*Article Submitted to Journal of Symbolic Computation*

# 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 $10$

Franck Leprévost[1], Michael Pohst[2] and Andreas Schöpp[3]

[1] *Université Joseph Fourier, UFR de Mathématiques, 100, rue des Maths - B.P. 74 - F-38402 St-Martin d'Hères Cedex, France, Franck.Leprevost@ujf-grenoble.fr*

[2] *Technische Universität Berlin, Fakultät II - Mathematik MA 8-1 - Straße des 17. Juni 136, D-10623 Berlin, Germany, pohst@math.tu-berlin.de*

[3] *Technische Universität Berlin, Fakultät II - Mathematik MA 8-1 - Straße des 17. Juni 136, D-10623 Berlin, Germany, schoepp@math.tu-berlin.de*

**Abstract**

We describe a method for constructing Jacobians of hyperelliptic curves of genus $g \geq 2$, defined over a number field, with a rational point of order some (well-chosen) integer $l \geq g+1$; it is based on a polynomial identity. We show that all hyperelliptic modular curves $X_0(N)$ with $N$ a prime number fit into this strategy, except for $N = 37$ in which case we give another explanation. Using this approach we construct new families of genus 2 curves defined over $\mathbb{Q}$, which contain the modular curves $X_0(31)$ (and $X_0(22)$ as a by-product) and $X_0(29)$, the Jacobians of which having a rational point of order 5 and 7 respectively. We also construct a new family of hyperelliptic genus 3 curves defined over $\mathbb{Q}$, which contains the modular curve $X_0(41)$, the Jacobians of which having a rational point of order 10.

## 1. Introduction

Let $A$ be an abelian variety of dimension $g$ defined over a number field $K$. Thanks to the theorem of Mordell-Weil, the set $A(K)$ of $K$-rational points of $A$ turns out to be a finitely generated abelian group isomorphic to $\mathbb{Z}^r \oplus A(K)_{\text{tors}}$, where $A(K)_{\text{tors}}$ is the group of $K$-rational torsion points of $A$. It is interesting to have a complete description of the finite groups that occur as rational torsion groups of an abelian variety defined over a number field. To date, this description has been essentially achieved only in the case $g = 1$ and $K = \mathbb{Q}$ by Mazur [1977], (see also [Kubert, 1976]), and in the case $g = 1$ and $K$ a quadratic field by Kamienny [1986]. Moreover, in the case of elliptic curves ($g = 1$), Merel [1996] has proved the uniform boundedness conjecture, which asserts that, given an integer $d \geq 1$, there exists a bound $B(d)$ depending only on $d$, such that for any elliptic curve $E$ defined on a number field $K$ of degree $d$, the inequality Card $E(K)_{\text{tors}} \leq B(d)$ holds. The version of this conjecture for abelian varieties of dimension $g \geq 2$ is still open; the only known results in this direction are that some groups occur as rational torsion groups of (families of) Jacobians of hyperelliptic curves of genus $g \geq 2$ [Flynn, 1990, 1991; Leprévost, 1992, 1994, 1996, 1997].

In this article, for some integers $l, g$ such that $l \geq g + 1 \geq 2$, we explicit in section 2 an equation involving four monic polynomials $Q_1, Q_2, F_1$ and $F_2$, defined over a field $K$ of characteristic zero and whose degrees depend on $l$ and $g$. If this equation is satisfied, and if $F_1F_2$ has no multiple roots, we show that the Jacobian of the genus $g$ hyperelliptic curve of equation $y^2 = F_1(x)F_2(x)$ has a $K$-rational torsion point of order dividing $l$. We also provide a variant of this approach using a quadratic extension of the field $K$. These methods are different from those of [Leprévost, 1992, 1994, 1996, 1997]. In section 3, we focus on hyperelliptic modular curves $X_0(N)$ with $N$ a prime number ($N = 23, 29, 31, 37, 41, 47, 59, 71$). We recall that, in particular for those eight values of $N$, the $\mathbb{Q}$-rational torsion group of its Jacobian $J_0(N)$ is a cyclic group of order $l = \frac{N-1}{\gcd(N-1,12)}$. We show that these curves, except $X_0(37)$ for which there is another explanation, fit into the strategy described in section 2. Our intention in this article is to generalize some of these modular curves in the following sense. In sections $4, 5$ and $6$, we show that the polynomial equation previously mentioned has families of solutions in the case $g = 2$ and $l = 5$ or $l = 7$, or $g = 3$ and $l = 10$, and we construct families of genus $g$ hyperelliptic curves defined over $\mathbb{Q}$, whose Jacobians have a rational point of order $l$. These families are different from those obtained in [Boxall-Grant-Leprévost, 2001] in the case $g = 2$ and $l = 5$. We further recover the curves $X_0(22), X_0(29), X_0(31)$ and $X_0(41)$ as specialisations of these new families. The limitation of the method is essentially a computing power problem, and we were not able to push the computations further in order to construct a family going through the other modular curves studied in section 3. It would have been interesting, for instance, to construct a family of genus 2 curves defined over $\mathbb{Q}$, whose Jacobians have a rational point of order 11, and which contains the modular curve $X_0(23)$. Such a result would in particular be relevant to the problem of finding new examples of imaginary and real quadratic fields with a class group having an 11-rank $\geq 3$ and $\geq 2$ respectively. (For examples see [Leprévost, 1993].)

