A NOTE ON THE RATIONAL POINTS OF $X_0^+(N)$

CARLOS CASTAÑO-BERNARD

Abstract. Let C be the image of a canonical embedding ϕ of the Atkin-Lehner quotient $X_0^+(N)$ associated to the Fricke involution w_N. In this note we exhibit some relations among the rational points of C. For each $g = 3$ (resp. the first $g = 4$) curve C we found that there are one or more lines (resp. planes) in $\mathbf{P}^{g-1}$ whose intersection with C consists entirely of rational Heegner points or the cusp point, where N is prime. We also discuss an explanation of the first non-hyperelliptic exceptional rational point.

Contents

1. Introduction

Fix an integer $N > 1$ and let $X_0(N)$ be the moduli space of (ordered) pairs (E, E') of generalised elliptic curves E and E' linked by a cyclic isogeny $\varphi\colon E \longrightarrow E'$ of degree N. Consider the Atkin-Lehner quotient curve $X_0^+(N)$ defined by the involution w_N of $X_0(N)$ induced by mapping an isogeny $\varphi\colon E \longrightarrow E'$ to its dual $\hat{\varphi}\colon E' \longrightarrow E$. The quotient curve $X_0^+(N)$ has been studied by Galbraith [3], Mazur [8], and Momose [9], among others. Galbraith [3] studied the rational points of a canonical image $C \subset \mathbb{P}^{g_N^+-1}$ of $X_0^+(N)$, where g_N^+ is the genus of $X_0^+(N)$. In particular he exhibits explicit formulæ for C for prime conductors N for which the curve has genus $g \leq 5$. In each case he locates the cusp and rational CM points and, moreover, for $N = 137$ he exhibits a rational point which is neither a cusp point nor a CM point. In this note we exhibit an explicit set of hyperplanes $\{H_1, \dots H_s\}$ in $\mathbb{P}^{g_N^+-1}$ such that the intersection of each H_i with C (over the complex numbers) consist entirely of rational points of C, for each prime level N such that $g_N^+ = 3$, i.e. $N = 97$, 109, 113, 127, 139, 149, 151, 179, and 239, and the first prime level N such that $g_N^+ = 4$, i.e. $N = 137$.

For the latter case we found a further plane defined by 3 different CM points that contains the exceptional point.

The material is organised as follows. Section 2 introduces some basic results that we used to compute an equation for C. The collinearity relations are discussed in Section 3, while the coplanarity relations are discussed in Section 4.

Acknowledgments I would like to thank the referee of Experimental Mathematics for his/her insightful comments, which led to some significant improvements on a previous version of this paper. I would also like to thank Barry Mazur for his interesting remarks. I would like to heartily thank Jenny and Kenneth Cowan for their hospitality while preparing this paper.

2. Preliminaries

Let X be an algebraic curve defined over a field k and let Ω^1_X be the k-vector space of its holomorphic differentials. Also let $\{\omega_1, \dots \omega_g\}$ be a basis of Ω^1_X. The integer g is called the *genus* of X. The *canonical map* ϕ of X in projective space $\mathbb{P}^{g-1}$ is the morphism

$$X \xrightarrow{\quad\phi\quad} \mathbb{P}^{g-1}$$

$$P \longmapsto (\omega_1(P) : \cdots : \omega_g(P))$$

It is well-known that the canonical map ϕ is an embedding, if the genus g exceeds 2 and X is not hyperelliptic. Now fix an integer $N > 1$ and recall that

$$X_0(N) = \Gamma_0(N) \backslash \mathcal{H}^*,$$

where

$$\Gamma_0(N) = \left\{ \mu = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \ \gamma \equiv 0 \pmod{N} \right\}.$$

The Atkin-Lehner quotient curve $X_0^+(N)$ may be defined as the curve $X_0(N)$ modulo de action of the Fricke involution w_N, which is defined by

$$\tau \mapsto -\frac{1}{N\tau}.$$

Every holomorphic differential ω on $X_0(N)$ may be expressed uniquely as $\omega = f d\tau$, where $f(\tau) = \sum_{n=1}^{\infty} a(n) q^n$ (where $q = e^{2\pi\tau}$) is a modular form for $\Gamma_0(N)$ and of weight 2 , and conversely every modular form for $\Gamma_0(N)$ and of weight 2 gives rise to a holomorphic differential $\omega = f d\tau$.

