ACTA ARITHMETICA
126.4 (2007)

Ranks of elliptic curves in cubic extensions

by

TIM DOKCHITSER (Cambridge)

For an elliptic curve over the rationals, Goldfeld's conjecture [4] asserts that the analytic rank, $\mathrm{ord}_{s=1} L(E_d/\mathbb{Q}, s)$, of quadratic twists E_d of E is positive for squarefree d's with density $1/2$. In other words, the analytic rank of E goes up in quadratic extensions $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ half of the time. In particular, for every $E/\mathbb{Q}$ there are

(a) infinitely many quadratic extensions where the rank goes up, and
(b) infinitely many ones where it does not.

In fact, both (a) and (b) are known for the analytic rank and also for the arithmetic (Mordell–Weil) rank $\mathrm{rk}\, E(K) = \dim_{\mathbb{Q}} E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$.

On the other hand, root number formulas in [2, 7] show that the situation is somewhat different for extensions $\mathbb{Q}(\sqrt[r]{m})/\mathbb{Q}$ with $r>2$ and varying $m>1$. We will be concerned with the case $r = 3$, and there are examples of curves (such as $E =$19A3, see [2, Cor. 7]) for which the analytic rank goes up in *every* non-trivial extension $\mathbb{Q}(\sqrt[3]{m})/\mathbb{Q}$; so (b) fails for cubic extensions. As for (a), the formulas do imply that the analytic rank goes up in infinitely many cubic extensions if $E/\mathbb{Q}$ is semistable. It turns out that the same is true of the arithmetic rank for any E over a number field K. Thus we have

THEOREM 1. *Let K be a number field and let E/K be an elliptic curve. There are infinitely many classes $[m] \in K^*/K^{*3}$ (with $m \in K^*$) such that*

$$\mathrm{rk}\, E(K(\sqrt[3]{m})) > \mathrm{rk}\, E(K).$$

Proof. First, E has finite torsion over the compositum $K(\mu_3, \{\sqrt[3]{m}\}_{m\in K^*})$, as every prime v of it has finite residue field, and prime-to-v torsion injects under the reduction map modulo v if E has good reduction at v.

Second, with $F = K(\mu_3, \sqrt[3]{m})$, the natural map

$$e:\ E(K)/lE(K) \to E(F)/lE(F)$$

2000 *Mathematics Subject Classification*: Primary 11G05.

is injective for $l \neq 2,3$; in fact, the kernel-cokernel exact sequence for the Kummer maps for $E(K)$ and $E(F)$ (see [8, §VIII.2]) shows that $\ker e$ is contained in $H^1(\mathrm{Gal}(F/K), E(F)[l])$, which is trivial for $l \neq 2,3$, because the order of $\mathrm{Gal}(F/K)$ divides 6.

It follows from these two facts that points of $E(K)$ can become divisible by some prime l only in finitely many of the extensions $K(\sqrt[3]{m})$. Thus it suffices to show that $E(L)$ is strictly larger than $E(K)$ for infinitely many distinct fields of the form $L = K(\sqrt[3]{m})$. (This argument works generally for any abelian variety and $\sqrt[r]{m}$ with $r \geq 2$.)

Now suppose E/K is given by

$$E:\ y^2 = x^3 + ax + b, \qquad a, b \in K,$$

assuming for the moment that $a \neq 0$. Let $\mathcal{P} = (x_{\mathcal{P}}, y_{\mathcal{P}})$ be a non-trivial 3-torsion point on E. Thus, $\mathcal{P}$ is an inflection point, and the function f (unique up to a constant) with divisor $3(\mathcal{P}) - 3(O)$ defines a line

$$\mathcal{L}:\ y - y_{\mathcal{P}} = \kappa(x - x_{\mathcal{P}}), \qquad \kappa = \frac{3x_{\mathcal{P}}^2 + a}{2y_{\mathcal{P}}}.$$

