Journal de Théorie des Nombres
de Bordeaux **17** (2005), 109–124

Critical and ramification points of the modular parametrization of an elliptic curve

par Christophe DELAUNAY

Résumé. Soit E une courbe elliptique définie sur $\mathbb{Q}$ de conducteur N et soit φ son revêtement modulaire :

$$\varphi \, : \, X_0(N) \longrightarrow E(\mathbb{C}) \, .$$

Dans cet article, nous nous intéressons aux points critiques et aux points de ramification de φ. En particulier, nous expliquons comment donner une étude plus ou moins expérimentale de ces points.

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N and denote by φ the modular parametrization:

$$\varphi \, : \, X_0(N) \longrightarrow E(\mathbb{C}) \, .$$

In this paper, we are concerned with the critical and ramification points of φ. In particular, we explain how we can obtain a more or less experimental study of these points.

1. Introduction and motivation

1.1. The modular parametrization. Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N. It is known from the work of Wiles, Taylor and Breuil, Conrad, Diamond, Taylor ([16], [14], [3]) that E is modular and, hence, that there exists a map φ, called the modular parametrization:

$$\varphi \, : \, X_0(N) \longrightarrow \mathbb{C}/\Lambda \simeq E(\mathbb{C}) \, ,$$

where $X_0(N)$ is the quotient of the extended upper half plane $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ by the congruences subgroup $\Gamma_0(N)$ (which we endow with its natural structure of compact Riemann surface). The analytic group isomorphism from $\mathbb{C}/\Lambda$ to $E(\mathbb{C})$ is given by the Weierstrass $\wp$ function and its derivative and we will often implicitly identify these two spaces. We now briefly describe the map φ.

The pull-back by φ of the holomorphic differential dz is given by:

$$\varphi^*(dz) = 2i\pi c f(z) dz \ \ ,$$

where $f(z)$ is a (normalized) newform of weight 2 on $\Gamma_0(N)$ and $c \in \mathbb{Z}$ is the Manin's constant. In this paper, we assume that we have $c = 1$; in fact all examples of elliptic curves we have studied satisfy this assumption (we use the first elliptic curves from the very large table constructed by Cremona [7]). Since the differential $2i\pi f(z)dz$ is holomorphic, the integral:

$$\widetilde{\varphi}(\tau) = 2i\pi \int_{\infty}^{\tau} f(z)dz$$

does not depend on the path and defines a map $\widetilde{\varphi} \ : \ \mathbb{H} \to \mathbb{C}$. Furthermore, if $\gamma \in \Gamma_0(N)$, we set:

$$\omega(\gamma) = \widetilde{\varphi}(\gamma\tau) - \widetilde{\varphi}(\tau) \ ,$$

the map ω does not depend on τ and $\omega(\gamma)$ is called a period of f (see [6] to compute it efficiently). The image of $\omega : \Gamma_0(N) \to \mathbb{C}$, which is a group homomorphism, is a lattice $\Lambda \subset \mathbb{C}$ and then, we get a map:

$$\varphi \ : \ X_0(N) \longrightarrow \mathbb{C}/\Lambda \ .$$

The curve E is in fact chosen (en even constructed) such that $\mathbb{C}/\Lambda \simeq E(\mathbb{C})$ and φ is the modular parametrization. This description of the modular parametrization is very explicit and allows us to evaluate φ at a point $\tau \in X_0(N)$, indeed:

• First, suppose that τ is not a cusp, then we have :

$$\varphi(\tau) = \sum_{n=1}^{\infty} \frac{a(n)}{n} q^n \mod \Lambda \qquad (q = e^{2i\pi\tau}) \ , \tag{1.1}$$

where the (integers) $a(n)$ are the coefficients of the Fourier expansion of f at the cusp ∞. Note that they are easily computable since $L(f,s) = \sum_n a(n)n^{-s} = L(E,s)$ is the L-function of E. The series (1.1) is a rapidly converging series and gives an efficient way to calculate φ.

• Suppose now that τ represents a cusp in $X_0(N)$. Then, the series (1.1) does not converge any more and we have to use a different method. Let $\{\tau\}$ be the "modular symbol" as described in [6] (it represents a path linking ∞ to τ on which we will integrate f). The Hecke operator T_p, where p is a prime number, acts on modular symbols and we have:

$$T_p\{\tau\} = \{p\tau\} + \sum_{j=0}^{p-1} \left\{ \frac{\tau + j}{p} \right\} \ .$$

If $p \equiv 1 \mod N$ then the cusps $p\tau$ and $(\tau + j)/p$ (for $j = 0, \ldots, p-1$) are equivalent to $\tau \mod \Gamma_0(N)$, so there exist M_0, M_1, ..., $M_p \in \Gamma_0(N)$ such

that:

$$M_j\tau = \frac{\tau + j}{p} \quad \text{for } j = 0, \ldots, p-1 \ ,$$
$$\text{and} \quad M_p\tau = p\tau \ .$$

Writing $\{(\tau+j)/p\} = \{(\tau+j)/p\} - \{\tau\} + \{\tau\}$ and using the fact that f is a Hecke eigenform with eigenvalue $a(p)$ for T_p, we obtain:

$$(1 + p - a(p))\widetilde{\varphi}(\tau) = \sum_{j=0}^{p} \omega(M_p) \in \Lambda \ .$$

And we deduce from it the value of the map φ at the cusp τ (of course, this is a torsion point and with the method above, we can compute it exactly and not only numerically).

