SOME REMARKS ON SELF-POINTS ON ELLIPTIC CURVES

by

Christophe Delaunay & Christian Wuthrich

Abstract. — In a previous article ([**DW09**]), we studied self-points on elliptic curves of prime conductors, p. The non-triviality of these points was proved in general using a local argument and the modular parametrization over the field $\mathbb{Q}_p$. In this paper, we focus on the special case of Neumann-Setzer curves and we give an alternative proof of the non-triviality of self-points using the complex side of the modular parametrization. To obtain this, we prove several estimates, which can be used further to get results about Neumann-Setzer curves and their modularity.

Résumé. — Dans un article précédent ([**DW09**]), nous avons étudié les self-points des courbes elliptiques de conducteurs premiers, p. La non trivialité de ces points a été établie en général en utilisant un argument local et la paramétrisation modulaire sur le corps $\mathbb{Q}_p$. Dans ce papier, nous nous concentrons sur le cas particulier des courbes de Neumann-Setzer et nous donnons une démonstration différente de la non-trivialité des self-points grâce à l'aspect complexe de la paramétrisation modulaire. Pour cela, nous obtenons plusieurs estimations que nous utilisons ensuite pour prouver d'autres résultats sur les courbes de Neumann-Setzer et sur leurs aspects modulaires.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. We denote by $X_0(N)$ the modular curve of level N, it is well known, from the modularity properties of E, that there exists a modular parametrization:

$$\varphi\colon X_0(N) \longrightarrow\!\!\!\!\!\rightarrow E$$

sending the cusp $\infty \in X_0(N)$ to the neutral element O of E. A non-cuspidal point $y \in X_0(N)$ can be understood as an isomorphism class of pairs (F, C) where F is an elliptic curve and C is a cyclic subgroup of order N of F. It is a classical and natural problem to study miscellaneous properties of the points $x = \varphi(y) \in E$ whenever y have some specific and "interesting" description in $X_0(N)$.

The first author is supported by the ANR project no. 07-BLAN-0248 "ALGOL". He is also a member of the project "TraSecure" financed by the "Région Rhônes-Alpes" in France.

For instance, if y is a cusp in $X_0(N)$, the theory of Manin-Drinfeld gives that $\varphi(y)$ is a torsion-point in E and that its order can be controlled. Modular symbols also allow us to compute the point $\varphi(y)$ in this case ([**Cre97**, chapter 2]).
An other example is given by Heegner points. An Heegner point has the form $y = (F, C) \in X_0(N)$, where F and F/C have complex multiplication by the same order $\mathcal{O}$ of an imaginary quadratic field. The Gross-Zagier theorem ([**GZ86**]) gives necessary and sufficient conditions that $x = \varphi(y)$ is a non-torsion point in $E(H)$ where H is some number field associated to $\mathcal{O}$. The Gross-Zagier theorem has many theoretical and explicit applications. In particular, in combination with the complex interpretation of Heegner points, it leads to a very efficient algorithm for computing a generator of the Mordell-Weil group $E(\mathbb{Q})$ whenever E has analytic rank 1 (for example, [**Coh07**, chapter 8]).
The images of some other natural points have also been considered (see [**Har79**], [**Kur73**], etc.) with the perspective to study the rank of the $E(L)$ in some infinite Iwasawa extensions L. A special case of these points are the so-called "self-points" in the title. They were defined and have also been investigated in [**DW09**] and [**Wut09**].

Definition 1.1. — A self-point, $P_C \in E$, is a point $P_C = \varphi(y_C)$ where y_C is of the form $y_C = (E, C) \in X_0(N)$.

Note that there are $\#\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ cyclic subgroups, $C \subset E$, of order N. The question of the rank generated by the self-points (and also by the "higher" self-points) has been studied in generality in [**Wut09**]. One of the key ingredient is to determine when the point P_C is a non-torsion point. This can indeed be done in most of the cases by considering the modular parametrization over the local field $\mathbb{Q}_p$ where p is some well-chosen prime dividing N.
Whenever the conductor $N = p$ is prime, the local argument is always valid and it can be shown ([**DW09**]) that the self-points P_C are non-torsion points in $E(\mathbb{Q}(C))$, where $\mathbb{Q}(C)$ is the field of definition of C. This implies that the points $(P_C)_C$, where C is running through the $p + 1$ cyclic subgroups of order p, generate a group of rank p in $E(K)$ where K is the compositum of the fields $\mathbb{Q}(C)$. Note that the Galois group of $K/\mathbb{Q}$ is $G \simeq \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$.

The aim of this paper is to focus on the special cases when E are Neumann-Setzer curves and to show that by considering the modular parametrization φ over the complex field $\mathbb{C}$ (rather than $\mathbb{Q}_p$) may also provide some results on these points.
In section 2, we will briefly sum up the results in [**DW09**] about self-points on elliptic curves of prime conductor.
Neumann-Setzer curves are special curves of prime conductor p and will be described in section 3.
Then, we will restrict our attention to these curves. In section 4, we will give a precise description of the modular parametrization over $\mathbb{C}$. This will allow us to study the map φ. In particular, we will obtain an alternative proof that the self-points are non-torsion.
This requires some technical and more or less precise estimates. We will also use them in order to give additional remarks that are not exactly related to the study of self-points but that we believe to be interesting nonetheless. In section 5, we will study the growth of the modular degree of the Neumann-Setzer curves and give an explicit way for computing the analytic order of the Tate-Shafarevich groups of the Neumann-Setzer curves.

2. Self-points on elliptic curves of prime conductor

Let E be an elliptic curve defined over $\mathbb{Q}$ with prime conductor p. We give here some basic properties related to the self-points of E, see **[DW09]** for proofs and more details.

