THE $p$-PART OF TATE-SHAFAREVICH GROUPS OF ELLIPTIC CURVES
CAN BE ARBITRARILY LARGE

REMKE KLOOSTERMAN

Abstract. In this paper it is shown that for every prime $p > 5$ the dimension of the $p$-torsion in the Tate-Shafarevich group of $E/K$ can be arbitrarily large, where $E$ is an elliptic curve defined over a number field $K$, with $[K : Q]$ bounded by a constant depending only on $p$. From this we deduce that the dimension of the $p$-torsion in the Tate-Shafarevich group of $A/Q$ can be arbitrarily large, where $A$ is an abelian variety, with dim $A$ bounded by a constant depending only on $p$.

1. Introduction

For the notations used in this introduction we refer to Section 2.
The aim of this paper is to give a proof of

Theorem 1.1. There is a function $g : \mathbb{Z} \to \mathbb{Z}$ such that for every prime number $p$ and every $k \in \mathbb{Z}_{>0}$ there exist infinitely many pairs $(E, K)$, with $K$ a number field of degree at most $g(p)$ and $E/K$ an elliptic curve, such that

$$\dim_{\mathbb{F}_p} \text{III}(E/K)[p] > k.$$  

A direct consequence is:

Corollary 1.2. For every prime number $p$ and every $k \in \mathbb{Z}_{>0}$ there exist infinitely many non-isomorphic abelian varieties $A/Q$, with $\dim A \leq g(p)$ and $A$ is simple over $Q$, such that

$$\dim_{\mathbb{F}_p} \text{III}(A/Q)[p] > k.$$  

In fact, a rough estimate using the present proof reveals that $g(p) = O(p^4)$, for $p \to \infty$.

For $p \in \{2, 3, 5\}$, it is known that the group $\text{III}(E/Q)[p]$ can be arbitrarily large. (See [Bo75, Cas64, Fis01 and Kr83] ) So we may assume that $p > 5$, in fact, our proof only uses $p > 3$.

The proof is based on combining the strategy used in [Fis01] to prove that $\dim_{\mathbb{F}_p} \text{III}(E/Q)[5]$ can be arbitrarily large and the strategy used in [KlSc03] to prove that $\dim_{\mathbb{F}_p} \text{S}^p(E/K)$ can be arbitrarily large, where $E$ and $K$ vary, but $[K : Q]$ is bounded by a function depending on $p$ of type $O(p)$.

In [KlSc03] the strategy was to find a field $K$, such that $[K : Q]$ is small and a point $P \in X_0(p)(K)$ such that $P$ reduces to one cusp for many primes $p$ and reduces to the other cusp for very few primes $p$. Then to $P$ we can associate an elliptic curve $E/K$ such that an application of a Theorem of Cassels ([Cas65]) shows that $S^p(E/K)$ gets large.

The strategy of [Fis01] can be described as follows. Suppose $K$ is a field with class number 1. Suppose $E/K$ has a $K$-rational point of order $p$, with $p > 3$ a prime number. Let $\varphi : E \to E'$ be the isogeny obtained by dividing out the point of order $p$. Then one can define a matrix $M$, such that the $\varphi$-Selmer group is isomorphic to the kernel of multiplication on the left by $M$, while the $\hat{\varphi}$-Selmer group is isomorphic to the kernel of multiplication on the right by $M$. One can then
show that the rank of $E(K)$ and of $E'(K)$ is bounded by the number of split multiplicative primes minus twice the rank of $M$ minus 1.

Moreover, one can prove that if the matrix $M$ is far from being square, then the dimension of the $p$-Selmer group of one of the two isogenous curves is large. If one has an elliptic curve with two rational torsion points of order $p$ and $q$ respectively, one can hope that for one isogeny the associated matrix has high rank, while for the other isogeny the matrix is far from being square. Fisher uses points on $X(5)$ to find elliptic curves $E/\mathbb{Q}$ with two isogenies, one such that the associated matrix has large rank, and the other such that the 5-Selmer group is large.