1.2. Critical and ramification points. The topological degree of φ can be efficiently computed by several methods ([6], [15], [17], [8]), and we denote by $d = \deg(\varphi)$ this integer. There are finitely many points $z \in E(\mathbb{C})$ for which $\sharp\{\varphi^{-1}(\{z\})\} < d$ (we will call z a ramification point). These points are image of critical points (and so critical points are finite in number). We are interested in localizing and studying the ramification and the critical points. From the Hurwitz formula there are exactly $2g-2$ critical points (counted with multiplicity) where g is the genus of $X_0(N)$ and is given by:

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2} \ .$$

In this formula, $\mu = [SL_2(\mathbb{Z}) : \Gamma_0(N)]$, ν_∞ is the number of cusps and ν_2 (resp. ν_3) is the number of elliptic points of order 2 (resp. order 3) of $X_0(N)$. Critical points are the zeros of the differential $d\varphi = 2i\pi f(z)dz$ and then we are led to find all the zeros of f. Nevertheless, a zero of f may not be a critical point because dz has only a polar part ([12]):

$$\operatorname{div}(dz) = -\left(\sum_{j=1}^{\nu_\infty} P_j + \frac{1}{2}\sum_{j=1}^{\nu_2} e_j + \frac{2}{3}\sum_{j=1}^{\nu_3} e'_3\right) \ ,$$

where P_j are the cusps and e_j (resp. e'_j) the elliptic elements of order 2 (resp. order 3) in $X_0(N)$. Thus, $c \in X_0(N)$ is a critical point for φ if and only if c is a zero of f not due to a pole of dz. For example, a cusp P is critical if and only if the order of vanishing of f at P is ≥ 2. Note that the differential form $f(z)dz$ is holomorphic and so a pole of dz is counterbalanced by a zero of f. Thus, the modular form f vanishes at all elliptic elements of $X_0(N)$. Furthermore, with the usual local coordinates for $X_0(N)$, the multiplicity of a zero of f at an elliptic element of order 2 (resp. order 3) has to be counted up with the weight 1/2 (resp. 1/3). So, a simple (resp. double) zero of f, viewed as a function $f : \mathbb{H} \to \mathbb{C}$,

at an elliptic element of order 2 (resp. order 3) compensates exactly the corresponding pole of dz (viewed in $X_0(N)$).

Let $c \in X_0(N)$ be a critical point of the modular parametrization, so $\varphi(c)$ is a ramification point and is also an algebraic point on $E(\overline{\mathbb{Q}})$ defined over a certain number field K. Then, the point $\mathrm{Tr}_{K/\mathbb{Q}}(\varphi(c))$ is a rational point on $E(\mathbb{Q})$. A natural question asked in [11] is to determine the subgroup generated by all such rational points. They denote by $E(\mathbb{Q})^{crit}$ this subgroup. A critical point $c \in X_0(N)$ is said to be a fundamental critical point if $c \in i\mathbb{R}$, we denote by $E(\mathbb{Q})^{fond}$ the subgroup of $E(\mathbb{Q})$ generated by $\mathrm{Tr}_{K/Q}(\varphi(c))$ where c runs over all the fundamental critical points. In [11], the authors proved the following:

Theorem 1.1 (Mazur-Swinerton-Dyer)**.** *The analytic rank of E is less than or equal to the number of fundamental critical points of odd order, and these numbers have the same parity.*

In this paper, we are concerned with studying these particular points of the modular parametrization. More precisely, for a fixed elliptic curve E, the questions and the problems we are interested in are to determine the critical points, to define a number field K in which live ramification points, to look at the behaviour of the subgroups $E(\mathbb{Q})^{crit}$ and $E(\mathbb{Q})^{fond}$, etc.. Although it is clear that these questions can be theoretically answered with a finite number of algebraic (but certainly unfeasible in the general case) calculations, the part 3 and 4 of our work is more or less experimental and some of the answers we give come from numerical computations and are not proved in a rigorous way. Nevertheless, there are some strong evidence to be enough self confident in their validity.

2. Factorization through Atkin-Lehner operators

In order to find (numerically) all the critical points of φ, we will explain, in the next section, how to solve the equation $f(z) = 0$, $z \in X_0(N)$. In fact, the results we have obtained by our method suggest that the zeros of f are often quadratic points in $X_0(N)$.
Let W_Q (with $Q \mid N$ and $\gcd(Q, N/Q) = 1$) be an Atkin-Lehner operator. Since f is an eigenform for W_Q, we have $f|_{W_Q} = \pm f$, we deduce that:

$$\varphi \circ W_Q = \pm\varphi + P \text{ , where } P \in E(\mathbb{Q})_{\mathrm{tors}} \ .$$

Furthermore, $2P = 0$ if the sign is $+1$. Suppose that $\varphi \circ W_Q = \varphi$, then we can factor the modular parametrization through the operator W_Q:

$$\varphi \ : X_0(N) \xrightarrow[2]{\pi_Q} X_0(N)/W_Q \xrightarrow{\bar{\varphi}} E(\mathbb{C}) \ .$$

The map π_Q is the canonical surjection, its degree is 2 and we have $\deg(\overline{\varphi}) = \deg(\varphi)/2$. The fixed points c of W_Q in $X_0(N)$ are critical points for π_Q and

thus are critical points for φ. The Hurwitz formula gives:

$$2g-2 = 2(2g_Q-2) + |\{\text{fixed points of } W_Q \text{ in } X_0(N)\}| \ ,$$

where g_Q is the genus of $X_0(N)/W_Q$. We define a function $H_n(\Delta)$ for $n \in \mathbb{N}$ and $\Delta \leq 0$.

If $n=1$, $H_1(\Delta) = H(|\Delta|)$ is the Hurwitz class number of Δ (cf. [5]).

