orbit of $(0,0)$ is the following (note that $\Delta \neq 0$ implies $w \neq 0$, the formula for $[4]P$ is only valid when $u \neq 1$):

$$\begin{aligned} P &= (0,0) \\ 2P &= (-w, (u-1)w) \\ 3P &= (-u+1, u-1-w) \\ 4P &= (-w(u-1-w)/(u-1)^2, w^2(-3u+2+w+u^2)/(u-1)^3). \end{aligned}$$

Suppose $P$ is a point of order $n = 4$. We have that $[-2]P = (-w, 0)$ and this has to equal $(-w, (u-1)w)$, so either $w = 0$ (and hence $E$ singular) or $u = 1$. If $u = 1$ we have that $[4]P = O$ and $[2]P \neq O$, so $P$ has order 4.

Suppose $P$ is a point of order $n = 6$, we have that $[-3]P = (1-u, (1-u)^2)$, so $[3]P = [-3]P$ if and only if $(u-1)^2 - (u-1) + w = 0$, so $w = (u-1)(2-u)$. Conversely, an elliptic curve with $w = (u-1)(2-u)$ will have $[6]P = O$, $[3]P \neq O \neq [2]P$.

Suppose $P$ is a point of order $n = 5$, then the $x$-coordinate of $[2]P$ will equal the $x$-coordinate of $[3]P$ precisely when $w = u - 1$.

Suppose $P$ is a point of order $n = 7$. Recall that $u \neq 1$, now

$$-u + 1 = x([3]P) = x(4[P]) = \frac{-w(u-1-w)}{(u-1)^2}$$

and this equation has as only solutions $w = (1/2 \pm 1/2\sqrt{5-4u})(u-1)$.

So if we have a point of order 7 then $1/2 \pm 1/2\sqrt{5-4u}$ is rational. Set $d_\pm := 1/2 \pm 1/2\sqrt{5-4u}$, then $4d_\pm^2 - 4d_\pm + 1 = 5 - 4u$, so $u = -d^2 + d + 1$ and $w = d(-d^2 + d) = d^2 - d^3$. If we take a curve with this $u, w$ then it is obvious that $[7]P = O$ and hence $P$ is a point of order 7. □

## 1.2 A curve modulo a finite subgroup

Take an elliptic curve $E$. Take a subgroup $H$ of $E$. One can ask if there is a curve isogenous to $E$ with $H$ as the kernel of the isogeny. The answer is yes if and only if $H$ is a finite group. In [Vél] an algorithm is described to obtain the isogenous curve if $H = \langle P \rangle$ and $P$ is a point of finite order.

If we apply this algorithm to the elliptic curves

$$\begin{aligned} E_{d,3} &: y^2 + xy + dy = x^3 \\ E_{d,5} &: y^2 + (d+1)xy + dy = x^3 + dx^2 \\ E_{d,7} &: y^2 + (1+d-d^2)xy + (d^2-d^3)y = x^3 + (d^2-d^3)x^2 \end{aligned}$$

then we get the isogenous curves:

$$\begin{aligned}
E'_{d,3} &: y^2+xy+dy = x^3-5dx-d(7d^2+1) \\
E'_{d,5} &: y^2+(d+1)xy+dy = x^3+dx^2+(5d^3-10d^2-5)x+(d^5-10d^4-5d^3-15d^2-d) \\
E'_{d,7} &: y^2+(1+d-d^2)xy+(d^2-d^3)y = \\
& \quad x^3+(d^2-d^3)x^2+(-5d^7+35d^5-70d^4+70d^3-35d^2+5d)x \\
& \quad -d^{11}-8d^{10}+46d^9-107d^8+202d^7-343d^6+393d^5-258d^4+94d^3-19d^2+d.
\end{aligned}$$

## 1.3 A more theoretical approach

In this section we will give some theory about elliptic curves with certain finite subgroups. This will explain why we could find the curves found in the last two sections.

In [Sil 2, Ch. 1] it is proven that every elliptic curve $E/\mathbb{C}$ is analytically isomorphic to a complex torus $\mathbb{C}/\Lambda$, where $\Lambda$ is a lattice determined by $E$ upto homothety. It is easy to see that every lattice is homothetic to a lattice of the form $\Lambda_\tau = \mathbb{Z}+\mathbb{Z}\tau$, with $\tau \in \{w \in \mathbb{C} : \mathrm{Im}(w) > 0\} =: \mathbb{H}$.

An even sharper statement is possible. On $\mathbb{H}$ an action of the group $SL_2(\mathbb{Z})$ exists: to a matrix $A \in SL_2(\mathbb{Z})$ we associate the transformation $\tau \mapsto (a\tau+b)/(c\tau+d)$. (Note that $\mathrm{Im}((a\tau+b)/(c\tau+d)) = (ad-bc)\mathrm{Im}(\tau)/|c\tau+d|^2 > 0$.) This action is so-called properly discontinuous. Let $\mathcal{F} = \{\tau \in \mathbb{H} | \, |\mathrm{Re}(\tau)| \leq \frac{1}{2}, | \tau | \geq 1\}$. Now $\mathcal{F}$ is a fundamental domain for $SL_2(\mathbb{Z})\backslash\mathbb{H}$, i.e. the natural map $\mathcal{F} \to SL_2(\mathbb{Z})\backslash\mathbb{H}$ is surjective and its restriction to the interior of $\mathcal{F}$ is injective. (This implies that every lattice in $\mathbb{C}$ is homothetic to a lattice $\Lambda_\tau$ with $\tau \in \mathcal{F}$.)

We extend $\mathbb{H}$ by adjoining $\mathbb{P}^1(\mathbb{Q})$ and denote it by $\mathbb{H}^*$. Now $SL_2(\mathbb{Z})$ acts in the obvious way on $\mathbb{P}^1(\mathbb{Q})$ and this action is transitive. So we can think of $SL_2(\mathbb{Z})\backslash\mathbb{H}^*$ as $SL_2(\mathbb{Z})\backslash\mathbb{H}$ with one extra point, called a cusp (at infinity).

We define the following subgroups of $SL_2(\mathbb{Z})$:

$$\begin{aligned}
\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c \equiv 0 \bmod N \right\} \\
\Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c \equiv 0 \bmod N, a \equiv d \equiv 1 \bmod N \right\} \\
\Gamma(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid b \equiv c \equiv 0 \bmod N, a \equiv d \equiv 1 \bmod N \right\}.
\end{aligned}$$

We want to use these groups to say something about isogenies of degree $p$ and cyclic subgroups of order $p$:

Consider $\Gamma_i(p)\backslash\mathbb{H}^*$, $i = 0, 1$. There is a natural map $\Gamma_i(p)\backslash\mathbb{H}^* \to SL_2(\mathbb{Z})\backslash\mathbb{H}^*$. Via this map we can associate to a $\tau \in \Gamma_i(p)\backslash\mathbb{H}^*$, an elliptic curve $E_\tau$. Consider $1/p \in \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$. Suppose $\gamma \in \Gamma_i(p)$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then one can show that $\gamma(1/p) = a/p \in \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\gamma(t))$.

From this we deduce that the isomorphism class of $(E_\tau, \langle 1/p \rangle)$ doesn't change under the action of $\Gamma_0(p)$. Conversely suppose that $(E, G)$ an $(E', G')$ are elliptic curves with $G$ and $G'$ are subgroups of order $p$, then $(E, G) \cong (E_\tau, \langle 1/p \rangle)$ and $(E', G') \cong (E_{\tau'}, \langle 1/p \rangle)$. Now we have that $\tau' = \gamma(\tau)$, with $\gamma \in \Gamma_0(p)$. Hence there is a 1-1 correspondence $\{(E,G)\}/\cong \longleftrightarrow \Gamma_0(p)\backslash\mathbb{H}$. There is a similar statement for $\Gamma_1(p)$ and points of order $p$.

As explained in e.g. [Shi, Ch. 1] there is a complex analytic structure on the spaces $\Gamma\backslash\mathbb{H}^*$, where $\Gamma = \Gamma_i(p), \Gamma(p)$ or $SL_2(\mathbb{Z})$.

**Theorem 1.3.1.** *Suppose $K$ is a field, $\mathbb{Q} \subset K \subset \mathbb{C}$. There exists smooth projective curves $X(1)/\mathbb{Q}$, $X_0(p)/\mathbb{Q}$, $X_1(p)/\mathbb{Q}$ such that*

1. *$X(1)(\mathbb{C}) \cong \Gamma(1)\backslash\mathbb{H}^* \cong \mathbb{P}^1(\mathbb{C})$ as complex analytic spaces, where the second isomorphism is taking the $j$-invariant.*

2. *$X_0(p)(\mathbb{C}) \cong \Gamma_0(p)\backslash\mathbb{H}^*$ as complex analytic spaces.*

3. *$X_1(p)(\mathbb{C}) \cong \Gamma_1(p)\backslash\mathbb{H}^*$ as complex analytic spaces.*

4. *Every point $\tau \in X_0(p)(K)$, not a cusp, gives an elliptic curve $E_\tau/K$ and a subgroup of $E_\tau(\overline{K})$ of order p, which is invariant under the action of $G_K$.*

5. *Every point $\tau \in X_1(p)(K)$, not a cusp, gives an elliptic curve $E_\tau/K$ and and a point $P \in E_\tau(K)$ of order p.*

*Proof.* See [Shi, 6.7]. □

We have the following tower of coverings:

$$\begin{array}{c} \Gamma(p)\backslash\mathbb{H}^* \\ \downarrow \phi_3 \\ \Gamma_1(p)\backslash\mathbb{H}^* \\ \downarrow \phi_2 \\ \Gamma_0(p)\backslash\mathbb{H}^* \\ \downarrow \phi_1 \\ \Gamma(1)\backslash\mathbb{H}^* . \end{array}$$

By a simple calculation one sees that the degrees of $\phi_1, \phi_2$ and $\phi_3$ are $p+1, (p-1)/2$ and $p$.

