RATIONAL POINTS OF ORDER 7

NEIL DUMMIGAN

Abstract. For an elliptic curve over the rationals, optimal in its isogeny class, with a rational point of order 7 but $L_E(1) \neq 0$, we prove that 7 divides the product of the Tamagawa factors with the order of the Shafarevich-Tate group. This is a small consequence of the Birch and Swinnerton-Dyer conjecture.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. By the modularity theorem [19],[17],[3], [9] there exists a morphism of finite degree $\phi : X_0(N) \to E$, defined over $\mathbb{Q}$, where N is the conductor of E,[11],[4]. Here $X_0(N)$ is the completion of the modular curve classifying elliptic curves with cyclic subgroups of order N. We may choose E uniquely in its isogeny class such that ϕ has minimal degree. Such an E is said to be $X_0(N)$-optimal, or equivalently, a strong Weil curve. If $J_0(N)$ is the jacobian of $X_0(N)$, then there are morphisms of abelian varieties $\pi : J_0(N) \to E$ and $\hat{\pi} : E \to J_0(N)$, with $\ker \pi$ connected and $\hat{\pi}$ injective.

Let $L_E(s)$ be the L-function of E. In the half-plane $\Re(s) > 3/2$ this is defined by a convergent Euler product, but it has an analytic continuation to the whole complex plane, given by

$$(2\pi)^{-s}\Gamma(s)L_E(s) = \int_0^\infty f(iy)y^{s-1}\,dy\,. \tag{1}$$

Here, if $L_E(s) = \sum_{n-1}^{\infty} a_n n^{-s}$ for $\Re(s) > 3/2$, then $f(z) = \sum_{n=1}^{\infty} a_n q^n$ (with $q = e^{2\pi i z}$) is the associated normalised newform of weight 2 for

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N \mid c \right\}.$$

Note that $X_0(N)(\mathbb{C}) \simeq \Gamma_0(N)\backslash\mathfrak{H}^*$, where $\mathfrak{H}^* = \mathfrak{H} \cup \{\text{cusps}\}$ is the completed upper half plane.

According to the conjecture of Birch and Swinnerton-Dyer, in the case that $E(\mathbb{Q})$ is finite,

$$\frac{L_E(1)}{\Omega} = \frac{\prod_p c_p \ \#Ш}{(\#E(\mathbb{Q}))^2}\ , \tag{2}$$

where Ω is the real period of a Néron differential ω, and c_p is the Tamagawa factor at p. In more detail, $c_p = [E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$, where $E^0(\mathbb{Q}_p)$ is the subgroup of points with nonsingular reduction, so c_p is trivial unless p is a prime of bad reduction. The Shafarevich-Tate group Ш of E (the group of everywhere locally trivial principal homogeneous spaces for $E/\mathbb{Q}$) is conjectured to be finite. If $L_E(1) \neq 0$ then $E(\mathbb{Q})$ and Ш are known to be finite, by a theorem of Kolyvagin [10].

Date: May 23rd, 2008.

1991 *Mathematics Subject Classification.* 11G05, 11G18, 11G40.

The homology $H_1(X_0(N)(\mathbb{C}),\mathbb{Q})$ has an action of complex conjugation, compatible with $z \mapsto -\overline{z}$ on $\mathfrak{H}$. The image $\mathbf{e}$ of the positive imaginary axis $[0, i\infty]$ represents a class in the eigenspace $H_1(X_0(N)(\mathbb{C}),\mathbb{Q})^+$, and $\phi_*([\mathbf{e}])$ belongs to the one-dimensional space $H_1(E(\mathbb{C}),\mathbb{Q})^+$. Either $\phi_*([\mathbf{e}]) = 0$ or there is a unique positive rational r such that $r^{-1}\phi_*(\mathbf{e})$ is a generator for $H_1(E(\mathbb{C}),\mathbb{Z})^+$. In the latter case the order of the rational point $\pi([(0)-(\infty)])$ on E is just the denominator of r. (Recall that $J_0(N)$ represents classes of degree-zero divisors on $X_0(N)$. Note also that the torsion subgroup of $E(\mathbb{C})$ is naturally isomorphic to $H_1(E(\mathbb{C}),\mathbb{Q})/H_1(E(\mathbb{C}),\mathbb{Z})$.) If $\phi_*([\mathbf{e}]) = 0$ then $\pi([(0)-(\infty)]) = O$, and we set $r := 0$.

