
PARAMETRIZING ELLIPTIC CURVES BY MODULAR UNITS

by

François Brunault

Abstract. — It is well-known that every elliptic curve over the rationals admits a parametrization by means of modular functions. In this short note, we show that only finitely many elliptic curves over \mathbf{Q} can be parametrized by modular units. This answers a question raised by Zudilin in a recent work on Mahler measures. Further, we give the list of all elliptic curves E of conductor up to 1000 parametrized by modular units supported in the rational torsion subgroup of E . Finally, we raise several open questions.

Since the work of Boyd [3], Deninger [6] and others, it is known that there is a close relationship between Mahler measures of polynomials and special values of L -functions. Although this relationship is still largely open, some strategies have been identified in several instances. Specifically, let $P \in \mathbf{Q}[x, y]$ be a polynomial whose zero locus defines an elliptic curve E . If the polynomial P is tempered, then the Mahler measure of P can be expressed in terms of a regulator integral

$$(1) \quad \int_{\gamma} \log |x| d \arg(y) - \log |y| d \arg(x)$$

where γ is a (non necessarily closed) path on E (see [6, 12]). If the curve E happens to have a parametrization by *modular units* $x(\tau)$, $y(\tau)$, then we may change to the variable τ in (1) and try to compute the regulator integral using [12, Thm 1]. In favourable cases, this leads to an identity between the Mahler measure of P and $L(E, 2)$: see for example [12, §3] and the references therein. The following natural question, raised by Zudilin, thus arises:

Which elliptic curves can be parametrized by modular units?

We show in Section 1 that only finitely many elliptic curves over \mathbf{Q} can be parametrized by modular units. The proof uses Watkins' lower bound on the modular degree of elliptic curves. Further, we give in Section 2 the list of all elliptic curves E of conductor up to 1000 parametrized by modular units supported in the rational torsion subgroup of E . It turns out that there are 30 such elliptic curves. Finally, we raise in Section 3 several open questions.

1. A finiteness result

Definition 1. — Let E/\mathbf{Q} be an elliptic curve of conductor N . We say that E can be *parametrized by modular units* if there exist two modular units $u, v \in \mathcal{O}(Y_1(N))^\times$ such that the function field $\mathbf{Q}(E)$ is isomorphic to $\mathbf{Q}(u, v)$.

Theorem 2. — *There are only finitely many elliptic curves over \mathbf{Q} which can be parametrized by modular units.*

Let E/\mathbf{Q} be an elliptic curve of conductor N . Assume that E can be parametrized by two modular units u, v on $Y_1(N)$. Then there is a finite morphism $\varphi : X_1(N) \rightarrow E$ and two rational functions $f, g \in \mathbf{Q}(E)^\times$ such that $\varphi^*(f) = u$ and $\varphi^*(g) = v$.

Let E_1 be the $X_1(N)$ -optimal elliptic curve in the isogeny class of E , and let $\varphi_1 : X_1(N) \rightarrow E_1$ be an optimal parametrization. By [9, Prop 1.4], there exists an isogeny $\lambda : E_1 \rightarrow E$ such that $\varphi = \lambda \circ \varphi_1$. Consider the functions $f_1 = \lambda^*(f)$ and $g_1 = \lambda^*(g)$. Note that $u = \varphi_1^*(f_1)$ and $v = \varphi_1^*(g_1)$. Theorem 2 is now a consequence of the following result.

