International Journal of Number Theory

Self-points on elliptic curves of prime conductor

Christophe Delaunay

Université de Lyon
Université Lyon1
CNRS, UMR 5208 Institut Camille Jordan
Batiment du Doyen Jean Braconnier
43 blvd du 11 novembre 1918
F - 69622 Villeurbanne Cedex
France
delaunay@math.univ-lyon1.fr

Christian Wüthrich

CSAG, Section de mathématiques
École polytechnique fédérale
1015 Lausanne
Switzerland
christian.wuthrich@epfl.ch

Received (Day Month Year)
Revised (Day Month Year)

Let E be an elliptic curve of conductor p. Given a cyclic subgroup C of order p in $E[p]$, we construct a modular point P_C on E, called self-point, as the image of (E, C) on $X_0(p)$ under the modular parametrisation $X_0(p) \longrightarrow\!\!\!\!\!\rightarrow E$. We prove that the point is of infinite order in the Mordell-Weil group of E over the field of definition of C. One can deduce a lower bound on the growth of the rank of the Mordell-Weil group in its $\mathrm{PGL}_2(\mathbb{Z}_p)$-tower inside $\mathbb{Q}(E[p^\infty])$.

Mathematics Subject Classification 2000: 11G05, 11G18, 11G40

Keywords: Elliptic curves, modular curves

1. Introduction

Let p be a prime number and let $E/\mathbb{Q}$ be an elliptic curve of conductor p. It is known that the Galois representation $\bar{\rho}_p\colon \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{GL}_2(\mathbb{F}_p)$ is surjective. (We will recall the classification of curve of prime conductor in Section 2.) Let ψ be an isogeny $E \longrightarrow\!\!\!\!\!\rightarrow E'$ of degree p with kernel $C \subset E[p]$. The field $\mathbb{Q}(C)$ of definition of ψ is a degree $p+1$ extension in $\mathbb{Q}(E[p])$ fixed by a Borel subgroup in $\mathrm{GL}_2(\mathbb{F}_p)$.

We consider now the point $x_C = (E, C)$ on the modular curve $X_0(p)$. Its image under the modular parametrisation $\varphi_E\colon X_0(p) \longrightarrow\!\!\!\!\!\rightarrow E$ will be denoted by P_C. It is a point on E defined over $\mathbb{Q}(C)$. Since the point represents the curve on itself, we

will call this P_C a *self-point* on E. Let K be the Galois closure of $\mathbb{Q}(C)$, it is the $\mathrm{PGL}_2(\mathbb{F}_p)$-extension inside $\mathbb{Q}(E[p])$.

Theorem 1. *The self-point P_C is of infinite order in $E(\mathbb{Q}(C))$. As C runs through all cyclic subgroups of order p in $E[p]$, the set $\{P_C\}_C$ generates a subgroup of rank p in $E(K)$ on which $\mathrm{PGL}_2(\mathbb{F}_p)$ acts like the Steinberg representation.*

The Steinberg representation is a p-dimensional irreducible representation of $\mathrm{PGL}_2(\mathbb{F}_p)$ whose definition will be recalled in Lemma 5.

There is a possibility to construct higher self-points P_D for all cyclic subgroups D of order p^n in $E[p^n]$. If C is the unique order p subgroup in D, let $\hat{C}$ be its dual in $(E/C)[p]$. Denote by $C^{(D)}$ the image of $\hat{C}$ under the natural map $E/C \longrightarrow E/D$. Then P_D is the image of $(E/D, C^{(D)})$ under the modular parametrisation φ_E. We will prove in Theorem 8 that all the points P_D are of infinite order. The points P_D generate a group of rank $p^n + p^{n-1} - 1$ in $E(K_n)$ where K_n is the $\mathrm{PGL}_2(\mathbb{Z}/p^n\mathbb{Z})$-extension in $\mathbb{Q}(E[p^n])$.

In Section 7, we will compute the parity of the p-Selmer group of E over $\mathbb{Q}(C)$ and the root number of E over this field using methods and results of Shuter [Shu06], Rohrlich [Roh06] and Dokchitser [Dok05]. These computations lead naturally to the conjecture that the rank of $E(\mathbb{Q}(C))$ is even if and only if p is congruent to 1 modulo 4. Interestingly our self-points do not behave like Heegner points with respect to root numbers.

In Section 8, we will give some numerical examples. We compute explicitly the self-points on the curves of conductor 11, 17 and 19. Eventhough they are fairly simple to define and have rather small canonical height, their coordinates have surprisingly complicated expressions. It seems plausible that the self-points are not divisible by any integer in $E(\mathbb{Q}(C))$.

These self-points have been considered earlier by Harris in [Har79] where he obtained asymptotic formula for the rank of $E(K_n)$ of the form mentioned above. The investigation is tightly linked to non-commutative Iwasawa theory. Though in the form presented here, it is concerned with the Iwasawa theory of the p-adic Lie extension K_∞/K for the prime p of multiplicative reduction. These are the first known points of infinite order defined over the $GL_2(\mathbb{Z}_p)$-extension $\mathbb{Q}(E[p^\infty])$ naturally attached to E. Nevertheless the computations of Rohrlich on the root numbers for the irreducible Artin representations of $\mathrm{GL}_2(\mathbb{Z}_p)$ and the recent results for the p-Selmer group in [CFKS06] suggest that the rank of $E(\mathbb{Q}(E[p^n]))$ should grows much faster than p^n, at least when $p \equiv 3 \pmod 4$.

In a forthcoming paper [Wut07], we will consider self-points on elliptic curves whose conductors are not necessarily prime. In this general setting, the situation is much more involved.

2. Classification of curves of prime conductor

The first few examples of elliptic curves $E/\mathbb{Q}$ of prime conductor p are listed in the following table. Only the strong Weil curves, i.e. optimal curves with respect to the modular parametrisation $\varphi_E\colon X_0(p) \longrightarrow\!\!\!\!\!\rightarrow E$ are included. ("s" stands for split multiplicative reduction at p and "n" for non-split multiplicative reduction.)

Curve	11a1	17a1	19a1	37a1	37b1	43a1	53a1	61a1	67a1	73a1
Torsion	5	4	3	1	3	1	1	1	1	2
Reduction	s	s	s	n	s	n	n	n	s	s
Rank	0	0	0	1	0	1	1	1	0	0

We summarise in the following proposition the facts known about curves of prime conductor.

Proposition 2. *Let E be an elliptic curve of prime conductor p and let E_0 be the strong Weil curve in its isogeny class. Then the Tamagawa number $c_p = -\operatorname{ord}_p(j)$ of E_0 at p is equal to the order of the torsion subgroup of $E(\mathbb{Q})$ and its Manin constant is trivial. We are in one of the following three cases*

- *The curve E_0 has no torsion points defined over $\mathbb{Q}$. Then the ℓ-adic Galois representations $\rho_\ell\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Aut}(T_\ell(E)) = \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective for all ℓ, hence there are no isogenies on $E_0 = E$ defined over $\mathbb{Q}$. The Tamagawa number c_p at p is 1.*
- *We have $\#E_0(\mathbb{Q})_{\mathrm{tors}} = 2$. Then the prime p is of the form u^2+64 for some integer $u \equiv 3 \pmod 4$. The curve E is one of the two isogenous curves.*

$$E_0\colon y^2 + xy = x^3 - \tfrac{u+1}{4}x^2 + 4x - u$$
$$E_1\colon y^2 + xy = x^3 - \tfrac{u+1}{4}x^2 - x$$

  For these curves we have that $E(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ and $Ш(E/\mathbb{Q})[2] = 0$. All ρ_ℓ for $\ell \neq 2$ are surjective.
- *We have $\#E_0(\mathbb{Q})_{\mathrm{tors}} > 2$. Then E_0 will be among the curves of conductor 11, 17, 19 or 37 shown in the table above.*

The curves in the second case are treated in [Set75] and [Neu71] and [Neu73]. They are called Neumann-Setzer curves in [SW04]. The first few primes for which we are in this situation are 73, 89, 113, 233, 353, 593, ...