By (1),

$$\begin{aligned} L_E(1) &= -\int_0^{i\infty} f(z)\,(2\pi i)dz = -\int_{\mathbf{e}} c^{-1}\phi^*\omega \\ &= -c^{-1}\int_{\phi_*(\mathbf{e})} \omega = \frac{r}{c}\,\Omega. \end{aligned}$$

Here, c is Manin's constant, and the sign of ω is chosen to make c positive. Since E is optimal, c is conjectured to equal 1. If, for an odd prime ℓ, we assume that $\ell^2 \nmid N$, then it is known that $\mathrm{ord}_\ell(c) = 0$, by Corollary 4.2 of [14], and its refinement [1]. If $\mathrm{ord}_\ell(c) = 0$ and $L_E(1) \neq 0$, the denominator of $L_E(1)/\Omega$, as the order of $\pi([(0)-(\infty)])$, divides $\#E(\mathbb{Q})$. Hence, according to (2), $\#E(\mathbb{Q})$ ought to divide $\prod_p c_p\,\#Ш$. This consequence of the Birch-Swinnerton-Dyer conjecture was noted at the end of §4.3 of [1], in the wider setting of modular abelian varieties. I am indebted to A. Agashe for bringing this problem to my attention.

There is no reason to expect always to have such a divisibility (with $E(\mathbb{Q})$ replaced by $E(\mathbb{Q})_{\mathrm{tors.}}$) in the case $L_E(1) = 0$ (though if there is a prime p of split multiplicative reduction with $\ell \nmid (p-1)$, then $\ell \mid \#E(\mathbb{Q})_{\mathrm{tors.}}$ forces $\ell \mid c_p$). Indeed, the elliptic curve E labelled 91b1 in [6] has rank 1, $\#E(\mathbb{Q})_{\mathrm{tors.}} = 3$ but c_7, c_{13} and the conjectural order of Ш all equal to 1.

Note that for any elliptic curve of *prime* conductor N, Mestre and Oesterlé proved that $\#E(\mathbb{Q})_{\mathrm{tors}} = c_N$ [15], and this was extended to modular abelian varieties (of prime conductor) by Emerton [8] when he proved Stein's "refined Eisenstein conjecture". Examples of optimal elliptic curves of rank 0 for which $\#E(\mathbb{Q}) = 3$ but all $c_p = 1$ are 4914n1 and 5859e1 (labelled as in [6]). These conductors factorise as $4914 = 2 \cdot 3^3 \cdot 7 \cdot 13$ and $5859 = 3^3 \cdot 7 \cdot 31$. The conjectured element of order 3 in Ш for 4914n1 cannot be constructed using a mod 3 congruence with another elliptic curve of level 4914 (but positive rank), as noted in [7]. For these examples, $L_E(1)/\Omega = 1$, and the conjectural order of Ш (according to BSD) is 3^2.

2. The theorem

Theorem 2.1. *Let $E/\mathbb{Q}$ be an $X_0(N)$-optimal elliptic curve of conductor N, such that $L_E(1) \neq 0$. Suppose that $E(\mathbb{Q})$ contains a point P of order 7. Then 7 divides $\prod_p c_p\,\#Ш$.*

Note that, by Mazur's theorem [13], if E has a rational point of prime order ℓ, the only possibilities for ℓ are $2, 3, 5$ and 7.