We will give some results from [Shi, Ch. 1]: The covering $\phi_1 \circ \phi_2 \circ \phi_3$ is Galois and ramifies above $i, \omega, \infty$ ($\omega^3 = 1, \omega \neq 1$), with ramification indices $2, 3, p$. For the covering $\phi_1$, let $\nu_2, \nu_3$ denote the number of non-ramified points above $i, \omega$ and $\nu_\infty$ the number of different points above $\infty$. Let $g$ be the genus of (the Riemann Surface) $\mathbb{H}^*\backslash\Gamma_0(p)$, then (see [Shi, Prop 1.40, Prop 1.43]):

$$\begin{aligned} \nu_2 &= 1 + \left(\frac{-1}{p}\right) \\ \nu_3 &= 1 + \left(\frac{-3}{p}\right) \\ \nu_\infty &= 2 \\ g &= 1 + \frac{p+1-3\nu_2-4\nu_3-6\nu_\infty}{12} = \frac{p+1-3\nu_2-4\nu_3}{12}. \end{aligned}$$

So $\nu_2, \nu_3 \leq 2$ hence $g \geq (p+1-6-8)/12 = (p-13)/12$. From this it follows that if $g = 0$ then $p \leq 13$.

For the first primes we have the following table:

| $p$ | $\nu_2$ | $\nu_3$ | $g$ |
|---|---|---|---|
| 2 | 1 | 0 | 0 |
| 3 | 0 | 1 | 0 |
| 5 | 2 | 0 | 0 |
| 7 | 0 | 2 | 0 |
| 11 | 0 | 0 | 1 |
| 13 | 2 | 2 | 0 |

*Remark* 1.3.2. If $X_0(p)$ has genus 0, then we can parameterize the image of $X_0(p)$ on the $j$-line by $\mathbb{P}^1(\mathbb{Q})$. There are two points on $X_0(p)$ above $\infty$, so the $j$-invariant of elliptic curves with a $G_\mathbb{Q}$-invariant subgroup of order $p$ can be parametrized by $\mathbb{Q}^*$.

$X_1(p)$ has genus 0 if and only if $p = 2, 3, 5, 7$. This tells us why we found a family of elliptic curves with a point of order 3,5,7. For more about this see [Maz].

## 1.4 Isogenies of degree 13

We want to construct a family of elliptic curves over $\mathbb{Q}$ with an isogeny of order $p$. Since $X_0(13)$ has genus 0, this is possible for $p = 13$.

It is known ([Mes]) that a curve with a rational subgroup of order 13 has $j$-invariant ($d \in \mathbb{Q}^*$)

$$\frac{(d^2+5d+13)(d^4+7d^3+20d^2+19d+1)^3}{d}.$$

To a $j$-invariant $j_0$ we can associate a curve $E_{j_0} : y^2 + xy = x^3 - 36/(j_0 - 1728)x - 1/(j_0 - 1728)$ which has $j$-invariant $j_0$ and discriminant:

$$\frac{j_0^2}{(j_0-1728)^3}.$$

In our special case we get the discriminant

$$d(d^2+5d+13)^2(d^4+7d^3+20d^2+19d+1)^6(d^2+6d+13)^9 *$$
$$*(d^6+10d^5+46d^4+108d^3+122d^2+38d-1)^6.$$

Suppose $13 \nmid d$, then a prime number $p$ dividing $d$ will give split multiplicative reduction at $p$. The other four factors in the discriminant divide $c_4$ (one sees this using $j_0\Delta = c_4^3$). So all the other bad primes will have additive reduction.

It is also known that the parameter of the isogenous curve will be $13/d$ and the curve has discriminant:

$$d^{13}(d^2+5d+13)^2(28561+15379d+3380d^2+247d^3+d^4)^6(d^2+6d+13)^9$$
$$*(-4826809-3712930d-1313806d^2-237276d^3-20618d^4-494d^5+d^6)^6.$$

At all primes dividing $d$ there is split multiplicative reduction and at all other bad primes there is additive reduction. (Note that $28561 = 13^4, 4826809 = 13^6$.)

The first curve is denoted by $E'_{d,13}$, the second by $E_{d,13}$.

# Chapter 2

# Selmer groups

In this chapter we define a group, called the $m$-Selmer group, which contains $E(\mathbb{Q})/mE(\mathbb{Q})$, but is in general bigger. The collection of the remaining parts (by varying $m$) is controlled by another group, called the Shafarevich-Tate group. The main part of this chapter will be about obtaining big $p$-Selmer groups. (For $p = 3, 5, 7, 13$)

We also find number fields of degree over $\mathbb{Q}$ less then $p^2$, with arbitrarily large $p$-Selmer groups (for every $p$).

Later on we will try to get simultaneously big 2- and big 3-Selmer groups. Also we will try to get big Shafarevich-Tate groups by making the 3- or 5-Selmer group big and keeping the 2-Selmer group small.

## 2.1 Definitions

Suppose $K$ is a number field. Take $E/K$ an elliptic curve and another elliptic curve $E'/K$ such that there is a non-zero isogeny $\phi : E \to E'$ defined over $K$. Then there is an exact sequence of $G_K$-modules

$$0 \to E[\phi] \to E \to E' \to 0.$$

By the long exact sequence of Galois-cohomology (see [Sil 1, App. B]) we obtain

$$\begin{array}{ccccccc} 0 & \to & E(K)[\phi] & \to & E(K) & \to & E'(K) \\ & \to & H^1(G_K, E[\phi]) & \to & H^1(G_K, E) & \to & H^1(G_K, E') \end{array}$$

and from this we extract

$$0 \to E'(K)/\phi(E(K)) \to H^1(G_K, E[\phi]) \to H^1(G_K, E)[\phi] \to 0.$$

If we take an absolute value $v$ on $K$, we can fix an extension of $v$ to $\overline{K}$, so we can fix an embedding $\overline{K} \subset \overline{K}_v$ and a decomposition group $G_v \subset G_K$. There is an action of $G_v$ on $E(\overline{K}_v)$ and $E'(\overline{K}_v)$. We obtain

$$0 \to E'(K_v)/\phi(E(K_v)) \to H^1(G_v, E[\phi]) \to H^1(G_v, E)[\phi] \to 0$$

and we have the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & E'(K)/\phi(E(K)) & \to & H^1(G_K, E[\phi]) & \to & H^1(G_K, E)[\phi] & \to & 0 \\ & & \downarrow & & \downarrow & \searrow \prod \beta_{\mathfrak{q}} & \downarrow & & \\ 0 & \to & \prod E'(K_{\mathfrak{q}})/\phi(E(K_{\mathfrak{q}})) & \to & \prod H^1(G_{\mathfrak{q}}, E[\phi]) & \to & \prod H^1(G_{\mathfrak{q}}, E)[\phi] & \to & 0. \end{array}$$

In this diagram the vertical arrows are in fact products of restriction maps. The products are to be taken over all finite and infinite primes $\mathfrak{q}$.

**Definition 2.1.1.** We define the *$\phi$-Selmer group* $S^\phi(K,E) := \ker \prod \beta_{\mathfrak{q}}$ and the *Shafarevich-Tate group* $\text{Ш}(K,E)$ as the kernel of the map

$$H^1(G_K,E) \to \prod H^1(G_{\mathfrak{q}},E).$$

One can show that these groups don't depend on the choice of the prolongation of $v$.

We have the following main properties:

**Proposition 2.1.2.** *For an elliptic curve $E/\mathbb{Q}$ we have the following exact sequence:*

$$0 \to E'(K)/\phi(E(K)) \to S^\phi(K,E) \to \text{Ш}(K,E)[\phi] \to 0.$$

*Furthermore the Selmer group $S^\phi(K,E)$ is finite and*

$$\dim_{\mathbb{F}_p} S^p(K,E) = r + \dim_{\mathbb{F}_p} E(K)[p] + \dim_{\mathbb{F}_p} \text{Ш}(E,K)[p],$$

*where $r$ is the rank of the curve.*

*Proof.* For the first and second property see [Sil 1, Thm X.4.2]. The third property follows directly from the first. □

**Proposition 2.1.3 ([Sch]).** *There is a long exact sequence:*

$$0 \to \frac{E(K)[\phi]}{\phi'(E'(K)[p])} \to S^{\phi'}(K,E') \to S^p(K,E') \to S^\phi(K,E) \to \frac{\text{Ш}(K,E)[\phi]}{\phi(\text{Ш}(K,E')[p])} \to 0$$

*Proof.* Consider the following commutative and exact diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & & & & & \\
 & & \downarrow & & & & & & \\
 & & E(K)[\phi]/\phi'(E(K)[p]) & & & & 0 & & \\
 & & \downarrow & & & & \downarrow & & \\
0 & \to & E(K)/\phi'(E'(K)) & \to & S^{\phi'}(K,E') & \to & \text{Ш}(K,E')[\phi'] & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & E'(K)/p(E'(K)) & \to & S^p(K,E') & \to & \text{Ш}(K,E')[p] & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & E'(K)/\phi(E(K)) & \to & S^\phi(K,E) & \to & \text{Ш}(K,E)[\phi] & \to & 0 \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}$$

First we compute the kernel $H$ of $S^{\phi'}(K,E') \to S^p(K,E)$. Since $\text{Ш}(K,E')[\phi'] \to \text{Ш}(K,E')[p]$ is injective, $H$ is isomorphic to the kernel of $E(K)/\phi'(E'(K)) \to E'(K)/p(E'(K))$, which is isomorphic to $E(K)[\phi]/\phi'(E(K)[p])$.