We made extensive use of the computer algebra systems KANT [2003], Magma [2003] and Maple [2003] for the computations done in this article.

*Aknowledgements:* The authors want to thank Josep González for useful discussions.

## 2. A polynomial equation related to torsion points of Jacobians of hyperelliptic curves

Let $K$ be a field of characteristic 0, $g$ and $l$ integers, such that $l \geq g+1 \geq 2$. We first prove the following theorem:

THEOREM 2.1: *Let $P, Q$ and $F$ be monic polynomials with coefficients in $K$, of degrees respectively $l$, $l-(g+1)$ and $2g+2$. Assume that $F$ has no multiple roots. Suppose that the following polynomial equation is satisfied:*

$$P^2(x) - Q^2(x)F(x) = \lambda \in K^*.$$

*Then the curve of equation $y^2 = F(x)$ is hyperelliptic of genus $g$, and its Jacobian has a $K$-rational point of order dividing $l$ and different from 1. In particular, if $l$ is prime, this point is exactly of order $l$.*

Note first that if the polynomial equation is satisfied, then $P$ and $Q$ have no common roots.

It is obvious that, if $F$ is of degree $2g+2$ without multiple roots, then the curve $C$ of equation $y^2 = F(x)$ is hyperelliptic and of genus $g$. Now, because $F$ is a monic polynomial, the points $+\infty$ and $-\infty$ are rational over $K$. (This is satisfied if the leading coefficient of $F$ is a square in $K$ as well. This latter case is not more general than supposing $F$ monic in the theorem.) It follows that the group $J(C)(K)$ of $K$-rational points of the Jacobian of $C$ contains the class of the rational divisor $D_\infty = (+\infty) - (-\infty)$. If the polynomial equation $P^2(x) - Q^2(x)F(x) = \lambda$ is satisfied for some $\lambda \in K^*$, it implies that the divisor of the function $\varphi(x,y) = P(x) - yQ(x)$ is $(\varphi) = lD_\infty$. This shows that the class of the $K$-rational divisor $D_\infty$ defines an element of $J(C)(K)$ of order dividing $l$. Furthermore, this point cannot be of order one, else $C$ would be birational to $\mathbb{P}^1$, and hence of genus 0, which is excluded ($g \geq 1$). This shows in particular, that if $l$ is a prime number, then the order of the point defined by the class of $D_\infty$ is equal to $l$.

The following theorem describes a method for the construction of polynomials $P, Q$ and $F$ satisfying the equation of Theorem 2.1. Its proof is straightforward.

THEOREM 2.2: *Let $Q_1, Q_2, F_1, F_2$ be four monic polynomials $\in K[x]$, of degrees $q_1, q_2, f_1, f_2$ respectively. Suppose that $2q_1 + f_1 = 2q_2 + f_2 = l$, that $f_1 + f_2 = 2g + 2$, and that these polynomials satisfy the following equation:*

$$Q_1^2(x)F_1(x) - Q_2^2(x)F_2(x) = 2t,$$

*for some $t \in K^*$. Then the polynomials $P(x) = Q_1^2(x)F_1(x) - t$, $Q(x) = Q_1(x)Q_2(x)$ and $F(x) = F_1(x)F_2(x)$ are of degrees $l$, $l-(g+1)$, and $2g+2$ respectively, and satisfy the following equation:*

$$P^2(x) - Q^2(x)F(x) = t^2 \in K^*.$$

Note further that $P$ and $Q$ have no common roots. If $F$ has no multiple roots, the conditions of Theorem 2.1 are satisfied, and the Jacobian of the genus $g$ hyperelliptic curve of equation $y^2 = F(x)$ has a $K$-rational point of order dividing $l$. The case where $l$ has the same parity as $g+1$, and $f_1 = f_2 = g+1$, where $q_1 = q_2 = \frac{l-(g+1)}{2}$ is of special interest.

The method described above has the following variant, whose proof is straightforward as well:

THEOREM 2.3: *Let $l \geq g+1 \geq 2$ be integers such that $l$ has the same parity as $g+1$. Let $d$ be an element of $K \setminus K^2$, and $Q_1$ and $F_1$ be two monic polynomials $\in K(\sqrt{d})[x]$, not defined over $K$, and of degrees $\frac{l-(g+1)}{2}$ and $g+1$ respectively. Let $\overline{Q_1}$ and $\overline{F_1}$ denote their conjugates with respect to $\sqrt{d} \longmapsto -\sqrt{d}$. Suppose that the following equation is satisfied:*

$$Q_1^2(x)F_1(x) - \overline{Q_1}^2(x)\overline{F_1}(x) = t - \overline{t} = 2u\sqrt{d},$$