The number field $\mathbb{Q}(E[p])$ obtained by adjoining the coordinates of the p-torsion points of E to $\mathbb{Q}$ is Galois and the Galois group $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ is identified with $\mathrm{GL}_2(\mathbb{F}_p)$ via the classical Galois representation:

$$\bar{\rho}_p\colon \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p),$$

which is an isomorphism.

Let $C \subset E$ be a cyclic subgroup of order p, then the field $\mathbb{Q}(C)$ is the subfield of $\mathbb{Q}(E[p])$ fixed by a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ and so it is a primitive non-Galois field of degree $p+1$. From the fact that $\mathbb{Q}(C)$ does not contain any non-trivial subfield, we can deduce that $E(\mathbb{Q}(C))_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$.

As C is running through all the $p+1$ cyclic subgroups of order p, the fields $\mathbb{Q}(C)$ are all conjugate. Their Galois closure is the field $K \subset \mathbb{Q}(E[p])$ and $\mathrm{Gal}(K/\mathbb{Q})$ is identified with $\mathrm{PGL}_2(\mathbb{F}_p)$ via $\bar{\rho}_p$. Since the map φ is defined over $\mathbb{Q}$, the self-points inherit of the algebraic properties of $\mathbb{Q}(C)$:

Proposition 2.1. — *We have:*

- *The point P_C lies in $E(\mathbb{Q}(C))$.*
- *The set $\{P_C\}_C$ form a single orbit under the action of $\mathrm{Gal}(K/\mathbb{Q})$ in $E(K)$.*

It follows immediately from this proposition and from $E(\mathbb{Q}(C))_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$ that if a self-point P_C were a torsion point it would be rational all the other self-points should also be rational and equal. This is trivially impossible if $\deg(\varphi) < p+1$ (see remark 5.1.1 about this fact). Furthermore, we have that $\mathrm{tr}_{K/\mathbb{Q}} P_C = \sum_C P_C$ is a torsion point, so if P_C were rational then P_C would be a torsion point.

In **[DW09]**, we proved that this case can not occur since we obtained:

Theorem 2.2. — *With the previous notations, we have:*

- *The self-points P_C are of infinite order.*
- *The $p+1$ self-points $\{P_C\}_C$ generate a rank p group in $E(K)$ and $\sum_C P_C$ is the rational torsion point $\varphi(0) \in E(\mathbb{Q})$.*

The first point is proved by considering the p-adic interpretation of φ. The second point comes from a linear argument (using the irreducibility of the Steinberg representation of $\mathrm{PGL}_2(\mathbb{F}_p)$) and from the first point. This second point is in fact a corollary of the first one. In section 4, we will give a new proof of the first point using the complex interpretation of the modular parametrization in the case when E is a Neumann-Setzer curve.

3. Neumann-Setzer curves

Let $u \in \mathbb{Z}$ be an odd integer such that $u \equiv 3 \pmod 4$. Suppose that $p = u^2+64$ is prime. Such a prime will be called a Neumann-Setzer prime. The Neumann-Setzer curves of conductor p

are the following two isogenous curves:

$$\begin{aligned} E_p \ : \ y^2+xy &= x^3-\frac{u+1}{4}x^2+4x-u \\ F_p \ : \ y^2+xy &= x^3-\frac{u+1}{4}x^2-x \end{aligned}$$

We will write E and F if the Neumann-Setzer prime is understood. The curves E and F are isogenous by an isogeny of degree 2.

The discriminant of E is $\Delta = -p^2$ and its j-invariant is $-(u^2-192)^3/p^2$. The 2-division polynomial of E is given by:

$$P(x) = (4x-u)(x^2+4)$$

The group $E(\mathbb{Q})$ contains a rational 2-torsion point which is given by $(u/4, -u/8)$. The two other points of order 2 are defined over $\mathbb{Q}(\sqrt{-1})$ and are the points $\pm(2\sqrt{-1}, \sqrt{-1})$.

The discriminant of F is $\Delta = p$ and its j-invariant is $(u^2+48)^3/p^2$. The 2-division polynomial of F is given by:

$$P(x) = 4x\left(x^2+\frac{u}{4}x-1\right).$$

The points of order 2 of F are:

$$(0,0),\ \left(\frac{u+\sqrt{p}}{8}, -\frac{u+\sqrt{p}}{16}\right) \text{ and } \left(\frac{u-\sqrt{p}}{8}, -\frac{u-\sqrt{p}}{16}\right).$$

So that in this case, $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{p})$.

The curves of prime conductor and, in particular, Neumann-Setzer curves have been studied by many authors: **[Miy73]**, **[Neu71]**, **[Neu73]**, **[Set75]**, **[SW04]**,... . From these sources and from **[AU96]**, we have the following theorem (see **[DW09]**, for details):

Theorem 3.1. — *Let $p = u^2+64$ be a Neumann-Setzer prime with $u \equiv 3 \pmod 4$. Let E and F be the Neumann-Setzer curves as above.*

- *We have $E(\mathbb{Q}) \simeq F(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.*
- *We have $Ш(E/\mathbb{Q})[2] \simeq Ш(F/\mathbb{Q})[2] \simeq \{0\}$.*
- *The local Tamagawa number of E and F at the prime p is $c_p = 2$.*
- *The curve E is the strong Weil curve in its isogeny class and the Manin constant of E is equal to 1.*
- *The modular degree of E is even if and only if $u \equiv -1 \pmod 8$.*

Furthermore, if G is an elliptic curve of prime conductor such that $G(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$ then G is a Neumann-Setzer curve.

If E is an elliptic curve of prime conductor which is *not* a Neumann-Setzer curve then E has conductor 11, 17, 19, 37 or $E(\mathbb{Q})_{\text{tors}}$ is trivial. In the last case, E is the only curve in its isogeny class (and note that its rank can be positive).

