Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 346 (2008) 483–486
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Number Theory

On the proportion of rank 0 twists of elliptic curves

Andrzej Dąbrowski

Institute of Mathematics, University of Szczecin, ul. Wielkopolska 15, 70-451 Szczecin, Poland

Received 7 November 2006; accepted after revision 25 March 2008

Presented by Jean-Pierre Serre

Dedicated to dear Ewa Beata

Abstract

Let E be an elliptic curve defined over $\mathbf{Q}$, let E_d denote its dth quadratic twist, and $r_{E_d} := \operatorname{rank} E_d(\mathbf{Q})$. We prove, that, for any positive integer k there are pairwise non-isogenous elliptic curves $E^1, \ldots, E^k$ such that $r_{E^1{}_p} = \cdots = r_{E^k{}_p} = 0$ for a positive proportion of primes p. ***To cite this article: A. Dąbrowski, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

Résumé

Sur la proportion de tordues de courbes elliptiques qui sont de rang 0. Soit E une courbe elliptique définie sur $\mathbf{Q}$, E_d la tordue quadratique de E par d, et $r_{E_d} := \operatorname{rang} E_d(\mathbf{Q})$. On démontre qu'il existe, pour tout entier positif k, des courbes elliptiques $E^1, \ldots, E^k$, qui sont 2 à 2 non isogènes, et telles que $r_{E^1{}_p} = \cdots = r_{E^k{}_p} = 0$ pour une famille de nombres premiers p de densité positive. ***Pour citer cet article : A. Dąbrowski, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

1. Introduction

Let E be an elliptic curve over $\mathbf{Q}$ given by the Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$ $(a, b, c \in \mathbf{Z})$. If d is a squarefree integer, then we define the dth quadratic twist E_d of E to be the elliptic curve given by the equation $y^2 = x^3 + adx^2 + bd^2x + cd^3$. Let r_{E_d} denote the rank of the Mordell–Weil group $E_d(\mathbf{Q})$.

From the work of Waldspurger [15] (combined with the work of Kolyvagin [11], and of Wiles and others [1]) it follows that $r_{E_d} = 0$ for infinitely many squarefree d's. It is believed [5] that a positive proportion of twists E_d have rank zero. Such an expectation follows, under the Riemann hypothesis, from the work of Iwaniec and Sarnak [8]. Conditional results (in a more general situation) are also proved in [3]. Unconditional results are only known for a few specific curves [9,10,14]. The best unconditional (but weaker) result in full generality is due to Ono and Skinner [12]: $|\{|d| \leqslant X\colon\ r_{E_d} = 0\}| \gg X/\log X$.

Hoffstein and Luo [6] proved that, for fixed E, there exist infinitely many odd squarefree d with the number of prime factors no greater than 3 with $r_{E_d} = 0$. Ono and Skinner [12] proved that, when E has conductor $\leqslant 100$, E_p or

E-mail address: dabrowsk@wmf.univ.szczecin.pl.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2008.03.025

E_{-p} has rank zero for a positive proportion of primes p. Dąbrowski and Wieczorek [4] proved (assuming there are infinitely many pairs of twin prime numbers) that, for any positive integer k, there are pairwise non-isogenous curves $E^1, \dots, E^k$ such that $r_{E^1_p} = \cdots = r_{E^k_p} = 0$ for a positive proportion of primes p.

Theorem 1. *For any positive integer k there are pairwise non-isogenous elliptic curves $E^1, \dots, E^k$ such that $r_{E^1{}_p} = \cdots = r_{E^k{}_p} = 0$ for a positive proportion of primes p.*

The proof is based on the 2-descent method, applied to explicit families of elliptic curves, and uses the result of Chen [2] (see also Remark (i)).