In particular the canonical maps for $X_0^+(N)$ are of the form

$$X_0^+(N) \xrightarrow{\quad\phi\quad} \mathbb{P}^{g-1}$$

$$P \longmapsto (f_1(\tau) : \cdots : f_{g_N^+}(\tau)),$$

where $\{f_1, \ldots f_{g_N^+}\}$ constitute a basis of the $+1$-eigenspace $S_2^+(\Gamma_0(N))$ of the $\mathbb{C}$-vector space of modular forms $S_2(\Gamma_0(N))$ with respect to the action of the Fricke involution w_N. It is a classical fact that the vector space $S_2(\Gamma_0(N))$ has a basis consisting of modular forms with rational integer coefficients only. The same is true for the eigenspace $S_2^+(\Gamma_0(N))$. A set of equations with integral coefficients S for the curve C may be computed by finding combinations of powers of the q-expansions which yield identically zero series. Using the method described in Galbraith [2, p. 19], with the help of William Stein's computer package Hecke [12] and Pari [11] it is easy to compute these equations S for small genera, such as $g_N^+ = 3$ and $g_N^+ = 4$. (See also Elkies [1] for related methods and results on the computation of equations for modular curves.) In these two cases Galbraith [2] has shown that the curves $X_0^+(N)$ are non-hyperelliptic. So in fact C is a complete intersection. (See Examples IV.5.2.1 and IV.3.3.2 of Hartshorne [7].) Once we have a set of such equations S for C in practice it only takes only a brute-force search to obtain as many rational points on C as predicted by the theory of Complex Multiplication (see Gross [4]), the cusp rational point, or some other rational points that come as a fixed point of certain hyperelliptic involution. Sometimes there are more rational points than these "obvious" ones; Galbraith [2] has shown that there exist rational points in C that are neither cusps nor CM rational points for non-hyperelliptic $X_0^+(N)$ of genus at least 4.

From now on let us assume that N is prime. Then using Proposition 3.1 of Gross [5, p. 347] and the Riemann-Hurwitz formula we may see that

$$g_N^+ = \frac{1}{2}\left(g_N + 1 - H(N)\right),$$

where

$$H(N) = \begin{cases} \frac{1}{2}h(-4N), & \text{if } N \equiv 1 \pmod 4 \\ \frac{1}{2}(h(-N) + h(-4N)), & \text{otherwise,} \end{cases}$$

with $h(D)$ the class number of the imaginary quadratic order of discriminant D, and g_N is genus of $X_0(N)$, which is given by $g_N = \lfloor \frac{N+1}{12} \rfloor$, unless $N = 12q + 1$ when $g = q - 1$. In particular, by using explicit upper bounds on the class number $h(D)$ it may be found that the prime conductors N such that $X_0^+(N)$ has genus 3 are indeed $N = 97$, 109, 113, 127, 139, 149, 151, 179, and 239. and all these curves $X_0^+(N)$ are non-hyperelliptic. Similarly it may be found that there are exactly 5

prime numbers N such that $X_0^+(N)$ has genus $g = 4$, namely $N = 137$, 173, 199, 251, and 311.

3. Genus three: collinearity relations

Let us assume N is one of the 9 prime conductors N such that $X_0^+(N)$ has genus $g_N^+ = 3$. So the canonical map ϕ associated to a basis of modular forms with integral Fourier coefficients $\{g_1, g_2, g_3\}$ is an embedding ϕ defined over $\mathbb{Q}$ of C into the projective plane $\mathbb{P}^2$ such that its image C is of degree $4 = 2(g_N^+ - 1)$. So we may obtain a projective equation $F(X, Y, Z) = 0$ for the plane curve C by computing a (non-trivial) linear relation among the elements in the set

$$\{g_1^a g_2^b g_3^c \in S_8(\Gamma_0(N)) \colon a, b, c \in \mathbb{Z}_{\geq 0}, a + b + c = 4\}.$$

