Journal de Théorie des Nombres
de Bordeaux **17** (2005), 787–800

The p-part of Tate-Shafarevich groups of elliptic curves can be arbitrarily large

par Remke KLOOSTERMAN

Résumé. Nous montrons dans ce papier que pour chaque nombre premier $p \geq 5$, la dimension de la partie de p-torsion du groupe de Tate et Shafarevich, Ш(E/K), peut être arbitrairement grande, où E est une courbe elliptique définie sur un corps de nombres K de degré borné par une constante dépendant seulement de p. En utilisant ce résultat, nous obtenons aussi que la partie de p-torsion du Ш$(A/\mathbb{Q})$ peut être arbitrairement grande, pour des variétées abéliennes A de dimension bornée par une constante dépendant seulement de p.

Abstract. In this paper we show that for every prime $p \geq 5$ 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 $[K : \mathbb{Q}]$ 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 $A/\mathbb{Q}$ 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*

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

Manuscrit reçu le 13 octobre 2003.

Mots clefs. Tate-Shafarevich group, elliptic curve, abelian variety.

The author wishes to thank Jaap Top and Bas Edixhoven for many useful conversations on this topic. The author wishes to thank Jasper Scholten for suggesting [10]. The author wishes to thank Stephen Donnelly and René Schoof for pointing out mistakes in earlier versions and an anonymous referee for suggesting many improvements.

The proof of this theorem starts on page 796. Using Weil restriction of scalars, we obtain as a direct consequence:

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

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

In fact, a rough estimate using the present proof reveals that $g(p) = O(p^4)$. It is an old open question whether $g(p)$ can be taken 1, i.e., for any p, the p-torsion of the Tate-Shafarevich groups of elliptic curves over $\mathbb{Q}$ are unbounded.

For $p \in \{2, 3, 5\}$, it is known that the group $Ш(E/\mathbb{Q})[p]$ can be arbitrarily large. (See [1], [2], [5] and [8].) So we may assume that $p > 5$, in fact, our proof only uses $p > 3$.

P.L. Clark communicated to the author that he proved by different methods that if E/K has full p-torsion then $Ш(E/L)[p]$ can be arbitrarily large if L runs over all extension of K of degree p, but E remains fixed. This gives a sharper bound in the case that E has potential complex multiplication. The elliptic curves we describe in the proof of Theorem 1.1 all have many primes $\mathfrak{p}$ for which the reduction at $\mathfrak{p}$ is split-multiplicative. Hence these curves do *not* have potential complex multiplication.

The proof of Theorem 1.1 is based on combining the strategy used in [5] to prove that $\dim_{\mathbb{F}_5} Ш(E/\mathbb{Q})[5]$ can be arbitrarily large and the strategy used in [7] to prove that $\dim_{\mathbb{F}_p} S^p(E/K)$ can be arbitrarily large, where E and K vary, but $[K : \mathbb{Q}]$ is bounded by a function depending on p of type $O(p)$.

In [7] the strategy was to find a field K, such that $[K : \mathbb{Q}]$ is small and a point $P \in X_0(p)(K)$ such that P reduces to one cusp for many primes $\mathfrak{p}$ and reduces to the other cusp for very few primes $\mathfrak{p}$. Then to P we can associate an elliptic curve E/K such that an application of a Theorem of Cassels [3] shows that $S^p(E/K)$ gets large.

The strategy of [5] 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 linear transformation T, such that the φ-Selmer group is isomorphic to the kernel of T, while the $\hat{\varphi}$-Selmer group is isomorphic to the kernel of an adjoint of T. 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 T minus 1.

Moreover, one can prove that if the difference between the dimension of the domain of T and the domain of the adjoint of T is large, 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 (or full p-torsion, if one wants to take $p = q$), one can hope that for one isogeny the associated transformation has high rank, while for the other isogeny the difference between the dimension of the domain of T and its adjoint is large. 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. We can still express the Selmer group attached to the isogeny as the kernel of a linear transformation T. In general, the transformation for the dual isogeny turns out to be different from any adjoint of T.

Remark. Fix an element $\xi \in S^p(E/K)$. Restrict this element to

$$H^1(K(E[p]), E[p]) \cong \mathrm{Hom}(G_{K(E[p])}, (\mathbb{Z}/p\mathbb{Z})^2).$$

Then ξ gives a Galois extension L of $K(E[p])$ of degree p or p^2, satisfying certain local conditions. (For the case of a cyclic isogeny, these conditions are made more precise in Proposition 2.1.) To check whether a given class in $H^1(K(E[p]), E[p])$ comes from an element in $S^p(E/K)$ we need also to check whether 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 [5], [7] and this paper have one thing in common, namely that the representation of the absolute Galois group of K on $E[p]$ is reducible. In this case the conditions on the interaction of the Galois group of $K(E[p])/K$ with the Galois group of $L/K(E[p])$ almost disappear.

