Jacobians of Genus-2 Curves with a Rational Point of Order 11

Nicolas Bernard, Franck Leprévost, and Michael Pohst

CONTENTS

2000 AMS Subject Classification: Primary 11Y40, 11G30, 14H40, 14Q05

Keywords: Genus-2 curves, torsion, modular curves, Jacobians, rational point of order 11

On the one hand, it is well known that Jacobians of (hyper)elliptic curves defined over $\mathbb{Q}$ having a rational point of order l can be used in many applications, for instance in the construction of class groups of quadratic fields with a nontrivial l-rank. On the other hand, it is also well known that 11 is the least prime number that is not the order of a rational point of an elliptic curve defined over $\mathbb{Q}$. It is therefore interesting to look for curves of higher genus whose Jacobians have a rational point of order 11. This problem has already been addressed, and Flynn found such a family $\mathfrak{F}_t$ of genus-2 curves. Now it turns out that the Jacobian $J_0(23)$ of the modular genus-2 curve $X_0(23)$ has the required property, but does not belong to $\mathfrak{F}_t$. The study of $X_0(23)$ leads to a method giving a partial solution of the considered problem. Our approach allows us to recover $X_0(23)$ and to construct another 18 distinct explicit curves of genus 2 defined over $\mathbb{Q}$ whose Jacobians have a rational point of order 11. Of these 19 curves, 10 do not have any rational Weierstrass point, and 9 have a rational Weierstrass point. None of these curves are $\overline{\mathbb{Q}}$-isomorphic to each other, nor $\overline{\mathbb{Q}}$-isomorphic to an element of Flynn's family $\mathfrak{F}_t$. Finally, the Jacobians of these new curves are absolutely simple.

1. INTRODUCTION

Elliptic curves defined over $\mathbb{Q}$ or Jacobians of hyperelliptic curves defined over $\mathbb{Q}$ with a rational point of order l are of substantial interest. For example, they can be used to construct quadratic fields $K/\mathbb{Q}$ with class groups $\mathrm{cl}(K/\mathbb{Q})$ of l-rank ≥ 1, sometimes significantly greater than 1.

According to Cohen–Lenstra's heuristics, this is quite rare. A general result due to Mordell–Weil states that given a g-dimensional abelian variety A over $\mathbb{Q}$, then $A(\mathbb{Q})$ is an abelian group of finite type. For $g = 1$ the situation is completely described by a result of Mazur [Mazur 77] that the torsion group of an elliptic curve defined over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 10$ or $n = 12$, or to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ for $1 \leq n \leq 4$.

Currently, there is no similar complete description of the possible torsion groups of abelian varieties of dimension $g \geq 2$, even under the assumption that the abelian varieties under consideration are Jacobians of (hyperelliptic) curves of genus $g \geq 2$. In particular, one does not have a complete list of the finite groups that arise as torsion groups of Jacobians of curves of genus $g = 2$.

Mazur's result implies that 11 is the least prime number that is not the order of a rational point of an elliptic curve defined over $\mathbb{Q}$. However, $\mathbb{Z}/11\mathbb{Z}$ turns out to be the subgroup of the rational points of the Jacobian of the genus-2 modular curve $X_0(23)$. It is therefore of interest to search for curves of genus $g = 2$ whose Jacobians have a rational point of order 11.

In this work we try to generalize the modular curve $X_0(23)$ in the following sense: we look for a family of genus-2 curves defined over $\mathbb{Q}$ whose Jacobians have a rational point of order 11 for which a specialization leads to the recovery of $X_0(23)$. Although this search was negative, we did find some new curves with the desired properties. In this article we describe our strategy and list the new results. Those results support our conjecture that such a family exists.

In Section 2, we briefly recall some useful concepts and tools related to Jacobians of hyperelliptic curves.

In Section 3, we illustrate these concepts with Flynn's explicit family of curves $\mathfrak{F}_t$ defined over $\mathbb{Q}$ whose Jacobians have a rational point of order 11 (see [Flynn 90]).