If $n \geq 2$, we write $\gcd(n,\Delta) = a^2 b$ with b squarefree, and we let:

$$H_n(\Delta) = \begin{cases} \left(\frac{\Delta/a^2b^2}{n/a^2b}\right) a^2 b\, H_1\left(\frac{\Delta}{a^2b^2}\right) & \text{if } a^2b^2 \mid \Delta \\ 0 & \text{otherwise.} \end{cases}$$

For $n \in \mathbb{N}$, we denote by $Q(n)$ the greatest integer such that $Q(n)^2 \mid n$, by $\sigma_0(n)$ the number of positive divisors of n and by $\mu(n)$ the Moebius function. Using the results of [13], we have:

Proposition 2.1. *Let* $\mathrm{tr}(W_Q, S_2(N))$ *be the trace of the operator* W_Q *in the space* $S_2(N)$ *of the cusp forms of weight 2 on* $\Gamma_0(N)$*, then:*

$$\mathrm{tr}(W_Q, S_2(N)) = \sum_{\substack{m \mid N \\ \mu\left(\frac{N}{m}\right) \neq 0}} \mu\left(\gcd\left(\frac{N}{m}, Q\right)\right) S(m, \gcd(m,Q)) \ ,$$

where:

$$\begin{aligned} S(m,n) = &-\frac{1}{2} \sum_{\substack{n' \mid n \\ n' > 4}} \left|\mu\left(\frac{n}{n'}\right)\right| H_{\frac{m}{n}}(-4n') \\ &-\frac{1}{2} \sum_{\substack{n' \mid n \\ 2 \leq n' \leq 4}} \left(\left|\mu\left(\frac{n}{n'}\right)\right| H_{\frac{m}{n}}(-4n') + 2H_{\frac{m}{n}}(n'^2 - 4n')\right) \\ &-\frac{1}{2}\left(|\mu(n)| H_{\frac{m}{n}}(-4) + 2H_{\frac{m}{n}}(-3) + 2\,|\mu(\gcd(4,n))|\, H_{\frac{m}{n}}(0)\right) \\ &-\frac{1}{2}\gcd(Q(n),2)\, Q\left(\frac{m}{n}\right) \\ &+\begin{cases} \sigma_0(n) & \textit{if } \frac{m}{n} \textit{ is a perfect square} \\ 0 & \textit{otherwise.} \end{cases} \end{aligned}$$

The numbers g_Q and $\mathrm{tr}(W_Q, S_2(N))$ are related by:

$$g_Q = (g + \mathrm{tr}(W_Q, S_2(N)))/2 \ ,$$

and so the number of fixed points of W_Q in $X_0(N)$ is given by the formula:

$$|\{\text{fixed points of } W_Q \in X_0(N)\}| = 2 - 2\,\mathrm{tr}(W_Q, S_2(N)) \ . \tag{2.1}$$

We are looking for all fixed points of W_Q. We let:

$$W_Q = \begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix} \quad , \quad \det(W_Q) = Q \ ,$$

and we search $\tau \in \mathbb{H}$ such that $W_Q\tau = M\tau$ with $M \in \Gamma_0(N)$. Changing the coefficients x, y, z et w of W_Q, we can assume that $M = Id$ and that $W_Q\tau = \tau$. Then, the matrix W_Q is "elliptic" and:

$$|x + w|\sqrt{Q} < 2 \ .$$

First, suppose that $Q \neq 2$, 3 then $x = -w$ and:

$$W_Q = \begin{pmatrix} Qx & y \\ Nz & -Qx \end{pmatrix} \quad .$$

Furthermore $Q = \det(W_Q) = -Q^2x^2 + yNz$ so we have $(2Qx)^2 = -4Q + 4Nyz$ and the point:

$$\tau = \frac{2xQ + \sqrt{-4Q}}{2Nz} \ , \tag{2.2}$$

is a fixed point of W_Q. Conversely, we can check that every fixed point has the form (2.2). In order to find all the fixed point:

- We search $\beta \pmod{2N}$ such that:

$$\beta^2 \equiv -4Q \pmod{4N} \quad \text{with} \quad \beta = 2Qx \ , \ x \in \mathbb{Z}. \tag{2.3}$$

- For each divisor z of $(\beta^2 + 4Q)/4N$, we get the fixed point:

$$\tau = \frac{\beta + \sqrt{-4Q}}{2Nz} \ . \tag{2.4}$$

For each new τ, we check that it is not equivalent mod $\Gamma_0(N)$ to a point already found. We try a new divisor z, eventually we change the solution β and we continue. We stop when we have obtained all the fixed points (their number is known by formula (2.1)).

The critical point τ in formula (2.4) has precisely the form of an Heegner point of discriminant Q' for some space $X_0(N')$ with Q' and N' convenient (see [4], [9] for more details about Heegner points). In fact, with the notations above:

- If $2 \mid N$ and $2 \mid y$ and $2 \nmid z$ then τ is an Heegner point of discriminant $-Q$ in the space $X_0(Q)$.
- If $2 \mid N$ and $2 \mid y$ and $2 \nmid z$ then τ is an Heegner point of discriminant $-4Q$ in the space $X_0(Q)$.
- Otherwise τ is an Heegner point of discriminant $-4Q$ ($-Q$ if $2 \mid y$ and $2 \mid z$) in the space $X_0(N)$.

If τ is a critical point for φ and an Heegner point of discriminant Δ, then write $\Delta = f^2\Delta'$ where Δ' is a fundamental discriminant and f is the conductor of the order $\mathcal{O}$ in the quadratic field $K = \mathbb{Q}(\sqrt{\Delta'})$. In this case, the ramification point $\varphi(\tau)$ is defined over the number field $H = K(j(\mathcal{O}))$, the ring class field of conductor f.

If $Q = 2$ or 3, we have $|x + w| = 0$ or $|x + w| = 1$. The first case is discussed above, for the second, we have to adapt the method with $w = 1 - x$; this changes nearly nothing. The equation (2.3) is replaced by:

$$\beta^2 - 2Q\beta \equiv 4Q \pmod{4N} \quad \text{with} \quad \beta = 2Qx \ , \ x \in \mathbb{Z}.$$

And the fixed points are:

$$\tau = \frac{-\beta + Q + \sqrt{\Delta}}{2Nz} \ ,$$

where $\Delta = -4$ (resp. $\Delta = -3$) whenever $Q = 2$ (resp. $Q = 3$).