The level of difficulty to construct large p-Selmer groups (and large p-parts in the Tate-Shafarevich groups) seems to be encoded in the size of the image of the Galois representation on $E[p]$.

Elliptic curves E/K with complex multiplication over a proper extension of K have an irreducible Galois-representation on $E[p]$ for all but finitely many p, but the representation is strictly smaller than $\mathrm{GL}_2(\mathbb{F}_p)$.

In view of the above remarks it seems that if one would like to produce examples of elliptic curves with large p-Selmer groups, and an irreducible representation of the Galois group on $E[p]$, one could start with the case of elliptic curves with complex multiplication. Unfortunately, we do not have a strategy to produce such examples.

The organization of this paper is as follows: In Section 2 we prove several lower and upper bounds for the size of φ-Selmer groups, where φ is an isogeny with kernel generated by a rational point of prime order at least 5. In Section 3 we use the modular curve $X(p)$ and the estimates from Section 2 to prove Theorem 1.1.

2. Selmer groups

In this section we give several upper and lower bounds for the p-Selmer group of an elliptic curve E/K with a K-rational point of order p, and $\zeta_p \in K$. We combine two of these bounds to obtain a lower bound for $\dim_{\mathbb{F}_p} Ш(E/K)[p]$.

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. The φ-Selmer group of E/K is

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

and the Tate-Shafarevich group of E/K is

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

In the usual definition of the φ-Selmer group one takes the product over all primes, also the archimedean ones. If φ is of odd degree then $H^1(K_{\mathfrak{p}}, E[\varphi]) = 0$ for all archimedean primes $\mathfrak{p}$, so in that case we may exclude the archimedean primes.

Notation. 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 $\langle P \rangle$. Let $\hat{\varphi} : E' \to E$ be the dual isogeny.

To φ we associate three sets of primes. Let $S_1(\varphi)$ be the set of primes $\mathfrak{p} \subset \mathcal{O}_K$, such that $\mathfrak{p}$ does not divide p, the reduction of E is split multiplicative at $\mathfrak{p}$, and $P \in E_0(K_{\mathfrak{p}})$ (notation from [18, Chapter VII]). Let $S_2(\varphi)$ be the set of primes $\mathfrak{p} \subset \mathcal{O}_K$, such that $\mathfrak{p}$ does not divide p, the reduction of E is split multiplicative at $\mathfrak{p}$, and $P \notin E_0(K_{\mathfrak{p}})$. Let $S_3(\varphi)$ be the set of all primes above p.

Suppose $\mathcal{S}$ is a finite sets of finite primes. Let

$$K(\mathcal{S}, p) := \{x \in K^*/K^{*p} \colon v_{\mathfrak{p}}(x) \equiv 0 \bmod p \;\forall \mathfrak{p} \notin \mathcal{S}, \mathfrak{p} \text{ non-archimedean}\}.$$

Let C_K denote the class group of K. Denote G_K the absolute Galois group of K. Let M be a G_K-module. Let $H^1(K, M; \mathcal{S})$ be the subgroup of $H^1(K, M)$ of all classes of cocycles not ramified outside $\mathcal{S}$.

For any cocycle $\xi \in H^1(K, M)$ denote $\xi_{\mathfrak{p}} := \mathrm{res}_{\mathfrak{p}}(\xi) \in H^1(K_{\mathfrak{p}}, M)$. Let $\delta_{\mathfrak{p}}$ be the map

$$E'(K_{\mathfrak{p}})/\varphi(E(K_{\mathfrak{p}})) \to H^1(K_{\mathfrak{p}}, E[\varphi])$$

induced by the boundary map.

Note that $S_1(\hat{\varphi}) = S_2(\varphi)$ and $S_2(\hat{\varphi}) = S_1(\varphi)$. (To define $S_i(\hat{\varphi})$ we need to start with a K-rational point P of order p. Since $\zeta_p \in K$, we have that $\#E'(K)[\hat{\varphi}] = p$, so we can take any generator P of the kernel of $\hat{\varphi}$.) If no confusion arises we write S_1 and S_2 for $S_1(\varphi)$ and $S_2(\varphi)$.

