Rational Points on $X_0^+(p)$

Steven D. Galbraith

CONTENTS

We study the rational points on $X_0^+(p) = X_0(p)/W_p$. It is known that there are rational points corresponding to cusps and elliptic curves with complex multiplication (CM). We use computational methods to exhibit exceptional rational points on $X_0^+(p)$ for $p = 73, 103, 137, 191$ and 311. We also provide the j-invariants of the corresponding non-CM quadratic $\mathbb{Q}$-curves.

1. INTRODUCTION

Rational points on modular curves have great arithmetic significance. The most famous result in this area is the proof [Mazur 1977] that, for $N \geq 13$, the only rational points on $X_1(N)$ are cusps. This result then provides the classification of torsion subgroups of elliptic curves over $\mathbb{Q}$.

Mazur also studied the modular curves $X_0(p)$ and listed all the primes p such that $X_0(p)$ has rational points which are not cusps. His work was continued in [Kenku 1981], and by others, until the situation for $X_0(N)$ was fully understood. The general philosophy is that the rational points on modular curves should correspond only to cusps or elliptic curves with complex multiplication (CM). For most families of modular curves there will also be a few cases where certain unexpected rational points arise. We call these points *exceptional* rational points.

The classic example here is the curve $X_0(37)$: it is hyperelliptic and has two rational cusps. The hyperelliptic involution maps each cusp to a noncuspidal rational point and these points do not arise from elliptic curves with complex multiplication. We will see further examples of how the hyperelliptic involution forces the existence of such exceptional rational points.

One may consider the modular curves obtained by taking quotients of $X_0(N)$ by Atkin–Lehner involutions [Atkin and Lehner 1970]. These curves should also follow the general philosophy outlined above. Some of these curves have great arithmetic

The author thanks the EPSRC and the Association of Commonwealth Universities for their support.

Mathematics Subject Classification (1991): Primary 14G05; Secondary 11G18, 14G35

Keywords: modular curves, Heegner points, Q-curves

1058-6458/1999 $0.50 per page

significance; thus, for example, the modular curve $X_{\mathrm{split}}(p)$ is isomorphic to

$$X_0(p^2)/W_{p^2}.$$

Momose [1984; 1986; 1987] has studied the case $X_0^+(N) = X_0(N)/W_N$ when N is composite and has shown that, if N has a prime factor $p \geq 11$ satisfying certain conditions, there are no exceptional rational points. The methods of Mazur and Momose do not apply to the case when N is a prime number. The case $N = p$ is singled out on page 145 of [Mazur 1977] as "extremely interesting".

The approach in this paper is to construct explicit equations for $X_0^+(p)$, to locate the predicted rational points on these equations, and then to search for any extra rational points. We find that the genus 2 curves $X_0^+(p)$, when $p = 73$, 103 and 191, have an exceptional rational point which is forced to exist by the hyperelliptic involution. Elkies has also studied this situation using similar methods and has independently found these hyperelliptic examples (see [Elkies 1998] for his description of the case $X_0^+(191)$). Indeed, Elkies conjectured that exceptional points on $X_0^+(p)$ only arise in the hyperelliptic case. In this paper we disprove his conjecture by finding an exceptional rational point on each of the nonhyperelliptic genus 4 curves $X_0^+(137)$ and $X_0^+(311)$.

2. ELLIPTIC CURVES AND HEEGNER POINTS

Let N be a positive integer (later we will specialise to the case $N = p$ prime). The modular curve $X_0(N)$ parametrises elliptic curves with a cyclic subgroup of order N.

Over $\mathbb{C}$, elliptic curves are $E_\tau = \mathbb{C}/\langle 1, \tau\rangle$ where $\tau \in \mathcal{H} := \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ and where τ is determined up to action by $\mathrm{SL}_2(\mathbb{Z})$. Consider the congruence subgroup $\Gamma_0(N) = \left\{\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) : a, b, c, d \in \mathbb{Z}, ad - bc = 1, c \equiv 0 \pmod{N}\right\}$ which acts on the extended upper half plane $\mathcal{H}^* := \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. The modular curve $X_0(N)(\mathbb{C})$ is the Riemann surface given by the quotient space $\Gamma_0(N)\backslash\mathcal{H}^*$. The points $\tau \in \mathbb{Q} \cup \{\infty\}$ correspond to "generalised" elliptic curves and these points are called "cusps". The other points τ of $X_0(N)$ correspond to elliptic curves $E_\tau = \mathbb{C}/\langle 1, \tau\rangle$ with the fixed cyclic N-element subgroup $C_\tau = \langle \frac{1}{N}, \tau\rangle$.

