JOURNAL OF NUMBER THEORY 15, 199–202 (1982)

On the Number of **Q**-Isomorphism Classes of Elliptic Curves in Each **Q**-Isogeny Class

M. A. KENKU*

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540

Communicated by S. Chowla

Received December 17, 1980

It is shown that there are at most eight **Q**-isomorphism classes of elliptic curves in each **Q**-isogeny class.

In the table of elliptic curves published in [1] one finds that the number of vertices in the graph of rational isogenies is at most 8. Serre [12] has asked whether in fact 8 is a universal bound. Below we show that this is so.

Let $\bar{\mathbf{Q}}$ denote the algebraic closure of $\mathbf{Q}$; N any positive integer; $Y_0(N)$ the algebraic curve over $\mathbf{Q}$ which is a moduli space for $\mathbf{C}$-isomorphism classes of pairs (E, A) of elliptic curves E and a cyclic subgroup of E of order N. $Y_0(N)(\mathbf{C})$ is the quotient space $H\backslash\Gamma_0(N)$, where H is the upper half plane. Its compactification $X_0(N)$ is a projective algebraic curve. If k is an algebraic number field, then the point of $Y_0(N)(k)$ corrsponding to (E, A) is k-rational if and only if there is a representative (E', A') in the $\mathbf{C}$-isomorphism class of (E, A) such that E' is k-rational and A' is a k-rational subgroup of E.

THEOREM 1. *$Y_0(N)(\mathbf{Q})$ is empty except for $N \leqslant 10$, and $N = 12$, 13, 16, 18, 25 (all of genus 0) 11, 14, 15, 17, 19, 21, 27, 37, 43, 67 and 163.*

Proof. Mazur [9] proved that if N is a prime and $Y_0(N) \neq \varnothing$ then $N = 2$, 3, 5, 7, 13, 11, 19, 37, 43, 67 or 163.

We define an integer N to be minimal of positive genus if the genus of $X_0(N)$ is > 0, but the genus of $X_0(d)$ is 0 for all proper divisors d of N. To decide the isogeny question for composite N, it therefore suffices to show that $Y_0(N)(Q)$ is finite (possibly empty) for all minimal N of positive genus, determine the invariants of the curves corresponding to the finitely many rational points on those curves, as well as the prime cases N, where genus $X_0(N) > 0$ and find out what other isogenies belong to elliptic curves with such invariants.

* Supported in part by NSF Grant MCS 77-18723 A03.

0022-314X/82/050199-04$02.00/0

The integers N which are minimal of positive genus are as follows: 13^2, $13 \cdot 7$, $13 \cdot 5$, $13 \cdot 3$, $13 \cdot 2$, 7^2, $7 \cdot 5$, $7 \cdot 3$, $7 \cdot 2$, 5^3, $5 \cdot 3$, $5 \cdot 2^2$, $5^2 \cdot 2$, 3^3, $3^2 \cdot 2^2$, $3 \cdot 2^3$ and 2^5.

The cases in which $X_0(N)$ is of genus 1 were all settled by Ligozat [8], Ogg [11] and Jean-René Joly; $N = 35, 50$ in [7]; $N = 26$ in [10]; $N = 39$ in [2]; $N = 65$ and 91 in [3]; $N = 169$ in [4] and $N = 125$ in [5]. $Y_0(N)(Q) = \varnothing$ except for the values $N = 11$, 14, 15, 17, 19, 21, 27, 37, 43, 67 and 163 amongst the values N prime with genus $X_0(N)$ greater that 0 and N minimal of positive genus. For N in this last list, the j-invariant of the curves corresponding to the rational points of $Y_0(N)$ are integral except for a pair of points on $Y_0(17)(Q)$, which are transposed by the Atkin–Lehner involution w_{17}, the j-invariant of one of which Velu has shown to be $-(17)^2 (101)^3 2^{-1}$; a quadruple of points on $Y_0(15)(Q)$ also transposed by w_3, w_5 and w_{15} and the j-invariant of one of which is $5^2 \cdot 2^{-1}$ (from the table in [1]) and lastly a quadruple of points on $Y_0(21)(Q)$ transposed by w_3, w_7 and w_{21} and the j-invariant of one which is $5^3 \cdot 3^3 \cdot 2^{-1}$.