Proposition 2.1. *We have that $S^{\varphi}(E/K)$ is the kernel of*

$$H^1(K, E[\varphi]; S_1 \cup S_3) \to \oplus_{\mathfrak{p} \in S_2} H^1(K_{\mathfrak{p}}, E[\varphi]) \oplus_{\mathfrak{p} \in S_3} (H^1(K_{\mathfrak{p}}, E[\varphi])/\operatorname{Im}(\delta_{\mathfrak{p}})).$$

Proof. Suppose $\mathfrak{p}$ is a prime such that p divides the Tamagawa number $c_{E,\mathfrak{p}}$. Since $4 < p \leq c_{E,\mathfrak{p}}$, we have that the reduction at $\mathfrak{p}$ is split multiplicative. Using Tate curves one easily shows that $c_{E,\mathfrak{p}}/c_{E',\mathfrak{p}} \neq 1$. This combined with if $\mathfrak{p} \nmid (p)$ then $\dim_{\mathbb{F}_p} H^1(K_{\mathfrak{p}}, E[\varphi]) \leq 2$ (see [21, Proposition 3]) and [15, Lemma 3.8] gives that $\iota_{\mathfrak{p}}^* : H^1(K_{\mathfrak{p}}, E[\varphi]) \to H^1(K_{\mathfrak{p}}, E)$ is either injective or the zero-map. A closer inspection of [15, Lemma 3.8] combined with [7, Proposition 3] shows that $\iota_{\mathfrak{p}}^*$ is injective if and only if $\mathfrak{p} \in S_2(\varphi)$. The proposition then follows from [16, Proposition 4.6]. ☐

Remark. Proposition 2.1 is false when the degree of the isogeny is 2 or 3. For degree 3 a similar proposition is stated in [16, Proposition 4.6]. First of all, if the degree is 2, one need to include a conditions for the archimedean primes. Moreover, one needs to give conditions for non-split multiplicative primes (if the degree is 2) and conditions for the additive primes (if the degree is either 2 or 3).

Consider for example the curve $y^2 = x(x + ax + a)$, for some square-free odd integer a. Let φ be the isogeny obtained by dividing out $\{O, (0, 0)\}$. Then S_2 is an empty set, and S_1 consists of a subset of all primes dividing $a - 4$. We can twist this curve such that S_2 remains empty and all multiplicative primes are split. If the above proposition were true for degree 2, then the size of the φ-Selmer group would depend on the number of prime factors of $a - 4$. Using [18, Proposition X.4.9] one can produce a such that the φ-Selmer group is much smaller than the kernel given in Proposition 2.1.

Definition. Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two disjoint finite sets of finite primes of K, such that none of the primes in these sets divides (p).

Let

$$T : K(\mathcal{S}_1, p) \to \oplus_{\mathfrak{p} \in \mathcal{S}_2} \mathcal{O}_{\mathfrak{p}}^* / \mathcal{O}_{\mathfrak{p}}^{*p}$$

be the $\mathbb{F}_p$-linear map induced by inclusion. Let $m(\mathcal{S}_1, \mathcal{S}_2)$ 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 $m(\varphi) := m(S_1(\varphi), S_2(\varphi))$.

Lemma 2.2. *We have*

$$\dim_{\mathbb{F}_p} K(\mathcal{S}, p) = \frac{1}{2}[K : \mathbb{Q}] + \#\mathcal{S} + \dim_{\mathbb{F}_p} C_K[p].$$

Hence the domain of T is finite-dimensional.

Proof. Since $\zeta_p \in K$ we have that K does not admit any real embedding. The above formula is a special case of [11, Proposition 12.6]. □

Proposition 2.3. *We have*

$$S^{\varphi}(E/K) \subset \{x \in K(S_1 \cup S_3, p) \colon x \in K_{\mathfrak{p}}^{*p} \text{ for all } \mathfrak{p} \in S_2\} = \ker T$$

and

$$S^{\varphi}(E/K) \supset \{x \in K(S_1, p) \colon x \in K_{\mathfrak{p}}^{*p} \text{ for all } \mathfrak{p} \in S_2 \cup S_3\}.$$

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 (see [13, X.3.b]), and Proposition 2.1. □

Proposition 2.4. *We have*

$$\begin{aligned} \#S_1 - \#S_2 + \dim_{\mathbb{F}_p} C_K[p] - \frac{3}{2}[K:\mathbb{Q}] \le \dim_{\mathbb{F}_p} S^{\varphi}(E/K) \\ \le \#S_1 + \dim_{\mathbb{F}_p} C_K[p] \\ - m(\varphi) + \frac{3}{2}[K:\mathbb{Q}]. \end{aligned}$$

Proof. Using Hilbert 90 ([13, Proposition X.3]) and [21, Proposition 3] we obtain that for every prime $\mathfrak{p}$

$$\dim_{\mathbb{F}_p} \mathcal{O}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^{*p} = \dim_{\mathbb{F}_p} H^1(K_{\mathfrak{p}}, \mu_{\mathfrak{p}}) - 1 = 1 + e(\mathfrak{p}/p),$$

where $e(\mathfrak{p}/p)$ is the ramification index of $\mathfrak{p}/p$, if $\mathfrak{p}$ divides p and zero otherwise. This yields

$$\dim \oplus_{\mathfrak{p}\in S_3} \mathcal{O}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^{*p} = \sum_{\mathfrak{p}\in S_3} (1 + e(\mathfrak{p}/p)) \le 2[K:\mathbb{Q}].$$

