Math. Proc. Camb. Phil. Soc. (1980), 87, 15
Printed in Great Britain

The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny

BY M. A. KENKU
University of Ibadan, Nigeria

(*Received* 30 *October* 1978, *revised* 17 *May* 1979)

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

An excellent account of the connexion of $X_0(N)$ with the problem of rational isogeny will be found in (10).

Recently Mazur (7) proved a deep and 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.

To treat the composite N it suffices to deal with those of minimal positive genus. Of these only the cases $N = 65, 91$ 125 and 169 are outstanding, $N = 39$ having been settled in (2).

The aim of this article is to show that both $X_0(65)$ and $X_0(91)$ have no $\mathbb{Q}$-rational non-cuspidal points.

By the recent work of Berkovic (1) it is known that each factor of the Eisenstein quotients of the Jacobians of both curves has Mordell–Weil rank 0. For $X_0(91)$ we show that the Mordell–Weil group of one such factor has order 7. By also showing that $X_0(91)/w_{13}$ is not hyperelliptic we deduce that the curve has no non-cuspidal $\mathbb{Q}$-rational points.

With respect to $X_0(65)$ we construct an equation for a model of the curve. The functions used are essentially modular units. Making use of a theorem of Mazur we show that the only possible prime factors of the denominator and numerator of the values of these functions are 2 and 13.

It is then a numerical exercise to show that $X_0(65)$ has no $\mathbb{Q}$-rational non-cuspidal point.

2. *Preliminaries on the Eisenstein quotient.* Let $J_{N\nu}$ denote the new part (Greek nu!) of the Jacobian J_N of $X_0(N)$, T the subring in $\mathrm{End}_{\mathbb{Q}}(J_{N\nu})$ generated over $\mathbb{Z}$ by Hecke operators T_l, $l\nmid N$ and Atkin–Lehner operators $U_q\, q|N$. The Hecke algebra T is commutative and free over $\mathbb{Z}$ of rank $= \dim(J_{N\nu})$.

The tensor product
$$T \otimes \mathbb{Q} \cong \Pi F_\alpha,$$
where F_α is a real algebraic number field. The factorisarion corresponds to the factorisation of
$$J_{N\nu} = \Pi J_\alpha,$$
which is unique up to isogeny.

We have that $\dim(J_\alpha) = [F_\alpha : \mathbb{Q}]$ and if $\rho_\alpha = \ker(T \to F_\alpha)$ then $J_\alpha \cong J_{N\nu}/\rho_\alpha(J_{N\nu})$.

Berkovic(1) proved that $T = \mathrm{End}_{\mathbb{Q}}(J_{N\nu})$ and that in the decomposition of $J_{N\nu}$ over $\mathbb{Q}$ each factor occurs with multiplicity one.

Let ρ be a non-trivial ideal of T, ρ corresponds with a non-trivial factor $J^{(\rho)}$ of $J_{N\nu}$. Suppose we put $a_\rho = \bigcap^{\infty} \rho^n$ then the ideal a_ρ is equal to the intersection of all minimal prime ideals ρ_α for which $\rho_\alpha + \rho \neq T$.

Consider the Eisenstein ideal I of T generated by $1 + l - T_l$ for all $l \nmid N$. I is a proper ideal of T and it is of finite index.

Let p be a prime number such that $\wp = I + pT \neq T$. Then $\wp$ corresponds to a factor of $J_{N\nu}$ and we denote it by $J_N^{(p)}$.

Suppose we specialize to the case $N = mn$ is a product of two odd primes n, m. Then $X_0(mn)$ has 4 cusps all rational. Denote them by P_1, P_n, P_m and P_{nm}.

The following theorem was proved by Ogg(9).

THEOREM 1. *Let m, n be different prime numbers. A class of divisor*

$$D = (P_1) + (P_m) - (P_n) - (P_{mn}) \quad on \quad X_0(mn)$$

has order $(m+1)(n-1)/h$, where $h = ((m+1)(n-1), 24)$.

We note that $w_m(D) = D$ but $w_n(D) = -D$. Also in the two cases we are interested in $J_N = J_{N\nu}$ since N is of minimal positive genus.

Berkovic(1) proved the following:

THEOREM 2. *Let m, n be different prime numbers, p an odd prime, $p \mid (m+1)$ but $p \nmid (n-1)$ if $p > 3$, and $9 \mid (m+1)(n-1)$ but $9 \nmid (n-1)$ if $p = 3$. Then the ideal $= (I, p, 1 - w_m) \neq T$ and the group $J_{mn}^{(p)}(Q)$ is finite.*

Subsequently we deal with $N = 65$ for which p would be either 3 or 7 and $N = 91$ for which we take $p = 7$.

We require the following theorem of Ogg(9) about a hyperelliptic Riemann surface X of genus g.