Given a point (E, C) of $X_0(N)$ we may consider the unique isogeny having kernel C, namely, $\pi : E \to E' = E/C$. For (E_τ, C_τ) one finds that E' is $E_{W_N(\tau)}$ where W_N is the Atkin–Lehner involution $W_N := \left(\begin{smallmatrix} 0 & -1 \\ N & 0\end{smallmatrix}\right)$. We define $X_0^+(N) = X_0(N)/W_N$.

There are cusps of $X_0(N)$ for each d dividing N and they correspond to generalised elliptic curves. On $X_0(p)$ there are just two cusps and they are both rational. We refer to [Ogg 1973] for further details.

The endomorphism ring of an elliptic curve $E_\tau = \mathbb{C}/\langle 1, \tau\rangle$ is $\mathrm{End}(E) = \{\lambda \in \mathbb{C} : \lambda\langle 1, \tau\rangle \subseteq \langle 1, \tau\rangle\}$. It is easily seen that $\mathrm{End}(E)$ is either $\mathbb{Z}$ or an order in an imaginary quadratic field.

A Heegner point (see [Birch 1969] or [Gross 1984]) is a noncusp point of $X_0(N)$ represented by (E, C) where E has complex multiplication by some order $\mathcal{O}$ and where $E' = E/C$ also has complex multiplication by the same order $\mathcal{O}$.

Orders in imaginary quadratic fields are uniquely determined by their discriminant D via $\mathcal{O} = \mathbb{Z}[(D+\sqrt{D})/2]$ in $K = \mathbb{Q}(\sqrt{D})$. The conductor of an order $\mathcal{O}$ in K is $f = [\mathcal{O}_K : \mathcal{O}]$ and this may be shown to be the largest integer f such that $D/f^2 \equiv 0, 1 \pmod{4}$.

If E_τ has complex multiplication by an order of discriminant D then τ is an imaginary quadratic number satisfying some equation $A\tau^2 + B\tau + C$ where $(A, B, C) = 1$ and $B^2 - 4AC = D$. The isomorphism classes of such CM elliptic curves E_τ correspond to $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of quadratic forms $AX^2 + BXY + CY^2$. It follows that the number of isomorphism classes of elliptic curves with complex multiplication by $\mathcal{O}$ is the class number $h_{\mathcal{O}}$ of $\mathrm{Pic}(\mathcal{O})$ (here $\mathrm{Pic}(\mathcal{O})$ is the group of classes of invertible $\mathcal{O}$-submodules of K, which is simply the ideal class group of K when $\mathcal{O}$ is a maximal order).

The following result is well-known and we refer to [Gross 1984] (also consult [Lang 1987, p. 90]) for the details.

Theorem 2.1. *The pair* $(E_\tau, C_\tau) = (\mathbb{C}/\langle 1, \tau\rangle, \langle \frac{1}{N}, \tau\rangle)$ *represents a Heegner point on* $X_0(N)$ *with complex multiplication by* $\mathcal{O}$ *if and only if there are integers* A, B, C *such that* $(NA, B, C) = (A, B, NC) = 1$, *disc*$(\mathcal{O}) = B^2 - 4NAC$ *and* $NA\tau^2 + B\tau + C = 0$.

Suppose E has complex multiplication by the order $\mathcal{O}$ of discriminant D in $K = \mathbb{Q}(\sqrt{D})$. Let $H_{\mathcal{O}}/K$ be the ring class field asociated with $\mathcal{O}$ (i.e., $H_{\mathcal{O}}/K$ is the Hilbert class field when $\mathcal{O}$ is a maximal order).

Then $H_{\mathcal{O}}/\mathbb{Q}$ is a Galois extension and the theory of complex multiplication states that E is defined over $H_{\mathcal{O}}$ and that

$$[H_{\mathcal{O}} : K] = [\mathbb{Q}(j(E)) : \mathbb{Q}] = h_{\mathcal{O}}.$$

It is necessary to study the action of $\mathrm{Gal}(H_{\mathcal{O}}/\mathbb{Q})$ on Heegner points (E, C). For this purpose it is best to use the notation of [Gross 1984], and hence we restrict attention to the case where the conductor f of $\mathcal{O}$ is coprime to N (which is no restriction for square-free N).