In Section 4, we discuss the Jacobian $J_0(23)$ of the modular genus-2 curve $X_0(23)$ with a rational point of order 11 that actually comes from its two rational cusps (see [Ogg 73]). It turns out that $X_0(23)$ does not belong to the family $\mathfrak{F}_t$. Beginning with this example, we develop a more general method for constructing genus-2 curves defined over $\mathbb{Q}$ whose Jacobians have a rational point of order 11.

As explained in the final section, this approach allows us to recover $X_0(23)$ and to construct nine new explicit curves of genus 2 defined over $\mathbb{Q}$ without any rational Weierstrass point and whose Jacobians have a rational point of order 11. Additionally, we find nine other genus-2 curves defined over $\mathbb{Q}$ having a rational Weierstrass point and whose Jacobians have a rational point of order 11.

This information is important because one can use simpler defining equations for hyperelliptic curves having a rational Weierstrass point. The Jacobians of all these new curves are absolutely simple, and these curves are neither $\overline{\mathbb{Q}}$-isomorphic to each other nor $\overline{\mathbb{Q}}$-isomorphic to an element of Flynn's family $\mathfrak{F}_t$.

2. BACKGROUND

Let us briefly recall some well-known facts about the arithmetic of Jacobians of hyperelliptic curves that will be useful in the subsequent sections.

Let C be a hyperelliptic curve of genus $g \geq 1$ defined over a field K of characteristic $\neq 2, 3$ (see, for example, [Silverman 92] for most of this section). Such a curve can be defined by an equation

$$y^2 = f(x),$$

where $f(x) \in K[x]$ is a priori of degree $2g + 2$ without multiple roots. If the leading coefficient of $f(x)$ is a square, then C admits two rational points $+\infty$ and $-\infty$.

If f has a rational root, then C admits a so-called rational Weierstrass point. Hence f can be defined by an equation of the form $y^2 = \tilde{f}(x)$, where $\tilde{f}(x) \in K[x]$ is monic, separable, and of degree $2g + 1$. In this second case, the curve has a unique point at ∞, which is rational.

A divisor of C is given by a formal sum

$$D = \sum_{i \in \mathbb{N}} n_i [P_i],$$

where $n_i \in \mathbb{Z}$, $n_i = 0$ for almost all values i, and $P_i \in C(\overline{K})$. The quantity $\sum_{i \in \mathbb{N}} n_i$ defines the degree of the divisor D. A divisor D is rational if $D^\sigma = D$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$, where D^σ is defined by $D^\sigma = \sum_{i \in \mathbb{N}} n_i [P_i^\sigma]$.

As an example, one can associate to each function $\varphi(x, y)$ on the curve a divisor $(\varphi) = (\varphi)_0 - (\varphi)_\infty$ given by the divisor obtained by the zeros minus the poles of φ. Computations show (see, for example, [Silverman 92, Proposition 3.1]) that the degree of the divisor of a function is equal to 0.

The set $\mathrm{Div}_0(C)$ of the divisors of degree 0 on the curve C forms a group, and the set of the divisors of the functions forms a subgroup of it. One defines the Jacobian of the curve C as the quotient

$$\mathrm{Jac}(C) = \mathrm{Div}_0(C)/\{(\varphi),\ \varphi \text{ a function on } C\},$$

and $\mathrm{Jac}(C)(K)$ as the group of rational points of the Jacobian of C, obtained as classes of the rational divisors of degree 0.

If K is a number field, then the theorem of Mordell–Weil mentioned in Section 1 states that $\mathrm{Jac}(C)(K)$ is an abelian group of finite type. Let l be a prime such that there is a rational divisor $D = (P) - (Q)$, with $P, Q \in C(K)$, and $l[D] = 0 \in \mathrm{Jac}(C)(K)$. Then the order of $[D]$ is exactly l. Indeed, otherwise, C would be isomorphic to $\mathbb{P}^1$, and hence of genus 0, which is excluded.