Proof. According to [MO89], the curves of conductor p with a torsion point have been classified by Miyawaki [Miy73] and Setzer in [Set75]. In Corollaire 5.2 in [MO89], it is shown that $E(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to the group of connected components of the Néron model of E at p. Furthermore, we know by Serre [Ser72] that for a semi-stable curve either there is a curve with a rational non-trivial torsion point in its isogeny class or the curve does not admit any isogeny defined over $\mathbb{Q}$. Moreover [Ser96] shows that the representation ρ_ℓ is surjective for all primes ℓ for

a semi-stable curve unless the curve admits an isogeny of degree ℓ defined over $\mathbb{Q}$. The statement about the Manin constant is proved in [AU96]. It remains to cite [SW04] for the result on the Mordell-Weil group and the 2-torsion part of the Tate-Shafarevich group of the Neumann-Setzer curves. □

Note that in particular the representation ρ_p is surjective. Given a cyclic subgroup C of $E[p]$, then the field $\mathbb{Q}(C)$ is the field fixed by a Borel subgroup and is therefore a non-Galois degree $p+1$ extension without any proper sub-extensions. As C runs through all possible cyclic subgroups in E of degree p, we obtain $p+1$ such extensions and their compositum is the field K fixed by the centre of $\mathrm{GL}_2(\mathbb{F}_p)$. The Galois group of $K/\mathbb{Q}$ is therefore $G \cong \mathrm{PGL}_2(\mathbb{F}_p)$.

3. The main theorem

The aim of this section is to prove Theorem 1. The theorem is split up in two propositions that we will prove separately.

Proposition 3. *The self-points P_C are of infinite order.*

Proof. Recall that K was defined to be the Galois closure of $\mathbb{Q}(C)$. Note that the points $\{P_C\}_C$ form a single orbit under the action of $\mathrm{Gal}(K/\mathbb{Q})$ in $E(K)$, because $G \cong \mathrm{PGL}_2(\mathbb{F}_p)$ acts transitively on the set of all C, which we will identify from now on with $\mathbb{P}^1(\mathbb{F}_p)$. It is therefore enough to show that one of the self-points is of infinite order.

First we fix an embedding of $\bar{\mathbb{Q}}$ into $\bar{\mathbb{Q}}_p$. We consider the modular parametrisation over $\mathbb{Q}_p$. The modular curve $X_0(p)$ over $\bar{\mathbb{Q}}_p$ has a neighbourhood of the cusp ∞ consisting of couples (A, C) of a Tate curve of the form $A = \bar{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}$ together with its subgroup generated by the p^{th} root of unity. The parameter q is a p-adic analytic uniformiser at ∞, so that the $\mathrm{Spf}\,\mathbb{Q}_p[\![q]\!]$ is the formal completion of $X_0(p)/\mathbb{Q}_p$ at the cusp ∞, see [DR73].

Let $f_E = \sum a_n\, q^n$ be the normalised newform associated to E and so $f_E/q \cdot dq$ is the associated differential, and since we know that the Manin constant is trivial, it coincides with $\varphi_E^*(\omega_E)$ where ω_E is the invariant differential on E. The rigid analytic map induced by φ_E on the completion can now be characterised as

$$\log_E(\varphi_E(q)) \;=\; \int_O^{\varphi_E(q)} \omega_E \;=\; \int_0^q f_E\,\frac{dq}{q} \;=\; \sum_{n\geqslant 1} \frac{a_n}{n}\cdot q^n\,.$$

Here $\log_E$ denotes the formal logarithm associated to E from the formal group $\hat{E}(p\mathbb{Z}_p)$ to $\hat{\mathbb{G}}_a(p\mathbb{Z}_p) = p\mathbb{Z}_p$.

Since E has multiplicative reduction at p, there is exactly one of the x_C in this neighbourhood, we call it x_0. The other self-points are p-adically close to the second cusp 0. Write P_0 for $\varphi_E(x_0)$. Let q_E be the p-adic Tate parameter associated to E.

By the above characterisation of φ_E, we know now that

$$\log_E(P_0) = \sum_{n \geqslant 1} \frac{a_n}{n} \cdot q_E^n \;=\; q_E + \frac{a_2}{2}\, q_E^2 + \cdots .$$

Since the valuation of q_E is equal to the Tamagawa number $c_p \geqslant 1$, the sum on the right converges and its value will be congruent to q_E modulo $p^{2 \cdot c_p}$. In particular the value is non zero and hence is a non torsion element in $p^{c_p}\,\mathbb{Z}_p$. Therefore P_0 is a non-torsion point in $\hat{E}(p^{c_p}\mathbb{Z}_p)$. □

This second proposition will now end the proof of Theorem 1.

Proposition 4. *The points $\{P_C\}_C$ generate a group of rank p in $E(K)$. The only relation is that the sum of all P_C is equal to the image $\varphi_E(0)$ of the cusp 0 on $X_0(p)$, which is a torsion point in $E(\mathbb{Q})$.*

Proof. We prove first the relation between the self-points. By definition the sum $\sum_C P_C$ is the image of the class of the divisor

$$D = \sum_{C \in \mathbb{P}^1(\mathbb{F}_p)} ((x_C) - (\infty))$$

under the map $J_0(p) \longrightarrow\!\!\!\!\!\rightarrow E$ where $J_0(p)$ is the Jacobian of $X_0(p)$. We compare this divisor to the divisor of the function $j - j(E)$ on $X_0(p)$. We have

$$\begin{aligned} \operatorname{div}(j - j(E)) &= -p \cdot (0) - (\infty) + \sum_{C \in \mathbb{P}^1(\mathbb{F}_p)} (x_C) \\ &= D - p \cdot ((0) - (\infty)) \,. \end{aligned}$$

Hence the sum of all P_C is equal to $p \cdot \varphi_E(0)$. If $p > 37$, then $\varphi_E(0)$ is a point of order at most 2 and p is an odd prime, so we have $p \cdot \varphi_E(0) = \varphi_E(0)$. For $p \leqslant 37$, we also have $p \equiv 1$ modulo the order of $E(\mathbb{Q})_{\text{tors}}$.

Further we need the following lemma defining the Steinberg representation.

Lemma 5. *Let V be the $\mathbb{Q}[G]$-module $\bigoplus_{C \in \mathbb{P}^1(\mathbb{F}_p)} \mathbb{Q} \cdot e_C$ with the natural action of $G \cong \mathrm{PGL}_2(\mathbb{F}_p)$ on $\mathbb{P}^1(\mathbb{F}_p)$. It splits into the sum of two irreducible $\mathbb{Q}[G]$-modules, the first 1-dimensional generated by $\sum_C e_C$ and the second p-dimensional given by*

$$\mathrm{St} = \Big\{ \sum a_C \cdot e_C \;\Big|\; \sum a_C = 0 \Big\},$$

called the Steinberg representation of G.

Proof. It is clear that V splits as $W_0 \oplus \mathrm{St}$ with W_0 generated by $\sum_C e_C$. We start to prove the irreducibility of St by showing that there are no one-dimensional submodules. Let $v = \sum a_C \cdot e_C$ be a fixed vector. By subtracting the obvious fixed vector $\sum e_C$, we may assume that one of the coordinates in v is zero. But then v can not be fixed by G since the action of G on $\mathbb{P}^1(\mathbb{F}_p)$ is transitive.

Let now g be an element of order p in G. The eigenvalues of g acting on St are exactly the p-th roots of unity. If now the $\mathbb{Q}[G]$-module St splits into two submodules, then necessarily one of them would have to be one-dimensional, which we have just excluded above. Therefore St is irreducible. □

Now we can end the proof of the proposition. There is a G-equivariant map from V to $E(K)\otimes\mathbb{Q}$ given by sending e_C to P_C. Since the sum of all P_C is torsion, the space W_0 is in the kernel. The restricted map $\mathrm{St} \longrightarrow E(K)\otimes\mathbb{Q}$ is an injective morphism of $\mathbb{Q}[G]$-modules by Proposition 3. Hence the group generated by the self-points $\{P_C\}$ is a full lattice in the image of this map which is a p-dimensional vector space.

Corollary 6. *The point P_C is not divisible by p^{c_p} in $E(\mathbb{Q}(C))$.*

Proof. This can be deduced from the proof of Proposition 3. It is shown there that the p-adic valuation of $\log_E(P_C)$ in $\mathbb{Q}_p$ is equal to c_p. Let $\mathfrak{p}$ be the place of $\mathbb{Q}(C)$ corresponding to the chosen embedding $\bar{\mathbb{Q}}$ in $\bar{\mathbb{Q}}_p$, then $\mathbb{Q}(C)_{\mathfrak{p}} = \mathbb{Q}_p$. Since the order of the group of components of E over $\mathbb{Q}_p$ and the number of non-singular points in the reduction $E(\mathbb{F}_p)$ are both prime to p, the question whether P_C is divisible by p^{c_p} in $E(\mathbb{Q}_p)$ is the same as to ask whether it is divisible by it in the formal group $\hat{E}(p\mathbb{Z}_p)$. But now the statement about the valuation of $\log_E(P_C)$ shows that P_C can not be divided by p^{c_p} in $E(\mathbb{Q}_p)$. □

3.1. *More on the Steinberg representation*

The character χ_{St} of the irreducible representation $\rho_{\mathrm{St}}\colon G \longrightarrow \mathrm{Aut}(\mathrm{St})$ of $G \cong \mathrm{PGL}_2(\mathbb{F}_p)$ can be explicitly described in the following manner. Of course $\chi_{\mathrm{St}}(1) = p$. There are three different types of non-trivial conjugacy classes in G. First the class of elements of order p, where χ_{St} takes the value 0. The second type consists of conjugacy classes containing a diagonal matrix. For all such classes, the value of χ_{St} is $+1$. Finally χ_{St} takes the value -1 on the remaining classes. This representation and its twist by the only non-trivial representation of G of dimension 1 are called Steinberg representations in [Lan02, page 712] and [Sil70].