We generalize this idea to number fields, without the class number 1 condition. To do this we express the Selmer group attached to the isogeny as the kernel of the multiplication on the left by some matrix $M$. In general, the matrix for the dual isogeny turns out to be different from the transpose of $M$.

Remark 1.3. An element of $S^p(E/K)$ corresponds to a Galois extension $L$ of $K(E[p])$ of degree $p$ or $p^2$, satisfying certain local conditions and such that the Galois group of $L/K(E[p])$ interacts in some prescribed way with the Galois group of $K(E[p])/K$. The examples of elliptic curves with large Selmer and large Tate-Shafarevich groups in [Fis01], [KlSc03] and this paper have one thing in common, namely that the representation of the absolute Galois group of $K$ minus twice the rank of $M$ from Section 2 to prove Theorem 1.1.

In general, the matrix for the dual isogeny turns out to be different from the transpose of $M$.

The organization of this paper is as follows: In Section 2 we prove several lower and upper bounds for the size of $\varphi$-Selmer groups, where $\varphi$ is an isogeny with kernel generated by a rational point of prime order at least 5. In Section 2 we use the modular curve $X(p)$ and the estimates from Section 2 to prove Theorem 1.1.

2. Selmer groups

Suppose $K$ is a number field, $E/K$ is an elliptic curve and $\varphi : E \to E'$ is an isogeny defined over $K$. Let $H^1(K,E[\varphi])$ be the first cohomology group of the Galois module $E[\varphi]$.

Definition 2.1. The $\varphi$-Selmer group of $E/K$ is

$$S^\varphi(E/K) := \ker H^1(K,E[\varphi]) \to \prod_{p \text{ prime}} H^1(K_p,E).$$

and the Tate-Shafarevich group of $E/K$ is

$$\Sha(E/K) := \ker H^1(K,E) \to \prod_{p \text{ prime}} H^1(K_p,E).$$

Notation 2.2. For the rest of this section fix a prime number $p > 3$, a number field $K$ such that $\zeta_p \in K$ and an elliptic curve $E/K$ such that there is a non-trivial point $P \in E(K)$ of order $p$. Let $\varphi : E \to E'$ be the isogeny obtained by dividing out $(P)$.

To $\varphi$ we associate three sets of primes. Let $S_1(\varphi)$ be the set of split multiplicative primes, not lying above $p$, such that $P$ is not in the kernel of reduction. Let $S_2(\varphi)$ be the set of split multiplicative primes, not lying above $p$, such that $P$ is in the kernel of reduction. Let $S_3(\varphi)$ be the set of primes above $p$.

Suppose $S$ is a finite sets of finite primes. Let

$$K(S,p) := \{ x \in K^*/K_0^p \mid v_p(x) \equiv 0 \text{ mod } p \forall p \notin S \}.$$ 

Let $H^1(K,M;S)$ the subgroup of $H^1(K,M)$ of all cocycles not ramified outside $S$.

For any cocycle $\xi \in H^1(K,M)$ denote $\xi_p := res_p(\xi) \in H^1(K_p,M)$. Let $\delta_p$ be the boundary map

$$E'(K_p)/\varphi(E(K_p)) \to H^1(K_p,E[\varphi]).$$
Let $C_K$ denote the class group of $K$.

Note that $S_1(\hat{\varphi}) = S_2(\varphi)$ and $S_2(\hat{\varphi}) = S_1(\varphi)$.