It is not known if there exist infinitely many elliptic curves of prime conductor. Nevertheless, classical conjectures can be applied for the number of Neumann-Setzer primes.

Conjecture 3.2. — *Let $\pi_{NS}(x)$ be the number of Neumann-Setzer prime $p \leqslant x$ and let:*

$$C = \frac{1}{2} \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p-1}\right)$$

where $\chi(\cdot) = \left(\frac{-4}{\cdot}\right)$ is the primitive Dirichlet character modulo 4. As $x \longrightarrow \infty$, we have:

$$\pi_{NS}(x) \sim C \int_2^{\sqrt{x}} \frac{dt}{\log t}.$$

The infinite product defining C is converging but is not absolutely convergent since:

$$1 - \frac{\chi(p)}{p-1} \sim 1 - \frac{\chi(p)}{p}$$

The number C is the Hardy-Littlewood constant of the polynomial $x^2 + 64$ (this is the same Hardy-Littlewood constant as for the polynomial $x^2 + 1$). One can find in **[Coh]** how to compute such constants numerically. In particular, we have:

$$C \approx 0.68640673140912300455609634836350934340891665467 54.$$

Of course, the conjecture above implies the less precise conjectural estimate $\pi_{NS}(x) \sim 2C\sqrt{x}/\log x$.

As expected, the comparison of the conjectural estimate with the exact values of the function $\pi_{NS}(x)$ for small x is quite convincing.

x	10^6	10^{12}	10^{18}
$\pi_{NS}(x)$	119	53996	34898579
$C \int_2^{\sqrt{x}} \frac{dt}{\log t}$	≈ 121.19	≈ 53969.76	≈ 34903256.44

4. Complex side of Neumann-Setzer curves

We give a description of the analytic point of view of the modular parametrization. We assume here that $p = u^2 + 64$ is a Neumann-Setzer prime with $u \equiv 3 \pmod 4$. We consider the Neumann-Setzer curve $E = E_p$ as in the previous section:

$$E \ : \ y^2 + xy = x^3 - \frac{u+1}{4}x^2 + 4x - u.$$

4.1. Complex points of E. — It is well known that there exists an analytic isomorphism between the complex points $E(\mathbb{C})$ of E and $\mathbb{C}/\Lambda$ where

$$\Lambda = \mathbb{Z}\omega_2 \oplus \mathbb{Z}\omega_1$$

is the period lattice associated to E. This isomorphism is expressed with the Weierstrass function and its derivative; we denote it by $\wp$ so that:

$$\wp\colon \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C}).$$

Following [**Coh93**, chapter 7], the numbers ω_1 and ω_2 can be given by:

$$\omega_1 = \frac{2\pi}{p^{1/4}\operatorname{agm}\left(1, \sqrt{\frac{1}{2}\left(1+\frac{u}{\sqrt{p}}\right)}\right)} \in \mathbb{R} \tag{1}$$

$$\omega_2 = \frac{\omega_1}{2} + i \cdot \frac{\pi}{p^{1/4}\operatorname{agm}\left(1, \sqrt{\frac{1}{2}\left(1-\frac{u}{\sqrt{p}}\right)}\right)} \tag{2}$$

Here $\operatorname{agm}(\cdot,\cdot)$ denotes the classical arithmetic-geometric mean.

4.2. Complex L-function of E. — We denote by $(a_n)_{n\geqslant 1}$ the coefficients of the L-function of E:

$$L(E,s) = \sum_{n\geqslant 1} a_n n^{-s} \text{ , for } \Re(s) > 3/2.$$

It is easy to see that the curve E has split multiplicative reduction at p hence $a_p = 1$. From the modularity of E, the function $L(E,s)$ has an analytic continuation to the whole complex plane and satisfies a functional equation. The sign of this functional equation is $a_p = +1$ so we have:

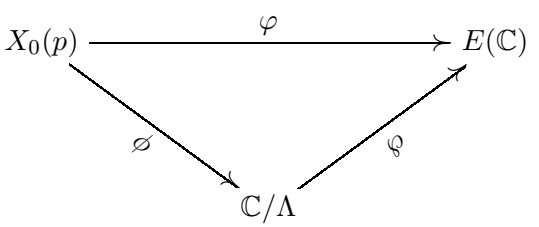
$$\Lambda(E,s) := \left(\frac{\sqrt{p}}{2\pi}\right)^s \Gamma(s)L(E,s) = \Lambda(E,2-s).$$

Furthermore, the function $f(\tau) = \sum_{n\geqslant 1} a_n q^n$ with $q = e^{2i\pi\tau}$ is a newform of weight 2 on $\Gamma_0(p)$. From the theory of Atkin-Lehner, we have:

$$f\left(W_p\tau\right) = -p\tau^2 f(\tau)$$

where $W_p = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$ is the Fricke involution.

4.3. Complex modular parametrization of E. — Let $\mathbb{H}$ be the upper half-plane, $\mathbb{H} = \{\tau \in \mathbb{C}, \Im(\tau) > 0\}$. The complex points of the space $X_0(p)$ can be interpreted as the quotient of $\mathbb{H} \cup \mathbb{Q} \cup \{i\infty\}$ by the congruences subgroup $\Gamma_0(p)$. Then the modular parametrization of E factorizes as $\varphi = \wp \circ \phi$:



where ϕ is given by the following converging series for $\tau \in X_0(p) \setminus \{\text{cusps}\}$:

$$\begin{aligned} \phi : \quad X_0(p) &\longrightarrow \mathbb{C}/\Lambda \\ \tau &\longmapsto \sum_{n\geqslant 1} \frac{a_n}{n} e^{2i\pi n\tau} \end{aligned}$$

The image of the cusp $0 \in X_0(p)$ is a rational torsion point, hence $\varphi(0) \in E(\mathbb{Q})_{\text{tors}}$. In fact, we have:

$$\phi(0) = L(E,1) = 2\sum_{n\geqslant 1} \frac{a_n}{n} e^{-2\pi n\sqrt{p}} \in \mathbb{Z}\frac{\omega_1}{2}.$$

So $\varphi(0) = k\left(\frac{u}{4}, -\frac{u}{8}\right)$ with $k = 0$ or $k = 1$.

