A NOTE ON THE INTEGRAL POINTS OF A MODULAR CURVE OF LEVEL 7

M. A. KENKU

§1. *Introduction.* Let $X_{ns}^{n}(N)$ denote the modular curve associated with the normalizer of a non-split Cartan group of level N, where N is an arbitrary integer. The curve $X_{ns}^{n}(N)$ is defined over $\mathbf{Q}$ and the corresponding scheme over $\mathbb{Z}[1/N]$ is smooth [**1**]. If N is a prime, the genus formula for $X_{ns}^{n}(N)$ is given in [**5, 6**]. The curve $X_{ns}^{n}(N)$ has genus 0 if $N<11$ and $X_{ns}^{n}(11)$ has genus 1. Ligozat [**5**] has shown that the group of $\mathbf{Q}$-rational points on $X_{ns}^{n}(11)$ has rank 1. If the genus $g(N)$ is greater than 1, very little is known about the $\mathbf{Q}$-rational points of $X_{ns}^{n}(N)$. Since under simple conditions imaginary quadratic fields with class number 1 give an integral point on these curves, Serre and others have asked whether all integral points are obtained in this way [**8**].

In this note we determine the j-invariants of elliptic curves corresponding to points of $X = X_{ns}^{n}(7)$ which are integral over $\mathbb{Z}[1/7]$. These are points which are rational over $\mathbf{Q}$ and do not give cusps modulo p for $p \neq 7$. We prove that each such point corresponds to an exceptional unit of the first kind of the field $K = \mathbf{Q}(\cos 2\pi/7)$. Nagell [**7**] has shown that there are 24 such units. Half of these (those arising from the choice of the generator of Gal $(K/\mathbf{Q})$; the other half relate to the other generator) correspond to the integral points of X. They are the values taken by a uniformizing parameter f of X at the integral points. By explicitly constructing f we are able to find a relationship between f and the modular invariant j. Eight of the 12 $\mathbb{Z}[1/7]$-integral points correspond to elliptic curves with complex multiplication (7 of them predictably so; the exception being the point corresponding to the j invariant having the value 0). The j invariants for all the $\mathbb{Z}[1/7]$-integral points and the corresponding units are given in a table at the end of the paper.

A similar investigation may be made of level 9 instead of level 7. The exceptional units of that field have also been determined by Nagell [**7**], but all of these correspond to elliptic curves with complex multiplication.

We note that both $N=7$ and $N=9$ give yet another proof that a 10th imaginary quadratic field with $h=1$ does not exist, since such a field would give an integral point on X, distinct from those already found, since 7 and 3 would respectively have to be inert in the field.

The author thanks J.-P. Serre who found the connection between the integral points and Nagell's units and suggested the determination of the invariants.

§2. *Units and integral points on X.* Let F be an algebraic number field, a unit E of F is called an exceptional unit if there exists another unit E_1 such that

$$E + E_1 = 1.$$

It is well known [2] that there are at most finitely many exceptional units in any given number field F. For F a cyclic cubic field Nagell [7] has called an exceptional unit of F which satisfies an equation of the form

$$X^3 - pX^2 + (p-3)X + 1 = 0, \tag{1}$$

where p is a rational integer, an exceptional unit of the first kind. The discriminant of the cubic equation is

$$(p^2 - 3p + 9)^2.$$

If E satisfies equation (1) then E_1 satisfies the equation

$$X^3 + (p-3)X^2 - pX + 1 = 0,$$

so that, if E is an exceptional unit of the first kind, so is E_1, and E_1 corresponds to $3-p$. For the field $F = K$, Nagell proved that there are 24 such units corresponding to values of p from $(1, 2)$, $(8, -5)$, $(15, -12)$ and $(1262, -1259)$.

The modular curve X has 3 conjugate cusps which are defined over the field K. Let $\mathbf{P}_1$ be the projective line and σ the automorphism $Z \to 1 - 1/Z$ of $\mathbf{P}_1$ which is of order 3 and permutes $1, 0, \infty$ cyclically. Using σ and $K/\mathbf{Q}$ we can obtain a "twist" C of P_1. The curve C therefore has genus 0 and is defined over $\mathbf{Q}$. It has 3 "marked" points (corresponding to the cusps on C) rational over K which are permuted by the non-trivial automorphisms of K. It is thus a model of X over $\mathbf{Q}$. Let s be the non-trivial automorphism of $K/\mathbf{Q}$ which corresponds to σ by its action on the marked points. We therefore have a K-isomorphism

$$f: X \to \mathbf{P}_1$$

taking the cusps of X to $0, 1, \infty$ and such that $f^s = 1 - f^{-1}$.