Sometimes, the Atkin-Lehner operators does not suffice to factor φ and we can also have to use other operators; those coming from the normalizer of $\Gamma_0(N)$ in $SL_2(\mathbb{R})$ ([1]). In practice, the computations are analogous.

Example. Let take E defined by:

$$E \ : y^2 = x^3 - 7x + 6 \ .$$

Its conductor is $N = 80$ and the genus of $X_0(80)$ is $g = 7$, furthermore $\deg(\varphi) = 4$ and we have to find 12 critical points for φ.

First of all, φ factors through the Atkin-Lehner operator W_{16} which has 4 fixed points in $X_0(N)$. The method above allows us to determine them:

$$c_1 = \frac{64 + \sqrt{-64}}{2 \times 80} \qquad c_2 = -\overline{c_1} \ ,$$
$$c_3 = \frac{256 + \sqrt{-64}}{2 \times 400} \qquad c_4 = -\overline{c_3} \ .$$

The operator:

$$\widetilde{W} = (W_2S_2)^2W_2 \ , \text{ where } S_2 = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix}$$

belongs to the normalizer of $\Gamma_0(N)$ and we have $\varphi \circ \widetilde{W} = \varphi$. The operator $\widetilde{W}$ is an involution of $X_0(N)$ (we can not simplify it because W_2 and S_2 do not commute). There are 4 fixed points of $\widetilde{W}$ which are:

$$c_5 = \frac{16 + \sqrt{-64}}{2 \times 80} \qquad c_6 = -\overline{c_5} \ ,$$
$$c_7 = \frac{-144 + \sqrt{-64}}{2 \times 400} \qquad c_8 = -\overline{c_7} \ .$$

In fact, φ is completely factorized:

$$\varphi \ : X_0(80) \xrightarrow[2]{\pi_2} X_0(80)/W_2 \xrightarrow[2]{\widetilde{\pi_2}} X_0(80)/(W_2, \widetilde{W}) \simeq E(\mathbb{C}) \ .$$

The critical points of π_2 are c_1, c_2, c_3 et c_4. We have $\overline{c_5} = \pi_2(c_5) = \pi_2(c_7)$ and $\overline{c_6} = \pi_2(c_6) = \pi_2(c_8)$, so in $X_0(80)/W_2$:

$$\widetilde{W}\overline{c_5} = \overline{c_5} \quad \text{and } \widetilde{W}\overline{c_6} = \overline{c_6} \ .$$

Thus, $\pi_2(c_5)$ and $\pi_2(c_6)$ are critical points for $\widetilde{\pi_2}$. Let denote by P_1, P_2, P_3 and P_4 the following different cusps of $X_0(N)$:

$$P_1 = \frac{1}{4} \ , \ P_2 = \frac{3}{4} \ , \ P_3 = \frac{1}{20} \ , \ P_4 = \frac{3}{20} \ .$$

We have $\pi_2(P_1) = \{P_1, P_2\}$ and $\pi_2(P_3) = \{P_3, P_4\}$. The operator $\widetilde{W}$ acts on these cusps by $\widetilde{W}P_1 = P_2$ and $\widetilde{W}P_3 = P_4$. We deduce that $\pi_2(P_1)$ and $\pi_2(P_3)$ are critical points for $\widetilde{W}$. Finally, we have obtained the 12 critical points for φ and the ramification points are:

$$\begin{aligned}
\varphi(c_1) = \varphi(c_4) &= (1+2i, -2+4i) \\
\varphi(c_2) = \varphi(c_3) &= (1-2i, -2-4i) \\
\varphi(c_5) = \varphi(c_7) &= (1-2i, 2+4i) \\
\varphi(c_6) = \varphi(c_8) &= (1+2i, 2-4i) \\
\varphi(P_1) = \varphi(P_2) &= (-3, 0) \\
\varphi(P_3) = \varphi(P_4) &= (1, 0)
\end{aligned}$$

Definition 1. *An elliptic curve E is involutory if there exists operators U_1, U_2, $\cdots$, U_k belonging to the normalisator of $\Gamma_0(N)$ in $SL_2(\mathbb{R})$ through which φ can be completely factorized :*

$$\varphi \ : X_0(N) \longrightarrow X_1 \longrightarrow X_2 \cdots \longrightarrow X_k \simeq E(\mathbb{C}) \ ,$$

and where $X_j = X_{j-1}/U_j$ and U_j is an involution of X_{j-1}.

The curve of the example is involutory and the critical and ramification points can be completely described. In the table (1), we give a list off all involutory curves E with conductor $N \leq 100$ such that E is not isomorphic to $X_0(N)$. The column $(U_j)_j$ gives, with order, involutions for a complete factorization of φ.