Note that a line L in the projective plane $\mathbb{P}^2$ will intersect the curve C in 4 points, if we take into account intersection multiplicities. So heuristically, the line defined by two rational points P_1 and P_2 of C (which is the tangent line of C at say P_1, in case $P_1 = P_2$) is not expected to intersect C in further rational points; the remaining points of intersection are expected to be in general two quadratic irrationals (one conjugate to the other). However, as we shall see it is possible to exhibit for each of the levels under consideration a non-empty set of lines $\{L_1, \dots L_s\}$ such that the intersection of each L_i with C (over the complex numbers) consists entirely of rational points. We describe these lines with the help of some diagrams below. Each diagram contains an equation for C and a table of rational points. Since all these rational points are CM points, or the cusp point, we label these rational points according to the discriminant D of the CM point. By the work of Galbraith [2] we know that in this case the relevant values of D are

$$D = -3, -4, -7, -8, -11, -12, -16,$$

$$-19, -27, -28, -43, -67, -163.$$

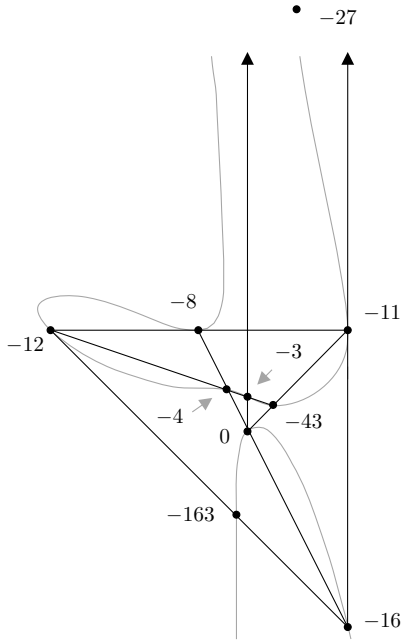
To ease notation we regard the cusp $i\infty$ labeled by $D = 0$. The discriminant D of each rational point of C exhibited was recognized in most cases by computing a suitable approximation of the image in C of the Heegner point of $X_0^+(N)$ of discriminant D so that it would be clear which of the rational points of C found previously corresponds to D.

Remark 3.1. Sometimes simply too many Fourier coefficients were necessary to obtain a suitable approximation for the image in C of a rational Heegner point, e.g. for $N = 97$. In these cases there were exactly two rational points of C, say P and Q, which needed further work to be labeled. We were able to resolve these kind of ambiguities by using a variant of a result of Ogg [10] which may be applied to describe the real locus $X_0^+(N)(\mathbb{R})$ in terms of certain indefinite binary quadratic forms.

More precisely, first we were able to locate (exactly) in a parametrisation π of $X_0^+(N)(\mathbb{R})$ all the Heegner (i.e. CM) rational points, and then by "walking along" a good polygonal approximation of the real locus of C in the direction determined by π, we paired the unmatched discriminants, say D_1 and D_2, with the points P and Q.

The diagrams are self explanatory; the intersection multiplicity ∂ of L_i with C at a specific point $P \in L_i \cap C$ is indicated only when necessary.

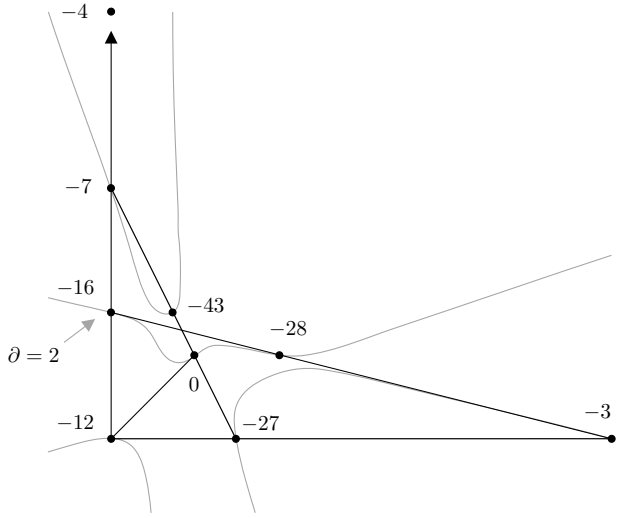
D	P
0	$(-4:-4:3)$
-3	$(-12:-5:9)$
-4	$(-9:-2:5)$
-8	$(-5:2:2)$
-11	$(1:1:1)$
-12	$(-6:1:1)$
-16	$(1:-6:1)$
-27	$(0:1:0)$
-43	$(-3:-3:4)$
-163	$(-13:-27:8)$