Gross writes a Heegner point as $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$, where $\mathfrak{n}$ is an invertible $\mathcal{O}$-module such that $\mathcal{O}/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$, and where $[\mathfrak{a}]$ is the class of an invertible $\mathcal{O}$-module in the class group $\mathrm{Pic}(\mathcal{O})$. Translating $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ to the notation (E, C) used earlier in this paper is accomplished by setting $E = \mathbb{C}/\mathfrak{a}$ and $C = \mathfrak{n}^{-1}\mathfrak{a}/\mathfrak{a}$. Note that the condition $\mathcal{O}/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$ combined with the condition $(f, N) = 1$ implies that every prime p dividing N must split or ramify in K.

Complex conjugation (which we denote by $\rho \in \mathrm{Gal}(K/\mathbb{Q})$) maps $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ to $(\mathcal{O}, \mathfrak{n}^{\rho}, [\mathfrak{a}]^{-1})$. To analyse the action of $\mathrm{Gal}(H_{\mathcal{O}}/K)$ we need to utilise the Artin symbol $\sigma : \mathrm{Pic}(\mathcal{O}) \to \mathrm{Gal}(H_{\mathcal{O}}/K)$. One sees from [Gross 1984, (4.2)] that

$$(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])^{\sigma[\mathfrak{b}]} = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}^{-1}]).$$

3. RATIONAL POINTS FROM HEEGNER POINTS

The involution W_N maps $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ to $(\mathcal{O}, \mathfrak{n}^{\rho}, [\mathfrak{a}\mathfrak{n}^{-1}])$. Therefore Heegner points give rise to $H_{\mathcal{O}}$-points on $X_0^+(N)$. To obtain rational points in this way it follows that the elements of $\mathrm{Gal}(H_{\mathcal{O}}/\mathbb{Q})$ must fix the pair $\{(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]), (\mathcal{O}, \mathfrak{n}^{\rho}, [\mathfrak{a}\mathfrak{n}^{-1}])\}$. This condition severely restricts the possibilities for $\mathcal{O}$. The categorisation is given in the following theorem.

Theorem 3.1. *Let $\mathcal{O}$ be an order in K of discriminant D and conductor f. Suppose $(N, f) = 1$. Then a Heegner point on $X_0^+(N)$ associated to $\mathcal{O}$ is a rational point if and only if one of the following conditions holds.*

1. $h_{\mathcal{O}} = 1$ *and every prime p dividing N either splits or ramifies in K.*
2. $h_{\mathcal{O}} = 2$ *and every prime p dividing N ramifies in K (i.e., p divides D), and the corresponding ideal $\mathfrak{n}$ is not a principal ideal.*

Proof. The ideal class group acts transitively and so the class number $h_{\mathcal{O}}$ must be at most 2. When $h_{\mathcal{O}} = 1$ then E and E' are defined over $\mathbb{Q}$ and it follows that $E \cong E'$.

When $h_{\mathcal{O}} = 2$ then any nontrivial element $\sigma \in \mathrm{Gal}(H_{\mathcal{O}}/K)$ maps $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ to $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}^{-1}])$ where $\mathfrak{b}$ is nonprincipal in $\mathrm{Pic}(\mathcal{O})$. It follows that $\mathfrak{n} = \mathfrak{n}^{\rho}$ or, in other words, that N is ramified in K. □

For future reference we list all the discriminants D of orders $\mathcal{O}$ having class number 1 and 2. The class number 1 discriminants are $\{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}$, whereas the class number 2 discriminants are $D \in \{-15, -20, -24, -32, -35, -36, -40, -48, -51, -52, -60, -64, -72, -75, -88, -91, -99, -100, -112, -115, -123, -147, -148, -187, -232, -235, -267, -403, -427\}$.

We now specialise to the case where N is a prime number p. Note that $X_0^+(p)$ always has one rational cusp so that, when the genus of $X_0^+(p)$ is zero, there will always be an infinite number of rational points. This is the case for $p \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}$.

The genus of $X_0^+(p)$ is one for $p \in \{37, 43, 53, 61, 79, 83, 89, 101, 131\}$ and it is well-known (see, for instance, [Cremona 1992]) that $X_0^+(p)$ is a rank one elliptic curve in these cases.

Theorem 3.2. *Let p be a prime such that the genus of $X_0^+(p)$ is at least 2. Then $X_0^+(p)$ has no $\mathbb{Q}$-rational Heegner points associated with orders of class number 2. Furthermore, if a noncuspidal $\mathbb{Q}$-rational point of $X_0^+(p)$ is neither a Heegner point nor the image of a rational point on $X_0(p)$ then the corresponding elliptic curves E and $E' = E/C$ do not have complex multiplication and are not defined over $\mathbb{Q}$.*

Proof. By theorem 3.1, a class number 2 Heegner point will arise only for those D with p dividing D. From the list above of class number 2 discriminants one sees that this never occurs for primes p such that $X_0^+(p)$ has genus at least 2.