Proposition 4.1. — *If we assume the truth of Birch and Swinnerton-Dyer conjecture for E then*

$$\varphi(0) = \left(\frac{u}{4}, -\frac{u}{8}\right).$$

Proof. — Indeed, if we assume the Birch and Swinnerton-Dyer conjecture is valid, then we have:

$$L(E,1) = \frac{\omega_1 \cdot c_p}{|E(\mathbb{Q})_{\text{tors}}|^2} |Ш(E/\mathbb{Q})| = \frac{\omega_1}{2} |Ш(E/\mathbb{Q})|$$

The result follows from the fact the $|Ш(E/\mathbb{Q})|$ is odd (if finite) by a theorem of Stein and Watkins [**SW04**]. □

The index of $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathbb{Z})$ is $p+1$. As a set of representative of $\mathrm{SL}_2(\mathbb{Z})$ modulo $\Gamma_0(p)$ we take the matrices:

$$S_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } S_j = \begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix} \quad \text{for} \quad j = 1, 2, \ldots, p.$$

Let $\tau_0 \in \mathbb{H}$ so that $j(\tau_0)$ is the j-invariant of E, then the analytic interpretation of the self-points (E, C) are the $p+1$ points τ_0, τ_1,...,τ_p with:

$$\tau_j = S_j\tau_0 = \frac{-1}{\tau + j} \quad \text{for} \quad j = 1, 2, \ldots, p.$$

The Hecke operator T_p acts on modular forms of weight 2 on $\Gamma_0(p)$, by definition we have:

$$T_p f(\tau) = \frac{1}{p}\sum_{j=1}^{p} f\left(\frac{\tau + j}{p}\right).$$

Since the function f is a Hecke eigenform with eigenvalue $a_p = 1$, we also have $T_p f(\tau) = a_p f(\tau) = f(\tau)$. Taking the primitive, we deduce:

$$\varphi(\tau) = \sum_{j=1}^{p} \varphi\left(\frac{\tau + j}{p}\right).$$

The constant term in the integration is 0 as it can been seen taking $\tau = i\infty$. Furthermore, f is also an eigenform of the Fricke involution so, $\varphi \circ W_p(\tau) = -\varphi(\tau) + \varphi(0)$. Hence:

$$\varphi(\tau) = -\sum_{j=1}^{p} \varphi\left(W_p\left(\frac{\tau + j}{p}\right)\right) + p\varphi(0)$$

Remark that in any case $p\varphi(0) = \varphi(0)$ and that $W_p\left(\frac{\tau+j}{p}\right) = S_j\tau$. So, we have:

Proposition 4.2. — *For $\tau \in X_0(p)$, we have:*

$$\varphi(\tau) + \sum_{j=1}^{p} \varphi(S_j\tau) = \varphi(0).$$

In particular, if we take $\tau = \tau_0$, we obtain an other approach in the proof of the second point of theorem 2.2:

Corollary 4.3. — *We have:*

$$\sum_C P_C = \varphi(0).$$

Note that the proof we have just given for the $\mathrm{tr}_{K/\mathbb{Q}} P_C$ is clearly analytic compared to the one given in[**DW09**]).

4.4. Estimates for ω_1 and ω_2. — Recall that $p = u^2 + 64$ with $u \equiv 3 \pmod 4$. Hence, we have $p \geqslant 73$ and:

$$\frac{|u|}{\sqrt{p}} = \sqrt{1 - \frac{64}{p}} = 1 - \frac{32}{p} + O\left(\frac{1}{p^2}\right).$$

We define x_+ and x_- by:

$$x_+ = \sqrt{\frac{1}{2}\left(1 + \frac{|u|}{p}\right)}$$

$$\text{and} \quad x_- = \sqrt{\frac{1}{2}\left(1 - \frac{|u|}{p}\right)}.$$

Proposition 4.4. — *With the notations above (in particular $p \geqslant 73$), we have:*

$$1 - \frac{7}{p} \leqslant \mathrm{agm}\,(1, x_+) \leqslant 1$$

Proof. — Let $x = x_+$, we clearly have that $x \leqslant \mathrm{agm}(1,x) \leqslant \frac{1}{2}(x+1)$. We obtain the proposition by a straight forward study of x in function of $p \geqslant 73$. □

For estimating $\mathrm{agm}(1, x_-)$, we will need the following lemma:

Lemma 4.5. — *For $x \in]0,1]$, we have:*

$$-\log x + \frac{3}{2}\log 2 \leqslant \frac{\pi}{2}\frac{1}{\mathrm{agm}(1,x)} \leqslant -\log x + \frac{5}{2}\log 2$$

