Hyperelliptic parametrizations of $\mathbb{Q}$-curves

Francesc Bars[*], Josep González [†] and Xavier Xarles

Abstract

For a square-free integer N, we present a procedure to compute $\mathbb{Q}$-curves parametrized by rational points of the modular curve $X_0^*(N)$ when this is hyperelliptic.

1 Introduction

Let X be a curve defined over $\overline{\mathbb{Q}}$. The curve X is said to be a $\mathbb{Q}$-curve if it is isogenous to all Galois conjugates. In [Elk04], Elkies proved that every $\mathbb{Q}$-curve without complex multilication (CM) is isogenous over $\overline{\mathbb{Q}}$ to a $\mathbb{Q}$-curve attached to a rational point of the modular curve $X_0^*(N) = X_0(N)/B(N)$ for some square-free integer N, where $B(N)$ denotes the group of the Atkin-Lehner involutions of $X_0(N)$. Every rational non-cuspidal point in $X_0^*(N)$ lifts to $X_0(N)$ providing $\mathbb{Q}$-curves, with or without CM, defined over abelian extensions of $\mathbb{Q}$ of type $(2, \cdots, 2)$.

In [GL98], it is given a procedure to parametrize the j-invariants of these $\mathbb{Q}$-curves when the genus g_N^* of $X_0^*(N)$ is at most 1. In these cases, the set $X_0^*(N)(\mathbb{Q})$ is infinite. Basically, in this paper it is given a method to determine the symmetric functions of the set $\{j(d\,z)\colon 1 \leq d|N\}$, where $j(z)$ denotes the usual generator of $\mathbb{Q}(X_0(1))$, from a suitable generators of $\mathbb{Q}(X_0^*(N))$. Here, we present a similar procedure for the case that $X_0^*(N)$ is hiperelliptic, that amounts to saying $g_N^* = 2$. In fact, there are exactly 36 values of N for which $g_N^* = 2$. By Faltings, for such a value of N, we are dealing with a finite number of cases. Firstly, we consider the rational points provided by Magma. Although the rank of $\mathrm{Jac}(X_0^*(N))$ is equal to 2 and the classical Chabauty method does not work, we can determine the full set $X_0^*(N)(\mathbb{Q})$ for 19 values of N by using a Chabauty procedure on a finite set of unramified 2-coverings of the curve.

The article is organized as follows. In Proposition 1 of §2, we present the main tool to parametrize $\mathbb{Q}$-curves from rational non-cuspidal points of $X_0^*(N)$. In §3, we give a list of equations of $X_0^*(N)$ when $g_N^* = 2$ together their rational points provided by Magma and, in Proposition 2, we determine all rational points for 19 values of N. In §4, we show how the j-invariants of the $\mathbb{Q}$-curves curves over these rational points are computed for the case $N = 67$. Next, for all values of N we determine which of the parametrized $\mathbb{Q}$-curves have CM and, for all of them, we give the discriminant D of the order of its endomorphism ring. Moreover, if the j-invariant of the $\mathbb{Q}$-curve lies in a quadratic field, it is given explicitly; otherwise, we provide the number field $\mathbb{Q}(j)$.

We recall that there is a finite number of discriminants D of orders of imaginary quadratic fields K such that $\mathrm{Gal}(H_D/\mathbb{Q})$ is of the type $(2, \cdots, 2)$, where H_D denotes the ring class field of the quadratic order of discriminant D. In fact, this condition is equivalent to say that the j-invariant of an elliptic curve with CM by the order of discriminant D generates a totally real number field. Moreover, $|\mathrm{Gal}(H_D/K)|$ divides 16 (for more detail, see [Bue89] and

[*]First and third author are supported by MTM2016-75980-P and MDM-2014-0445.

[†]Second author is partially supported by DGI grant MTM2015-66180-R.

CM-computations in the web-page https://mat-web.upc.edu/people/joan.carles.lario/). The results obtained when $g_N^* = 2$ show that almost these $\mathbb{Q}$-curves have CM, which reinforces the conjecture that for a large enough N, the curve $X_0^*(N)$ does not have rational points parametrizing $\mathbb{Q}$-curves without CM.

2 Preliminary results

Let X be a genus two curve defined over a subfield K of the complex field $\mathbb{C}$ that is the normalization of the curve given by the affine equation

$$y^2 = x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0\,,$$

with $a_i \in K$ for all $i \leq 5$. Let us denote by w the hyperelliptic involution. There are two points P_0 and $P_1 = w(P_0)$ over the singularity at infinity, defined over K that are not Weierstrass points and both satisfy $\left(\frac{y}{x^3}\right)^2(P_i) = 1$. Denote by P_0 such a point satisfying $\left(\frac{y}{x^3}\right)(P_0) = 1$ and, thus, $\left(\frac{y}{x^3}\right)(P_1) = -1$. For an integer $n \geq 1$, we consider the K-vector space

$$\mathcal{L}_i = \{f \in K(X)\colon\ \mathrm{div}(f) \geq -n\,P_0\}\,.$$

It is clear that $\dim \mathcal{L}_n = 1$ for $n \leq 2$ and, by the Riemann-Roch Theorem, we know that $\dim \mathcal{L}_n = n-1$ when $n > 2$. We denote by $\mathrm{div}^- f$ the polar part of $\mathrm{div}\, f$, i.e. $\mathrm{div}\, f + .\, \mathrm{div}^- f \geq 0$.

Proposition 1. *Keeping the above notation, the functions $f_3, f_4, f_5 \in K(X)$ defined by*

$$\begin{aligned}
f_3 &= \frac{8a_3 - 4a_4\,a_5 + a_5^3}{32} + \frac{4a_4 - a_5^2}{16}x + \frac{a_5}{4}x^2 + \frac{1}{2}x^3 + \frac{1}{2}y\,,\\
f_4 &= \frac{64a_2 - 16a_4^2 - 32a_3a_5 + 24a_4a_5^2 - 5a_5^4}{256} + x\,f_3\,,\\
f_5 &= \frac{128a_1 - 64a_3a_4 - 64a_2a_5 + 48a_4^2a_5 + 48a_3a_5^2 - 40a_4a_5^3 + 7a_5^5}{512} + x\,f_4\,,
\end{aligned}$$

vanish at $w(P_0)$ and satisfy that $\mathrm{div}^- f_i = i\,P_0$ for all $i \in \{3,4,5\}$. In particular, $\mathcal{L}_3 = \langle 1, f_3\rangle$, $\mathcal{L}_4 = \langle 1, f_3, f_4\rangle$ and $\mathcal{L}_5 = \langle 1, f_3, f_4, f_5\rangle$.

Proof. Let $g_3 \in \mathcal{L}_3$ be a non constant function. By adding a constant, if necessary, we can assume $g_3(w(P_0)) = 0$. We have that the function $h = g_3 - (g_3|w)$ satisfies $h|w = -h$ and $\mathrm{div}^- h = 3(P_0) + 3(w(P_0))$. Hence, $h = A\,y$ for some non zero $A \in K$. Putting $f_3 = g_3/A$, we get $f_3 - (f_3|w) = y$. Moreover, the functions $f_3 + (f_3|w)$ and $f_3 \cdot (f_3|w)$ are invariant under the action of w and satisfy

$$\mathrm{div}^-(f_3 + (f_3|w)) = 3(P_0) + 3(w(P_0)) \quad \text{and} \quad \mathrm{div}^-(f_3 \cdot (f_3|w)) \leq 2(P_0) + 2(w(P_0))\,.$$

Therefore, $f_3 + (f_3|w)$ is a polynomial in x of degree 3 and $f_3 \cdot (f_3|w)$ must be a polynomial in x of degree at most 2. Since

$$x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 - (f_3 + (f_3|w))^2 = -4((f_3 \cdot (f_3|w))\,,$$

the polynomial $P(X)^2 = (f_3 + (f_3|w))^2$ is determined and, thus, $P(x)$ is determined up to sign. Hence, f_3 must be $1/2(y \pm P(x))$. Since $(y/x^3)(P_0) = 1$, we take the sign such that $f_3 = 1/2(y + x^3 + \cdots)$.