4. The torsion subgroup of E over K

The group $\mathrm{PGL}_2(\mathbb{F}_p)$ admits only one non-trivial 1-dimensional representation χ (over $\mathbb{C}$). It is defined as

$$\chi\colon \mathrm{PGL}_2(\mathbb{F}_p) \xrightarrow{\det} \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2} \longrightarrow \{\pm 1\}$$

with kernel $\mathrm{PSL}_2(\mathbb{F}_p)$. Hence there is a unique quadratic subfield L inside K and it has to be the unique quadratic extension that is only ramified at p, that is

$$L = \mathbb{Q}(\sqrt{p^*}) \quad \text{with} \quad p^* = (-1)^{\frac{p-1}{2}}\cdot p\,.$$

Theorem 7. *Let E be an elliptic curve of prime conductor p and let K, L and $\mathbb{Q}(C)$ as before. Then we have $E(K)_{\mathrm{tors}} = E(L)_{\mathrm{tors}}$. Moreover, we have $E(K)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$ except for the Neumann-Setzer curves E_1 and the curves 17a2, 17a3 and 17a4. In particular $E(\mathbb{Q}(C))_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$.*

Proof. First let ℓ be a prime for which the mod ℓ representation $\bar{\rho}_\ell\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[\ell])$ is surjective. Suppose that $E(K)$ contains an ℓ-torsion point. Then $\mathbb{Q}(E[\ell])$ must be contained in K since $K/\mathbb{Q}$ is Galois. Since $\mathrm{Gal}(K/L) = \mathrm{PSL}_2(\mathbb{F}_p)$ is a simple group, either $\mathbb{Q}(E[\ell])$ is equal to K or to L. But since the degree $[\mathbb{Q}(E[\ell]) : \mathbb{Q}]$ is $\ell \cdot (\ell-1)^2 \cdot (\ell+1)$ it is certainly impossible that $\mathbb{Q}(E[\ell]) = L$. But it can not be equal to K either as the equation

$$\ell \cdot (\ell-1)^2 \cdot (\ell+1) = p \cdot (p-1) \cdot (p+1)$$

implies that $\ell < p$, unless $\ell = p = 2$ which is impossible because $p \geqslant 11$. But if $\ell < p$ then the left hand side is not divisible by p unless $\ell = 2$ and $p = 3$ which is not possible either. Hence $E(K)$ does not contain any ℓ-torsion points. For the first class of curves in Proposition 2 this means that $E(K)_{\mathrm{tors}} = 0$.

So we may suppose that E has a torsion point over $\mathbb{Q}$. By the classification, we know that there is a unique prime $\ell \leqslant 5$ dividing $\#E(\mathbb{Q})_{\mathrm{tors}}$. The above guarantees that $E(K)_{\mathrm{tors}}$ is an ℓ-primary group.

Suppose now that $E(K)$ has a torsion point S which is not defined over L. By taking a multiple of S, we may suppose that $\ell \cdot S$ is defined over L. Hence the Galois closure of $L(S)$ is of degree at most $\ell! \leqslant 120$ as the Galois group is a permutation group of the set $\{T | \ell \cdot T = \ell \cdot S\}$. This is a contradiction with the fact that $\mathrm{PSL}_2(\mathbb{F}_p)$ is a simple group with at least $\#\,\mathrm{PSL}_2(\mathbb{F}_{11}) = 660$ elements. Therefore $E(K)_{\mathrm{tors}} = E(L)_{\mathrm{tors}}$.

Next we compute $E(L)_{\mathrm{tors}} = E(K)_{\mathrm{tors}}$ for the four isogeny classes of curves with $\#E(\mathbb{Q})_{\mathrm{tors}} > 2$ this can be done directly and the result is given in the table below.

Curve	11a1	11a2	11a3	17a1	17a2	17a3	17a4	19a1	19a2	19a3	37b1	37b2	37b3
$E(\mathbb{Q})_{\mathrm{tors}}$	5	1	5	4	[2,2]	2	4	3	1	3	3	1	3
$E(K)_{\mathrm{tors}}$	5	1	5	4	[2,4]	[2,2]	[2,4]	3	1	3	3	1	3

Finally, we treat the Neumann-Setzer curves. We have to compute the 2-primary torsion of E over L. For such curves we have $L = \mathbb{Q}(\sqrt{p})$. For the curve E_0, we find that the 2-torsion points are generated by $T = (\frac{u}{4}, -\frac{u}{8})$ and $(2 \cdot i, -i)$ with $i^2 = -1$. So we have $E(L)[2] = \mathbb{Z}/2\mathbb{Z}\,T$. Trying to divide T by 2, we find that the S such that $2 \cdot S = T$ are the conjugates of

$$S = \Big(\frac{\alpha^2}{2p}, \frac{\alpha}{4} - \frac{\alpha^2}{2p}\Big) \quad \text{with} \quad \alpha^4 - p\,u\,\alpha^2 + 16\,p^2 = 0\,.$$

Note that $\alpha^2 = \frac{p}{2} \cdot (u + \sqrt{p})$ belongs to $\mathbb{Q}(\sqrt{p})$, but its norm is equal to $-16 \cdot p^2$ and so it can never be the norm of a square in $\mathbb{Q}(\sqrt{p})$. Therefore S is not defined

over L and we conclude that

$$E_0(K)_{\text{tors}} = E_0(L)_{\text{tors}} = E_0(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z}\,T\,.$$

For E_1 we find that a basis of the 2-torsion point can be given by

$$T_1 = (0,0) \qquad \text{and} \qquad T_2 = \Big(\frac{u+\sqrt{p}}{8}, -\frac{u+\sqrt{p}}{16}\Big)\,.$$

So $E[2] \subset E(L)$. The x-coordinates of 4-torsion points are defined over $\mathbb{Q}(i)$ or over the field defined by $\beta^2 - 2\,x(T_2)\,\beta - 1$. The discriminant of this equation is equal to $\frac{1}{8}(p + u\,\sqrt{p})$ whose norm is p. So we conclude that there are no 4-torsion points defined over L and that

$$E_0(K)_{\text{tors}} = E_0(L)_{\text{tors}} = \mathbb{Z}/2\mathbb{Z}\,T_1 \oplus \mathbb{Z}/2\mathbb{Z}\,T_2 \qquad E_0(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z}\,T_1\,.$$

This end the proof of the proposition. □

5. Curves with isogenies

Let E be an elliptic curve of conductor p who admits an isogeny defined over $\mathbb{Q}$. According to the Proposition 2, the prime p is either of the form $u^2 + 64$ and there are two curves in the isogeny class or p is in the set $\{11, 17, 19, 37\}$ as shown in the table in Section 2.

Let $E'/\mathbb{Q}$ be one of the elliptic curves isogenous to E. The image of a given cyclic subgroup C of order p on E under the isogeny is a cyclic subgroup C' of order p in E', since the degree of the isogeny is prime to p. Similar to the self-points, we can also consider the point $x'_C = (E', C')$ on the modular curve $X_0(p)$ and its image P'_C in E. This point, just as the self-point P_C is also defined over $\mathbb{Q}(C)$. The proof of Proposition 3 applies just the same to show that the point P'_C is of infinite order in $E(\mathbb{Q}(C))$. The set of points $\{P'_C\}$ as C runs through all cyclic subgroups C of order p in E will be a copy of the Steinberg representation in $E(K)$, hence of rank p. The only way that this group generated by P'_C could intersect the group generated by P_C is that, for every given C, the points P_C and P'_C are linearly dependant. Unfortunately we are not able to show that P_C and P'_C are linearly independent, but it might well be the case.