**Proposition 2.3.** We have 
\[ S^\varphi(E/K) = \{ \xi \in H^1(K, E[\varphi]; S_1(\varphi) \cup S_3(\varphi)) | \xi_p = 0 \forall p \in S_2(\varphi) \text{ and } \xi_p \in \delta_p(E'(K_p)/\varphi(E(K_p))) \forall p \in S_3(\varphi) \}. \]

**Proof.** Note that if $p$ divides the Tamagawa number $c_{E,p}$ then the reduction at $p$ is split multiplicative. If this is the case then $c_{E,p}/c_{E',p} \neq 1$. This combined with $\dim H^1(K_p, E[\varphi]) \leq 2$ (for $p \nmid (p)$) and [Sch90] Lemma 3.8 gives that $\iota_p^* : H^1(K_p, E[\varphi]) \to H^1(K_p, E)$ is either injective or the zero-map. A closer inspection of [Sch90] Lemma 3.8 combined with [KSc03] Proposition 3 shows that $\iota_p^*$ is injective if and only if $p \in S_2(\varphi)$.

The Proposition follows then from [ScSt01] Proposition 4.6. \hfill \Box

**Proposition 2.4.** We have 
\[ S^\varphi(E/K) \subset \{ x \in K(S_1(\varphi) \cup S_3(\varphi), p) | x \in K_p^\times \forall p \in S_2(\varphi) \} \]
and 
\[ S^\varphi(E/K) \supset \{ x \in K(S_1(\varphi), p) | x \in K_p^\times \forall p \in S_2(\varphi) \cup S_3(\varphi) \}. \]

**Proof.** This follows from the identification $E[\varphi] \cong \mathbb{Z}/p\mathbb{Z} \cong \mu_p$, the fact $H^1(L, \mu_p) \cong L^* / L^p$ for any field $L$ of characteristic different from $p$, and Proposition 2.3. \hfill \Box

**Definition 2.5.** Let $S_1$ and $S_2$ be two disjoint finite sets of finite primes of $K$, such that none of the primes in these sets divides $(p)$.

Let 
\[ T : K(S_1, p) \to \bigoplus_{p \in S_2} O^*_p / O^*_p \]
be the $\mathbb{F}_p$-linear map induced by inclusion.

Let $m(S_1, S_2)$ be the rank of $T$.

In the special case of an isogeny $\varphi : E \to E'$ with associated sets $S_1(\varphi)$ and $S_2(\varphi)$ as above we write $m(\varphi) := m(S_1(\varphi), S_2(\varphi))$.

Note that $K$ does not admit any real embedding. So 
\[ \dim K(S, p) = \frac{1}{2}[K : Q] + \#S + \dim_{F_p} C_K[p] \]
for any set of finite primes $S$.

**Proposition 2.6.** We have 
\[ \#S_1(\varphi) - \#S_2(\varphi) + \dim_{F_p} C_K[p] - \frac{1}{2}[K : Q] \leq \dim S^\varphi(E/K) \leq \#S_1(\varphi) + \dim_{F_p} C_K[p] - m(\varphi) + \frac{3}{2}[K : Q]. \]

**Proof.** Using Proposition 2.4 twice we obtain 
\[ \frac{1}{2}[K : Q] + \#S_1(\varphi) + \dim_{F_p} C_K[p] - \#S_2(\varphi) \leq \dim K(S_1(\varphi), p) - \#S_2(\varphi) - \#S_3(\varphi) \leq \dim S^\varphi(E/K) \leq \dim K(S_1(\varphi) \cup S_3(\varphi), p) - m(\varphi) \leq \#S_1(\varphi) + \#S_3(\varphi) + \dim_{F_p} C_K[p] - m(\varphi) + \frac{1}{2}[K : Q] \leq \#S_1(\varphi) + \dim_{F_p} C_K[p] - m(\varphi) + \frac{3}{2}[K : Q]. \] \hfill \Box

