1

The distribution of ranks in families of quadratic twists of elliptic curves

A. Silverberg[1]

Department of Mathematics,
University of California at Irvine,
Irvine, CA 92697
USA

This paper gives a very brief survey, in the form of a table, of some results and conjectures about densities of ranks of elliptic curves over $\mathbb{Q}$ in families of quadratic twists. The table summarizes some of the knowledge to date on the density of quadratic twists of rank r or $\geq r$, for some small values of r. We also give a commentary on the table. For a more extensive survey of ranks of elliptic curves over $\mathbb{Q}$, see [RS02]. The author thanks Roger Heath-Brown for helpful comments.

We first fix notation. If E is an elliptic curve of the form $y^2 = f(x)$, let $E^{(d)}$ denote $dy^2 = f(x)$, the quadratic twist of E by d. If E is an elliptic curve over $\mathbb{Q}$, it suffices to consider d that are squarefree integers. Let

$$N_*(X) = \#\{\text{squarefree } d \in \mathbb{Z} : |d| \leq X, \text{rank}(E^{(d)}(\mathbb{Q})) \text{ is } *\},$$

where $*$ can be "2", "odd", "≥ 3", etc. The table below gives a summary of some of the known results (and conjectures) to date on the rate of growth of $N_r(X)$ and $N_{\geq r}(X)$.

It is well-known (see Theorem 333 of [HW79]) that

$$N_{\geq 0}(X) = \#\{\text{squarefree } d \in \mathbb{Z} : |d| \leq X\} \sim 2X \prod_p (1 - \frac{1}{p^2}) = \frac{2}{\zeta(2)} X = \frac{12}{\pi^2} X.$$

The first part of the Birch and Swinnerton-Dyer Conjecture [BSD63/5] says that the rank of an elliptic curve E over $\mathbb{Q}$ should be equal to the analytic rank (i.e., the order of vanishing at $s = 1$ of the L-function of E over $\mathbb{Q}$). In particular, the Birch and Swinnerton-Dyer Conjecture implies the Parity Conjecture, which says that the rank has the same

[1] Supported by NSA grant MDA904-03-1-0033.

parity as the analytic rank. The parity of the analytic rank can be read off from the sign in the functional equation for the L-function. Using the way that the sign varies as one twists the curve, one can show that the Parity Conjecture implies that, as $|d|$ grows, the ranks of the quadratic twists by squarefree $d \in \mathbb{Z}$ of a fixed elliptic curve over $\mathbb{Q}$ are even half the time and odd half the time. (See the N_{odd}, N_{even} table entry.)

In 1979, Goldfeld [G79] conjectured that for every fixed elliptic curve, the average rank of its quadratic twists is $\frac{1}{2}$.

Goldfeld Conjecture *If E is an elliptic curve over $\mathbb{Q}$, then*

$$\lim_{X\to\infty} \frac{\sum_{\text{squarefree } d\in\mathbb{Z}, |d|\le X} \operatorname{rank}(E^{(d)}(\mathbb{Q}))}{\#\{\text{squarefree } d \in \mathbb{Z} : |d| \le X\}} = \frac{1}{2}.$$

If one assumes both the Parity Conjecture and Goldfeld's Conjecture, then for every fixed elliptic curve, the ranks of the quadratic twists should be zero half the time and one half the time. (See the last N_0 and N_1 table entries.)

In the table, "w/PC" means that the result is conditional on the Parity Conjecture, and "w/PC & GC" means that the result is conditional on both the Parity Conjecture and Goldfeld's Conjecture. Further, "w/RMTC" means this is a conjecture made in [CKRS02] (see Conjecture 1 and (7)), which is based on Random Matrix Theory.

All "$\gg$" and "$\ll$" entries in the table, and in the discussion below, should be read as "there is a positive constant, depending on E but not on X, such that for all sufficiently large X, we have ...".

Ono and Skinner [OS98], using results of Waldspurger and of Friedberg and Hoffstein, show that $N_0(X) \gg X/\log X$ for all elliptic curves. It was known earlier that $N_0(X) \gg X/\log X$ for certain elliptic curves (see for example [R74] for $y^2 = x^3 - x$).

Work of Monsky [Mo90]), Birch [B69, B70], and Heegner [H52] shows that certain elliptic curves E have $\operatorname{rank}(E^{(p)}) \ge 1$ for all primes p in certain congruence classes (for example, for $y^2 = x^3 - x$ and all primes $p \equiv 5$ or $7 \pmod 8$), and thus $N_{\ge 1}(X) \gg X/\log X$ (in fact, $N_1(X) \gg X/\log X$).

For the elliptic curve $y^2 = x^3 - x$, Heath-Brown (see Theorem 2 of [HB94]) showed that $N_0(X) > (.279)6X/\pi^2$, and, subject to the Parity Conjecture, $N_1(X) > (.559)6X/\pi^2$.