Theorem 3. — *If N is sufficiently large, then $\varphi_1^*(\mathbf{Q}(E_1)) \cap \mathcal{O}(Y_1(N)) = \mathbf{Q}$.*

Proof. — Let $C_1(N)$ be the set of cusps of $X_1(N)$. Let $f \in \mathbf{Q}(E_1) \setminus \mathbf{Q}$ be such that $\varphi_1^*(f) \in \mathcal{O}(Y_1(N))$. Let P be a pole of f . Then $\varphi_1^{-1}(P)$ must be contained in $C_1(N)$, and we have

$$\deg \varphi_1 = \sum_{Q \in \varphi_1^{-1}(P)} e_{\varphi_1}(Q) \leq \sum_{Q \in C_1(N)} e_{\varphi_1}(Q).$$

Let g_N be the genus of $X_1(N)$. By the Riemann-Hurwitz formula for φ_1 , we have

$$2g_N - 2 = \sum_{Q \in X_1(N)} (e_{\varphi_1}(Q) - 1).$$

It follows that

$$\begin{aligned} \deg \varphi_1 &\leq \#C_1(N) + \sum_{Q \in C_1(N)} (e_{\varphi_1}(Q) - 1) \\ &\leq \#C_1(N) + 2g_N - 2. \end{aligned}$$

By the classical genus formula [8, Prop 1.40], and since $X_1(N)$ has no elliptic points for $N \geq 4$, we have

$$\#C_1(N) + 2g_N - 2 = \frac{1}{12} [\mathrm{SL}_2(\mathbf{Z}) : \Gamma_1(N)] = \frac{\phi(N)\nu(N)}{12} \quad (N \geq 4)$$

where $\phi(N)$ denotes Euler's function, and $\nu(N)$ is defined by

$$\nu(N) = N \prod_{i=1}^k \left(1 + \frac{1}{p_i}\right) \quad \text{if } N = \prod_{i=1}^k p_i^{\alpha_i}.$$

We thus get

$$(2) \quad \deg \varphi_1 \leq \frac{\phi(N)\nu(N)}{12}.$$

We are now going to show that (2) contradicts lower bounds of Watkins [11] on the modular degree if N is sufficiently large. Let E_0 be the strong Weil curve in the isogeny class of E . We have a commutative diagram

$$(3) \quad \begin{array}{ccc} X_1(N) & \xrightarrow{\pi} & X_0(N) \\ \downarrow \varphi_1 & & \downarrow \varphi_0 \\ E_1 & \xrightarrow{\lambda_0} & E_0. \end{array}$$

We deduce that

$$\deg \varphi_1 = \frac{\deg \pi \cdot \deg \varphi_0}{\deg \lambda_0}.$$

We have $\deg \pi = \frac{\phi(N)}{2}$. For every $\alpha \in (\mathbf{Z}/N\mathbf{Z})^\times / \pm 1$, there exists a unique point $A(\alpha) \in E_1(\mathbf{Q})_{\mathrm{tors}}$ such that $\varphi_1 \circ \langle \alpha \rangle = t_{A(\alpha)} \circ \varphi_1$, where $t_{A(\alpha)}$ denotes translation by $A(\alpha)$. The map $\alpha \mapsto A(\alpha)$ is a morphism of groups and its image is $\ker(\lambda_0)$. It follows that $\deg(\lambda_0) \leq \#E_1(\mathbf{Q})_{\mathrm{tors}} \leq 16$. By [11], we have $\deg \varphi_0 \gg N^{7/6-\varepsilon}$ for any $\varepsilon > 0$. It follows that $\deg \varphi_1 \gg \phi(N)N^{7/6-\varepsilon}$. Since $\nu(N) \ll N^{1+\varepsilon}$ for any $\varepsilon > 0$, this contradicts (2) for N sufficiently large. \square

Remark 4. — It would be interesting to determine the complete list of elliptic curves over \mathbf{Q} parametrized by modular units. Unfortunately, the bound on the conductor N provided by Watkins' result, though effective, is too large to permit an exhaustive search. However, we observed numerically in [4] that the ramification index of φ_0 at a cusp of $X_0(N)$ seems to be always a divisor of 24. If this observation is true, then we can replace (2) by the better bound $\deg \varphi_1 \leq 12\phi(N) \sum_{d|N} \phi((d, N/d))$. Combining this with known linear lower bounds on $\deg \varphi_0$ (see [11]), this yields a better (but still large) bound on N . Furthermore, if we restrict to semistable elliptic curves, then φ_0 , π and φ_1 are unramified at the cusps; in this case we get that N has at most 6 prime factors and $N \leq 233310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 101$.

