THE MODULAR CURVE $X_0(169)$ AND RATIONAL ISOGENY

M. A. KENKU

1. *Introduction*

Let N be an integer $\geqslant 1$. The affine modular curve $Y_0(N)$ parametrizes isomorphism classes of pairs $(E; C_N)$ where E is an elliptic curve defined over $\mathbb{C}$, the field of complex numbers, and C_N is a cyclic subgroup of E of order N. The compactification $X_0(N)$ is an algebraic curve defined over $\mathbb{Q}$.

Recently Mazur [**6**] proved a very important theorem on rational points on the modular curves $X_0(N)$, listing those primes N for which the curve has non-cuspidal rational points. The question of isogenies for composite N, rational over $\mathbb{Q}$, will be settled if one determines $X_0(N)(\mathbb{Q})$ for all N which are minimal of positive genus. In view of the articles [**2, 3, 6**] the outstanding cases are $N = 169$ and 125. We show here that $Y_0(169)(\mathbb{Q})$ is empty.

By the recent work of Berkovic [**1**] it is known that the Eisenstein quotient $J_0^{(7)}(169)$ has Mordell-Weil rank 0 over $\mathbb{Q}$. It then follows that $X_0(169)(\mathbb{Q})$ is finite. That result also enables us to apply a theorem of Mazur to show that, for a rational pair (E, C_N) corresponding to a rational point on $X_0(169)$, E has potentially good reduction at all primes except possibly 2, 13 and those primes $n \equiv 1\ (13)$.

We construct an affine model of the curve making use of functions which are essentially modular units. The restriction on the primes at which E has potentially bad reduction translates into a similar restriction on the prime factors of the coordinate functions of our model. It is then deduced from this that $Y_0(169)(\mathbb{Q})$ is empty.

2. *Preliminaries*

As in the previous papers, let η be the modular form of dimension $-\frac{1}{2}$ given by

$$\eta(z) = q^{1/24}\prod(1-q^n)$$

where $q = \exp(2\pi i z)$. The following lemma of Newmann [**8**] is well known.

LEMMA 1. *The expression* $\prod_{d\mid n} \eta(dz)^{r(d)}$ *(where* $r(d) \in \mathbb{Z}$*) is a function of* $X_0(N)$ *so long as* (i) $\sum_{d\mid n} r(d) = 0$, (ii) $\prod_{d\mid n} d^{r(d)}$ *is a square, and* (iii) $\prod_{d\mid n} \eta(dz)^{r(d)}$ *has integral order at every cusp of* $X_0(N)$.

For an arbitrary positive integer m, let $G(m)$ denote the multiplicative group of units of the ring of congruence classes modulo m. The following lemma is well-known.

Received 10 July, 1979; revised 9 November, 1979.

LEMMA 2. (i) *$G(p^r)$ is cyclic of order $(p-1)p^{r-1}$ if p is an odd prime, and r is a positive integer.*

(ii) $G(2^r) = \mathbb{Z}_2 \times \mathbb{Z}_{2^{r-2}}$.

The following theorem of Ogg [9] about cusps of $X_0(N)$ is very useful.

LEMMA 3. *For each $d \mid N$, and $t = (d, N/d)$ we have $\phi(t)$ conjugate cusps $\begin{pmatrix} x \\ d \end{pmatrix}$ of $X_0(N)$, each with ramification degree $e = t$ in $X_1(N) \to X_0(N)$ and these are all the cusps of $X_0(N)$. In particular all cusps are rational if N or $N/2$ is a square free integer.*

Berkovic [1] proved the following theorem.

LEMMA 4. *If m is a prime number different from 2, 3, 5, 11 and $h = (m-1, 12)$ and $12 = hq$ then for every $p \mid (m+1)/2q$, the ideal $I + pT \neq T$ and the group $J_{m^2}^{(p)}(\mathbb{Q})$ is finite.*

In the statement above, T is the Hecke algebra of $J_0(N)$ and I is the Eisenstein ideal.

LEMMA 5. *Let $N = q^2$ or q^3 where q is an odd prime. Let n be an odd prime which is different from q and such that $n \not\equiv 1(q)$.*

Suppose that $E/\mathbb{Q}$ is an elliptic curve possessing a $\mathbb{Q}$-rational cyclic group C_N of order N. Let $x = j(E; C_N)$ belong to $Y_0(N)(\mathbb{Q})$. Suppose there exists an optimal quotient $f: J_0(N)^{new} \to A$ such that $f(x)$ is of finite order in $A(\mathbb{Q})$. (This is necessarily true if the Mordell–Weil group $A(\mathbb{Q})$ is finite.) Then E has potentially good reduction at n.

