Rank Frequencies for Quadratic Twists of Elliptic Curves

Karl Rubin and Alice Silverberg

CONTENTS

We thank NSF, NSA, and the Alexander-von-Humboldt Stiftung for financial support, and AIM and the Mathematics Institute of the University of Erlangen for congenial working environments.

We give explicit examples of infinite families of elliptic curves E over $\mathbb{Q}$ with (nonconstant) quadratic twists over $\mathbb{Q}(t)$ of rank at least 2 and 3. We recover some results announced by Mestre, as well as some additional families. Suppose D is a squarefree integer and let $r_E(D)$ denote the rank of the quadratic twist of E by D. We apply results of Stewart and Top to our examples to obtain results of the form

$$\#\{D : |D| < x,\ r_E(D) \geq 2\} \gg x^{1/3},$$
$$\#\{D : |D| < x,\ r_E(D) \geq 3\} \gg x^{1/6}$$

for all sufficiently large x.

1. INTRODUCTION

Throughout this paper E is an elliptic curve over $\mathbb{Q}$ defined by a Weierstrass equation $y^2 = f(x)$, where f is a monic cubic polynomial. The curve $Dy^2 = f(x)$ will be denoted E_D. When D is a nonzero integer, let $r_E(D)$ denote the rank of $E_D(\mathbb{Q})$. Let

$$N_r(E,x) = \#\{\text{squarefree } D \in \mathbb{Z} : |D| < x \text{ and } r_E(D) \geq r\},$$
$$N_r^+(E,x) = \#\{\text{squarefree } D \in \mathbb{Z} : |D| < x,\ r_E(D) \geq r,\ r_E(D) \equiv r \bmod 2\}.$$

Gouvêa and Mazur [1991] showed (using the fact that the twist $E_{f(u)}$ has rank one over $\mathbb{Q}(u)$) that if the Parity Conjecture holds then

$$N_2^+(E,x) > x^{(1/2)-\varepsilon}$$

for all sufficiently large x.

Mestre [1992, Théorème 1] showed that if $j(E) \notin \{0, 1728\}$ then there is a polynomial $g(u) \in \mathbb{Q}[u]$ of degree 14 such that the twist $E_{g(u)}$ has rank at least 2 over $\mathbb{Q}(u)$. Stewart and Top [1995, Theorem 3] used Mestre's result to show that

$$N_2(E,x) \gg x^{1/7}/(\log x)^2$$

for such E and for all sufficiently large x. For a special family of elliptic curves E, using a twist of E over $\mathbb{Q}(u)$ of rank at least 3, Stewart and Top [1995, Theorem 6] found lower bounds for $N_3(E,x)$. Mestre announced in [1998, Théorème 2] that if the torsion subgroup of $E(\mathbb{Q})$ contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, then E has a (nonconstant) quadratic twist over $\mathbb{Q}(u)$ of rank at least 3.

For certain elliptic curves E, Howe, Leprévost, and Poonen constructed polynomials $g(u)$ of degree 6 such that the twist $E_{g(u)}$ has rank 2 over $\mathbb{Q}(u)$. See [Howe et al. 2000, Proposition 4].

In this paper we describe a method (Section 2) for constructing (nonconstant) quadratic twists of E over $\mathbb{Q}(u)$ of ranks (at least) 2 and 3, and obtain further examples. In the rank 2 case (Section 3) we show that this method recovers the above mentioned results of Howe, Leprévost, and Poonen and of Mestre. The rank 3 cases (Section 4) include Mestre's curves and some other infinite families. In Section 5 we use results of Stewart and Top to obtain lower bounds for $N_r(E,x)$ (and for $N^+_{r+1}(E,x)$, subject to the Parity Conjecture) for these examples, with $r = 2$ or 3.

The idea behind the method is that given an elliptic curve E over $\mathbb{Q}(t)$, it is easy to find twists of E of rank r over extensions $K/\mathbb{Q}(t)$ with

$$\mathrm{Gal}(K/\mathbb{Q}(t)) \cong (\mathbb{Z}/2\mathbb{Z})^{r-1}.$$

When $r \le 3$, we show how to do this with $K = \mathbb{Q}(u)$ for some u, for certain families of curves.