The function $x f_3$ lies in $\mathcal{L}_4$ and $\operatorname{div}^- x\, f_3 = 4P_0$. There exists $k \in K$ such that the function $f_4 = x\, f_3 + k$ vanishes at $w(P_0)$. By construction, $f_4 - (f_4|w) = x \cdot y$ and $f_4 + (f_4|w)$ is a polynomial in x of degree 4. We can determine k by using that the function $x^2y^2 - (f_4 + (f_4|w))^2$ is a polynomial in x of degree at most 3, because it is equal to the function $-4((f_4 \cdot (f_4|w))$.

Similarly, $x\, f_4 \in \mathcal{L}_5 \backslash \mathcal{L}_4$ and there exists $k \in K$ such that the function $f_5 = x\, f_4 + k$ vanishes at $w(P_0)$. Now, $f_5 - (f_5|w) = x^2 \cdot y$ and $f_5 + (f_5|w)$ is a polynomial in x of degree 5. We determine k by using that $x^4y^2 - (f_5 + (f_5|w))^2$ is a polynomial in x of degree at most 4. □

Corollary 1. *For an integer $n \geq 3$ and function $f \in \mathcal{L}_n$, the function $f - f(\infty')$ is a K-linear combination of the functions $\{f_5 f_3^k, f_4 f_3^k, f_3^{k+1} \colon 0 \leq k \leq \lfloor n/3 \rfloor\}$.*

Proof. For an integer $n \geq 3$, let $i \in \{0, 1, 2\}$ be such that $n \equiv i \pmod 3$. The statement follows from the fact that the function $h = f_{i+3} f_3^{(n-i)/3-1}$ lies in $\mathcal{L}_n$ with $\operatorname{div}^- h = nP_0$ and $h(\infty') = 0$. □

Remark 1. *Note that if q is an analytic uniformizing parameter at P such that $x = 1/q + \cdots$ and $y = 1/q^3 + \cdots$, then $f_i = 1/q^i + \cdots$ for $i \in \{3, 4, 5\}$.*

3 Application to genus two curves $X_0^*(N)$

In [HH96], it is proved that when N is square-free, $X_0^*(N)$ is hyperelliptic if, and only if, it has genus two. There are 35 square-free integers N such that $X_0^*(N)$ has genus two (cf. [Has97, Remark 1]). In all these cases, there is an only basis h_1 and h_2 of $S_2(\Gamma_0(N))^{B(N)}$ such that their q-expansions lie in $\mathbb{Z}[[q]]$ and are of the form $h_1(q) = q + \sum_{n\geq 3} b_n q^n$ and $h_2(q) = q^2 + \sum_{n\geq 3} c_n q^n$. The functions on $X_0^*(N)$ defined as follows

$$x = \frac{h_1}{h_2} = 1/q + \cdots, \quad y = -q\frac{d\,x}{d\,q}/h_2 = 1/q^3 + \cdots$$

satisfy an equation of the form $y^2 = x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ with $a_i \in \mathbb{Z}$ for all i. Denoting by ∞ the infinity cusp and by $\infty' = w(\infty)$, we have $\operatorname{div}^- x = \infty + \infty'$, $\operatorname{div}^- y = 3\infty + 3\infty'$ and $(y/x^3)(\infty) = 1$.

Consider the symmetric functions obtained from the functions $j(d\,z)$ for $1 \leq d|N$:

$$J_1(z) = \sum_{1\leq d|N} j(d\,z)\,, \cdots, J_m(z) = \prod_{1\leq d|N} j(d\,z)\,,$$

where $m = 2^{\omega(N)}$ and $\omega(N)$ denotes the number of primes dividing N. We determine every function J_i as a $\mathbb{Q}$-linear combination of functions of the form $f_5 f_3^k, f_4 f_3^k, f_3^k$ for $k \geq 0$. Given a non-cuspidal $Q \in X_0^*(N)$, the j-invariants of the $\mathbb{Q}$-curves attached to this point are the roots of the polynomial in z:

$$z^m + \sum_{i=1}^{n} (-1)^i J_i(Q) z^{n-i}\,.$$

We know that for a non trivial automorphism u of $X_0^*(N)$, one has $u(\infty) \neq \infty$ (cf. [BH03, Lemma 3.1]). Hence, for all these curves $|X_0^*(N)(\mathbb{Q})\backslash\{\infty\}| \geq 1$ and for the bielliptic curves, i.e. for $N \in \{106, 122, 129, 158, 166, 215, 390\}$ (cf. [BG19, Theorem 1]), we have that $|\operatorname{Aut}(X_0^*(N))| = 4$ and, thus, $|X_0^*(N)(\mathbb{Q})\backslash\{\infty\}| \geq 3$. Next, in Table 1, we present the equations with the functions x and y obtained following the procedure mentioned above, together with the rational points with x-coordinate with height less than 10^4.