Proof. Suppose that E has potentially bad reduction at n. Then the point x specialises to one of the cusps at n. Let P_0, P_∞ denote the unitary cusps which are rational. We assert that either x specialises to the reduction of P_0 or that of P_∞.

Suppose we take first the case $N = q^2$. Then besides P_0 and P_∞ there are $q-1$ other cusps P_i, $i = 1, \dots, q-1$ which are rational in $K = \mathbb{Q}(\xi_q)$, the cyclotomic field of q-th roots of unity, and which are conjugate by Lemma 3.

Since $n \not\equiv 1 \pmod q$, then the reduction $\tilde{P}_i$ of P_i, $i = 1, \dots, q-1$ are not $\mathbb{Z}/p\mathbb{Z}$ rational; so $\tilde{x} \neq \tilde{P}_i$.

The argument for $N = q^3$ is similar. The rest of the proof now follows as in Corollary 4.3 of [6].

3. *The modular curve $X_0(169)$*

Consider the functions

$$X(\omega) = 13\eta^2(169\omega)/\eta^2(13\omega), \qquad Y(\omega) = \eta^2(\omega)/\eta^2(13\omega).$$

Both functions satisfy conditions (i) and (ii) of Lemma 1. Let $j(\omega)$ be the classical modular invariant with $j(\sqrt{-1}) = 1728$. It is easy to show that the scheme of zeros of X, Y, $j(\omega)$ and $j(13\omega)$ is as follows:

	P_0	P_i	P_∞
X	-1	-1	13
Y	13	-1	-1
$j(\omega)$	-169	-1	-1
$j(13\omega)$	-13	-13	-13 ;

X and Y therefore also satisfy condition (iii).

Now let

$$f(\tau) = 13\eta^2(13\tau)/\eta^2(\tau), \qquad g(\tau) = \eta^2(\tau/13)/\eta^2(\tau).$$

It is shown on page 62 of [4] that $j(\tau) = F(T)/T$ where $T = f(\tau)$ or $g(\tau)$ and

$$F(T) = (T^2+5T+13)(T^4+7T^3+20T^2+19T+1)^3.$$

Suppose we put $\tau = 13\omega$; then we have $j(13\omega) = F(X)/X = F(Y)/Y$. Hence

$$YF(X)-XF(Y) = 0\,. \tag{1}$$

Since X and Y are of degree 13 in $\mathbb{Q}(X_0(169))$ it is clear that

$$\mathbb{Q}(X,\, Y) = \mathbb{Q}(X_0(169))$$

especially as X does not belong to $\mathbb{Q}(Y) = \mathbb{Q}(X_0(13))$. Equation (1) has $X-Y$ as a factor. The other factor

$$XY\{X^{12}+X^{11}Y+\ldots+15145(X+Y)\}-13 = 0 \tag{2}$$

is irreducible and is the equation of an affine model of $X_0(169)$.

The less complex equation (1) will be used most of the time but we make use of (2) to establish a congruence condition modulo 3 on X and Y.

THEOREM 1. *The curve $X_0(169)(\mathbb{Q})$ contains only two points which are the unitary cusp P_0 and P_∞.*

Proof. Let $x = j(E\,;C_{169})$ belong to $Y_0(169)(\mathbb{Q})$. By Lemma 5, the curve E has potentially good reduction at all primes p except perhaps for $p = 2, 13$ and those $p \equiv 1(13)$ at which E reduces to one of the $P_{i,s}$, $i = 1, \ldots, 12$. Consequently, if ω_0 belonging to the upper half plane H is a representative of the point on the orbit space $H/\Gamma_0(169)$ corresponding to x, then the denominator of $j(\omega_0)$ has only 2, 13 and $p \equiv 1(13)$ as possible prime factors. Since $j(13\omega_0)$ is the modular invariant of an elliptic curve which is isogenous to E by an isogeny of order 13, the denominators of $j(\omega_0)$ and $j(13\omega_0)$ have the same prime factors. As $j(13\omega) = F(X)/X = F(Y)/Y$ it follows that the only possible prime factors of the numerators and denominators of X are Y are 2, 13 and primes $p \equiv 1(13)$.