To complete the proof of the theorem, it therefore suffices to show that if an elliptic curve has an isogeny of degre $N = 11$, 14, 15, 17, 19, 21, 27, 37, 43, 67 and 163 rational over $\mathbf{Q}$, then no elliptic curve E $\mathbf{C}$-isomorphic to it and defined over $\mathbf{Q}$ has a $\mathbf{Q}$-rational cyclic isogeny of degree $m = N'N$, where $N' \neq 1$ is prime. If the genus of $X_0(N')$ is > 0 and $N' \neq N$, then this cannot happen because for no distinct values N', N in the above list does the same j-invariant appear. Suppose then that $N' = N$; let (E, A) be a rational representative of a point of $Y_0(N^2)(Q)$. Then $(E/NA, {}_NE/NA)$ and $(E/NA, A/NA)$ are two representatives of points of $Y_0(N)(Q)$ which are distinct if $\mathrm{Aut}(E/NA, A/NA)$ is ± 1. But this is so unless the j-invariant of E/NA is either 0 or 1728 which is not so for any N in the list.

It now remains to check the cases $N' = 2$, 3, 5, 7 and 13. Klein–Fricke [6] gives the j-invariant of a curve with N'-isogeny in terms of uniformising parameter t as follows:

$$
\begin{aligned}
j &= (t + 16)^3/t && \text{if } N' = 2;\\
&= (t + 27)(t + 3)^3/t && \text{if } N' = 3;\\
&= (t^2 + 10t + 5)^3/t && \text{if } N' = 5;\\
&= (t^2 + 13t + 49)(t^2 + 5t + 1)^3/t && \text{if } N' = 7;\\
&= (t^2 + 5t + 13)(t^4 + 7t^3 + 20t^2 + 19t + 1)^3/t && \text{if } N' = 13.
\end{aligned}
$$

If (E, A) is a representative of a point of $Y_0(N'N)(Q)$ which is $\mathbf{Q}$-rational, then (E, NA) is a representative of a point of $Y_0(N')(Q)$ so that there is a rational number t_0 such that $j(E) = R_{N'}(t_0)/t_0$. Since, as we indicated earlier,

we can choose E such that $j(E)$ is either an integer or has 2 as its denominator, it suffices to check $R_{N'}(t_0)/t_0$ for

$$\begin{aligned}
t_0 &= \pm 2^s, && 0 \leqslant s \leqslant 13 && \text{for } N' = 2;\\
&= \pm 2^i \cdot 3^s, && i = 0 \text{ or } 1,\ 0 \leqslant s \leqslant 6 && \text{for } N' = 3;\\
&= \pm 2^i \cdot 5^s, && i = 0 \text{ or } 1,\ 0 \leqslant s \leqslant 3 && \text{for } N' = 5;\\
&= \pm 2^i \cdot 7^s, && i = 0 \text{ or } 1,\ 0 \leqslant s \leqslant 2 && \text{for } N' = 7;\\
&= \pm 2^i \cdot 13^s, && i = 0 \text{ or } 1,\ 0 \leqslant s \leqslant 1 && \text{for } N' = 13.
\end{aligned}$$

The only j invariants of points of $Y_0(N)(Q)$ for N in the list which showed up are those in which N' divides N, i.e., $N' = 2$, $N = 14$; $N' = 3$, $N = 15$ and $N' = 3$, $N = 21$. So to complete the proof it suffices to show in these cases that $Y_0(N'N)(Q)$ is empty.

Let (E, A) be a rational pair representing a point of $Y_0(N'N)(Q)$ in the above three cases. Consider the pairs $(E/N'A,\ A/N'A)$ and $(E/N'A,\ N'A + {}_{N'}E/N'A)$. These should represent two distinct points of $Y_0(N)(Q)$ with the same j-invariant. As we mentioned earlier, this does not arise. This completes the proof of Theorem 1.

THEOREM 2. *There are at most* 8**Q***-isomorphism classes of elliptic curves in each* **Q***-isogeny class.*

Proof. Let $C(E)$ denote the number of **Q**-isomorphism classes of elliptic curves in the **Q**-isogeny class of E. $C(E)$ is also the number of distinct **Q**-rational cyclic subgroups of E-(including the identity subgroup).