$N = 97$

$$-48Z^4 - 91Z^3Y - 15Z^2Y^2 + 4ZY^3 + 3Z^3X - 26Z^2YX + 25ZY^2X + 3Y^3X + 54Z^2X^2 + 29ZYX^2 + 18Y^2X^2 + 29ZX^3 + 11YX^3 + 4X^4 = 0$$

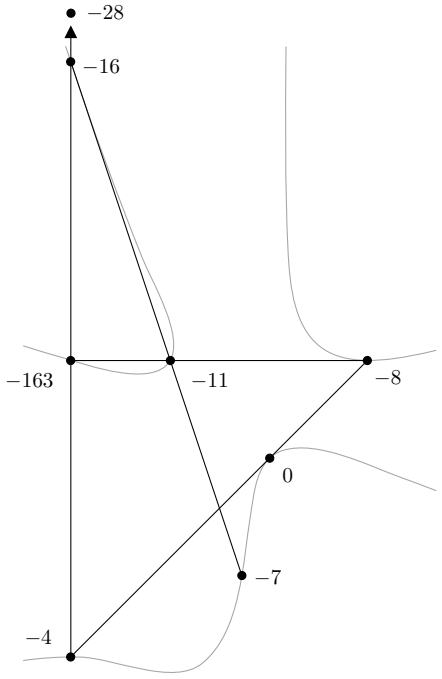
D	P
0	$(-2:-2:3)$
-3	$(11:-3:1)$
-4	$(0:1:0)$
-7	$(-3:4:1)$
-12	$(-3:-3:1)$
-16	$(-6,1,2)$
-27	$(1:-6:2)$
-28	$(5:-2:3)$
-43	$(-5:2:4)$



$N = 109$

$$24Z^4 + 39Z^3X + 25Z^2X^2 + 2ZX^3 - 2X^4 + 77Z^3Y + 122Z^2YX + 41ZYX^2 - 3YX^3 + 51Z^2Y^2 + 79ZY^2X + 23Y^2X^2 + 13ZY^3 + 9Y^3X = 0$$

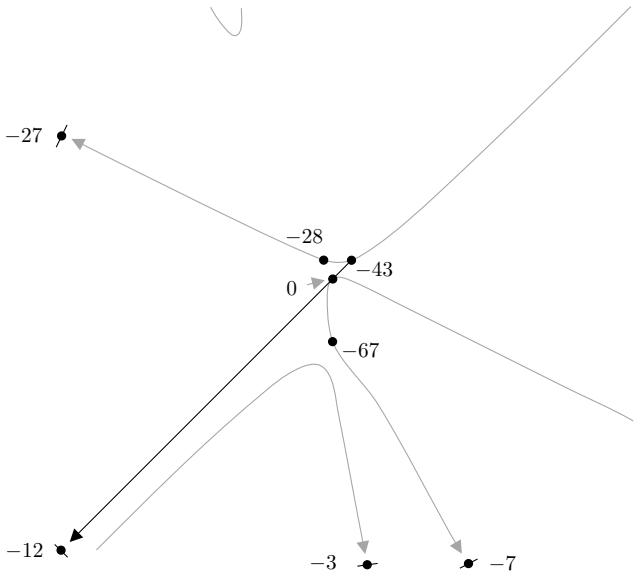
D	P
0	$(1:0:0)$
-4	$(1:2:-1)$
-7	$(-1:1:0)$
-8	$(1:1:-1)$
-11	$(0:1:0)$
-16	$(-1:0:1)$
-28	$(1:1:-2)$
-163	$(3:3:-1)$