**Lemma 2.7.** We have 
\[ \text{rank } E(K) \leq \#S_1(\varphi) + \#S_2(\varphi) + 2 \dim C_K[p] + 3[K : Q] - m(\varphi) - m(\hat{\varphi}) - 1. \]
Proof. Note
\[
1 + \text{rank } E(K) \leq \dim_{\mathbb{F}_p} E(K)/pE(K) \leq \dim S^p(E/K) \leq \dim S^\varphi(E/K) + \dim S^\varphi(E'/K)
\]
\[
\leq \#S_1(\varphi) + \#S_1(\hat{\varphi}) + 2 \dim C_K[p] + 3|K : \mathbb{Q}| - m(\varphi) - m(\hat{\varphi}),
\]
which proves the Lemma. \hfill \square

By a theorem of Cassels we can compute the difference of \(\dim S^\varphi(E/K)\) and \(\dim S^\varphi(E'/K)\). We do not need the precise difference, but only an estimate, namely

**Lemma 2.8.** There is an integer \(t\), with \(|t| \leq 2|K : \mathbb{Q}| + 1\) such that
\[
\dim S^\varphi(E'/K) = \dim S^\varphi(E/K) - \#S_1(\varphi) + \#S_2(\varphi) + t.
\]

**Proof.** This follows from [Cas65] and [Klo03] Proposition 3. \hfill \square

**Lemma 2.9.**
\[
\dim S^\varphi(E/K) + \dim S^\varphi(E'/K) \geq |\#S_1(\varphi) - \#S_2(\varphi)| + 2 \dim_{\mathbb{F}_p} C_K[p] - 3|K : \mathbb{Q}| - 1.
\]

**Proof.** We may assume that \(\#S_1 \geq \#S_2\). From Proposition 2.10 we know
\[
\dim S^\varphi(E/K) \geq \#S_1(\varphi) - \#S_2(\varphi) + \dim_{\mathbb{F}_p} C_K[p] - \frac{1}{2}|K : \mathbb{Q}|.
\]
From this inequality and Lemma 2.8 we obtain that
\[
\dim S^\varphi(E'/K) \geq \dim S^\varphi(E/K) - 2|K : \mathbb{Q}| - 1 - \#S_1(\varphi) + \#S_2(\varphi) \geq \dim_{\mathbb{F}_p} C_K[p] - \frac{5}{2}|K : \mathbb{Q}| - 1.
\]
Summing both inequalities gives the Lemma. \hfill \square

**Lemma 2.10.** Suppose \(\dim S^\varphi(E/K) + \dim S^\varphi(E'/K) = k + 1\) and \(\text{rank } E(K) = r\), then
\[
\max(\dim \text{III}(E/K)[p], \dim \text{III}(E'/K)[p]) \geq \frac{(k - r)}{2}.
\]

**Proof.** This follows from the exact sequence
\[
0 \to E'(K)[\hat{\varphi}]/\varphi(E(K)[p]) \to S^\varphi(E/K) \to S^p(E/K) \to S^\varphi(E'/K) \to \text{III}(E'/K)[\hat{\varphi}]/\varphi(\text{III}(E/K)[p]).
\]
(See [ScSt01] Lemma 9.1.) \hfill \square

**Lemma 2.11.** Let \(\psi : E_1 \to E_2\) be some isogeny obtained by dividing out a \(K\)-rational point of order \(p\), with \(E_1\) an elliptic curve in the \(K\)-isogeny network of \(E\). Then
\[
\max(\dim \text{III}(E/K)[p], \dim \text{III}(E'/K)[p]) \geq -\min(\#S_1(\varphi), \#S_2(\varphi)) - 3|K : \mathbb{Q}| - 1 + \frac{1}{2}(m(\psi) + m(\hat{\psi})).
\]

**Proof.** Use Lemma 2.10 for the isogeny \(\psi\) to obtain the bound for the rank of \(E(K)\). Then combine this with Lemma 2.9 and Lemma 2.10 and use that
\[
\#S_1(\varphi) + \#S_2(\varphi) = \#S_1(\psi) + \#S_2(\psi).
\]
\hfill \square

3. Modular curves

In this section we prove Theorem 1.1. The following result will be used in the proof of Theorem 1.1.