Secondly, we want to know what $S^\phi(K,E)/\phi(S^p(K,E'))$ is. But $E'(K)/p(E'(K)) \to E'(K)/\phi(E(K))$ is surjective, hence

$$S^\phi(K,E)/\phi(S^p(K,E')) \cong \text{Ш}(K,E)[\phi]/\phi(\text{Ш}(K,E')[p]).$$

□

To compute the size of the Selmer group, we can use the following relation of Cassels ([Cas 2],[Tat, Thm 5.2]):

$$\frac{\#S^{\phi'}(K,E')}{\#S^\phi(K,E)} = \frac{\#E'(K)[\phi'] \prod_v \int_{E(K_v)} |\omega|_v \prod c_{E,\mathfrak{q}}}{\#E(K)[\phi] \prod_v \int_{E'(K_v)} |\omega'|_v \prod c_{E',\mathfrak{q}}},$$

where $v$ runs through the archimedean valuations and $c_{E,\mathfrak{q}} := E(K_{\mathfrak{q}})/E_0(K_{\mathfrak{q}})$. For determining $c_{E,\mathfrak{q}}$ see [Tat, p. 46]. Very briefly this states that $c_{E,\mathfrak{q}} \leq 4$ or there is split multiplicative reduction at $\mathfrak{q}$.

*Remark* 2.1.4. If $\phi$ is an isogeny of degree $p^n$, then the $\phi$-Selmer groups will be $\mathbb{F}_p$-vector spaces. So if $p$ were bigger then 3, then we only need to consider the primes at which there is split multiplicative reduction.

## 2.2 Large $p$-Selmer groups

In this section we will prove that the $S^p(\mathbb{Q}, E)$ can be big, for $p = 3, 5, 7, 13$.

The proof given here is a slightly generalised version of a proof given at a pre-ANTS talk by Schaefer ([Sch]) at Leiden, June 2000.

In the proof we will use the families $E'_{d,p}$ for $p = 3, 5, 7, 13$ and we need some information about these curves:

$$\begin{array}{rcl}
E_{d,3} & : & \Delta = -d^3(27d-1) \\
 & & c_4 = 1 - 24d \\
E'_{d,3} & : & \Delta = -d(27d-1)^3 \\
 & & c_4 = 1 + 216d \\
E_{d,5} & : & \Delta = -d^5(d^2+11d-1) \\
 & & c_4 = d^4 + 12d^3 + 14d^2 - 12d + 1 \\
E'_{d,5} & : & \Delta = -d(d^2+11d-1)^5 \\
 & & c_4 = d^4 - 228d^3 + 494d^2 - 12d + 241 \\
E_{d,7} & : & \Delta = d^7(d-1)^7(d^3-8d^2+5d+1) \\
 & & c_4 = d^8 - 12d^7 + 42d^6 - 56d^5 + 35d^4 + 4d + 1 \\
E'_{d,7} & : & \Delta = d(d-1)(d^3-8d^2+5d+1)^7 \\
 & & c_4 = (d^2-d+1)(d^6+229d^5+270d^4-1695d^3+1430d^2-235d+1) \\
E_{d,13} & : & \Delta = d^{13}(d^2+5d+13)^2(28561+15379d+3380d^2+247d^3+d^4)^6(d^2+6d+13)^9 \\
 & & *(-4826809-3712930d-1313806d^2-237276d^3-20618d^4-494d^5+d^6)^6 \\
E'_{d,13} & : & \Delta = d(d^2+5d+13)^2(d^4+7d^3+20d^2+19d+1)^6(d^2+6d+13)^9 \\
 & & *(d^6+10d^5+46d^4+108d^3+122d^2+38d-1)^6
\end{array}$$

The $c_4$ of $E_{d,13}$ and $E'_{d,13}$ are even more complicated then their $\Delta$. The essential information is that if $\ell \nmid d$, $\ell \neq 13$ and $\ell \mid \Delta$ then $\ell \mid c_4$.

Take $p \in \{3, 5, 7, 13\}$. If $\ell$ is a prime dividing $d$ then $c_4 \not\equiv 0 \bmod \ell$, so by [Sil 1, Prop VII.5.1] we obtain that $E_{d,p}$ has multiplicative reduction for all those $\ell$. If one takes the reduced curve one gets $y^2 + xy = x^3$, which has tangent lines $y = 0$ and $y = -x$ at the singular point $(0, 0)$, so these lines are defined over $\mathbb{F}_\ell$ and hence the reduction is split.

We want to compute $c_{E,\ell} = \#(E(\mathbb{Q}_\ell)/E_0(\mathbb{Q}_\ell))$. If $E$ has good reduction then $c_{E,\ell} = 1$. A theorem states ([Sil 1, Thm VIII.6.1], [Tat, p. 46]) that if $E$ has split multiplicative reduction at $\ell$ then $c_{E,\ell} = v_\ell(\Delta(E))$. If $E$ does not have split multiplicative reduction then $c_{E,\ell} \leq 4$. (For a discussion about this see [Sil 1, App. C.15], [Sil 2], [Tat])

**Lemma 2.2.1.** *Take $p \in \{3, 5, 7, 13\}$. Suppose $E = E_{d,p}$. If $p$ divides $c_{E,\ell}$ then there is a split multiplicative reduction at $\ell$ or $p = \ell = 3$.*

*Proof.* If $p \geq 5$ this is obvious (if there were an other type of reduction than split multiplicative reduction then $c_{E,\ell}$ would be smaller then 5).

If 3 divides $c_{E,\ell}$ and the reduction is split multiplicative at $\ell$ then $c_{E,\ell} = 3$. By [Tat] we know that the reduction is additive.

In that case $\ell$ has to divide $24d-1$, hence $\ell$ does not divide $d$. Since $\ell$ is a bad prime, it divides $\Delta$. This implies that $\ell$ divides both $27d-1$ and $24d-1$ hence it divides $3d$, hence $\ell = 3$. $\square$

**Lemma 2.2.2.** *Suppose $E/\mathbb{Q}$ is an elliptic curve. Suppose $\phi : E \to E'$ is an isogeny of degree $m \neq 0$, defined over $\mathbb{Q}$. Suppose that either $E'[2] \not\subset E'(\mathbb{R})$ or $2 \nmid m$. Then $\phi(E(\mathbb{R})) = E'(\mathbb{R})$.*

*Proof.* First consider $[m] : E' \to E'$. We can write $E'(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ or $E'(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $2 \nmid m$ then on both groups multiplication by $m$ is surjective. If $2 \mid m$ then we assumed that $E'(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ and on this group $[m]$ is surjective.

Consider the dual isogeny $\phi' : E' \to E$. Then

$$E'(\mathbb{R}) \stackrel{\phi'}{\to} E(\mathbb{R}) \stackrel{\phi}{\to} E'(\mathbb{R})$$

is the same as multiplication by $m$, hence surjective and we conclude that also $\phi : E(\mathbb{R}) \to E'(\mathbb{R})$ is surjective. $\square$

*Notation* 2.2.3. Suppose $E/\mathbb{Q}$ is an elliptic curve. Suppose $E$ is given by a global minimal equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4 + a_6$$

then we write

$$\begin{aligned} \omega &:= \frac{dx}{y + a_1x + a_3} \\ \Omega_E &:= \int_{E(\mathbb{R})} \omega \end{aligned}$$

(note that $\Omega_E$ doesn't depend on the chosen equation).

**Lemma 2.2.4.** *Take $p \in \{3,5,7,13\}$. Suppose $E = E_{d,p}$ and $E' = E'_{d,p}$. If $p \neq 13$ then $\Omega_E = p\Omega_{E'}$. If $p = 13$ and $E = E_{d,13}$ then $\Omega_E = p\Omega_{E'}$ if the kernel of $\phi : E \to E'$ is contained in $E(\mathbb{R})$ and $p\Omega_E = \Omega_{E'}$ if that kernel is not contained in $E(\mathbb{R})$.*

*Proof.* Take $\omega = dx/(y+a_1x+a_3)$, an invariant differential on $E$, then $\omega' := dx'/(y'+a_1'x'+a_3') = \phi^*\omega$ (the last equality by [Vél]).

Now the kernel of $\phi$ has $p$ elements and $\ker(\phi)\cap E(\mathbb{R})$ has either 1 or $p$ elements. If $\ker(\phi)\cap E(\mathbb{R})$ has only one element then we have $p = 13$.

Suppose $\ker(\phi) \cap E(\mathbb{R})$ has $p$ elements. Take $P \in E'(\mathbb{R})$. The set $\phi^{-1}(P) \cap E(\mathbb{R})$ will have $p$ elements, hence:

$$\Omega_E = \int_{E(\mathbb{R})} |\omega|_\infty = p\int_{\phi(E(\mathbb{R}))} |\omega'|_\infty = p\int_{E'(\mathbb{R})} |\omega'|_\infty = p\Omega_{E'}.$$

Suppose $\ker(\phi) \cap E(\mathbb{R})$ has 1 element. Then $\phi'^*\omega' = [p]^*\omega = p\omega$. Hence:

$$\Omega_{E'} = \int_{E'(\mathbb{R})} |\omega'|_\infty = p\int_{[p](E(\mathbb{R}))} |\omega|_\infty = p\int_{E(\mathbb{R})} |\omega|_\infty = p\Omega_E.$$

$\square$

If $p = 13$ then we know that $\#E(\mathbb{Q})[\phi] = 1 = \#E'(\mathbb{Q})[\phi']$. For the other $p$:

**Lemma 2.2.5.** *Suppose $p \in \{3,5,7\}$, $E = E_{d,p}$ and $\phi : E \to E'$ an isogeny of degree $p$ defined over $\mathbb{Q}$ and $\ker\phi \subset E(\mathbb{Q})$. Then*

$$\frac{\#E'(\mathbb{Q})[\phi']}{\#E(\mathbb{Q})[\phi]} = \frac{1}{p}.$$

*Proof.* We know that $\#E(\mathbb{Q})[\phi] = p$ and $E'(\mathbb{Q})[\phi']$ has either 1 or $p$ elements.