The above bound combined with Lemma 2.2 and Proposition 2.3 gives us

$$\begin{aligned} \dim_{\mathbb{F}_p} S^{\varphi}(E/K) &\ge \dim_{\mathbb{F}_p} K(S_1, p) - \#S_2 - \#S_3 \\ &\ge -\frac{3}{2}[K:\mathbb{Q}] + \#S_1 + \dim_{\mathbb{F}_p} C_K[p] - \#S_2. \end{aligned}$$

For the other inequality, we obtain using Proposition 2.3

$$\dim_{\mathbb{F}_p} S^{\varphi}(E/K) \le \dim_{\mathbb{F}_p} \ker T \le \dim_{\mathbb{F}_p} K(S_1 \cup S_3, p) - m(\varphi).$$

Using $\#S_3 \le [K:\mathbb{Q}]$ and applying Lemma 2.2 to the right hand side of this inequality yields

$$\dim_{\mathbb{F}_p} S^{\varphi}(E/K) \le \#S_1 + \dim_{\mathbb{F}_p} C_K[p] - m(\varphi) + \frac{3}{2}[K:\mathbb{Q}].$$

□

Lemma 2.5. *We have*

$$\operatorname{rank} E(K) \le \#S_1(\varphi) + \#S_2(\varphi) + 2\dim_{\mathbb{F}_p} C_K[p] + 3[K:\mathbb{Q}] - m(\varphi) - m(\hat{\varphi}) - 1.$$

Proof. This follows from the following sequences of inequalities

$$\begin{aligned} 1 + \operatorname{rank} E(K) &\le \dim_{\mathbb{F}_p} E(K)/pE(K) \\ &\le \dim_{\mathbb{F}_p} S^p(E/K) \\ &\le \dim_{\mathbb{F}_p} S^{\varphi}(E/K) + \dim_{\mathbb{F}_p} S^{\hat{\varphi}}(E'/K). \end{aligned}$$

The first inequality follows from the fact that $E(K)$ has p-torsion, the second one follows from the long exact sequence in cohomology associated to $0 \to E[p] \to E \to E \to 0$ and the third one follows from the exact sequence

$$0 \to E'(K)[\hat{\varphi}]/\varphi(E(K)[p]) \to S^{\varphi}(E/K) \to S^p(E/K) \to S^{\hat{\varphi}}(E'/K).$$

(See [16, Lemma 9.1].)

Applying Proposition 2.4 gives

$$\begin{aligned} &\dim_{\mathbb{F}_p} S^{\varphi}(E/K) + \dim_{\mathbb{F}_p} S^{\hat{\varphi}}(E'/K) \\ &\qquad \le \#S_1(\varphi) + \#S_1(\hat{\varphi}) + 2\dim_{\mathbb{F}_p} C_K[p] + 3[K:\mathbb{Q}] - m(\varphi) - m(\hat{\varphi}). \end{aligned}$$

□

By a theorem of Cassels we can compute the difference of $\dim_{\mathbb{F}_p} S^{\varphi}(E/K)$ and $\dim_{\mathbb{F}_p} S^{\hat{\varphi}}(E'/K)$. We do not need the precise difference, but only an estimate, namely

Lemma 2.6. *There is an integer t, with $|t| \le 2[K:\mathbb{Q}] + 1$ such that*

$$\dim_{\mathbb{F}_p} S^{\hat{\varphi}}(E'/K) = \dim_{\mathbb{F}_p} S^{\varphi}(E/K) - \#S_1(\varphi) + \#S_2(\varphi) + t.$$

Proof. This follows from [3] (see [7, Proposition 3] for the details). □

Lemma 2.7.

$$\begin{aligned} &\dim_{\mathbb{F}_p} S^{\varphi}(E/K) + \dim_{\mathbb{F}_p} S^{\hat{\varphi}}(E'/K) \\ &\qquad \ge |\#S_1 - \#S_2| + 2\dim_{\mathbb{F}_p} C_K[p] - 5[K:\mathbb{Q}] - 1. \end{aligned}$$

Proof. After possibly interchanging E and E' we may assume that $\#S_1 \ge \#S_2$. From Proposition 2.4 we know

$$\dim_{\mathbb{F}_p} S^{\varphi}(E/K) \ge \#S_1 - \#S_2 + \dim_{\mathbb{F}_p} C_K[p] - \frac{3}{2}[K:\mathbb{Q}].$$

