MATHEMATICS OF COMPUTATION
Volume 74, Number 250, Pages 949–951
S 0025-5718(04)01690-4
Article electronically published on July 7, 2004

ON STANDARDIZED MODELS OF ISOGENOUS ELLIPTIC CURVES

SAMIR SIKSEK

ABSTRACT. Let $E,\ E'$ be isogenous elliptic curves over $\mathbb{Q}$ given by standardized Weierstrass models. We show that (in the obvious notation)

$$a_1' = a_1, \qquad a_2' = a_2, \qquad a_3' = a_3$$

and, moreover, that there are integers $t,\ w$ such that

$$a_4' = a_4 - 5t \text{ and } a_6' = a_6 - b_2 t - 7w,$$

where $b_2 = a_1^2 + 4a_2$.

1. INTRODUCTION

Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass model

$$E: \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

We say that this model for E is a standardized model if it is minimal with $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{-1, 0, 1\}$. Each elliptic curve has a unique standardized model. The models given for elliptic curves in Cremona's tables [3] and the earlier Antwerp IV tables [1] are standardized models.

Anyone pondering those tables is likely to conjecture at least part of the following theorem.

Theorem 1.1. *Suppose that E, E' are isogenous elliptic curves given by standardized models. Then (in the obvious notation)*

$$a_1' = a_1, \quad a_2' = a_2, \quad a_3' = a_3.$$

Moreover, there are integers $t,\ w$ such that

$$a_4' = a_4 - 5t \quad \textit{and} \quad a_6' = a_6 - b_2 t - 7w,$$

where $b_2 = a_1^2 + 4a_2$.

It is the purpose of this note to establish this theorem. There are two obvious attempts at proving this theorem that, at first sight, seem to be promising lines of attack. We would like to start by warning that these two approaches are either fallacious or at best tortuous.

Received by the editor November 8, 2003.
2000 *Mathematics Subject Classification.* Primary 11G05.
Key words and phrases. Elliptic curves, formal groups, isogenies, standardized models.
The author's work is funded by a grant from Sultan Qaboos University (IG/SCI/DOMS/-02/06).

The first is to use Vélu's formulae for isogenous curves [3, pp. 99–100]. Suppose E is given by a standardized model as in (1). If l is an odd prime and E' is an elliptic curve that is l-isogenous to E, then Vélu gives the following model for E':

$$E' : \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + (a_4 - 5t)x + (a_6 - b_2t - 7w)$$

for a certain $t,\ w$. At first sight this does seem to prove the above theorem. However, the $t,\ w$ given by Vélu's construction are often non-integers. Even when the model given by Vélu's formulae has integral coefficients, it is not necessarily minimal. We are grateful to Professor John Cremona for supplying us with the following example, which shows that these possibilities can indeed occur, and so that our theorem does not follow from Vélu's formulae. Consider the curve 11A1 in Cremona's tables [3] given by the standardized model

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

This curve has two torsion subgroups of order 5 that are rational as a whole. Applying Vélu's formulae to one of these gives us a 5-isogeny to the curve 11A2. If we apply Vélu's formulae to the other subgroup, we get values of $t = 39.6$ and $w = -382.8$. This gives us the following non-minimal model for the curve 11A3:

$$y^2 + y = x^3 + x^2 - 208x + 2818.$$

The second obvious line of attack at proving our theorem is to look at the reduction of the two elliptic curves modulo 2, 3, 5 and 7. If these are primes of good reduction, then the reduced curves must be isogenous, and one could probably benefit from enumerating all pairs of isogenous elliptic curves modulo 2, 3, 5 and 7. It is not clear how to proceed if the curves have bad reduction. In any case this approach is likely to be long–winded.

We will see that Theorem 1.1 follows from a theorem of T. Honda, with the aid of some calculations on a computer algebra system.

2. A theorem of Honda

Before stating Honda's Theorem, we need some terminology. Given one parameter formal group laws $\mathcal{F},\ \mathcal{F}'$ over a ring R, we say that they are strictly isomorphic if there is a power series $f(T) \in R[\![T]\!]$ such that

- $f(T) = T +$ terms of higher order, and
- $f(\mathcal{F}(X, Y)) = \mathcal{F}'(f(X), f(Y))$.

Theorem 2.1 (Honda)**.** *Suppose that $E,\ E'$ are elliptic curves over $\mathbb{Q}$. Let $\mathcal{F},\ \mathcal{F}'$ be formal group laws of minimal models of $E,\ E'$, respectively. If E is isogenous to E', then $\mathcal{F}$ and $\mathcal{F}'$ are strictly isomorphic over $\mathbb{Z}$.*

In fact, given an elliptic curve E over the rationals, Honda [5] constructs a formal group law related to its L-function and proves [6, Theorem 9] that this is strictly isomorphic over $\mathbb{Z}$ to the formal group law of (any) minimal model for E. The above theorem follows since if two elliptic curves are isogenous, their L-functions are identical. Honda's results are also explained in [4, Section VI.33].