The methods for finding lower bounds for $N_{\ge r}(X)$ when $r \ge 2$ involve finding twists $E^{(g(T))}$ of E over $\mathbb{Q}(T)$ of rank $\ge r$, and specializing T. By Theorem C of [Si83], for all but finitely many $t \in \mathbb{Q}$ one has

$N_{\geq 0}(X)$	$\sim \frac{12}{\pi^2} X$	
$N_{\text{odd}}(X)$ $N_{\text{even}}(X)$	$\sim \frac{6}{\pi^2} X$	w/PC
$N_0(X)$	$\gg \frac{X}{\log X}$	[OS98]
	$> (.279) \frac{6}{\pi^2} X$	for $y^2 = x^3 - x$ [HB94]
	$\sim \frac{6}{\pi^2} X$	w/PC & GC
$N_1(X)$	$\gg \frac{X}{\log X}$	for $y^2 = x^3 - x$ [H52, B69, B70, Mo90]
	$> (.559) \frac{6}{\pi^2} X$	for $y^2 = x^3 - x$ w/PC [HB94]
	$\sim \frac{6}{\pi^2} X$	w/PC & GC
$N_{\geq 1}(X)$	$\gg X^{\frac{1}{2}}$	[ST95, GM91]
	$\geq \frac{6}{\pi^2} X$	w/PC
	$\sim \frac{6}{\pi^2} X$	w/PC & GC
$N_{\geq 2}(X)$	$\gg \frac{X^{\frac{1}{7}}}{\log X}$	$j(E) \neq 0, 1728$ [ST95]
	$\gg X^{\frac{1}{3}}$	for some E [ST95, RS01]
	$\gg X^{\frac{1}{2}}$	w/PC [ST95, GM91]
	$\gg X^{\frac{3}{4}-\epsilon}, \ll X^{\frac{3}{4}+\epsilon}$	w/RMTC [CKRS02]
$N_{\geq 3}(X)$	$\gg X^{\frac{1}{6}}$	for some E [ST95, RS01]
	$\gg X^{\frac{1}{3}}$	for some E w/PC [ST95, RS01]
$N_{\geq 4}(X)$	$\to \infty$	for some E [Me98, RS04]
	$\gg X^{\frac{1}{6}}$	for some E w/PC [RS01, RS04]
$N_{\geq 5}(X)$	$\to \infty$	for some E w/PC [Me98, RS04]

$\text{rank}(E^{(g(t))}) \geq r$. Using sieve theory, one can find a lower bound on the number of squarefree integers d such that $|d| \leq X$ and $d = g(t)z^2$ for some $t, z \in \mathbb{Q}$ (so $\text{rank}(E^{(d)}(\mathbb{Q})) = \text{rank}(E^{(g(t))}(\mathbb{Q}))$); see [GM91, ST95]. Mestre [Me92, Me98, Me00] has techniques for finding elliptic curves of "large" rank over $\mathbb{Q}(T)$ (and over $\mathbb{Q}$). See also work of Howe, Leprévost, and Poonen [HLP00]. Gouvêa and Mazur [GM91] showed that, assuming the Parity Conjecture, $N_{\geq 2,\text{even}}(X) \gg X^{1/2-\varepsilon}$. Stewart and Top [ST95], without assuming the Parity Conjecture, showed that if $j(E) \neq 0$ or 1728, then $N_{\geq 2}(X) \gg X^{1/7}/(\log X)^2$. For elliptic curves of the form

$$y^2 = ax^3 + bx^2 + bx + a$$

with $a, b \in \mathbb{Q}$ and $a(3a-b)(a+b) \neq 0$, they showed $N_{\geq 2}(X) \gg X^{1/3}$. For

$$y^2 = x(x-1)(x - (\frac{b^2+1}{2b})^2)$$

with $b \in \mathbb{Q} - \{0, 1, -1\}$, they showed $N_{\geq 3}(X) \gg X^{1/6}$ (based on an idea of Schoen [Sc90] who they say also obtained it independently).

Building on the work of Mestre, Gouvêa and Mazur, and Stewart and Top, Rubin and Silverberg [RS01, RS04] show that $N_{\geq 2}(X) \gg X^{\frac{1}{3}}$ holds, for example, for every elliptic curve $y^2 = x^3 + ax + b$ such that the cubic has a non-zero rational root. Further, $N_{\geq 3}(X) \gg X^{\frac{1}{3}}$ holds (subject to the Parity Conjecture), for example, for every elliptic curve E of the form $y^2 = x^3 + ax + b$ such that the cubic has three real roots (equivalently, the discriminant $\Delta(E) > 0$) and either

(a) the largest or the smallest root is rational, or
(b) E has a rational subgroup of order 3.