*where $t = u\sqrt{d}$ for some $u \in K^*$. Then the polynomials $P(x) = Q_1^2(x)F_1(x) - t$, $Q(x) = Q_1(x)\overline{Q_1}(x)$, and $F(x) = F_1(x)\overline{F_1}(x)$ are elements of $K[x]$, of degrees $l$, $l-(g+1)$ and $2g+2$ respectively, and satisfy the following equation:*

$$P^2(x) - Q^2(x)F(x) = t^2 = u^2 d \in K^*.$$

## 3. Hyperelliptic modular curves $X_0(N)$ with $N$ prime

Let $N \geq 1$ be an integer. Then the group

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ c \equiv 0 \bmod N\}$$

acts on the upper half-plane $\mathfrak{H} = \{z \in \mathbb{C} \ : \ \mathrm{Im}(z) > 0\}$. Let $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{i\infty\}$. Then $X_0(N)$ is the modular curve defined over $\mathbb{Q}$ which corresponds to $\Gamma_0(N)$, *i.-e.* $X_0(N)(\mathbb{C}) \simeq \mathfrak{H}^*/\Gamma_0(N)$. These curves have a rational equation over $\mathbb{Q}$, and 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 $X_0(N)$.

If $N$ is prime, a now classical result due to Ogg [1973] asserts that $J_0(N)_{\mathrm{tors}}(\mathbb{Q})$ is generated by the class of the divisor $(0)-(\infty)$, where $0$ and $\infty$ 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

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

where $q = \exp(2i\pi\tau)$. Then the function $\varphi_N = (\frac{\Delta}{\Delta_N})^{\frac{1}{\gcd(N-1,12)}}$ is a modular form for $\Gamma_0(N)$, whose divisor is precisely $l((0)-(\infty))$.

On the other hand, Ogg [1974] has also determined the 19 values of $N$ for which $X_0(N)$ is hyperelliptic of genus $g \geq 2$.

We focus here on the case where both properties are satisfied, namely $N$ is a prime such that $X_0(N)$ is hyperelliptic of genus $g \geq 2$. The corresponding values for $N$ are $23, 29, 31, 37$ ($g = 2$), $41$ ($g = 3$), $47$ ($g = 4$), $59$ ($g = 5$), and $71$ ($g = 6$).

For all these values, except for $N = 37$, we recall in the following table the equations of $X_0(N)$ of the form $y^2 = f_N(x)$ obtained mainly from [Gonzàlez

Rovira, 1991] (see also [Hibino-Murabayashi, 1997] for other related questions). It turns out that, for the values $N$ considered in this table, $f_N(x)$ admits a factorisation

$$f_N(x) = F_{1,N}(x)F_{2,N}(x)$$

over $\mathbb{Q}$ or over a quadratic number field which is specified in the table. We show that these curves fit into the strategy described in section 2: there are explicit polynomials $Q_{1,N}$ and $Q_{2,N}$ in $\mathbb{Q}[x]$, such that an equation

$$Q_{1,N}^2 F_{1,N} - Q_{2,N}^2 F_{2,N} = 2t$$

is satisfied for some $t \in \mathbb{Q}^*$, or there is an explicit polynomial $Q_{1,N}$ defined over $\mathbb{Q}(\sqrt{d})$ for some $d \in \mathbb{Q} \setminus \mathbb{Q}^2$, such that an equation

$$Q_{1,N}^2 F_{1,N} - \overline{Q_{1,N}}^2 \overline{F_{1,N}} = t - \overline{t} = 2u\sqrt{d},$$

is satisfied for some $u \in \mathbb{Q}^*$. We provide in this table the equations for these polynomials and the values $2t$ or $t - \overline{t}$. In the latter case, we keep the notations $Q_{2,N} = \overline{Q_{1,N}}$, and $F_{2,N} = \overline{F_{1,N}}$. In other words, one can express the modular function $\varphi_N$ as a function of the polynomials $Q_1$ and $Q_2$.

The remaining case $N = 37$ is different. An equation of $X_0(37)$ is [Gonzàlez Rovira, 1991]:

$$y^2 = f_{37}(x) = x^6 - 4x^5 - 40x^4 + 348x^3 - 1072x^2 + 1532x - 860.$$

Computations show that the divisor of the function

$$2\varphi_{37} = y + A_3(x) = y + x^3 - 2x^2 - 22x + 56$$

is equal to

$$(\varphi_{37}) = 3((3,1) - (+\infty)).$$

Indeed, the following equation holds:

$$f_{37} - A_3^2 = 2^2 37(x-3)^3.$$

The cusp $(0)$ corresponds to the point $(3,1)$ on the equation of the curve, and the cusp $(\infty)$ to the point $+\infty$. The explanation of this different behaviour comes essentially from the fact that the hyperelliptic involution is not the Atkin-Lehner involution in the case $N = 37$ (see [Lehner-Newman, 1964]). Actually, Ogg has proved (see [Ogg, 1974], p. 450) that $N = 37$ is the only case where $X_0(N)$ is hyperelliptic and its hyperelliptic involution does not belong to the subgroup of $\mathrm{Aut}(X_0(N))$ defined by automorphisms of $\mathfrak{H}$.

