THE ANALYTIC ORDER OF Ш FOR MODULAR ELLIPTIC CURVES

J.E.CREMONA

Abstract. In this note we extend the computations described in [4] by computing the analytic order of the Tate–Shafarevich group Ш for all the curves in each isogeny class; in [4] we considered the strong Weil curve only. While no new methods are involved here, the results have some interesting features suggesting ways in which strong Weil curves may be distinguished from other curves in their isogeny class.

1. Introduction

In this note we extend the computations described in [4] by computing the analytic order of the Tate–Shafarevich group Ш for all the curves in each isogeny class; in [4] we considered the strong Weil curve only. While no new methods are involved here, the results have some interesting features suggesting ways in which strong Weil curves may be distinguished from other curves in their isogeny class.

In [4] we computed all the modular elliptic curves of conductors[1] up to 1000. For each "strong Weil" curve E found we listed generators of the Mordell–Weil group $E(\mathbb{Q})$. We also computed the following quantity:

$$S = \frac{L^{(r)}(E,1)\cdot R}{\Omega(E)} \Big/ \frac{\prod c_p}{\left|E(\mathbb{Q})_{\text{torsion}}\right|^2}\ . \tag{1.1}$$

We call S the "analytic order of Ш", since according to the Birch–Swinnerton-Dyer conjectures we should have $S = |Ш|$ where Ш is the Tate–Shafarevich group of $E/\mathbb{Q}$. Here $L(E,s)$ is the Hasse–Weil L-function of E; if $f(z)$ is the newform of weight 2 attached to E, then $L(E,s) = L(f,s)$. Also $\Omega(E) = \Omega(f)$, the least real period of E (or f) times the number of connected components of the real locus $E(\mathbb{R})$. Finally R is the regulator of $E(\mathbb{Q})$, r is its rank, and c_p is the local index $[E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$. These quantities are tabulated in Table 4 of [4].

If E is replaced by an isogenous curve E', none of the above quantities, except for $L(E,1)$, is invariant. The purpose of this note is to investigate their variation within an isogeny class. Roughly speaking, our results suggest that S is minimal for the strong Weil curve: see Section 3 for details.

[1]Note that in [4], the conductor $N = 702$ was omitted accidentally, including 16 strong Weil curves and a further 8 curves isogenous to these. The missing data is available via anonymous file transfer from the site given at the end of this paper.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

2. Some computational details

In [4] can be found a detailed description of the methods used to compute all the factors on the right-hand side of (1.1) for a modular elliptic curve E. The only non-trivial task in extending the computations to the other curves in each of the 2463 isogeny classes was the determination of generators for the Mordell–Weil groups, in order to compute the regulators R. For most of the curves these generators were easily found by the same search procedure, speeded up by a simple sieving technique, as was described in §3.5 of [4]. This procedure had been successful for all the strong Weil curves, the "worst" case being the curve $873\mathrm{C}_1$ whose generator is $P = (x, y) = \left(227473/16^2, 106817593/16^3\right)$.

For a few curves of rank 1, however, this search did not find any points of infinite order. In these cases we were able to use Vélu's formulae from [6] to map points across from one curve in the class to another. We recall these formulae here.

Let E be a curve defined over $\mathbb{Q}$ with usual Weierstrass coefficients $[a_1, a_2, a_3, a_4, a_6]$, and associated quantities b_2, b_4, b_6. If Q is a point of odd order m on E, then there is an m-isogeny $\phi\colon E \to E'$ with kernel $\langle Q\rangle$. Both the isogeny ϕ and the curve E' will be defined over $\mathbb{Q}$ if the subgroup $\langle Q\rangle$ is. For $1 \le j \le (m-1)/2$, set

$$\begin{aligned} x_j &= x(jQ);\\ t_j &= 6x_j^2 + b_2x_j + b_4;\\ u_j &= 4x_j^3 + b_2x_j^2 + 2b_4x_j + b_6 \end{aligned}$$

and

$$t = \sum_{j=1}^{(m-1)/2} t_j; \qquad w = \sum_{j=1}^{(m-1)/2} (u_j + x_jt_j).$$

