ON THE MODULAR CURVES $X_0(125)$, $X_1(25)$ AND $X_1(49)$

M. A. KENKU

1. *Introduction*

Let N be a positive integer greater than 1. Examples of elliptic curves defined over $\mathbb{Q}$ possessing rational cyclic N isogenies are known for the values of N given in the following table.

N	g	v	N	g	v	N	g	v
$\leqslant 10$	0	∞	11	1	3	27	1	1
12	0	∞	14	1	2	37	2	2
13	0	∞	15	1	4	43	3	1
16	0	∞	17	1	2	67	5	1
18	0	∞	19	1	1	163	13	1
25	0	∞	21	1	4			

In this table, g is the genus of $X_0(N)$ and v the number of non-cuspidal rational points of $X_0(N)$.

The curve $X_0(N)$ is the compactification of the affine modular curve $Y_0(N)$ which parametrises 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. It is well known that $X_0(N)$ is defined over $\mathbb{Q}$ and if k is an algebraic number field a point x belongs to $Y_0(N)(k)$ if and only if there is a k-rational pair (E, C_N) in the corresponding class.

One of the objects of this paper is to show that there are no $\mathbb{Q}$-rational cyclic isogenies beyond those exhibited in the above table. In the light of known results enumerated in [**9**] and subsequent works [**3**, **4**, **5**] it suffices to show that $Y_0(125)(\mathbb{Q})$ is empty. The proof of this assertion is contained in Section 3 of this paper.

We construct an affine model of the curve by making use of functions which are essentially modular units. A point on this curve belonging to a $\mathbb{Q}$-rational class corresponds to a point on a particular hyperelliptic curve C which is defined over the cyclotomic field $k = \mathbb{Q}(\sqrt[5]{1})$. We deduce that $Y_0(125)(\mathbb{Q})$ is empty from the fact that the jacobian of C has only finitely many points rational in k. The proof of the latter fact forms the subject of Section 2.

The other subject touched upon here relates to elliptic curves defined over quadratic fields and their torsion points of order 25 and 49. We show that such points cannot be rational over such quadratic fields.

In an earlier paper [**6**] we proved this for $N = 32$. Our technique consists in showing that the number of $\mathbb{Q}$-rational points on the jacobian of a certain non-hyperelliptic curve is finite. The finiteness of the Mordell-Weil group in that case was proved by the method of Mazur and Tate [**10**]. With respect to the situation when $N = 25$ this has already been done for a curve B by Kubert [**7**]. Consequently we show that the curve B is not hyperelliptic, determine the exact order of $J(B)(\mathbb{Q})$ and then deduce that $Y_1(25)$ has no point of degree 2.

In the case when $N = 49$, the appropriate curve turns out to be a $\mathbb{Q}$-descent of

Received 21 February, 1980; revised 25 April, 1980.

[J. London Math. Soc. (2), 23 (1981), 415–427]

the Klein curve $X(7)$. It is well known that the jacobian of this has only finitely many points rational over $\mathbb{Q}(\sqrt[7]{1})$. The same procedure as outlined above is followed in this case.

On the advice of Barry Mazur and the referee the exposition has been rather simplified. I am grateful to both of them.

2. *The curve* $y^5 = x(x-\alpha)$

Let $k = \mathbb{Q}(\sqrt[5]{1})$ denote the cyclotomic field of the 5-th roots of unity. Suppose we put $\varepsilon = \exp(2\pi i/5)$ and $\alpha = (\varepsilon-\varepsilon^4)\sqrt{5}$. We will consider the hyperelliptic curve

$$C : y^5 = x(x-\alpha).$$

The curve C is of genus 2. Both C and its jacobian J are defined over k and have good reduction everywhere in k except at the ideal $p = (1-\varepsilon)$ which is completely ramified in k. The automorphism

$$x \longrightarrow x, \qquad y \longrightarrow y\varepsilon$$

of C induces on J complex multiplication by $\mathbb{Z}[\varepsilon]$, the ring of integers of k.

We note that on C we have the following decomposition into prime divisors:

$$(x) = 5(P_0 - P_\infty),$$

where

$$(x-\alpha) = 5(P_1 - P_\infty) \qquad \text{and} \qquad (y) = P_0 + P_1 - 2P_\infty.$$

Our main aim in this section is to prove the following.

PROPOSITION 1. *The jacobian J has only finitely many points rational over k.*

Proof. Let $R = \mathbb{Z}[\varepsilon, 1/(1-\varepsilon)]$ and $S = \operatorname{Spec}(R)$. We denote the Neron model of J over S by the same letter J. This is an abelian S-scheme. The closure of the group generated by the class of $P_0 - P_\infty$ in the scheme J is a finite and flat group scheme over S. Since the Galois module of this group scheme is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ (and also to μ_5), the scheme itself is isomorphic over S to both $\mathbb{Z}/5\mathbb{Z}$ and μ_5. This follows from Theorem 3 of Oort and Tate [**13**], since 5 is totally ramified in k and the ramification degree is 4.