One important issue is to distinguish curves that are actually $\overline{K}$-isomorphic to each other. One has a complete answer to this question in the situation of genus $g = 1, 2$, as explained below.

In the genus-1 case, i.e., if E is an elliptic curve defined over K by the equation

$$y^2 = x^3 + ax + b,$$

then the j-invariant of E is defined as

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

It turns out that two elliptic curves E and $\tilde{E}$ defined over K are $\overline{K}$-isomorphic if and only if $j(E) = j(\tilde{E})$.

In the genus-2 case, the Igusa invariants α, β, γ play a similar role (see [Igusa 60]). More precisely, two genus-2 curves C and $\tilde{C}$ defined over K are $\overline{K}$-isomorphic if and only if $\alpha(C) = \alpha(\tilde{C})$, $\beta(C) = \beta(\tilde{C})$, and $\gamma(C) = \gamma(\tilde{C})$. These invariants are elements of K. Although their equations can be explicitly computed, they are quite complicated and are therefore not reproduced here.

A final important issue is to check whether the Jacobian of a genus-2 curve C defined over K by an equation $y^2 = f(x)$ is absolutely simple or whether it is isogenous, over an extension of K, to the product of two elliptic curves. We use here an explicit criterion in the case $K = \mathbb{Q}$ (see [Leprévost 95]). Let us consider a model of C such that $f(x) \in \mathbb{Z}[x]$, p is a prime that does not divide the discriminant of $f(x)$, and $N_1 = \#C(\mathbf{F}_p)$, $N_2 = \#C(\mathbf{F}_{p^2})$. Let

$$\begin{aligned} G_f(z) = z^4 &+ (N_1 - p - 1)z^3 \\ &+ \left(\frac{N_1^2 + N_2}{2} - N_1(p+1) + p\right) z^2 \\ &+ p(N_1 - p - 1)z + p^2. \end{aligned}$$

If $\mathrm{Gal}(G_f) \simeq D_4$, where D_4 denotes the dihedral group with eight elements, then the Jacobian of C is absolutely simple.

3. FLYNN'S FAMILY OF CURVES $\mathfrak{F}_t$

We illustrate the previous section with a particular family of curves. In [Flynn 90] (see also [Flynn 91]), Flynn obtained the family of genus-2 curves $\mathfrak{F}_t$,

$$y^2 = x^6 + 2x^5 + (2t+3)x^4 + 2x^3 + (t^2+1)x^2 + 2t(1-t)x + t^2,$$

whose Jacobians have a rational point of order 11. This point is given by the class of the divisor

$$D_\infty = (+\infty) - (-\infty).$$

The curves $\mathfrak{F}_t$ define a family of curves, because the first Igusa invariant is

$$\alpha(\mathfrak{F}_t) = \frac{16t^6 + 448t^5 + 944t^4 - 1120t^3 + 640t^2 - 120t + 9}{16(4t^3 + 56t^2 - 16t + 3)^2} \notin K,$$

supplementing Flynn's paper [Flynn 91]. For later reference, let us also compute the third Igusa invariant of $\mathfrak{F}_t$:

$$\gamma(\mathfrak{F}_t) = \frac{t^7(16t^3 + 432t^2 - 104t + 9)}{8(4t^3 + 56t^2 - 16t + 3)^5}.$$

Finally, the Jacobians of these curves are generically absolutely simple. Indeed, the specialization $t = 1$ leads to

$$\mathrm{Gal}(G_{\mathfrak{F}_1}(z)) \simeq D_4,$$

and the criterion stated in the previous section applies.