We used PARI and Mathematica to perform the computations in this paper. The results of the computations, including those which are too long to display in the paper, are available electronically; see the section on Electronic Availability at the end of this article. After writing this paper we learned that the method we use here to construct rank 2 and 3 quadratic twists is essentially the same as one of the methods used by Mestre to prove the results announced in [Mestre 1998]. Since Mestre's proofs and explicit descriptions of the twists he obtains have not been published, and we need explicit forms of these twists for the applications in Section 5, we include the details here.

2. CONSTRUCTING USEFUL TWISTS

We begin with the following well-known result.

Lemma 2.1. *If F is a field of characteristic different from 2, A is an elliptic curve over F, and K is an abelian extension of F with $\mathrm{Gal}(K/F) \cong (\mathbb{Z}/2\mathbb{Z})^d$, then*

$$\mathrm{rank}\, A(K) = \sum_{\chi} \mathrm{rank}\, A^{\chi}(F)$$

where the sum is over characters $\chi : \mathrm{Gal}(K/F) \to \{\pm 1\}$, and A^{χ} is A if $\chi = 1$ and otherwise A^{χ} is the quadratic twist of A corresponding to χ.

Corollary 2.2. *Suppose E is an elliptic curve over $\mathbb{Q}$, $g_1, \ldots, g_r \in \mathbb{Q}(t)^{\times}$, the fields $\mathbb{Q}(t, \sqrt{g_i})$ are distinct quadratic extensions of $\mathbb{Q}(t)$, and $\mathrm{rank}\, E_{g_i}(\mathbb{Q}(t)) > 0$ for every i. Then*

$$\mathrm{rank}\, E_{g_1}(\mathbb{Q}(t, \sqrt{g_1 g_2}, \ldots, \sqrt{g_1 g_r})) \ge r.$$

If in addition $\mathbb{Q}(t, \sqrt{g_1 g_2}, \ldots, \sqrt{g_1 g_r}) = \mathbb{Q}(u)$ for some u, and $g(u) = g_1(t)$, then $\mathrm{rank}\, E_{g(u)}(\mathbb{Q}(u)) \ge r$.

Proof. Take $A = E_{g_1}$, $F = \mathbb{Q}(t)$, and

$$K = \mathbb{Q}(t, \sqrt{g_1 g_2}, \ldots, \sqrt{g_1 g_r}).$$

By Lemma 2.1,

$$\begin{aligned}\mathrm{rank}\, & E_{g_1}(\mathbb{Q}(t, \sqrt{g_1 g_2}, \ldots, \sqrt{g_1 g_r})) \\ &\ge \mathrm{rank}\, E_{g_1}(\mathbb{Q}(t)) + \sum_{i=2}^{r} \mathrm{rank}\, E_{g_1(g_1 g_i)}(\mathbb{Q}(t)) \\ &= \sum_{i=1}^{r} \mathrm{rank}\, E_{g_i}(\mathbb{Q}(t)) \ge r.\end{aligned}$$

This proves the first part of the corollary, and the second is immediate. □

Given an elliptic curve E over $\mathbb{Q}$, we want to use Corollary 2.2 to construct twists of E over $\mathbb{Q}(u)$ of "large" rank. The following lemma provides us with elements $g \in \mathbb{Q}(t)$ such that $\mathrm{rank}\, E_g(\mathbb{Q}(t)) > 0$.

Lemma 2.3. *Suppose E is the elliptic curve over $\mathbb{Q}$ defined by $y^2 = f(x)$. Then for every nonconstant $h \in \mathbb{Q}(t)$ we have*

$$\mathrm{rank}\, E_{f(h(t))}(\mathbb{Q}(t)) > 0.$$

Proof. The point $(h(t), 1)$ belongs to $E_{f(h(t))}(\mathbb{Q}(t))$. Since this point is nonconstant, it cannot be a torsion point. □

Remark 2.4. Conversely, if $g \in \mathbb{Q}(t)$ and $E_g(\mathbb{Q}(t))$ has positive rank, there is an $h \in \mathbb{Q}(t)$ such that

$E_g \cong E_{f(h(t))}$. To see this, let (h,k) be a point of infinite order in $E_g(\mathbb{Q}(t))$, and then $f \circ h = k^2 g$.