3. Proof of Theorem 1.1

Suppose that $E,\ E'$ are isogenous elliptic curves given by standardized models as in the statement of the theorem. Let $\mathcal{F},\ \mathcal{F}'$ be the formal group laws attached to these standardized models of E, E', respectively. Honda's Theorem 2.1 asserts that $\mathcal{F},\ \mathcal{F}'$ are strictly isomorphic. Let $f(T) \in \mathbb{Z}[\![T]\!]$ be the power series defining

this strict isomorphism. By a well-known result [4, IV.18.2] on homomorphisms of formal group laws

$$f(T) = \exp_{\mathcal{F}'}(\alpha \log_{\mathcal{F}}(T)), \tag{2}$$

where $\exp_{\mathcal{F}'}$ and $\log_{\mathcal{F}}$ are the formal exponential and logarithm of $\mathcal{F}'$ and $\mathcal{F}$, respectively, and α is some rational number. However, since f is a strict isomorphism, its linear coefficient is 1. Comparing the coefficients of T on both sides of (2), we see that $\alpha = 1$. It follows that $(\exp_{\mathcal{F}'} \circ \log_{\mathcal{F}})(T) \in \mathbb{Z}[\![T]\!]$.

Explicit formulae for the formal exponential and logarithm can be deduced from Silverman's book [7, Chapter IV]. We used the computer package MAGMA [2] to calculate the first few terms of the series $(\exp_{\mathcal{F}'} \circ \log_{\mathcal{F}})(T)$. We found that

$$(\exp_{\mathcal{F}'} \circ \log_{\mathcal{F}})(T) = T + \frac{1}{2}(a_1 - a_1')T^2 + [\frac{1}{6}(a_1 - a_1')(2a_1 - a_1') + \frac{1}{3}(a_2 - a_2')]T^3 + \cdots.$$

By the above, the coefficients of this power series must be integral. Since $a_1, a_1' \in \{0, 1\}$ and $a_2, a_2' \in \{-1, 0, 1\}$, we immediately see that $a_1' = a_1$, and $a_2' = a_2$.

We continued to compute the next two terms of the above power series with the simplifying assumptions $a_1' = a_1$ and $a_2' = a_2$. We found

$$(\exp_{\mathcal{F}'} \circ \log_{\mathcal{F}})(T) = T + \frac{1}{2}(a_3 - a_3')T^4 + [\frac{7}{10}a_1(a_3 - a_3') + \frac{2}{5}(a_4 - a_4')]T^5 + \cdots$$

and from this we quickly deduce that $a_3' = a_3$ and $a_4' = a_4 - 5t$ for some integer t. Continuing with the computation of the series, we find that

$$(\exp_{\mathcal{F}'} \circ \log_{\mathcal{F}})(T) = T + 2tT^5 + 3a_1tT^6 + \frac{(25a_1^2 + 16a_2)t + 3(a_6 - a_6')}{7}T^7 + \cdots.$$

We deduce that

$$a_6' \equiv a_6 + \frac{(25a_1^2 + 16a_2)t}{3} \equiv a_6 - (a_1^2 + 4a_2)t \equiv a_6 - b_2t \pmod 7.$$

This completes the proof.

Remarks.
(1) We suspect that Theorem 1.1 might streamline the search for elliptic curves isogenous to a given elliptic curve.
(2) It is clear from the proof of Theorem 1.1 that the coefficients of isogenous elliptic curves must satisfy an infinite list of congruence conditions. It would be interesting to have a more conceptual understanding of these conditions.

References

1. B.J. Birch and W. Kuyk (eds.), *Modular Functions of One Variable IV*, Lecture Notes in Mathematics **476**, Springer–Verlag, 1975. MR 51:12708
2. W. Bosma, J. Cannon and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265 (see also `http://www.maths.usyd.edu.au:8000/u/magma`). MR 98f:68006
3. J.E. Cremona, *Algorithms for Modular Elliptic Curves* (second edition), Cambridge University Press, 1996. MR 99e:11068
4. M. Hazewinkel, *Formal Groups and Applications*, Academic Press, 1978. MR 82a:14020
5. T. Honda, *Formal Groups and Zeta-Functions*, Osaka J. Math. **5** (1968), 199–213. MR 40:2683
6. T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan **22** (1970), 213–246. MR 41:212
7. J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, 1986. MR 87g:11070

Department of Mathematics and Statistics, College of Science, P.O. Box 36, Sultan Qaboos University, Al-Khod 123, Oman

E-mail address: `siksek@squ.edu.om`