3.1 Equations and rational points

N	equation	$X_0^*(N)(\mathbb{Q})\backslash\{\infty,\infty'\}$
67	$y^2 = x^6 - 4x^5 + 6x^4 - 6x^3 + 9x^2 - 14x + 9$	$(-1,\pm7), (0,\pm3), (1,\pm1), (2,\pm1)$
73	$y^2 = x^6 - 4x^5 + 6x^4 + 2x^3 - 15x^2 + 10x + 1$	$(0,\pm1), (1,\pm1), (2,\pm3), (\frac{3}{2},\pm\frac{5}{8})$
85	$y^2 = (x^2 - 2x + 5)(x^4 - 2x^3 + 3x^2 - 6x + 5)$	$(0,\pm5), (1,\pm2), (2,\pm5), (\frac{3}{2},\pm\frac{17}{8}), (-\frac{4}{3},\pm\frac{425}{27})$
93	$y^2 = (x^3 - 2x^2 - x + 3)(x^3 + 2x^2 - 5x + 3)$	$(-1,\pm3), (0,\pm3), (1,\pm1), (2,\pm3), (\frac{3}{2},\pm\frac{9}{8}), (\frac{1}{4},\pm\frac{143}{64})$
103	$y^2 = x^6 - 10x^4 + 22x^3 - 19x^2 + 6x + 1$	$(0,\pm1), (1,\pm1), (3,\pm19)$
106	$y^2 = x^6 - 4x^5 + 4x^4 + 2x^3 + 4x^2 - 4x + 1$	$(-1,\pm4), (0,\pm1), (1,\pm2), (2,\pm5), (\frac{1}{2},\pm\frac{5}{8})$
107	$y^2 = x^6 - 4x^5 + 10x^4 - 18x^3 + 17x^2 - 10x + 1$	$(0,\pm1), (2,\pm1)$
115	$y^2 = (x^3 - 2x^2 + 3x - 1)(x^3 + 2x^2 - 9x + 7)$	$(1,\pm1), (2,\pm5), (\frac{1}{2},\pm\frac{5}{8}), (\frac{4}{3},\pm\frac{35}{27})$
122	$y^2 = x^6 + 4x^4 - 6x^3 + 4x^2 + 1$	$(-1,\pm4), (0,\pm1), (1,\pm2), (\frac{3}{2},\pm\frac{37}{8}), (\frac{2}{3},\pm\frac{37}{27})$
129	$y^2 = x^6 - 4x^5 - 4x^4 + 12x^3 + 4x^2 - 12x + 4$	$(-1,\pm3), (0,\pm2), (1,\pm1), (\frac{1}{2},\pm\frac{3}{8}), (-\frac{7}{5},\pm\frac{383}{125}), (\frac{7}{12},\pm\frac{383}{1728})$
133	$y^2 = x^6 + 4x^5 - 18x^4 + 26x^3 - 15x^2 + 2x + 1$	$(0,\pm1), (1,\pm1), (\frac{3}{5},\pm\frac{83}{125})$
134	$y^2 = x^6 - 4x^5 + 2x^4 - 2x^3 + x^2 + 2x + 1$	$(-1,\pm3), (0,\pm1), (1,\pm1), (-\frac{1}{2},\frac{7}{8})$
146	$y^2 = x^6 - 4x^5 + 2x^4 + 6x^3 + x^2 + 2x + 1$	$(-1,\pm1), (0,\pm1), (1,\pm3), (2,\pm5)$
154	$y^2 = (x - 2)(x^2 + x + 2)(x^3 - 3x^2 - x - 1)$	$(0,\pm2), (1,\pm4), (2,0), (-\frac{3}{2},\pm\frac{77}{8}), (-\frac{1}{3},\pm\frac{56}{27}), (4,\pm22)$
158	$y^2 = x^6 - 4x^4 + 2x^3 - 4x^2 + 1$	$(0,\pm1), (2,\pm1), (\frac{1}{2},\pm\frac{1}{8})$
161	$y^2 = (x^3 - 2x^2 + 3x - 1)(x^3 + 2x^2 + 3x - 5)$	$(-1,\pm7), (1,\pm1), (-\frac{1}{2},\pm\frac{35}{8}), (-\frac{1}{4},\pm\frac{209}{64})$
165	$y^2 = (x - 1)(x + 3)(x^2 - x - 1)(x^2 - x + 3)$	$(-1,\pm4), (0,\pm3), (1,0), (2,\pm5), (-\frac{1}{2},\pm\frac{15}{8}), (-3,0), (\frac{2}{3},\pm\frac{55}{27}), (\frac{5}{2},\pm\frac{99}{8})$
167	$y^2 = x^6 - 4x^5 + 2x^4 - 2x^3 - 3x^2 + 2x - 3$	$(-1,\pm1)$
170	$y^2 = (x^2 - 5x + 5)(x^4 - 11x^3 + 48x^2 - 87x + 53)$	$(1,\pm2), (2,\pm1), (\frac{3}{2},\pm\frac{5}{8}), (4,\pm5), (\frac{11}{3},\frac{38}{27})$
177	$y^2 = x^6 + 2x^4 - 6x^3 + 5x^2 - 6x + 1$	$(0,\pm1), (\frac{3}{2},\pm\frac{17}{8})$
186	$y^2 = (x^3 - 2x^2 + x + 1)(x^3 + 2x^2 + 5x + 1)$	$(-1,\pm3), (0,\pm1), (1,\pm3), (2,\pm9), (-\frac{1}{2},\pm\frac{3}{8}), (-\frac{4}{3},\pm\frac{143}{27})$
191	$y^2 = x^6 + 2x^4 + 2x^3 + 5x^2 - 6x + 1$	$(0,\pm1), (2,\pm11)$
205	$y^2 = x^6 + 2x^4 + 10x^3 + 5x^2 - 6x + 1$	$(0,\pm1), (-2,\pm7)$
206	$y^2 = x^6 + 2x^4 + 2x^3 + 5x^2 + 6x + 1$	$(-1,\pm1), (0,\pm1), (\frac{1}{2},\pm\frac{19}{8})$
209	$y^2 = x^6 - 4x^5 + 8x^4 - 8x^3 + 8x^2 + 4x + 4$	$(0,\pm2), (-\frac{1}{2},\pm\frac{19}{8})$
213	$y^2 = x^6 + 2x^4 + 2x^3 - 7x^2 + 6x - 3$	$(1,\pm1)$
215	$y^2 = x^6 + 4x^5 - 12x^4 + 20x^3 - 20x^2 + 12x - 4$	$(1,\pm1), (2,\pm10)$
221	$y^2 = x^6 + 4x^5 + 2x^4 + 6x^3 + x^2 - 2x + 1$	$(0,\pm1), (\frac{1}{2},\pm\frac{9}{8})$
230	$y^2 = (x^3 - 2x^2 + 5x + 1)(x^3 + 2x^2 + x + 1)$	$(0,\pm1), (1,\pm5), (-2,\pm5), (3,\pm35)$
266	$y^2 = x^6 + 4x^5 + 10x^4 + 14x^3 + 17x^2 + 10x + 1$	$(-1,\pm1), (0,\pm1), (-\frac{5}{2},\pm\frac{83}{8})$
285	$y^2 = x(x^2 + x + 4)(x^3 - x^2 - x - 3)$	$(-1,\pm4), (0,0), (3,\pm24), (-\frac{3}{2},\pm\frac{57}{8})$
286	$y^2 = (x^3 - x^2 + 3x + 1)(x^3 + x^2 - 4)$	$(-1,\pm4), (\frac{5}{2},\pm\frac{143}{8})$
287	$y^2 = x^6 - 4x^5 + 2x^4 + 6x^3 - 15x^2 + 14x - 7$	$(-2,\pm9)$
299	$y^2 = x^6 - 4x^5 + 6x^4 + 6x^3 - 7x^2 - 10x - 3$	$(-\frac{1}{2},\pm\frac{1}{8})$
357	$y^2 = x^6 + 8x^4 - 8x^3 + 20x^2 - 12x + 12$	$(2,\pm14)$
390	$y^2 = (x^2 - x + 1)(x^4 + 5x^3 - 8x^2 + 5x + 1)$	$(0,\pm1), (1,\pm2)$

Table 1

3.2 Determination of the rational points

In order to determine the rational points of the curves $X_0^*(N)$ we will use the so-called elliptic Chabauty method, which uses a Chabauty procedure on a finite set of unramified 2-coverings of the curve.

Proposition 2. *For the values $N = 85, 93, 106, 115, 122, 129, 154, 158, 161, 165, 170, 186, 209, 215, 230, 285, 286, 357$ and 390, the set of rational points of $X_0^*(N)(\mathbb{Q})$ is the set given in Table 1 together with the two points at infinity.*

Proof. The proposition is proved by using some computations in MAGMA [BP97]. A file with all the computations can be downloaded from the github account of the third author. We explain the main ideas in the computation, that can be done for any hyperelliptic curve X of genus g ($g = 2$ in our cases) given by an equation of the form $y^2 = f(x)$, whit $\deg f(x) = 2g+2$.

The computation is done in two steps: first one computes the finite set of twists C_ξ of the unramified coverings of the curve X with Galois group $\cong (\mathbb{Z}/2\mathbb{Z})^{2g}$ which have points locally for any prime p; this is completely analogous to the 2 descent for elliptic curves, as described in [BS09]. Each twists C_ξ is associated to an element $\xi \in (\mathbb{Q}[x]/f(x))^*$ (where the twist corresponding the points at infinity corresponds to $\xi = 1$). If some of the curves does not have rational points (apparently), one needs to show this by using either a Mordell-Weil sieve or a higher descent. For our curves this never happens, so we will not analyze this case further. Our aim now is the determination of the rational points in $C_\xi(\mathbb{Q})$.

Now, the jacobian of any of this curves has quotients isomorphic to the Weil restriction of elliptic curves E_ξ defined over some number fields K, and the rational points in $C_\xi(\mathbb{Q})$ give points in $E_\xi(K)$ whose image with respect to a given map $\varphi_\xi : E_\xi \to \mathbb{P}^1$ is in $\mathbb{P}^1(\mathbb{Q})$; this is the necessary data for the elliptic Chabauty function, which computes the set of points in $E_\xi(K)$ verifying this condition if $\mathrm{rank}_{\mathbb{Z}}(E_\xi(K)) < \deg(K/\mathbb{Q})$. In practice, the fields K we need are the minimal field of definition of some fixed factorization $f(x) = g(x)h(x)$ where $g(x)$ has degree 4.

For example, if $g = 2$ and the polynomial $f(x)$ is irreducible, we consider the field $L_0 := \mathbb{Q}[x]/f(x)$. Suppose furthermore that $f(x) = (x-\alpha)f_1(x)$ in $L[x]$ again with $f_1(x)$ irreducible; then the minimal field of definition of a factorization $f(x) = g(x)h(x)$ where $g(x)$ has degree 4 is a field of degree 15 over $\mathbb{Q}$. In this case, the elliptic curves correspond to the jacobians of the curves $H_\xi : y^2 = \xi g(x)$, and the map $\varphi_\xi : H_\xi \to \mathbb{P}^1$ is given by the x-coordinate. In this case the necessary Chabauty condition is $\mathrm{rank}_{\mathbb{Z}}(E_\xi(K)) < 15$, which is quite likely to be fulfilled; but right now the computation of the rank and a finite index subgroup of $E(K)$ for $K/\mathbb{Q}$ of such degree is unfeasible. This situation is what happens in all the values of N which we were not able to determine the set of rational points (including all prime values of N).

The other extreme case is when there is a factorization $f(x) = g(x)h(x)$ already defined over $\mathbb{Q}$; in this case we need to compute the rational points of the curves $y^2 = d_\xi g(x)$ for some values $d_\xi \in \mathbb{Q}^*$, which are only finite if the rank is zero (which is very unlikely to happen for all the necessary twists d_ξ).