The isomorphism between C and X extends to that of their corresponding schemes over $\mathbb{Z}[1/7]$ since the scheme corresponding to X is smooth over $\mathbb{Z}[1/7]$. We prove

LEMMA 1. *Let $x \in X$ be integral over $\mathbb{Z}[1/7]$ (equivalently $x \in X(\mathbf{Q})$ and the j-invariant is in $\mathbb{Z}[1/7]$). Put $\varepsilon = f(x)$, where $f: X \to \mathbf{P}_1$ is the function above, then ε is a unit of K and $s(\varepsilon) = 1 - \varepsilon^{-1}$.*

Proof. Let $x \in X$ be a point of X which is integral over $\mathbb{Z}[1/7]$. Then $\varepsilon = f(x)$ is a unit over $\mathbb{Z}[1/7]$. Also since the $\mathbf{Q}$-rational points of X are defined as those corresponding under f to points y in $\mathbf{P}_1(K)$ satisfying

$$s(y) = 1 - 1/y$$

it suffices to prove that ε is a genuine unit of K.

Let ρ be a generator of the prime ideal above 7 in K. *A priori* we have $\varepsilon = \rho^m u$, where $m \in \mathbb{Z}$ and u is a unit. Hence it suffices to show that $m = 0$.

If $m > 0$ we obtain a contradiction from the equation

$$s(\varepsilon) = 1 - \varepsilon^{-1},$$

since $s(\varepsilon)$ is a conjugate of ε and so is a unit if ε is a unit. Similarly if $m < 0$ we obtain a contradiction. Hence we have $m = 0$ and $\varepsilon = u$. So that ε is a unit. It is an exceptional unit since

$$\varepsilon - \varepsilon \,.\, s(\varepsilon) = 1.$$

From the equation $s(\varepsilon) = 1 - \varepsilon^{-1}$ we can also deduce that it is of the first kind (see Nagell [7]).

Since f is a K-isomorphism, the proof of the lemma shows also that any exceptional unit of the first kind ε of K which satisfies $s(\varepsilon) = 1 - \varepsilon^{-1}$ corresponds to a $\mathbb{Z}[1/7]$-integral point of X.

§3. *The function f and the modular invariant j.* To relate the function f to the modular invariant j we consider X as a covering of $X(1)$, the j-line.

The covering

$$X \longrightarrow X(1)$$

is of degree 21 and is defined over $\mathbf{Q}$. If we extend scalars to $\mathbf{Q}(\sqrt{-7})$, this can be factored through a curve Y

$$X \xrightarrow{d_3} Y \xrightarrow{d_7} X(1)$$

where Y is the modular curve attached to the symmetric group $S_4 \subset PSL_2(F_7)$, and d_3, d_7 are covering maps of degrees 3 and 7 respectively. We may identify Y with the projective line over $\mathbf{Q}(\sqrt{-7})$ by a uniformizing parameter y such that the map

$$Y \xrightarrow{d_7} X(1)$$

is given by

$$j = y(y^2 + 7\lambda y + 7\lambda - 21)^3 \quad \text{where } \lambda = \tfrac{1}{2}(1 + \sqrt{-7})$$

(see [3, p. 89] and [4, p. 752]). It should be noted that the parameters in Fricke-Klein [4] and here are related by $J = j/(2^6 3^3)$ and $\lambda\tau = y$.

Since the point $y = \infty$ on Y corresponds to $f = 0$, 1 and ∞ on X and $y = 0$ on Y has a cubic ramification in the covering $X \to Y$, y must be given by an equation

$$y = \frac{a(f-b)^3}{f(f-1)},$$

for some coefficients a and b in the field $\mathbf{Q}(\sqrt[7]{1})$. So to determine the values of j corresponding to the exceptional units it suffices to determine a and b explicitly. We do this by writing f explicitly in terms of Klein forms $k_{(r,s)}$ where r, s are integers not both congruent to 0 mod 7. Following the method described in [5, Ch. II] we obtain a function

$$f = \mu \frac{k_{(1,0)}k_{(0,1)}k_{(3,2)}k_{(2,3)}k_{(2,5)}k_{(3,5)}k_{(5,3)}k_{(2,9)}}{k_{(1,1)}k_{(2,1)}k_{(1,2)}k_{(1,5)}k_{(1,6)}k_{(3,0)}k_{(0,3)}k_{(5,1)}}$$

where $\mu = \xi^{-2}(1-\xi^2)(1-\xi)/(1-\xi^3)^2$ and $\xi = \exp(2\pi i/7)$. The function f