$N = 113$

$$Y^2 + Y^3 + X + 3YX + 5Y^2X + 2Y^3X + 4X^2 + 8YX^2 + 7Y^2X^2 + 6X^3 + 7YX^3 + 3X^4 = 0$$

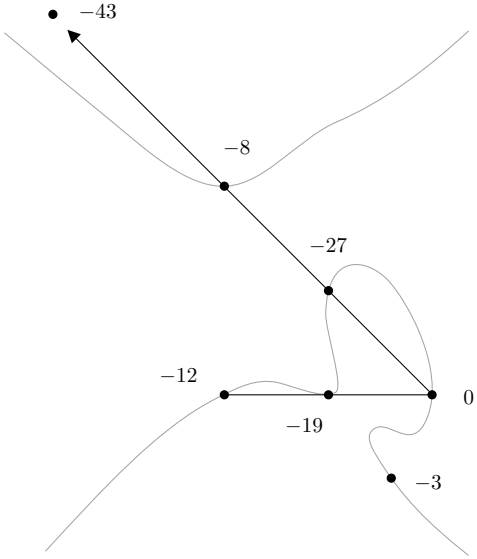
D	P
0	$(-1:-1:1)$
-3	$(-1:5:0)$
-7	$(-1:2:0)$
-12	$(1:1:0)$
-27	$(-2:1:0)$
-28	$(-3:0:2)$
-43	$(0:0:1)$
-67	$(-1:-4:1)$



$N = 127$

$$10X^4 + 17X^3Y + 45X^3Z - 12X^2Y^2 + 9X^2YZ + 81Z^2X^2 - 13XY^3 - 99XY^2Z - 81XYZ^2 + 54XZ^3 - 2Y^4 - 36ZY^3 - 162Y^2Z^2 - 135YZ^3 = 0$$

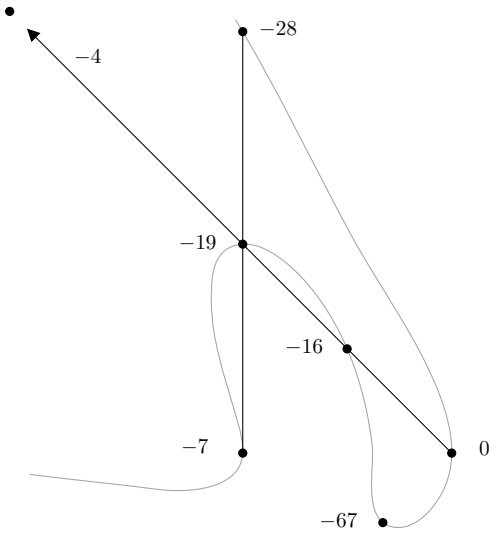
D	P
-3	$(-5:2:1)$
-8	$(1:1:-1)$
-12	$(-1:0:1)$
-19	$(-2:0:1)$
-27	$(2:1:-1)$
-43	$(0:-1:1)$



$N = 139$

$$X^2Y^2 + XY^3 - Y^4 + X^3Z + 3X^2YZ + 3XY^2Z - 2Y^3Z + 5X^2Z^2 + 8XYZ^2 - 2Y^2Z^2 + 8XZ^3 + 3YZ^3 + 4Z^4 = 0$$

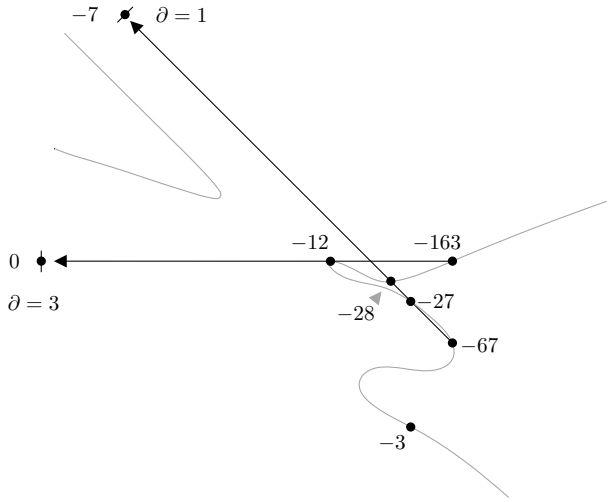
D	P
0	$(1:0:0)$
-4	$(0:-1:1)$
-7	$(-1:0:1)$
-16	$(2:1:-1)$
-19	$(1:1:-1)$
-28	$(1:2:-1)$
-67	$(-3:1:1)$