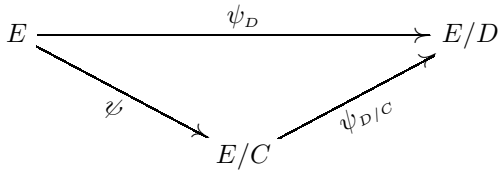
So it looks likely that we actually have $\text{rank}(E(K)) \geqslant i \cdot p$ where i is the number of curves in the isogeny class of E over $\mathbb{Q}$. For the curves of conductor 11, 17 and 19 we will prove it later. Note that if all the 2-torsion points of E were defined over $\mathbb{Q}$ – something which can never happen for optimal curves of prime conductor – then we would have a relation between the points $\{P'_C\}$. For more details on these more subtle questions, we refer to [Wut07].

6. Higher Self-points

Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor p. We also fix a cyclic subgroup C of order p on E. Applying the Atkin-Lehner involution w_p to x_C gives a point

$y_C = (E/C, \hat{C})$ on $X_0(p)$ whose image in $E(\mathbb{Q}(C))$ differs from $a_p \cdot P_C$ by a rational 2-torsion point. Recall that $a_p = \pm 1$ with the sign depending on whether E has split or non-split multiplicative reduction at p. The cyclic group $\hat{C}$ of order p on the isogenous curve E/C is the kernel of the dual isogeny.

Let $n \geqslant 1$ be an integer and let D be a cyclic subgroup of E of order p^n which contains C. The isogeny ψ_D of kernel D factors through



We consider the point $y_D = (E/D, \psi_{D/C}(\hat{C}))$ on $X_0(p)$. Note that this is well-defined since $\psi_{D/C}(\hat{C})$, which we denoted by $C^{(D)}$ in the introduction, is indeed cyclic of order p. We define P_D to be the image of y_D in $E(\mathbb{Q}(D))$. The Galois closure of $\mathbb{Q}(D)$ is denoted by K_n, it is a $\mathrm{PGL}_2(\mathbb{Z}/p^n\mathbb{Z})$-extension of $\mathbb{Q}$ inside $\mathbb{Q}(E[p^n])$.

Theorem 8. *The group generated by the points P_D in $E(K_n)$ as D runs through all the cyclic subgroups of order p^k with $k \leqslant n$ is of rank $p^n + p^{n-1} - 1$. In particular all of the points P_D are of infinite order.*

Proof. Let B be the subgroup of D of order p^{n-1} and let C be the subgroup of order p. In fact, we will prove the following trace relation

$$\mathrm{tr}_{\mathbb{Q}(D)/\mathbb{Q}(B)}(P_D) = a_p \cdot P_B \,. \tag{6.1}$$

The Hecke operator T_p acts on the divisor $(y_B) - (\infty)$ as

$$T_p\big((y_B) - (\infty)\big) = \sum_A \Big(\big((E/B)/A, (\psi_{B/C}(\hat{C}) + A)/A\big) - (\infty)\Big)$$

where A runs over all cyclic subgroups of order p in E/B with trivial intersection with $\psi_{B/C}(\hat{C})$. Let D' be the preimage of A under ψ_B. It has order p^n and the fact that it intersects trivially with $\psi_{B/C}(\hat{C})$ proves that D' is a cyclic subgroup of E. Moreover the cyclic subgroup $(\psi_{B/C}(\hat{C}) + A)/A$ of order p is equal to $\psi_{D'/C}(\hat{C})$. Hence

$$T_p\big((y_B) - (\infty)\big) = \sum_{D'} \big((E/D', \psi_{D'/C}(\hat{C})) - (\infty)\Big) = \sum_{D'} \Big((y_{D'}) - (\infty)\Big)$$

with the sum this time running over all cyclic subgroups D' of E of order p^n containing B. Now we consider the image of the above under the modular parametrisation $\varphi_E \colon J_0(p) \longrightarrow E$. The left hand side will map to $a_p \cdot P_B$ and the right hand side to

$$a_p \cdot P_B = \sum_{D'} P_{D'} = \mathrm{tr}_{\mathbb{Q}(D)/\mathbb{Q}(B)}(P_D)$$

since the Galois conjugates of y_D are exactly all of the $y_{D'}$.

Having proved the formula (6.1), we know by induction on n that the points P_D are of infinite order. Let us look at the rational $\mathrm{PGL}_2(\mathbb{Z}/p^n\mathbb{Z})$-representation V whose basis $\{e_D\}$ is in bijection with the set $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$ of all cyclic subgroups D in E of order p^n. According to [Sil70], page 58, this representations decomposes as

$$V = W_0 \oplus W_1 \oplus W_2 \oplus \cdots \oplus W_n$$

where W_i is an irreducible representation of dimension $p^i - p^{i-2}$ if $i > 1$, denoted $u_{1,i}$ in [Sil70], and $W_1 = \mathrm{St}$ is the Steinberg representation considered earlier. There is a $\mathrm{Gal}(K_n/\mathbb{Q})$-equivariant map from V to $E(K_n) \otimes \mathbb{Q}$ sending e_D to P_D. We prove by induction on n that the kernel of this map is the trivial subspace W_0. For $n = 1$ this coincides with the statement of Theorem 1. To prove the statement it is now enough to note that if the map from W_n to $E(K_n) \otimes \mathbb{Q}$ were not injective then all of the P_D would have to be of finite order in contradiction with (6.1).

Hence $\mathrm{rank}(E(K_n)) \geqslant \dim_{\mathbb{Q}}(V) - \dim_{\mathbb{Q}}(W_0) = (p+1) \cdot p^{n-1} - 1$. □

A little bit stronger, we can even claim that we have the following bound

$$\mathrm{rank}(E(K_n)) \geqslant p^n + p^{n-1} - 1 + \mathrm{rank}(E(\mathbb{Q}))\,.$$

Such asymptotic lower bound were already found by Harris in [Har79]. It is likely that one could obtain the formula $i \cdot (p^n + p^{n-1} - 1)$ with i begin the number of curves in the isogeny class of E over $\mathbb{Q}$. On the other hand this bound is far from the upper bounds coming from non-commutative Iwasawa theory. We find in lemma 3.3 in [HS05] a lemma due to Howson giving an upper bound of the form $C \cdot p^{3n}$ for some constant C. Moreover the computations of root numbers (as in the next section) suggests that the rank of $E(K_n)$ should grow much faster than our bound. See also the recent work of Coates, Fukaya, Kato and Sujatha [CFKS06]. But we wish to emphasise that the self-points are so far the only explicitly known points of infinite order in the tower $E(K_n)$.

Of course, one can more generally consider higher self-points. Let ℓ be any prime different from p. Given a cyclic subgroup D of order ℓ in $E[\ell]$, one can consider the points $\varphi_E(E/D, (C+D)/D)$ which are defined over $\mathbb{Q}(C, D)$. They satisfy trace-relations like (6.1). These points live in the $\mathrm{PGL}_2(\mathbb{Z}_\ell)$-extension of $\mathbb{Q}(C)$. We will investigate these points in more details and greater generality in [Wut07].

7. Root numbers and Parity of the Selmer Group

We return now to the first layer of the tower. Let E be an elliptic curve of conductor p and let K and $\mathbb{Q}(C)$ be the fields as before. Since the point P_C is of infinite order the L-series of E over K and $\mathbb{Q}(C)$ should vanish at $s = 1$; at least if we believe the conjecture of Birch and Swinnerton-Dyer. More precisely the L-function $L(E, \rho_{\mathrm{St}}, s)$ twisted by the Steinberg representation which appeared in the proof of Propositions 4 should vanish at $s = 1$. Unfortunately, it is not even known whether or not this L-series admits an analytic continuation to $s = 1$. One is often able to

predict the vanishing of the L-series just by computing the associated root number, i.e. the sign of the conjectured functional equation. But unlike in the case of Heegner points, there will not be a link between the non-triviality of the self-point and some root number.

We define the root number of a representation as the product of the local ϵ-factors as in [Dok05]. It should coincide with the root number appearing in the functional equation of the corresponding L-series. In particular, by the root number $w(E/F)$ of E over a field F, we will mean the root number of E over F. Similarly $w(E, \rho)$ is the root number of E twisted by the Artin representation ρ.

Recall from section 4 that $\mathrm{PGL}_2(\mathbb{F}_p)$ admits a unique non-trivial 1-dimensional representation χ corresponding to the quadratic subfield $L = \mathbb{Q}(\sqrt{p^*})$ in K fixed by $\mathrm{PSL}_2(\mathbb{F}_p)$.