The best cases are when one can find such a factorization over a field of degree ≤ 4 for any twists verifying the corresponding Chabauty condition. In some cases we used distinct fields for different twists, as we explain in the following example.

Example. We explain in detail the case $X_0^*(85)$, where $f(x) = (x^2-2x+5)(x^4-2x^3+3x^2-6x+5)$. We have

$$X_0^*(85)(\mathbb{Q}) = \{(0, \pm 5), (1, \pm 2), (2, \pm 5), (\frac{3}{2}, \pm\frac{17}{8}), (-\frac{4}{3}, \pm\frac{425}{27}), \pm\infty\}.$$

We have 5 twists, corresponding to the x-coordinates of the rational points, except that the points with $x = 1$ already appear in the trivial twists corresponding to the points at infinity.

If we consider the given factorization over $\mathbb{Q}$, the corresponding elliptic curves for all the twists except the trivial one have rank 1. On the other hand the curve H given by the equation $y^2 = x^4 - 2x^3 + 3x^2 - 6x + 5$ has rank 0 and 4 points, corresponding to the points at infinity and the points with $x = 1$.

If we adjoint a root of $x^2 - 2x + 5$ we get a quadratic extension $K_2/\mathbb{Q}$. Over this extension we get also a factorization of $x^4 - 2x^3 + 3x^2 - 6x + 5 = h_1(x)h_2(x)$ with $\deg(h_i(x)) = 2$ for

$i = 1, 2$. So we can take $f(x) = g(x)h_1(x)$ for some $g(x)$ of degree 4. The twists corresponding to the points with x-coordinate $\frac{3}{2}$ and $-\frac{4}{3}$ have rank 1, and Chabauty method succeeds. But the ones corresponding to the points with x-coordinate 0 and 2 have rank 2.

If we adjoint a root of $x^4 - 2x^3 + 3x^2 - 6x + 5$ we get a field K_4 where $f(x)$ has 4 roots and a degree 2 factor. By considering the corresponding degree 4 polynomial as a product of two (adequate) degree one factors and the degree two factor we finally get that the remaining twist have jacobian of rank 1 and we find a non-torsion point in each case, and Chabauty computations succeeds.

There is one case were the approach described above did not succeed.

Example. In the case $X_0^*(390)$ we had to do a slightly modified approach; in fact, we tried fields of degree 1 and 2 and the Chabauty condition was not fulfilled, and we had to go to a degree 8 extension, where the rank computation did not succeed.

Instead, we showed that all the rational points in $X_0^*(390) : y^2 = (x^2 - x + 1)(x^4 + 5x^3 - 8x^2 + 5x + 1)$ came from the trivial twists over $\mathbb{Q}$. This means that their x-coordinates verify that

$$y_1^2 = x^2 - x + 1 \text{ and } y_2^2 = x^4 + 5x^3 - 8x^2 + 5x + 1$$

for some $y_1, y_2 \in \mathbb{Q}$. The curve X' determined by these equations is an hyperelliptic curve of genus 3, whose hyperelliptic equation can be computed by parametrizing the first equation. We get the equation

$$X' : z^2 = t^8 + 10t^7 - 41t^6 + 42t^5 + 33t^4 - 76t^3 + 44t^2 - 16t + 4.$$

Now we apply the above method to this new curve X'. The curve has (apparently) 12 rational points (two above each rational point of $X_0^*(390)$, as it is an unramified 2-covering), with 6 possible values for the x-coordinates. We computed there are exactly 6 possible twists, one for each x-coordinate. Over $K = \mathbb{Q}(\sqrt{5})$ the defining hyperelliptic polynomial factors as a product of two degree 4 polynomials. For every twists one of the two quotient elliptic curves of the corresponding covering has rank one, and the Chabauty computation succeeds. □

4 An example and results

First, we show, for the case $N = 67$, the procedure used. The equation obtained in Table 1 is $y^2 = x^6 - 4x^5 + 6x^4 - 6x^3 + 9x^2 - 14x + 9$. Let $j_{67}(q) := j(q^{67}) = 1/q^{67} + 744 + \cdots$ and put $J_1 = j + j_{67}$ and $J_2 = j \cdot j_{67}$. With the notation of before section, we have

$$f_3 = \frac{1}{2}\left(-1 + x - 2x^2 + x^3 + y\right), \quad f_4 = x\, f_3 + 1\,, \quad f_5 = x\, f_4 - 1\,.$$

After computing, we obtain

$$\begin{aligned} J_1 = \; & -23f_3^{22} + f_3^{21}f_4 - 1279f_3^{21} - 781f_3^{20}f_4 + 186f_3^{20}f_5 - 99914f_3^{20} - 39399f_3^{19}f_4 + 14954f_3^{19}f_5 - 2698696f_3^{19} - 265633f_3^{18}f_4 + \\ & 380472f_3^{18}f_5 - 20514523f_3^{18} + 6929641f_3^{17}f_4 + 1576893f_3^{17}f_5 - 49240824f_3^{17} + 67627402f_3^{16}f_4 - 16450546f_3^{16}f_5 - \\ & 61401116f_3^{16} + 190686364f_3^{15}f_4 - 81315034f_3^{15}f_5 - 56264079f_3^{15} + 259977664f_3^{14}f_4 - 148558638f_3^{14}f_5 - 88533538f_3^{14} + \\ & 95806265f_3^{13}f_4 - 69608123f_3^{13}f_5 - 162557463f_3^{13} - 295479289f_3^{12}f_4 + 158123161f_3^{12}f_5 - 27169544f_3^{12} - 558873206f_3^{11}f_4 + \\ & 260674425f_3^{11}f_5 + 456803156f_3^{11} - 423722114f_3^{10}f_4 + 202709065f_3^{10}f_5 + 731171796f_3^{10} - 51627779f_3^{9}f_4 + 133780373f_3^{9}f_5 + \\ & 234273070f_3^{9} + 264268555f_3^{8}f_4 - 64460559f_3^{8}f_5 - 502745764f_3^{8} + 337312727f_3^{7}f_4 - 318069668f_3^{7}f_5 - 623447279f_3^{7} + \\ & 158991342f_3^{6}f_4 - 299948399f_3^{6}f_5 - 229889114f_3^{6} - 28504966f_3^{5}f_4 - 91453878f_3^{5}f_5 + 60433254f_3^{5} - 60041832f_3^{4}f_4 + \\ & 24362830f_3^{4}f_5 + 79628320f_3^{4} - 20570848f_3^{3}f_4 + 26593344f_3^{3}f_5 + 23436576f_3^{3} - 941600f_3^{2}f_4 + 8600928f_3^{2}f_5 + 1047456f_3^{2} + \\ & 647200f_3f_4 + 1386464f_3f_5 - 571936f_3 + 81536f_4 + 92000f_5 - 65536\,, \end{aligned}$$

and

$$\begin{aligned}J_2 = {} & f_5f_3^{21} + 720f_4f_3^{21} + 179980f_3^{22} + 17300122f_5f_3^{20} + 410510311f_4f_3^{20} + 5149868567f_3^{21} + 42380978353f_5f_3^{19} + \\ & 176848900626f_4f_3^{19} + 839384847849f_3^{20} + 3347632163474f_5f_3^{18} + 5490095012794f_4f_3^{18} + 20232433296285f_3^{19} + \\ & 58903607428273f_5f_3^{17} + 52642797600751f_4f_3^{17} + 194740838424278f_3^{18} + 465038243745693f_5f_3^{16} + \\ & 252244831282013f_4f_3^{16} + 1049935814900775f_3^{17} + 2137932776610224f_5f_3^{15} + 718160756825707f_4f_3^{15} + \\ & 3682889678423580f_3^{16} + 6483265127099687f_5f_3^{14} + 1296256091753552f_4f_3^{14} + 9112585010431660f_3^{15} + \\ & 13905322982585428f_5f_3^{13} + 1455284181206971f_4f_3^{13} + 16698439687036025f_3^{14} + 22013212259613947f_5f_3^{12} + \\ & 785970239416766f_4f_3^{12} + 23380324317471236f_3^{13} + 26434965501463926f_5f_3^{11} - 389286347179143f_4f_3^{11} + \\ & 25533239990035759f_3^{12} + 24511794195150313f_5f_3^{10} - 1257772458271356f_4f_3^{10} + 22044986048091002f_3^{11} + \\ & 17745745315071401f_5f_3^9 1369085873848977f_4f_3^9 + 15174609069161127f_3^{10} + 10090414014987393f_5f_3^8 - \\ & 954179629348608f_4f_3^8 + 8365619455927489f_3^9 + 4511870660986624f_5f_3^7 - 476646738132432f_4f_3^7 + 3699701950122944f_3^8 + \\ & 1580542220676176f_5f_3^6 - 178202666014272f_4f_3^6 + 1312789289946672f_3^7 + 429477284579616f_5f_3^5 - 51157416030048f_4f_3^5 + \\ & 374258702810464f_3^6 + 88841374862944f_5f_3^4 - 11506808706816f_4f_3^4 + 86310527850080f_3^5 + 13536732334080f_5f_3^3 - \\ & 2038076477952f_4f_3^3 + 16327740526336f_3^4 + 1432454117376f_5f_3^2 - 272275906560f_4f_3^2 + 2547759661312f_3^3 + \\ & 93842541824f_5f_3 - 24005742848f_4f_3 + 313280547584f_3^2 + 2852000000f_5 - 1009741824f_4 + 26269884672f_3 + 1073741824\,.\end{aligned}$$