To prove the second claim, let (E, C) correspond to such a $\mathbb{Q}$-rational point of $X_0^+(p)$. In other words, we have a p-isogeny $\pi : E \to E' = E/C$ such that each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ maps $E \xrightarrow{\pi} E'$ to either $E \xrightarrow{\pi} E'$ or $E' \xrightarrow{\hat{\pi}} E$.

If E is defined over $\mathbb{Q}$ then it follows that we have either a Heegner point of class number 1 or a rational point of $X_0(p)$.

If E is not defined over $\mathbb{Q}$ then both E and E' must be conjugate and defined over a quadratic field. They cannot have CM, as the first half of the theorem shows there are no Heegner points of class number 2. □

From [Mazur 1977] it is known that $X_0(p)$ has noncuspidal rational points only when $p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$. Of these, when $p \in \{19, 43, 67, 163\}$ there is just one noncuspidal rational point and it is a Heegner point.

A rational point on $X_0^+(p)$ which is not a cusp, a Heegner point or rational point of $X_0(p)$ will be called exceptional.

4. EQUATIONS FOR $X_0^+(p)$

In [Galbraith 1996], many explicit equations (over $\mathbb{Q}$) for modular curves $X_0(N)$ and their quotients by Atkin–Lehner involutions were computed. Methods for dealing with the hyperelliptic cases are fairly well-known (see any of [Murabayashi 1992; Hasegawa 1995; Galbraith 1996]), so we omit the details.

In order to obtain equations for the nonhyperelliptic curves, the canonical embedding associated with the holomorphic differentials is used. This method of constructing equations for $X_0(N)$ has also been used by [Shimura 1995]. The canonical embedding (see [Hartshorne 1977, IV.5]) of a nonhyperelliptic curve C of genus $g > 2$ is the map

$$\begin{array}{rccl} \varphi: & C & \longrightarrow & \mathbb{P}^{g-1}, \\ & P & \longmapsto & [\omega_1(P), \dots, \omega_g(P)], \end{array}$$

where $\{\omega_1, \dots, \omega_g\}$ is a $\mathbb{C}$-basis for the vector space $\Omega^1(C)$ of holomorphic differentials on C. In the case of $X_0(N)$ it is well-known (see [Shimura 1971]) that the vector space $\Omega^1(X_0(N))$ is isomorphic to the space $S_2(\Gamma_0(N))$ of weight 2 cusp forms of level N. Suppose now that $X_0(N)$ is a nonhyperelliptic curve of genus $g > 2$ and choose a basis $\{f_1(\tau), \dots, f_g(\tau)\}$ for $S_2(\Gamma_0(N))$. Then the canonical embedding of $X_0(N)$ is the map

$$\begin{array}{rccl} \varphi: & \Gamma_0(N)\backslash\mathcal{H}^* & \longrightarrow & \mathbb{P}^{g-1}(\mathbb{C}), \\ & \tau & \longmapsto & [f_1(\tau) : \cdots : f_g(\tau)]. \end{array} \tag{4–1}$$

If the forms $f_j(\tau)$ are represented as q-expansions (i.e., taking the local parameter $q(\tau) = \exp(2\pi i\tau)$ at the cusp ∞ and writing $f = \sum_{n\geq 1} a_n q(\tau)^n)$ then the right hand side of equation (4–1) is a curve given by some equations in the f_j. These equations may be thought of as giving relations between the coefficients of the q-expansions.

The method used in [Galbraith 1996] is to begin by taking a basis for $S_2(\Gamma_0(N))$ consisting of forms whose q-expansions at infinity have rational integer coefficients (so that the model we obtain is defined over $\mathbb{Q}$). There are various methods available to construct such a basis; the easiest way to proceed is to consult the tables [Cohen et al. 1992] or [Stein n.d.] (I have also used some data kindly provided by Michael Müller in Essen). Once we possess a suitably represented choice of $\{f_1, \dots f_g\}$ as truncated q-expansions, it is necessary to find linear relations between the monomials of degree d in the f_j (for choices of d between 2 and 4, depending on the genus). This computation may be performed by formally manipulating the q-expansions, and the relations may be found by linear algebra on the q-expansion coefficients. The relations obtained give projective equations for the image of the canonical map of $X_0(N)$.