Then E' has Weierstrass coefficients $[a_1, a_2, a_3, a_4 - 5t, a_6 - b_2t - 7w]$. Also, if P is any point in $E(\mathbb{Q}) \setminus \langle Q\rangle$, then its image on E' has x-coordinate

$$x(P') = x(P) + \sum_{j=1}^{(m-1)/2} \frac{t_j}{x(P) - x_j} + \sum_{j=1}^{(m-1)/2} \frac{u_j}{(x(P) - x_j)^2}.$$

For $m = 2$, we define instead $t = 3x^2 + 2a_2x + a_4 - a_1y$, $u = 4x^3 + b_2x^2 + 2b_4x + b_6$ and $w = u + xt$, where $Q = (x, y)$.

Of course, when $m \ge 5$, the x-coordinates x_j are not necessarily rational, so that t_j and u_j are not rational; but t and w will be rational provided that the subgroup $\langle Q\rangle$ is defined over $\mathbb{Q}$.

Example 1. Let E be the curve $874\mathrm{E}_1$ of [4], with coefficients $[1, 1, 1, -410, 903]$ and rank 1. A generator is $P = (-3, 47)$ and $Q = (21, 35)$ has order 5. Using $2Q = (67, -563)$ and the above formulae we obtain $t = 28382$, $w = 2940550$, so that the 5-isogenous curve E' has coefficients $[1, 1, 1, -142320, -20724857]$ (this is curve $874\mathrm{E}_2$ of [4]) and the image of P is $P' = (-9623549/210^2, 1006133969/210^3)$.

Example 2. Let E be the curve $975\mathrm{A}_1$ of [4]. There are 8 curves in its isogeny class, linked by 2-isogenies. For example, there is a chain of 2-isogenies

$$A_1 \overset{2}{\longleftrightarrow} A_2 \overset{2}{\longleftrightarrow} A_3 \overset{2}{\longleftrightarrow} A_5 \overset{2}{\longleftrightarrow} A_8$$

With suitable choices of points Q of order 2 on each curve, starting with the generator $P_1 = (26, 23)$ of A_1 we obtain points P_i of infinite order on A_i as follows:

$$\begin{aligned} P_1 = (26,23) \mapsto P_2 = (79/4, 83/8) \mapsto P_3 &= (-321/4, 959/8) \\ \mapsto P_5 &= (-878361/58^2, 27647851/58^3) \\ \mapsto P_8 &= (7765202319/3538^2, 380236785822631/3538^3). \end{aligned}$$

Note that each of these points has exactly double the canonical height of the previous one, with that of P_8 being $11.56\ldots$. This point would not be easy to find by searching.

3. Results and comments

First we give a summary of the results for the "strong Weil" curves, as tabulated in [4]. The 2463 curves comprise 1321 of rank 0, 1124 of rank 1, and just 18 of rank 2. The values of S were as follows:

S	Number of curves	Curve codes
1	2459	
4	3	$571A_1$, $960D_1$, $960N_1$
9	1	$681B_1$

The curves with $S > 1$ were all of rank 0; in these cases the value of S is computed exactly, since the regulator R is identically 1 and the ratio $L(E,1)/\Omega(E)$ is known exactly using modular symbols. (The other quantities in (1.1) are integers.)

When the computations were extended to include all the curves (5113 in all, comprising 3081 of rank 0, 2014 of rank 1 and 18 of rank 2) we found many more cases where $S > 1$:

S	Number of curves	Curve codes
1	5008	
4	66	$66B_3$, $102B_5$, $114C_3$, $120A_5$, $130B_3$, $195A_7$,..., $990K_3$
9	27	$182B_3$, $300B_2$, ..., $938D_3$
16	5	$210E_7$, $210E_8$, $582D_3$, $930O_5$, $930O_6$
25	5	$275B_3$, $570L_3$, $570L_4$, $870I_3$, $870I_4$
49	2	$546F_2$, $858K_2$

Several comments may be made on these results.