From the Kummer sequence

$$0 \longrightarrow \mathbb{Z}/5\mathbb{Z} \longrightarrow J \xrightarrow{\lambda} J \longrightarrow 0$$

of S-schemes in the *fppf*-topology [**2**; exposé IV, 6.3], where $\lambda = 1-\varepsilon$, we get the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}/5\mathbb{Z} & \longrightarrow & J(k) & \xrightarrow{\lambda} & J(k) & \xrightarrow{\alpha} & H^1(S,\mu_5) \longrightarrow \\
 & & \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_3} & & \downarrow{\scriptstyle \rho} \\
0 & \longrightarrow & \mathbb{Z}/5\mathbb{Z} & \longrightarrow & J(K) & \xrightarrow{\lambda} & J(K) & \xrightarrow{\alpha'} & H^1(K,\mu_5) \longrightarrow .
\end{array}$$

Here $K = \mathbb{Q}_5(\varepsilon)$ where $\mathbb{Q}_5$ is the 5-adic completion of $\mathbb{Q}$; Spec K is an S-scheme. Note that we have used the above isomorphism of $\mathbb{Z}/5\mathbb{Z}$ and μ_5 to equate $H^1(S, \mu_5)$ and $H^1(S, \mathbb{Z}/5\mathbb{Z})$, and the corresponding ones for K. Also in the diagram, γ_1, γ_2 and γ_3 are injective since they are just embeddings.

LEMMA 1. *To complete the proof of the proposition it suffices to show that*

(i) ρ *is injective,*

(ii) $\operatorname{Im}\rho \cap \operatorname{Im}\alpha' = \mathbb{Z}/5\mathbb{Z}$.

Proof. (i) and (ii) imply that the image of α is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. Hence multiplication by λ induces a surjective map on $J(k)/\mathrm{Tors}$ which is a torsion-free $\mathbb{Z}[\varepsilon]$-module. This is impossible unless $J(k)/\mathrm{Tors}$ is trivial.

LEMMA 2. *The map* ρ *is injective.*

Proof. From the Kummer sequence

$$0 \longrightarrow \mu_5 \longrightarrow G_m \longrightarrow G_m \longrightarrow 0,$$

where G_m is the multiplicative group, we have that

$$H^1(S, \mu_5) = R^\times/R^{\times 5} \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}.$$

The first isomorphism follows from Hilbert's 'Theorem 90'. Similarly,

$$H^1(K, \mu_5) \cong K^\times/K^{\times 5} \cong \underbrace{\mathbb{Z}/5\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/5\mathbb{Z}}_{6 \text{ copies}}.$$

As a basis of the latter group we can take λ, ε, $E_a = \exp(\lambda^a)$, where $a = 2, 3, 4$ and 5. We note that $V_\lambda(5) = 4$. A basis for $R^\times$ is λ, ε, $1+\varepsilon$. Note that when we embed k in K, $(1+\varepsilon)/E_2$ is a fifth power.

Since ρ is just the embedding of k in K, it is obvious that λ, ε and $1+\varepsilon$ are not fifth powers in K. Hence ρ is injective.

LEMMA 3. *We have* $\operatorname{Im}\rho \cap \operatorname{Im}\alpha' = \mathbb{Z}/5\mathbb{Z}$.

Proof. Following Faddeev [1] we use an explicit form of the maps α and α'.

Let D be a divisor class of degree 0 on C rational over an extension L of k. Suppose $d = \sum_{i=1}^{r} n_i P_i$ is a divisor in the class D; then we put

$$((x), d) = \prod_{i=1}^{r} x(P_i)^{n_i}.$$

In the product the factor corresponding to P_∞ is to be omitted while $x(P_0)$ should be equated to α^{-1}.

We also define

$$\beta(D) = ((x), d) \,.\, L^{\times 5}$$

First, we show that $\beta(D)$ is independent of the choice of the representative d chosen. To do this we shall show that $((x), d)$ is a fifth power in L if d is a principal divisor rational in L.

We write (f) for the divisor of a rational function f. The following computations are straight forward: $((x), (x)) = \alpha^{-5}$; and $((x), (x-a)) = a^5$ for $a \in \bar{L}$, the algebraic closure of L, and $a \neq 0$. Using the multiplicative property of the symbol we have $((x), (f(x))) = f(0)^5$, if $f(x) \in \bar{L}(x)$ and $f(0) \neq 0$ or ∞, while

$$((x), (y)) = 1 \qquad \text{and} \qquad ((x), (y-a)) = a^5 \text{ for } a \neq 0 \,.$$

Hence $((x), (f(y))) = (f(0))^5$ for $f(y) \in \bar{L}(y)$ and $f(0) \neq 0$ or ∞.

Let Nm denote the norm from $\bar{L}(x, y)$ to $\bar{L}(x)$. Suppose $P \neq P_0$ is a prime divisor of C. Then $x(P)$ is the value at $x = 0$ of the function $x(P) - x$ whose divisor is $\mathrm{Nm}(P - P_\infty)$. Consequently if $d = (f(x, y))$ and P_0 does not occur in d, then

$$((x), d) = \mathrm{Nm} f(x, y)\,|_{(0,0)} = \prod_{i=0}^{4} f(x, y\varepsilon^i)\,|_{(0,0)} \,.$$

This is obviously a fifth power in L if $f(x, y) \in L(x, y)$.