Hence, the j-invariants of the $\mathbb{Q}$-curves attached to ∞' are the solutions of the equation

$$z^2 - J_1(\infty')\,z + J_2(\infty') = 0\,.$$

Since $(J_1(\infty'), J_2(\infty')) = (-65536, 1073741824)$, we get $j = -32^3$, which corresponds to an elliptic curve with CM by the quadratic order of discriminant -11. The remaining rational non-cuspidal points provide $\mathbb{Q}$-curves with CM:

point	j	point	j	point	j	point	j
$(-1,\ 7)$	255^3	$(0,\ 3)$	$-3\cdot 160^3$	$(1,\ 1)$	20^3	$(2,\ 1)$	-960^3
$(-1,-7)$	-5280^3	$(0,-3)$	0	$(1,-1)$	-15^3	$(2,-1)$	$2\cdot 30^3$

Next, we show the results obtained.

4.1 N is a prime: $\mathrm{Gal}(\mathbb{Q}(j)/\mathbb{Q}) \hookrightarrow \mathbb{Z}/2\mathbb{Z}$.

N	point	CM	D	j-invariant
67	∞'	yes	-11	-32^3
	$(-1,7)$	yes	-7	255^3
	$(-1,-7)$	yes	-67	-5280^3
	$(0,3)$	yes	-27	$-3\cdot 160^3$
	$(0,-3)$	yes	-3	0
	$(1,1)$	yes	-8	20^3
	$(1,-1)$	yes	-7	-15^3
	$(2,1)$	yes	-43	-960^3
	$(2,-1)$	yes	-12	$2\cdot 30^3$
73	∞'	yes	-12	$2\cdot 30^3$
	$(0,1)$	yes	-27	$-3\cdot 160^3$
	$(0,-1$	yes)	-4	12^3
	$(1,1)$	yes	-19	-96^3
	$(1,-1)$	yes	-8	20^3
	$(2,3)$	yes	-67	-5280^3
	$(2,-3)$	yes	-16	66^3
	$(3/2,5/8)$	yes	-3	0
	$(3/2,-5/8)$	non	$-$	$20\left(\frac{3(-26670989 \pm 15471309\sqrt{-127})}{2^{26}}\right)^3$

N	point	CM	D	j-invariant
103	∞'	yes	-67	-5280^3
	$(0,1)$	yes	-43	-960^3
	$(0,-1)$	yes	-27	$-3\cdot 160^3$
	$(1,1)$	yes	-19	$-96^3]$
	$(1,-1)$	yes	-12	$2\cdot 30^3$
	$(3,19)$	non	$-$	$19(48(1623826405 \pm 30228849\sqrt{2885}))^3$
	$(3,-19)$	yes	-3	0
107	∞'	yes	-8	20^3
	$(0,1)$	yes	-7	-15^3
	$(0,-1)$	yes	-43	-960^3
	$(2,1)$	yes	-67	-5280^3
	$(2,-1)$	yes	-28	255^3
167	∞'	yes	-43	-960^3
	$(-1,1)$	yes	-67	-5280^3
	$(-1,-1)$	yes	-163	-640320^3
191	∞'	yes	-43	-960^3
	$(0,1)$	yes	-11	-32^3
	$(0,-1)$	yes	-7	-15^3
	$(2,11)$	non	$-$	j_0
	$(2,-11)$	yes	-28	255^3

where

$$j_0 = (724537954586714121 \pm 16056976492100\sqrt{2036079533})\left(\frac{480(7725788647437 \pm 95942438\sqrt{2036079533})}{191^2}\right)^3$$

4.2 N is a product of two primes: $\mathrm{Gal}(\mathbb{Q}(j)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^2$.

N	point	CM	D	j or $\mathbb{Q}(j)$
85	∞'	yes	-19	-96^3
	$(0,5)$	yes	-35	$-(16(15 \pm 7\sqrt{5}))^3$
	$(0,-5)$	yes	-60	$(3(470 \pm 213\sqrt{5})^3(1 \pm \sqrt{5})/2)$
	$(1,2)$	yes	-16	66^3
	$(1,-2)$	yes	-4	12^3
	$(2,5)$	yes	-115	$-(48(785 \pm 351\sqrt{5}))^3$
	$(2,-5)$	yes	-15	$-(3(25 \pm 9\sqrt{5})/2)^3(-1 \pm \sqrt{5})/2$
	$(3/2,17/8)$	yes	-51	$-(48(37 \pm 9\sqrt{17}))^3(-4 \pm \sqrt{17})$
	$(3/2,-17/8)$	non	$-$	$\mathbb{Q}(\sqrt{17},\sqrt{-95})$
	$(-4/3,425/27)$	non	$-$	$\mathbb{Q}(\sqrt{85},\sqrt{-4295})$
	$(-4/3,-425/27)$	yes	-595	$\mathbb{Q}(\sqrt{5},\sqrt{17})$