**Theorem 3.1** ([Har73] Theorem 10.4). Let \(f \in \mathbb{Z}[X]\) be a polynomial of degree at least 1. Suppose that for every prime \(\ell\), there exists a \(y \in \mathbb{Z}/\ell\mathbb{Z}\) such that \(f(y) \not\equiv 0 \mod \ell\). Then there exists a constant \(n\) depending on the degree of \(f\) and the degree of its irreducible factors such that
there exist infinitely many primes \( \ell \), such that \( f(\ell) \) has at most \( n \) prime factors. Moreover, there exist \( \delta > 0, d \in \mathbb{Z} \), such that

\[
\# \{ y \in \mathbb{Z} \mid 0 \leq y \leq x \text{ and the number of prime factors of } f(y) \leq n \} \leq \delta \frac{x}{\log^d x} \left( 1 + O \left( \frac{1}{\sqrt{\log(x)}} \right) \right)
\]
as \( x \to \infty \).

**Notation 3.2.** Denote \( X(p)/\mathbb{Q} \) the curve parameterizing triples \( (E, Q_1, Q_2) \) with \( \{Q_1, Q_2\} \) an ordered basis for \( E[p] \).

By the work of Vélu (see [Vélu78, [Fish10] Chapter 4]) there exists cusps of \( X(p) \) defined over \( \mathbb{Q} \). Fix a cusp \( T_0 \in X_p(\mathbb{Q}) \). Let \( R_1 \in X_0(p) \) be the unramified cusp, let \( R_2 \in X_0(p) \) be the ramified cusp.

Let \( \tilde{\pi}_i : X(p) \to X_0(p) \) be the morphisms obtained by mapping \( (E, Q_1, Q_2) \) to \( (E, \langle Q_i \rangle) \).

Let \( \pi_i : X(p) \to X_0(p) \) be either \( \tilde{\pi}_i \) or \( \tilde{\pi}_i \) composed with the Atkin-Lehner involution on \( X_0(p) \), such that \( \pi_i(T_0) = R_1 \).

Let \( P \in X(p) \) a point, not a cusp. Denote \( \varphi_{P,i} \) the morphism corresponding to \( \pi_i(P) \).

Note that the maps \( \pi_i \) are defined over \( \mathbb{Q} \).

**Definition 3.3.** Let \( T \) be a cusp of \( X(p) \). We say that \( T \) is of type \( (\delta, \epsilon) \in \{1, 2\}^2 \) if \( \pi_1(T) = R_3 \) and \( \pi_2(T) = R_\epsilon \).

Note that being of type \( (\delta, \epsilon) \) is invariant under the action of the absolute Galois group of \( \mathbb{Q} \).

For all points \( P \in X(p)(\overline{\mathbb{Q}}) \) and all primes \( p \mid (p) \) of \( \overline{\mathbb{Q}} \) such that \( P = T \) mod \( p \) implies that \( p \in S_\delta(\varphi_{P_1}, \varphi_{P_2}) \).

**Proof of Theorem 3.1.** Fix a component \( Y \) of \( X(p)/\mathbb{Q}(\zeta_p) \). Fix a (possibly singular) model \( C_1 \) for \( Y \) in \( \mathbb{P}^2 \), such that the line \( X = 0 \) intersects \( C_1 \) only in cusps of type \( (1, 1) \) and no other point, all \( x \)-coordinates of other the cusps are distinct and finite, if two \( x \)-coordinates of cusps are conjugate under \( \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \), then the type of these cusps coincide and all \( y \)-coordinates of the cusps are finite. Let \( C = \cup_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})} C_1^\sigma \). Then \( C/\mathbb{Q} \) is a model for \( X(p) \).

Denote \( h \) the defining polynomial of \( C \).