2. Preimages of torsion points under modular parametrizations

In order to find elliptic curves parametrized by modular units, we consider the following related problem. Let E be an elliptic curve over \mathbf{Q} of conductor N , and let $\varphi : X_1(N) \rightarrow E$ be a modular parametrization sending the 0-cusp to 0. By the Manin-Drinfeld theorem, the image by φ of a cusp of $X_1(N)$ is a torsion point of E . Conversely, given a point $P \in E_{\text{tors}}$, when does the preimage of P under φ consist only of cusps? The link between this question and parametrizations by modular units is given by the following easy lemma.

Lemma 5. — *Suppose that there exists a subset S of $E(\mathbf{Q})_{\text{tors}}$ satisfying the following two conditions:*

- (1) *We have $\varphi^{-1}(S) \subset C_1(N)$.*
- (2) *There exist two functions f, g on E supported in S such that $\mathbf{Q}(E) = \mathbf{Q}(f, g)$.*

Then E can be parametrized by modular units.

Proof. — By condition (1), the functions $u = \varphi^*(f)$ and $v = \varphi^*(g)$ are modular units of level N , and by condition (2), we have $\mathbf{Q}(E) \cong \mathbf{Q}(u, v)$. \square

We are therefore led to search for elliptic curves E/\mathbf{Q} admitting sufficiently many torsion points P such that $\varphi^{-1}(P) \subset C_1(N)$.

We first give an equivalent form of condition (2) in Lemma 5.

Proposition 6. — *Let S be a subset of $E(\mathbf{Q})_{\text{tors}}$. Let \mathcal{F}_S be the set of nonzero functions f on E which are supported in S . The following conditions are equivalent:*

- (a) *There exist two functions $f, g \in \mathcal{F}_S$ such that $\mathbf{Q}(E) = \mathbf{Q}(f, g)$.*
- (b) *The field $\mathbf{Q}(E)$ is generated by \mathcal{F}_S .*
- (c) *We have $\#S \geq 3$, and there exist two points $P, Q \in S$ such that $P - Q$ has order ≥ 3 .*

In order to prove Proposition 6, we show the following lemma.

Lemma 7. — *Let $P \in E(\mathbf{Q})_{\text{tors}}$ be a point of order $n \geq 2$. Let f_P be a function on E such that $\text{div}(f_P) = n(P) - n(0)$. Then the extension $\mathbf{Q}(E)/\mathbf{Q}(f_P)$ has no intermediate subfields. Moreover, if $P, P' \in E(\mathbf{Q})_{\text{tors}}$ are points of order $n \geq 4$ such that $\mathbf{Q}(f_P) = \mathbf{Q}(f_{P'})$, then $P = P'$.*

Proof. — Let K be a field such that $\mathbf{Q}(f_P) \subset K \subset \mathbf{Q}(E)$. If K has genus 1, then K is the function field of an elliptic curve E'/\mathbf{Q} and f_P factors through an isogeny $\lambda : E \rightarrow E'$. Then $\text{div}(f_P)$ must be invariant under translation by $\ker(\lambda)$. This obviously implies $\ker(\lambda) = 0$, hence $K = \mathbf{Q}(E)$. If K has genus 0, then we have $K = \mathbf{Q}(h)$ for some function h on E , and we may factor f_P as $g \circ h$ with $g : \mathbf{P}^1 \rightarrow \mathbf{P}^1$. We may assume $h(P) = 0$ and $h(0) = \infty$. Then $g^{-1}(0) = \{0\}$ and $g^{-1}(\infty) = \{\infty\}$, which implies $g(t) = at^m$ for some $a \in \mathbf{Q}^\times$ and $m \geq 1$.