Suppose it has $p$ elements, then $E'(\mathbb{R})[\phi']$ has $p$ elements. Since $\phi : E(\mathbb{R}) \to E'(\mathbb{R})$ is either surjective or the cokernel has two elements, we would have that $E(\mathbb{R})$ has an subgroup of $p$ elements which is not the kernel of the map. Hence $E[p] \subset E(\mathbb{R})$ and this is impossible when $p \in \{3,5,7\}$. $\square$

Now we will prove our main theorem:

**Theorem 2.2.6.** *Take $p \in \{3,5,7,13\}$. For any positive integer $m$ there exist infinitely many non-isomorphic elliptic curves $E$ such that $\dim S^p(\mathbb{Q}, E_{d,p}) \geq m$.*

*Proof.* Take two curves $E$ and $E'$ defined over $\mathbb{Q}$ such that there exists an isogeny $\phi$ of degree $p$, defined over $\mathbb{Q}$. Let $\phi'$ be its dual isogeny.

We want to have large $S^p$ and we will use Cassels' relation:

$$\frac{\#S^{\phi'}(\mathbb{Q}, E')}{\#S^{\phi}(\mathbb{Q}, E)} = \frac{\#E'(\mathbb{Q})[\phi']\Omega_E \prod c_{E,\ell}}{\#E(\mathbb{Q})[\phi]\Omega_{E'} \prod c_{E'\ell}}$$

We need some notation: dim means the dimension over $\mathbb{F}_p$, $s(\phi) = \dim S^{\phi}(\mathbb{Q}, E)$. So we can reformulate the relation and fill in the earlier results:

$$s(\phi') - s(\phi) = (0 \text{ or } \pm 1) + \sum_{\ell} \mathrm{ord}_p(c_{E,\ell}) - \mathrm{ord}_p(c_{E',\ell}),$$

where the sum is taken over all primes $\ell$. (If $p = 13$ we should have the $\pm 1$.)

Let $\mathcal{P}$ be

- the set of all prime numbers bigger then 3 if $p = 3$.
- the set of all prime numbers if $p = 5, 7$.
- the set of all prime numbers except 13 if $p = 13$.

Let $a_p := p$ for $p = 3, 5, 7$ and $a_p = 1$ for $p = 13$.

Take now for $d'$ the product of the first $m + a_p$ elements of $\mathcal{P}$. Then there exist infinitely many primes $p'$ such that (when $d = d'p'$) $27d - 1$ exists of at most 3 primes (when $p = 3$), $d^2 + 11d - 1$ consists of at most 5 primes (when $p = 5$) or $(d^3 - 8d^2 + 5d + 1)$ has at most seven primes when $p = 7$. (See corollary A.0.2, note that this is counted with multiplicity.)

Now we will show that for these $d$, the infinitely many curves $E_{d,p}$ are the ones we were looking for.

If $\ell$ is a prime dividing $d$ then $c_{E,\ell} := p$. Suppose $p = 3, 5, 7$ then it can happen at most $a_p$ times that $p \mid c_{E',\ell}$ if $\ell$ ranges over the primes of bad reduction. If $p = 13$ this will never happen.

Now the exact sequence

$$0 \to \frac{E(\mathbb{Q})[\phi]}{\phi'(E'(\mathbb{Q})[p])} \to S^{\phi'}(\mathbb{Q}, E') \to S^p(\mathbb{Q}, E')$$

will give that (when $p = 3, 5, 7$)

$$s(p) \geq s(\phi') - 1 \geq ((m + a_p + 1) - a_p) - 1 = m$$

or (when $p = 13$)

$$s(p) \geq s(\phi') - 1 \geq (-1 + (m + a_p + 1 - 0)) - 1 = m.$$

Consider the $j$-invariants of the $E'_{d,p}$ (or the $c_4$ and $\Delta$). Fix a $j_0$. There are only a finite number of $E_{d,p}$ with $j$-invariant $j_0$. There are infinitely many $d$'s with $\dim S^p(\mathbb{Q}, E'_{d,p}) \geq m$, hence there are infinitely many non-isomorphic elliptic curves with that property. □

**Corollary 2.2.7.** *In the family $E_{d,p}$ one of the following three possibilities occurs ($p \in \{3, 5, 7, 13\}$):*

1. *For every $m$ there exists infinitely many non-isomorphic elliptic $E$ curves such that the rank of $E$ is bigger then $m$.*
2. *For every $m$ there exists infinitely many non-isomorphic elliptic curves such that the $p$-part of the Shafarevich-Tate group has $\mathbb{F}_p$-dimension bigger then $m$.*
3. *Both (1) and (2) happen.*

*Proof.* Use the following relation:

$$\dim S^p(\mathbb{Q}, E) = r + \dim E(\mathbb{Q})[p] + \dim Ш(\mathbb{Q}, E)[p]$$

with $r$ the rank of $E$. The lefthandside can be arbitrarily large and the middle term of the righthandside will be smaller than or equal to 1. □

## 2.3 $S^2$ and $S^3$ simultaneous large

We will prove a similar proposition as stated in the last section, but now concerning 2 different Selmer groups. We show that $S^2(\mathbb{Q}, E)$ and $S^3(\mathbb{Q}, E)$ get simultaneously large. The importance of this is the following: it is conjectured that there is no upper bound on the rank of elliptic curves. This would mean that all $p$-Selmer groups could become simultaneously arbitrarily big.

**Lemma 2.3.1.** *Suppose $E_d/\mathbb{Q}$ is an elliptic curve given by*

$$E_d : y^2 + (d+1)xy - (d-1)dy = x^3 - (d-1)dx^2$$

*Suppose $p \neq 2, 3$, then:*
*If $p$ divides $d(d-1)$ then $E_d$ has split multiplicative reduction at $p$.*
*If $p$ divides $9d-1$ then $E_d$ has multiplicative reduction at $p$. This reduction is split if and only if $-3$ is a square modulo $p$ (if and only if $p \equiv 1 \bmod 3$).*

*Proof.* Suppose $E_d$ is such an elliptic curve, then this curve has discriminant $d^6(9d-1)(d-1)^3$ and $c_4 = (3d-1)(3d^3-3d^2+9d-1)$. If $p$ divides both $c_4$ and $\Delta$ then $p = 2$ or $p = 3$. In all other cases there is multiplicative reduction at $p$.

Suppose $p$ divides $d$ then

$$\tilde{E}_d : y^2 + xy = x^3$$

hence the singular point is (0,0) and the tangent lines are $y = 0$ and $y = -x$.

Suppose $p$ divides $d-1$ then

$$\tilde{E}_d : y^2 + 2xy = x^3$$

hence the singular point is (0,0) and the tangent lines are $y = 0$ and $y = -2x$.

Suppose $p$ divides $9d-1$. then

$$\tilde{E}_d : y^2 + \frac{10}{9}xy + \frac{8}{81}y = x^3 + \frac{8}{81}x^2$$

hence the singular point is (-4/27,8/243). If we translate this point to $(0,0)$, we have the following equation

$$y^2 + \frac{10}{9}xy = x^3 - \frac{28}{81}x^2$$

The tangent lines at $(0,0)$ are

$$y^2 + \frac{10}{9}xy + \frac{28}{81}x^2 = 0$$

and they are defined over $\mathbb{F}_p$ if and only if $9^2\Delta = 100 - 4 * 28 = -12 = -3 * 2^2$ is a square modulo $p$. This finishes the proof. ☐

**Proposition 2.3.2.** *For every $m$ there exist infinitely many non-isomorphic elliptic curves $E/\mathbb{Q}$ such that the dimension of $S^2(\mathbb{Q}, E)$ and the dimension of $S^3(\mathbb{Q}, E)$ are both bigger then $m$.*

*Proof.* Consider the family of elliptic curves $E_d$:

$$y^2 + (d+1)xy - (d-1)dy = x^3 - (d-1)dx^2.$$

Every elliptic curve in this family has a 6 torsion point. (see proposition 1.1.2, where we replaced $d$ by $d+1$).

We reparametrize the family by setting $d' = 9d - 1$ and we change the coordinates by the transformation $x = u^2x'$ $y = u^3y$, with $u = 1/9$. This leads to our curves $E_d$. The essential data of these curves are:

$$\Delta = 3^6 d(d-8)^3(d+1)^6, \ c_4 = 9(d-2)(d^3 - 6d^2 + 228d - 8).$$

Now we divide out a point of order 2. This gives a curve $E'_d$ with

$$\Delta = 3^6 d^2 (d-8)^6 (d+1)^3,\ c_4 = 9(d+4)(d^3+228d^2+48d+64).$$

and dividing out a point of order 3 gives a curve $E''_d$ with

$$\Delta = 3^6 d^3 (d-8)(d+1)^2,\ c_4 = 9(d-2)(d^3-6d^2-12d-8).$$

Note that for the (square free) $d$'s we will consider, the quantities above will be those associated to a minimal Weierstrass equation at a prime $p$ dividing $d$.

Furthermore one can show that if $p \mid gcd(\Delta, c_4)$ then $p \in \{2,3,241\}$. So these are the only primes, which could give additive reduction.

Now there is a integer $n$ such that for every $a \in \mathbb{Z}$, there exist infinitely many primes $\ell$ such that $(a\ell-8)(a\ell+1)$ has at most $n$ prime divisors. (see corollary A.0.2)

Take $a$ to be the product of the first $m+n+5$ primes bigger then 3 and not equal to 241 and such that -3 is a square modulo every prime dividing $a$. Multiply this by a prime $\tilde{\ell}$ bigger then 3 and different from 241 such that $(a\tilde{\ell}-8)(a\tilde{\ell}+1)$ has at most $n$ prime divisors. Take $d = a\tilde{\ell}$.