| $g$ | $N$ | $l$ | $f_N(x) = F_{1,N}(x)F_{2,N}(x), Q_{1,N}(x), Q_{2,N}(x)$ and $Q_{1,N}^2 F_{1,N} - Q_{2,N}^2 F_{2,N}$ |
|---|---|---|---|
| 2 | 23 | 11 | $F_{1,23}(x) = x^3 - x + 1$<br>$F_{2,23}(x) = x^3 - 8x^2 + 3x - 7$<br>$Q_{1,23}(x) = x^4 - 17x^3 + 91x^2 - 143x - 40$<br>$Q_{2,23}(x) = x^4 - 13x^3 + 45x^2 - 9x - 82$<br>$Q_{1,23}^2 F_{1,23} - Q_{2,23}^2 F_{2,23} = 2^2 23^3$ |
| 2 | 29 | 7 | $F_{1,29}(x) = x^3 + (1+\sqrt{29})x^2 + (\frac{11+3\sqrt{29}}{2})x + 5 + \sqrt{29}$<br>$F_{2,29}(x) = x^3 + (1-\sqrt{29})x^2 + (\frac{11-3\sqrt{29}}{2})x + 5 - \sqrt{29}$<br>$Q_{1,29}(x) = x^2 - (\frac{7+\sqrt{29}}{2})x - (\frac{1-3\sqrt{29}}{2})$<br>$Q_{2,29}(x) = x^2 - (\frac{7-\sqrt{29}}{2})x - (\frac{1+3\sqrt{29}}{2})$<br>$Q_{1,29}^2 F_{1,29} - Q_{2,29}^2 F_{2,29} = 2^2 29\sqrt{29}$ |
| 2 | 31 | 5 | $F_{1,31}(x) = x^3 - 17x - 27$<br>$F_{2,31}(x) = x^3 + 4x^2 + 3x + 1$<br>$Q_{1,31}(x) = x - 2$<br>$Q_{2,31}(x) = x - 4$<br>$Q_{1,31}^2 F_{1,31} - Q_{2,31}^2 F_{2,31} = -2^2 31$ |
| 3 | 41 | 10 | $F_{1,41}(x) = x^4 + 2x^3 - (6-\sqrt{41})x^2 - (21 - 3\sqrt{41})x - (31 - \frac{5\sqrt{41}}{2})$<br>$F_{2,41}(x) = x^4 + 2x^3 - (6+\sqrt{41})x^2 - (21 + 3\sqrt{41})x - (31 + \frac{5\sqrt{41}}{2})$<br>$Q_{1,41}(x) = x^3 - 4x^2 - (\frac{5+\sqrt{41}}{2})x + \frac{29+3\sqrt{41}}{2}$<br>$Q_{2,41}(x) = x^3 - 4x^2 - (\frac{5-\sqrt{41}}{2})x + \frac{29-3\sqrt{41}}{2}$<br>$Q_{1,41}^2 F_{1,41} - Q_{2,41}^2 F_{2,41} = 2^2 41\sqrt{41}$ |
| 4 | 47 | 23 | $F_{1,47}(x) = x^5 - x^4 + x^3 + x^2 - 2x + 1$<br>$F_{2,47}(x) = x^5 - 5x^4 + 5x^3 - 15x^2 + 6x - 11$<br>$Q_{1,47}(x) = x^9 - 17x^8 + 112x^7 - 355x^6 + 546x^5$<br>$-388x^4 + 149x^3 + 292x^2 - 740x + 36$<br>$Q_{2,47}(x) = x^9 - 15x^8 + 84x^7 - 207x^6 + 172x^5$<br>$+120x^4 - 283x^3 + 266x^2 - 66x - 194$<br>$Q_{1,47}^2 F_{1,47} - Q_{2,47}^2 F_{2,47} = 2^2 47^3$ |
| 5 | 59 | 29 | $F_{1,59}(x) = x^3 + 2x^2 + 1$<br>$F_{2,59}(x) = x^9 + 2x^8 - 4x^7 - 21x^6 - 44x^5 - 60x^4 - 61x^3 - 46x^2$<br>$-24x - 11$<br>$Q_{1,59}(x) = x^{13} - 7x^{12} + 2x^{11} + 70x^{10} - 68x^9 - 276x^8 + 161x^7$<br>$+644x^6 + 210x^5 - 808x^4 - 727x^3 - 202x^2 + 332x + 720$<br>$Q_{2,59}(x) = x^{10} - 7x^9 + 4x^8 + 63x^7 - 99x^6 - 166x^5$<br>$+306x^4 + 183x^3 - 194x^2 - 312x + 166$<br>$Q_{1,59}^2 F_{1,59} - Q_{2,59}^2 F_{2,59} = 2^2 59^3$ |
| 6 | 71 | 35 | $F_{1,71}(x) = x^7 + 4x^6 + 5x^5 + x^4 - 3x^3 - 2x^2 + 1$<br>$F_{2,71}(x) = x^7 - 7x^5 - 11x^4 + 5x^3 + 18x^2 + 4x - 11$<br>$Q_{1,71}(x) = x^{14} - 8x^{13} + 7x^{12} + 82x^{11} - 132x^{10} - 414x^9 + 610x^8$<br>$+1533x^7 - 1366x^6 - 3829x^5 + 1313x^4 + 5207x^x + 338x^2$<br>$-3100x - 612$<br>$Q_{2,71}(x) = x^{14} - 6x^{13} - 5x^{12} + 76x^{11} - 8x^{10} - 408x^9 + 2x^8 + 1231x^7$<br>$+484x^6 - 2049x^5 - 1575x^4 + 1185x^3 + 1570x^2 + 500x - 310$<br>$Q_{1,71}^2 F_{1,71} - Q_{2,71}^2 F_{2,71} = 2^2 71^3$ |