2. Proof of Theorem 1

For integers A, B, m satisfying $2^{2m} = A + B$ we consider the elliptic curve $E^{m,A}$ given by the equation $y^2 = x(x + A)(x - B)$. Let $E'^{m,A}$ be the elliptic curve given by the equation $y^2 = x^3 - 2(A - B)x^2 + 2^{4m}x$. Consider the two-isogeny $\phi : E_r^{m,A} \to E_r'^{m,A}$, defined by $\phi((x, y)) = (y^2/x^2, -y(ABr^2 + x^2)/x^2)$; let $\hat{\phi}$ denote the dual isogeny. In the first part of this section, we compute the Selmer groups $S^{(\phi)}(E_r^{m,A}/\mathbf{Q})$, and $S^{(\hat{\phi})}(E_r'^{m,A}/\mathbf{Q})$ in a case AB is a product of two or three different primes and r runs over the suitable set of primes of positive proportion. We use the notations and results from chapter X of Silverman's book [13]. Let

$$C_d^{(r)}(m, A)\colon\ dy^2 = d^2 - 2rd(A - B)x^2 + 2^{4m}r^2x^4,$$
$$C_d'^{(r)}(m, A)\colon\ dy^2 = d^2 + 4rd(A - B)x^2 - 16ABr^2x^4$$

be the principal homogeneous spaces under the actions of the elliptic curves previously defined. Let $\Sigma(M)$ and $\Delta(M)$ be the support of an integer M in the set of prime numbers and the set of divisors of M in $\mathbf{Z}$ respectively. Using [13, Proposition 4.9, p. 302], we have the following identifications:

$$S^{(\phi)}\big(E_r^{m,A}/\mathbf{Q}\big) \simeq \big\{d \in \Delta(2ABr)\colon\ C_d^{(r)}(m, A)(\mathbf{Q}_l) \neq \emptyset\ \forall l \in \Sigma(2ABr) \cup \{\infty\}\big\},$$
$$S^{(\hat{\phi})}\big(E_r'^{m,A}/\mathbf{Q}\big) \simeq \big\{d \in \Delta(2ABr)\colon\ C_d'^{(r)}(m, A)(\mathbf{Q}_l) \neq \emptyset\ \forall l \in \Sigma(2ABr) \cup \{\infty\}\big\}.$$

To check that $C_d^{(r)}(m, A)$ has no $\mathbf{Q}_l$-rational point (x, y), we show that the number of terms in the equality $dy^2 = d^2 - 2rd(A - B)x^2 + 2^{4r}r^2x^4$ which have minimal l-adic valuation is at most two. If there is only one term, we are done. If there are two terms, we show that the ratio of those terms is (after changing the sign if appropriate) not a square modulo l (modulo 8, if $l = 2$).

Lemma 1. *Let p and q be odd prime numbers such that $2^{2m} = p + q$. If $p \equiv 1 \pmod 4$, then we have*

$$S^{(\phi)}\big(E_r^{m,p}/\mathbf{Q}\big) \simeq (0) \quad \text{and} \quad S^{(\hat{\phi})}\big(E_r'^{m,p}/\mathbf{Q}\big) \simeq (\mathbf{Z}/2\mathbf{Z})^2$$

for primes r satisfying $pr \equiv 3 \pmod 8$ and $(\frac{q}{r}) = -(\frac{p}{r}) = 1$.

Proof. We have $C_{pk}^{(r)}(m, p)(\mathbf{Q}_p) = \emptyset$ for squarefree integers k, $(k, p) = 1$, as can be checked by examining the p-adic valuations of both sides of the equation defining $C_{pk}^{(r)}(m, p)$. Similarly, we have $C_{qk}^{(r)}(m, p)(\mathbf{Q}_q) = \emptyset$. Of course, $C_d^{(r)}(m, p)(\mathbf{R}) = \emptyset$ for $d < 0$. Consequently, we obtain $S^{(\phi)}(E_r^{m,p}/\mathbf{Q}) \subset \langle 2, r\rangle \simeq (\mathbf{Z}/2\mathbf{Z})^2$. Using the assumptions $p \equiv 1 \pmod 4$ and $pr \equiv 3 \pmod 8$, we conclude that $C_{2k}^{(r)}(m, p)(\mathbf{Q}_2) = \emptyset$ for $k \in \{1, r\}$. On the other hand, $(\frac{r}{p}) = -1$ implies $C_r^{(r)}(m, p)(\mathbf{Q}_p) = \emptyset$.