The factorizations through operators (completely or partially) explain most of the time why some critical points are quadratic. Nevertheless there are cases for which critical points are quadratic whereas no factorization seems to be possible. This is the case, for example, for the curve E defined by:

$$E \ : y^2 + xy = x^3 + x^2 - 11x \ ,$$

N	$[a_1,a_2,a_3,a_4,a_6]$	$(U_j)_j$	N	$[a_1,a_2,a_3,a_4,a_6]$	$(U_j)_j$
26	$[1,0,1,-5,-8]$	W_2	58	$[1,-1,0,-1,1]$	W_2, W_{29}
26	$[1,-1,1,-3,3]$	W_{13}	61	$[1,0,0,-2,1]$	W_61
30	$[1,0,1,1,2]$	W_5	62	$[1,-1,1,-1,1]$	W_{31}
34	$[1,0,0,-3,1]$	W_{17}	64	$[0,0,0,-4,0]$	$(W_2S_2)^2$
35	$[0,1,1,9,1]$	W_5	65	$[1,0,0,-1,0]$	W_{65}
37	$[0,0,1,-1,0]$	W_{37}	66	$[1,0,1,-6,4]$	W_2, W_{11}
38	$[1,1,1,0,1]$	W_{19}	66	$[1,1,1,-2,-1]$	W_3, W_{11}
39	$[1,1,0,-4,-5]$	W_3	69	$[1,0,1,-1,-1]$	W_{23}
40	$[0,0,0,-7,-6]$	$(W_2S_2)^2$	70	$[1,-1,1,2,-3]$	W_5, W_{14}
42	$[1,1,1,-4,5]$	W_7	72	$[0,0,0,6,-7]$	W_2, $(W_2S_2)^2$
43	$[0,1,1,0,0]$	W_{43}	77	$[0,0,1,2,0]$	W_7, W_{11}
44	$[0,1,0,3,-1]$	W_{11}	79	$[1,1,1,-2,0]$	W_{79}
45	$[1,-1,0,0,-5]$	W_5	80	$[0,0,0,-7,6]$	W_2, $(W_2S_2)^2W_2$
48	$[0,1,0,-4,-4]$	$(W_2S_2)^2$	80	$[0,-1,0,4,-4]$	$(S_2W_2)^2$, (S_2W_2)
50	$[1,0,1,-1,-2]$	W_2	82	$[1,0,1,-2,0]$	W_2, W_{41}
50	$[1,1,1,-3,1]$	W_5	83	$[1,1,1,1,0]$	W_{83}
51	$[0,1,1,1,-1]$	W_{17}	88	$[0,0,0,-4,4]$	W_2, W_{11}, $(W_2S_2)^2$
53	$[1,-1,1,0,0]$	W_{53}	89	$[1,1,1,-1,0]$	W_{89}
54	$[1,-1,1,1,-1]$	W_3	91	$[0,0,1,1,0]$	W_7, W_{13}
55	$[1,-1,0,-4,3]$	W_{11}	92	$[0,1,0,2,1]$	W_{23}
56	$[0,0,0,1,2]$	W_7	94	$[1,-1,1,0,-1]$	W_{47}
56	$[0,-1,0,0,-4]$	S_2W_7, $(S_2W_2)^2$	96	$[0,1,0,-2,0]$	W_2, $(S_2W_2)^2$
57	$[0,-1,1,-2,2]$	W_3, W_{19}	99	$[1,-1,1,-2,0]$	W_3, W_{11}

TABLE 1. Involutory curves with conductor $N \leq 100$, and such that $\deg(\varphi) \neq 1$. The curves are given in the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

with conductor $N = 33$, the 4 critical points are the following Heegner points:

$$c_1 = \frac{36+\sqrt{-24}}{2\times 33} \qquad c_2 = -\overline{c_1}\ ,$$
$$c_2 = \frac{36+\sqrt{-24}}{4\times 33} \qquad c_4 = -\overline{c_3}\ .$$

We have $\deg(\varphi) = 3$ and it is hard to explain this by a natural operator. If one wants to prove that a quadratic point is a zero of f, one can use the following way.

Let $\gamma_1, \gamma_2, \ldots, \gamma_\mu$ be a set of representatives for the right cosets of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$, then classical arguments show that the coefficients of:

$$P(X) = \prod_{j=1}^{\mu}\left(X - N^6\frac{f^6(\gamma_j z)}{\Delta(\gamma_j z)}\right)$$

belong to $\mathbb{Z}[j]$ (at least if N is squarefreee), where j is the modular invariant and Δ the usual cusp form of weight 12 on the full modular group. The computation of $P(X)$ is possible (but delicate and long since the coefficients explode with N). Consider the constant term of this polynomial $P(0) = G(j)$ where G is a polynomial with integer coefficients. We have:

$$G(j(z)) = (-1)^{\mu} N^{6\mu} \left(\prod_{j=1}^{\mu} f(\gamma_j z) \right)^6 \Delta(z)^{-\mu}$$

Let z_0 be a quadratic point. Then, $j(z_0)$ belongs to the ring of integers of a certain number field and so belongs to some discrete subgroup of $\mathbb{C}$, hence it is easy to determine if $G(j(z_0)) = 0$. Furthermore, the factorization of $G(x)$ in irreducible elements gives the order of vanishing at $j(z_0)$. Now, by numerical computations, we can decide which γ_j are such that $f(\gamma_j z_0) \neq 0$, the others γ_j lead to zero of f (Δ does not vanish in $\mathbb{H}$).

Coming back to the example of the elliptic curve E with conductor $N = 33$. We let $f(\tau) = q + q^2 - q^3 - q^4 - 2q^5 + \dots$ be the newform of weight 2 on $\Gamma_0(33)$ associated to the elliptic curve E. Then, in this case, we have:

$$G(j) = 33^{24} 3^{48} (j^2 - 4834944j + 14670139392)^{12} \ ,$$

And the points $j(c_1), \cdots\ j(c_4)$, where $c_1, \cdots\ c_4$ are defined above, are the zeros of this polynomial.

3. Localization of the zeros of f

Whenever a zero of f is neither a quadratic point on $X_0(N)$ nor a cusp then it is a transcendental number in $\mathbb{H}$ (because $j(z)$ and z are both algebraic if and only if z is quadratic). In this section, we propose to give a method in order to calculate at least numerically the zeros of f and hence the critical and ramification points of the modular parametrization.