4. THE GENUS-2 CURVE $X_0(23)$

Let $\mathfrak{H} = \{z = x + iy \in \mathbb{C} \mid x, y \in \mathbb{R},\ y > 0\}$ be Poincaré's upper half-plane. The group

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

acts on $\mathfrak{H}$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$

Let $N \geq 1$ be an integer, and

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod N \right\}.$$

The subgroup $\Gamma_0(N)$ acts on $\mathfrak{H}$ as well, and one denotes by $X_0(N)$ the Riemann compact surface obtained by adding the cusps (arising from the extended action of $\Gamma_0(N)$ on $\mathbb{Q} \cup \{i\infty\}$) to the variety $\Gamma_0(N) \setminus \mathfrak{H}$:

$$X_0(N)(\mathbb{C}) = \widehat{\Gamma_0(N) \setminus \mathfrak{H}}.$$

These curves can be defined by equations over $\mathbb{Q}$. They classify pairs (E, E') of generalized elliptic curves together with a cyclic isogeny $E \longrightarrow E'$ of degree N.

Let $J_0(N)$ be the Jacobian of $X_0(N)$, and suppose now that N is an odd prime number. A result due to Ogg [Ogg 73] asserts that $J_0(N)_{\mathrm{tors}}(\mathbb{Q})$ is generated by the class of the divisor $(0) - (\infty)$, where 0 and ∞ are the two rational cusps, and that the order of this group is

equal to $l = \frac{N-1}{\gcd(N-1,12)}$. More precisely, for $\tau \in \mathfrak{H}$, one defines the functions

$$\Delta(\tau) = q\prod_{i\geq 1}(1-q^i)^{24},$$
$$\Delta_N(\tau) = \Delta(N\tau) = q^N\prod_{i\geq 1}(1-q^{iN})^{24},$$

$q = \exp(2i\pi\tau)$. Then the function

$$\varphi_N = \left(\frac{\Delta}{\Delta_N}\right)^{1/\gcd(N-1,12)}$$

is a modular form of $\Gamma_0(N)$, whose divisor is precisely $l\,((0)-(\infty))$.

Let us consider the particular case $N = 23$. An equation (see [Rovira 91]) of $X_0(23)$ is

$$\begin{aligned} y^2 &= x^6 - 8x^5 + 2x^4 + 2x^3 - 11x^2 + 10x - 7 \\ &= (x^3 - x + 1)(x^3 - 8x^2 + 3x - 7). \end{aligned}$$

Ogg's result shows that the divisor $(+\infty) - (-\infty)$ defines a point of $J_0(23)(\mathbb{Q})$ of order 11. Note that another defining equation for $X_0(23)$ is

$$\begin{aligned} y^2 = &\left(x^3 - x^2 - \frac{x}{13} - \frac{191}{2197}\right)^2 \\ &- 4\left(\frac{8}{13}\right)^2\left(x^2 + \frac{15}{169}\right)^2. \end{aligned}$$

These observations are the starting point of the following method for constructing genus-2 curves defined over $\mathbb{Q}$ whose Jacobians have a rational point of order 11.

5. OUR METHOD

We intend to calculate new genus-2 curves defined over $\mathbb{Q}$ whose Jacobians have a rational point of order 11. (In that sense they generalize the modular curve $X_0(23)$.) The observations made within the previous section, especially at the end, lead us to the following approach. Let K be a field of characteristic 0, and for $a, b, c, d \in K$, let $R = x^3 - x^2 + ax + b$ and $S = x^2 + d$ be such that the curve $C_{a,b,c,d}$ defined by

$$y^2 = F(x) = R^2(x) - 4c^2S^2(x)$$

is of genus 2 (see also [Leprévost et al. 04] for a slightly different approach). Let $\delta = \sqrt{-d} \in \overline{K}$ and $\overline{\delta} = -\delta$. Then $S(x) = (x-\delta)(x-\overline{\delta})$. Let $P_\delta = (\delta, R(\delta))$ and $P_{\overline{\delta}} = (\overline{\delta}, R(\overline{\delta}))$. Let us consider the rational divisors