The resulting curve $E_d$ has at most $m+2n+6$ bad primes. $m+n+5$ of these primes have $c_{E,\ell} = 1$, $c_{E',\ell} = 2$ and $c_{E'',\ell} = 3$. About $\tilde{\ell}$ we only know that $c_{E,\tilde{\ell}} = 1$. The additive primes (at most 3) have $c_{E,\ell} \mid 12$. The other primes (at most $n+1$ minus the number of additive primes) have $c_{E,\ell} \mid 6$.

Take $\phi$ to be the isogeny coming from dividing out a point of order 3. Now $\dim S^{\phi'}(\mathbb{Q}, E''_d) - \dim S^{\phi}(\mathbb{Q}, E) \leq -(m+n+5-n-1) = -m-4$ and hence by the same exact sequence as used before

$$0 \to \frac{E'(\mathbb{Q})[\phi']}{\phi(E(\mathbb{Q})[p])} \to S^{\phi}(\mathbb{Q}, E) \to S^{p}(\mathbb{Q}, E)$$

we obtain that $\dim S^3(\mathbb{Q}, E_d) \geq m$.

Take $\psi$ to be the isogeny coming from dividing out a point of order 2. Now $\dim S^{\psi'} - \dim S^{\psi} \leq -(m+n+5-n-1-3) = -m-1$ and hence by the same exact sequence as above (replace $\phi$ by $\psi$) we obtain that $\dim S^2(\mathbb{Q}, E_d) \geq m$. □

## 2.4 $S^{11}$ big over a number field

In this section we will prove that 11-Selmer group can be arbitrarily large.

In this section $K$ is always a number field.

**Lemma 2.4.1 ([Sil 2, Exer. V.5.15]).** *Suppose $E/K$ has split multiplicative reduction at $\mathfrak{q}$, $\phi : E \to E'$ is an isogeny of degree $p$. Then*

$$\frac{c_{E,\mathfrak{q}}}{c_{E',\mathfrak{q}}} = p \text{ or } \frac{1}{p}.$$

*Proof.* Since the reduction is split $E$ (resp. $E'$) is isomorphic over $K_{\mathfrak{q}}$ to a Tate curve $E_{q_1}$ (resp. $E_{q_2}$). ([Sil 2, Thm V.5.3])

Note that $c_{E,\mathfrak{q}} = v(\Delta) = v(q_1) > 0$ and $c_{E',\mathfrak{q}} = v(q_2) > 0$.

We have the following model:

$$\frac{\overline{K}^*_{\mathfrak{q}}}{q_1^{\mathbb{Z}}} \xrightarrow{\phi} \frac{\overline{K}^*_{\mathfrak{q}}}{q_2^{\mathbb{Z}}} \xrightarrow{\phi'} \frac{\overline{K}^*_{\mathfrak{q}}}{q_1^{\mathbb{Z}}}$$

The composed map has to come from the isogeny $[p]$ on $E$, hence this is the map $x \mapsto x^p$. There is an $m$ such that replacing $q_2$ by $q_2\zeta_p^m$ gives that one of the maps is the identity map and the other map is $x \mapsto x^p$. By interchanging $q_1$ and $q_2$ i.e., replacing $\phi$ and $\phi'$, if necessary, we can assume that $\phi$ is induced from the identity.

The kernel of $\phi$ will have $p$ elements. Suppose $q_3$ generates the kernel. $\phi$ is surjective so $q_2^{\mathbb{Z}} = \langle q_1, q_3 \rangle$. We can choose $q_3$ in such a way that $v(q_3) \geq 0$

Suppose $v(q_3) = 0$. There is a $k$ with $q_3 = q_2^k$. We have $0 = v(q_3) = kv(q_2)$, so $k = 0$, but then $q_3 = 1$ so it doesn't generate a subgroup of order $p$. So $v(q_3) > 0$.

We know that $\langle q_2 \rangle = \langle q_1, q_3 \rangle$. Hence $q_2 = q_1^k q_3^l$. On the other hand $q_1 = q_2^m$, $q_3^p = q_1^a$, with $1 \le a < p$ and $l < p$. If $l = 0$ then $k = m = 1$ and $a = p$, so $l > 0$.

We have

$$q_2^p = q_1^{kp} q_3^{pl} = q_1^{kp+al} = q_2^{m(kp+al)}$$

so $p = m(kp + al)$. Since $al > 0$, we have $k = 0$ (otherwise $kp + al > p$). So $p = mal$ and $a, l < p$. This gives $a = l = 1$ and $m = p$. We obtain $pv(q_1) = v(q_2)$. ☐

**Proposition 2.4.2.** *Let $E/\mathbb{Q}$ be an elliptic curve. Let $p$ be a prime number, not dividing the minimal discriminant of $E$. Let $K = \mathbb{Q}(E[p])$. Suppose $\mathfrak{q} \subset \mathcal{O}_K$ is a bad prime not dividing $p$. Choose $P \in E(K)$ a point of exact order $p$. Let $E'/K$ be the elliptic curve such that $\phi : E \to E'$ is an isogeny with $\ker(\phi) = \langle P \rangle$. Then, if the reduction is split multiplicative at $\mathfrak{q}$*

$$\frac{c_{E,\mathfrak{q}}}{c_{E',\mathfrak{q}}} = \begin{cases} \frac{1}{p} & \text{if } \ker(\phi) \subset E_0(K) \\ p & \text{if } \ker(\phi) \not\subset E_0(K) \end{cases}$$

*and if the reduction is non-split multiplicative or additive and $p > 3$ then*

$$\frac{c_{E,\mathfrak{q}}}{c_{E',\mathfrak{q}}} = 1.$$

*Proof.* Consider the following commutative and exact diagram (*):

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \langle P \rangle \cap E_0(K_\mathfrak{q}) & \to & \langle P \rangle & \to & H & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & E_0(K_\mathfrak{q}) & \to & E(K_\mathfrak{q}) & \to & E(K_\mathfrak{q})/E_0(K_\mathfrak{q}) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & E'_0(K_\mathfrak{q}) & \to & E'(K_\mathfrak{q}) & \to & E'(K_\mathfrak{q})/E'_0(K_\mathfrak{q}) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & E'_0(K_\mathfrak{q})/\phi(E_0(K_\mathfrak{q})) & \to & E'(K_\mathfrak{q})/\phi(E(K_\mathfrak{q})) & \to & G & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

It is easy to see that $\#G$ and $\#H$ are $p$-th powers and that $H$ has either 1 or $p$ elements. Hence

$$\frac{c_{E,\mathfrak{q}}}{c_{E',\mathfrak{q}}} = \frac{E(K_\mathfrak{q})/E_0(K_\mathfrak{q})}{E'(K_\mathfrak{q})/E'_0(K_\mathfrak{q})} = \frac{\#H}{\#G}$$

is a $p$-th power.

So if the reduction is not split multiplicative at $\mathfrak{q}$ and $p > 3$, this quotient is 1.

We know that $\#H \le p$ and

$$\dim G \le \dim E'(K_\mathfrak{q})/\phi(E(K_\mathfrak{q})) = \dim E(K_\mathfrak{q})[\phi] + v_\mathfrak{q}(p) \dim_{\mathbb{F}_p} \mathbb{F}_v$$

(see [P-S, Lemma 12.10]). So if $\mathfrak{q} \nmid p$, then $\#G \le p$.

If $\mathfrak{q} \nmid p$ then $c_{E,\mathfrak{q}}/c_{E',\mathfrak{q}} = 1/p$ precisely when $H$ has 1 element. This happens precisely when $\ker(\phi) \subset E_0(K)$. ☐

**Theorem 2.4.3.** *For every $m$ there exists infinitely many couples $(E, K)$, where $K$ is a quadratic extension of $\mathbb{Q}$ and $E/K$ an elliptic curve, such that*

$$\dim S^{11}(K, E) \ge m.$$

*Proof.* Consider an elliptic curve given by

$$E_{s,t} : y^2 + (st + t - s^2)xy + s(s-1)(s-t)t^2y = x^3 + s(s-1)(s-t)tx^2$$

where $(t, s)$ is a point on the curve $C : s^2 - s = t^3 - t^2$. The curve $E_{s,t}$ has a point of order 11, namely $(0, 0)$. The discriminant of $E_{s,t}$ is of the form $t^{11}(t-1)^{11}f(t, s)$. Let $E'_{s,t}$ be the curve such that there is an isogeny $\phi : E_{s,t} \to E'_{s,t}$ with $\ker(\phi) = \langle(0, 0)\rangle$.

Suppose $t_0 \in \mathbb{Q}$, $t_0 \neq 0, 1$, (hence there is no $s_0 \in \mathbb{Q}$, with $s_0^2 - s_0 = t_0^3 - t_0^2$). Suppose $(t_0, s_0) \in C(\overline{\mathbb{Q}})$. Then $s_0 = 1/2(1 \pm \sqrt{1 - 4t_0^2 + 4t_0^3})$. Take $s_0 = 1/2(1 + \sqrt{1 - 4t_0^2 + 4t_0^3})$. Suppose $\ell | t$. Then there are two primes $\mathfrak{q}_1, \mathfrak{q}_2$ above $\ell$ in $\mathbb{Q}(s_0)$. Choose them in such a way that $s_0 \equiv 1 \bmod \mathfrak{q}_1$ and $s_0 \equiv 0 \bmod \mathfrak{q}_2$.