Theorem 9. *The root number $w(E/\mathbb{Q}(C))$ of E over $\mathbb{Q}(C)$ is $+1$ if $p \equiv 1 \pmod 4$ and -1 if $p \equiv 3 \pmod 4$. The root number of the twist by the twisted Steinberg representation $w(E, \chi \otimes \rho_{\mathrm{St}})$ is equal to -1. Over $\mathbb{Q}(E[p])$ and over K, the root number is always $+1$.*

Let s be $(-1)^{\frac{p-1}{2}}$. So L is a real quadratic field if and only if $s = +1$. We list the root numbers again in the following table.

$$\begin{aligned} w(E/\mathbb{Q}) &= a_p & w(E, \chi) &= -s \\ w(E/\mathbb{Q}(C)) &= s & w(E, \rho_{\mathrm{St}}) &= a_p \cdot s \\ w(E/K) &= +1 & w(E, \rho_{\mathrm{St}} \otimes \chi) &= -1 \end{aligned}$$

We refer to Rohrlich's article [Roh06] for the computation of the root number of E twisted by representations of $\mathrm{PGL}_2(\mathbb{F}_p)$ in the case E has good reduction at p.

Proof. We simply apply the nice formula of Vladimir Dokchitser in [Dok05]. For any number field F, his theorem 3 asserts that $w(E/F) = (-1)^{u+s}$ where u is the number of infinite primes in F and s is the number of places where E has split multiplicative reduction. So we will need the following

Lemma 10. *The prime p decomposes in $\mathbb{Q}(C)$ as $\mathfrak{p} \cdot \mathfrak{q}^p$ for two prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ with residue field $\mathbb{F}_p$. The reduction is split over these primes if and only if it is split at p over $\mathbb{Q}$.*

Proof. We suppose first that E has *split* multiplicative reduction at p.

From the description of E as a Tate curve over $\mathbb{Q}_p$, we get a short exact sequence of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules

$$0 \longrightarrow \mu[p] \longrightarrow E[p] \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0\,.$$

This sequence is not split. Hence there is only one cyclic subgroup C of order p on E defined over $\mathbb{Q}_p$. The other subgroups C are defined over a field obtained by adjoining a p-th root u of the Tate parameter q_E to $\mathbb{Q}_p$. Since $c_p = \mathrm{ord}_p(q_E) \leqslant 5$

is not divisible by p, the extension $\mathbb{Q}_p(u)$ is a totally ramified extension of degree p. So there are at least two embeddings of $\mathbb{Q}(C)$ into $\bar{\mathbb{Q}}_p$, i.e. there are at least two places above p in $\mathbb{Q}(C)$ of which one, say $\mathfrak{p}$, is non-ramified and the other, say $\mathfrak{q}$ has ramification index $e_\mathfrak{q} = p$. Since the degree of $[\mathbb{Q}(C) : \mathbb{Q}]$ is equal to $p+1$, we can not have any other places and the residue field degrees are $f_\mathfrak{q} = f_\mathfrak{p} = 1$. This proves the claim for curves with split multiplicative reduction.

Suppose now that the reduction is non-split multiplicative. Then there is a quadratic extension M of $\mathbb{Q}$, inert at p, over which the curve acquires split multiplicative reduction. See [Sil94, Ex. V.11]. The only quadratic sub-extension in K is the one fixed by $\mathrm{PSL}_2(\mathbb{F}_p)$ which must be the unique quadratic extension unramified outside p and therefore ramified at p. Therefore K is linearly disjoint from M.

Hence, we can pass from $\mathbb{Q}$ to M over which E has split reduction at the unique unramified prime above p. Then the decomposition in the claim holds for $M \cdot \mathbb{Q}(C)/M$. He can get down to $\mathbb{Q}(C)/\mathbb{Q}$ afterwards. □

In fact one can prove easily that $\mathbb{Q}(E[p])$ has p^2-1 places above p with $e = p\cdot(p-1)$ and $f = 1$. Similarly for K, the $\mathrm{PGL}_2(\mathbb{F}_p)$-extension, there are $p+1$ places above p with $e = p\cdot(p-1)$ and $f = 1$. Since f is always equal to 1, the type of reduction at a place above p can never change from non-split to split multiplicative reduction.

Since p is odd, we know that $E(\mathbb{R})[p] = \mathbb{Z}/p\mathbb{Z}$. Therefore we have that $E(\mathbb{C})[p]$ splits into $\mathbb{Z}/p\mathbb{Z} \oplus \mu[p]$ as a $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-module. Therefore there are exactly two embeddings of $\mathbb{Q}(C)$ into $\mathbb{R}$, i.e. two real places in $\mathbb{Q}(C)$ and $\frac{p-1}{2}$ complex places.

Hence we can compute the various root numbers. For $\mathbb{Q}(C)$, this yields $u = 2 + \frac{p-1}{2}$ and $s = 2$, if the reduction is split, and $s = 0$, if the reduction is non-split. Therefore we conclude that

$$w(E/\mathbb{Q}(C)) = (-1)^{\frac{p-1}{2}} = s\,.$$

For $\mathbb{Q}(E[p])$ there are no real places, so $u \equiv 0 \pmod 2$ and $s = p^2-1$ or $s = 0$. Finally for K, we have no real places either and $p+1$ prime ideals above p.

The part of St on which the action of the complex conjugation is -1 has dimension $\frac{p-1}{2}$. The subspace of St fixed by the inertia group I_p at any place above p, which can be represented as the group of matrices $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$, is 1-dimensional with trivial action of Frobenius on it. Therefore theorem 1 in [Dok05] implies

$$\begin{aligned} w(E, \rho_{\mathrm{St}}) &= w(E/\mathbb{Q})^p \cdot (-1)^{\dim(\rho^-)} \cdot (-a_p)^{\dim\rho - \dim\rho^{I_p}} \cdot \det(\mathrm{Frob}_p\,|\rho^{I_p}) \\ &= a_p^p \cdot (-1)^{\frac{p-1}{2}} \cdot (-a_p)^{p-1} \cdot 1 = (-1)^{\frac{p-1}{2}} \cdot a_p = s \cdot a_p\,. \end{aligned}$$

It is also possible to use the previous computations of $w(E/\mathbb{Q}(C))$ and the fact that $\mathrm{Ind}_{\mathbb{Q}}^{\mathbb{Q}(C)}\,\mathbb{1} = \mathbb{1} \oplus \rho_{\mathrm{St}}$ together with the Artin formalism. With the same sort of computation one finds the versions twisted by χ.

From the above theorem and the parity conjecture, it is natural to expect that the rank of the Mordell-Weil group $E(\mathbb{Q}(C))$ is even if and only if p is congruent

to 1 modulo 4. We can only prove a weaker result by replacing the rank of the Mordell-Weil group by the corank of the Selmer group.

For any number field F, let $Ш(E/F)$ be the Tate-Shafarevich group of E over F. We will denote by $\mathrm{Sel}_{p^\infty}(E/F)$ the usual p-power Selmer group which fits into the exact sequence

$$0 \longrightarrow E(F) \otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p} \longrightarrow \mathrm{Sel}_{p^\infty}(E/F) \longrightarrow Ш(E/F)(p) \longrightarrow 0\,.$$

By the corank of the p-power Selmer, we mean the rank of the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(E/F)$. Hence if the p-primary part $Ш(E/F)(p)$ of the Tate-Shafarevich group is finite, then this corank is nothing else but the rank of the Mordell-Weil group $E(F)$.

Theorem 11. *Let E be an elliptic curve of conductor p and let $\mathbb{Q}(C)$ be the field obtained by adjoining a cyclic group of order p in E to $\mathbb{Q}$. Then the corank of the p-power Selmer group is even if $p \equiv 1 \pmod 4$ and odd if $p \equiv 3 \pmod 4$.*

Proof. One way to state the parity conjecture is the say that the parity of the p-power Selmer group is even if and only if the root number is $+1$. In our when case E admits an isogeny of degree p over $\mathbb{Q}(C)$, the parity conjecture has been proved in [DD06]. Hence the theorem follows from theorem 9.

Equally well one can also show the theorem directly. The proof of Shuter in [Shu06] in the case of good reduction can be adapted to our situation. The result actually does not differ from Shuter's result. □

7.1. *Examples*

In the following examples we will assume that all relevant Tate-Shafarevich groups are finite. For the curves of conductor 11, the above theorem shows that the rank over $\mathbb{Q}(C)$ must be odd. If we even believe that the points constructed via isogenies in 5 are linearly independent of the self-points then the rank would have to be at least 3.

On the other hand, the curve of conductor 17 must have even rank over $\mathbb{Q}(C)$. Since the self-point P_C is of infinite order, the rank has to be at least 2.