$N = 149$

$$X^2Y^2 + XY^3 + Y^4 + X^3Z + 2X^2YZ + 6XY^2Z + 4Y^3Z + 4X^2Z^2 + 7XYZ^2 + 7Y^2Z^2 + 4XZ^3 + 5YZ^3 + Z^4 = 0$$

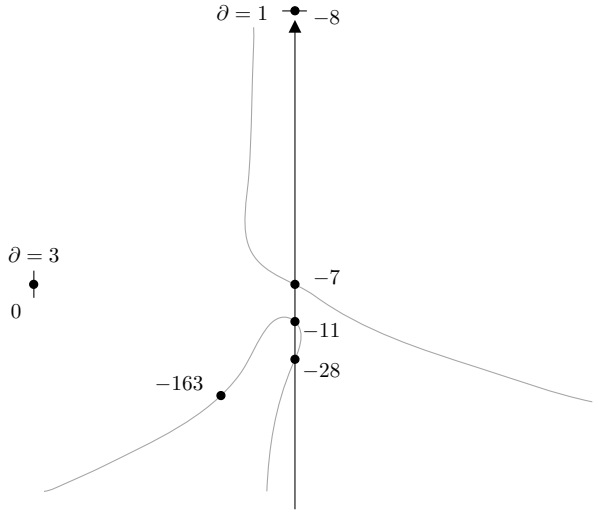
D	P
0	$(1:0:0)$
-3	$(0:-4:1)$
-7	$(-1:1:0)$
-12	$(-2:0:1)$
-27	$(0:-1:1)$
-28	$(1:1:-2)$
-67	$(1:-2:1)$
-163	$(1:0:1)$



$N = 151$

$$XY^3 + Y^4 - X^3Z - X^2YZ + 5XY^2Z + 8Y^3Z$$
$$-3X^2Z^2 + 6XYZ^2 + 20Y^2Z^2 + 17YZ^3 + 4Z^4 = 0$$

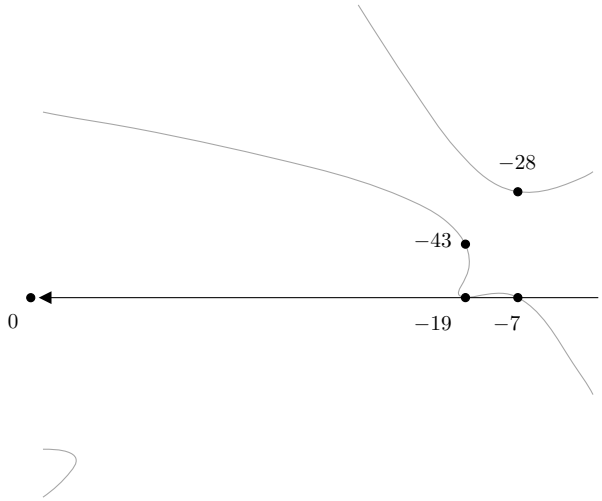
D	P
0	$(1:0:0)$
-7	$(-1:0:1)$
-8	$(0:1:0)$
-11	$(1:1:-1)$
-28	$(1:2:-1)$
-163	$(3:3:-1)$



$N = 179$

$$XY^3 + X^3Z + 2X^2YZ + 2XY^2Z + 2Y^3Z + 4X^2Z^2$$
$$+7XYZ^2 + 5Y^2Z^2 + 6XZ^3 + 7YZ^3 + 3Z^4 = 0$$

D	P
0	$(1:0:0)$
-7	$(-1:0:1)$
-19	$(-2:0:1)$
-28	$(-1:2:1)$
-43	$(-2:1:1)$



$N = 239$

$$X^2Y^2 - XY^3 - Y^4 + X^3Z - 2X^2YZ + 4XY^2Z + 2Y^3Z + 5X^2Z^2 - 5XYZ^2 + 8XZ^3 - YZ^3 + 4Z^4 = 0$$

4. Genus four: coplanarity relations

Now we will study the rational points of the first genus 4 Atkin-Lehner quotient curve $X_0^+(N)$. Again by the work of Galbraith [2] we know that C may be given as the intersection in $\mathbb{P}^3$ of

$$XY + WY + 2Y^2 + 2WZ + XZ + 6YZ + 3Z^2 = 0,$$

and

$$X^3 + WX^2 + 6X^2Z - 2XY^2 - 5XYZ + XZW + 13XZ^2 + 2Y^3 + 3WY^2 + W^2Y + 3WYZ - 6YZ^2 + ZW^2 - 4Z^2W + 14Z^3 = 0.$$

(See also Example IV.5.2.2 of Hartshorne [7].) By a brute-force search we may find in C the rational points

D	P
0	$[1:0:0:0]$
-4	$[2:-4:-3:2]$
-7	$[2:-1:-2:1]$
-8	$[-1:1:0:0]$
-11	$[1:1:-1:0]$
-16	$[2:0:-1:0]$
-19	$[1:-2:-1:1]$
-28	$[0:1:2:-1]$

We may also find in C the non-CM rational point $[19:2:-16:4]$.