From this inequality and Lemma 2.6 we obtain that

$$\begin{aligned} \dim_{\mathbb{F}_p} S^{\hat{\varphi}}(E'/K) &\ge \dim_{\mathbb{F}_p} S^{\varphi}(E/K) - 2[K:\mathbb{Q}] - 1 - \#S_1 + \#S_2 \\ &\ge \dim_{\mathbb{F}_p} C_K[p] - \frac{7}{2}[K:\mathbb{Q}] - 1. \end{aligned}$$

Summing both inequalities gives the Lemma. □

Lemma 2.8. *Let* $s := \dim_{\mathbb{F}_p} S^{\varphi}(E/K) + \dim_{\mathbb{F}_p} S^{\hat{\varphi}}(E'/K) - 1$ *and* $r := \operatorname{rank} E(K)$*, then*

$$\max(\dim_{\mathbb{F}_p} Ш(E/K)[p], \dim_{\mathbb{F}_p} Ш(E'/K)[p]) \geq \frac{(s-r)}{2}.$$

Proof. The exact sequence

$$0 \to E'(K)[\hat{\varphi}]/\varphi(E(K)[p]) \to S^{\varphi}(E/K) \to S^{p}(E/K) \to \\ \to S^{\hat{\varphi}}(E'/K) \to Ш(E'/K)[\hat{\varphi}]/\varphi(Ш(E/K)[p])$$

(See [16, Lemma 9.1]) implies

$$\dim_{\mathbb{F}_p} Ш(E'/K)[\hat{\varphi}] + \dim_{\mathbb{F}_p} S^{p}(E/K) \geq s - 1 + \dim_{\mathbb{F}_p} E(K)[p].$$

The lemma follows now from the following inequality coming from the long exact sequence in Galois cohomology

$$\dim_{\mathbb{F}_p} Ш(E'/K)[p] + \dim_{\mathbb{F}_p} Ш(E/K)[p] \\ \geq \dim_{\mathbb{F}_p} Ш(E'/K)[\hat{\varphi}] + \dim_{\mathbb{F}_p} S^{p}(E/K) - r - \dim_{\mathbb{F}_p} E(K)[p].$$

□

Lemma 2.9. *Let* $\psi : E_1 \to E_2$ *be some isogeny obtained by dividing out a* K*-rational point of order* p*, with* E_1 K*-isogenous to* E*. Then*

$$\max(\dim_{\mathbb{F}_p} Ш(E/K)[p], \dim_{\mathbb{F}_p} Ш(E'/K)[p]) \\ \geq -\min(\#S_1(\varphi), \#S_2(\varphi)) - 5[K:\mathbb{Q}] - 1 + \frac{1}{2}(m(\psi) + m(\hat{\psi})).$$

Proof. Use Lemma 2.5 for the isogeny ψ to obtain the bound for the rank of $E(K)$. Then combine this with Lemma 2.7 and Lemma 2.8 and use that

$$\#S_1(\varphi) + \#S_2(\varphi) = \#S_1(\psi) + \#S_2(\psi).$$

□

3. Modular curves

In this section we prove Theorem 1.1. We construct certain fields $K/\mathbb{Q}$ such that $X(p)(K)$ contains points with certain reduction properties. These reduction properties translate into certain properties of elliptic curves E/K admitting two cyclic isogenies φ, ψ such that $m(\psi)$ is much larger then $\min(\#S_1(\varphi), \#S_2(\varphi))$ (notation from the previous section). Then applying the results of the previous section gives us a proof of Theorem 1.1.

The following result will be used in the proof of Theorem 1.1.

Theorem 3.1 ([6, Theorem 10.4])**.** *Let* $f \in \mathbb{Z}[X]$ *be a polynomial of degree at least 1. Let* d *be the number of irreducible factors of* f*. Suppose that for every prime* ℓ*, there exists a* $y \in \mathbb{Z}/\ell\mathbb{Z}$ *such that* $f(y) \not\equiv 0 \bmod \ell$*. 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 ℓ, such that $f(\ell)$ has at most n prime factors. Moreover, let*

$$f(x) := \# \left\{ y \in \mathbb{Z}\colon \begin{array}{l} 0 \leq y \leq x \text{ and the number of prime} \\ \text{factors of } f(y) \text{ is at most } n. \end{array} \right\}$$

then there exist $\delta > 0$, such that

$$f(x) \geq \delta \frac{x}{\log^d x} \left(1 + \mathcal{O}\left(\frac{1}{\sqrt{\log(x)}} \right) \right)$$

as $x \to \infty$.

Any improvement on the n will give a better function $g(p)$ (notation from Theorem 1.1), but the new $g(p)$ will still be of type $O(p^4)$.