A computation shows that $x_{\mathcal{P}} = \kappa^2/3$ and $y_{\mathcal{P}} = (\kappa^4 + 3a)/6\kappa$, so $\mathcal{L}$ is defined over the field $K(\kappa) = K(x_{\mathcal{P}}, y_{\mathcal{P}}) = K(\mathcal{P})$. Parametrise $\mathcal{L}$ by $(x, y) = (x_{\mathcal{P}} - \tau/3, y_{\mathcal{P}} - \kappa\tau/3)$, express the right-hand side solely in terms of κ and τ, and use this to define a map from $\mathbb{A}^2$ to $\mathbb{A}^2$. In other words, let k and t be indeterminates and consider the rational map $\phi : \mathbb{A}^2_{k,t} \to \mathbb{A}^2_{x,y}$ given by

$$x = \frac{k^2 - t}{3}, \quad y = \frac{k^4 + 3a - 2k^2 t}{6k}.$$

Substituting these into the equation for E shows that the Zariski closure of $\phi^{-1}(E)$ is the affine curve

$$C:\ 4k^2t^3 = k^8 + 18ak^4 + 108bk^2 - 27a^2.$$

The degree 8 polynomial $P(k)$ on the right has discriminant $-2^{24}3^{21}a^2(4a^3 + 27b^2)^3 \neq 0$, so C is non-singular and geometrically irreducible; in fact, C has geometric genus 7. It is also clear from the construction that $P(\kappa) = 0$, although the fact that the equation of C has no terms with t and t^2 is somewhat surprising, and depends on the exact choice of expressions for $x_{\mathcal{P}}$ and $y_{\mathcal{P}}$ in terms of κ.

Now every $x \in K^*$ gives a point $Q_x = (x, \sqrt[3]{m_x}) \in C(K(\sqrt[3]{m_x}))$ with $m_x = P(x)/4x^2$. These Q_x lie in infinitely many distinct extensions $K(\sqrt[3]{m})/K$, for otherwise the compositum $F = K(\{\sqrt[3]{m_x}\}_{x \in K^*})$ would be a number field with $C(F)$ infinite, contradicting Faltings' theorem. Finally, if $m_x \notin K^{*3}$, then the point $\phi(Q_x)$ is in $E(K(\sqrt[3]{m_x}))$ but not in $E(K)$.

It remains to note that the same construction works when $a = 0$, except that the equation of C has to be divided by k^2, in which case C has geometric genus 4 rather than 7. ∎

REMARK 2. For $K = \mathbb{Q}$, a related result due to Fearnley and Kisilevsky ([3, Thm. 1a]) is that for any $E/\mathbb{Q}$, the set of *abelian* cubic extensions $L/\mathbb{Q}$ for which $\operatorname{rk} E(L) > \operatorname{rk} E(\mathbb{Q})$ is either empty or infinite. (Note also the appearance of the polynomial $P(x)$ in Prop. 3 of [3].)

REMARK 3. Call a prime v of K *anomalous* for $E[p]$ if E has good reduction at v, and the reduced curve $\widetilde{E}$ has non-trivial p-torsion over the residue field k_v; so p is anomalous for $E/\mathbb{Q}$ as defined by Mazur in [6] if it is anomalous for $E[p]$ in this terminology.

Suppose that $P(x)$ is irreducible over K, so that it is a minimal polynomial for κ. Then for all but finitely many primes v of K, $P(x)$ has a root modulo v if and only if v is anomalous for $E[3]$. It follows easily that apart from finitely many exceptions, every extension $K(\sqrt[3]{m})/K$ produced in the proof of the theorem is ramified at some anomalous prime for $E[3]$. The appearance of anomalous primes in the construction is not coincidental, and has possibly a deep connection to Iwasawa theory. We illustrate this with one example.

EXAMPLE 4. Take $E = X_1(11)$ of conductor 11 over $K = \mathbb{Q}$,

$$E:\ y^2 = x^3 - \frac{1}{3}x + \frac{19}{108}.$$

If $m > 1$ is a cube-free integer, then the analytic rank of $E/\mathbb{Q}(\sqrt[3]{m})$ is odd if and only if $11 \mid m$. Let us look at the even rank case.

Define $M = \mathbb{Q}(\mu_3)$. From 3-descents for $E/\mathbb{Q}$ and $E_{-3}/\mathbb{Q}$, one obtains $E(M) \cong \mathbb{Z}/5\mathbb{Z}$ and $\text{Ш}(E/M)[3] = 1$. It follows that the cyclotomic Euler characteristic $\chi_{\mathrm{cyc}}(E/M)$ is 1, as it is the 3-part of the quantity

$$(\dagger) \qquad |\text{Ш}(E/M)[3^\infty]| \cdot \prod_{v|3} |\widetilde{E}(k_v)|^2 \cdot \prod_{v} c_v \cdot |E(M)|^{-2},$$

and all of the terms are 3-adic units.