N	point	CM	D	j or $\mathbb{Q}(j)$
93	∞'	yes	-12	$2\cdot 30^3$
	$(0,3)$	yes	-60	$(3(470\pm 213\sqrt{5})^3(1\pm\sqrt{5})/2)$
	$(0,-3)$	yes	-24	$(12(5\pm 2\sqrt{2}))^3(3\pm 2\sqrt{2})$
	$(-1,3)$	yes	-123	$-(480(461\pm 72\sqrt{41}))^3(-32\pm 5\sqrt{41})$
	$(-1,-3)$	yes	-75	$-(48(-69\pm 31\sqrt{5}))^3(\pm\sqrt{5})$
	$(1,1)$	yes	-11	-32^3
	$(1,-1)$	yes	$-3,-12$	$0,-3\cdot 160^3$
	$(2,3)$	yes	-147	$-3(480(142\pm 31\sqrt{21}))^3(\pm\sqrt{21})$
	$(2,-3)$	yes	-15	$-(3(-5\pm 4\sqrt{5}))^3(-3\pm\sqrt{5})/2$
	$(3/2,9/8)$	yes	-48	$4(15(30\pm 17\sqrt{3}))^3$
	$(3/2,-9/8)$	non	$-$	$\mathbb{Q}(\sqrt{-15},\sqrt{-109})$
	$(1/4,143/64)$	yes	-3	0
	$(1/4,-143/64)$	non	$-$	$\mathbb{Q}(\sqrt{-23},\sqrt{-143})$
106	∞'	yes	-7	-15^3
	$(-1,4)$	yes	-36	$4(21\pm 20\sqrt{3})^3(7\pm 4\sqrt{3})$
	$(-1,-4)$	yes	-148	$(60(2837\pm 468\sqrt{37}))^3$
	$(0,1)$	yes	-40	$(6(65\pm 27\sqrt{5}))^3$
	$(0,-1)$	yes	$-4,-16$	$12^3,66^3$
	$(1,2)$	yes	-24	$(12(9\pm 7\sqrt{2}))^3(-1\pm\sqrt{2})$
	$(1,-2)$	yes	-52	$(30(31\pm 9\sqrt{13}))^3$
	$(2,5)$	yes	-100	$(6(2927\pm 1323\sqrt{5}))^3$
	$(2,-5)$	yes	-4	12^3
	$(1/2,5/8)$	non	$-$	$\mathbb{Q}(\sqrt{33},\sqrt{-591})$
	$(1/2,-5/8)$	yes	$-7,-28$	$-15^3,255^3$
115	∞'	yes	-115	$(48(-785\pm 351\sqrt{5}))^3$
	$(1,1)$	yes	-19	-96^3
	$(1,-1)$	yes	-11	-32^3
	$(2,5)$	yes	-235	$(528(-8875\pm 3969\sqrt{5}))^3$
	$(2,-5)$	yes	-15	$-(3/2(25\pm 9\sqrt{5}))^3(-1\pm\sqrt{5})/2$
	$(1/2,5/8)$	non	$-$	$\mathbb{Q}(\sqrt{65},\sqrt{-3495})$
	$(1/2,-5/8)$	yes	-40	$(6(65\pm 27\sqrt{5}))^3$
	$(4/3,35/27)$	yes	-60	$(3(470\pm 213\sqrt{5})^3(1\pm\sqrt{5})/2)$
	$(4/3,-35/27)$	non	$-$	$\mathbb{Q}(\sqrt{10},\sqrt{-9278})$
122	∞'	yes	-36	$-(4(102\pm 61\sqrt{3}))^3(-2\pm\sqrt{3})$
	$(-1,4)$	yes	-52	$(30(31\pm 9\sqrt{13}))^3$
	$(-1,-4)$	yes	-100	$(6(2927\pm 1323\sqrt{5}))^3$
	$(0,1)$	yes	$-3,-12$	$0,2\cdot 30^3$
	$(0,-1)$	yes	$-4,-16$	$12^3,66^3$
	$(1,2)$	yes	-88	$(60(155\pm 108\sqrt{2}))^3$
	$(1,-2)$	yes	-20	$(2(25\pm 13\sqrt{5}))^3$
	$(3/2,37/8)$	yes	-232	$(30(140989\pm 26163\sqrt{29}))^3$
	$(3/2,-37/8)$	non	$-$	$\mathbb{Q}(\sqrt{-15},\sqrt{1585})$
	$(2/3,37/27)$	yes	-4	12^3
	$(2/3,-37/27)$	non	$-$	$\mathbb{Q}(\sqrt{1258},\sqrt{-1598})$

N	point	CM	D	j or $\mathbb{Q}(j)$
129	∞'	yes	-75	$-(48(69 \pm 31\sqrt{5}))^3(\pm\sqrt{5})$
	$(-1, 3)$	yes	-123	$-(480(-461 \pm 72\sqrt{41}))^3(32 \pm 5\sqrt{41})$
	$(-1, -3)$	yes	-48	$4(15(30 \pm 17\sqrt{3}))^3$
	$(0, 2)$	yes	-147	$-3(480(362 \pm 79\sqrt{21}))^3(\pm\sqrt{21})$
	$(0, -2)$	yes	-8	20^3
	$(1, 1)$	yes	$-3, -27$	$0, -3 \cdot 160^3$
	$(1, -1)$	yes	-12	$2 \cdot 30^3$
	$(1/2, 3/8)$	yes	-51	$-(48(37 \pm 9\sqrt{17}))^3(-4 \pm \sqrt{17})$
	$(1/2, -3/8)$	non	$-$	$\mathbb{Q}(\sqrt{57}, \sqrt{-687})$
	$(-7/5, 383/125)$	yes	-3	0
	$(-7/5, -383/125)$	non	$-$	$\mathbb{Q}(\sqrt{1149}, \sqrt{-1059})$
	$(7/12, 383/1728)$	non	$-$	$\mathbb{Q}(\sqrt{-7}, \sqrt{-444783})$
	$(7/12, -383/1728)$	non	$-$	$\mathbb{Q}(\sqrt{85}, \sqrt{-347})$
133	∞'	non	$-$	$\mathbb{Q}(\sqrt{2}, \sqrt{69})$
	$(0, 1)$	yes	-27	$-3 \cdot 160^3$
	$(0, -1)$	yes	-19	-96^3
	$(1, 1))$	yes	-91	$(48(-227 \pm 63\sqrt{13}))^3$
	$(1, -1)$	yes	-12	$2 \cdot 30^3$
	$(3/5, 83/125)$	yes	-3	0
	$(3/5, -83/125)$	non	$-$	$\mathbb{Q}(\sqrt{-31}, \sqrt{-3651})$
134	∞'	yes	-52	$(30(31 \pm 9\sqrt{13}))^3$
	$(-1, 3)$	yes	-7	-15^3
	$(-1, -3)$	yes	-232	$(30(140989 \pm 26163\sqrt{29}))^3$
	$(0, 1))$	yes	-20	$(2(25 \pm 13\sqrt{5}))^3$
	$(0, -1)$	yes	$-3, -12$	$0, 2 \cdot 30^3$
	$(1, 1)$	yes	-8	20^3
	$(1, -1)$	yes	$-7, -28$	$-15^2, 255^3$
	$(-1/2, 7/8)$	non	$-$	$\mathbb{Q}(\sqrt{113}, \sqrt{-1271})$
	$(-1/2, -7/8)$	yes	-72	$(20(389 \pm 158\sqrt{6}))^3(-5 \pm 2\sqrt{6})$
146	∞'	yes	$-3, -12$	$0, 2 \cdot 30^3$
	$(-1, 1)$	yes	-36	$-(4(102 \pm 61\sqrt{3}))^3(-2 \pm \sqrt{3})$
	$(-1, -1)$	yes	-148	$(60(2837 \pm 468\sqrt{37}))^3$
	$(0, 1))$	yes	$-4, -16$	$12^3, 66^3$
	$(0, -1)$	yes	-24	$(12(9 \pm 7\sqrt{2}))^3(-1 \pm \sqrt{2})$
	$(1, 3)$	yes	-8	20^3
	$(1, -3)$	yes	-72	$-(20(389 \pm 158\sqrt{6}))^3(-5 \pm 2\sqrt{6})$
	$(2, 5)$	yes	-100	$(6(2927 \pm 1323\sqrt{5}))^3$
	$(2, -5)$	yes	-4	12^3
158	∞'	yes	-7	-15^3
	$(0, 1)$	yes	$-3, -12$	$0, 2 \cdot 30^3$
	$(0, -1)$	yes	-24	$(12(9 \pm 7\sqrt{2}))^3(-1 \pm \sqrt{2})$
	$(2, 1))$	yes	-232	$(30(140989 \pm 26163\sqrt{29}))^3$
	$(2, -1)$	yes	-148	$(60(2837 \pm 468\sqrt{37}))^3$
	$(1/2, 1/8)$	non	$-$	$\mathbb{Q}(\sqrt{1169}, \sqrt{-1247})$
	$(1/2, -1/8)$	yes	$-7, -28$	$-15^3, 255^3$