Non-existence of dyadic points on $C_{2k}'^{(r)}(m, p)$ (k odd) implies $S^{(\hat{\phi})}(E_r'^{m,p}/\mathbf{Q}) \subset \langle -1, p, q, r\rangle \simeq (\mathbf{Z}/2\mathbf{Z})^4$. The sets $C_{-pr}'^{(r)}(m, p)(\mathbf{Q})$ and $C_{qr}'^{(r)}(m, p)(\mathbf{Q})$ contain the point $(1/2, 0)$, hence $\langle -pr, qr\rangle \subset S^{(\hat{\phi})}(E_r'^{m,p}/\mathbf{Q})$. Using the assumptions $r \equiv 3 \pmod 4$ and $(\frac{pq}{r}) = -1$, we obtain $C_{-1}'^{(r)}(m, p)(\mathbf{Q}_r) = \emptyset$. Similarly, a closer examination of the situations, using the assumptions of the lemma, enables one to conclude that $C_p'^{(r)}(m, p)(\mathbf{Q}_r) = \emptyset$ and $C_r'^{(r)}(m, p)(\mathbf{Q}_2) = \emptyset$. The assertion now follows. □

Let $Ш(E/\mathbf{Q})$ denote the Shafarevich–Tate group of an elliptic curve E over $\mathbf{Q}$.

Lemma 2. *Fix odd primes p, q_1 and q_2 satisfying $2^{2m} = p + q_1q_2$.*

(i) *Consider the set of primes $r \equiv 5 (\mathrm{mod}\ 8)$ satisfying $(\frac{p}{r}) = -(\frac{q_1}{r}) = -(\frac{q_2}{r}) = 1$. We have $S^{(\phi)}(E_r^{m,A}/\mathbf{Q}) \simeq (0)$ and $S^{(\hat{\phi})}(E_r^{'m,A}/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^2$, where $A = q_1q_2$ if $p \equiv 1 (\mathrm{mod}\ 4)$ and $A = p$ if $p \equiv 3 (\mathrm{mod}\ 8)$.*

(ii) *If $p \equiv 7 (\mathrm{mod}\ 8)$, then*

$$\dim_2 S^{(\phi)}\big(E_r^{m,q_1q_2}/\mathbf{Q}\big) + \dim_2 S^{(\hat{\phi})}\big(E_r^{'m,q_1q_2}/\mathbf{Q}\big) - \dim_2 Ш\big(E_r^{m,q_1q_2}/\mathbf{Q}\big)[\phi] - \dim_2 Ш\big(E_r^{'m,q_1q_2}/\mathbf{Q}\big)[\hat{\phi}] = 2$$

for a positive proportion of primes r (we abbreviate $\dim_2 = \dim_{\mathbf{F}_2}$).

Proof. (i) Assume $p \equiv 1 (\mathrm{mod}\ 4)$. Following the same line as in the proof of lemma 1, we obtain $S^{(\phi)}(E_r^{m,q_1q_2}/\mathbf{Q}) \subset \langle 2, r\rangle$ and $\langle pr, -q_1q_2r\rangle \subset S^{(\hat{\phi})}(E_r^{'m,q_1q_2}/\mathbf{Q}) \subset \langle -1, p, q_1q_2, r\rangle$. A closer examination of the situations, using the assumptions of the lemma, leads to $C_k^{(r)}(m, q_1q_2)(\mathbf{Q}_2) = \emptyset$ ($k \in \{2, r\}$), $C_l^{'(r)}(m, q_1q_2)(\mathbf{Q}_2) = \emptyset$ ($l \in \{-1, r, q_1q_2\}$), and $C_{\pm q_i}^{'(r)}(m, q_1q_2)(\mathbf{Q}_r) = \emptyset$ ($i = 1, 2$). The assertion now follows.