Let \( f_{\delta, \epsilon} \in \mathbb{Z}[X] \) be the radical polynomial with as roots all \( x \)-coordinates of the cusps of type \( (\delta, \epsilon) \) of \( X(p) \) and content 1. After a transformation of the form \( x \to cx \), we may assume that \( f_{1,2}(0)/f_{2,2}(0) = 1 \) and \( f_{1,2}f_{2,2} \in \mathbb{Z}[X] \). Let \( n \) denote the constant of Theorem 3.1 for the polynomial \( f_{1,2}f_{2,2} \). Note that the discriminant of \( f_{1,1}f_{1,2}f_{2,1}f_{2,2} \) is non-zero.

Let \( B \) consist of \( p \), all primes \( \ell \) dividing the leading coefficient or the discriminant of \( f_{1,1}f_{1,2}f_{2,1}f_{2,2} \), all primes \( \ell \) smaller then the degree of \( f_{1,2}f_{2,2} \) and all primes dividing the leading coefficient of \( \text{res}(h, f_{2,1}, x) \).

Let \( \mathcal{P}_2 \) be the set of primes not in \( B \) such that every irreducible factor of \( f_{2,1}(x)(x^p - 1) \) mod \( \ell \) and every irreducible factor of \( \text{res}(h, f_{2,1}, x) \mod \ell \) has degree 1. Note that by Frobenius’ Theorem [SilLe00] the set \( \mathcal{P}_2 \) is infinite. The condition mentioned here, implies that if we take a triple \( (x_0, \ell, y_0) \) with \( x_0 \in \mathbb{Z} \), the prime \( \ell \in \mathcal{P}_2 \) divides \( f_{2,1}(x_0) \) and \( y_0 \) is a zero of \( h(x_0, y) \) then every prime \( q \) of \( \mathbb{Q}(\zeta_p, y_0) \) over \( \ell \) satisfies \( f(q/\ell) = 1 \).

Fix \( S_1 \) and \( S_2 \) two sets of primes, such that

\[
m(S_1, S_2) = 2k + 4(n + 3) \deg(h)(p - 1) + 2,
\]

\( S_1 \cap B = \emptyset \) and \( S_2 \subset \mathcal{P}_2 \). (The existence of such sets follows from Dirichlet’s theorem on primes in arithmetic progression and the fact that \( \ell \in S_2 \) implies \( \ell \equiv 1 \mod p \).)

**Lemma 3.4.** There exists an \( x_0 \in \mathbb{Z} \) such that

- \( x_0 \equiv 0 \mod \ell \), for all primes \( \ell \) smaller then the degree of \( f_{1,2}f_{2,2} \) and all \( \ell \) dividing the leading coefficient of \( f_{1,2}f_{2,2} \).
\begin{itemize}
  \item \(x_0 \equiv 0 \mod \ell\), for all \(\ell \in \mathcal{S}_1\),
  \item \(f_{2,1}(x_0) \equiv 0 \mod \ell\), for all \(\ell \in \mathcal{S}_2\),
  \item \(f_{1,2}(x_0)f_{2,2}(x_0)\) has at most \(n\) prime divisors.
  \item \(h(x_0,y)\) is irreducible.
\end{itemize}

**Proof.** The existence of such an \(x_0\) can be proven as follows. Take an \(a \in \mathbb{Z}\) satisfying the above three congruence relations. Take \(b\) to be the product of all primes mentioned in the above congruence relations. Define \(\tilde{f}(Z) = f_{1,2}(a+b\mathbb{Z})f_{2,2}(a+b\mathbb{Z})\). We claim that the content of \(\tilde{f}\) is one. Suppose \(\ell\) divides this content. Then \(\ell\) divides the leading coefficient of \(\tilde{f}\). From this one deduces that \(\ell\) divides \(b\). We distinguish several cases:

\begin{itemize}
  \item If \(\ell \in \mathcal{S}_1\) then \(f_{1,2}(a) \equiv 0 \mod \ell\) and \(\ell\) does not divide the discriminant of the product of \(f_{\delta,r}\), so we have \(\tilde{f}(0) \equiv f_{1,2}(a)f_{2,2}(a) \neq 0 \mod \ell\).
  \item If \(\ell\) divides \(b\) and is not in \(\mathcal{S}_1 \cup \mathcal{S}_2\) then \(\tilde{f}(0) \equiv f_{1,2}(0)f_{2,2}(0) = 1 \mod \ell\).
\end{itemize}