Take $\sigma \in Gal(\mathbb{Q}(s_0)/\mathbb{Q}), \sigma \neq id$. Then

$$f(t_0, s_0)\sigma(f(t_0, s_0)) = -t_0^{12}(t_0^5 - 18t_0^4 + 35t_0^3 - 16t_0^2 - 2t_0 + 1).$$

Suppose we have a prime $\mathfrak{q}$ of $\mathbb{Q}(s)$ with $v_\mathfrak{q}(t_0) = 0$ and $v_\mathfrak{q}(f(t_0, s_0)) > 1$, then $\mathfrak{q}$ lies above a prime $\ell$ of $\mathbb{Q}$ with $\ell$ dividing $t_0^5 - 18t_0^4 + 35t_0^3 - 16t_0^2 - 2t_0 + 1$. So by theorem A.0.3 we can find a $t_0 \in \mathbb{Q}$, such that $t_0$ is the product of $m+22$ primes bigger than 3 and $t_0^5 - 18t_0^4 + 35t_0^3 - 16t_0^2 - 2t_0 + 1$ has at most 11 prime divisors in $\mathbb{Q}$.

In $\mathbb{Q}(s_0)$, this would imply that there are at most 22 primes dividing $f(t_0, s_0)$ and not dividing $t_0$.

For any prime $\mathfrak{q}$, dividing $t_0$ and not dividing $s_0$, we have that $v_\mathfrak{q}(j) = -v_\mathfrak{q}(t_0)$. So we have multiplicative reduction at $\mathfrak{q}$. From

$$E_{s,t} : y^2 \equiv x^3 + xy \bmod \mathfrak{q}$$

we see that at $\mathfrak{q}$ the reduction is split multiplicative and the point $(0, 0)$ reduces to the singular point. Hence

$$\frac{c_{E,\mathfrak{q}}}{c_{E',\mathfrak{q}}} = p.$$

If $s_0 \equiv 0 \bmod \mathfrak{q}$ or $t_0 \equiv s_0 \equiv 1 \bmod \mathfrak{q}$, the reduced curve has equation

$$y^2 \pm xy \equiv x^3$$

so $(0, 0)$ is the singular point. So the kernel of $\phi$ reduces to the singular point. This implies

$$\frac{c_{E,\mathfrak{q}}}{c_{E',\mathfrak{q}}} = p \text{ or } 1.$$

For any prime $\mathfrak{q}$ dividing $f(t_0, s_0)$ and not dividing $t_0$, we have that

$$\frac{c_{E,\mathfrak{q}}}{c_{E',\mathfrak{q}}} = \frac{1}{p}, p \text{ or } 1.$$

Since $t_0 > 1$ we have that $4t_0^3 - 4t_0^2 + 1 > 1$. So $\mathbb{Q}(s_0)$ is a real extension and by the same reasoning as in lemma 2.2.4 we obtain

$$\frac{\int_{E(\mathbb{R})} |\omega|}{\int_{E'(\mathbb{R})} |\omega'|} = p$$

and this happens twice.

Since $\mathbb{Q}(s_0)$ is a real extension, we have

$$\frac{E'(\mathbb{Q}(s_0))[\phi']}{E(\mathbb{Q}(s_0))[\phi]} = \frac{1}{p}.$$

By Cassels' relation we have that, if $\phi'$ is the dual of $\phi$, then

$$\dim S^{\phi'}(\mathbb{Q}(s_0), E') \geq (m + 22 - 22) + 2 - 1 = m + 1$$

and hence

$$\dim S^{11}(\mathbb{Q}(s_0), E') \geq m.$$

□

It is likely that the ideas used above can be generalized as follows:

**Conjecture 2.4.4.** *Suppose $E$ is an elliptic curve over the function field of $X_0(p)$ with non-constant $j$-invariant and such that $E$ has a subgroup of order $p$. Then*

$$\sup_{t\in X_0(p)(K),[K:\mathbb{Q}]\leq p+1} \dim S^p(K, E_t) = \infty$$

*where $E_t$ is the specialised curve at $t \in X_0(K)$ and the supremum is taken over all $K$ and $t$.*

*Evidence.* There is a universal family of elliptic curves with a subgroup of order $p$. This is an elliptic surface over $X_0(p)$. Since $X_0(p) \to \mathbb{P}^1$ is a covering of degree $p+1$, we can specialise in extensions $K$ of degree $p+1$. If we take a point of $X_0(K)(p)$ such that the specialised elliptic curve has very many primes dividing its discriminant to the power $p$ and having split multiplicative reduction at these primes, then we would have a proof.

## 2.5 Example

In this section we study a curve which has a nine (or higher) dimensional 3-Selmer group (or bigger) and then compute the 2-Selmer group. The curve we use is a curve with a point of order 6. Such curves are also studied in section 2.3 and we use some results from that section.

First we will give some general information about an explicit 2-descent. The following definitions are from [Sil 1, Ch. X]:

Suppose $E/K$ is given by $y^2 = x^3 + ax^2 + bx$, $E'$ will be given by $y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. Let $S = \{\text{primes dividing } 2b(a^2 - 4b)\} \cup \{\text{primes above } \infty\} = \{\text{primes dividing } 2\Delta\} \cup \{\text{primes above } \infty\}$.

Define $K(S, 2) := \{b \in K^*/K^{*2} \mid \mathrm{ord}_v(b) \equiv 0 \bmod 2 \ \forall v \notin S\}$.

Let $C_t$ be the homogeneous space for $E/K$ given by $tw^2 = t^2 - 2atz^2 + (a^2 - 4b)z^4$.

We have ([Sil 1, X.4.9]):

$$S^\phi(E, K) \cong \{t \in K(S, 2) \mid C_t(K_v) \neq \emptyset \ \forall v \in S\}$$

Take an element $t \in K^*/K^{*2}$. We can take a representant $t' \in K^*$ of $t$ with $ord_v(t') = 0, 1 \ \forall v$ (and $t = \overline{t'} \in K^*/K^{*2}$). The same is valid for elements of $K(S, 2)$. From now on we identify $t \in K(S, 2)$ and a representant $t'$.

**Lemma 2.5.1.** *Suppose $t \in K(S, 2)$, $\mathfrak{p}$ prime of $K$, $\mathfrak{p}$ divides $(t)$ and $\mathfrak{p}$ doesn't divide $(c_1), (c_2)$. Then the equation $t^2 + c_1tz^2 + c_2z^2 - tw^2 = 0$ has no solution in $K_\mathfrak{p}$.*

*Proof.* Suppose $t$ satisfies the hypothesis of the proposition, and suppose $(z, w)$ is a solution of the equation.

The valuations of the 4 summands are

$$1 + 2v(w), 2, 1 + 2v(z), 4v(z).$$

The lowest two have to equal each other. If $v(z) > 0$ then we need $1 + 2v(w) = 2$, which is impossible.

So $v(z) \leq 0$ and we have $2 > 1 + 2v(z) > 4v(z)$. So $1 + 2v(w) = 4v(z)$. But the lefthandside is odd and righthandside even, which gives a contradiction. □

Later on we will do a 2 and a 3-descent on a curve. For this we use a curve with a torsion point of order 6. Consider the curves of the form $y^2 + (d+2)xy - d(d+1)y = x^3 - d(d+1)x^2$. These curves have discriminant $d^3(9d+8)(d+1)^6$.

By a coordinate change we can write the equation for the curve as

$$y^2 = x^3 - (2 + 3d + \frac{3}{4}d^2)x^2 + (d+1)^3 x.$$

The 2-isogenous curve is

$$y^2 = x^3 + (4 + 6d + 4d^2)x^2 + 81d^3(9d+8)x.$$

Take a $t \in \mathbb{Q}(S, 2)$. The associated homogeneous spaces are defined by:

$$C_t : tw^2 = t^2 + (4 + 6d + \frac{3}{2}d^2)tz^2 + 81d^3(9d+8)z^4$$

$$C_t' : tw^2 = t^2 - (8 + 12d + 3d^2)tz^2 + 16(d+1)^3 z^4$$

Now we want to look for fixed $t$ for rational points in $C_t$.

**Lemma 2.5.2.** *Let $p$ be prime, then $p$ cannot divide both $d+1$ and $3d^2 + 12d + 8$. If $p$ divides both $d$ and $3d^2 + 12d + 8$ then $p = 2$. The number $p$ cannot divide both $d$ and $d+1$. If $p$ divides $d+1$ then it doesn't divide $9d+8$.*

*Proof.* The last three statements are trivial. We proof the first one.

Suppose $p$ divides $d+1$. Then $3d^2 + 12d + 8 \equiv 3 - 12 + 8 = -1 \bmod p$. □

**Lemma 2.5.3.** *Suppose $t < 0$, $d > 0$. Then $C_t'(\mathbb{R})$ is empty.*

*Proof.* Suppose $t < 0$, $d > 0$ then all the coefficients on the righthandside are positive and hence every solution will have a $z$ coordinate such that the righthandside is positive. The lefthandside will always be non-positive. This is impossible so there is not a solution. □

Note that the squares modulo 5 are 0,1,4 and the squares modulo 7 are 0,1,2,4. We will use this in the following proposition.

**Proposition 2.5.4.** *Take an elliptic curve $E = E_d$ as above with $d = 5 * 7 * 11 * 13 * 17 * 19 * 23 = 37182145$. Take an elliptic curve $E''$ given by $\psi : E \to E''$ and $\ker(\psi) = \langle 2(0,0) \rangle$. Then $\dim_{\mathbb{F}_3} Ш(\mathbb{Q}, E'')[3] \geq 6$.*

*Proof.* This gives the following decompositions: $9d + 8 = 334639313, d + 1 = 2 * 227 * 81899$ and $3d^2 + 12d + 8 = 1523 * 1080232981 * 2521$. This curve has $c_4 = 9221 * 3716161 * 12097 * 41498278154196893$. Hence the reduction is multiplicative at every bad prime. It is split at every prime $p \neq 334639313$ by lemma 2.3.1. By the same lemma and

$$\left(\frac{-3}{334639313}\right) = -1$$

it follows that the reduction is non-split at 334639313.