THEOREM 3. *Let v be a hyperelliptic involution of X and w another involution. Let $u = vw$ (also an involution). Then the fixed point sets of u, v and w are disjoint. If g is even, then w and u have two fixed points each; if g is odd then w has four fixed points and u none or vice-versa.*

We require also the following theorem ((7), cor. 4·3).

THEOREM 4. *Let K be a number field, and N a square free number. Let $\wp$ be a prime of K of characteristic p (possibly dividing N) such that the ramification index at $\wp$ satisfies the inequality*

$$e_\wp(K/Q) < p - 1.$$

Let E/k be an elliptic curve possessing a K-rational cyclic subgroup C_N of order N. Let $x = j(E; C_N) \in X_0(N)(K)$.

Suppose there exists an optimal quotient $f: J_0(N_v) \to A$ such that $f(x)$ is of finite order in $A(K)$. Then E has potentially good reduction at $\wp$.

3. $X_0(65)$. Let η be the modular form of dimension $-\frac{1}{2}$,

$$\eta(z) = q^{\frac{1}{24}} \Pi(1 - q^n),$$

where $q = \exp(2\pi iz)$. The following lemma of Newman (8) is well known.

LEMMA 5.
$$\prod_{d|N} \eta(dz)^{r(d)}$$
is a function on $X_0(N)$ so long as

(i) $\sum_{d|N} r(d) = 0$,

(ii) $\Pi d^{r(d)}$ is a square,

(iii) $\Pi \eta(dz)^{r(d)}$ has integral order at every cusp of $X_0(N)$.

We consider two such functions
$$R(\tau) = \frac{\eta(13\tau)\,\eta(5\tau)}{\eta(65\tau)\,\eta(\tau)}, \quad S(\tau) = \frac{\eta^2(5\tau)}{\eta^2(65\tau)}.$$

The zero scheme of R and S is

	P_1	P_5	P_{13}	P_{65}
R	-2	2	2	-2
S	1	5	-1	-5

Both of them satisfy the conditions of the lemma and are therefore on $X_0(65)$.

For $N'|65$, let $w_{N'}$ be the corresponding Atkin–Lehner involution. By a theorem in Kenku (3), w_5 and w_{13} each has no fixed points but w_{65} has 8: $X_0(65)$ is of genus 5 but the quotient spaces $X_0(65)/w_5$ and $X_0(65)/w_{13}$ each has genus 2 while $X_0(65)/w_{65}$ and $X_0(65)/\{w_{65}, w_5\}$ each has genus 1.
$$w_{65}(R) = R \quad \text{and} \quad w_5(R) = R^{-1},$$
while
$$w_{65}(S) = 13R^2S^{-1} \quad \text{and} \quad w_5(S) = SR^{-2}.$$
$$Y = (S/R + 13R/S)(R + R^{-1}) \quad \text{and} \quad L = (R - R^{-1})$$
are functions on $E = X_0(N)/\{w_{65}, w_5\}$. By considering the behaviour of Y and L at the only cusp of E which is their only pole, we obtain the following relation
$$Y^2 + 5Y(L^2+4) = (L^2+4)(L^3 - 10L^2 + 3L - 50).$$
Substituting $H = (Y + 2L^2 + L + 10)/(L-2)$ we get
$$H^2 + HL = L^3 + 4L + 1,$$
which is the equation of the Néron model of E.

In terms of R and S, we have
$$R(S^2+13R^2)^2(R^4+2R^2+1) + 5SR(S^2+13R^2)(R^4-1)(R^2-1)$$
$$= S^2(R^4+2R^2+1)(R^6 - 10R^5 - 30R^3 - 10R - 1)\ldots \quad (1)$$
Now write $T(\tau)$ for $13\eta^2(13\tau)/\eta^2(\tau)$.

Then $T(\tau)$ is a univalent function on $X_0(13)$ and if $j(\tau)$ denotes the classical modular invariant with $j(\sqrt{-1}) = 1728$ we have from ((4), p. 62)
$$j(\tau) = (T^2+5T+13)(T^4+7T^3+20T^2+19T+1)^3/T$$
$$= F(T)/T.$$
So $j(5\tau) = SF(13S^{-1})/13$ or $F(M)/M$, where $M = 13S^{-1}$.

THEOREM 6. *The curve $X_0(65)$ has no non-cuspidal points which are $\mathbb{Q}$-rational.*

Proof. Suppose there is such a point x. Suppose ω is a point in the fundamental region of $\Gamma_0(65)$ corresponding to such a point; then $S(\omega)$ and $R(\omega)$ both belong to Q.