In particular, it holds for all elliptic curves over $\mathbb{Q}$ for which all the 2-torsion is rational.

Conjecture 1 of [CKRS02] predicts that $N_{\geq 2}(X) \sim CX^{3/4} \log^m(X)$ for some C and m. This prediction is based on random matrix theory. The workshop announcement [CFMS04] states that random matrix theory also predicts that $N_3(X) \sim CX^{1/4} \log^m(X)$, which is inconsistent with the $N_{\geq 3}(X) \gg X^{\frac{1}{3}}$ results stated above.

In [Me98], Mestre stated that if E is an elliptic curve over $\mathbb{Q}$ with torsion subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then E has infinitely many (non-isomorphic) quadratic twists with rank at least 4 over $\mathbb{Q}$. Theorems 3.2, 3.6, and 5.1 and Corollary 5.2 of [RS04] give other "$N_{\geq r}(X) \to \infty$" results for $r = 4$ and, assuming the Parity Conjecture, for $r = 5$.

All the entries in the table apply for example to the elliptic curves

$$y^2 = x(x+n)(x-n-1) \tag{1}$$

with n = 1, 8, 16, 21, 56, 65, 85, 96, 161, 176, 208, 261, 341, 408, 456, 533, and 560 (see Corollary 5.2 of [RS04]). All except the $N_{\geq 5}(X)$ entry are known to hold for the elliptic curves

$$y^2 = x(x-1)(x + \frac{a^2-1}{a^2+2}) \tag{2}$$

with $a \in \mathbb{Q} - \{0, \pm 1\}$ (see Theorem 5.5 of [RS01] and Theorem 3.2 of [RS04]), and all of those entries except the $N_{\geq 4}(X) \to \infty$ entry are known to hold even when $a = 0$. We remark that (2) is the quadratic twist by $\frac{a^2+2}{3}$ of (1) with $n = \frac{a^2-1}{3}$, and (2) for $a = 0$ is the quadratic twist by 2 of the curve $y^2 = x^3 - x$.

References

[B69] B. J. Birch, *Diophantine analysis and modular functions*, in Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), 35–42, Oxford Univ. Press, London, 1969.

[B70] B. J. Birch, *Elliptic curves and modular functions*, in Symposia Mathematica, Vol. IV (INDAM, Rome, 1968/69), 27–32 Academic Press, London, 1970.

[BSD63/5] B. J. Birch, H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I, II*, J. Reine Angew. Math. **212** (1963), 7–25; **218** (1965), 79–108.

[CFMS04] J. B. Conrey, D. Farmer, F. Mezzadri, N. C. Snaith, workshop announcement: *Special Week on Ranks of Elliptic Curves and Random Matrix Theory, 9–13 February, 2004*, `http://www.newton.cam.ac.uk/programmes/RMA/rmaw01.html` .

[CKRS02] J. B. Conrey, J. P. Keating, M. O. Rubinstein, N. C. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions*, in Number theory for the millennium, I (Urbana, IL, 2000), A. K. Peters, Natick, MA, 2002, 301–315.

[G79] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, in Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), M. B. Nathanson, ed., Lect. Notes in Math. **751**, Springer, Berlin, 1979, 108–118.

[GM91] F. Gouvêa, B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23.

[HW79] G. H. Hardy, E. M. Wright, An introduction to the theory of numbers, fifth edition, The Clarendon Press, Oxford University Press, New York, 1979.

[HB94] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), 331–370.

[H52] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253.

[HLP00] E. Howe, F. Leprévost, B. Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), 315–364.

[Me92] J-F. Mestre, *Rang de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris **314** (1992), 919–922.

[Me98] J-F. Mestre, *Rang de certaines familles de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris **327** (1998), 763–764.

[Me00] J-F. Mestre, *Ranks of twists of elliptic curves*, lecture at MSRI, September 11, 2000.

[Mo90] P. Monsky, *Mock Heegner points and congruent numbers*, Math. Z. **204** (1990), 45–67.

[OS98] K. Ono, C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. **134** (1998), 651–660.

[R74] M. J. Razar, *The non-vanishing of $L(1)$ for certain elliptic curves with no first descents*, Amer. J. Math. **96** (1974), 104–126.

[RS01] K. Rubin, A. Silverberg, *Rank frequencies for quadratic twists of elliptic curves*, Exper. Math. **10** (2001), 559–569.

[RS02] K. Rubin, A. Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc. **39** (2002), 455–474.

[RS04] K. Rubin, A. Silverberg, *Twists of elliptic curves of rank at least four*, this volume.

[Sc90] C. Schoen, *Bounds for rational points on twists of constant hyperelliptic curves*, J. Reine Angew. Math. **411** (1990), 196–204.

[Si83] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211.

[ST95] C. L. Stewart, J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.