In the next two sections, we focus on the case of genus 2 curves (which are automatically hyperelliptic) whose Jacobians have a rational point of prime order $l = 5$ or $l = 7$.

## 4. Two new families of genus 2 curves whose Jacobians have a rational point of order 5

Using the method described in the theorems of section 2, we construct here two new families of genus 2 curves defined over $\mathbb{Q}$, whose Jacobians have a rational point of order 5. With the notations of Theorem 2.2, the conditions $2q_1 + f_1 = 2q_2 + f_2 = 5$ and $f_1 + f_2 = 6$ imply that $(f_1, f_2) = (1, 5)$ or $(3, 3)$. We do not suppose here *a priori* that the genus 2 curve we are looking for has a rational Weierstrass point, because this case has been treated extensively in [Boxall-Grant-Leprévost, 2001]. As a consequence, we consider here $(f_1, f_2) = (3, 3)$ and $(q_1, q_2) = (1, 1)$. More precisely, we first show the following result:

THEOREM 4.1: *Let $a$ and $b$ be two parameters. The curve $C_{a,b,5}$ defined by the equation*

$$y^2 = (x^3 + (a-2)x^2 + (2b-2a+1)x + a - 3b)(x^3 + ax^2 + 2bx + b)$$

*is generically of genus 2 and its Jacobian has a $\mathbb{Q}(a, b)$-rational point of order 5. Furthermore, this family contains the modular curves $X_0(22)$ and $X_0(31)$.*

Let $Q_1 = x - u_1$ and $Q_2 = x - u_2$ be elements of $\mathbb{Q}[x]$, and let $F_1$ and $F_2$ be two monic polynomials of degree 3 defined over $\mathbb{Q}$. Suppose that these polynomials satisfy the equation

$$Q_1^2 F_1 - Q_2^2 F_2 = 2t \in \mathbb{Q}^*.$$

One may first suppose $u_1 = 0$ (change $x$ into $x + u_1$), and, because $u_2 \neq 0$ (otherwise $x^2$ would divide the left hand side of the previous equation, what is impossible), one may further suppose that $u_2 = 1$ (change $x$ into $u_2 x$). It is easy to check that the polynomials we are looking for are $F_1 = x^3 + (a-2)x^2 + (2b-2a+1)x + a - 3b$ and $F_2 = x^3 + ax^2 + 2bx + b$. They satisfy the equation:

$$x^2 F_1 - (x-1)^2 F_2 = -b.$$

One easily checks that the curve of equation $y^2 = F_1F_2$ defines generically a genus 2 curve over $\mathbb{Q}(a,b)$, whose Jacobian has a rational point of order 5, thanks to Theorems 2.1 and 2.2. The family $C_{a,b,5}$ contains the curve $X_0(31)$, which corresponds to the choice of the parameters $(a,b) = (5, \frac{31}{8})$. Finally, one shows that the genus 2 curve $X_0(22)$ (see [Gonzàlez Rovira, 1991] for an equation of this curve) corresponds to the choice of the parameters $(a,b) = (-\frac{7}{2}, \frac{11}{8})$.

Using Theorem 2.3, one can construct another family: *a priori* $Q_1 = x - (v + w\sqrt{d})$, but again, we can assume that $v = 0$ and $w = 1$ (since $w \neq 0$), so $Q_1 = x - \sqrt{d}$. The equation $Q_1^2F_1 - \overline{Q_1}^2\overline{F_1} = 2u\sqrt{d}$ for a non-zero $u$ yields

$$F_1 = (x^3 + ax^2 + bx + ad) + 2(x^2 + ax + b - d)\sqrt{d},$$

and with these notations

$$Q_1^2F_1 - \overline{Q_1}^2\overline{F_1} = 4d(b-d)\sqrt{d},$$

hence:

$$\begin{aligned} F(x) = F_1(x)\overline{F_1}(x) \quad = \quad & x^6 + 2ax^5 + (a^2 + 2b - 4d)x^4 - 2a(3d - b)x^3 \\ & +(b^2 + 8d^2 - 8bd - 2a^2d)x^2 + 2ad(4d - 3b)x \\ & -d(4b^2 + 4d^2 - 8bd - a^2d). \end{aligned}$$

There are now two cases to consider. First, if $a = 0$, then one finds the curve $C_{b,d,0,5}$ with equation

$$y^2 = x^6 + 2(b - 2d)x^4 + (8d^2 - 8db + b^2)x^2 - 4d(b-d)^2.$$

Obviously, its Jacobian is isogeneous to a product of elliptic curves. We do not further consider this family (see however [Howe-Leprévost-Poonen, 2000] for some results with split Jacobians).