$$D_\delta = (P_\delta) + (P_{\overline{\delta}}) - (+\infty) - (-\infty)$$

and

$$D_\infty = (+\infty) - (-\infty).$$

Computations show that the divisor of the function $\varphi(x, y) = y - R(x)$ is

$$(\varphi) = 2D_\delta + D_\infty.$$

Suppose now that there exists a rational function $\psi(x, y) = yU(x) - V(x)$ such that its divisor is

$$(\psi) = D_\delta - 5D_\infty.$$

Then one has

$$\left(\frac{\varphi}{\psi^2}\right) = 11D_\infty.$$

This establishes that the class of the rational divisor D_∞ defines a rational point of the Jacobian of $C_{a,b,c,d}$ of order dividing 11, hence exactly 11 (see Section 2).

The function $\psi(x, y)$ we are looking for belongs to the linear space

$$\begin{aligned} \mathfrak{L}(6(+\infty)) &\subset \mathfrak{L}(6((+\infty)+(-\infty))) \\ &= \left\langle \left\{ 1, x, x^2, x^3, x^4, x^5, x^6, y, xy, x^2y, x^3y \right\} \right\rangle. \end{aligned}$$

This leads to $\psi(x, y) = yU(x) - V(x)$, where U and V are the following monic polynomials:

$$U(x) = x^3 + u_2x^2 + u_1x + u_0$$

and

$$V(x) = x^6 + v_5x^5 + v_4x^4 + v_3x^3 + v_2x^2 + v_1x + v_0.$$

The condition on the zeros of $\psi(x, y)$ now leads to the equation

$$F(x)U^2(x) - V^2(x) - tS(x) = 0, \quad t \in K^*.$$

A priori, the left-hand side of the preceding equation is a polynomial

$$G(x) = \sum_{i=0}^{11} t_ix^i$$

of degree 11. One chooses the values $(u_i)_{0\leq i\leq 2}$, $(v_j)_{0\leq j\leq 5}$, and t such that (after clearing the denominators)

$$G(x) = t_1(a, b, c, d)x + t_0(a, b, c, d) \in K[a, b, c, d][x].$$

Finally, we need to determine appropriate a, b, c, d such that t_0 and t_1 vanish simultaneously. This amounts to finding zeros of the resultant of t_1 and t_0 with respect to b because b is the variable arising with the lowest degree in t_0 and t_1. This resultant admits a factorization,