Let:

$$\alpha_j = \begin{pmatrix} 0 & -1 \\ 1 & j-1 \end{pmatrix} \quad \text{for } j = 1, 2, \cdots, N \ ,$$

$$\text{and} \quad \alpha_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ .$$

Then, we complete the set $\{\alpha_0, \dots, \alpha_N\}$ by matrices $\alpha_{N+1}, \dots, \alpha_\mu$ in order to obtain a set of representatives for the right cosets of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$. i.e.:

$$SL_2(\mathbb{Z}) = \bigcup_{j=1}^{\mu} \Gamma_0(N) \alpha_j \ .$$

If N is prime, we need not complete the first set since, in this case, we have $\mu = N + 1$. We let:

$$\mathcal{F} = \{z \in \mathbb{H},\ -\frac{1}{2} < \Re e(z) \leq \frac{1}{2},\ |z| \geq 1\}$$

be the classical fundamental domain for the full modular group $SL_2(\mathbb{Z})$. Then, we define:

$$\mathcal{F}_N = \bigcup_{j=1}^{\mu} W_N\, \alpha_i\, \mathcal{F}\ ,$$

where $W_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ is the Fricke involution, $\mathcal{F}_N$ is a fundamental domain for $X_0(N)$. It may be not connected. We will search the zeros of f in $\mathcal{F}_N$.

Proposition 3.1. *There exists a positive real number $B = B_f < 0.27$ such that:*

$$\begin{cases} f(z) = 0 \\ \Im m(z) > B \end{cases} \implies z = \infty\ .$$

Proof. We apply Rouché's theorem to the function $q \mapsto \sum_n a(n)q^n$, $\mathbb{D} \to \mathbb{D}$. The (very bad) bound $B < 0.27$ comes from $|a(n)| \leq 2n$. □

For applications we compute a more accurate numerical value for B, in fact B seems to decrease as N grows. In [11], we say that a cusp a/b is a unitary cusp if $\gcd(b, N/b) = 1$ (in this definition, we implicitly suppose that the representative a/b is such that $\gcd(a, b) = 1$ and $b|N$).

Corollary 3.1. *Let a/b be an unitary cusp, there exists a neighborhood $V \subset X_0(N)$ of a/b such that:*

$$\begin{cases} f(z) = 0 \\ z \in V \end{cases} \implies z = \frac{a}{b}\ .$$

Proof. If a/b is unitary, one can find an Atkin-Lehner operator W such that $Wa/b = \infty$, and we take $V = W(\{\Im(z) > B\})$. □

This also proves that an unitary cusp is never a critical point for φ; in fact, one can also prove this by determining the Fourier expansion of f at the cusp a/b. If a/b is not unitary, then a/b may be a critical point (see the example above). At least, we remark that:

$$f(z) = 0 \iff f\left(W_N z\right) = 0\ .$$

Thus, we can always choose $z' \in \{z, W_N z\}$ such that $|z'| \geq 1/\sqrt{N}$ and we can forget the half-disk $\{z \in \mathbb{H}\ ,\ \ |z| < 1/\sqrt{N}\}$ when we are looking for critical points.

All the considerations above allow us to restrict the domain of search for the zeros of f (see figure 1).

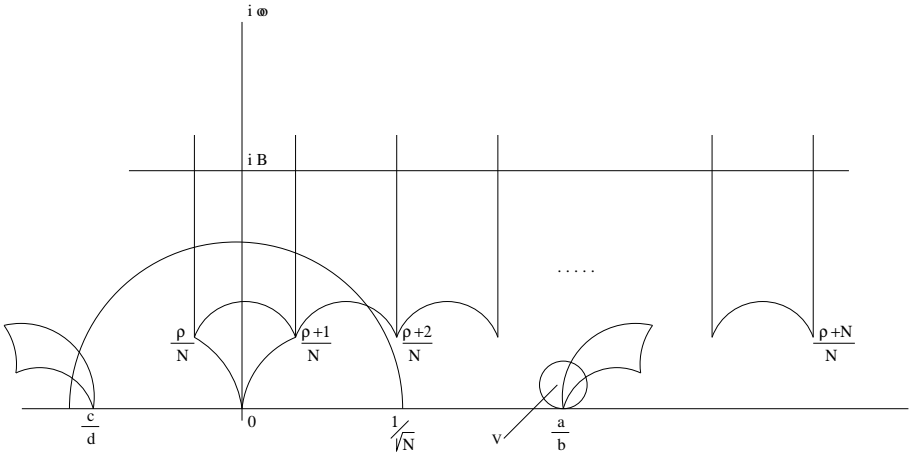

FIGURE 1. Fundamental domain for $X_0(N)$ (and restrictions)

Then, in the domain left, we localize the zeros of f using Cauchy's integral. More precisely, we partition the domain in small parts R and for each R we compute:

$$Ind_R = \frac{1}{2i\pi}\int_{\partial R}\frac{f'(z)}{f(z)}dz = \frac{1}{2i\pi}\int_{\partial f(R)}\frac{dz}{z} \ .$$

It is an integer: if it is zero then R does not contain any zero of f, otherwise R contains some zeros. Then, we divide R in small parts and continue. When the localization of a zero is enough precise, we use Newton method in order to obtain the desired accuracy.

Once the zeros of f obtained, we check that they are inequivalent (because the Newton 's method may jump a zero out of the restricted domain). We eliminate those coming from the elliptic points. There must have $2g-2$ critical points left. The method above is quite efficient in practice, even in the case where zeros are multiple. Let denote by c_1, c_2, ..., c_{2g-2} the critical points of φ. Then, we consider the ramification points associated: $z_j = \varphi(c_j) = (x_j, y_j)$. From the algebraic properties of the z_j the polynomials:

$$P_x(X) = \prod_{j=1}^{2g-2}(X - x_j)$$

$$P_y(X) = \prod_{j=1}^{2g-2}(X - y_j)$$

have rational coefficients. We can compute them numerically and we verify that the results we obtain are closed to certain rational polynomials; this

provides a check of computations. Indeed, in each case we have considered, we get a polynomial very close to a rational polynomial and we can then be enough self confident in the results. Furthermore, P_x and P_y enable us to define a number field K where the points z_j are defined.