So for all primes \(\ell\) dividing \(b\) we have that \(\tilde{f} \neq 0 \mod \ell\). This proves the claim on the content of \(\tilde{f}\).

Suppose \(\ell\) is a prime smaller than the degree of \(\tilde{f}\), then \(\tilde{f}(0) \equiv 1 \mod \ell\). If \(\ell\) is different from these primes, then there is a coefficient of \(\tilde{f}\) which is not divisible by \(\ell\) and the degree of \(\tilde{f}\) is smaller than \(\ell\). So for every prime \(\ell\) there is an \(z_\ell \in \mathbb{Z}\) with \(\tilde{f}(z_\ell) \neq 0 \mod \ell\). From this we deduce that we can apply Theorem 3.1. The constant for \(\tilde{f}\) depends only on the degree of the irreducible factors of \(\tilde{f}\), hence equals \(n\). The set

\[\{x_1 \in \mathbb{Z} \mid \tilde{f}(x_1)\text{ has at most } n\text{ prime divisors}\}\]

is not a thin set. So

\[\mathcal{H} := \{x_1 \in \mathbb{Z} \mid \tilde{f}(x_1)\text{ has at most } n\text{ prime divisors and } h(a+bx_1, y)\text{ is irreducible}\}\]

is not empty by Hilbert’s Irreducibility Theorem [Ser89, Chapter 9].) Fix such an \(x_1 \in \mathcal{H}\). Let \(x_0 = a + bx_1\). This proves the claim on the existence of such an \(x_0\). \(\square\)

Fix an \(x_0\) satisfying the conditions of Lemma 3.1. Adjoin a root \(y_0\) of \(h(x_0, y)\) to \(\mathbb{Q}(\zeta_p)\). Denote the field \(\mathbb{Q}(\zeta_p, y_0)\) by \(K_1\). Let \(P\) be the point on \(X(p)(K_1)\) corresponding to \((x_0, y_0)\). Let \(E/K_1\) be the elliptic curve corresponding to \(P\). Let \(K = K_1(\sqrt{\epsilon_p(E)})\). Then if \(q\) is a prime such that \(E/K_q\) has multiplicative reduction, then \(E/K_\infty\) has split multiplicative reduction.

For every prime \(p\) of \(K\) over \(\ell \in \mathcal{S}_1\) we have that \(P \mod q\) is a cusp of type \((1,1)\). Over every prime \(\ell \in \mathcal{S}_2\) there exists a prime \(q\) such that \(P \mod q\) is a cusp of type \((2,1)\). From our assumptions on \(x_0\) it follows that \(p\) does not divide \(f(q/\ell)\). Let \(T_1\) consists of the primes of \(K\) lying over the primes in \(\mathcal{S}_1\). Let \(T_2\) be the set of primes \(q\) such that \(q\) lies over a prime in \(\mathcal{S}_2\) and \(P \mod q\) is a cusp of type \((2,1)\).

Note that the set of primes of \(K\) such that \(P\) reduces to a cusp of type \((*,2)\) has at most \(n[K: \mathbb{Q}]\) elements.