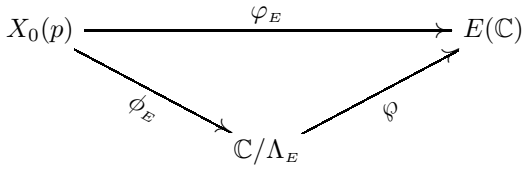
For the curve of conductor 43, the rank over $\mathbb{Q}(C)$ should be odd. The curve has a point of infinite order in $E(\mathbb{Q})$ and there is the self-point P_C which is of infinite order. Hence the rank of $E(\mathbb{Q}(C))$ has to be at least 3.

In the following table, we summarise the situation. The first line contains the root number $w(E/\mathbb{Q}) = a_p$, the second the value of s and the third the number of isogenous curves of E over $\mathbb{Q}$. Finally the last line gives a lower bound on the rank of $E(\mathbb{Q}(C))$ assuming that the Tate-Shafarevich groups are finite and that points constructed via isogenous curves are linearly independent.

Curve	11a1	17a1	19a1	37a1	37b1	43a1	53a1	61a1	67a1	73a1
a_p	$+1$	$+1$	$+1$	-1	$+1$	-1	-1	-1	$+1$	$+1$
s	-1	$+1$	-1	$+1$	$+1$	-1	$+1$	$+1$	-1	$+1$
i	3	4	3	1	3	1	1	1	1	2
r	3	4	3	2	4	3	2	2	1	2

8. Numerical examples

We use the analytic point of view of the modular parametrisation in order to give an experimental and a computational study of our self-points. Let $\mathbb{H}$ denote the upper half plane. The space $X_0(p)$ can be defined as the quotient of $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ by the congruences subgroup $\Gamma_0(N)$. The modular parametrisation is then given by the following diagram.



where $\Lambda_E = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ is the period lattice attached to E with ω_1 the real and ω_2 the imaginary period of E. The map $\wp$ is the analytic isomorphism from $\mathbb{C}/\Lambda_E$ to $E(\mathbb{C})$ given by the Weierstrass function and its derivative. For $\tau \in X_0(N) \setminus \{\text{cusps}\}$, the value $\phi_E(\tau)$ is given by the converging series

$$\begin{aligned} \phi_E \colon X_0(p) &\longrightarrow \mathbb{C}/\Lambda \\ \tau &\longmapsto \sum_{n \geqslant 1} \frac{a_n}{n} q^n \quad \text{with } q = \exp(2i\pi\tau)\,. \end{aligned}$$

This is a rapidly converging series; bounding the coefficients a_n/n by 2 it is easy tho control the error made by truncating the series. One can also compute efficiently $\phi_E(0)$ since

$$\phi_E(0) = L(E,1) = 2\sum_{n \geqslant 1} \frac{a_n}{n} e^{-2\pi n/\sqrt{N}} \in \mathbb{C}/\Lambda\,.$$

As above the error made by truncating the series of the right hand size can be easily controlled. Since we know that $\varphi_E(0)$ is a rational torsion point of order dividing the numerator T of $(p-1)/12$ in $E(\mathbb{Q})$ we just have to recognise the number $\phi_E(0)$ in the finite set $\{j\omega_1/T,\ j = 0, 1, \ldots, T-1\}$. This can be done as soon as the error term is smaller than $\omega_1/2T$.

The index of the congruences subgroup $\Gamma_0(p)$ in $SL(2,\mathbb{Z})$ is $p+1$ and as a set of representative of $SL_2(\mathbb{Z})$ modulo $\Gamma_0(p)$ we choose the matrices

$$\begin{aligned} M_0 &= \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \\ M_j &= \left(\begin{smallmatrix} 0 & -1 \\ 1 & j \end{smallmatrix}\right) \quad \text{for } j = 1,\, 2 \ldots, p\,. \end{aligned}$$

With our analytic point of view, the self-points $x_C = (E, C)$ where C runs through all cyclic subgroups of order p are the $p+1$ points $\tau_0 = M_0\tau$, $\tau_1 = M_1\tau$,...,$\tau_p = M_p\tau$ where $\tau = \omega_2/\omega_1$. Our goal is to write down the points $P_C = \varphi_E(x_C)$ as an algebraic point in $E(\overline{\mathbb{Q}})$. For this, consider the polynomials

$$A_x(X) = \prod_{0 \leqslant j \leqslant p} (X - x(\varphi_E(\tau_j)))$$
$$A_y(X) = \prod_{0 \leqslant j \leqslant p} (X - y(\varphi_E(\tau_j)))$$

in $\mathbb{Q}[X]$ where $x(.)$ and $y(.)$ are the x and the y-coordinate functions of the minimal model of E. Since $\mathbb{Q}(C)$ is a primitive extension, the polynomials A_x and A_y are irreducible over $\mathbb{Q}$. In our numerical applications, those polynomials are given by real approximation of their coefficients, in order to recognise them as rational polynomials one need to bound their denominators.

Proposition 12. *Let $\mu = c_p$ if $\varphi_E(0) \neq O$ and $\mu = (p+1)c_p$ otherwise. Then the polynomials $p^{2\mu} \cdot A_x(X)$ and $p^{3\mu} \cdot A_y(X)$ have p-integral coefficients.*

Proof. For a point $P \neq O$ in the formal group $\widehat{E}(\mathfrak{m})$ with $\mathfrak{m}$ the maximal ideal in the integer ring of $\bar{\mathbb{Q}}_p$, we call $-\frac{1}{2}\log_p |x(P)|_p \in \mathbb{Q}$ the p-adic valuation of P where $\log_p$ is the logarithm in base p and $|\cdot|_p$ is the normalized p-adic absolute value. All points outside the formal group are said to have p-adic valuation 0.

If $\widetilde{C}$ corresponds to the point $x_{\tilde{C}}$ close to the cusp ∞, the exact denominator is given in the proof of Proposition 3 as we know that $\varphi_E(x_{\tilde{C}}) \in \hat{E}(p^{c_p}\mathbb{Z}_p)$. So $P_{\tilde{C}}$ has p-adic valuation c_p. Each of the other p points x_C is defined over a totally ramified extensions of degree p of $\mathbb{Q}_p$. All the points x_C are conjugate to each other, so they have the same p-adic valuation say $\lambda \in \frac{1}{p}\mathbb{Z}$. Proposition 4 asserts that

$$\sum_{C \neq \widetilde{C}} \varphi_E(x_C) = \varphi_E(0) + \varphi_E(x_{\tilde{C}})\,.$$

The sum on the left hand side must have p-adic valuation greater or equal to λ. If $\varphi_E(0) \neq O$ then the right hand size of the equation above has p-adic valuation 0 and so $\lambda = 0$. Whenever $\varphi_E(0) = O$ then the right hand size has p-adic valuation c_p and so $\lambda \leqslant c_p$. □

We believe that we always have $\lambda = 0$.

Proposition 13. *Suppose that the genus of $X_0(p)$ is 1 or that E is an involutary curve (i.e. $E \simeq X_0(p)/w_p$, where w_p is the Fricke involution), then the polynomials $p^{2c_p} \cdot A_x(X)$ and $p^{3c_p} \cdot A_y(X)$ have integral coefficients.*

Proof. Suppose that we are in the first case, the curve is the strong Weil curve and the genus is 1 hence the modular parametrisation is an isomorphism. We continue

to write $X_0(p)$ for the minimal model over $\mathbb{Z}$. Let υ be any place in $\mathbb{Q}(C)$ above $\ell \neq p$. Since the curve E has good reduction at υ, the point x_C can not belong to the kernel of reduction

$$X_0(\mathbb{Q}(C)_\upsilon) \longrightarrow \widetilde{X_0(p)}(\mathbb{F}_\upsilon)$$

where $\mathbb{Q}(C)_\upsilon$ is the completion of $\mathbb{Q}(C)$ at υ and $\mathbb{F}_\upsilon$ the reduction. Since E is isomorphic to $X_0(p)$, we see that the denominator ideal of $x(P_C)$ must be prime to υ. For the prime p, we are in the first case of proposition 12 since $\varphi_E(0)$ is different from O for all curves with $X_0(p)$ having genus 1.