Now, if $a \neq 0$, one can assume that $a = 1$ (change $x$ into $ax$, $b$ into $ba^2$, and $d$ into $da^2$), and one obtains the following result:

THEOREM 4.2: *Let $b$ be a parameter and $d$ an element of $\mathbb{Q}\backslash\mathbb{Q}^2$. The curve $C_{b,d,1,5}$ defined by the equation*

$$\begin{aligned} y^2 = \quad & x^6 + 2x^5 + (2b - 4d + 1)x^4 + 2(b - 3d)x^3 \\ & +(b^2 + 8d^2 - 8bd - 2d)x^2 - 2d(3b - 4d)x - d(4b^2 - 8bd + 4d^2 - d) \end{aligned}$$

*is generically of genus* 2 *and its Jacobian has a* $\mathbb{Q}(b,d)$*-rational point of order* 5.

The curves $C_{a,b,5}$ and $C_{b,d,1,5}$ define families of genus 2 curves in the sense that their Igusa invariants [Igusa, 1960] are non-constant, as one easily checks. As a consequence, the specialisation of the parameters in these families of curves provides infinitely many genus 2 curves defined over $\mathbb{Q}$, whose Jacobians have a $\mathbb{Q}$-rational point of order 5. Finally, one proves, with the techniques described in [Leprévost, 1995], that the Jacobians of these families are generically absolutely irreducible.

## 5. Two new families of genus 2 curves whose Jacobians have a rational point of order 7

Again, using the method described in the theorems of section 2, we construct here two new families of genus 2 curves defined over $\mathbb{Q}$, whose Jacobians have a rational point of order 7. With the notations of Theorem 2.2, the conditions $2q_1+f_1 = 2q_2+f_2 = 7$ and $f_1+f_2 = 6$ implies that $(f_1, f_2) = (1,5)$ or $(3,3)$. The first case corresponds to the situation where the genus 2 curve has a rational Weierstrass point. The methods of [Leprévost, 1991a] and [Leprévost, 1991b] would apply, and we prefer here to consider the latter case, where $(f_1, f_2) = (3,3)$ and $(q_1, q_2) = (2,2)$.

One first applies Theorems 2.1 and 2.2, and one may assume that $Q_1 = x^2 + q_0$ and $Q_2 = x^2 + x + p_0$. Let $D_0, a_2, a_1, a_0, b_2, b_1$ and $b_0$ be as follows:

$$
\begin{aligned}
D_0 &= 3\,{q_0}^2 - 6\,p_0\,q_0 + q_0 + 3\,{p_0}^2 - 2\,p_0,\\
2D_0a_2 &= 2\,{q_0}^3 - 6\,p_0\,{q_0}^2 + 9\,{q_0}^2 + 3\,q_0 + 6\,{p_0}^2 q_0 - 24\,p_0\,q_0 - 8\,p_0\\
&\quad +15\,{p_0}^2 - 2\,{p_0}^3,\\
D_0a_1 &= p_0\,(3\,{q_0}^2 - 6\,p_0\,q_0 + 2\,p_0 - 3\,q_0 - 2 + 3\,{p_0}^2)\,,\\
-2D_0a_0 &= {q_0}^4 + 3\,{q_0}^3 - 6\,p_0\,{q_0}^3 + 3\,{q_0}^2 - 12\,p_0\,{q_0}^2 + 12\,{p_0}^2{q_0}^2 + q_0\\
&\quad +21\,{p_0}^2 q_0 - 10\,{p_0}^3 q_0 - 6\,p_0\,q_0 + 5\,{p_0}^2 + 3\,{p_0}^4 - 12\,{p_0}^3,\\
2D_0b_2 &= 2\,{q_0}^3 - 6\,p_0\,{q_0}^2 - 3\,{q_0}^2 - q_0 + 6\,{p_0}^2 q_0 + 3\,{p_0}^2 - 2\,{p_0}^3,\\
D_0b_1 &= -9\,p_0\,{q_0}^2 + 6\,{p_0}^2 q_0 - 3\,p_0\,q_0 - {p_0}^3 + 4\,{q_0}^3 + 2\,{q_0}^2,\\
2D_0b_0 &= -2\,{q_0}^2 + 3\,{p_0}^2 q_0 - 3\,{q_0}^3 + 12\,{p_0}^2{q_0}^2 - 6\,{p_0}^3 q_0 - 10\,p_0\,{q_0}^3\\
&\quad +3\,{q_0}^4 + {p_0}^4.
\end{aligned}
$$

With these notations, one shows the following result:

THEOREM 5.1: *The equation* $y^2 = (x^3+a_2x^2+a_1x+a_0)(x^3+b_2x^2+b_1x+b_0)$ *defines generically a genus* 2 *curve* $C_{p_0,q_0,7}$ *over* $\mathbb{Q}(p_0,q_0)$ *whose Jacobian has a rational point of order* 7.