We have the following diagram

\[\begin{array}{ccc}
\mathbb{Q}(\mathcal{S}_1, p) & \rightarrow & \oplus_{\ell \in \mathcal{S}_2} \mathbb{Z}_\ell^p / \mathbb{Z}_\ell^{p} \\
\downarrow & & \downarrow \\
K(T_1, p) & \rightarrow & \oplus_{q \in T_2} \mathcal{O}_{K_\infty}^p / \mathcal{O}_{K_\infty}^{p}.
\end{array}\]

Since \(p \nmid f(q/\ell)\) for all \(\ell \in \mathcal{S}_2\), the arrow in the right column is injective. This implies

\[m(\varphi_{p,1}/K) \geq m(T_1, T_2) \geq m(S_1, S_2) = 2k + 4(n + 3) \deg(h)(p - 1) + 2.\]
Since \( S_2(\varphi_{p,2}/K) \leq [K : Q] n \) and \([K : Q] \leq 2(p − 1) \deg(h)\) we obtain by Lemma 2.11 that for some \( E' \) isogenous to \( E \) we have

\[
\dim_{F_p} \text{III}(E'/K)[p] \geq -\#S_2(\varphi_{p,2}) - \frac{3[K : Q]}{2} - 1 + \frac{1}{2}m(S_1, S_2) \geq (n + 3)[K : Q] - 1 + \frac{1}{2}m(S_1, S_2) = k.
\]

Note that \( \deg(h) \) can be bounded by a function of type \( O(p^3) \), hence \([K : Q]\) can be bounded by a function of type \( O(p^4) \).

To finish, we prove Corollary 1.2.

**Proof of Corollary 1.2.** Let \( E/K \) be an elliptic curve such that \( \dim \text{III}(E/K)[p] \geq kg(p) \) and \([K : Q] \leq g(p)\).

Let \( R := \text{Res}_{K/Q}(E) \) be the Weil restriction of scalars of \( E \). Then by [Mi72, Proof of Theorem 1] \( \dim \text{III}(R/Q)[p] = \dim \text{III}(E/K)[p] \).

From this it follows that there is a factor \( A \) of \( R \), with \( \dim \text{III}(A/Q)[p] \geq k \). \( \square \)

**References**

[Böl75] R. Bölling, Die Ordnung der Schafarewitsch-Tate Gruppe kann beliebig groß werden, *Math. Nachr.* 67 (1975), 157–179.

[Cas64] J.W.S. Cassels, Arithmetic on Curves of Genus 1 (VI). The Tate-Šafarevič group can be arbitrarily large, *J. Reine Angew. Math.* 214/215 (1964), 65–70.

[Cas65] 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.

[Fis00] T. Fisher, *On 5 and 7 descents for elliptic curves*, PhD Thesis, Cambridge, 2000.

[Fis01] T. Fisher, Some examples of 5 and 7 descent for elliptic curves over \( Q \), *J. Eur. Math. Soc.* 3 (2001) 169–201.

[HaRi74] H. Halberstam, H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[KlSc03] R. Kloosterman, E.F. Schaefer, Selmer groups of elliptic curves that can be arbitrarily large, *J. Number Theory* 99 (2003), 148–163.

[Kr83] K. Kramer, A family of semistable elliptic curves with large Tate-Shafarevich groups, *Proc. Amer. Math. Soc.* 89 (1983), 379–386.

[Mi72] J. S. Milne, On the arithmetic of abelian varieties, *Invent. Math.* 17 (1972), 177–190.

[Ser89] J.-P. Serre, *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1989.

[Sch96] E.F. Schaefer, Class groups and Selmer groups, *J. Number Theory* 56 (1996), 79–114.

[ScSt01] E.F. Schaefer and M. Stoll, How to do a \( p \)-descent on an elliptic curve, preprint, 2001.

[StLe96] P. Stevenhagen, H.W. Lenstra, Jr, Chebotarëv and his density theorem, *Math. Intelligencer* 18 (1996), 26–37.

[Vélu78] J. Vélu, *Courbes elliptiques munies d’un sous-groupe \( Z/nZ \times \mu_n \).* Bull. Soc. Math. France Mém. No. 57, 1978.