1. All the curves with $S > 1$ have rank 0.

2. Six curves with $S = 4$ and one with $S = 9$ have conductor less than 200, and so are included in the Antwerp tables [1]. For convenience, we give the Antwerp codes for these. For $S = 4$ they are 66H, 102L, 114J, 120J, 130D and 195H, and for $S = 9$ the curve is 182C. We do not know if it had been observed before that any of the Antwerp curves had non-trivial Ш.

3. We have carried out a 2-descent on all the curves with $S = 4$ or $S = 16$. For the former, we can confirm that the 2-rank of Ш is 2 in each case, which is consistent with $|Ш| = 4$ and $Ш \cong (\mathbb{Z}/2\mathbb{Z})^2$. Note that as these are modular curves with $L(E,1) = L(f,1) \neq 0$, we know *a priori* that their rank is 0 and that Ш

is finite by Kolyvagin's results (see [5]). The curves with $S = 16$ also have the 2-rank of Ш equal to 2, suggesting that for these curves $Ш \cong (\mathbb{Z}/4\mathbb{Z})^2$ rather than $(\mathbb{Z}/2\mathbb{Z})^4$.

4. It is known that the Birch–Swinnerton-Dyer conjecture is invariant under isogeny (see [3]), and that under an l-isogeny (for prime l) the order of Ш can only change by a power of l. In most cases this observation "explains" the computed values of S: for $l = 2, 3, 5$ and 7 the curves with $S = l^2$ are all l-isogenous to curves with $S = 1$, except for one case: the curves $681\mathrm{B}_1$–B_4, which are linked by 2-isogenies, all have $S = 9$. For the three strong Weil curves with $S = 4$ given in the first table, $571\mathrm{A}_1$ has no isogenies, while $960\mathrm{D}_1$ and $960\mathrm{N}_1$ are each 2-isogenous to curves with $S = 1$. Apart from these two cases, the strong Weil curve always has the minimal value of S.

5. The analytic order of Ш has been computed elsewhere for other classes of curves. For example, Brumer and McGuiness, in their study of curves of prime conductor (see [2]), came across curves with $S = 289$.

6. We examined the values of the regulator R to see whether any particularly small values occurred. There are only 69 curves with $R < 0.05$, and all but three of these are strong Weil curves (the exceptions being $405\mathrm{D}_2$ with $R = 0.043$, $242\mathrm{A}_2$ with $R = 0.041$, and $338\mathrm{E}_2$ with $R = 0.030$). Only 6 curves have $R < 0.02$, the smallest value being for $280\mathrm{B}_1$ where $R = 0.011$. Thus we observe that the strong Weil curves tend to have the smallest values of R, and no new very small value was encountered.

For obvious reasons of space we cannot include here all the detailed results of the computations. These are available by anonymous file transfer from gauss.math.mcgill.ca, in the directory ~`ftp/pub/cremona`. The file `Shas` contains the list of curves with $S > 1$, while the file `bsdextra` contains all the information of Table 1 of [4] for each curve, namely the rank r, real period Ω, regulator R, value of $L^{(r)}(E, 1)$, and S.

We are grateful to Noam D. Elkies of Harvard University for suggesting that these further computations would be of interest.

References

1. B.J.Birch and W.Kuyk (eds.), *Modular Functions of One Variable IV*, Lecture Notes in Mathematics 476, Springer-Verlag, 1975.
2. A. Brumer and O. McGuinness, *The behaviour of the Mordell–Weil group of elliptic curves*, Bull. AMS (New Series) **23** (1990), 375–382.
3. J.W.S. Cassels, *Arithmetic on curves of genus 1 (VIII). On the conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–189.
4. J.E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1992.
5. V.I. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш_{E/\mathbb{Q}}$ for a subclass of Weil curves*, Math. USSR Izvest. **32** (1989), 523–542.
6. J.Vélu, *Isogénies entre courbes elliptiques*, C.R.Acad.Sc. Paris, 238–241.

Department of Mathematics, University of Exeter, North Park Road, Exeter EX4 4QE U.K.

E-mail address: `cremona@maths.exeter.ac.uk`