Thus $\operatorname{div}(f) = m \operatorname{div}(h)$. Since $\operatorname{div}(h)$ must be a principal divisor, it follows that $m = 1$ and $K = \mathbf{Q}(f_P)$.

Let $P, P' \in E(\mathbf{Q})$ be points of order $n \geq 4$ such that $\mathbf{Q}(f_P) = \mathbf{Q}(f_{P'})$ and $P \neq P'$. Then $f_{P'} = (af_P + b)/(cf_P + d)$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{GL}_2(\mathbf{Q})$. Considering the divisors of f_P and $f_{P'}$, we must have $f_{P'} = af_P + b$ for some $a, b \in \mathbf{Q}^\times$. Then the ramification indices of $f_P : E \rightarrow \mathbf{P}^1$ at $P, P', 0$ are equal to n , which contradicts the Riemann-Hurwitz formula for f_P . \square

Proof of Proposition 6. — It is clear that (a) implies (b). Let us show that (b) implies (c). If $\#S \leq 2$, then $\mathcal{F}_S/\mathbf{Q}^\times$ has rank at most 1 and cannot generate $\mathbf{Q}(E)$. Assume that for every points $P, Q \in S$, we have $P - Q \in E[2]$. Translating S if necessary, we may assume $0 \in S$. It follows that $S \subset E[2]$ and $\mathcal{F}_S \subset \mathbf{Q}(x) \not\subset \mathbf{Q}(E)$.

Finally, let us assume (c). Translating S if necessary, we may assume $0 \in S$. Let us first assume that S contains a point P of order 2. Then $\mathbf{Q}(f_P) = \mathbf{Q}(x)$ has index 2 in $\mathbf{Q}(E)$ and is the fixed field with respect to the involution $\sigma : p \mapsto -p$ on E . By assumption, there exist two points $Q, R \in S$ such that $Q - R$ has order $n \geq 3$. Let g be a function on E such that $\operatorname{div}(g) = n(Q) - n(R)$. Then it is easy to see that $\operatorname{div}(g)$ is not invariant under σ . It follows that $g \notin \mathbf{Q}(f_P)$ and $\mathbf{Q}(f_P, g) = \mathbf{Q}(E)$. Let us now assume that $S \cap E[2] = \{0\}$. By assumption, S contains two distinct points P, Q having order ≥ 3 . If P or Q has order ≥ 4 , then Lemma 7 implies that $\mathbf{Q}(f_P, f_Q) = \mathbf{Q}(E)$. If P and Q have order 3, then we must have $Q = -P$ because $\mathbf{Q}(E[3])$ contains $\mathbf{Q}(\zeta_3)$. It follows that the function g on E defined by $\operatorname{div}(g) = (P) + (-P) - 2(0)$ has degree 2, so we have $g \notin \mathbf{Q}(f_P)$ and $\mathbf{Q}(f_P, g) = \mathbf{Q}(E)$. \square

Let E/\mathbf{Q} be an elliptic curve of conductor N . Fix a Néron differential ω_E on E , and let f_E be the newform of weight 2 and level N associated to E . We define $\omega_{f_E} = 2\pi i f_E(z) dz$. Let $\varphi_E : X_1(N) \rightarrow E$ be a modular parametrization of minimal degree. We have $\varphi_E^* \omega_E = c_E \omega_{f_E}$ for some integer $c_E \in \mathbf{Z} - \{0\}$ [9, Thm 1.6], and we normalize φ_E so that $c_E > 0$. Conjecturally, we have $c_E = 1$ [9, Conj. I].