The proofs for most of the below mentioned properties of $X_0(p)$ and $X(p)$ can be found in [17] or [20]. See also [4, Chapter 4].

Notation. Denote $X(p)/\mathbb{Q}$ the compactification of the curve parameterizing pairs $((E, O), f)$ where (E, O) is an elliptic curve and f is an isomorphism $f : \mathbb{Z}/p\mathbb{Z} \times \mu_p \to E[p]$ with the property that the standard pairing on the left equals f composed with the Weil-pairing.

Denote $X_0(p)/\mathbb{Q}$ the curve obtained by dividing out the Galois-invariant Borel subgroup of $\mathrm{Aut}(X(p)) = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, leaving invariant $((E, O), f|_{\mathbb{Z}/p\mathbb{Z}\times\{1\}})$. The curve $X_0(p)$ is a course moduli space for pairs $((E, O), \varphi)$ where $\varphi : E \to E'$ is an isogeny of degree p. (See for example [9, Chapter 2].)

Let $R_1 \in X_0(p)$ be the unramified cusp (classically called 'infinity'), let $R_2 \in X_0(p)$ be the ramified cusp.

Let $\pi_i : X(p) \to X_0(p)$ be the morphism obtained by mapping (E, f) to (E, φ_i) where φ_i is the isogeny obtained by dividing out $f(\mathbb{Z}/p\mathbb{Z} \times \{1\})$ when $i = 1$, and $f(\{0\} \times \mu_p)$ when $i = 2$. The maps π_i are defined over $\mathbb{Q}$.

Let $P \in X(p)$ be a point, which is not a cusp. The isogeny $\varphi_{P,i}$ is obtained as follows: To $\pi_i(P) \in X_0(p)$ we can associate a pair $(E_P, \varphi_{P,i})$ representing $\pi_i(P)$.

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

Being of type (δ, ϵ) is invariant under the action of the absolute Galois group of $\mathbb{Q}$, since the morphisms π_i are defined over $\mathbb{Q}$ and the cusps on $X_0(p)$ are $\mathbb{Q}$-rational.

Suppose T is a cusp of type (δ, ϵ). Then for all number fields $K/\mathbb{Q}(\zeta_p)$ and all points $P \in X(p)(K)$ we have that if $\mathfrak{p} \nmid (p)$ is a prime of K such that $P \equiv T \bmod \mathfrak{p}$ then $\mathfrak{p} \in S_\delta(\varphi_{P,1})$ and $\mathfrak{p} \in S_\epsilon(\varphi_{P,2})$. This statement can be shown by an easy consideration on the behavior of the Tate-parameter q

of the curve representing the point $P \in X(p)(K)$ and the relation between q and the j-invariant. (Compare [7, Proof of Proposition 3].)

Lemma 3.2. *$X(p)$ has $(p-1)/2$ cusps of each of the types $(2,1)$ and $(1,2)$. The other $(p-1)^2/2$ cusps are of type $(2,2)$. All cusps of type $(1,2)$ are $\mathbb{Q}$-rational.*

Proof. A cusp of type $(1,1)$ would give rise to elliptic curves $E/K_{\mathfrak{p}}$, with multiplicative reduction such that its reduction $\tilde{E}$ modulo $\mathfrak{p}$ has $(\mathbb{Z}/p\mathbb{Z})^2$ as a subgroup, but over an algebraically closed field L of characteristic p, we have $\#\tilde{E}(L)[p] \leq p$, a contradiction.

The ramification index of every point in $\pi_i^{-1}(R_1)$ is p, hence there are $(p-1)/2$ points in $\pi_i^{-1}(R_1)$. From this it follows that there exists $(p-1)/2$ cusps of type $(1,2)$ and $(2,1)$, respectively. The remaining cusps are of type $(2,2)$.

An argument as in [12, page 44 and 45] shows that there is a cusp of type $(1,2)$ that is $\mathbb{Q}$-rational. From this it follows that all cusps of type $(1,2)$ are $\mathbb{Q}$-rational. (See [4, Chapter 4].) □