Proof. — We let

$$g(x) = \int_0^{\pi/2} \frac{dt}{\sqrt{\cos^2 t + x^2 \sin^2 t}}$$

so that we have $\mathrm{agm}(1,x) = \frac{\pi}{2} \cdot \frac{1}{g(x)}$. The change of variables $t' = \cos t / \sin t$ gives

$$g(x) = \int_0^\infty \frac{dt}{\sqrt{(t^2+1)(t^2+x^2)}}\,.$$

Now, we split the integral $\int_0^\infty$ as the sum $\int_0^{\sqrt{x}} + \int_{\sqrt{x}}^\infty$. The change of variables $t' = x/t$, for $x > 0$, in the latter integral shows that we have

$$g(x) = 2\int_0^{\sqrt{x}} \frac{dt}{\sqrt{(t^2+1)(t^2+x^2)}}\,.$$

This gives us the inequalities

$$\frac{2}{\sqrt{1+x}} \int_0^{\sqrt{x}} \frac{dt}{\sqrt{t^2+x^2}} \leqslant g(x) \leqslant 2\int_0^{\sqrt{x}} \frac{dt}{\sqrt{t^2+x^2}}$$

and, since we have $2\int_0^{\sqrt{x}} \frac{dt}{\sqrt{t^2+x^2}} = -\log x + 2\log(1+\sqrt{1+x})$, the lemma follows from

$$\left(-\log x + 2\log(1+\sqrt{1+x})\right) \frac{1}{\sqrt{1+x}} \leqslant g(x) \leqslant -\log x + 2\log(1+\sqrt{1+x})$$

and from a study of the functions on the right and on the left of this inequality. □

Proposition 4.6. — *We have:*

$$\frac{1}{\pi}\left(\log p + \log\frac{8}{25}\right) \leqslant \frac{1}{\mathrm{agm}(1,x_-)} \leqslant \frac{1}{\pi}\left(\log p + \log 2\right).$$

Proof. — We have $\log x_- = \frac{1}{2}\log\left(\frac{1}{2}\left(1-\sqrt{1-64/p}\right)\right)$ and an easy calculation proves that, for $p \geqslant 73$:

$$\frac{16}{p} \leqslant \frac{1}{2}\left(1-\sqrt{1-64/p}\right) \leqslant \frac{25}{p}.$$

Hence,

$$-\frac{1}{2}\log\frac{25}{p} \leqslant -\log x_- \leqslant -\frac{1}{2}\log\frac{16}{p}.$$

Then, we use lemma 4.5 to conclude. □

Corollary 4.7. — *Let $p = u^2 + 64$ be a Neumann-Setzer prime with $u \equiv 3 \pmod 4$. If $u > 0$, we have:*

$$\frac{2\pi}{p^{1/4}}\frac{1}{1-\frac{4}{p}} \leqslant \omega_1 \leqslant \frac{2\pi}{p^{1/4}}\frac{1}{1-\frac{7}{p}}.$$

Whereas, if $u < 0$:

$$\frac{2}{p^{1/4}}\left(\log p + \log\frac{8}{25}\right) \leqslant \omega_1 \leqslant \frac{2}{p^{1/4}}\left(\log p + \log 2\right)$$

Proof. — We apply the two propositions above with the definitions of ω_1 and ω_2 (see equations (1) and (2)). □

Let remark that in any case ($u > 0$ or $u < 0$):

$$\omega_1 \geqslant \frac{2\pi}{p^{1/4}} \tag{3}$$

4.5. Proof that the self-points are non-torsion. — We can now prove that the self points are non-torsion using the complex modular parametrization.
It follows from $E(\mathbb{Q}(C))_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$ that if P_C were a torsion point then it would be a rational torsion point. So, in order to prove that P_C is not a torsion point it is sufficient to prove that $\phi(\tau_0) \neq 0 \pmod{\frac{1}{2}\Lambda}$ for a certain $\tau_0 \in \mathbb{H}$ such that $j(\tau_0)$ is the j-invariant of E. For that we let $\tau_0 = \omega_2/\omega_1$ if $u > 0$ and $\tau_0 = (\omega_2 - \omega_1)/(2\omega_2 - \omega_1)$ if $u < 0$. In fact, for $u < 0$, we have:

$$\tau_0 = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \frac{\omega_2}{\omega_1}.$$

Since the matrix above belongs to $\mathrm{SL}_2(\mathbb{Z})$, we see that in each case the image of $y_C = (E, C) \in X_0(p)$ in $\mathbb{C}/\Lambda$ (for a certain C depending on the sign of u) is given by $\phi(\tau_0)$. It is easy to see that we have:

$$\tau_0 = \frac{1}{2} + i \cdot \frac{\operatorname{agm}(1, x_+)}{2\operatorname{agm}(1, x_-)} \in \mathbb{H}.$$

Hence, $\phi(\tau_0)$ is real and we just need to prove that $\phi(\tau_0) \neq 0 \pmod{\frac{\omega_1}{2}}$.

Theorem 4.8. — *With the notations above, we have the following estimates:*

$$-\frac{6}{p} \leqslant \phi(\tau_0) \leqslant -\frac{1}{10p}.$$

In particular, $\phi(\tau_0) \neq 0, \omega_1/2 \pmod{\omega_1}$ *and* P_C *is a non-torsion point.*

Proof. — We let $t = \Im(\tau_0)$ and $q = e^{2i\pi\tau_0} = -e^{-2\pi t}$. From propositions 4.4 and 4.6, we have:

$$\frac{1}{2\pi}\left(1 - \frac{7}{p}\right)\log\frac{8p}{25} \leqslant t \leqslant \frac{1}{2\pi}\log 2p$$

Hence,

$$\frac{1}{2p} \leqslant e^{-2\pi t} \leqslant \left(\frac{25}{8p}\right)^{1-7/p}.$$

But, we have $\left(\frac{25}{8p}\right)^{1-7/p} \leqslant 5/p$ whenever $p \geqslant 73$. Finally, we obtain that $q < 0$ and:

$$\frac{1}{2p} \leqslant |q| \leqslant \frac{5}{p}. \tag{4}$$

We have $\frac{a_n}{n} \leqslant 1$ (see **[GJP+09]**) so $\phi(\tau_0) = q + \varepsilon$ where:

$$|\varepsilon| \leqslant \sum_{n \geqslant 2} |q|^n = \frac{|q|^2}{1 - |q|} \leqslant \frac{25}{p(p-5)}. \tag{5}$$

Then (4) and (5) give the inequality for $\phi(\tau_0)$. We deduce that $\phi(\tau_0) \neq 0$ and that $|\phi(\tau_0)| < \pi/p^{1/4} \leqslant \omega_1/2$ by equation (3). □

In fact, we have proved that:

$$\phi(\tau_0) = q + O\left(1/p^2\right)$$

where the constant is absolute and where $q \asymp \frac{1}{p}$. We will use that in the next section.