If E is involutary then we are in one of the following nine cases:

$$E = 37\text{a1, } 43\text{a1, } 53\text{a1, } 61\text{a1, } 79\text{a1, } 83\text{a1, } 89\text{a1, } 101\text{a1 or } 131\text{a1.}$$

We can use the same argument for any place υ not above p in $\mathbb{Q}(C)$. Now, we have $\varphi_E(0) = O$ and we know that $p^{2(p+1)c_p} \cdot A_x(X)$ have integral coefficients hence we can compute it exactly and since there are finitely many curves we can see that in fact $p^{2c_p} \cdot A_x(X) \in \mathbb{Q}[X]$ in all cases. □

Whenever the genus of $X_0(p)$ is not 1 and E is not involutary, the proposition above is false in general. Numerical experimentions show that other primes than p could appear in the denominator of $A_x(X)$ and $A_y(X)$. Those "extra" primes can be large and are not well understood. For example, we computed numerically the polynomial $A_x(X)$ for the curve $E = 37b1$. We obtain a polynomial in $\mathbb{Q}[X]$ which agrees with $A_x(X)$ up to a large precision but we are not able to prove that it is the correct one (nevertheless a finite number of tedious computations could do it). We found that the denominator of $A_x(X)$ should be

$$3^2 \cdot 7^2 \cdot 37^6 \cdot 4137179^2 \cdot 94843837382759^2 .$$

The factor 37^6 is explained by Proposition 12. The occurrence of the other factors is rather surprising (especially for the large ones) and it would be interesting to understand where they come from.

When the genus is 1 or the curve E is involutary, we make use of the Proposition 13 to write down the point $P_C = \varphi_E(x_C)$ as an algebraic point. We explain this by the following examples.

8.1. *Example* $N = 11$

Consider

$$\begin{aligned} E = 11\text{a1} &: y^2 + y = x^3 - x^2 - 10\,x - 20 \\ 11\text{a2} &: y^2 + y = x^3 - x^2 - 7820 - 263580 \\ 11\text{a3} &: y^2 + y = x^3 - x^2 \end{aligned}$$

the three elliptic curves, up to isomorphism, with conductor $N = 11$ given in Cremona's table [Cre97]. The curve E =11a1 is the strong Weil curve. We use the

system pari-gp [PAR06] to perform the following computations. We have $L(E,1) = \omega_1/5$ and then the corresponding point in $E(\mathbb{C})$ is $\varphi_E(0) = \wp(\omega_1/5) = (16,-61)$ which is, of course, a rational point of order 5. We put $\tau = \omega_2/\omega_1 \approx 1/2 + 1.1494\imath$ and obtain

$$\begin{aligned} A_x(X) &= (X - \varphi_E(\tau)) \prod_{j=0}^{10} \left(X - \varphi_E\left(\frac{-1}{\tau + j}\right)\right) \\ &\approx X^{12} - 1858429.3660X^{11} + \cdots + 1027552848072306586730.7357 \end{aligned}$$

By the proposition above, we easily recognise

$$\begin{aligned} A_x(X) = {} & 11^{-10}(25937424601\, X^{12} - 48202871557476252\, X^{11} - 627575688471844224310\, X^{10} \\ & - 458658732238088364917875 6\, X^9 + 189861110415625174383936023\, X^8 \\ & - 945030753721506958510760088\, X^7 - 131769177742981760013465117 96\, X^6 \\ & + 558725269921007151668021541368\, X^5 + 410224605513627944306906984 3703\, X^4 \\ & + 127450465206787617939655862799 24\, X^3 + 256883853478668238668187276 20042\, X^2 \\ & + 329634625395858290679544840019 96\, X + 266520745204182602894841236 48825) \end{aligned}$$

This polynomial defines the primitive number field $\mathbb{Q}(C)$ of degree 12. The following polynomial $A(X)$ defines an isomorphic number field

$$X^{12} - 4\,X^{11} + 55\,X^9 - 165\,X^8 + 264\,X^7 - 341\,X^6 + 330\,X^5 - 165\,X^4 - 55\,X^3 + 99\,X^2 - 41\,X - 111$$

One can show that the class group of $\mathbb{Q}(C)$ is trivial. One can perform the same computations for the y-coordinate function. We find the following algebraic point $P_1 = P_C = (x_1, y_1)$ with

$$\begin{aligned} x_1 = {} & 2^{-1}\cdot 5^{-3}\cdot 11^{-10}\cdot 19^{-1}\cdot(133792802077952089\, \theta^{11} - 312848945005283368\, \theta^{10} - 502878903201648831\, \theta^9 \\ & + 6475439902255323868\, \theta^8 - 11358894741986615604\, \theta^7 + 17292758289068725628\, \theta^6 \\ & - 18719462641364369973\, \theta^5 + 16016249446153991254\, \theta^4 + 982764516960529358\, \theta^3 \\ & - 2408156353187544234\, \theta^2 + 8344249326459947483\, \theta + 7914557261562811262) \\ y_1 = {} & 2^{-1}\cdot 5^{-3}\cdot 11^{-15}\cdot 19^{-1}\cdot(28765696339563795386130989\, \theta^{11} - 65657747550440506261377918\, \theta^{10} \\ & - 11269698586114866747056593 1\, \theta^9 + 13884319285530415635459291 68\, \theta^8 - 23621336322675621662352755504\, \theta^7 \\ & + 35406441076323262080660464 28\, \theta^6 - 37320147448494291435816447 73\, \theta^5 + 30852734269897485022352084 04\, \theta^4 \\ & + 55656995201591500953587315 8\, \theta^3 - 63894778162756748817116588 4\, \theta^2 + 17768990222332713878701247 83\, \theta \\ & + 18481996667436121905878639 62) \end{aligned}$$

where θ is a root of $A(X)$. Note that the numerator of these numbers are actually divisible in the ring of integers of $\mathbb{Q}(C)$ by the integers different from 11 appearing in the denominator above; just as predicted by the proof of Proposition 13. As θ is running through the roots of $A(X)$ in a fixed Galois closure of $\mathbb{Q}$, the points given by the above formula describe the conjugates of the image by φ_E of our self-point. In other words we obtain all the points P_C as C runs through the cyclic subgroups

of order p in $E[p]$. Then, one can explicitly compute the point $\sum_C P_C$ and we find the 5-torsion point $(16,-61)$ as predicted by Proposition 4.

In fact, one has the easier expression for P_1 since we have $P_1 = (x_1', y_1') + (16,-61)$ with

$$\begin{aligned} x_1' &= 2^{-1}\cdot 5^{-3}\cdot 11^{-2}\cdot 19^{-1}\cdot(-1669\theta^{11}+33828\theta^{10}-81349\theta^9-183828\theta^8+1717484\theta^7-3471788\theta^6+4165033\theta^5 \\ &\quad -4576634\theta^4+2336882\theta^3+3088214\theta^2-4748743\theta+4861598)\,, \\ y_1' &= 2^{-1}\cdot 5^{-3}\cdot 11^{-3}\cdot 19^{-1}\cdot(-233091\theta^{11}+1788042\theta^{10}-2346611\theta^9-1607379 2\theta^8+829493 76\theta^7-148123732\theta^6 \\ &\quad +18127978 7\theta^5-175063476\theta^4+56212398\theta^3+138667596\theta^2-195077977\theta+186910572)\,. \end{aligned}$$

We can also compute with the same method the algebraic points on E coming from the self-points of the isogenous curves 11a2 and 11a3. We find the following points $P_2 = (x_2, y_2) + (16,-61)$ and $P_3 = (x_3, y_3)$ with

$$\begin{aligned} x_2 &= 2^{-1}\cdot 5^{-3}\cdot 11^{-2}\cdot 19^{-1}\cdot(1594026\theta^{11}-6388637\theta^{10}+702246\theta^9+86307137\theta^8-265102036\theta^7+450584852\theta^6 \\ &\quad -609415332\theta^5+67851076 1\theta^4-389518078\theta^3-208816706\theta^2+158121422\theta-162620467)\,, \\ y_2 &= 2^{-1}\cdot 5^{-3}\cdot 11^{-2}\cdot 19^{-1}\cdot(-16692116\theta^{11}+95324467\theta^{10}-78704636\theta^9-1037899217\theta^8+4171219776\theta^7 \\ &\quad -7057412532\theta^6+8919208962\theta^5-122722847 51\theta^4+97185455 98\theta^3-6416053004\theta^2+86043233 48\theta-356847003) \end{aligned}$$

and

$$\begin{aligned} x_3 &= 2^{-1}\cdot 5^{-3}\cdot 11^{-2}\cdot(11\theta^{11}+40293\theta^{10}-485694\theta^9+1502457\theta^8-2828496\theta^7+4716822\theta^6-5419227\theta^5+2855721\theta^4 \\ &\quad +1781967\theta^3-2734116\theta^2+1252592\theta+1304413)\,, \\ y_3 &= 2^{-1}\cdot 5^{-3}\cdot 11^{-2}\cdot(-9727989\theta^{11}+90416293\theta^{10}-386035694\theta^9+853672457\theta^8-1247148496\theta^7+1474894322\theta^6 \\ &\quad -1275534227\theta^5+521439721\theta^4+268493467\theta^3-363165616\theta^2+55053592\theta+386303413)\,. \end{aligned}$$