We now describe an algorithm to compute the set S_E of points $P \in E(\mathbf{Q})_{\text{tors}}$ such that $\varphi_E^{-1}(P) \subset C_1(N)$. Let $P \in E(\mathbf{Q})_{\text{tors}}$. We define an integer e_P by

$$e_P = \sum_{\substack{x \in C_1(N) \\ \varphi_E(x) = P}} e_{\varphi_E}(x).$$

It is clear that $\varphi_E^{-1}(P) \subset C_1(N)$ if and only if $e_P = \deg \varphi_E$. Let d be a divisor of N , and let C_d be the set of cusps of $X_1(N)$ of denominator d (that is, the set of cusps $\frac{a}{b}$ satisfying $(b, N) = d$). Every cusp $x \in C_d$ can be written (non uniquely) as $x = \langle \alpha \rangle \sigma(\frac{1}{d})$ with $\alpha \in (\mathbf{Z}/N\mathbf{Z})^\times / \pm 1$ and $\sigma \in \operatorname{Gal}(\mathbf{Q}(\zeta_d)/\mathbf{Q})$. Since $e_{\varphi_E}(x) = e_{\varphi_1}(x) = e_{\varphi_1}(1/d)$, we get

$$e_P = \sum_{d|N} e_{\varphi_1}(1/d) \cdot \#\{x \in C_d : \varphi_E(x) = P\}.$$

Recall that for each $\alpha \in (\mathbf{Z}/N\mathbf{Z})^\times$, there exists a unique point $A(\alpha) \in E(\mathbf{Q})_{\text{tors}}$ such that $\varphi_E \circ \langle \alpha \rangle = t_{A(\alpha)} \circ \varphi_E$, where $t_{A(\alpha)}$ denotes translation by $A(\alpha)$. We let $A_E \subset E(\mathbf{Q})_{\text{tors}}$ be the image of the map $\alpha \mapsto A(\alpha)$. Note that the set $\{x \in C_d : \varphi_E(x) = P\}$ is empty unless $\varphi_E(1/d) \in P + A_E$, in which case we have $\varphi_E(C_d) = P + A_E$ and the number of cusps $x \in C_d$ such that $\varphi_E(x) = P$ is given by $\#C_d/\#A_E$. Thus we get

$$e_P = \frac{1}{\#A_E} \sum_{\substack{d|N \\ \varphi_E(1/d) \in P + A_E}} e_{\varphi_1}(1/d) \cdot \#C_d.$$

Furthermore, let $\pi : X_1(N) \rightarrow X_0(N)$ and $\varphi_0 : X_0(N) \rightarrow E_0$ be the maps as in (3). The ramification index of π at $\frac{1}{d}$ is equal to $(d, N/d)$. Thus $e_{\varphi_1}(1/d) = (d, N/d) \cdot e_{\varphi_0}(1/d)$. The quantity $e_{\varphi_0}(1/d)$ is equal to the order of vanishing of ω_{f_E} at the cusp $1/d$, and may be computed numerically (see [4, §7]). Moreover, the number of cusps of $X_0(N)$ of denominator d is given by $\phi((d, N/d))$. It follows that $\#C_d = \phi((d, N/d)) \cdot \phi(N)/(2(d, N/d))$ and we get

$$(4) \quad e_P = \frac{\phi(N)}{2\#A_E} \sum_{\substack{d|N \\ \varphi_E(1/d) \in P+A_E}} e_{\varphi_0}(1/d) \cdot \phi((d, N/d)).$$

Finally, using notations from Section 1, the modular degree of E may be computed as

$$(5) \quad \deg \varphi_E = \frac{\phi(N)}{2} \cdot \frac{\text{covol}(\Lambda_{E_0})}{\text{covol}(\Lambda_E)} \cdot \deg \varphi_0$$

where Λ_{E_0} and Λ_E denote the Néron lattices of E_0 and E . We read off the modular degree $\deg \varphi_0$ from Cremona's tables [5, Table 5]. Formulas (4) and (5) lead to the following algorithm.