Suppose that R is the integral closure of $\mathbb{Z}[j]$ in $\mathbb{Q}(X_0(169))$. We note that X and Y are units in $R[1/13]$.

Suppose then that 2 divides the denominator of $j(13\omega_0)$. Since the reduction of the $P_{i,s}$ modulo a prime ideal dividing 2 is not rational over $\mathbb{F}_2$, we know that x cannot reduce to any of them modulo 2. So x reduces to the reduction of either P_0 or P_∞ modulo 2.

Suppose that 2 divides the denominator of X. This implies that X specializes to ∞ at 2. Since X has a pole at P_0, while Y has a zero, we have that 2 divides the numerator of Y. It is easy to see from equation 1 (or by applying Theorem 9 and preceeding results of [5]) that if 2^n, for a positive integer n, exactly divides the denominator of X, that 2^{13n} divides the numerator of Y and vice versa.

Similarly if p is a prime $\equiv 1(13)$ and divides the denominator of $j(13\omega_0)$ then x reduces modulo p to the reduction of one of the $P_{i,s}$. The prime p then divides the denominator of X and Y to the same power since X and Y have poles at the $P_{i,s}$.

On the other hand, it is possible for the prime 13 to divide the numerator of X and neither the numerator nor the denominator of Y and vice versa. Although this is possible, 13^2 does not divide the numerator of X. Before we examine the possible cases we make a useful observation: E has a potentially good reduction at 3, and hence 3 divides neither the numerator nor the denominator of X and Y. By reducing equation (2) modulo 3 it is easy to see that the only possible solutions for X and Y modulo 3, rational over $\mathbb{F}_3$ are $X \equiv \pm 1(3)$ and $X \not\equiv Y(3)$.

Finally we note that the Atkin–Lehner involution W_{169} permutes X and Y.

From the remarks above, we have only the following cases:

(i) $X = \varepsilon_1/2^n \cdot 13^r \cdot m;\quad Y = \varepsilon_2 2^{13n} \cdot 13^{13r+1}/m,$

(ii) $X = \varepsilon_1 2^{13n}/13^r \cdot m;\quad Y = \varepsilon_2 13^{13r+1}/2^n \cdot m,$

(iii) $X = \varepsilon_1 \cdot 13^r \cdot 2^{13n}/m; Y = \varepsilon_2 13^r/2^n \cdot m,$

(iv) $X = \varepsilon_1 13 \cdot 2^{13n}/m;\quad Y = \varepsilon_2/2^n \cdot m,$

(v) $X = \varepsilon_1 2^{13n}/13^r \cdot m;\quad Y = \varepsilon_2/m \cdot 13^r \cdot 2^n,$

where $\varepsilon_i = \pm 1$ for $i = 1$ and 2, both r and n are non-negative integers and m is either 1 or a finite product of primes $\equiv 1(13)$.

We recall that

$$F(T) = T^{14}+26T^{13}+325T^{12}+2548T^{11}+13832T^{10}+54340T^9+157118T^8$$
$$+333580T^7+509366T^6+534820T^5+354536T^4+124852T^3+15145T^2+476T+13,$$

and note that all but the first and the coefficient of T are divisible by 13.

Since $X \not\equiv Y \bmod (3)$ it is clear that $\varepsilon_1 \neq \varepsilon_2$ in all the five cases. In case (1)

$$\varepsilon_2\{1+26\varepsilon_1(2^n \cdot 13^r \cdot m)+\ldots+2^{14n} \cdot 13^{14r+1} \cdot m^{14}\}$$
$$= \varepsilon_1\{13^{(14r+1)13} \cdot 2^{14\times 13n}+2\varepsilon_2 13^{(13r+1)13} \cdot 2^{13\times 13n}+\ldots+m^{14}\}.$$

Hence, 2^{n+1} divides $m^{14}\varepsilon_2-\varepsilon_1$. Since $\varepsilon_1 \neq \varepsilon_2$, we have $n = 0$. This implies that 13 divides $m^{14}+1$. This is impossible since $m \equiv 1(13)$. So case (i) is impossible. For case (ii) we have

$$\varepsilon_2\{2^{13n\times 14}+26\varepsilon_1(2^{13\times 13n}\cdot 13^r\cdot m)+\ldots+13^{14r+1}\cdot m^{14}\}$$

$$=\varepsilon_1\{13^{(14r+1)\times 13}+2\varepsilon_2(13^{13(13r+1)}\cdot 2^n\cdot m)+\ldots+2^{14n}\cdot m^{14}\}.$$

Hence 13 divides $2^{14n}\{\varepsilon_1 m^{14}-\varepsilon_2 2^{14n\times 12}\}$. This is impossible since $\varepsilon_1 \neq \varepsilon_2$ and both components are congruent to $1(13)$.