Now let $F_m = M(\sqrt[3]{m})$ for some cube-free m which is prime to 11. This is an abelian cubic extension of M, and an application of a formula by Hachimori and Matsuno for the λ-invariant in p-power Galois extensions shows that the following conditions are equivalent (cf. [5, Thm. 3.1] and [1, Cor. 3.20, 3.24]):

(i) either $\operatorname{rk} E(F_m) > 0$, or $\operatorname{rk} E(F_m) = 0$ and $\chi_{\mathrm{cyc}}(E/F_m) \neq 1$,
(ii) $v \mid m$ for some prime v of M such that $\widetilde{E}(k_v)[3] \neq 0$.

Moreover, the expression for $\chi_{\mathrm{cyc}}(E/F_m)$ as in ($\dagger$) shows that (i) actually reads "either $\operatorname{rk} E(F_m) > 0$ or $|\text{Ш}(E/F_m)[3]| \neq 0$", because the other terms stay prime to 3.

As for (ii), a prime v of M with $v \mid l$ ($l \neq 3, 11$) is anomalous for the 3-torsion of E/M if and only if l is anomalous for the 3-torsion of $E/\mathbb{Q}$. This is clear if l splits in M, and for l inert this follows by inspection of the possible conjugacy classes of Frobenius of $l \equiv 2 \pmod 3$ in

$\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_3)$. To be precise, it is not hard to see that the possible degrees of the irreducible factors of

$$P(x) = x^8 - 6x^4 + 19x^2 - 3$$

modulo such l are $(1,1,2,2,2)$ and (8), so $P(x)$ has a linear factor over $\mathbb{F}_l$ if and only if it has one over $\mathbb{F}_{l^2}$.

For $E = X_1(11)$, the above equivalence shows that anomalous primes are responsible for either the rank of E or Ш[3] going up in cubic extensions. Incidentally, this proves that $\mathrm{rk}\, E(\mathbb{Q}(\sqrt[3]{m}))$ is zero for infinitely many m (those not divisible by 11 or anomalous primes), but does not say whether it is the rank or Ш[3] that goes up otherwise. On the other hand, the construction in Theorem 1 implies the following:

LEMMA 5. *For* $E = X_1(11)$, *we have* $\mathrm{rk}\, E(\mathbb{Q}(\sqrt[3]{m})) > 0$ *for infinitely many distinct cube-free integers* $m > 1$ *that are prime to* 11, *and infinitely many of those with* $11 \parallel m$.

Proof. It is easy to see that every $x \in \mathbb{Q}^*$ which is an 11-adic unit and satisfies $x \equiv \pm 1 \mod 11$ (resp. $x \not\equiv \pm 1 \mod 11$) gives a point $\phi(Q_x)$ of $E(\mathbb{Q}(\sqrt[3]{m}))$ with $11 \parallel m$ (resp. $11 \nmid m$). ∎

Acknowledgements. The author would like to thank J. Coates, V. Dokchitser, A. J. Scholl and J. Top for discussions of this problem.

References

[1] T. Dokchitser and V. Dokchitser, *Computations in non-commutative Iwasawa theory*, with an appendix by J. Coates and R. Sujatha, Proc. London Math. Soc., to appear.

[2] V. Dokchitser, *Root numbers of non-abelian twists of elliptic curves*, Proc. London Math. Soc. (3) 91 (2005), 300–324.

[3] J. Fearnley and H. Kisilevsky, *Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves*, preprint, 2004.

[4] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, in: Number Theory (Carbondale, IL, 1979), Lecture Notes in Math. 751, Springer, 1979, 108–118.

[5] Y. Hachimori and K. Matsuno, *An analogue of Kida's formula for Selmer groups of elliptic curves*, J. Algebraic Geom. 8 (1999), 581–601.

[6] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. 18 (1972), 183–266.

[7] D. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compositio Math. 100 (1996), 311–349.

[8] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

Robinson College
Cambridge, CB3 9AN, United Kingdom
E-mail: t.dokchitser@dpmms.cam.ac.uk

Received on 10.11.2005
and in revised form on 4.11.2006 (5094)