Proof of Theorem 1.1. Let D be an effective divisor on $X(p)$, such that D is invariant under $G_{\mathbb{Q}}$, the support of D is contained in the set of cusps of type $(1,2)$, the dimension of the linear system $|D|$ is at least 2 and the morphism $\varphi_{|D|} : X(p) \to \mathbb{P}^n$ is injective at almost all geometric points of $X(p)$. Let L be a 2-dimensional linear subsystem of $|D|$ containing D and such that the corresponding morphism is injective at almost all geometric points. Let $C \subset \mathbb{P}^2$ be the image of $X(p)$ given by L. We may assume that the intersection of $X = 0$ with C is precisely D. An automorphism ψ of $\mathbb{P}^2$ fixing the line $X = 0$, is of the form $[X,Y,Z] \mapsto [a_1X, b_1X + b_2Y + b_3Z, c_1X + c_2Y + c_3Z]$. It is easy to see that we can choose a_1, b_i, c_i in such a way that none of the cusps is on the line $Z = 0$, and the function $x = X/Z$ takes distinct values at any pair of cusps with $x \neq 0$. So we may assume that we have a fixed (possibly singular) model $C/\mathbb{Q}$ for $X(p)$ in $\mathbb{P}^2$, such that the line $X = 0$ intersects C only in cusps of type $(1,2)$ and no other points, all x-coordinates of other the cusps are distinct and finite, and all y-coordinates of the cusps are finite. Denote $H \in \mathbb{Z}[X,Y,Z]$ a defining polynomial of C. Set $h(x,y) := H(X,Y,1)$.

Let $f_{\delta,\epsilon} \in \mathbb{Z}[X]$ be the square-free polynomial with roots all x-coordinates of the cusps of type (δ,ϵ) of $X(p)$ and content 1. After a simultaneous transformation of the $f_{\delta,\epsilon}$ of the form $x \mapsto cx$, we may assume that $f_{2,1}(0) = 1$ and $f_{2,1} \in \mathbb{Z}[X]$. Let n denote the constant of Theorem 3.1 for the polynomial $f_{2,1}$. The discriminant of $f_{1,2}f_{2,1}f_{2,2}$ is non-zero, since every cusp has only one type and all cusps have distinct x-coordinate.

Let $\mathcal{B}$ consist of p, all primes ℓ dividing the leading coefficient or the discriminant of $f_{1,2}f_{2,1}f_{2,2}$, all primes ℓ smaller then the degree of $f_{2,1}$ and all primes dividing the leading coefficient of $\mathrm{res}(h, f_{2,2}, x)$, the resultant of h and $f_{2,2}$ with respect to x.

Let $\mathcal{P}_2$ be the set of primes not in $\mathcal{B}$ such that every irreducible factor of $f_{2,1}(x)(x^p - 1) \bmod \ell$ and every irreducible factor of $\mathrm{res}(h, f_{2,1}, x) \bmod \ell$ has degree 1. Note that by Frobenius' Theorem ([19]) the set $\mathcal{P}_2$ is infinite. The condition mentioned here, implies that if we take a triple (x_0, ℓ, 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 $\mathfrak{q}$ of $\mathbb{Q}(\zeta_p, y_0)$ over ℓ satisfies $f(\mathfrak{q}/\ell) = 1$, where $f(\mathfrak{q}/\ell)$ denotes the degree of the extension of the residue fields.

Fix $\mathcal{S}_1$ and $\mathcal{S}_2$ two finite, disjoint sets of primes, not containing an archimedean prime such that

$$m(\mathcal{S}_1, \mathcal{S}_2) > 2k + 2(n+5)\deg(h)(p-1) + 2,$$

$S_1 \cap \mathcal{B} = \emptyset$ and $S_2 \subset \mathcal{P}_2$, with $m(\mathcal{S}_1, \mathcal{S}_2)$ as defined in Section 2. (The existence of such sets follows from Dirichlet's theorem on primes in arithmetic progression and the fact that $\ell \in \mathcal{S}_2$ implies $\ell \equiv 1 \bmod p$.)

Lemma 3.3. *There exists an $x_0 \in \mathbb{Z}$ such that*

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

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 $\tilde{f}(Z) = f_{2,1}(a + bZ)$. We claim that the content of $\tilde{f}$ is one. Suppose ℓ divides this content. Then ℓ divides the leading coefficient of $\tilde{f}$. From this one deduces that ℓ divides b. We distinguish several cases:

- If $\ell \in \mathcal{S}_i$ then $f_{i,2}(a) \equiv 0 \bmod \ell$ and ℓ does not divide the discriminant of the product of the $f_{\delta,\epsilon}$, so we have $\tilde{f}(0) \equiv f_{2,1}(a) \not\equiv 0 \bmod \ell$.
- If ℓ divides b and is not in $\mathcal{S}_1 \cup \mathcal{S}_2$ then $\tilde{f}(0) \equiv f_{2,1}(0) \equiv 1 \bmod \ell$.

So for all primes ℓ dividing b we have that $\tilde{f} \not\equiv 0 \bmod \ell$. This proves the claim on the content of $\tilde{f}$.