In case (iii) equation (1) reduces to

$$\varepsilon_1\{2^{13n\times 14}13^{14r-1}+26\varepsilon_2(2^{13n\times 13}\cdot 13^{13r-1}\cdot m)+\ldots+m^{14}\}$$

$$=\varepsilon_2\{13^{14r-1}+26\varepsilon_1(2^n\cdot 13^{13r-1}\cdot m)+\ldots+2^{14n}\cdot m^{14}\}.$$

This shows that 2^{n+1} divides $m^{14}\varepsilon_1-13^{14r-1}\varepsilon_2$. Since $\varepsilon_1 \neq \varepsilon_2$ and $m^{14} \equiv 1(8)$ while $13^{14r-1} \equiv 5(8)$, it follows that $n = 0$. This implies that m divides $2\times 13^{14r-1}$ which is impossible; so case (iii) is also impossible.

In respect of case (iv) we have

$$\varepsilon_2\{2^{13n\times 14}\cdot 13^{13}+26\varepsilon_1(2^{13n\times 13}\cdot 13^{12}m)+\ldots+m^{14}\}$$

$$=\varepsilon_1\{1+26\varepsilon_2(2^n\cdot m)+\ldots+2^{14n}\cdot 13\cdot m^{14}\}.$$

Again 2^{n+1} divides $m^{14}\varepsilon_2-\varepsilon_1$. Since $\varepsilon_1 \neq \varepsilon_2$ then $n = 0$. But then 13 will divide $m^{14}+746m^{13}+1$. Since $m \equiv 1(13)$ and $746 \equiv 5(13)$ this is impossible.

Finally in case (v) we have

$$\varepsilon_2\{2^{13n\times 14}+26\varepsilon_1(2^{13n\times 13}\cdot 13^r\cdot m)+\ldots+13^{14r+1}\cdot m^{14}\}$$

$$=\varepsilon_1\{1+26\varepsilon_2(2^n\cdot 13^r\cdot m)+\ldots+13^{14r+1}\cdot m^{14}\cdot 2^{14n}\}.$$

This implies that 2^{n+1} divides $13^{14r+1}\cdot m^{14}\varepsilon_2-\varepsilon_1$. Again since $\varepsilon_1 \neq \varepsilon_2$, we have $n = 0$; if this is so, then 13 divides 2. This is absurd.

This concludes the proof of the theorem.

Remark. In the proof of Theorem 7 of [3] we did not explain why $(u)-(\omega(u))$ is linearly equivalent to $(p')-(\omega(p'))$ if it is of order 7. This follows from the fact the $X_0(91)$ has exactly four points (the unitary cusps) rational over $\mathbb{F}_2$. This can be quickly seen from the characteristic polynomial of T_2.

References

1. B. G. Berkovic, "The rational points on the jacobians of modular curves", *Math. USSR Sb.*, 30 (1976), 478–500.
2. M. A. Kenku, "The modular curve $X_0(39)$ and rational isogeny", *Math. Proc. Cambridge Philos. Soc.*, 85 (1979), 21–23.
3. M. A. Kenku, "The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny", *Math. Proc. Cambridge Philos. Soc.*, 87 (1980), 15–20.

4. F. Klein and R. Fricke, "Vorlesungen über die Theorie der elliptischen Modul-funktionen". Vol. 2 (Chelsea).
5. D. Kubert and S. Lang, "Units in Modular Function Field I", Math. Ann., 218 (1975), 67–96.
6. B. Mazur, "Rational isogenies of prime degree", *Invent. Math.*, 44 (1978), 129–162.
7. B. Mazur, "Modular curves and the Eisenstein ideal", Publications Mathématiques 47 (Institut des Hautes Études Scientifiques, Paris, 1978), pp. 33–186.
8. M. Newmann, "Construction and application of a class of modular functions", *Proc. London Math. Soc.*, (3), 7 (1957), 331–350, 9 (1959), 373–387.
9. A. P. Ogg, "Rational points on certain elliptic modular curves", Proceedings Symposia in Pure Mathematics 24 (American Mathematical Society, Providence, R.I., 1973), pp. 221–231.

Department of Mathematics,
University of Ibadan,
Nigeria.