Equations for $X_0^+(p)$, or, more generally, any

$$X_0(N)/\langle W_{p_1}, \dots, W_{p_m}\rangle,$$

may be found using the methods described above, by restricting to the subset of $S_2(\Gamma_0(N))$ consisting of those forms which have eigenvalue $+1$ with respect to W_p.

As an example, to compute an equation for the genus 4 curve $X_0^+(137)$, we take a basis for the weight 2 cusp forms on $\Gamma_0(137)$ which have eigenvalue $+1$ under W_{137}. The q-expansions (as taken from [Cohen et al. 1992]) are

$$\begin{aligned} w &= q - q^2 + q^3 - q^4 - 3q^5 + \cdots, \\ x &= q^2 - 2q^3 - 2q^4 + 3q^5 + \cdots, \\ y &= -2q^3 + q^4 + 3q^5 + 3q^6 + \cdots, \\ z &= q^3 - 2q^5 - 2q^6 + \cdots. \end{aligned}$$

We expect the canonical embedding of a genus 4 curve to be the complete intersection of a quadric surface with a cubic surface in $\mathbb{P}^3$. Hence we find the formal relations

$$wy + 2wz + xy + xz + 2y^2 + 6yz + 3z^2 = 0,$$

and

$$w^2y + w^2z + wx^2 + wxz + 3wy^2 + 3wyz - 4wz^2 + x^3 \\ + 6x^2z - 2xy^2 - 5xyz + 13xz^2 + 2y^3 - 6yz^2 + 14z^3 = 0.$$

For further details of these computations we refer to [Galbraith 1996]. Note that we obtain equations with very small coefficients using this method.

When the genus is large, the image in $\mathbb{P}^{g-1}$ may become quite complicated to describe. In [Galbraith 1996] we demonstrated that the image of the canonical map of the genus 5 curves $X_0^+(181)$ and $X_0^+(227)$ is not a complete intersection. When the genus is 6 or more the image of the canonical embedding is never a complete intersection. Hence we restrict attention, in this paper, to the case of genus 2, 3, 4 and 5.

The image of the canonical embedding is a nonsingular curve. The hyperelliptic curves we consider will always be given in the form

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

where $p(x)$ is a monic polynomial with integer coefficients and degree $2g+2$. Above the singular point ∞ on the projective model there are two rational points.

5. METHODS

We have obtained equations for $X_0^+(p)$ which are parametrised by modular forms or functions with explicit expansions in $q(\tau) = \exp(2\pi i\tau)$. We may locate the cusp simply by considering the order of vanishing of the various forms at ∞. We then search for rational points of small height on the model. Comparing the number of points found with the number of Heegner points reveals whether an exceptional rational point has been found.

If so, we find the Heegner points on the model by evaluating the modular forms at suitable values of τ (i.e., roots of $NA\tau^2 + B\tau + C$ as described in Theorem 2.1) and then taking ratios and rounding to get rational numbers. We use 150 to 1000 terms in the q-expansion to recognise the rational points (when $|D|$ is small the convergence of the q-expansions is poor).

Our search method is very crude, merely trying all rational points of naïve projective height less than some chosen bound B. For the genus 2 curves Colin Stahlke has kindly searched up to $B = 10^6$, for the genus 3 curves we search over coprime integers $|x|, |y|, |z| \leq B = 300$ (the choice for B is determined by considerations of computer time rather than any theoretical ideas). For the genus 4 cases we eliminate a variable to get a plane curve and then perform the search as above with $B = 300$. For the genus 5 cases we also eliminate variables as above, and search with $B = 300$, except for the case of $p = 227$, for which the geometry is more complicated, where we took $B = 100$. Searching for points on curves of genus 6 or more would be very difficult and this explains why we restrict to the case of genus at most 5 in this article.

In some cases we find exceptional rational points using this search strategy. We expect that we have found all the rational points on our models for $X_0^+(p)$, but since the rank of $J_0^+(p)$ is equal to the genus of $X_0^+(p)$, there are no general computational methods available to prove that we have found all points.

To compute the j-invariant of the corresponding $\mathbb{Q}$-curve we use the method of [Elkies 1998] and a fair amount of computational effort.

6. RESULTS

Table 1 lists the cases where exceptional rational points have been found. For a more complete list of Heegner points on $X_0^+(p)$, see [Galbraith 1996]. We have checked, in total, the 23 cases $p \in \{67, 73, 97, 103, 107, 109, 113, 127, 137, 139, 149, 151, 157, 167, 173, 179, 181, 191, 227, 239, 251, 263, 311\}$, which are all the values of p for which $X_0^+(p)$ has genus $2 \leq g \leq 5$.