To apply Corollary 2.2 we also need to know when $\mathbb{Q}(t, \sqrt{g_1 g_2}, \ldots, \sqrt{g_1 g_d})$ is a rational function field. For this we use the following well-known result.

Lemma 2.5. *Let $k \in \mathbb{Q}[t]$ be a nonconstant squarefree polynomial. Then the curve $s^2 = k(t)$ has genus $\left[\frac{1}{2}(\deg k - 1)\right]$.*

Corollary 2.6. (i) *If $k \in \mathbb{Q}[t]$ is squarefree and $1 \le \deg k \le 2$, then the function field $\mathbb{Q}(t, \sqrt{k})$ has genus zero.*

(ii) *If $k_1, k_2 \in \mathbb{Q}[t]$ are linear and linearly independent over $\mathbb{Q}$, then the function field $\mathbb{Q}(t, \sqrt{k_1}, \sqrt{k_2})$ has genus zero.*

Proof. The first statement is immediate from Lemma 2.5. The second statement follows without difficulty by applying (i) first to the extension $\mathbb{Q}(t, \sqrt{k_1})/\mathbb{Q}(t)$, and then to the extension $\mathbb{Q}(t, \sqrt{k_1}, \sqrt{k_2})/\mathbb{Q}(t, \sqrt{k_1})$. □

If $g(t) \in \mathbb{Q}(t) \subseteq \mathbb{Q}(u)$, then $g(u) \in \mathbb{Q}(u)$ will denote the element $g(t(u))$, where $t(u)$ is the image of t in $\mathbb{Q}(u)$. We regard f as an element of $\mathbb{Q}[t]$.

The next two propositions summarize a method for producing twists of E over $\mathbb{Q}(u)$ with ranks (at least) 2 and 3.

Proposition 2.7. *Suppose $h \in \mathbb{Q}(t)$ is such that $f \circ h = kfj^2$ with $j \in \mathbb{Q}(t)$, $k \in \mathbb{Q}[t]$, and k squarefree. If $\deg k = 1$, then the function field $\mathbb{Q}(t, \sqrt{k(t)}) = \mathbb{Q}(u)$ with $u = \sqrt{k(t)}$, and we have $\deg f(u) = 6$ and $\operatorname{rank} E_{f(u)}(\mathbb{Q}(u)) \ge 2$. If $\deg k = 2$ and the curve $s^2 = k(t)$ has a rational point, then $\mathbb{Q}(t, \sqrt{k}) = \mathbb{Q}(u)$ for some u, and $\operatorname{rank} E_{f(u)}(\mathbb{Q}(u)) \ge 2$.*

Proof. This follows directly from Corollary 2.2 (with $g_1 = f$ and $g_2 = f \circ h$), Lemma 2.3, and Corollary 2.6. □

Proposition 2.8. *Suppose $h_1, h_2 \in \mathbb{Q}(t)$ are such that $f \circ h_i = k_i f j_i^2$ for $i = 1, 2$, with $j_i \in \mathbb{Q}(t)$, $k_i \in \mathbb{Q}[t]$, and k_i linear and $\mathbb{Q}$-linearly independent. If the curve $s^2 = k_1(t), r^2 = k_2(t)$ has a rational point, then the function field $\mathbb{Q}(t, \sqrt{k_1}, \sqrt{k_2}) = \mathbb{Q}(u)$ for some u, and $\operatorname{rank} E_{f(u)}(\mathbb{Q}(u)) \ge 3$.*

Proof. This follows directly from Corollary 2.2, Lemma 2.3, and Corollary 2.6. □

To apply Propositions 2.7 or 2.8, we want to find elements $h \in \mathbb{Q}(t)$ such that $f \circ h = kfj^2$ with $j \in \mathbb{Q}(t)$, $k \in \mathbb{Q}[t]$, and k linear. The following two propositions give two possible ways of doing this.