Example Let consider the elliptic curve of conductor $N = 46$ defined by the equation:

$$y^2 + xy = x^3 - x^2 - 10x - 12 \ .$$

It is the first curve (for the conductor) for which the critical points are not Heegner points. The genus of $X_0(46)$ is $g = 5$ so there are 8 critical points. We determine them by the method explained above:

$$\begin{aligned} c_1 &= 0.118230\cdots + 0.088094\ldots\ i & c_2 &= -\overline{c_1} \\ c_3 &= 0.345846\cdots + 0.047527\ldots\ i & c_4 &= -\overline{c_3} \\ c_5 &= 0.172454\cdots + 0.010527\ldots\ i & c_6 &= -\overline{c_5} \\ c_7 &= 0.435609\cdots + 0.019852\ldots\ i & c_8 &= -\overline{c_7} \end{aligned}$$

And then, we can compute P_x and P_y (numerically):

$$\begin{aligned} P_x(X) &= \frac{1}{23^2}(23X^4 - 70X^3 + 567X^2 + 2472X + 3184)^2 \\ P_y(X) &= \frac{1}{23^3}(12167X^8 + 37030X^7 + 7085747X^6 + 12153116X^5 + \\ &\qquad 971389940X^4 - 3448946432X^3 - 1586824496X^2 + \\ &\qquad 9784853696X + 7416293824) \ . \end{aligned}$$

There are 93 isogeny classes of elliptic curves with conductor $N \leq 100$. Among them, 46 are involutory and are listed in table (1) (more precisley those which are not isomorphic to $X_0(N)$). There are 30 non involutory curves for which all the critical points are quadratic (so due to some factorization and "accidental" reason as for the case $N = 33$). Some cusps are critical points for 4 of the 93 curves, they are all involutory ($N = 48$, $N = 64$ and the 2 curves with $N = 80$). The first case for which the group $E(\mathbb{Q})^{fond}$ is not of finite index in $E(\mathbb{Q})$ is obtained by the curve $y^2 + y = x^3 + x^2 - 7x + 5$ with conductor $N = 91$. For this curve $E(\mathbb{Q})^{crit}$ is of finite index. The curve $y^2 = x^3 - x + 1$ with conductor $N = 92$ is the first example of curve with rank 1 for which $E(\mathbb{Q})^{crit}$ is a torsion sub-group.

4. A rank 2 curve

In this section, we comment some of the results we obtained concerning the first elliptic curve of rank 2 over $\mathbb{Q}$. This is the elliptic curve with conductor $N = 389$ defined by:

$$E \ : \ y^2 + y = x^3 + x^2 - 2x \ .$$

The group $E(\mathbb{Q})$ is torsion free of rank 2 generated by $G_1 = (0,0)$ and $G_2 = (1,0)$. The genus of $X_0(389)$ is $g = 32$, there are 2 cusps (389 is prime) and no elliptic element. Furthermore, $\deg(\varphi) = 40$. We computed the 62 critical points of φ. As predicted by theorem 1.1, there are 2 fundamental critical points:

$$\begin{aligned} c_1 &\approx 0.016929839464381450186921 6816 \times i \\ c_2 &\approx 0.151843973051963138200024 7052 \times i \ . \end{aligned}$$

More astonishing, 2 critical points are Heegner points of discriminants -19:

$$c_3 = \frac{337 + \sqrt{-19}}{2 \times 19} \quad \text{and} \quad c_4 = \frac{-337 + \sqrt{-19}}{2 \times 19}$$

Two critical points belong to the line $\Re e(s) = 1/2$:

$$\begin{aligned} c_5 &\approx \frac{1}{2} + 0.008015879627931564443796916 \times i \\ c_6 &\approx \frac{1}{2} + 0.080175046492899577113086416 \times i \ . \end{aligned}$$

The last remark comes from a generalization of theorem 1.1:

Theorem 4.1. *Let r be the analytic rank of E and m be the number of critical points of odd order lying on the line $1/2 + i\mathbb{R}$.*

- *If $2 \nmid N$ or $4 \mid N$, then $r \leq m$ and these numbers have the same parity. If $a(2) = 2$ we have the stronger inequality $r + 2 \leq m$.*
- *If $2||N$ then $r \leq m$ and these numbers have the same parity if and only if $a(2) = -1$.*

Proof. First, the end points of the line $I = 1/2 + i\mathbb{R}$ are not critical point since f has only a single zero at the cusp $1/2$ (indeed, if $4 \mid N$ then $f(\tau + 1/2) = -f(\tau)$, if $2||N$ then $1/2$ is a unitary cusp and so a single zero of f and if $2 \nmid N$ the cusp $1/2$ and ∞ are equivalent). A direct calculation also shows that there are not any elliptic point on I (because $N \geq 11$), thus all zeros of f on $I \cap \mathbb{H}$ are critical points for φ.

If $4 \mid N$ then $f(\tau + \frac{1}{2}) = -f(\tau)$ and the proposition comes from theorem 1.1. Otherwise, let $L^*(E,s) = -\sum_{n \geq 1} (-1)^n a(n) n^{-s}$, we have:

$$L^*(E,s) = (2L_2(E, 2^{-s}) - 1) L(E,s) \ ,$$

where $L(E,s)$ is the L-function of E (or f) and $L_2(E,X)$ is its Euler factor at $p = 2$. One can see that the order of vanishing ν of $2L_2(E, 2^{-s}) - 1$ at

$s = 0$ is :

- $\nu = 2$ if $a(2) = 2$ (in this case, we have $2 \nmid N$).
- $\nu = 1$ if $2||N$ and $a(2) = 1$.
- $\nu = 0$ otherwise.