Using Theorem 2.3, one can construct other families. Let $Q_1 = x^2 + (u_1 + v_1\sqrt{d})x + u + v_0\sqrt{d}$. One may first assume that $u_1 = 0$ (the changement of $x$ into $x - \frac{u_1}{2}$ does affect $\overline{Q_1}$ in a compatible way), and that $(v_0, v_1) = (1,0)$; $(0,1)$; $(-1,1)$. The case $(v_0,v_1) = (1,0)$ does not lead to any solution. The case $(v_0,v_1) = (0,1)$ leads to the curve $\hat{C}_{u,d,7}$ defined by the equation

$$y^2 = x^2\Big(x^2 + \frac{ud}{u+d} + u + d\Big)^2 - 4d\Big(x^2 + \frac{ud}{u+d}\Big)^2.$$

Obviously, its Jacobian is isogeneous to a product of elliptic curves, and we do not further consider this family here. In the last case $(v_0,v_1) = (-1,1)$ computations show that

$$Q_1^2F_1 - \overline{Q_1}^2\overline{F_1} = \frac{4(u+1)^3d\sqrt{d}}{u-3+d}$$

is satisfied with

$$\begin{aligned} F_1 = \;& x^3 + \tfrac{3u-1+d}{u-3+d}x^2 + \tfrac{u^2-3u+3ud-2d+d^2}{u-3+d}x + \tfrac{3u^2+3ud-d^2+6d-u}{u-3+d} \\ & +2(x^2 + 2\tfrac{u+1}{u-3+d}x + \tfrac{ud-3u+1}{u-3+d})\sqrt{d}. \end{aligned}$$

It is then easy to prove the following result:

THEOREM 5.2: *Let* $u$ *be a parameter, and* $d$ *an element of* $\mathbb{Q}\setminus\mathbb{Q}^2$. *The curve* $\tilde{C}_{u,d,7}$ *defined by the equation*

$$\begin{aligned} y^2 = \;& \Big(x^3 + \tfrac{3u-1+d}{u-3+d}x^2 + \tfrac{u^2-3u+3ud-2d+d^2}{u-3+d}x + \tfrac{3u^2+3ud-d^2+6d-u}{u-3+d}\Big)^2 \\ & -4d\Big(x^2 + 2\tfrac{u+1}{u-3+d}x + \tfrac{ud-3u+1}{u-3+d}\Big)^2 \end{aligned}$$

*is generically of genus* 2 *and its Jacobian has a* $\mathbb{Q}(u,d)$*-rational point of order* 7. *Moreover this family contains the modular curve* $X_0(29)$.

One recovers the curve $X_0(29)$ with the choice $(u,d) = (-\frac{57}{25}, \frac{116}{25})$ of the parameters. Again, the Igusa invariants of the curves $C_{p_0,q_0,7}$ and $\tilde{C}_{u,d,7}$ are non-constant, and the Jacobians of these families of genus 2 curves are generically absolutely irreducible. The specialisation of the parameters in these families of curves provides infinitely many genus 2 curves defined over $\mathbb{Q}$, whose Jacobians have a $\mathbb{Q}$-rational point of order 7.

# 6. A new family of hyperelliptic genus 3 curves whose Jacobians have a rational point of order 10

The method used in this last section is similar to what has been done in the two previous sections, and we only sketch the proof of Theorem 6.1 below. Let

$$\begin{aligned} Q_1 = &\ x^3 + x^2 + q(x + q - t) - \sqrt{qt}x, \\ F_1 = &\ x^4 + (t - q + 2)x^3 + (1 + 2t)x^2 + (q + t)x + q(t - q^2 + 2qt + q - t^2) \\ &+2(x^2 + (t + 1 - q)x + t)\sqrt{qt}. \end{aligned}$$

Then the following equation holds:

$$Q_1^2 F_1 - \overline{Q_1}^2 \overline{F_1} = 4qt(q - t)^2 \sqrt{qt}.$$

With these notations, we obtain the following theorem:

THEOREM 6.1: *Let $q, t$ be parameters such that $qt$ is an element of $\mathbb{Q} \setminus \mathbb{Q}^2$. The curve $C_{q,t,10}$ defined by the equation*

$$\begin{aligned} y^2 = &\ \Big(x^4 + (t - q + 2)x^3 + (1 + 2t)x^2 + (q + t)x + q(t - q^2 + 2qt + q - t^2)\Big)^2 \\ &-4qt\Big(x^2 + (t + 1 - q)x + t\Big)^2 \end{aligned}$$