Finally if P_0 occurs in the decomposition of $d = (f(x, y))$ with multiplicity n, then $(f(x, y)y^{-n})$ has no P_0 as a summand and this is a fifth power in $L^\times$ if $f(x, y) \in L^\times$.

It follows that $\beta(D)$ does not depend on the choice of the representative d and the map $D \to \beta(D)$ is a homomorphism.

The group of values of β (for a fixed L) is generated by the norms of the x values of the points on the curve C with coordinates algebraic over L. In fact, by the Riemann-Roch theorem, it suffices to compute this for representatives of the form $P + Q - 2P_\infty$, where $P + Q$ is rational over K (either both P and Q are rational or they are conjugate over K and lie in a quadratic extension of K).

Suppose we now fix $L = K$. From the equation

$$y^5 = x(x - \alpha)$$

we can express x explicitly in terms of y as follows:

$$x = \frac{\alpha}{2} \pm \frac{\alpha}{2}\left(1 + \frac{4y^5}{\alpha^2}\right)^{1/2}$$

if y^5/α^2 lies in the ideal $p = (\lambda)$, and

$$x = \pm y^{5/2}\left(1 + \frac{\alpha^2}{4y^5}\right)^{1/2} + \alpha/2$$

if α^2/y^5 does. Since $V_\lambda(y^5/\alpha^2) = 5V_\lambda(y) - 6$, it is clear that if y is at most quadratic

over K, then $V_\lambda(y^5/\alpha^2)$ cannot lie between -1 and $+3/2$ and the convergence of the binomial series is assured.

Let P be a K-rational prime divisor corresponding to (x_0, y_0) with $x_0 \neq 0$ and $y_0 \neq 0$. Suppose that $V_\lambda(x_0) > 0$. Then $V_\lambda(y_0^5/\alpha^2) \geqslant 4$; x_0 is of the form $\alpha \,.\, u \,.\, \gamma^5$ with $\gamma \in K^\times$ if $V_\lambda(x_0) = 3$, and of the form $\alpha^4 \,.\, u \,.\, \gamma^5$ if $V_\lambda(x_0) > 3$. In both cases $V_\lambda(u-1) \equiv 4 \pmod 5$. However, $V_\lambda(x_0)$ cannot take either the value 1 or 2.

If $V_\lambda(x_0) \leqslant 0$, then $V_\lambda(\alpha^2/y^5) \geqslant 6$; it is also congruent to 6 modulo 5. Thus it follows that x_0 is of the form $u \,.\, \gamma^5$ where $V_\lambda(u-1) \equiv 3 \pmod 5$.

Let now $P+Q$ be K-rational with P (and Q) rational in a quadratic extension of K. If y_0 lies in K, then $x(P) \,.\, x(Q) = y_0^5$. If λ is not ramified in the quadratic extension then the situation will be the same as in the case of a K-rational P. Otherwise, we can first suppose that $V_\lambda(x(P)) \leqslant 0$; then $2V_\lambda(x_0) \equiv 0 \pmod 5$ and $V_\lambda(y_0^5) = 2V_\lambda(x_0)$. Also $V_\lambda(\alpha^2/y^5) \equiv 1 \pmod 5$, and is greater than or equal to 6.

Suppose $V_\lambda(x(P)) \geqslant 3$; then $2V_\lambda(y_0^5) \geqslant 15$. In this case, if $V_\lambda(y_0^5) \geqslant 10$, then $V_\lambda(y^5/\alpha^2) \geqslant 4$, so that $x(P) \,.\, x(Q) = \alpha^i \,.\, u \,.\, \gamma^5$ with $i = 2$ or 3 and $V_\lambda(u-1) \geqslant 4$. If $2V_\lambda(y_0^5) = 15$, then $2V_\lambda(y^5/\alpha^2) = 3$ so that $x(P) \,.\, x(Q) = \alpha^i \,.\, u \,.\, \gamma^5$ with $V_\lambda(u-1) \geqslant 2$ and $i = 2$ or 3.

Lastly, we can have $2V_\lambda(x(P)) = 5$ with $V_\lambda(y_0^5) = 5$ so that $V_\lambda(\alpha^2/y_0^5) = 1$ and $x(P) \,.\, x(Q) = u \,.\, \gamma^5$ with $V_\lambda(u-1) \geqslant 1$.

In the two latter cases, it can, with a lot of difficulty, be shown that $V_\lambda(u-1) \geqslant 3$. However we can argue as follows. The map β is a homomorphism so that the image of the $J(K)$ under it is a group. Furthermore $x(P_0) = \alpha^{-1}$ and $x(P_1) = \alpha$. Also, by the Riemann-Roch theorem, every divisor class of degree 0 on C has a representation of the form $P'+Q'-2P_\infty$. Suppose, for instance, that the value of β on the class of $P+Q-2P_\infty$ were $u_0 \,.\, \gamma^5$ with $V_\lambda(u_0-1) = 1$; then that of $P+Q+P_1-3P_\infty$, which is also rational, would be $\alpha \,.\, u_0 \,.\, \gamma$. However this does not occur in all the possible cases we have examined. Hence we must have $V_\lambda(u_0-1) \geqslant 3$.