N	point	CM	D	j or $\mathbb{Q}(j)$
161	∞'	yes	-7	-15^3
	$(-1,7)$	yes	-91	$-(48(227\pm63\sqrt{13}))^3$
	$(-1,-7)$	yes	-483	$\mathbb{Q}(\sqrt{21},\sqrt{69})$
	$(1,1))$	yes	-115	$-(48(785\pm351\sqrt{5}))^3$
	$(1,-1)$	yes	-19	-96^3
	$(-1/2,35/8)$	non		$\mathbb{Q}(\sqrt{-7},\sqrt{32009})$
	$(-1/2,-35/8)$	yes	-112	$(15(2168\pm819\sqrt{7}))^3$
	$(-1/4,209/64)$	yes	-8	255^3
	$(-1/4,-209/64)$	non		$\mathbb{Q})(\sqrt{209},\sqrt{-1140391})$
177	∞'	yes	$--11$	32^3
	$(0,1)$	yes	-24	$(12(9\pm7\sqrt{2}))^3(-1\pm\sqrt{2})$
	$(0,-1)$	yes	-8	20^3
	$(3/2,17/8)$	yes	-267	$-(240(562501\pm59625\sqrt{89}))^3(-500\pm53\sqrt{89})$
	$(3/2,-17/8)$	non	$-$	$\mathbb{Q}(\sqrt{-23},\sqrt{2881})$
205	∞'	yes	-115	$-(48(785\pm351\sqrt{5}))^3$
	$(0,1)$	yes	-16	66^3
	$(0,-1)$	yes	-40	$(6(65\pm27\sqrt{5}))^3$
	$(-2,7)$	yes	-4	12^3
	$(-2,-7)$	yes	-1435	$\mathbb{Q}(\sqrt{5},\sqrt{21})$
206	∞'	yes	-24	$(12(9\pm7\sqrt{2}))^3(-1\pm\sqrt{2})$
	$(-1,1)$	yes	$-3,-12$	$0,2\cdot30^3$
	$(-1,-1)$	yes	-88	$(60(155\pm108\sqrt{2}))^3$
	$(0,1)$	yes	-40	$6(65\pm27\sqrt{5})$
	$(0,-1)$	yes	-20	$(2(25\pm13\sqrt{5}))^3$
	$(1/2,19/8)$	yes	-148	$(60(2837\pm468\sqrt{37}))^3$
	$(1/2,-19/8)$	non	$-$	$\mathbb{Q}(\sqrt{193},\sqrt{-27119})$
209	∞'	yes	-8	20^3
	$(0,2)$	yes	-19	-96^3
	$(0,-2)$	yes	-88	$(60(155\pm108\sqrt{2}))^3$
	$(-1/2,19/8)$	non	$-$	$\mathbb{Q}(\sqrt{-1007},\sqrt{902537})$
	$(-1/2,-19/8)$	yes	-627	$\mathbb{Q}(\sqrt{33},\sqrt{57})$
213	∞'	-51	yes	$-(48(37\pm9\sqrt{17}))^3(-4\pm\sqrt{17})$
	$(1,1)$	yes	-123	$(480(461\pm72\sqrt{41}))^3(-32\pm5\sqrt{41})$
	$(1,-1)$	yes	-11	-32^3
215	∞'	non	$-$	$\mathbb{Q}(\sqrt{2},\sqrt{47645})$
	$(1,1)$	yes	-235	$-(528(8875\pm3969\sqrt{5}))^3$
	$(1,-1)$	yes	-19	-96^3
	$(2,10)$	non	$-$	$\mathbb{Q}(\sqrt{85},\sqrt{3418805})$
	$(2,-10)$	yes	-115	$-(48(785\pm351\sqrt{5}))^3$
221	∞'	yes	-16	66^3
	$(0,1)$	yes	-43	-960^3
	$(0,-1)$	yes	-51	$-(48(37\pm9\sqrt{17}))^3(-4\pm\sqrt{17})$
	$(1/2,9/8)$	non	$-$	$\mathbb{Q}(\sqrt{1081},\sqrt{-779263})$
	$(1/2,-9/8)$	yes	-4	12^3

N	point	CM	D	j or $\mathbb{Q}(j)$
287	∞'	yes	-91	$-(48(227 \pm 63\sqrt{13}))^3$
	$(-2, 9)$	yes	-1435	$\mathbb{Q}(\sqrt{5}, \sqrt{41})$
	$(-2, -9)$	non	$-$	$\mathbb{Q}(\sqrt{8321}, \sqrt{2904137173})$
299	∞'	yes	-91	$-(48(227 \pm 63\sqrt{13}))^3$
	$(-1/2, 1/8)$	yes	-43	-960^3
	$(-1/2, -1/8)$	non		$\mathbb{Q}(\sqrt{1513}, \sqrt{-3325543})$

4.3 N is a product of three primes: $\mathrm{Gal}(\mathbb{Q}(j)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^3$.

N	point	CM	D	j or $\mathbb{Q}(j)$
154	∞'	yes	-40	$(6(65 \pm 27\sqrt{5}))^3$
	$(0, 2)$	yes	-24	$(12(9 \pm 7\sqrt{2}))^3(-1 \pm \sqrt{2})$
	$(0, -2)$	yes	-52	$(30(31 \pm 9\sqrt{13}))^3$
	$(1, 4)$	yes	-7	-15^3
	$(1, -4)$	yes	$-7, -28$	$-15^3, 255^3$
	$(2, 0)$	yes	-84	$\mathbb{Q}(\sqrt{3}, \sqrt{7})$
	$(-3/2, 77/8)$	non	$--$	$\mathbb{Q}(\sqrt{-143}, \sqrt{-185}, \sqrt{-455})$
	$(-3/2, -77/8)$	yes	-1540	$\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{11})$
	$(-1/3, 56/27)$	non	$--$	$\mathbb{Q}(\sqrt{7}, \sqrt{5 \cdot 11}, \sqrt{-479})$
	$(-1/3, -56/27)$	yes	$-28, -112$	$255^3, (15(2168 \pm 819\sqrt{7}))^3$
	$(4, 22)$	yes	-1848	$\mathbb{Q}(\sqrt{2}, \sqrt{21}, \sqrt{33})$
	$(4, -22)$	yes	-132	$\mathbb{Q}(\sqrt{3}, \sqrt{11})$
165	∞'	yes	-11	-32^3
	$(0, 3)$	yes	-195	$\mathbb{Q}(\sqrt{5}, \sqrt{13})$
	$(0, -3)$	yes	-51	$(48(37 \pm 9\sqrt{17}))^3(-4 \pm \sqrt{17})$
	$(1, 0)$	yes	-24	$(12(9 \pm 7\sqrt{2}))^3(-1 \pm \sqrt{2})$
	$(2, 5)$	yes	-435	$\mathbb{Q}(\sqrt{5}, \sqrt{29})$
	$(2, -5)$	yes	-35	$-(16(15 \pm 7\sqrt{5}))^3$
	$(-1/2, 15/8)$	non	$--$	$\mathbb{Q}(\sqrt{-15}, \sqrt{265}, \sqrt{1745})$
	$(-1/2, -15/8)$	yes	-120	$\mathbb{Q}(\sqrt{2}, \sqrt{5})$
	$(-3, 0)$	yes	-1155	$\mathbb{Q}(\sqrt{5}, \sqrt{21}, \sqrt{33})$
	$(2/3, 55/27)$	yes	$-11, -99$	$-32^3, (16(3751 \pm 653\sqrt{33}))^3(-23 \pm 4\sqrt{33})$
	$(2/3, -55/27)$	non	$--$	$\mathbb{Q}(\sqrt{-11}, \sqrt{47}, \sqrt{-661})$
	$(5/2, 99/8$	yes	-1320	$\mathbb{Q}(\sqrt{5}, \sqrt{6}, \sqrt{22})$
	$(5/2, -99/8)$	non	$--$	$\mathbb{Q}(\sqrt{-7}, \sqrt{33}, \sqrt{393})$
170	∞'	yes	-36	$-(4(102 \pm 61\sqrt{3}))^3(-2 \pm \sqrt{3})$
	$(-1, 2)$	yes	$-4, -16$	$12^3, 66^3$
	$(-1, -2)$	yes	-340	$\mathbb{Q}(\sqrt{5}, \sqrt{17})$
	$(0, 1)$	yes	$-4, -100$	$12^3, (6(2927 \pm 1323\sqrt{5}))^3$
	$(0, -1)$	yes	-15	$-(3(25 \pm 9\sqrt{5})/2)^3(-1 \pm \sqrt{5})/2$
	$(2, 5)$	yes	-280	$\mathbb{Q}(\sqrt{2}, \sqrt{5})$
	$(2, -5)$	yes	$-15, -60$	$-(3(25 \pm 9\sqrt{5})/2)^3(-1 \pm \sqrt{5})/2, -(3(470 \pm 213\sqrt{5}))^3(1 \pm \sqrt{5})/2$
	$(-1/2, 5/8)$	yes	-120	$\mathbb{Q}(\sqrt{2}, \sqrt{5})$
	$(-1/2, -5/8)$	non	$--$	$\mathbb{Q}(\sqrt{17}, \sqrt{-95}, \sqrt{65})$
	$(5/3, 38/27)$	non	$--$	$\mathbb{Q}(\sqrt{73}, \sqrt{19}, \sqrt{-5})$
	$(5/3, -38/27)$	yes	-4	12^3