The fact that they are non-zero follows from the properties of the η function. Suppose

$$S(\omega) = m/n \quad \text{where} \quad m, n \in \mathbb{Z}$$

and m and n coprime. Let q be a prime dividing m. If $q \neq 13$, then

$$j(5\omega) = \frac{m}{13n} F\left(\frac{13n}{m}\right)$$

has q as a factor of its denominator. The same is true for $q = 13$ if 13^2 divides m. Similarly, if a prime q divides n, $j(5\omega)$ again has q as a factor of its denominator.

If $x = j(E, C_N)$ with C_N $\mathbb{Q}$-rational, $j(\omega)$ is the invariant of E while $j(5\omega)$ is the invariant of the isomorphism class of elliptic curves corresponding to $w_5(x)$.

Also we know that q divides the denominator of $j(5\omega)$ only if the $\mathbb{Q}$-rational elliptic curve corresponding to $w_5(x)$ has potential multiplicative reduction at the prime q. Since E is isogenous to one such curve, the same holds for E.

By Theorem 2 we know that for $p = 3$ or $p = 7$ the corresponding Eisenstein quotient has finite Mordell–Weil group over $\mathbb{Q}$. Hence if we take $K = \mathbb{Q}$ in theorem 4 it follows that E should have potentially good reduction at q if $q \neq 2$.

This therefore implies that the only prime factor that can divide n is 2 while m is divisible at most by 2 or 13 and no higher power of 13.

Suppose we write

$$R(\omega) = \frac{u}{v} \quad \text{where } u, v \in \mathbb{Z} \text{ but } u \text{ and } v \text{ are coprime.}$$

In the same way a power of 2 can divide either u or v but no other prime. The factor 13 can be removed by considering the function $H = (\eta^2(5\tau))/\eta^2(\tau)$ and a similar expression on page 253 of (11) giving $j(\tau) = (G^3(H))/H^3$. Without loss of generality we can consider $S = \pm 2^t 13^i$, $R = \pm 2^h$, where $i = 0$ or 1 and t, h both ≥ 0. This can be seen by using the Atkin–Lehner involutions. Considering equation (1):

$$R(S^2+13R^2)^2(R^4+2R^2+1)+5SR(S^2+13R^2)(R^4-1)(R^2-1)$$
$$= S^2(R^4+2R^2+1)(R^6-10R^5-30R^3-10R-1);$$

it is easy to see by 2-adic considerations that the only possibilities for t and h are $2t = 5h$, so that $t = 5k$ and $h = 2k$, provided that none of the three terms is zero. It can be quickly checked that the latter is not possible. When $2t = 5h$, the exponent of 2 dividing the first term is $10k$, that of the second is $11k$ and the third is $10k$.

It is easy to check if $13 \nmid S$ that the 2-exponent of the difference of the first and third terms is at most $10k+3$ if $k > 1$, which implies that $k \leq 3$. In fact, $k = 1$ if R is positive and $k = 3$ if R is negative. If 13 divides S the exponent of 2 in the difference is $10k+1$ or $12k+1$ depending on the sign of R. If it is $10k+1$ then $k \leq 1$, if it is $12k+1$, then $12k+1 = 11k$ which is impossible.

Checking case by case we see that no such solution exists. This proves the theorem.

4. $X_0(91)$. As in Section 3 we consider 2 functions:

$$R_1(\tau) = \frac{\eta(13\tau)\,\eta(7\tau)}{\eta(91\tau)\,\eta(\tau)}, \quad S_1(\tau) = \frac{\eta^2(7\tau)}{\eta^2(91\tau)}.$$

The zero scheme for R_1 and S_1 is

	P_1	P_7	P_{13}	P_{91}
R_1	-3	3	3	-3
S_1	1	7	-1	-7

Both of them satisfy the conditions of Lemma 5 and are therefore functions on $X_0(91)$. w_{13} has 4 fixed points, w_7 none and w_{91} has 8.

$X_0(91)/w_{13}$ is of genus 3, $X_0(91)/w_7$ is of genus 4 and $X_0(91)/w_{91}$ is of genus 2.

$$w_{91}(R_1) = R_1 \quad \text{and} \quad w_7(R_1) = R_1^{-1},$$

$$w_{91}(S_1) = 13R_1^2 S_1^{-1} \quad \text{and} \quad w_7(S_1) = S_1 R_1^{-2}.$$

Write $L_1 = R_1 + R_1^{-1}$ and $H_1 = (S_1/R_1) + (13R_1/S_1)$. Both L_1 and H_1 are defined over $X_0(91)/\{w_7, w_{13}\}$ which is an elliptic curve E' of conductor 91. By considering the expansions of L_1 and H_1 at the only 'cusp' which is also their only pole we have the following relationship:

$$L_1^4 - 21L_1^3 - 11L_1^2 + 49L_1 + 16 = H_1^3 + 7H^2L_1 + 21H_1L_1^2 - 25H_1.$$

This is the equation for a singular model of E'. We do not require this equation; we give it just for the record.