**Lemma 2.5.5.** *Suppose $\psi : E \to E'$ is an isogeny with $\ker(\psi) = \langle [2](0,0) \rangle$. Then $\dim S^3(\mathbb{Q}, E') \geq 9$.*

*Proof.* From the information above it follows that $c_{E,\ell}/c_{E',\ell} = 3$ if $\ell$ is a bad prime and $\neq 334639313$. If $\ell = 334639313$ then $c_{E,\ell}/c_{E',\ell} = 1$. For all other $\ell$ the reduction is good and $c_{E,\ell}/c_{E',\ell} = 1$.

There are eleven bad primes. Applying Cassels' relation gives:

$$\dim S^{\phi'}(\mathbb{Q}, E') - \dim S^{\phi}(\mathbb{Q}, E) \geq 10$$

and from this we conclude $\dim S^3(\mathbb{Q}, E') \geq \dim S^{\psi'}(\mathbb{Q}, E') - 1 \geq 9$. □

Set $p_1 = 1080232981, p_2 = 334639313$. Now our set $S$ of bad primes will be

$$\{\infty, 2, 5, 7, 11, 13, 17, 19, 23, 227, 81899, p_2\}.$$

Let $\phi : E \to E''$ be the isogeny of degree 2, as described above and let $\phi'$ be its dual.

Applying the lemmas from above we conclude that $S^{\phi'}(\mathbb{Q}, E'')$ is a subgroup of the group generated by $2, 227, 81899$ (considered as a subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$).

The map $E''(\mathbb{Q})/\phi'(E(\mathbb{Q})) \to S^{\phi'}(\mathbb{Q}, E'')$ will map $(0,0)$ to $d+1$, hence $2 * 227 * 81899$ is in the $\phi'$ Selmer group.

The homogeneous space associated to a $t \in \mathbb{Q}(S, 2)$ is

$$C'_t : tw^2 = t^2 - 1132 * 2521 * p_1 t z^2 + 16(2 * 227 * 81899)^3 z^4.$$

To check whether $t \in \langle 2, 227, 81899\rangle$ is in $S^{\phi'}(\mathbb{Q}, E'')$ we should check whether there is a solution in every $\mathbb{Q}_p$, where $p$ runs over the primes in $S$. To check whether one of these elements is in $S^{\phi'}(\mathbb{Q}, E'')$, we use the following:

**Lemma 2.5.6.** *Suppose we have a prime $\ell$, with $v(t) = v(a) = v(b) = 0$ and $v(a^2 - 4b) > 0$.*

*Suppose also that*

$$\left(\frac{t}{\ell}\right) = -1, \ \left(\frac{-2a}{\ell}\right) = 1$$

*then there are no $(z, w) \in \mathbb{Q}_\ell^2$ with*

$$tw^2 = t^2 + 4atz^2 + 16bz^4 (*)$$

*Proof.* Note that $a^2 \equiv 4b \bmod \ell$, hence $(b/\ell) = 1$.

Suppose such a $(z, w)$ exists, then either one of the following cases occur:

1. $v(z) > 0, v(w) = 0$
2. $v(w) = 2v(z) < 0$
3. $v(z) = v(w) = 0$
4. $v(w) > 0, v(z) = 0$.

Now we handle each of these cases.

If $v(z) > 0$ then $(*)$ will be $w^2 \equiv t \bmod \ell$, so if there is an solution then $(t/\ell) = 1$.

If $v(w) = 2v(z) < 0$ then multiplying $(*)$ by $\ell^{-v(w)}$ and then looking mod $\ell$ gives $tw'^2 \equiv 16bz'^4 \bmod \ell$, so if there is any solution then $(bt/\ell) = 1$, but we have $(bt/\ell) = -1$.

Suppose $v(z) = v(w) = 0$. Consider $(*)$ as a polynomial in $z^2$. This has discriminant

$$16a^2t^2 - 4 * 16b(t^2 - tw^2) \equiv 16t^2(a^2 - 4b) + 4 * 16btw^2 \equiv 64btw^2 \bmod \ell.$$

So this could only have a solution mod $\ell$ when $(bt/\ell) = 1$.

Suppose $v(z) = 0, v(w) > 0$ then $(*)$ considered as a polynomial in $z^2$ has discriminant

$$\Delta \equiv 64btw^2 \equiv 0 \bmod p$$

So $z^2 \equiv \frac{-4at}{32b} \bmod p$ and this is possible when $(-2abt/\ell) = 1$, but we have $(-2abt/\ell) = -1$. $\square$

We are interested in the curve with

$$4a = 1132 * 2521 * p_1, b = 16 * (2 * 227 * 81899)^3$$

This gives

$$\left(\frac{-2a}{5}\right) = \left(\frac{-2a}{7}\right) = 1, \left(\frac{2}{5}\right) = \left(\frac{227}{5}\right) = -1, \left(\frac{2 * 227}{7}\right) = -1.$$

So for $t = 2, 227$ we have that $C'_t(\mathbb{Q}_5)$ is empty and for $t = 2 * 227$ we have that $C'_t(\mathbb{Q}_7)$ is empty.

But by the group law, also $2 * 81899$, $2 * 227$ and $81899$ are not in $S^{\phi'}(\mathbb{Q}, E'')$. Hence $\dim S^{\phi'}(\mathbb{Q}, E'') = 1$ and, by Cassels, $\dim S^{\phi}(\mathbb{Q}, E) = 4$.

An easy computation shows that $\ker\phi \subset E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$, hence $\#\phi(E(\mathbb{Q})[2]) = 1$. We know that $\#E''(\mathbb{Q})[\phi'] = 2$.

We have the following exact sequence

$$0 \to \frac{E''(\mathbb{Q})[\phi']}{\phi(E(\mathbb{Q})[p])} \to \frac{E''(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \to \frac{E(\mathbb{Q})}{pE(\mathbb{Q})} \to \frac{E(\mathbb{Q})}{\phi'(E''(\mathbb{Q}))} \to 0$$

and this gives, with all the data:

$$\begin{aligned} \dim E(\mathbb{Q})/2E(\mathbb{Q}) &= \dim E''(\mathbb{Q})/\phi(E(\mathbb{Q})) + \dim E(\mathbb{Q})/\phi'(E''(\mathbb{Q})) - 1 \\ &\leq \dim S^{\phi}(\mathbb{Q}, E) + \dim S^{\phi'}(\mathbb{Q}, E'') - 1 \leq 4. \end{aligned}$$

Now the rank of $E$ will be at most 3. Since the rank of $E''$ will equal the rank of $E$, we have

$$\dim Ш(\mathbb{Q}, E'')[3] = \dim S^p(\mathbb{Q}, E'') - r \geq 9 - 3 = 6.$$

(Here we used the lower bound on the size of the $p$-Selmer group given in lemma 2.5.5, and that $E''(\mathbb{Q})[3] = \{O\}$.) □

*Remark* 2.5.7. If we want to have large 3-parts of the Ш using the above method, we need to find $d$ and $d+1$ with a large number of prime divisors and the difference between the number of prime divisors of $d$ and $d+1$ small. Then we get automatically huge $S^3$s. To get the $S^2$ small we need to consider a series of quadratic congruences and we can hope, as happens in the above example, that most of them fail.

*Remark* 2.5.8. Cassels ([Cas 1]) proved that $S^3$ and the 3-part of the Ш can be arbitrarily large. He used a family of curves with $j = 0$. His method also applies to the $S^2$ and the 2-part of the Ш. It uses that $E$ has an automorphism of order 2, 3. So it is not usable for other primes $p$.

The method we used, can be used for every $S^p(\mathbb{Q}, E)$. If $E(\mathbb{Q})[2] = \{O\}$, then we can do a 2-descent in $\mathbb{Q}(P)$ (with $[2]P = 0$). We have to try to find a sufficient sharp upperbound for the rank of $E$ over $K$. This would also give an upperbound for the rank over $\mathbb{Q}$.

## 2.6 Combined 2 & 5 descent

In section 2.2 we proved that the 5-Selmer group can be very large. In this section we give some information on computing the 2-Selmer group of the curves used in the proof. This may be used to see how large the $p$-part of the Shafarevich-Tate group can be.

**Proposition 2.6.1.** *Let $E = E_{d,5}$. Suppose $d$ is a product of different primes $p$ bigger then 3 and such that there are at most 5 primes dividing $\Delta$ and not dividing $d$. Suppose $K = \mathbb{Q}(P)$, where $P$ is a point of order 2. Let $E'/K$ be the elliptic curve such that there is an isogeny $\phi : E \to E'$, with* $\ker(\phi) = \{O, P\}$. *Then*

$$|\dim S^{\phi'}(K, E') - \dim S^{\phi}(K, E) - 1| \leq 10$$

*Proof.* $E$ can be given by an equation of the form $y^2 = x^3 + Ax + B =: \tilde{f}(x)$, With

$$A = -27d^4 - 324d^3 - 378d^2 + 324d - 27, B = 54(d^2 + 1)(d^4 + 18d^3 + 74d^2 - 18d + 1)$$

Let $\alpha$ be a root of $\tilde{f}$. Over $K = \mathbb{Q}(\alpha)$ this curve is isomorphic to $y^2 = x^3 + ax^2 + bx = f(x)$, with $a = 3\alpha$, $b = A + 3\alpha^2$. Since $a, b \in \mathbb{Z}[\alpha]$, $a$ and $b$ are in the ring of integers of $K$.

Suppose $p$ divides $d$ then $f \equiv X^3 - 27X + 54 \equiv (X-3)^2(X+6) \bmod p$. If $p$ ramifies completely then $f \equiv (X + a)^3 \bmod p$. This is only possible when $p = 3$.

Suppose $\mathfrak{p}$ divides $a$, $b$ and $d$ then it divides $\alpha$ and $-27 + 3\alpha^2$, so $\mathfrak{p} \mid 3$.