The fact that the degree of C is 6 implies that the planes Π in $\mathbb{P}^3$ will intersect C (over a fixed algebraic closure of $\mathbb{Q}$) at 6 points, if we take into account multiplicities. So if Π is a plane defined by 3 rational points of C, then the other intersection points of Π with C are in general expected to be defined over a cubic extension of $\mathbb{Q}$. Hovever,

it turns out that there are 3 different planes Π_1, Π_2, and Π_3 in $\mathbb{P}^3$ such that each of these planes intersects C at exactly 6 rational points (with multiplicities):

- Π_1: $z = 0$:
$$2(0) + 2(-8) + (-11) + (-16)$$
- Π_2: $x + 2y + 3z + 1 = 0$
$$(-7) + (-8) + 2(-11) + (-16) + (-19)$$
- Π_3: $x + y + 3z = 0$
$$(0) + 2(-7) + (-11) + (-19) + (-28)$$

There are some other remarkable properties about the set of rational points of C. The set $\{-7, -11, -19\}$ is contained in one line, say, L_1, and also the set $\{-8, -11, -16\}$ is contained in one line, say, L_2. These two lines meet at $D = -11$ and, moreover, both are contained in plane Π_2. Finally, the 3 planes Π_1, Π_2, Π_3 meet at $D = -11$..

Another property worth mentioning is that the plane Π_e defined by the points $D = 0, -4, -11$
$$2x + 2y + 7z = 0$$
also contains the exceptional point, which is quite unexpected since this may not be heuristically explained by the small size of the coefficients of the Jacobi form involved. (See Gross, Kohnen and Zagier [6].) However, the remaining two points of intersection are not rational; these are two conjugate points defined over the real quadratic field of discriminant $\Delta = 8$.

5. Concluding remarks

It seems to be an open question whether these relations may have an interesting explanation, or else if these relations are only a consequence of an "accident" due to the small size of the genus g_N^+ of $X_0^+(N)$, perhaps related to the fact that the field K_f generated by the Fourier coefficients of the newform f of level N and "-1" sign in the functional equation of its Λ-function, is an abelian extension of $\mathbb{Q}$ for each prime N with $g_N^+ = 3$. It seems worthwhile to extend the above list of examples to higher levels, hoping that a more extensive experimental evidence may help to grasp the nature of this phenomenon. This may shed some more light into the nature of $X_0^+(N)(\mathbb{Q})$ for prime levels N, which is "extremely interesting", as expressed in Mazur [8].

References

1. Noam D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 21–76.

2. S. D. Galbraith, *Equations for modular curves*, Oxford Ph.D. thesis (1996), v+91.
3. ———, *Rational points on $X_0^+(p)$*, Experiment. Math. **8** (1999), no. 4, 311–318.
4. B. H. Gross, *Heegner points on $X_0(N)$*, Modular forms (Durham, 1983), Horwood, Chichester, 1984, pp. 87–105.
5. ———, *Heegner points and the modular curve of prime level*, J. Math. Soc. Japan **39** (1987), no. 2, 345–362.
6. B. H. Gross, W. Kohnen, and D. B. Zagier, *Heegner points and derivatives of L-series. II*, Math. Ann. **278** (1987), no. 1–4, 497–562.
7. R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.
8. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).
9. F. Momose, *Rational points on the modular curves $X_0^+(N)$*, J. Math. Soc. Japan **39** (1987), no. 2, 269–286.
10. A. P. Ogg, *Real points on Shimura curves*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 277–307.
11. The PARI Group, Bordeaux, *PARI/GP, Version 2.1.5*, http://www.parigp-home.de/.
12. W. A. Stein, *HECKE: Modular Forms Calculator, Version 0.4*, http://modular.fas.harvard.edu/Tables/hecke-cpp.html.

E-mail address: ccastanobernard@gmail.com