Suppose ℓ is a prime smaller then the degree of $\tilde{f}$, then $\tilde{f}(0) \equiv 1 \bmod \ell$. If ℓ is different from these primes, then there is a coefficient of $\tilde{f}$ which is not divisible by ℓ and the degree of $\tilde{f}$ is smaller then ℓ. So for every prime ℓ there is an $z_\ell \in \mathbb{Z}$ with $\tilde{f}(z_\ell) \not\equiv 0 \bmod \ell$. 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

$$\{x_1 \in \mathbb{Z}\colon \tilde{f}(x_1) \text{ has at most } n \text{ prime divisors}\}$$

is not a thin set. So

$$\mathcal{H} := \left\{ x_1 \in \mathbb{Z}\colon \begin{array}{l} \tilde{f}(x_1) \text{ has at most } n \text{ prime divisors} \\ \text{and } h(a+bx_1, y) \text{ is irreducible.} \end{array} \right\}$$

is not empty by Hilbert's Irreducibility Theorem [14, 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. □

Fix an x_0 satisfying the conditions of Lemma 3.3. 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 $K = K_1(\sqrt{c_4(E)})$. Then if $\mathfrak{q}$ is a prime such that $E/K_\mathfrak{q}$ has multiplicative reduction then $E/K_\mathfrak{q}$ has split multiplicative reduction.

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

Note that the set of primes of K such that P reduces to a cusp of type $(2,1)$ has at most $n[K:\mathbb{Q}]$ elements.

We have the following diagram

$$\begin{array}{ccc} \mathbb{Q}(\mathcal{S}_1, p) & \rightarrow & \oplus_{\ell \in \mathcal{S}_2} \mathbb{Z}_\ell^*/\mathbb{Z}_\ell^{*p} \\ \downarrow & & \downarrow \\ K(\mathcal{T}_1, p) & \rightarrow & \oplus_{\mathfrak{q} \in \mathcal{T}_2} \mathcal{O}_{K_\mathfrak{q}}^*/\mathcal{O}_{K_\mathfrak{q}}^{*p}. \end{array}$$

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

$$m(\varphi_{P,1}/K) \geq m(\mathcal{T}_1, \mathcal{T}_2) \geq m(\mathcal{S}_1, \mathcal{S}_2) = 2k + 4(n+5)\deg(h)(p-1) + 2.$$

Since $S_2(\varphi_{p,2}/K) \leq [K:\mathbb{Q}]n$ and $[K:\mathbb{Q}] \leq 2(p-1)\deg(h)$ we obtain by Lemma 2.9 that for some E' isogenous to E we have

$$\begin{aligned} \dim_{\mathbb{F}_p} \text{Ш}(E'/K)[p] &\geq -\#S_1(\varphi_{P,2}) - 5[K:\mathbb{Q}] - 1 + \frac{1}{2}m(\mathcal{S}_1, \mathcal{S}_2) \\ &\geq -(n+5)[K:\mathbb{Q}] - 1 + \frac{1}{2}m(\mathcal{S}_1, \mathcal{S}_2) = k. \end{aligned}$$

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

$$\dim_{\mathbb{F}_p} Ш(E/K)[p] \geq kg(p)$$

and $[K : \mathbb{Q}] \leq g(p)$.

Let $R := \mathrm{Res}_{K/\mathbb{Q}}(E)$ be the Weil restriction of scalars of E. Then by [10, Proof of Theorem 1]

$$\dim_{\mathbb{F}_p} Ш(R/\mathbb{Q})[p] = \dim_{\mathbb{F}_p} Ш(E/K)[p].$$

From this it follows that there is a factor A of R, with $\dim_{\mathbb{F}_p} Ш(A/\mathbb{Q})[p] \geq k$. □

References

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

[2] 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.

[3] 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.

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

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

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

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

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

[9] B. Mazur, A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$. Invent. Math. **76** (1984), 179–330.

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

[11] B. Poonen, E.F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line.* J. Reine Angew. Math. **488** (1997), 141–188.

[12] D.E. Rohrlich, *Modular Curves, Hecke Correspondences, and L-functions.* In Modular forms and Fermat's last theorem (Boston, MA, 1995), 41–100, Springer, New York, 1997.

[13] J.-P. Serre, *Local fields.* Graduate Texts in Mathematics **67**, Springer-Verlag, New York-Berlin, 1979.

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

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

[16] E.F. Schaefer, M. Stoll, *How to do a p-descent on an elliptic curve.* Preprint, 2001.

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

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

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

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

[21] L.C. Washington, *Galois cohomology.* Modular forms and Fermat's last theorem (Boston, MA, 1995), 101–120, Springer, New York, 1997.

Remke KLOOSTERMAN
Institute for Mathematics and Computer Science (IWI)
University of Groningen
P.O. Box 800
NL-9700 AV Groningen, The Netherlands

Current address:
Institut für Geometrie
Universität Hannover
Welfengarten 1
D-30167 Hannover, Germany
E-mail : kloosterman@math.uni-hannover.de