i	a	b	c	d	$\alpha(C_i)$	$\gamma(C_i)$
1	$-101/48$	$-61/48$	$1/4$	$-5/12$	$\frac{7\cdot11\cdot13\cdot46573841}{2^4\cdot193147^2}$	$-\frac{2^9\cdot3^{19}\cdot7^2\cdot73\cdot109}{193147^5}$
2	$473/147$	$-4013/343$	$6/7$	$207/49$	$\frac{7\cdot547\cdot76169029}{2^4\cdot231269^2}$	$-\frac{2^{21}\cdot3^{21}\cdot7^2\cdot11\cdot29}{231269^5}$
3	$8/49$	$-134/49$	$3/7$	$47/49$	$\frac{10106939\cdot41843}{2^4\cdot571212^3}$	$-\frac{2^{32}\cdot3^{12}\cdot139\cdot521}{571223^5}$
4	$1159/81$	$261607/2187$	$40/9$	$13/27$	$\frac{8689\cdot272630161267}{2^4\cdot3\cdot181^2\cdot294013^2}$	$-\frac{2^{11}\cdot5^8\cdot43\cdot67\cdot73\cdot631187^2\cdot24095051\cdot2083}{3^6\cdot11\cdot181^5\cdot294013^5}$
5	$-1/13$	$-191/2197$	$8/13$	$15/169$	$\frac{409^2}{2^4\cdot11^2\cdot13^2}$	$-\frac{23^6}{2^3\cdot11^5\cdot13^5}$
6	$-28/169$	$103/2197$	$3/13$	$-4/169$	$\frac{233^2\cdot593^2}{2^4\cdot181^2\cdot829^2}$	$\frac{3^{12}\cdot11^6\cdot43^2}{2^3\cdot181^5\cdot829^5}$
7	$594/1805$	$13348/34295$	$8/19$	$-64/361$	$\frac{97\cdot131\cdot761122823\cdot212621}{2^4\cdot920017471^2}$	$-\frac{2^{17}\cdot3^{14}\cdot5^7\cdot11^6\cdot29\cdot307\cdot967}{920017471^5}$
8	$208/867$	$1338/4913$	$5/17$	$-39/289$	$\frac{66150707372809}{2^4\cdot7^2\cdot11^2\cdot29^2\cdot37^2\cdot193^2}$	$-\frac{2^7\cdot3^7\cdot5^{14}\cdot53\cdot2729}{7^5\cdot11^5\cdot29^5\cdot37^5\cdot193^5}$
9	$415/1089$	$-2207/1089$	$8/33$	$119/121$	$\frac{139\cdot84737\cdot89641667}{2^4\cdot347^2\cdot86293^2}$	$-\frac{2^{14}\cdot3^{17}\cdot5^{13}\cdot17\cdot103\cdot389}{347^5\cdot86293^5}$
10	$4989/2500$	$-13599/12500$	$27/50$	$-81/250$	$\frac{4339\cdot9995849\cdot47460779}{2^4\cdot7^2\cdot264104339^2}$	$-\frac{2^7\cdot3^{17}\cdot5^6\cdot13^{17}\cdot71\cdot701}{7^4\cdot264104339^5}$
j	a	b	c	d	$\alpha(\tilde{C}_j)$	$\gamma(\tilde{C}_j)$
1	-3	59	4	-7	$\frac{148023553}{2^4\cdot3^2\cdot3797^2}$	$\frac{2^7\cdot11\cdot89\cdot1061^2\cdot3529}{3^7\cdot3797^5}$
2	$-163/1215$	$-367/3645$	$2/3$	$13/243$	$-\frac{109\cdot2207\cdot5557}{2^4\cdot39113^2}$	$\frac{2^{12}\cdot3^{13}\cdot5^7\cdot7\cdot139}{39113^5}$
3	$-13/18$	$71/6$	$5/3$	$-13/3$	$\frac{653\cdot3431783}{2^4\cdot7^2\cdot36599^2}$	$-\frac{3^6\cdot5^{12}\cdot743}{2^2\cdot7^5\cdot36599^5}$
4	$-2287/27$	$-1171/9$	$10/3$	$-323/3$	$\frac{13\cdot51004311730341481}{2^6\cdot5^2\cdot7^2\cdot12592\cdot9649^2}$	$\frac{3^7\cdot29\cdot67^2\cdot313\cdot107183\cdot82457\cdot16259101^2\cdot16067}{2^{14}\cdot5^2\cdot7^5\cdot12595\cdot9649^5}$
5	$121/147$	$-141/343$	$2/7$	$15/49$	$\frac{2543}{2^7\cdot7^2}$	$\frac{3^7\cdot53}{2^{21}\cdot7^5}$
6	$-13/18$	$71/6$	$15/9$	$-13/3$	$\frac{653\cdot3431783}{2^4\cdot7^2\cdot36599^2}$	$-\frac{3^6\cdot5^{12}\cdot743}{2^7\cdot7^5\cdot36599^5}$
7	$-1494/847$	$19480/9317$	$2/11$	$-256/121$	$\frac{31\cdot127\cdot5189\cdot357293}{2^4\cdot1505167^2}$	$-\frac{2^9\cdot3^15\cdot5^6\cdot7^7\cdot11\cdot6911}{1505167^5}$
8	$125/121$	$-223/1331$	$6/11$	$29/121$	$\frac{151^2\cdot2521}{2^4\cdot11^2\cdot6269^2}$	$\frac{2^{13}\cdot3^{12}\cdot5^6\cdot7^2\cdot113}{11^5\cdot6569^5}$
9	$187/361$	$-649/6859$	$6/19$	$23/361$	$\frac{63067}{2^6\cdot199^2}$	$\frac{3^{14}\cdot7\cdot19}{2^{14}\cdot199^5}$