Consequently the image of β is of the form

$$\alpha^i \,.\, u \,.\, \gamma^5 \quad \text{with} \quad i \in \mathbb{Z}, \quad \gamma \in K^\times,$$

and $V_\lambda(u-1) = m$ where m is congruent to 0, 3 or 4 modulo 5.

By Theorem 1 of [**1**] we know that β and α' are the same. We have already seen that the elements of $\operatorname{Im}\rho$ are of the above form with $m = 0$, 1 or 2 (modulo 5); so $\operatorname{Im}\alpha' \cap \operatorname{Im}\rho$ is isomophic to $\mathbb{Z}/5\mathbb{Z}$.

This completes the proof of Proposition 1.

The equation $y^5 = x(x-\alpha)$ reduces modulo 11 to

$$y^5 = x(x-\bar{4}). \tag{2}$$

This is still of genus 2. There are 23 points on it rational in GF(11) and 103 points in GF(121).

Suppose $f(X)$ is the characteristic polynomial associated with the zeta function of the reduction of C over GF(q). Let $F(Y)$ be the polynomial such that $X^g F(x+q/X) = f(X)$, where g is the genus of C. Then $F(Y) = Y^2 + 11Y + 29$ for the curve (1) with $q = 11$. The number of points on the reduction of the jacobian J of C at $q = 11$ is thus $f(12) = 305$.

3. *The modular curve* $X_0(125)$

Let $\eta(z)$ be the modular form of dimension $-\frac{1}{2}$

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

where $q = \exp(2\pi iz)$. The functions

$$X(\omega) = \eta(\omega)/\eta(25\omega) \quad \text{and} \quad Y(\omega) = \eta(5\omega)/\eta(125\omega)$$

satisfy the hypothesis of a theorem of Newmann [**11**] and are therefore functions on $X_0(125)$ defined over $\mathbb{Q}$. The algebraic equation relating $X(\omega)$ and $Y(\omega)$ can be deduced as follows.

Let

$$f(\tau) = \eta^2(\tau/5)/\eta^2(\tau) \qquad \text{and} \qquad g(\tau) = \eta(\tau/25)/\eta(\tau).$$

Weber [**14**; p. 256] showed that

$$f^3 = g^5 + 5g^4 + 15g^3 + 25g^2 + 25g = g\,G(g).$$

We note that

$$X(\omega) = g(25\omega) \qquad \text{and} \qquad Y(\omega) = g(125\omega).$$

If we put

$$h(\omega) = f(25\omega) \qquad \text{and} \qquad l(\omega) = f(125\omega),$$

then

$$h^3(\omega) = XG(X) \qquad \text{and} \qquad l^3(\omega) = YG(Y).$$

Since $Y^2 = hl$ it follows that

$$Y^5 = XG(X)G(Y). \tag{3}$$

Let $j(\omega)$ be the classical modular invariant with $j(\sqrt{-1}) = 1728$. Weber [**14**; p. 256] showed that

$$\sqrt[3]{j(25\omega)} = (h^6 + 10h^3 + 5)/h \tag{4}$$

and

$$\sqrt[3]{j(125\omega)} = (l^6 + 10l^6 + 5)/l. \tag{5}$$

The scheme of zeros of X, Y, $j(\omega)$ and $j(5\omega)$ is as follows.

	P_0	P_i	P_j	P_∞
X	5	0	-1	-1
Y	1	1	0	-5
$j(\omega)$	-125	-5	-1	-1
$j(5\omega)$	-25	-25	-5	-5

Here the cusps P_0, P_∞ are the rational cusps, while P_i, P_j for $i, j = 1, 2, 3, 4$ form two complete sets of conjugates over $\mathbb{Q}$ and lie in $\mathbb{Q}(\sqrt[5]{1})$ (Ogg [**12**; Proposition 2]).

The function X is a 'Hauptmodul' for $X_0(25)$ while Y is not invariant by $\Gamma_0(25)$. From the scheme of zeros of X and Y we see that the degrees $[\mathbb{Q}(X_0(125)) : \mathbb{Q}(X)]$ and $[\mathbb{Q}(X_0(125)) : \mathbb{Q}(Y)]$ are both equal to 5; hence

$$\mathbb{Q}(X, Y) = \mathbb{Q}(X_0(125)).$$

In particular, corresponding to a $\mathbb{Q}$-rational point x on $X_0(125)$ there is a $\mathbb{Q}$-rational pair (X', Y'), although the converse is not necessarily true.

Lastly we note that $X(\omega)$ and $Y(\omega)$ are units in the integral closure of $\mathbb{Z}[j(\omega), \frac{1}{5}]$ in $\mathbb{Q}(X_0(125))$ [**8**; p. 163] and that the Atkin-Lehner involution W_{125} takes X to $5/Y$ and Y to $5/X$.