Similarly, we obtain $S^{(\phi)}(E_r^{m,p}/\mathbf{Q}) = \{1\}$ and $S^{(\hat{\phi})}(E_r^{'m,p}/\mathbf{Q}) = \langle -pr, q_1q_2r\rangle$ if $p \equiv 3 (\mathrm{mod}\ 8)$.

(ii) If $q_1 \equiv 3, 5 (\mathrm{mod}\ 8)$, then

$$S^{(\phi)}\big(E_r^{m,q_1q_2}/\mathbf{Q}\big) = \{1\} \quad \text{and} \quad S^{(\hat{\phi})}\big(E_r^{'m,q_1q_2}/\mathbf{Q}\big) = \langle pr, -q_1q_2r\rangle$$

for primes $r \equiv 7 (\mathrm{mod}\ 8)$ satisfying $(\frac{p}{r}) = -(\frac{q_1q_2}{r}) = 1$.

If $q_1 \equiv 1, 7 (\mathrm{mod}\ 8)$, then $S^{(\phi)}(E_r^{m,q_1q_2}/\mathbf{Q}) = \{1\}$ and $S^{(\hat{\phi})}(E^{'m,q_1q_2}/\mathbf{Q}) = \langle pr, -q_1q_2r, kq_1, kq_2\rangle$ ($k = 1$ or -1) for primes $r \equiv 5 (\mathrm{mod}\ 8)$ satisfying $(\frac{p}{r}) = -(\frac{q_1q_2}{r}) = 1$. One checks that $C_{\pm q_i}^{'(r)}(m, q_1q_2)(\mathbf{Q}) = \emptyset$. Consequently, the group $W(E_r^{'m,q_1q_2}/\mathbf{Q}) = E_r^{m,q_1q_2}(\mathbf{Q})/\hat{\phi}(E_r^{'m,q_1q_2}(\mathbf{Q}))$ (as the subgroup of $S^{(\hat{\phi})}(E_r^{'m,q_1q_2}/\mathbf{Q})$ consisting of homogeneous spaces with rational point) equals $\langle pr, -q_1q_2r\rangle$. The proof now follows from the following exact sequence (see [13], Theorem 4.2, p. 298): $0 \to W(E_r^{'m,q_1q_2}/\mathbf{Q}) \to S^{(\hat{\phi})}(E_r^{'m,q_1q_2}/\mathbf{Q}) \to Ш(E_r^{'m,q_1q_2}/\mathbf{Q})[\hat{\phi}] \to 0$ (and its variant for E_r^{m,q_1q_2}). □

Proof of Theorem 1. We will apply the fundamental formula (compare [13], p. 314):

$$r_{E_d^{m,A}} = \dim_2 S^{(\phi)}\big(E_d^{m,A}/\mathbf{Q}\big) + \dim_2 S^{(\hat{\phi})}\big(E_d^{'m,A}/\mathbf{Q}\big) - \dim_2 Ш\big(E_d^{m,A}/\mathbf{Q}\big)[\phi] - \dim_2 Ш\big(E_d^{'m,A}/\mathbf{Q}\big)[\hat{\phi}] - 2.$$

Chen [2] showed that every sufficiently large even number is the sum of a prime and a natural number which has at most two prime factors. We apply these results to the sequence 2^{2m}, $m \geqslant m_0$. Theorem 1 follows from the fundamental formula, and (the proof of) Lemmata 1 and 2 combining with Dirichlet theorem on primes in arithmetic progressions. □