4.6. Isogeneous self-points. — Let F be the Neumann-Setzer curve that is isogeneous to E (see section 3). Then, one can consider the point $z_D = (F, D) \in X_0(p)$ where $D \subset F$ is a sub-group of order p. The image $Q_D = \varphi(z_D)$ are also interesting point in $E(K)$. We can use exactly the same method as before to proof that Q_D is a non-torsion point for all D. The question of the independence of the $p+1$ points Q_D and the $p+1$ points P_C is natural. We believe that the only relations between those points are given by:

$$\mathrm{tr}_{K/\mathbb{Q}} P_C = \mathrm{tr}_{K/\mathbb{Q}} Q_D = \varphi(0)$$

This would follow from the fact that if C and D are chosen so that they are defined over the same field $\mathbb{Q}(C)$ then the points P_C and Q_D are independent in $E(\mathbb{Q}(C))$ (see [**DW09**]).

Let t_0 be as in the previous section so that t_0 correspond to

$$(E, C) = \left(\mathbb{C}/\mathbb{Z}\tau_0 \oplus \mathbb{Z}, \langle\frac{1}{p}\rangle\right)$$

where $\langle\frac{1}{p}\rangle$ denotes the cyclic sub-group of order p generated by $1/p \pmod{\mathbb{Z}\tau_0 \oplus \mathbb{Z}}$. For the curve F, we can choose the point $\tau_0' = 2\tau_0$ corresponding to:

$$(F, D) = \left(\mathbb{C}/\mathbb{Z}\tau_0' \oplus \mathbb{Z}, \langle\frac{1}{p}\rangle\right)$$

where $\langle\frac{1}{p}\rangle$ denotes here the cyclic sub-group of order p generated by the point $1/p \pmod{\mathbb{Z}\tau_0' \oplus \mathbb{Z}}$. The 2-isogeny between F and E correspond to the map induced by the identity:

$$\mathbb{C}/\mathbb{Z}\tau_0' \oplus \mathbb{Z} \longrightarrow \mathbb{C}/\mathbb{Z}\tau_0 \oplus \mathbb{Z}$$

$$x \pmod{\mathbb{Z}\tau_0' \oplus \mathbb{Z}} \longmapsto x \pmod{\mathbb{Z}\tau_0 \oplus \mathbb{Z}}$$

since $\mathbb{Z}\tau_0' \oplus \mathbb{Z} \subset \mathbb{Z}\tau_0 \oplus \mathbb{Z}$. This 2-isogeny being rational, the point (E, C) and (F, D) are defined over the same field, $E(\mathbb{Q}(C)) = E(\mathbb{Q}(D))$.
We have $q' = e^{2\pi\tau_0'} = q^2$ with $q = e^{2i\pi\tau_0}$ from the previous section. Using the same technique as in the previous section, we prove that:

$$\phi(\tau_0') = q^2 + O\left(\frac{1}{p^4}\right)$$

where the implied constant is absolute.

We believe that the points P_C and Q_D are linearly independent in $E(\mathbb{Q}(C))$ but we are not able to prove it. Nevertheless, if there exists a linear relationship of these points, it would involve rather large coefficients since:

Theorem 4.9. — *With the notations above, suppose that there exist ℓ, $m \in \mathbb{Z} \setminus \{0\}$ such that:*

$$\ell P_C + m Q_D \in E(\mathbb{Q}(C))_{\mathrm{tors}}$$

then $\max(|\ell|, |m|) \gg p^{3/4}$, where the implied constant is absolute.

Proof. — Recall that $E(\mathbb{Q}(C))_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$, hence if $\ell P_C + mQ_D \in E(\mathbb{Q}(C))_{\text{tors}}$, we would have:

$$\ell\phi(\tau_0) + m\phi(\tau_0') \in \frac{\omega_1}{2}\mathbb{Z}.$$

If $\ell\phi(\tau_0) + m\phi(\tau_0') = 0 \in \mathbb{C}$ then $\ell \neq 0$ since $\phi(\tau_0')$ does not correspond to a torsion point and so:

$$\frac{|m|}{|\ell|} = \frac{|\phi(\tau_0)|}{|\phi(\tau_0')|} \gg p \ ,$$

and $|m| \gg p$.

If $\ell\phi(\tau_0) + m\phi(\tau_0') = \lambda\omega_1/2$ for some $\lambda \in \mathbb{Z} \setminus \{0\}$ then in this case:

$$|\ell|\frac{1}{p} + |m|\frac{1}{p^2} \gg |\ell\phi(\tau_0) + m\phi(\tau_0')| \geqslant \frac{\omega_1}{2} \geqslant \frac{2\pi}{p^{1/4}}$$

so $|\ell| \gg p^{3/4}$ or $m \gg p^{7/8}$. □

5. Some other consequences

5.1. Growth of the modular degree of Neumann-Setzer curves. — There is an interesting consequence about the degree of the modular parametrization of the optimal Neumann-Setzer curve E. Indeed, using our estimates for ω_1 and ω_2, it is not difficult to see that we have:

$$\text{vol}(E) = \omega_1 \cdot \Im(\omega_2) \sim \frac{2\pi \log(p)}{\sqrt{p}} \quad \text{as} \quad p = u^2 + 64 \longrightarrow \infty.$$

Furthermore, since the Neumann-Setzer curves are semi-stable, the modular degree is given by the following formula.

$$\deg(\varphi) = \frac{p\ L(\text{Sym}^2 f, 2)}{2\pi\ \text{vol}(E)}\,.$$

Where $L(\text{Sym}^2 f, s)$ is the symmetric-square L-function associated to $L(E, s)$ normalized so that $s = 3/2$ is the point of symmetry in the functional equation (let's remark that the conductor being square-free, there is no difference between the primitive and the imprimitive symmetric-square).