TABLE 1. Results.

and we calculate explicitly the factor $\mathrm{Res}(a,c,d)$ of this resultant, which vanishes at the values a,c,d corresponding to the modular curve $X_0(23)$:

$$\mathrm{Res}(a,c,d) = A_{28}(c^2,d)a^{28} + \cdots + A_1(c^2,d)a + A_0(c^2,d),$$

with $A_{28}(c^2,d) = d+9$ and for $0 \le i \le 27$, $A_i(c^2,d) \in \mathbb{Z}[c,d]$ of degree $29-i$ in c^2 and in d.

The strategy is to find suitable values a,c,d with

$$\mathrm{Res}(a,c,d) = 0.$$

For those triples (a,c,d) we deduce the value b for which $t_0(a,b,c,d)$ and $t_1(a,b,c,d)$ vanish simultaneously. Then we check whether the genus of $C_{a,b,c,d}$ is still 2.

Note that $\mathrm{Res}(a,c,d)$ satisfies the following properties:

$$\mathrm{Res}(c^2+1,c,0) = \mathrm{Res}(c^2-1,c,-1) = 0,$$

so that one can write

$$\begin{aligned}\mathrm{Res}(a,c,d) = {} & (d+1)(a-1-c^2)M(a,c,d) \\ & - d(a+1-c^2)N(a,c,d)\end{aligned}$$

with explicit polynomials $M, N \in K[a,c,d]$. In principle, one should be able to use this remark for calculating a family of genus-2 curves defined over $\mathbb{Q}$ whose Jacobians have a rational point of order 11. Our efforts in this direction have yet to be successful.

6. RESULTS

The parameters a,b,c,d are chosen as follows:

1. We set $c = \frac{c_1}{c_2}$ with c_1, c_2 integers such that $0 < c_1, c_2 \le 50$ and $\gcd(c_1,c_2) = 1$.
2. We set $d = \frac{d_1}{d_2}$ with relatively prime integers d_1, d_2 subject to the conditions $-B \le d_1 \le B$, $1 \le d_2 \le B$ for $B = 400$.

3. For fixed values c and d we obtain a from those resultants $\mathrm{Res}(a, c, d)$ admitting a linear factor $aa_2 - a_1$ with $a, a_1, a_2 \in \mathbb{Z}$.

4. The value b is then deduced as described above.

We store the values $b \in \mathbb{Q}$ for which $C_{a,b,c,d}$ is a genus-2 curve.

Table 1 contains the parameters a, b, c, d that lead to 19 genus-2 curves $C_{a,b,c,d}$ whose Jacobians have a rational point of order 11. The first 10 curves, which we denote by C_i, do not have a Weierstrass rational point. The last 9 curves, denoted by $\tilde{C}_j$, have a rational Weierstrass point.

Note that C_5 coincides with $X_0(23)$. Table 1 also contains the first and third Igusa invariants $\alpha(C_i)$ and $\gamma(C_i)$ (respectively $\alpha(\tilde{C}_j)$ and $\gamma(\tilde{C}_j)$). It is obvious that the values $\alpha(C_i), \alpha(\tilde{C}_j)$ are distinct; hence the curves $C_i, \tilde{C}_j$ are not $\overline{\mathbb{Q}}$-isomorphic. Our computations also show that none of the C_i's and $\tilde{C}_j$'s belong to Flynn's family $\mathfrak{F}_t$.