Then the order of vanishing of (the analytic continuation of) $L^*(E, s)$ at $s = 1$ is $r' = r + \nu$. Furthermore,

$$L^*(E, s) = \frac{-2\pi}{\Gamma(s)} \int_0^\infty f\left(\frac{1}{2} + it\right) (2\pi t)^{s-1} dt$$

and we can follow the proof of Mazur and Swinnerton-Dyer. Since the order of vanishing of $L^*(E, s)$ at $s = 1$ is r' then:

$$J_\alpha = \int_0^\infty (\log(2\pi t))^\alpha f\left(\frac{1}{2} + it\right) dt = 0 \text{ for } \alpha = 0, \ldots, r' - 1 \ .$$

Let $1/2+it_1, \ldots, 1/2+it_m$ the zeros of f of odd order lying on $I \cap \mathbb{H}$. Then, $f\left(\frac{1}{2} + it\right) \prod_{j=1}^m \log(2\pi t) - \log(2\pi t_j)$ is of constant sign, and the integral:

$$\int_0^\infty f\left(\frac{1}{2} + it\right) \prod_{j=1}^m (\log(2\pi t) - \log(2\pi t_j))\, dt$$

is not zero. But, this integral is a linear combination of $J_0, \ldots, J_m$ and so $m \geq r'$. This proves the inequalities of the theorem.

If N is odd then the Fricke involution:

$$W_N = \begin{pmatrix} N & (-1-N)/2 \\ 2N & -N \end{pmatrix}$$

maps the line $\Re e(s) = 1/2$ to itself. Since $f(z) = 0 \Leftrightarrow f(W_N z) = 0$ with the same order of vanishing, the parity of the number of zero of odd order of f lying on $I \cap \mathbb{H}$ is given by the parity of the order of vanishing of f at the fixed point of W_N (i.e. at $\tau = 1/2\sqrt{N}$). But, $f|_{W_N} = -\varepsilon f$, where ε is the sign of the functional equation of $L(E, s)$, so we see that this order has the same parity than the analytic rank of E.

If $2||N$ then the Atkin-Lehner involution:

$$W_{N/2} = \begin{pmatrix} N/2 & (-1-N/2)/2 \\ N & -N/2 \end{pmatrix}$$

maps the line I to itself. The same argument as before allows us to conclude except that in this case we have $f|_{W_{N/2}} = a(2)\varepsilon f$ which explains the eventual difference between the parities. □

For our curve E with conductor $N = 389$, we have $\varphi(c_3) = \varphi(c_4) = 0$ so we have determined the polynomial $P_{xr}(X) = \prod_*(X - x(\varphi(c)))$ where the product runs through the critical points except c_3 and c_4 and where $x(P)$ denotes the x-coordinate of P. The numerical computations of $P_{xr}(X)$ lead

to a polynomial which is closed to a rational polynomial, giving a check of computations. This polynomial is the square of an irreducible polynomial over $\mathbb{Q}$ of degree 30 with denominator:

$$2^{52} \times 7^6 \times 11^3 \times 19^5 \times 67^3 \times 389^7 \ .$$

It also appears that the sub-group $E(\mathbb{Q})^{crit}$ is a torsion group.

Acknowledgement. Parts of this work has been written during a Post-doctoral position at the École Polytechnique Fédérale de Lausanne. The author is very pleased to thank the prof. Eva Bayer and the members of the "Chaire des structures algébriques et géométriques" for their support and their kindness.

References

[1] A.O.L. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(N)$. Math. Ann. **185** (1970), 134–160.
[2] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, `pari-gp`, available at http://www.math.u-psud.fr/~belabas/pari/
[3] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild 3-adic exercises*. J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).
[4] B. Birch, *Heegner points of elliptic curves*. Symp. Math. Inst. Alta. Math. **15** (1975), 441–445.
[5] H. Cohen, *A course in computational algebraic number theory*. Graduate Texts in Math. **138**, Springer-Verlag, New-York, 4-th corrected printing (2000).
[6] J. Cremona, *Algorithms for modular elliptic curves*. Cambridge University Press, (1997) second edition.
[7] J. Cremona, *Elliptic curve data for conductors up to 25000*. Available at http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html
[8] C. Delaunay, *Computing modular degrees using L-functions*. Journ. theo. nomb. Bord. **15** (3) (2003), 673–682.
[9] B. Gross, *Heegner points on* $X_0(N)$. Modular Forms, ed. R. A. Ramkin, (1984), 87–105.
[10] B. Gross, D. Zagier, *Heegner points and derivatives of L-series*. Invent. Math. **84** (1986), 225–320.
[11] B. Mazur, P. Swinnerton-Dyer, *Arithmetic of Weil curves*. Invent. Math. **25** (1974), 1–61.
[12] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*. Math. Soc of Japan **11**, Princeton university Press (1971).
[13] N. Skoruppa, D. Zagier, *Jacobi forms and a certain space of modular forms*. Inv. Math. **98** (1988), 113–146.
[14] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*. Ann. of Math. (2) **141** (1995), no. 3, 553–572.
[15] M. Watkins, *Computing the modular degree*. Exp. Math. **11** (4) (2002), 487–502.
[16] A. Wiles, *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. (2) **141** (1995), no.3, 443–551.
[17] D. Zagier, *Modular parametrizations of elliptic curves*. Canad. Math. Bull. **28** (3) (1985), 372–384.

Christophe Delaunay
Institut Camille Jordan
Bâtiment Braconnier
Université Claude Bernard Lyon 1
43, avenue du 11 novembre 1918
69622 Villeurbanne cedex, France
E-mail : `delaunay@igd.univ-lyon1.fr`