LEMMA 4. *Suppose (x_0, y_0) is a $\mathbb{Q}$-rational point on the curve defined by equation* (3) *with (x_0, y_0) being neither $(0, 0)$ nor (∞, ∞). Then either*

(i) $x_0 = \delta 5^{5s+1} t^5/mn$ *and* $y_0 = \delta 5^{s+1} tr/n^5$

or

(ii) $x_0 = \delta t^5/5^s mn$ *and* $y_0 = \delta tr/5^{5s} n^5$,

where n, m, t and r are pair-wise coprime positive integers not divisible by 5, s is a non-negative rational integer and $\delta = \pm 1$. Furthermore $x_0 y_0 \geqslant 0$.

Proof. Let p be a prime number not equal to 5. Suppose $v_p(x_0) = u$. If $u > 0$ then $v_p(G(x_0)) = 0$; clearly $v_p(y_0) > 0$ and $v_p(G(y_0)) = 0$, so that $u = 5v_p(y_0)$ and p divides t.

If $u < 0$, then $v_p(x_0 G(x_0)) = 5u$; if $v_p(y_0) < 0$ then $v_p(y_0) = 5u = -v_p(y_0^{-5} G(y_0))$; this implies that p divides n. On the other hand if $v_p(y_0) = 0$, then $v_p(G(y_0)) = -5u$ so that p divides m. The case in which $v_p(y_0) > 0$ is not possible.

Now suppose $v_p(y_0) = u$. Suppose first that $u > 0$. Then $v_p(G(y_0)) = 0$, so $v_p(x_0 G(x_0)) = 5u$. If $v_p(x_0) \neq 0$ then $v_p(x_0) = 5u$ and p divides t. If $v_p(x_0) = 0$ then p divides r.

Suppose $u < 0$; then $v_p(x_0(G(x_0))) < 0$, and consequently $u = 5v_p(x_0)$; this implies that p divides n.

Hence (x_0, y_0) conforms to the patterns of (i) and (ii) with respect to $p \neq 5$.

Suppose we put $v_5(x_0) = 0$. Suppose $u > 0$; then $v_5(x_0 G(x_0)) = u + 2 = v_5(y_0^5 G(y_0)^{-1})$. Hence if $v_5(y_0) > 0$, then $u \equiv 1 \pmod 5$ and we are in case (i). However $v_5(y_0)$ cannot be zero if u is positive.

Suppose that $u \leqslant 0$; then $v_5(x_0 G(x_0)) = 5u$; this implies that $v_5(y_0^5 G(y_0)^{-1}) = v_5(y_0) = 5u$ and we are in case (ii).

As G is positive definite, $x_0 y_0 \geqslant 0$. This completes the proof of the lemma.

Remark. The primes p dividing m and r are those primes at which (x_0, y_0) reduces to the same point of $X_0(125)(\mathrm{GF}(p))$ as one of the non-rational cusps. Since the reductions of these cusps are not $\mathrm{GF}(p)$ rational unless $p \equiv 1 \pmod 5$, it follows that the primes dividing m and r are congruent to 1 modulo 5. In particular, 2 does not divide either m or r.

Suppose we write $\bar{G}(u, v)$ for $v^4 G(u/v)$. The polynomial $\bar{G}(u, v)$ can be factorised over $\mathbb{Z}[\varepsilon]$ as

$$\bar{G}(u, v) = \prod_{i=1}^{4} (u - \theta_i v), \tag{6}$$

where $\theta_1 = \varepsilon\sqrt{5}$ and $\theta_2 = -\varepsilon^2\sqrt{5}$, while $\theta_3 = -\varepsilon^3\sqrt{5}$ and $\theta_4 = \varepsilon^4\sqrt{5}$.

If u and v are coprime rational integers and 5 does not divide u, then the only common factors of any pair of the factors on the right hand side of (6) in $\mathbb{Z}[\varepsilon]$ are units.

LEMMA 5. *Suppose u_0 and v_0 are coprime non-zero rational integers and 5 does not divide u_0. If u_0 and v_0 satisfy the equation*

$$\bar{G}(u, v) = z^5 \tag{7}$$

for some rational integer z_0 coprime to 10, then

$$u_0 - \theta_1 v_0 = \zeta^5$$

where ζ is an integer of $\mathbb{Z}[\varepsilon]$. Furthermore 10 divides v_0.

Proof. From the remarks above it follows that

$$u_0 - \theta_1 v_0 = \mu\zeta^5,$$

where μ is a unit and ζ is an integer of $\mathbb{Z}[\varepsilon]$. The units of $\mathbb{Z}[\varepsilon]$ are generated by $\pm 1, \varepsilon$ and $1+\varepsilon$. Also we can write

$$\theta_1 = -(2+\varepsilon+2\varepsilon^2) \quad \text{and} \quad \theta_2 = (2\varepsilon^3+\varepsilon^2+2\varepsilon)$$

while

$$\theta_3 = -(2+2\varepsilon+\varepsilon^3) \quad \text{and} \quad \theta_4 = -(\varepsilon^3-\varepsilon^2-\varepsilon+1).$$

Hence we have that

$$u_0 + (2+\varepsilon+2\varepsilon^2)v_0 = \varepsilon^i(1+\varepsilon)^j\zeta^5 \tag{9}$$

with $0 \leqslant i, j \leqslant 4$. If we write

$$\zeta = a + b\varepsilon + c\varepsilon^2 + d\varepsilon^3$$

with a, b, c, and $d \in \mathbb{Z}$, then we get

$$\zeta^5 = A + B\varepsilon + C\varepsilon^2 + D\varepsilon^3$$

with A, B, C and D belonging to $\mathbb{Z}$, and each expressible in terms of a, b, c and d. It is easy to see that all but A are divisible by 5 if 5 does not divide z_0.