- (1) Compute generators $\alpha_1, \dots, \alpha_r$ of $(\mathbf{Z}/N\mathbf{Z})^\times$.
- (2) For each j , compute numerically $\int_{z_0}^{(\alpha_j)z_0} \omega_{f_E}$ for $z_0 = (-\alpha_j + i)/N$.
- (3) Deduce $A_j = A(\alpha_j) \in E(\mathbf{Q})_{\text{tors}}$.
- (4) Compute the subgroup A_E generated by A_1, \dots, A_r .
- (5) Compute the list (P_1, \dots, P_n) of all rational torsion points on E .
- (6) Initialize a list $(e_{P_1}, \dots, e_{P_n}) = (0, \dots, 0)$.
- (7) For each d dividing N , do the following:
 - (a) Compute numerically $z_d = \int_0^{1/d} \omega_{f_E}$.
 - (b) Check whether the point $Q_d = \varphi_E(1/d)$ is rational or not.
 - (c) If Q_d is rational, then do the following:
 - (i) Compute numerically $e_{\varphi_0}(1/d)$.
 - (ii) For each $B \in A_E$, do $e_{Q_d+B} \leftarrow e_{Q_d+B} + e_{\varphi_0}(1/d)\phi((d, N/d))$.
- (8) Output $S_E = \{P \in E(\mathbf{Q})_{\text{tors}} : e_P = \#A_E \cdot \frac{\text{covol}(\Lambda_{E_0})}{\text{covol}(\Lambda_E)} \cdot \deg \varphi_0\}$.

The following table gives all elliptic curves E of conductor ≤ 1000 such that S_E satisfies condition (c) of Proposition 6. Computations were done using Pari/GP [10] and the Modular Symbols package of Magma [2].

Remarks 8. — (1) In order to compute the points A_j in step (3) and Q_d in step (7b), we implicitly make use of Stevens' conjecture that $c_E = 1$. This conjecture is known for all elliptic curves of conductor ≤ 200 [9].

(2) Of course, steps (2), (7a) and (7ci) are done only once for each isogeny class.

(3) If x is a cusp of $X_1(N)$, then the order of $\varphi_E(x)$ is bounded by the exponent of the cuspidal subgroup of $J_1(N)$. Hence we may ascertain that $\varphi_E(x)$ is rational or not by a finite computation.

(4) We compute $e_{\varphi_0}(\frac{1}{d})$ by a numerical method. It would be better to use an exact method.

3. Further questions

Note that in Lemma 5, we considered functions on E which are supported in $E(\mathbf{Q})_{\text{tors}}$. In general, the image by φ_E of a cusp of $X_1(N)$ is only rational over $\mathbf{Q}(\zeta_N)$, and we may use functions on E supported in these non-rational points. In fact, let S'_E denote the set of points $P \in E(\mathbf{Q}(\zeta_N))_{\text{tors}}$ such that $\varphi_E^{-1}(P) \subset C_1(N)$. The set S'_E is stable under the action of $\text{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q})$. Then E can be parametrized by modular units if *and only if* there exist two

E	$E(\mathbf{Q})_{\text{tors}}$	S_E	E	$E(\mathbf{Q})_{\text{tors}}$	S_E
11a3	$\mathbf{Z}/5\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$	26a3	$\mathbf{Z}/3\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
14a1	$\mathbf{Z}/6\mathbf{Z}$	$\{0, (9, 23), (1, -1), (2, -5)\}$	27a3	$\mathbf{Z}/3\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
14a4	$\mathbf{Z}/6\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$	27a4	$\mathbf{Z}/3\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
14a6	$\mathbf{Z}/6\mathbf{Z}$	$\{0, (2, -2), (2, -1)\}$	30a1	$\mathbf{Z}/6\mathbf{Z}$	$\{0, (3, 4), (-1, 0), (0, -2)\}$
15a1	$\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$	$\{0, (-2, 3), (-1, 0), (8, 18)\}$	32a1	$\mathbf{Z}/4\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
15a3	$\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$	$\{0, (0, 1), (1, -1), (0, -2)\}$	32a4	$\mathbf{Z}/4\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
15a8	$\mathbf{Z}/4\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$	35a3	$\mathbf{Z}/3\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
17a4	$\mathbf{Z}/4\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$	36a1	$\mathbf{Z}/6\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
19a3	$\mathbf{Z}/3\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$	36a2	$\mathbf{Z}/6\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
20a1	$\mathbf{Z}/6\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$	40a3	$\mathbf{Z}/4\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
20a2	$\mathbf{Z}/6\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$	44a1	$\mathbf{Z}/3\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
21a1	$\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$	$\{0, (-1, -1), (-2, 1), (5, 8)\}$	54a3	$\mathbf{Z}/3\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
24a1	$\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$	56a1	$\mathbf{Z}/4\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
24a3	$\mathbf{Z}/4\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$	92a1	$\mathbf{Z}/3\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$
24a4	$\mathbf{Z}/4\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$	108a1	$\mathbf{Z}/3\mathbf{Z}$	$E(\mathbf{Q})_{\text{tors}}$