N	point	CM	D	j or $\mathbb{Q}(j)$
186	∞'	yes	$-3,-12$	$0, 2\cdot 30^3$
	$(-1,-3)$	yes	-228	$\mathbb{Q}(\sqrt{3},\sqrt{19})$
	$(0,1)$	yes	-15	$-(3(25\pm 9\sqrt{5})/2)^3(-1\pm\sqrt{5})/2$
	$(0,-1)$	yes	-24	$(12(9\pm 7\sqrt{2}))^3(-1\pm\sqrt{2})$
	$(1,3)$	yes	-168	$\mathbb{Q}(\sqrt{6},\sqrt{14})$
	$(1,-3)$	yes	-120	$\mathbb{Q}(\sqrt{2},\sqrt{5})$
	$(2,9)$	yes	-708	$\mathbb{Q}(\sqrt{3},\sqrt{59})$
	$(2,-9)$	yes	$-15,-60$	$-(3(25\pm 9\sqrt{5})/2)^3(-1\pm\sqrt{5})/2, -(3(470\pm 213\sqrt{5}))^3(1\pm\sqrt{5})/2$
	$(-1/2,3/8)$	non	$-$	$\mathbb{Q}(\sqrt{-15},\sqrt{177},\sqrt{1257})$
	$(-1/2,-3/8)$	yes	$-12,-48$	$2\cdot 30^3, 4(15(30\pm 17\sqrt{3}))^3$
	$(-4/3,143/27)$	non	$-$	$\mathbb{Q}(\sqrt{37},\sqrt{-143},\sqrt{2077})$
	$(-4/3,-143/27)$	yes	-332	$\mathbb{Q}(\sqrt{3},\sqrt{31})$
230	∞'	yes	-40	$(6(65\pm 27\sqrt{5}))^3$
	$(0,1)$	yes	-20	$(2(25\pm 13\sqrt{5}))^3$
	$(0,-1)$	yes	-15	$-(3(25\pm 9\sqrt{5})/2)^3(-1\pm\sqrt{5})/2$
	$(1,5)$	yes	-520	$\mathbb{Q}(\sqrt{5},\sqrt{13})$
	$(1,-5)$	yes	-120	$\mathbb{Q}(\sqrt{2},\sqrt{5})$
	$(-2,5)$	yes	$-15,-60$	$-(3(25\pm 9\sqrt{5})/2)^3(-1\pm\sqrt{5})/2, -(3(470\pm 213\sqrt{5}))^3(1\pm\sqrt{5})/2$
	$(-2,-5)$	yes	-1380	$\mathbb{Q}(\sqrt{3},\sqrt{5},\sqrt{23})$
	$(3,35)$	non	$-$	$\mathbb{Q}(\sqrt{685},\sqrt{705},\sqrt{19043})$
	$(3,-35)$	yes	-180	$\mathbb{Q}(\sqrt{3},\sqrt{5})$
266	∞'	yes	-52	$(30(31\pm 9\sqrt{13}))^3$
	$(-1,1)$	yes	-84	$\mathbb{Q}(\sqrt{3},\sqrt{7})$
	$(-1,-1)$	yes	$-3,-12$	$0, 2\cdot 30^3$
	$(0,1)$	yes	-280	$\mathbb{Q}(\sqrt{2},\sqrt{5})$
	$(0,-1)$	yes	-40	$(6(65\pm 27\sqrt{5}))^3$
	$(-5/2,83/8)$	non	$-$	$\mathbb{Q}(\sqrt{1041},\sqrt{-415},\sqrt{105})$
	$(-5/2,-83/8)$	yes	-532	$\mathbb{Q}(\sqrt{17},\sqrt{19})$
285	∞'	yes	-51	$-(48(37\pm 9\sqrt{17}))^3(-4\pm\sqrt{17})$
	$(-1,4)$	yes	-15	$-(3(25\pm 9\sqrt{5})/2)^3(-1\pm\sqrt{5})/2$
	$(-1,-4)$	yes	-60	$-(3(470\pm 213\sqrt{5}))^3(1\pm\sqrt{5})/2$
	$(0,0)$	yes	$-3,-75$	$0, -(48(-69\pm 31\sqrt{5}))^3(\pm\sqrt{5})$
	$(3,24)$	non	$-$	$\mathbb{Q}(\sqrt{3},\sqrt{95},\sqrt{60197})$
	$(3,-24)$	yes	-240	$\mathbb{Q}(\sqrt{3},\sqrt{5})$
	$(-3/2,57/8)$	non		$\mathbb{Q}(\sqrt{-79},\sqrt{57},\sqrt{11985})$
	$(-3/2,-57/8)$	yes	-1995	$\mathbb{Q}(\sqrt{5},\sqrt{21},\sqrt{57})$
286	∞'	yes	-40	$(6(65\pm 27\sqrt{5}))^3$
	$(-1,4)$	yes	-52	$(30(31\pm 9\sqrt{13}))^3$
	$(-1,-4)$	yes	-88	$(60(155\pm 108\sqrt{2}))^3$
	$(5/2,143/8)$	non	$-$	$\mathbb{Q}(\sqrt{39},\sqrt{168917},\sqrt{232})$
	$(5/2,-143/8)$	non	$-$	$\mathbb{Q}(\sqrt{1841},\sqrt{-3367},\sqrt{37609})$
357	∞'	yes	-168	$\mathbb{Q}(\sqrt{6},\sqrt{14})$
	$(-1,4)$	non	$-$	$\mathbb{Q}(\sqrt{293},\sqrt{89997},\sqrt{21})$
	$(-1,-4)$	yes	-35	$-(16(15\pm 7\sqrt{5}))^3$

4.4 N is a product of four primes: $\mathrm{Gal}(\mathbb{Q}(j)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^4$.

N	point	CM	D	j or $\mathbb{Q}(j)$
390	∞'	yes	-5460	$\mathbb{Q}(\sqrt{3},\sqrt{5},\sqrt{7},\sqrt{11})$
	$(0,1)$	yes	-120	$\mathbb{Q}(\sqrt{2},\sqrt{5})$
	$(0,-1)$	yes	-420	$\mathbb{Q}(\sqrt{3},\sqrt{5},\sqrt{7})$
	$(1,2)$	yes	-660	$\mathbb{Q}(\sqrt{3},\sqrt{5},\sqrt{11})$
	$(1,-2)$	yes	$-4,-36$	$12^3, -(4(102\pm 61\sqrt{3}))^3(-2\pm\sqrt{3})$

References

[BG19] Francesc Bars and Josep González. Bielliptic modular curves $X_0^*(N)$ with square-free levels. *Math. Comp.*, 88(320):2939–2957, 2019.

[BH03] Matthew H. Baker and Yuji Hasegawa. Automorphisms of $X_0^*(p)$. *J. Number Theory*, 100(1):72–87, 2003.

[BP97] J. Bosma, W. Cannon and C. Playoust. The magma algebra system. i. the user language. *Math. Comp.*, 24:235–265, 1997.

[BS09] Nils Bruin and Michael Stoll. Two-cover descent on hyperelliptic curves. *Math. Comp.*, 78(268):2347–2370, 2009.

[Bue89] Duncan A. Buell. *Binary quadratic forms*. Springer-Verlag, New York, 1989. Classical theory and modern computations.

[Elk04] Noam D. Elkies. On elliptic K-curves. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 81–91. Birkhäuser, Basel, 2004.

[GL98] Josep González and Joan-C. Lario. Rational and elliptic parametrizations of **Q**-curves. *J. Number Theory*, 72(1):13–31, 1998.

[Has97] Yuji Hasegawa. Hyperelliptic modular curves $X_0^*(N)$. *Acta Arith.*, 81(4):369–385, 1997.

[HH96] Yuji Hasegawa and Ki-ichiro Hashimoto. Hyperelliptic modular curves $X_0^*(N)$ with square-free levels. *Acta Arith.*, 77(2):179–193, 1996.

Francesc Bars Cortina
Departament Matemàtiques, Edif. C, Universitat Autònoma de Barcelona
08193 Bellaterra, Catalonia
francesc@mat.uab.cat

Josep González Rovira
Departament de Matemàtiques, Universitat Politècnica de Catalunya EPSEVG,
Avinguda Víctor Balaguer 1, 08800 Vilanova i la Geltrú, Catalonia
josep.gonzalez@upc.edu

Xavier Xarles
Departament Matemàtiques, Edif. C, Universitat Autònoma de Barcelona
08193 Bellaterra, Catalonia
xarles@mat.uab.cat