By comparing coefficients in equation (9) and its conjugates, it is not difficult to see that the only possibilities for i and j are as follows:

(I) $i = 0$ and $j = 0$ when 5 divides v_0;

(II) $i = 0$ and $j = 2$ when 5 divides u_0;

(III) $i = 2$ and $j = 3$ when 5 divides u_0;

(IV) $i = 4$ and $j = 4$ when 5 divides u_0.

Hence, if we assume as in the hypothesis that 5 does not divide u_0, we are left with the case where $i = 0$ and $j = 0$, and we have that 5 divides v_0.

In this case, by again comparing coefficients, we see that both D and C should be even ($D = 0$). This is possible only if exactly three of a, b, c and d are even; this implies that v_0 is even.

This completes the proof of the lemma.

We can now prove the main theorem.

THEOREM 1. *The curve* $Y_0(125)(\mathbb{Q})$ *is empty.*

Proof. Let $x \in Y_0(125)(\mathbb{Q})$ and let ω_0 be a point in the upper half plane H which corresponds to x in the orbit space $H/\Gamma_0(125)$. Put $X' = X(\omega_0)$ and $Y' = Y(\omega_0)$. Both X' and Y' are rational numbers; by well-known properties of the eta-function, $(X', Y') \neq (0, 0)$ and $(X', Y') \neq (\infty, \infty)$. They also satisfy equation (3).

By Lemma 4, there are two possibilities for X' and Y': either

(i) $X' = \delta 5^{5s+1} t^5/mn$ and $Y' = \delta 5^{s+1} tr/n^5$, or

(ii) $X' = \delta t^5/5^s mn$ and $Y' = \delta tr/5^{5s} n^5$,

where m, n, t and r are coprime positive integers, not divisible by 5, s is a non-negative integer and $\delta = \pm 1$. Also $X'Y' \geqslant 0$. Furthermore we know that the prime factors of m and r are congruent to 1 modulo 5.

The two cases are not independent really; one corresponds to the other under the Atkin-Lehner involution W_{125}. It therefore suffices to deal with just one of them, say (i).

For $\bar{G}$ as described earlier, by substituting the expression in (i) for X' and Y' in equation (3), one finds that

$$\bar{G}(mn, \delta 5^{5s} . t^5) = r^5 , \tag{10}$$

where mn, $\delta 5^{5s} . t^5$ and r satisfy the hypothesis of Lemma 5, so that

$$mn - \theta_1 . \delta 5^{5s} . t^5 = \zeta_1^5 \tag{11}$$

for some integer ζ_1 of $\mathbb{Z}[\varepsilon]$; also $s > 0$ and t is even.

Taking one of the conjugates of (11) in $\mathbb{Z}[\varepsilon]$, we also have

$$mn - \theta_4 \delta 5^{5s} . t^5 = \zeta_1'^5 . \tag{12}$$

Combining equations (11) and (12) leads to

$$(mn - \theta_1 \delta 5^{5s} t^5)(mn - \theta_4 \delta 5^{5s} t^5) = \zeta_1^5 \zeta_1'^5 . \tag{13}$$

Dividing through by $5^{10s} . t^{10}$ and substituting

$$y' = \zeta_1 \zeta_1' / 5^s t \qquad \text{and} \qquad h' = (mn/\delta 5^{5s} t^5) - \theta_1 \delta$$

leads to

$$y'^5 = h'(h' - \alpha) . \tag{14}$$

To complete the proof it suffices to show that (14) is impossible.

From Proposition 1 we have that $|J(\mathbb{Q}(\varepsilon))|$ is finite and from reduction modulo 11 we know that its order is odd.

Since the curve C has good reduction modulo 2, this implies that the reduction mapping modulo 2 induces an injective mapping of $J(\mathbb{Q}(\varepsilon))$.

Let P be the point on C corresponding to (h', y') of (14). As t is even, 2 divides the denominators of h' and y' so that $\tilde{P} = \tilde{P}_\infty$ where $\sim$ indicates the reduction of the point modulo 2. Clearly P is not P_∞. Hence the divisor class of $P - P_\infty$ reduces to 0 modulo 2. Since reduction modulo 2 is injective on J, this implies that $P - P_\infty$ is linearly equivalent to 0. But C has genus 2; hence $P = P_\infty$ and this leads to a contradiction.

This completes the proof of Theorem 1.

4. *The curves* $X_1(25)$ *and* $X_1(49)$

We consider the modular curves $X_1(N)$ for $N = 25$ and $N = 49$.