Using the system magma [BCP97], we can compute the canonical Néron-Tate height of these points.

$$\hat{h}(P_1) = 3.733 \qquad \hat{h}(P_2) = 6.420 \qquad \hat{h}(P_3) = 2.117$$

The determinant of the height matrix is equal to 1301.155. This proves the assertion that the the three selfpoints P_1, P_2 and P_3 generate a group of rank 3 in $E(\mathbb{Q}(C))$. From the proof of Theorem 8, we can now deduce that the rank of the group generated by higher self-points in $E(K_n)$ is at least

$$\operatorname{rank} E(K_n) \geqslant 3\cdot p^n + 3\cdot p^{n-1} - 3\,.$$

8.2. *Conductor* 17 *and* 19

Let E be the curve 17a1; its isogeny class contains four elliptic curves. The field $\mathbb{Q}(C)$ is defined by the polynomial

$$X^{18}-7X^{17}+17X^{16}+17X^{15}-935X^{14}+799X^{13}+9231X^{12}-41463X^{11}+192780X^{10}+291686X^9-390014X^8$$
$$+6132223X^7-3955645X^6+2916112X^5+45030739X^4-94452714X^3+184016925X^2-141466230X+113422599\,.$$

The four selfpoints P_1, P_2, P_3 and P_4 coming from the four isogenous elliptic curves have rather complicated coordinates but can be computed with the same method as for $p = 11$. The canonical Néron-Tate height of these points are as follows.

$$\hat{h}(P_1) = 2.707 \qquad \hat{h}(P_2) = 2.271 \qquad \hat{h}(P_3) = 2.896 \qquad \hat{h}(P_4) = 1.786$$

The determinant of the height matrix is equal to 4594.647. This proves the assertion that the four selfpoints P_1, P_2, P_3 and P_4 generate a group of rank 4 in $E(\mathbb{Q}(C))$. From the proof of Theorem 8, we can now deduce that that the rank of the group generated by higher self-points in $E(K_n)$ is at least

$$\operatorname{rank} E(K_n) \geqslant 4 \cdot p^n + 4 \cdot p^{n-1} - 4\,.$$

Let E be the curve 19a1; there are three elliptic curves in its isogeny classes. The field $\mathbb{Q}(C)$ is defined by the polynomial

$$X^{20}-5X^{19}+76X^{18}-247X^{17}+1197X^{16}-8474X^{15}+15561X^{14}-112347X^{13}+325793X^{12}-787322X^{11}$$
$$+3851661X^{10}-5756183X^{9}+20865344X^{8}-48001353X^{7}+45895165X^{6}-245996344X^{5}$$
$$+8889264X^{4}-588303992X^{3}-54940704X^{2}-538817408X+31141888\,.$$

In this case, the canonical Néron-Tate height of the points P_1, P_2 and P_3 are

$$\hat{h}(P_1) = 2.257 \qquad \hat{h}(P_2) = 3.207 \qquad \hat{h}(P_3) = 1.576$$

The determinant of the height matrix is equal to 469.791. This proves that

$$\operatorname{rank} E(K_n) \geqslant 3 \cdot p^n + 3 \cdot p^{n-1} - 3\,.$$

8.3. *Example of the involutary curve E=37a1*

Let E be the involutary curve 37a1; there is just E in its isogeny classes. The field $\mathbb{Q}(C)$ is defined by

$$X^{38}-12X^{37}+6845X^{34}-4107X^{33}+611943X^{32}+6419241X^{31}-23619357X^{30}-1139989573X^{29}-7189689558X^{28}$$
$$+15195444123X^{27}+421676681701X^{26}+1049261700469X^{25}-24717066801390X^{24}-348296732228468X^{23}$$
$$-2419574069703120X^{22}-8165136099970176X^{21}+1447503346302976 2X^{20}+268023003210734612X^{19}$$
$$+329661477773764104X^{18}-114200153548012456 70X^{17}-945680585900565727 26X^{16}-270708469237425691308X^{15}$$
$$+701411470253839139591X^{14}+856800261728055274 5928X^{13}+225636679683326896060 38X^{12}$$
$$-668822156499688413109 16X^{11}-706898153127401380189661X^{10}-217221050084659700064 1917X^{9}$$
$$-931554706376597876718 57X^{8}+254763955902223383154039 99X^{7}+115054283689855001616765285X^{6}$$
$$+297976894378693703291782499X^{5}+526572254394503227631311356X^{4}+665351270233256888369987865X^{3}$$
$$+573638845689345417051088091X^{2}+357303812435373401026408215X+585578575222824132475605000\,.$$

In this case, the curve E has rank one over $\mathbb{Q}$ and hence

$$\operatorname{rank} E(K_n) \geqslant p^n + p^{n-1}\,.$$

Acknowledgments

The authors would like to thank John Coates, Henri Darmon, Vladimir Dokchitser, Bas Edixhoven, Yoshitaka Hachimori, Xavier-François Roblot, and Mike Shuter for helpful discussions. The second author is supported by a fellowship of the Swiss National Science Foundation

References

[AU96] Ahmed Abbes and Emmanuel Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. **103** (1996), no. 3, 269–286.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[CFKS06] John Coates, Takako Fukaya, Kazuya Kato, and Ramdorai Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory*, In preparation, 2006.

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[DD06] Tim Dokchitser and Vladimir Dokchitser, *Parity of Ranks for Elliptic Curves with a Cyclic Isogeny*, preprint, available at *http://arxiv.org/format/math.NT/0604149* , 2006.

[Dok05] Vladimir Dokchitser, Root numbers of non-abelian twists of elliptic curves*, Proc. London Math. Soc. (3)* ***91*** *(2005), no. 2, 300–324, With an appendix by Tom Fisher.*

[DR73] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II, Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.*

[Har79] Michael Harris, Systematic growth of Mordell-Weil groups of abelian varieties in towers of number fields*, Invent. Math.* ***51*** *(1979), no. 2, 123–141.*

[HS05] Yoshitaka Hachimori and Romyar T. Sharifi, On the failure of pseudo-nullity of Iwasawa modules*, J. Algebraic Geom.* ***14*** *(2005), no. 3, 567–591.*

[Lan02] Serge Lang, Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.*

[Miy73] Isao Miyawaki, Elliptic curves of prime power conductor with **Q**-rational points of finite order*, Osaka J. Math.* ***10*** *(1973), 309–323.*

[MO89] J.-F. Mestre and J. Oesterlé, Courbes de Weil semi-stables de discriminant une puissance m-ième*, J. Reine Angew. Math.* ***400*** *(1989), 173–184.*

[Neu71] Olaf Neumann, Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. I*, Math. Nachr.* ***49*** *(1971), 107–123.*

[Neu73] ———, Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. II*, Math. Nachr.* ***56*** *(1973), 269–280.*

[PAR06] The PARI Group, Bordeaux, PARI/GP, version `2.3.1`*, 2006, available from http://pari.math.u-bordeaux.fr/* .

[Roh06] David E. Rohrlich, Root numbers of semistable elliptic curves in division towers*, Math. Res. Lett.* ***13*** *(2006), no. 2-3, 359–376.*

[Ser72] Jean-Pierre Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math.* ***15*** *(1972), no. 4, 259–331.*

[Ser96] ———, Travaux de Wiles (et Taylor, ...). I*, Astérisque (1996), no. 237, Exp.*

No. 803, 5, 319–332, Séminaire Bourbaki, Vol. 1994/95.

[Set75] *Bennett Setzer,* Elliptic curves of prime conductor*, J. London Math. Soc. (2)* ***10*** *(1975), 367–378.*

[Shu06] *Micheal Shuter,* Rational Points of Elliptic Curves in p-Division Fields*, preprint in preparation, 2006.*

[Sil70] *Allan J. Silberger,* PGL_2 over the p-adics: its representations, spherical functions, and Fourier analysis*, Lecture Notes in Mathematics, Vol. 166, Springer-Verlag, Berlin, 1970.*

[Sil94] *Joseph H. Silverman,* Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.*

[SW04] *William Stein and Mark Watkins,* Modular parametrizations of Neumann-Setzer elliptic curves*, Int. Math. Res. Not. (2004), no. 27, 1395–1405.*

[Wut07] *Christian Wuthrich,* Self-points on elliptic curves*, In preparation, 2007.*