Indeed, one can compute the two polynomials

$$I_{1,i}(t) = \mathrm{Numer}(\alpha(\mathfrak{F}_t) - \alpha(C_i)),$$
$$I_{2,i}(t) = \mathrm{Numer}(\gamma(\mathfrak{F}_t) - \gamma(C_i)),$$

where $\mathrm{Numer}(z)$ denotes the numerator of $z \in \mathbb{Q}(t)$. Then we verify that the resultant of $I_{1,i}$ and $I_{2,i}$ with respect to t is nonzero (mutatis mutandis with $\tilde{I}_{1,j}(t) = \mathrm{Numer}(\alpha(\mathfrak{F}_t) - \alpha(\tilde{C}_j))$ and $\tilde{I}_{2,j}(t) = \mathrm{Numer}(\gamma(\mathfrak{F}_t) - \gamma(\tilde{C}_j))$).

Finally, from the criterion of Section 2, computations show that the Jacobians of all the curves $(C_i)_{1\le i\le 10}$ and $(\tilde{C}_i)_{1\le i\le 9}$ are absolutely simple. It is likely that one can find other genus-2 curves with the required properties by enlarging the search box.

A perhaps more geometric way to present our results is to consider $\mathfrak{M}_2$, the moduli variety of the genus-2 curves. Flynn's family of curves $\mathfrak{F}_t$ is a line on $\mathfrak{M}_2$, and the curves $(C_i)_{1\le i\le 10}$, and $(\tilde{C}_j)_{1\le j\le 9}$ are distinct points on $\mathfrak{M}_2$ not belonging to the line $\mathfrak{F}_t$.

REFERENCES

[Flynn 90] E. V. Flynn. "Large Rational Torsion on Abelian Varieties." *J. Number Theory* 36 (1990), 257–265.

[Flynn 91] E. V. Flynn. "Sequences of Rational Torsions on Abelian Varieties." *Inventiones Math.* 106 (1991), 433–442.

[Igusa 60] J.-I. Igusa. "Arithmetic Variety of Moduli for Genus Two." *Annals of Math.* 72 (1960), 612–649.

[Leprévost 95] F. Leprévost. "Jacobiennes de certaines courbes de genre 2: torsion et simplicité." *J. Théorie des Nombres de Bordeaux* 7 (1995) 283–306.

[Leprévost et al. 04] F. Leprévost, M. Pohst, and A. Schöpp. "Rational Torsion of $J_0(N)$ for Hyperelliptic Modular Curves and Families of Jacobians of Genus 2 and Genus 3 Curves with a Rational Point of Order 5, 7 or 10." *Abh. Math. Sem. Univ. Hamburg* 74 (2004), 193–203.

[Mazur 77] B. Mazur. "Rational Points of Modular Curves." In *Modular Functions of One Variable V*, Lecture Notes in Math. 601, pp. 107–148. Berlin-Heidelberg: Springer, 1977.

[Ogg 73] A. P. Ogg. "Rational Points on Certain Elliptic Modular Curves." *Proc. Symp. Pure Math. A.M.S. Providence* 24 (1973), 221–231.

[Rovira 91] J. G. Rovira. "Equations of Hyperelliptic Modular Curves." *Annales de l'Institut Fourier* 41 (1991), 779–795.

[Silverman 92] J. H. Silverman. *The Arithmetic of Elliptic Curves*, GTM in Mathematics 106. New York: Springer, 1992.

Nicolas Bernard, University of Luxembourg, LACS, 162 A, Avenue de la Faïencerie, L-1511 Luxembourg (nicolas.bernard@uni.lu)

Franck Leprévost, University of Luxembourg, LACS, 162 A, Avenue de la Faïencerie, L-1511 Luxembourg (franck.leprevost@uni.lu)

Michael Pohst, Technische Universität Berlin, Fakultät II, Institut für Mathematik-Sekr. MA 8-1, Strasse des 17. Juni 136, D-10623 Berlin (pohst@mail.math.tu-berlin.de)

Received February 27, 2008; accepted in revised form June 4, 2008.