First we note that of the eight fixed points of w_{91} on $X_0(91)$ two of them arise from complex multiplication by $\lambda = \sqrt{-91}$ in the order $\mathbb{Z}[1, \frac{1}{2}(1+\sqrt{-91})]$ which has class-number 2 and the other six in the order $\mathbb{Z}[1, \sqrt{-91}]$ which has class-number 6.

Since w_{13} is defined over $\mathbb{Q}$ it interchanges those two and permutes the six. Hence, on $X_1 = X_0(91)/w_{13}$, of the four fixed points of the image w of w_{91}, one of them x is $\mathbb{Q}$-rational and the other three are conjugate over $\mathbb{Q}$.

Suppose X_1 is hyperelliptic with hyperelliptic involution v. As before v permutes the fixed points of w. Since the fixed points of v, u, and w are disjoint, x is not a fixed point of u and hence must be taken to one of the other non-rational fixed points. This is impossible since u is also $\mathbb{Q}$-rational. Hence X_1 is not hyperelliptic.

$p = 7$ satisfies the condition of theorem 2 so that $J_{91}^{(7)}$ is a factor of the Eisenstein quotient of J_{91}. We will see shortly that

$$J_{91} = E' \times J_{91}^{(7)} \times J_{91}^{(4)} \times E''$$

up to isogeny where $J_{91}^{(4)}$ is the factor corresponding to 4, E' is the elliptic curve $X_0(91)/\{w_7, w_{13}\}$ and E'' is the elliptic curve corresponding to the cusp form with an eigenvalue -1 with respect to Atkin–Lehner operators w_7 and w_{13}.

Using the procedure described in (5, 6) we find that the characteristic polynomials of T_2, T_5 are respectively

$$x(x+2)(x^2-2)(x^3-x^2-4x+2),$$

$$(x+3)^2(x^2-6x+7)(x^3-2x^2-3x+2).$$

Consequently we deduce that the reduction of J_{1-} over the primes 2 and 5 has 7 elements. J_{1-} is $(1-w)J_1$ where w is the image of w_{91} on X_1.

J_1 factorises as $J_{1+} \times J_{1-}$ and as $E' \times J_{91}^{(7)}$ so that J_{1-} is isogenous to $J_{91}^{(7)}$. Consequently the order of the Mordell–Weil group of J_{1-} is 7.

Let p' be the image of one of the cusps on X_1. Then $(p') - w(p')$ is of order 7. If u is any $\mathbb{Q}$-rational non-cuspidal point of X_1 not x then $(u) - (w(u)) \in J_{1-}$. Hence the order of $(u) - (w(u))$ is either 1 or 7. Both are impossible since X_1 is not hyperelliptic as shown above. Hence we have proved

THEOREM 7. *$X_0(91)$ has no non-cuspidal $\mathbb{Q}$-rational points.*

REFERENCES

(1) BERKOVIC, B. G. Rational points on the jacobians of modular curves. (In Russian.) *Math. Sbornik J.* **101** (1976) (143), no. 4 (12), 542–567. *Translation. Math USSR Sbornik*, vol. **30** (1976), no. 4.

(2) KENKU, M. A. The modular curve $X_0(39)$ and rational isogeny. *Math. Proc. Cambridge Philos. Soc.* **85** (1979), 21–23.

(3) KENKU, M. A. Atkin–Lehner involutions and class-number residuality. *Acta Arithmetica* **33** (1977), 1–9.

(4) KLEIN, F. and FRICKE, R. *Vorlesungen uber die Theories der elliptischen Modulfunktionen*, vol. 2 (Chelsea).

(5) LIGOZAT, G. Courbes modulaires de niveau 11. In *Modular functions of one variable*, vol. v, 148–237. Lecture Notes in Mathematics, no. 601 (Berlin, Heidelberg, New York, Springer, 1977).

(6) MANIN, Y. Parabolic points and zeta-functions of modular curves. *Math. U.S.S.R. Izvestija* **6** (1972), no. 1, 19–64.

(7) MAZUR, B. Rational isogenies of prime degree. *Inventiones Math.* **44** (1978), 129–162.

(8) NEWMAN, M. Construction and applications of a class of modular functions. *Proc. London Math. Soc.* (3) **7** (1967), 334–350; **9** (1959), 373–387.

(9) OGG, A. P. Hyperelliptic modular curves. *Bull. Soc. Math. France* **102** (1974), 449–462.

(10) OGG, A. P. Rational points on certain modular curves. *Proc. Symp. Pure Math. A.M.S. Providence* **24** (1973), 221–231.

(11) WEBER, H. *Lehrbuch der Algebra*, vol. III (Chelsea, New York).