Using the classical upper bound $L(\text{Sym}^2 f, 2) \ll \log(p)^3$ and the deeper lower bound $L(\text{Sym}^2 f, 2) \gg 1/\log(p)$ obtained by Goldfeld, Hoffstein and Lieman [**HL94**], we deduce:

Theorem 5.1. — *Suppose that there are infinitely many Neumann-Setzer primes p then for the Neumann-Setzer curves E of conductor p we have as $p \longrightarrow \infty$:*

$$\deg(\varphi) \ll p^{3/2}\ \log(p)^2$$
$$\deg(\varphi) \gg p^{3/2}/\log(p)^2$$

Note that the degree of the modular parametrization is "large" because the j-invariants tend to infinity with p. Indeed, in [**Del03**]), it is proved that:

Theorem 5.2. — *Let $\mathcal{G}$ be an infinite family of semi-stable elliptic curves G defined over $\mathbb{Q}$ with conductor N_G such that the j-invariant of G is bounded for all $G \in \mathcal{G}$ and such that G are the strong Weil curves in their isogeny classes. If φ_G denotes the modular parametrization of G, then as $N_G \longrightarrow \infty$:*

$$\begin{aligned} \deg(\varphi_G) &\ll N_G^{7/6}(\log N_G)^3 \\ \deg(\varphi_G) &\gg N_G^{7/6}/\log N_G \end{aligned}$$

In this context, the power $3/2$ of theorem 5.1 should be compared with the power $3/2$ in the previous estimates.

5.1.1. Remark. — In fact, Watkins **[Wat04]** gave a very explicit version of the lower bound $L(\mathrm{Sym}^2 f, 2) \gg 1/\log p$. (He normalized $L(\mathrm{Sym}^2 f, s)$ so that $1/2$ is the point of symmetry.) Using his work and our estimates we have for a Neumann-Setzer curve E of conductor p:

$$\deg(\varphi) \geqslant 0.0006 \cdot \frac{p^{3/2}}{\log(p)^2}\,.$$

Hence the inequality $\deg(\varphi) < p+1$ never occurs for $p > 1.8 \cdot 10^{12}$ (but there probably exists a much smaller value of B such that $\deg(\varphi) \geqslant p+1$ for all $p > B$).

5.2. Explicit computations of the analytic order of the Tate-Shafarevich groups of Neumann-Setzer curves. — Throughout this section, we assume the truth of the Birch and Swinnerton-Dyer conjecture for E. So that we have:

$$|Ш(E)| = \frac{2L(E,1)}{\omega_1} \tag{6}$$

Suppose that we want to compute numerically the values of $|Ш(E)|$. Then, we have to compute numerically the series:

$$L(E,1) = 2\sum_{n\geqslant 1} \frac{a_n}{n} e^{-2\pi n/\sqrt{p}}.$$

And we need to truncate the series using sufficiently many coefficient. That means that we write:

$$\sum_{n\geqslant 1} \frac{a_n}{n} e^{-2\pi n/\sqrt{p}} = \sum_{n<N_0} \frac{a_n}{n} e^{-2\pi n/\sqrt{p}} + \text{ Error} \tag{7}$$

and we need to take N_0 sufficiently large to be are able to recognize $|Ш(E)|$ from equation (6).

Theorem 5.3. — *Let $\eta > 0$, there exists an explicit $K > 0$ such that for all Neumann-Setzer curves of conductor $p > K$ it is sufficient to take*

$$N_0 > \frac{1+\eta}{4\pi}\sqrt{p}\log p$$

in equation (7) in order to determine $|Ш(E)|$.

Proof. — Let $\eta > 0$, it is well known that there is an absolute constant K_0 such that $|a_n| \leqslant n^{1/2+\eta}$ for all $n \geqslant K_0$ (this is in fact true for all elliptic curves defined over $\mathbb{Q}$; note that for $\eta = 1/2$ we can take $K_0 = 1$).
We write $S = \sum_{n<N_0} \frac{a_n}{n} e^{-2\pi n/\sqrt{p}}$ and $\varepsilon = \sum_{n\geqslant N_0} \frac{a_n}{n} e^{-2\pi n/\sqrt{p}}$. Hence we have:

$$\frac{1}{\omega_1}(4S - 4|\varepsilon|) \leqslant |Ш(E)| \leqslant \frac{1}{\omega_1}(4S + 4|\varepsilon|).$$

Since $|Ш(E)|$ is an odd square, the length of the interval in the inequality above has to be less than 4 in order to determine $|Ш(E)|$. So, we need $|\varepsilon| < \omega_1/2$ hence, we need:

$$\varepsilon < \frac{\pi}{p^{1/4}}.$$

Suppose that $\sqrt{p} > K_0$ then $N_0 > \sqrt{p}$ and we have:

$$\begin{aligned} |\varepsilon| &\leqslant \sum_{n\geqslant N_0} \frac{|a_n|}{n} e^{-2\pi n/\sqrt{p}} \leqslant \sum_{n\geqslant N_0} \frac{1}{n^{1/2-\eta}} e^{-2\pi n/\sqrt{p}} \\ &\leqslant \frac{1}{p^{\frac{1-2\eta}{4}}} \frac{\left(e^{-2\pi/\sqrt{p}}\right)^{N_0}}{\left(1 - e^{-2\pi/\sqrt{p}}\right)} \leqslant \frac{1}{p^{\frac{1-2\eta}{4}}} \frac{p^{1/2}}{4} \left(e^{-2\pi/\sqrt{p}}\right)^{N_0}. \end{aligned}$$

(Note that $p \geqslant 73$). The values of N_0 is sufficient for the theorem. □

In particular, taking $\eta = 1/2$, we need to take $N_0 > \frac{1}{8}\sqrt{p}\log p$.