TABLE 1. Some elliptic curves parametrized by modular units

functions $f, g \in \mathbf{Q}(E)^\times$ supported in S'_E such that $\mathbf{Q}(E) = \mathbf{Q}(f, g)$. As the next example shows, this yields new elliptic curves parametrized by modular units.

Example 9. — Consider the elliptic curve $E = X_0(49) = 49a1 : y^2 + xy = x^3 - x^2 - 2x - 1$. The group $E(\mathbf{Q})_{\text{tors}}$ has order 2 and is generated by the point $Q = (2, -1)$, which is none other than the cusp ∞ (recall that the cusp 0 is the origin of E). The set S'_E consists of all cusps of $X_0(49)$. Let P be the cusp $\frac{1}{7}$. It is defined over $\mathbf{Q}(\zeta_7)$ and its Galois conjugates are given by $\{P^\sigma\}_\sigma = \{P, 3P + Q, -5P, -P + Q, -3P, 5P + Q\}$. There exists a function $v \in \mathbf{Q}(E)$ of degree 7 such that $\text{div}(v) = \sum(P^\sigma) + (Q) - 7(0)$. Since $x - 2$ and v have coprime degrees, the curve E can be parametrized by the modular units $u = x - 2$ and v .

Example 10. — Consider the elliptic curve $E = 64a1 : y^2 = x^3 - 4x$. Its rational torsion subgroup is given by $E(\mathbf{Q})_{\text{tors}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. There is a degree 2 morphism $\varphi_0 : X_0(64) \rightarrow E$, and we have $S_E = E(\mathbf{Q})_{\text{tors}}$. However, the image of the cusp $\frac{1}{8}$ is given by $P = \varphi_0(\frac{1}{8}) = (2i, -2\sqrt{2} + 2i\sqrt{2})$. This point is defined over $\mathbf{Q}(\zeta_8)$ and we have $S'_E = S_E \cup \{P^\sigma\}_\sigma$. We can check that $\mathcal{F}_{S'_E}/\mathbf{Q}^\times$ is generated by $x, x \pm 2$ and $x^2 + 4$, hence it cannot generate $\mathbf{Q}(E)$. However, if we base change to the field $\mathbf{Q}(\sqrt{2})$, then we find that the function $v = y - \sqrt{2}x + 2\sqrt{2}$ is supported in S'_E and has degree 3. Hence $E/\mathbf{Q}(\sqrt{2})$ can be parametrized by the modular units $u = x$ and v .

Example 10 suggests the following question : which elliptic curves E/\mathbf{Q} of conductor N can be parametrized by modular units *defined over* $\mathbf{Q}(\zeta_N)$? The argument in Section 1, which is of geometrical nature, shows that S'_E is empty if N is sufficiently large; however, it crucially uses the fact that the modular parametrization $X_1(N) \rightarrow E$ is defined over \mathbf{Q} .

Finally, here are several questions to which I don't know the answer.