There are strong similarities between the j-invariants shown in Table 1 and the j-invariants of the CM $\mathbb{Q}$-curves. In analogy with the results of [Gross and Zagier 1985] for singular moduli, the norms $N(j)$ over $\mathbb{Q}$ are “nearly cubes”, whereas the norms $N(j-1728)$ are squares; see [González 1998] for partial results in this context. Moreover, if we write

$$j = a + b\sqrt{d},$$

the coefficients b are very smooth and are divisible by p; see Table 2.

$X_0^+(73)$	$y^2 = x^6 + 2x^5 + x^4 + 6x^3 + 2x^2 - 4x + 1$ $\qquad P = (\frac{1}{2}, -\frac{5}{8})$ cusp ∞ $\quad D = -8$ $(0,-1)$ $\quad D = -19$ $(0,1)$ $D = -3$ $(\frac{1}{2}, \frac{5}{8})$ $\quad D = -12$ ∞ $\quad D = -27$ $(-1, 1)$ $D = -4$ $(-1, -1)$ $\quad D = -16$ $(1, -3)$ $\quad D = -67$ $(1, 3)$ $j = \bigl(814500172065991097081405 25 \pm 147586922701401551573491 65\sqrt{-127}\bigr)/2^{74}$ $N(j) = 2^{-74} \cdot 3^6 \cdot 5^2 \cdot 13967^3 \cdot 33191^3$ $N(j - 1728) = 2^{-74} \cdot 3^6 \cdot 7^4 \cdot 19^2 \cdot 23^4 \cdot 94843933^2$
$X_0^+(103)$	$y^2 = x^6 + 6x^5 + 5x^4 + 2x^3 + 2x^2 + 1$ $\qquad P = (2, 19)$ cusp ∞ $D = -3$ $(2, -19)$ $\quad D = -12$ $(0, -1)$ $\quad D = -43$ $(-1, -1)$ $D = -11$ $(0, 1)$ $\quad D = -27$ $(-1, 1)$ $\quad D = -67$ ∞ $j = 35982263935929364331785036841779200 \pm 6699086354721249807317015327539 20\sqrt{5 \cdot 577}$ $N(j) = 2^{30} \cdot 3^6 \cdot 5^3 \cdot 19^2 \cdot 173^3 \cdot 158341^3 \cdot 999049^3$ $N(j - 1728) = 2^{12} \cdot 3^{12} \cdot 23^4 \cdot 68358487^2 \cdot 15947995498069^2$
$X_0^+(137)$	$xy + wy + 2y^2 + 2wz + xz + 6yz + 3z^2 = 0$ $x^3 + wx^2 + 6x^2z - 2xy^2 - 5xyz + xzw$ $\quad + 13xz^2 + 2y^3 + 3wy^2 + w^2y + 3wyz - 6yz^2 + zw^2 - 4z^2w + 14z^3 = 0$ $\qquad P = [19{:}2{:}{-16}{:}4]$ cusp $[1{:}0{:}0{:}0]$ $\quad D = -8$ $[-1{:}1{:}0{:}0]$ $\quad D = -19$ $[1{:}{-2}{:}{-1}{:}1]$ $D = -4$ $[2{:}{-4}{:}{-3}{:}2]$ $\quad D = -11$ $[1{:}1{:}{-1}{:}0]$ $\quad D = -28$ $[0{:}1{:}2{:}{-1}]$ $D = -7$ $[2{:}{-1}{:}{-2}{:}1]$ $\quad D = -16$ $[2{:}0{:}{-1}{:}0]$ $j = \bigl(-4235548491023653492855276120803960977119898 43$ $\qquad \pm 928104030879091696744309588622453400515566 5\sqrt{-31159}\bigr)/2^{138}$ $N(j) = 2^{-138} \cdot 3^6 \cdot 11^3 \cdot 203834255299859^3$ $N(j - 1728) = 2^{-138} \cdot 3^{12} \cdot 5^2 \cdot 7^4 \cdot 11^2 \cdot 103^2 \cdot 823^2 \cdot 19661147685293^2$
$X_0^+(191)$	$y^2 = x^6 + 2x^4 + 2x^3 + 5x^2 - 6x + 1$ $\qquad P = (2, -11)$ cusp ∞ $\quad D = -11$ $(0, -1)$ $\quad D = -28$ $(2, 11)$ $D = -7$ $(0,1)$ $\quad D = -19$ ∞ $j = 289124951156223166895576426642806310208257095680000 0$ $\qquad \pm 6407493927137554671415525409106656684013158400 0\sqrt{61 \cdot 229 \cdot 145757}$ $N(j) = 2^{30} \cdot 3^6 \cdot 5^6 \cdot 4421^3 \cdot 253876253183601617^3$ $N(j - 1728) = 2^{12} \cdot 3^{12} \cdot 7^4 \cdot 55931^2 \cdot 660013^2 \cdot 49275262718204232316829^2$
$X_0^+(311)$	$x^2 + wy - 2xy + 2y^2 + 7xz - 8yz + 13z^2 = 0$ $wx^2 - 2wxy + x^2y - wy^2 - xy^2 - 2y^3 + w^2z + 6wxz$ $\quad - x^2z - wyz + 5xyz + 4y^2z + 7wz^2 - 4xz^2 - 2z^3 = 0$ $\qquad P = [6{:}8{:}{-1}{:}{-2}]$ cusp $[1{:}0{:}0{:}0]$ $D = -11$ $[-1{:}1{:}1{:}0]$ $\quad D = -19$ $[1{:}2{:}{-1}{:}{-1}]$ $\quad D = -43$ $[2{:}0{:}{-1}{:}0]$ $j = 3124418359443327073099098579305858972915260167782400000 0$ $\qquad \pm 15658105389980517153973396894921950350775512678400 0\sqrt{11 \cdot 17 \cdot 9011 \cdot 23629}$ $N(j) = 2^{30} \cdot 3^6 \cdot 5^6 \cdot 17^3 \cdot 2087^3 \cdot 313879^3 \cdot 11769971^3 \cdot 8978186297^3$ $N(j - 1728) = 2^{12} \cdot 3^{12} \cdot 7^4 \cdot 11^2 \cdot 19^4 \cdot 2087^2 \cdot 4339^2 \cdot 543068481424247323239808720460 29^2$