Let Γ denote the group $(\mathbb{Z}/N\mathbb{Z})^\times / \{\pm 1\}$. If m is coprime to N, we denote its image in Γ by γ_m. Now $\Gamma \cong \Gamma_0(N)/\Gamma_1(N)$ and this induces an action of Γ on $X_1(N)$.

Let us fix $N = 25$. The cyclic covering $X_1(25) \xrightarrow{10} X_0(25)$ can be factored through a curve B of genus 4 over $\mathbb{Q}$: we have

$$X_1(25) \xrightarrow{2} B \xrightarrow{5} X_0(25)$$

and $B = X_1(25)/\gamma_2^5$. The curve B has 5 rational cusps, a collection of 4 cusps of degree 4 and one of 5 cusps of degree 5.

Kubert [7], following the method of [10], has shown that $J(B)(\mathbb{Q})$ is finite for the jacobian $J(B)$ of B. The rational cusps also generate a group of order 71. We shall show that $|J(B)(\mathbb{Q})| = 71$.

As we described in [6; p. 238], the number of points on B defined over a finite field $GF(q)$ can be computed by using the moduli properties of B.

We denote by $C_p^{(i)}$ the number of points of B in $\mathrm{GF}(p^i)$. We have

$$C_2^{(1)} = 5 \quad \text{and} \quad C_3^{(1)} = 5,$$

$$C_2^{(2)} = 5 \quad \text{and} \quad C_3^{(2)} = 5,$$

$$C_2^{(3)} = 20 \quad \text{and} \quad C_3^{(3)} = 20,$$

$$C_2^{(4)} = 29 \quad \text{and} \quad C_3^{(4)} = 89.$$

The fifteen additional points on GF(8) arise from the curves with complex multiplication by $\mathbb{Z}\left[\frac{1+\sqrt{-31}}{2}\right]$: there are 5 for each of the 3 conjugate invariants. The 9 cusps are rational in GF(16) and the other 20 points correspond to complex multiplication by $\mathbb{Z}\left[\frac{1+\sqrt{-39}}{2}\right]$. The 15 additional points on GF(27) are from complex multiplication by $\mathbb{Z}\left[\frac{1+\sqrt{-59}}{2}\right]$ while the 80 others on GF(81) arise from curves with complex multiplication by $\mathbb{Z}[\sqrt{-56}]$, $\mathbb{Z}[\sqrt{-14}]$ and $\mathbb{Z}[5(1+\sqrt{-11})/2]$.

Let $F(y)$ be the function defined in Section 1. Then for the curve B at $q = 2$,

$$F(y) = y^4+2y^3-6y^2-7y+11$$

so that

$$F(3) = |J(B)(\mathrm{GF}(2))| = 71.$$

At $q = 3$ we have

$$F(y) = y^4+y^3-14y^2-14y+31,$$

so that

$$F(4) = |J(B)(\mathrm{GF}(3))| = 71.$$

It follows easily then that $J(B)(\mathbb{Q}) = 71$.

If B were hyperelliptic then it would have at most $2(8+1)$ points on GF(8); since $C_2^{(3)} = 20$ it follows that B is not hyperelliptic.

THEOREM 2. *There are no non-cusp points of degree* 2 *on* $X_1(25)$.

Proof. Let P be a point of degree 2 on $X_1(25)$ and let P' be its image on B. Then P' is also a non-cusp point of degree 1 or 2. If the degree is 1 let Q be any point of degree 1 on B; otherwise let Q be the conjugate of P'. Since the only points of B over GF(4) are the reductions of rational cusps, there are cusps P_1 and P_2 such that P', Q have the same reduction modulo 2 as P_1 and P_2. So $P'+Q-2P_\infty$ and $P_1+P_2-2P_\infty$ reduce modulo 2 to the same point of $J(B)(\mathrm{GF}(2))$; since $|J(B)(\mathbb{Q})| = 71$, reduction modulo 2 is injective on $J(B)(\mathbb{Q})$, and so $P'+Q-2P_\infty$ and $P_1+P_2-2P_\infty$ are the same point of $J(B)(\mathbb{Q})$. So $P'+Q$ is linearly equivalent to P_1+P_2; as they are different and B is not hyperelliptic this is not possible.

Suppose now that we fix $N = 49$. The cyclic covering $X_1(49) \xrightarrow{21} X_0(49)$

factors through a curve A defined over $\mathbb{Q}$,

$$X_1(49) \xrightarrow{7} A \xrightarrow{3} X_0(49),$$

where $A = X_1(49)/\gamma_2^3$ and is of genus 3. The curve A possesses 3 cusps rational over $\mathbb{Q}$, 3 conjugate ones in a cubic field and 3 collections of 6 cusps rational in fields of degree 6.