For a prime p, let $C_p(E)$ be the p component of $C(E)$. We have the product formula

$$C(E) = \prod_p C_p(E).$$

From the definition of $C(E)$ it is independent of the choice of the representative of the class; so also are the p-factors. By Manin's theorem $C_p(E)$ is bounded for each p as E varies over all the **Q**-isogeny classes of elliptic curves. By considering ${}_pE$ as a $\mathrm{Gal}(\bar{Q}/Q)$-module and using Theorem 1, we have the following table for bounds C_p of $C_p(E)$

p	2	3	5	7	11	13	17	19	37	43	67	163
C_p	8	4	3	2	2	2	2	2	2	2	2	2

and $C_p = 1$ for all other primes. Mazur [9] has already determined C_p for all p except $p = 5$ and 13. In the case of $p = 2$ we have that $C_p(E) = 2t$ if an

elliptic curve in the class of E has a $\mathbf{Q}$-rational cyclic group of order 2^t and none has one of order 2^{t+1}.

Let us now fix a Q-isogeny class and a representative E of that class. If $C_p(E) = 2$ for a $p \geqslant 11$ then by Theorem 1, $C_q(E) = 1$ for all other primes. So $C(E) = 2$.

If $C_7(E) = 2$, then $C_5(E) = 1$ by Theorem 1, also either $C_3(E) \leqslant 2$ and $C_2(E) = 1$ or $C_3(E) = 1$ and $C_2(E) \leqslant 2$. All these yield $C(E) \leqslant 4$.

If $C_5(E) = 3$, then by Theorem 1, $C_p(E) = 1$ for all primes $p \neq 5$. This follows because then a curve in the class of E has a $\mathbf{Q}$-rational cyclic subgroup of order 25.

If $C_5(E) = 2$, then either $C_3(E) \leqslant 2$ and $C_2(E) = 1$ or $C_3(E) = 1$ and $C_2(E) = 2$. Hence $C(E) \leqslant 4$.

If $C_3(E) = 4$, there exists a representative of the class of E with a Q-rational cyclic subgroup of order 27; by Theorem 1 $C_2(E) = 1$ so $C(E) \leqslant 4$.

If $C_3(E) = 3$, then by Theorem 1 $C_2(E) \leqslant 2$ so that $C_3(E) \leqslant 6$.

If $C_3(E)$ is $\leqslant 2$, then again $C_2(E) \leqslant 4$ so that $C(E) \leqslant 8$. This completes the proof of the theorem.

We will like to note that in fact $C(E) = 8$ is possible only if $C_2(E) = 8$ or if $C_3(E) = 2$ and $C_2(E) = 4$.

REFERENCES

1. B. BIRCH AND W. KUYK (Eds.), "Modular Functions of One Variable IV," Lecture Notes in Mathematics No. 476, Springer–Verlag, Berlin, Heidelberg, New York, 1975.
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. M. A. KENKU, The modular curve $X_0(169)$ and rational isogeny, *J. London Math. Soc.* (2) **22** (1980), 239–244.
5. M. A. KENKU, On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$, *J. London Math. Soc.* *2* **23** (1981), 415–427.
6. F. KLEIN AND R. FRICKE, "Vorlesungen über die Theorie der elliptischen Modulfunctionen," Vol. 2, Chelsea, New York.
7. S. D. KUBERT, Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc.* (3) **33** (1976), 193–237.
8. G. LIGOZAT, Courbes Modulaires de genre 1, *Bull. Soc. Math. France, Memoire* **43** (1975), 1–80.
9. B. MAZUR, Ratonal isogenies of prime degree, *Inventiones Math.* **44** (1978), 129–162.
10. B. MAZUR AND J. VELU, Courbes de Weil de conducteur 26, *C. R. Acad. Sci. Paris Sé. A* **275**, 743–745.
11. A. OGG, Rational points on certain elliptic modular curves, *Proc. Symp. Pure Math.* **24**, 221–231.
12. J. P. SERRE, Points rationnels des courbes modulaires $X_0(N)$, *in* "Seminaire Bourbaki 30e annèe," 1977/78, no. 511.