TABLE 1. Exceptional rational points found. For each modular curve we give an equation for the curve (for details on what modular forms the variables correspond to, see [Galbraith 1996]); the coordinates of the exceptional point P, as found during the search; the coordinates of the cusp and those of each rational Heegner point; the j-invariant of the $\mathbb{Q}$-curve corresponding to the exceptional point, and the norms of j and $j - 1728$.

$j = 73$	$2^{-74} \cdot 3^5 \cdot 5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 23^2 \cdot 29 \cdot 31 \cdot 41 \cdot 53 \cdot 59 \cdot 73 \cdot 151 \cdot 1669$
$j = 103$	$2^{16} \cdot 3^7 \cdot 5 \cdot 7 \cdot 17 \cdot 19 \cdot 23^2 \cdot 31 \cdot 41 \cdot 43 \cdot 47 \cdot 83 \cdot 103 \cdot 107 \cdot 487 \cdot 683$
$j = 137$	$2^{-138} \cdot 3^8 \cdot 5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 23 \cdot 29 \cdot 31 \cdot 71 \cdot 83 \cdot 97 \cdot 131 \cdot 137 \cdot 151 \cdot 157 \cdot 199 \cdot 563 \cdot 683 \cdot 2593 \cdot 26183$
$j = 191$	$2^{16} \cdot 3^7 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 41 \cdot 59 \cdot 83 \cdot 103 \cdot 139 \cdot 181 \cdot 191 \cdot 499 \cdot 1151 \cdot 3769 \cdot 8171$
$j = 311$	$2^{15} \cdot 3^7 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19^2 \cdot 29 \cdot 31 \cdot 41 \cdot 61 \cdot 71 \cdot 89 \cdot 101 \cdot 227 \cdot 271 \cdot 311 \cdot 349 \cdot 521 \cdot 661 \cdot 123191$

TABLE 2. Factorisation of the coefficient of the radical in the expression of j.

7. CONCLUSION

We have shown that exceptional rational points do exist on $X_0^+(p)$ when its genus is at least 2. Three of these examples are due to the action of the hyperelliptic involution. In [Hasegawa and Hashimoto 1996] it is shown that $X_0^+(p)$ will not be hyperelliptic when it has genus at least 3, so we do not expect any further occurrences of rational points arising from the action of involutions. We have also provided two examples of exceptional rational points on nonhyperelliptic curves $X_0^+(p)$. We have only studied the case when the genus of $X_0^+(p)$ is at most 5, and we do not go so far as to suggest that there are no further values of p for which exceptional rational points on $X_0^+(p)$ occur. It would be very interesting to have an argument which shows, for instance, that exceptional rational points on $X_0^+(p)$ do not arise for all p greater than some bound.