So the primes $p$ with $p \mid d$ can be written as $p = \mathfrak{p}_1^2\mathfrak{p}_2$, with $\alpha \equiv 3 \bmod \mathfrak{p}_1$, $\alpha \equiv -6 \bmod \mathfrak{p}_2$, and

$$b \equiv -27 + 3\alpha^2 \equiv 0 \bmod \mathfrak{p}_1.$$

Suppose $v_{\mathfrak{p}_1}(a) > 0$. Then $v_{\mathfrak{p}_1}(b) = 0$ and $0 = v_{\mathfrak{p}_1}(a^2 - 4b) = 5$, which is impossible. Hence $v_{\mathfrak{p}_1}(a) = 0$.

So we have that $v_{\mathfrak{p}_2}(b) > 0$, hence $v_{\mathfrak{p}_2}(a) = 0$ and $v_{\mathfrak{p}_2}(a^2 - 4b) = 0$.

Now this data gives:

| $v(a)$ | $v(b)$ | $v(a^2-4b)$ | $v(\Delta)$ | $v(\Delta')$ |
|---|---|---|---|---|
| 0 | 0 | 5 | 5 | 10 |
| 0 | 5 | 0 | 10 | 5 |

From this we obtain (it is obvious that at those primes the reduction is split):

$$\frac{c_{E,\mathfrak{p}_1}}{c_{E',\mathfrak{p}_1}} = 2, \text{ and } \frac{c_{E,\mathfrak{p}_2}}{c_{E',\mathfrak{p}_2}} = \frac{1}{2}.$$

There are in $\mathbb{Q}$ at most 5 other bad primes.

If a prime ramifies completely in $\mathbb{Q}(\alpha)$ then we have $c_{E,\mathfrak{q}}/c_{E',\mathfrak{q}} = 1/2$. If a prime ramifies, but not completely we can have $c_{E,\mathfrak{q}_1}c_{E,\mathfrak{q}_2}/(c_{E',\mathfrak{q}_1}c_{E',\mathfrak{q}_2}) = 1$ or $1/4$. If a prime doesn't ramify then we have $\prod c_{E,\mathfrak{q}_i}/c_{E',\mathfrak{q}_i} = 1/8$, but then there at most 4 bad primes.

So

$$|v_2(\prod_{\mathfrak{p}|p, p|\Delta, p\nmid d} \frac{c_{E,\mathfrak{p}}}{c_{E',\mathfrak{p}}})| \leq 10$$

and

$$\frac{E'(\mathbb{Q})[\phi']}{E(\mathbb{Q})[\phi]} = 1 \text{ and } \frac{\Omega_E}{\Omega_{E'}} = 2$$

will finish the proof. □

So we need to determine either $S^\phi$ or $S^{\phi'}$ to determine the size of the $S^2$. Very helpful could be

**Proposition 2.6.2.** *Suppose $E/\mathbb{Q}(\alpha)$ is an elliptic curve as before. Suppose $\mathfrak{q} \mid q$ is a prime with $v(\Delta) > 0, v(d) > 0$ and $v(a) = v(a^2 - 4b) = 0$ (hence $v(b) > 0$, $v(q) = 2$). Suppose $v(t) = 0$. Then*

$$tw^2 = t^2 - 2atz^2 + (a^2 - 4b)z^4 (*)$$

*has no solution in $K_\mathfrak{q}$, when the following conditions are fulfilled*

$$\left(\frac{t}{\mathfrak{q}}\right) = -1, \left(\frac{a}{\mathfrak{q}}\right) = 1.$$

*Proof.* Note that $b \equiv 0 \bmod \mathfrak{q}$, so $(a^2 - 4b/\mathfrak{q}) = 1$ .

Suppose there exists $(z, w)$ with (*), then either one of the following cases occur:

1. $v(z) > 0, v(w) = 0$
2. $v(w) = 2v(z) < 0$
3. $v(z) = v(w) = 0$
4. $v(w) > 0, v(z) = 0.$

If $v(z) > 0$ then $(*) \bmod \ell$

$$w^2 \equiv t,$$

so if there is an solution then $(t/\mathfrak{q}) = 1$, and this not the case.

If $v(w) = 2v(z) < 0$ then looking mod$\mathfrak{q}^{-v(w)}$ gives

$$tw'^2 \equiv (a^2 - 4b)z'^4,$$

so there is no solution when $(t(a^2 - 4b)/\mathfrak{q}) = -1$ and this is not the case.

If $v(z) = v(w) = 0$ the equation (*) has discriminant (considered as polynomial in $z^2$)

$$4a^2t^2 - 4(a^2 - 4b)(t^2 - tw^2) \equiv 4a^2tw^2 \bmod \mathfrak{q}$$

and this has a square root precise when $(t/\mathfrak{q}) = 1$.

If $v(w) > 0, v(z) = 0$ the equation (*) has discriminant (considered as polynomial in $z^2$)

$$4a^2t^2 - 4(a^2 - 4b)t^2 \equiv 0 \bmod \mathfrak{q},$$

so

$$z^2 \equiv \frac{2at}{2(a^2 - 4b)} \equiv \frac{t}{a} \bmod \mathfrak{q}$$

and this has no solution when $(at/\mathfrak{q}) = -1$, so $(a/\mathfrak{q}) = 1$. □

Suppose we manage to determine $K(S, 2)$. Then to exclude some elements we could do the following:

Suppose $p \mid d$, then we can write $p = \mathfrak{p}_1^2\mathfrak{p}_2$. Take $t \in K(S, 2)$. If $v_{p_1}(t) = 1$, then $t \notin K(S, 2)$. So we may assume that $v_{p_1}(t) = 0$. We know that $(a/\mathfrak{p}_1) = (3\alpha/\mathfrak{p}_1) = (9/\mathfrak{p}_1) = 1$, so we need to check whether $(t/\mathfrak{p}_1) = -1$. If this conditions is fulfilled for very many $t \in K(S, 2)$, we would find an upper bound for the rank of $E$ over $K$ and hence we may conclude that $Ш(\mathbb{Q}, E)[5]$ gets arbitrarily large. More precisely, there should be an $f : \mathbb{Z} \to \mathbb{R}$, such that,

$$2 \dim S^\phi(K, E) \leq cm + f(m)$$

with $m$ the number of primes dividing $d$ (in $\mathbb{Q}$) and $\lim_{m\to\infty}(c - 1)m + f(m) = -\infty$.

Unfortunately, we haven't been able to prove this.

# Appendix A

# Sieves

In the proof of theorem 2.2.6 we used the following theorem ([H-R, Thm 9.8]):

**Theorem A.0.1.** *Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $d \geq 1$. Assume that for every prime $p$ there exist a $n \in \mathbb{Z}/p\mathbb{Z}$ such that $\overline{f}(n) \not\equiv 0 \bmod p$.*

*Furthermore assume that if $p$ doesn't divide $f(0)$ and if $p \leq d+1$ then there exist a $n, n' \in \mathbb{Z}$ with $n' \not\equiv n \bmod p$ and $\overline{f}(n) \not\equiv 0 \not\equiv \overline{f}(n') \bmod p$.*

*Then there exist infinitely many primes $p$ such that $f(p)$ consists of at most $2d+1$ prime factors (counted with multiplicity).*

We can obtain the following corollary:

**Corollary A.0.2.** *Suppose $f$ satisfies the properties of the theorem. Then for every $m$ there exists infinitely many numbers $n$ with $m$ distinct prime factors, such that $f(n)$ has at most $2d+1$ prime factors.*

*Proof.* Take $n'$ be the product of the first $m-1$ primes which don't divide $f(0)$. Define $f'(x) := f(n'x)$. It is obvious that $f'$ satisfy the assumption of theorem if $f$ does it. Now there exists infinitely many primes $p$ such that $f'(p) = f(np)$ has at most $2d+1$ prime factors. Since $n := n'p$ has $m$ distinct prime factors, this finishes the proof. □

We used in the proof of theorem 2.3.2 a statement for a product of polynomials:

**Theorem A.0.3.** *If $f$ satisfies the conditions of the theorem above, but is not irreducible, then there exists a constant $r$, depending on the degree of $f$ and the number of irreducible factors in $\mathbb{Q}[X]$, such that there are infinitely many primes $p$ with $f(p)$ having less then $r$ factors ([H-R, Thm 10.6]).*

This theorem also has a corollary of the type above.

# Bibliography


[Cas 1] J.W.S. Cassels, Arithmetic on curves of genus 1 (VI). The Tate-Shafarevich group can be arbitrarly large, *J. Reine Angew. Math* **214/215** (1964), 65-70.

[Cas 2] J.W.S. Cassels, Arithmetic on curves of genus 1 (VIII). On the conjectures of Birch and Swinnerton-Dyer, *J. Reine Angew. Math* **217** (1965), 180-189.

[H-R] H. Halberstam, H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[Maz] B. Mazur, Rational Isogenies of Prime Degree, *Invent. Math* **44** (1978), 129-162.

[Mes] J.-F. Mestre, La méthode des graphes. Examples et aplications, *Proceedings of the international conference on class numbers and fundamental units of algebraic number field*, Katata, 1986.

[P-S] B. Poonen, E.F. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line, *J. Reine Angew. Math* **488** (1977), 141-188.

[Sch] Ed Schaefer, Can the 5-part of the Shafarevich-Tate group of an elliptic curve be arbitrarily large?, Notes available at `http://math.scu.edu/~eschaefe/nt.html`.

[Shi] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, Princeton, 1971.

[Sil 1] J. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, New York, 1986.

[Sil 2] J. Silverman, *Advanced topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer-Verlag, New York, 1994.

[Tat] J. Tate, Algorithm for determining the type of a singular fibre in an elliptic pencil, *Modular functions of one variable IV*, Lecture Notes in Math. **476**, Springer-Verlag, Berlin, 1975.

[Vél] J. Vélu, Isogénies entre courbes elliptiques, *C.R. Acad. Sc. Paris* **273** (1971), 238-241.