Proof. We consider the isogenous curve $E' = E/\langle P\rangle$, and let $\theta : E \to E'$ be the isogeny of degree 7. This θ is an "étale" isogeny in the sense of [16] or [18], i.e. its extension to Néron models is an étale morphism. In particular (2.2 of [16]) $\theta^*\omega_{E'} = \omega_E$, for Néron differentials ω_E and $\omega_{E'}$ on E and E' respectively. It

follows that the real periods Ω_E and $\Omega_{E'}$ are related by $\Omega_{E'} = \Omega_E/7$. Admitting for the moment that $E'(\mathbb{Q})$ does not also have a rational point of order 7, looking at (2), and using the isogeny invariance of the Birch and Swinnerton-Dyer conjecture [5], we see that in passing from E to E', from $\prod_p c_p \ \#Ш$ to $\prod_p c'_p \ \#Ш'$ say, the power of 7 has gone down by one. Since this product is still an integer, it follows that, for E, it must have been a multiple of 7, as required.

It remains to justify the claim that E' does not have a rational point of order 7. Suppose for a contradiction that it does have such a point, P' say, and let $\theta' : E' \to E''$ be an isogeny with kernel $\langle P' \rangle$, from E' to another elliptic curve E'', also defined over $\mathbb{Q}$. The kernel of the isogeny $\theta'\theta : E \to E''$ has composition factors $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules, so is not $E[7]$ (which has composition factors $\mathbb{Z}/7\mathbb{Z}$, μ_7). Therefore this rational isogeny of degree 7^2 is cyclic.

According to 5.2 of [12], there are no non-cuspidal rational points on $X_0(49)$, hence no cyclic rational isogenies of degree 49 between elliptic curves. □

Note that, although the analogue of the theorem for $\ell = 3$ or 5 ought to be true, the same proof will not work, since $X_0(9)$ and $X_0(25)$ have infinitely many rational points (as noted in the table at the beginning of [14]).

References

[1] A. Abbes, S. Ullmo, À propos de la conjecture de Manin pour les courbes elliptiques modulaires, *Compositio Math.* **103** (1996), 269–286.

[1] A. Agashe, W. Stein, Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero, *Math. Comp.* **74** (2005), 455–484.

[3] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), 843–939.

[4] H. Carayol, Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert, *Ann. Sci. École Norm. Sup. (4)* **19** (1986), 409–468.

[5] J. W. S. Cassels, Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer, *J. Reine Angew. Math.* **217** (1965), 180–199.

[6] J. Cremona, Elliptic curve data, http://www.maths.nott.ac.uk/ personal/jec/ftp/data/INDEX.html.

[7] J. E. Cremona, B. Mazur, Visualizing elements in the Shafarevich-Tate group, *Experiment. Math.* **9** (2000), 13–28.

[8] M. Emerton, Optimal quotients of modular Jacobians, *Math. Ann.* **327** (2003), 429–458.

[9] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366.

[10] V. A. Kolyvagin, Euler Systems, in The Grothendieck Festschrift, Vol. II, Progr. Math. 87, Birkhäuser, Boston, 1990, pp. 435-483.

[11] R. P. Langlands, Modular forms and ℓ-adic representations, in *Modular Functions of One Variable II,* Lect. Notes Math. **349,** 361–500, Springer-Verlag, 1973.

[12] G. Ligozat, Courbes modulaires de genre 1, Bull. Soc. Math. France, Mém. 43, supplement to *Bull. Soc. Math. France* **103** (1975), 1–80.

[13] B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. IHES* **47** (1977), 33–186.

[14] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–162.

[15] J.-F. Mestre, J. Oesterlé, Courbes de Weil semi-stables de discriminant une puissance m-ième, J. reine angew. Math. **400** (1989), 173–184.

[16] G. Stevens, Stickelberger elements and modular parametrisations of elliptic curves, *Invent. Math.* **98** (1989), 75–106.

[17] R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. Math.* **141** (1995), 553–572.

[18] V. Vatsal, Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves, *J. Inst. Math. Jussieu* **4** (2005), 281–316.

[19] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. Math.* **141** (1995), 443–551.

University of Sheffield, Department of Pure Mathematics, Hicks Building, Hounsfield Road, Sheffield, S3 7RH, U.K.

E-mail address: n.p.dummigan@shef.ac.uk