Question 11. — Let E/\mathbf{Q} be an elliptic curve of conductor N . Assume E can be parametrized by modular units of some level N' (not necessarily equal to N). Then we have a non-constant morphism $X_1(N') \rightarrow E$ and N must divide N' . Does it necessarily follow that E admits a parametrization by modular units of level N ? In other words, does it make a difference if we

allow modular units of arbitrary level in Definition 1? Similarly, does it make a difference if we replace $Y_1(N)$ by $Y(N)$ or $Y(N')$ in Definition 1?

Question 12. — Does it make a difference if we allow the function field of E to be generated by more than two modular units in Definition 1?

Question 13. — What about elliptic curves over \mathbf{C} ? It is not hard to show that if E/\mathbf{C} can be parametrized by modular functions, then E must be defined over $\overline{\mathbf{Q}}$. In fact, by the proof of Serre’s conjecture due to Khare and Wintenberger, it is known that the elliptic curves over $\overline{\mathbf{Q}}$ which can be parametrized by modular functions are precisely the \mathbf{Q} -curves [7]. Which \mathbf{Q} -curves can be parametrized by modular units?

Question 14. — It is conjectured in [1] that only finitely many smooth projective curves over \mathbf{Q} of given genus $g \geq 2$ can be parametrized by modular functions. Is it possible to prove, at least, that only finitely many smooth projective curves over \mathbf{Q} of given genus $g \geq 2$ can be parametrized by modular units?

Question 15. — According to [1], there are exactly 213 curves of genus 2 over \mathbf{Q} which are new and modular, and they can be explicitly listed. Which of them can be parametrized by modular units?

Question 16. — Let u and v be two multiplicatively independent modular units on $Y_1(N)$. Assume that u and v do not come from modular units of lower level. Can we find a lower bound for the genus of the function field generated by u and v ?

References

- [1] M. H. BAKER, E. GONZÁLEZ-JIMÉNEZ, J. GONZÁLEZ & B. POONEN – “Finiteness results for modular curves of genus at least 2”, *Amer. J. Math.* **127** (2005), no. 6, p. 1325–1387.
- [2] W. BOSMA, J. CANNON & C. PLAYOUST – “The Magma algebra system. I. The user language”, *J. Symbolic Comput.* **24** (1997), no. 3-4, p. 235–265, Computational algebra and number theory (London, 1993).
- [3] D. W. BOYD – “Mahler’s measure and special values of L -functions”, *Experiment. Math.* **7** (1998), no. 1, p. 37–82.
- [4] F. BRUNAUT – “On the ramification of modular parametrizations at the cusps”, Preprint, <http://arxiv.org/abs/1206.2621>, 2012.
- [5] J. E. CREMONA – *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.
- [6] C. DENINGER – “Deligne periods of mixed motives, K -theory and the entropy of certain \mathbf{Z}^n -actions”, *J. Amer. Math. Soc.* **10** (1997), no. 2, p. 259–281.
- [7] K. A. RIBET – “Abelian varieties over \mathbf{Q} and modular forms”, in *Modular curves and abelian varieties*, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, p. 241–261.
- [8] G. SHIMURA – *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kano Memorial Lectures, 1.
- [9] G. STEVENS – “Stickelberger elements and modular parametrizations of elliptic curves”, *Invent. Math.* **98** (1989), no. 1, p. 75–106.
- [10] The PARI Group – Bordeaux, *PARI/GP version 2.7.3*, 2015, available from <http://pari.math.u-bordeaux.fr/>.
- [11] M. WATKINS – “Explicit lower bounds on the modular degree of an elliptic curve”, Preprint, <http://arxiv.org/abs/math/0408126>, 2004.
- [12] W. ZUDILIN – “Regulator of modular units and Mahler measures”, *Math. Proc. Cambridge Philos. Soc.* **156** (2014), no. 2, p. 313–326.

F. BRUNAUT, ÉNS Lyon, UMPA, 46 allée d'Italie, 69007 Lyon, France

E-mail : francois.brunault@ens-lyon.fr • *Url* : <http://perso.ens-lyon.fr/francois.brunault>