# The modular curve $X_0(39)$ and rational isogeny

## By M. A. KENKU

### University of Ibadan

#### (Received 10 May 1978)

1. Introduction. Recently (3) Mazur proved that if N is a prime number such that some elliptic curve E over Q admits a Q-rational isogeny then N is one of 2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67 or 163.

He then defined an integer N to be minimal of positive genus if the genus of

 $X_0(N) > 0$ 

but the genus of  $X_0(d) = 0$  for all proper divisors d of N. Of such integers it has been shown that except perhaps for  $N = 13^2$ , 13.7, 13.5, 13.3 and 5<sup>3</sup>,  $X_0(N)$  has no rational non-cuspidal points.

The purpose of this paper is to give a short proof that  $X_0(39)$  has no non-cuspidal rational point so that there is no Q-rational 39 isogeny.

We construct an explicit model of  $X_0(39)$ ; the quotient  $X_0(39)/W_3$ , where  $W_3$ , the Atkin-Lehner involution corresponding to the prime 3, is an elliptic curve that has only four rational points.

Two of those points are the images of the cusps (all rational) and the other two belong to points from  $Q(\sqrt{-7})$ .

2.  $X_0(39)$ . By a theorem of Ogg(5) we know that  $X_0(39)$  has 4 cusps all rational. Suppose we denote them by  $P_1 = \infty$ ,  $P_2 = 0$ ,  $P_3 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$ ,  $P_4 = \begin{pmatrix} 1 \\ 13 \end{pmatrix}$ .

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

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

 $\prod_{d \mid N} \eta(dz)^{r(d)}$ 

where  $q = \exp(2\pi i z)$ . The following lemma of Newmann (4) is well known.

LEMMA 1.

is

a function on 
$$X_0(N)$$
 so long as

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

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

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

We consider two of such functions

$$R(\tau) = \frac{\eta(13\tau)\eta(3\tau)}{\eta(39\tau)\eta(\tau)},$$
$$S(\tau) = \frac{\eta^2(3\tau)}{\eta^2(39\tau)}.$$

Table	e 1
-------	-----

	$P_1 = \infty$	$P_2 = 0$	$P_3 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$	$P_4 = \begin{pmatrix} 1 \\ 13 \end{pmatrix}$	
$R(\tau)$	- 1	- 1	1	1	
S( au)	- 3	1	3	- 1	

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

The zero scheme of the function is as in Table 1. For N'|39, let  $W_{N'}$  be the corresponding Atkin-Lehner involution. By a theorem in Kenku(2)  $W_3$  has four fixed points on  $X_0(39)$  and  $W_{39}$  has 8;  $W_{13}$  has none.

The quotient space  $X_0(39)/W_3$  (resp.  $X_0(39)/W_{39}$ ) has genus 1 (resp. 0):

$$egin{aligned} W_{39}(R( au)) &= R( au), \ W_{39}(S( au)) &= rac{13R^2( au)}{S( au)} \end{aligned}$$

Consequently  $R(\tau)$  and  $L(\tau) = S(\tau) + (13R^2(\tau)/S(\tau)(1))$  are functions on  $X_0(39)/W_{39}$  which is of genus 0. Moreover  $R(\tau)$  is a univalent function on  $X_0(39)/W_{39}$ .

As  $R(\tau)$  and  $S(\tau)$  cannot have poles at non-cusp points (property of  $\eta$ -function), it is not difficult to show, either by considering the expansions at the cusps, or otherwise, that

$$L = \frac{R^4 - 3R^3 - 3R^2 - 3R + 1}{R}$$

so that

$$(S^2 + 13R^2) R = S(R^4 - 3R^3 - 3R^2 - 3R + 1).$$

The degrees of R and S are 2 and 4 respectively. Clearly S does not belong to Q(R) so the equation above is the equation for a model of  $X_0(39)$ .

The equation clearly has some singularities, but this will not deter us.

$$W_3(S) = S/R^2; \quad W_3(R) = 1/R.$$

Suppose we put T = R + 1/R and  $H = S(1 + 1/R^2)$ .

Then we have that

$$H^2 + 13T^2 = H(T^3 - 3T^2 - 5T)$$

Next substitute M = H/T. This gives

$$M^2 - 3MH = H^3 + 7H^2 + 13H,$$
  
 $N = M - 2H,$ 

leading to 
$$N^2 + NH = H^3 + 7H^2 + 13H$$
.

- Finally,  $x = H+2, \quad y = N-1$
- lead to  $y^2 + xy = x^3 + x^2 4x 5$ ,

which is the strong Weil curve of conductor 39 (see (1), table 1).

It has 4 rational points, the 2 division points; they are  $(\infty, \infty)$  (2, -1), (-2, 1)  $(-\frac{13}{4}, -\frac{13}{8})$ . The first point is the image of the cusps  $P_1$  and  $P_4$ ; the second that of  $P_2$  and  $P_3$ .

The two others correspond to

$$H = -6, \quad T = \frac{3}{2} \quad \text{and} \quad H = -\frac{39}{8}, \quad T = \frac{3}{2}.$$
$$R = \frac{1}{4}(3 \pm \sqrt{-7}), \quad S = -3 \mp \sqrt{-7},$$
$$R = \frac{1}{4}(3 \pm \sqrt{-7}), \quad S = \frac{1}{16}[-13(3 \pm \sqrt{-7})].$$

So that and

Consequently there are no non-cuspidal rational points on  $X_0(39)$ . We note that the points on  $X_0(N)$  defined over  $Q(\sqrt{-7})$  listed above do not arise from complex multiplication.

Furthermore, let j(z) be the classical modular invariant

$$j(\tau) + j(39\tau) \in \mathbf{Q}(R)$$
; so also is  $j(\tau) \cdot j(39\tau)$ .  
 $j(\tau) + j(39\tau) = F(R)/R^{13}$ ,

In fact,

where F is a polynomial of degree 52 with coefficients in  $\mathbb{Z}$  and

$$j( au).j(39 au) = G(R)/R^{16},$$

where G(R) is a polynomial of degree 56 with coefficients in  $\mathbb{Z}$ .

Consequently the modular invariant of the points or  $X_0(39)$  can be easily computed once F(R) and G(R) are known. The coefficients can be computed by considering the Fourier expansion at  $\infty$ .

#### REFERENCES

- BIRCH, B. J. and KUYK, W. Modular functions of one variable, 1st ed., vol. IV (Lecture Notes in Mathematics, no. 476; Berlin, Heidelberg, New York, Springer, 1973).
- (2) KENKU, M. A. Atkin-Lehner involutions and class number residuality. Acta Arith. 33 (1977), 1-9.
- (3) MAZUR, B. Rational isogenies of prime degree. Inventiones Math. 44 (1978), 129-162.
- (4) NEWMAN, M. Construction and application of a class of modular functions. Proc. London Math. Soc. (3) 7 1957, 334-350; 9 (1959), 373-387.
- (5) OGG, A. P. Rational points on certain elliptic modular curves. Proc. Symp. Pure Math. AMS Providence, 24 (1973), 221-231.