ACKNOWLEDGEMENTS

I would like to thank Professor Bryan Birch for his guidance over the duration of this research. Also, thanks to Michael Müller and Colin Stahlke for computational input. This work has also benefited from comments by the referees and communication I have had with Peter Bending, Imin Chen, Noam Elkies, Frazer Jarvis, Richard Pinch, Andrew Robertson, Richard Taylor and John Wilson.

REFERENCES

[Atkin and Lehner 1970] A. O. L. Atkin and J. Lehner, "Hecke operators on $\Gamma_0(m)$", *Math. Ann.* **185** (1970), 134–160.

[Birch 1969] B. J. Birch, "Diophantine analysis and modular functions", pp. 35–42 in *Algebraic Geometry* (Bombay, 1968), Tata Inst. Fund. Res. Stud. math. **4**, Oxford Univ. Press, London, 1969.

[Cohen et al. 1992] H. Cohen, N.-P. Skoruppa, and D. Zagier, "Tables of modular forms", preprint, 1992.

[Cremona 1992] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge Univ. Press, Cambridge, 1992.

[Elkies 1998] N. D. Elkies, "Elliptic and modular curves over finite fields and related computational issues", pp. 21–76 in *Computational perspectives on number theory* (Chicago, 1995), edited by D. A. Buell and J. T. Teitelbaum, AMS/IP Stud. Adv. Math. **7**, Amer. Math. Soc., Providence, RI, 1998.

[Galbraith 1996] S. D. Galbraith, *Equations for modular curves*, Doctoral thesis, Oxford Univ., 1996.

[González 1998] J. González, "On the j-invariants of the quadratic $\mathbb{Q}$-curves", preprint, 1998.

[Gross 1984] B. H. Gross, "Heegner points on $X_0(N)$", pp. 87–105 in *Modular forms* (Durham, 1983), edited by R. A. Rankin, Horwood, Chichester, 1984.

[Gross and Zagier 1985] B. H. Gross and D. B. Zagier, "On singular moduli", *J. Reine Angew. Math.* **355** (1985), 191–220.

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977.

[Hasegawa 1995] Y. Hasegawa, "Table of quotient curves of modular curves $X_0(N)$ with genus 2", *Proc. Japan Acad. Ser. A Math. Sci.* **71**:10 (1995), 235–239.

[Hasegawa and Hashimoto 1996] Y. Hasegawa and K.-i. Hashimoto, "Hyperelliptic modular curves $X_0^*(N)$ with square-free levels", *Acta Arith.* **77**:2 (1996), 179–193.

[Kenku 1981] M. A. Kenku, "On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$", *J. London Math. Soc.* (2) **23**:3 (1981), 415–427.

[Lang 1987] S. Lang, *Elliptic functions*, 2nd ed., Addison-Wesley, Reading, MA, 1987.

[Mazur 1977] B. Mazur, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186.

[Momose 1984] F. Momose, "Rational points on the modular curves $X_{\text{split}}(p)$", *Compositio Math.* **52**:1 (1984), 115–137.

[Momose 1986] F. Momose, "Rational points on the modular curves $X_0^+(p^r)$", *J. Fac. Sci. Univ. Tokyo Sect. 1A Math.* **33**:3 (1986), 441–466.

[Momose 1987] F. Momose, "Rational points on the modular curves $X_0^+(N)$", *J. Math. Soc. Japan* **39**:2 (1987), 269–286.

[Murabayashi 1992] N. Murabayashi, "On normal forms of modular curves of genus 2", *Osaka J. Math.* **29**:2 (1992), 405–418.

[Ogg 1973] A. P. Ogg, "Rational points on certain elliptic modular curves", pp. 221–231 in *Analytic number theory* (St. Louis, MO, 1972), edited by H. G. Diamond, Proc. Sympos. Pure Math. **24**, Amer. Math. Soc., Providence, 1973.

[Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan, Princeton Univ. Press, Princeton, and Iwanami Shoten, Tokyo, 1971.

[Shimura 1995] M. Shimura, "Defining equations of modular curves $X_0(N)$", *Tokyo J. Math.* **18**:2 (1995), 443–456.

[Stein n.d.] W. A. Stein, "The modular forms database", See http://shimura.math.berkeley.edu/~was/Tables.

Steven D. Galbraith, Department of Mathematics, Royal Holloway University of London, Egham, Surrey TW20 0EX
(S.Galbraith@rhbnc.ac.uk)

Received September 30, 1997; accepted in revised form November 5, 1998