Remarks. (i) Let us sketch the proof of Theorem 1 using Setzer–Neumann curves (and generalizations). Let $u^2 + 64 = p$ or p_1p_2 (p, p_1, p_2 primes), where the sign of u is chosen so that $u \equiv 1 (\mathrm{mod}\ 4)$. Consider the elliptic curves $E^u : y^2 = x^3 + ux^2 - 16x$ and E'^u: $y^2 = x^3 - 2ux^2 + x$. Let $\phi : E_r^u \to E_r'^u$ be the two-isogeny defined by $\phi((x, y)) = (y^2/x^2, -(16r^2 + x^2)/x^2)$. One can show, that $\dim_2 S^{(\phi)}(E_r^u/\mathbf{Q}) + \dim_2 S^{(\hat{\phi})}(E_r'^u/\mathbf{Q}) - \dim_2 Ш(E_r^u/\mathbf{Q})[\phi] - \dim_2 Ш(E_r'^u/\mathbf{Q})[\hat{\phi}] = 2$ for a positive proportion of primes r. To finish the proof of Theorem 1, one applies the following result of Iwaniec [7]: there are infinitely many integers n such that $n^2 + 64$ is the product of at most two primes.

(ii) The method of proof of Theorem 1 leads to the following conditional result. Assume the parity conjecture holds true. Then for any positive integer k there are pairwise non-isogenous elliptic curves $E^1, \ldots, E^k$ such that $r_{E^1{}_p} = \cdots = r_{E^k{}_p} = 1$ for a positive proportion of primes p.

Acknowledgements

The article was written during my visit to the Max-Planck-Institut für Mathematik in Bonn in September–December 2006. I would like to thank the Institute for the hospitality and support. I would like to thank the anonymous referee for the constructive criticism and comments which improved the final version.

References

[1] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over **Q**, J. Amer. Math. Soc. 14 (2001) 843–939.
[2] J.R. Chen, On the representation of a large even number as the sum of a prime and the product of at most two primes, Sci. Sinica 16 (1973) 157–176.
[3] A. Dąbrowski, J. Pomykała, Nonvanishing of motivic L-functions, Math. Proc. Cambridge Philos. Soc. 130 (2001) 221–235.
[4] A. Dąbrowski, M. Wieczorek, On the equation $y^2 = x(x - 2^m)(x + q - 2^m)$, J. Number Theory 124 (2007) 364–379.
[5] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, in: Lecture Notes in Math., vol. 751, Springer-Verlag, 1979, pp. 108–118.
[6] J. Hoffstein, W. Luo, Nonvanishing of L-series and the combinatorial sieve, Math. Res. Lett. 4 (1997) 435–444.
[7] H. Iwaniec, Almost-primes represented by quadratic polynomials, Invent. Math. 47 (1978) 171–188.
[8] H. Iwaniec, P. Sarnak, The non-vanishing of central values of automorphic L-functions and Landau–Siegel zeros, Israel J. Math. 120 (2000) 155–177.
[9] K. James, L-series with non-zero central critical value, J. Amer. Math. Soc. 11 (1998) 635–641.
[10] W. Kohnen, On the proportion of quadratic twists of L-functions attached to cusp forms not vanishing at the central point, J. Reine Angew. Math. 508 (1999) 179–187.
[11] V.A. Kolyvagin, Finiteness of $E(\mathbf{Q})$ and $Ш(E, \mathbf{Q})$ for a subclass of Weil curves, Izv. Acad. Nauk USSR 52 (1988) 522–540 (in Russian).
[12] K. Ono, C. Skinner, Non-vanishing of quadratic twists of modular L-functions, Invent. Math. 34 (1998) 651–660.
[13] J.H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1985.
[14] V. Vatsal, Rank-one twists of a certain elliptic curve, Math. Ann. 311 (1998) 791–794.
[15] J.L. Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier, J. Math. Pures Appl. 60 (1981) 375–484.