*is generically of genus 3, and its Jacobian has a $\mathbb{Q}(q, t)$-rational point of order 10. Moreover this family contains the curve $X_0(41)$.*

One easily checks, that the order of the class of the divisor $(+\infty) - (-\infty)$ is different from 2 and 5, hence is equal to 10. The curve $X_0(41)$ corresponds to the choice $(q, t) = (\frac{1}{50}, \frac{41}{50})$ of the parameters. Because the genus is 3, the Igusa invariants cannot be used in this case, but the techniques described in [Leprévost, 1992, 1994, 1996, 1997] apply and show, that the curve $C_{q,t,10}$ is not isotrivial. The specialisation of the parameters in this curve provides infinitely many hyperelliptic genus 3 curves defined over $\mathbb{Q}$, whose Jacobians have a $\mathbb{Q}$-rational point of order 10.

*The authors thank the FNR (project FNR/04/MA6/11) for their support.*

## References

Boxall, J.; Grant, D.: Examples of torsion points on genus two curves. Trans. Amer. Math. Soc. 352, 4533-4555 (2000)

Boxall, J.; Grant, D.; Leprévost, F.: 5-torsion points on curves of genus 2. J. Lond. Math. Soc., II Ser. 64, No. 1, 29-43 (2001)

Flynn, E.V.: Large rational torsion on abelian varieties. J. Number Theory 36, No. 3, 257-265 (1990)

Flynn, E.V.: Sequences of rational torsions on abelian varieties. Invent. Math. 106, No. 2, 433-442 (1991)

Gonzàlez Rovira, J.: Equations of hyperelliptic modular curves. Ann. Inst. Fourier, Grenoble 41, 4, 779-795 (1991)

Hibino, T.; Murabayashi, N.: Modular equations of hyperelliptic $X_0(N)$ and an application. Acta Arith. 82.3, 279-291 (1997)

Howe, E.W.; Leprévost, F.; Poonen, B.: Large torsion subgroups of split Jacobians of curves of genus two or three. Forum Math. 12, No. 3, 315-364 (2000)

Igusa, J.: Arithmetic variety of moduli for genus two. Ann. Math. (2) 72, 612-649 (1960)

Kamienny, S.: Torsion points on elliptic curves over all quadratic fields. Duke Math. J. 53, No. 1, 157-162 (1986)

KANT: *http://www.math.tu-berlin.de/~kant*

Kubert, D.: Universal bounds on the torsion of elliptic curves. Proc. Lond. Math. Soc., III Ser. 33, 193-237 (1976)

Lehner, J.; Newman, M.: Weierstraß points of $\Gamma_0(n)$. Ann. Math. (2) 79, 360-368 (1964)

Leprévost, F.: Familles de courbes des genre 2 munies d'une classe de diviseurs rationnels d'ordre 13. C. R. Acad. Sci., Paris, Sér. I, 313, No. 7, 451-454 (1991)

Leprévost, F.: Familles de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 15, 17, 19 ou 21. C. R. Acad. Sci., Paris, Sér. I, 313, No. 11, 771-774 (1991)

Leprévost, F.: Torsion sur des familles de courbes de genre $g$. Manuscr. Math. 75, No. 3, 303-326 (1992)

Leprévost, F.: Courbes modulaires et 11-rang de corps quadratiques. Exp. Math. 2, No.2, 137-146 (1993)

Leprévost, F.: Famille de courbes hyperelliptiques de genre $g$ munies d'une classe de diviseurs rationnels d'ordre $2g^2 + 4g + 1$. (David, S. (ed.): Séminaire de théorie des nombres, Paris, 1991-92. Birkhäuser) Prog. Math. 116, 107-119 (1994)

Leprévost, F.: Jacobiennes de certaines courbes de genre 2: torsion et simplicité. J. Théor. Nombres Bordx. 7, No. 1, 283-306 (1995)

Leprévost, F.: Sur une conjecture sur les points de torsion rationnels des jacobiennes de courbes. J. Reine Angew. Math. 473, 59-68 (1996)

Leprévost, F.: Sur certains sous-groupes de torsion de jacobiennes de courbes hyperelliptiques de genre $g \geq 1$. Manuscr. Math. 92, No. 1, 47-63 (1997)

Magma: *http://magma.maths.usyd.edu.au*

Maple: *http://www.maplesoft.com*

Mazur, B.: Rational points on modular curves. (Modular Funct. one Var. V, Proc. Int. Conf., Bonn 1976) Lect. Notes Math. 601, 107-148 (1977)

Merel, L.: Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. Math. 124, No. 1-3, 437-449 (1996)

Ogg, A.P.: Rational points on certain elliptic modular curves. (Analytic Number Theory) Proc. Symp. Pure Math. 24, 221-231, Providence (1973)

Ogg, A.P.: Hyperelliptic modular curves. Bull. Soc. Math. France 102, 449-462 (1974)