Using this, we have computed several values of $|Ш(E)|$ of Neumann-Setzer curves. We give here some numerical investigations related to these values. In particular, we consider the study of the frequencies of $|Ш(E)|$ that are divisible by the primes q for $q = 3, 5, 7, \cdots$ (trivially, the case $q = 2$ is a special one, and there is nothing to say about it). Computing sufficiently enough values of $|Ш(E)|$, we can compare these numerical frequencies with the heuristics on Tate-Shafarevich groups ([**Del01**], [**Del07**]). In this case, the heuristics predict that, if q is (an odd) prime, the frequency of occurrences of $q \mid |Ш(E)|$ should be given by:

$$f(q) = 1 - \prod_{k\geqslant 1} \left(1 - \frac{1}{q^{2k-1}}\right) = \frac{1}{q} + \frac{1}{q^3} - \frac{1}{q^5} + \cdots.$$

We first computed the values of $|Ш(E)|$ for the 53996 Neumann-Setzer curves of conductor $p \leqslant 10^{12}$. The largest value $|Ш(E)| = 123^2$ was obtained for $p = 974419714193$ ($u = 987127$). It is worth noting that $|Ш(E)| = 113^2$ occured for $u = 984355$ (113 is prime). In fact, except for $q = 97$ and $q = 109$, all the primes $q \leqslant 113$ divides $|Ш(E)|$ for at least one Neumann-Setzer curve E with $p \leqslant 10^{12}$.

We obtained the following results for the frequency of occurrences of $q \mid |Ш(E)|$:

q	3	5	7	11
Frequency of $q \mid \|Ш(E)\|$	0.353	0.185	0.118	0.056
$f(q) \approx$	0.361	0.207	0.145	0.092

Expect for $p = 3$, the numerical values are not so close than the expected ones. Indeed, we believe that Tate-Shafarevich groups acquire their expected behavior for rather large conductor. To illustrate this, we also computed the orders of 10000 Tate-Shafarevich groups of the first Neumann-Setzer curves E having conductor $p > 10^{15}$. We obtained the following table:

q	3	5	7	11
Frequency of $q \mid \lvert Ш(E)\rvert$	0.368	0.198	0.140	0.084

We should mention that the largest value is $|Ш(E)| = 299^2$ and that the average value for these 10000 values of $|Ш|$ is ≈ 1378.

References

[AU96] Ahmed Abbes and Emmanuel Ullmo. À propos de la conjecture de Manin pour les courbes elliptiques modulaires. *Compositio Math.*, 103(3):269–286, 1996.

[Coh] Henri Cohen. High precision computation of hardy-littlewood constants. available on http://www.math.u-bordeaux1.fr/∼cohen/.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Coh07] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

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

[Del01] Christophe Delaunay. Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$. *Experiment. Math.*, 10(2):191–196, 2001.

[Del03] Christophe Delaunay. Computing modular degrees using L-functions. *J. Théor. Nombres Bordeaux*, 15(3):673–682, 2003.

[Del07] Christophe Delaunay. Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 323–340. Cambridge Univ. Press, Cambridge, 2007.

[DW09] Christophe Delaunay and Christian Wuthrich. Self-points on elliptic curves of prime conductor. *Int. J. Number Theory*, 5(5):911–932, 2009.

[GJP+09] Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William A. Stein, and Corina Tarniţă. Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves. *Math. Comp.*, 78(268):2397–2425, 2009.

[GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[Har79] Michael Harris. Systematic growth of Mordell-Weil groups of abelian varieties in towers of number fields. *Invent. Math.*, 51(2):123–141, 1979.

[HL94] Jeffrey Hoffstein and Paul Lockhart. Coefficients of Maass forms and the Siegel zero. *Ann. of Math. (2)*, 140(1):161–181, 1994. With an appendix by Dorian Goldfeld, Hoffstein and Daniel Lieman.

[Kur73] P. F. Kurčanov. Elliptic curves of finite rank over Γ-extensions. *Mat. Sb. (N.S.)*, 90(132):320–324, 327, 1973.

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

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

[Neu73] Olaf Neumann. Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. II. *Math. Nachr.*, 56:269–280, 1973.

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

[SW04] William Stein and Mark Watkins. Modular parametrizations of Neumann-Setzer elliptic curves. *Int. Math. Res. Not.*, (27):1395–1405, 2004.

[Wat04] Mark Watkins. Explicit lower bounds on the modular degree of an elliptic curve. available on math.NT/0408126, 2004.

[Wut09] Christian Wuthrich. Self-points on elliptic curves. *Algebra Number Theory*, 3(3):283–315, 2009.

April 6, 2010

Christophe Delaunay, Université de Lyon, CNRS, Université Lyon 1, Institut Camille Jordan, 43, boulevard du 11 novembre 1918, F-69622 Villeurbanne Cedex, France. • *E-mail :* `delaunay@math.univ-lyon1.fr` *Url :* `http://math.univ-lyon1.fr/~delaunay`

Christian Wuthrich, Shool of Mathematical Sciences, University of Nottingham, Nottingham NG7 2RD, United Kingdom. • *E-mail :* `christian.wuthrich@nottingham.ac.uk`