takes 0, 1 and ∞ respectively at the cusps of X and is normalized so that expansion of y at the cusp, where f has a pole of order 1, is

$$\xi^{\alpha}q^{-1/7}-3\lambda+(\text{terms with positive powers of } q).$$

The constant α satisfies $0\leqslant\alpha\leqslant 6$ and reflects the ambiguity of y. Expressing y as a function of f gives values a and b depending on α. The only value of α which gives y lying in $\mathbf{Q}(\sqrt{-7})$ for the exceptional units is 4. It yields the values $a=\xi^4u^{-1}$ and $b=1+\xi+\xi^4$. From these we obtain the following table.

f	y	p	j	Discriminant d and conductor l of the order corresponding to j for CM cases
$-(\xi+\xi^6)$	$-(\lambda)^6$	1	2^63^3	$d=-4,\quad l=1$
$-(\xi^2+\xi^5)$	-1	1	2^65^3	$d=-8,\quad l=1$
$-(\xi^3+\xi^4)$	$-(\bar\lambda)^3$	1	-2^{15}	$d=-11,\quad l=1$
$-(\xi+\xi^6)^3(\xi^2+\xi^5)^4$	$(3-\lambda)^3$	15	$-2^{18}3^35^3$	$d=-43,\quad l=1$
$(\xi^2+\xi^5)^3(\xi^3+\xi^4)^4$	$-(\lambda)^3$	15	$2^33^311^3$	$d=-4,\quad l=2$
$-(\xi^3+\xi^4)^3(\xi+\xi^6)^4$	$(-3+2\lambda)^3$	15	$2^{15}3^35^311^3$	$d=-67,\quad l=1$
$-(\xi^3+\xi^4)^3(\xi^2+\xi^5)^2$	$1-2\lambda$	-5	0	$d=-3,\quad l=1$
$-(\xi^2+\xi^5)^3(\xi+\xi^6)^2$	$-(1+5\bar\lambda)$	-5	$2^25^37^5$	Non-CM case
$-(\xi+\xi^6)^3(\xi^3+\xi^4)^2$	$-(13+9\lambda)$	-5	7^52^5	Non-CM case
$-440+244(\xi^2+\xi^5)-305(\xi^3+\xi^4)$	$(-1+5\lambda)^3$	-1259	$-2^{18}3^35^323^329^3$	$d=-163, l=1$
$-135+305(\xi^2+\xi^5)+549(\xi^3+\xi^4)$	$(5+\bar\lambda)^3$	-1259	$2^917^619^329^3149^3$	Non-CM case
$-684-549(\xi^2+\xi^5)-244(\xi^3+\xi^4)$	$(-13+4\lambda)^3$	-1259	$2^611^323^3149^3269^3$	Non-CM case

References

1. P. Deligne and M. Rapoport. Schémas de modules des courbes elliptiques, Vol. II of the *Proceedings of the International Summer School on Modular Functions, Antwerp* (1972). *Lecture Notes in Mathematics*, 349 (Springer, Berlin, 1973).
2. S. Chowla. Proof of a conjecture of Julia Robinson. *K. norske Vidensk. Selsk. Forh., Trondheim*, 34 (1961).
3. F. Klein. *Gesammelte mathematische Abhandlungen, Vol. 3* (Springer, Berlin, 1923).
4. R. Fricke and F. Klein. *Vorlesungen über die Theorie der elliptischen Modulfunctionen, Vol. 3* (Chelsea).
5. G. Ligozat. Courbes Modulaires de Niveau 11. *Proceedings of the International Conference, University of Bonn on Modular Functions of one Variable* (1976). *Lecture Notes in Mathematics*, 601 (Springer, Berlin, 1977).
6. B. Mazur. Rational points on modular curves. *Proceedings of the International Conference, University of Bonn on Modular Functions of one Variable* (1976). *Lecture Notes in Mathematics*, 601 (Berlin-Heidelberg-New York, Springer, 1977).
7. T. Nagell. Sur un type particulier d'unités algébriques. *Arkiv für Mat.*, 8 (1969), 163-184.
8. J.-P. Serre. Autour du théorème de Mordell-Weil. *Pub. Math. U. Pierre et Marie Curie*, No. 65.

Dr. M. A. Kenku,
Department of Mathematics,
University of Lagos,
Akoka, Lagos, Nigeria.

14K07: *ALGEBRAIC GEOMETRY; Special ground fields, arithmetic problems; Elliptic curves.*

Received on the 23*rd of January*, 1984.