We can describe A as $\overline{H/\Gamma_*}$ where

$$\Gamma_* = \left\{\Gamma_1(49), \begin{pmatrix} -13 & 3 \\ 147 & -34 \end{pmatrix}\right\}$$

so that $\begin{pmatrix} -13 & 3 \\ 147 & -34 \end{pmatrix}$ has the same effect as γ_2^3 on $X_1(49)$. It turns out that Γ_* is conjugate to the Kleinian group $\Gamma(7)$. In fact, if $U = \begin{pmatrix} 0 & -1 \\ 7 & 0 \end{pmatrix}$, then

$$\Gamma_* = U\Gamma(7)U^{-1} = \Gamma_0(49) \cap \Gamma_1(7).$$

The curve A is thus a $\mathbb{Q}$-descent of $X(7)$ which is birationally isomorphic to it over $\mathbb{Q}(\sqrt[7]{1})$. It is well known (Fadeev [1]) that $X(7)$ can be defined by the equation

$$x^3y + y^3 + x = 0,$$

and that it is birationally isomorphic to

$$x^2(1-x) = y^7$$

over $\mathbb{Q}(\sqrt[7]{1})$. Furthermore if $J(7)$ is the jacobian of $X(7)$, then $|J(7)(\mathbb{Q}(\sqrt[7]{1}))|$ is finite. We therefore have that, if $J(A)$ is the jacobian of A, then $J(A)(\mathbb{Q})$ is finite.

As in the case of B we have for A that $C_2^{(1)} = 3$ while $C_2^{(2)} = 5$ and $C_2^{(3)} = 24$; the two non-cusp points on GF(4) come from the supersingular invariant and are ramified over $X_0(49)$ while those in GF(8) are all the cusps. For $q = 2$,

$$F(y) = y^3 - 6y + 5 = (y-1)(y^2 + y - 5)$$

so that

$$F(3) = |J(A)(\mathrm{GF}(2))| = 14.$$

Again since $C_2^{(3)} = 24$, we see that A is not hyperelliptic.

The rational cusps of A generate a group of order 7 on $J(A)(\mathbb{Q})$; this can be seen by using the method of Ogg [**12**].

Finally we note that the only cusps of A rational in GF(3) and GF(9) are the 3 rational cusps. Three of the remaining are rational in GF(27) and the rest in GF(3^6) since the residue degree of 3 is 6 in $\mathbb{Q}(\sqrt[7]{1})$.

THEOREM 3. *There are no non-cusp points of degree* 2 *on* $X_1(49)$.

Proof. Let P be a non-cusp point of degree 2 on $X_1(49)$. Then its reduction

modulo 3 on $X_1(49)$ is a cusp. This follows from the fact that by the Riemann hypothesis no elliptic curve defined over GF(9) can have a torsion point of order 49 rational in GF(9) and that $X_1(N)$ is a fine moduli scheme for $N > 3$.

So let P' be the projection on A. The reduction of P' in GF(9) is rational in GF(9) and therefore a cusp. Let Q be defined in a way similar to that in Theorem 2 and let P_1 and P_2 be cusps with the same reduction as P' and Q.

Since 3 does not divide $|J(A)(\mathbb{Q})|$ the reduction of $J(A)$ modulo 3 is injective. However the class of $P'+Q-P_1-P_2$ reduces to the zero class. Hence $P'+Q$ is linearly equivalent to P_1+P_2. As P' is different from either P_1 or P_2 and A is not hyperelliptic we get a contradiction.

This completes the proof of the theorem.

References

1. D. K. Faddeev, "On the divisor class groups of some algebraic curves", *Dokl. Akad. Nauk. SSSR*, 136 (1961), 296–298; *Soviet Math. Dokl.*, 2 (1961), 67–69.
2. M. Demazure and A. Grothendieck, *Schémas en Groupes* I, Lecture Notes in Mathematics, 151 (Springer, Berlin, 1970).
3. M. A. Kenku, "The modular curve $X_0(39)$ and rational isogeny", *Math. Proc. Cambridge Philos. Soc.*, 85 (1979), 21–23.
4. 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.
5. M. A. Kenku, "The modular curve $X_0(169)$ and rational isogeny", *J. London Math. Soc.* (2), 22 (1980), 239–244.
6. M. A. Kenku, "Certain torsion points on elliptic curves defined over quadratic fields", *J. London Math. Soc.* (2), 19 (1978), 233–240.
7. S. D. Kubert, "Universal bounds on the torsion of elliptic curves", *Proc. London Math. Soc.* (3), 33 (1976), 193–237.
8. S. Lang, *Elliptic functions* (Addison-Wesley, Reading, Mass., 1973).
9. B. Mazur, "Rational isogenies of prime degree", *Invent. Math.*, 44 (1978), 129–162.
10. B. Mazur and J. Tate, "Points of order 13 on elliptic curves", *Invent. Math.*, 22 (1973), 41–49.
11. M. Newmann, "Construction and application of a class of modular functions", *Proc. London Math. Soc.* (3), 7 (1957), 331–350; 9 (1959), 373–387.
12. A. P. Ogg, "Rational points on certain elliptic modular curves", Proceedings Symposia in Pure Mathematics 24 (American Mathematical Society, Providence, 1973), pp. 221–231.
13. F. Oort and J. Tate, "Group schemes of prime order", *Ann. Sci. Ecole Norm. Sup.* (4), 3 (1976), 1–21.
14. H. Weber, *Lehrbuch der Algebra*, Vol. III (Teubner, 1908, and Chelsea, New York, 1961).

School of Mathematics,
The Institute of Advanced Study,
Princeton,
New Jersey 08540,
U.S.A.