Proposition 2.9. *Suppose*

$$h(t) = \frac{\alpha t + \beta}{t + \delta} \in \mathbb{Q}(t)$$

is a linear fractional transformation which permutes the roots of f. Then

$$f(h(t)) = f(\alpha)(t+\delta) f(t) (t+\delta)^{-4}.$$

Proof. Both sides have the same divisor, and evaluate to $f(\alpha)$ at $t = \infty$. □

Remark 2.10. Suppose $\tilde{E}$ is an elliptic curve $Y^2 = \tilde{f}(X)$ with $\tilde{f}$ a monic cubic, and suppose $\varphi : \tilde{E} \to E$ is an isogeny. Then $\varphi(X,Y) = (\varphi_x(X), Y\varphi_y(X))$ with $\varphi_x, \varphi_y \in \mathbb{Q}(t)$, since the x-coordinate of φ is an even function on $\tilde{E}$ and the y-coordinate is an odd function.

Proposition 2.11. *Suppose $\tilde{E}$ is an elliptic curve $Y^2 = \tilde{f}(X)$ with $\tilde{f}$ a monic cubic, and suppose $\varphi : \tilde{E} \to E$ is an isogeny. Let φ_x and φ_y be as in Remark* 2.10. *If*

$$\mu(t) = \frac{\alpha t + \beta}{t + \delta} \in \mathbb{Q}(t)$$

is a linear fractional transformation which sends the roots of f to the roots of g, and if $h(t) = \varphi_x(\mu(t))$, then

$$f(h(t)) = \tilde{f}(\alpha)(t+\delta) f(t) \Big(\frac{\varphi_y(\mu(t))}{(t+\delta)^2} \Big)^2.$$

Proof. By Remark 2.10, $f(\varphi_x(X)) = Y^2 \varphi_y(X)^2 = \tilde{f}(X)\varphi_y(X)^2$. As in the proof of Proposition 2.9,

$$\tilde{f}(\mu(t)) = \tilde{f}(\alpha)(t+\delta) f(t) (t+\delta)^{-4}$$

and the identity of the proposition follows. □

Remark 2.12. Suppose $g(u) \in \mathbb{Q}[u]$ is squarefree and nonconstant, and let C be the curve $s^2 = g(u)$. Then

$$\operatorname{rank} E_g(\mathbb{Q}(u)) = \operatorname{rank} \operatorname{Hom}_{\mathbb{Q}}(\operatorname{Jac}(C), E) \le \operatorname{genus} C;$$

see [Stewart and Top 1995, § 4].

3. RANK 2

The following statement is a reformulation of a result of Howe, Leprévost, and Poonen in a special

case. The proof below is different from theirs, and uses the method described in the preceding sections.

Theorem 3.1 [Howe et al. 2000, Proposition 4]. *Suppose that either*

(a) $E[2]$ *has a nontrivial Galois-equivariant automorphism and* $\mathrm{End}_{\mathbb{C}}(E) \neq \mathbb{Z}[i]$, *or*
(b) E *has a rational subgroup of odd prime order* p *and* $\mathrm{End}_{\mathbb{C}}(E) \not\supset \mathbb{Z}[\sqrt{-p}]$.

Then there is a squarefree polynomial $g(u)$ *of degree* 6 *such that the twist* E_g *has rank two over* $\mathbb{Q}(u)$.

Proof. Suppose first that we are in case (a). Let $h(t)$ be the linear fractional transformation which (after identifying the roots of $f(x)$ with the nonzero elements of $E[2]$) agrees with the given automorphism of $E[2]$ on the roots of f. It follows from the Galois-equivariance of the automorphism that $h \in \mathbb{Q}(t)$. If $h(t) = \alpha t + \beta$, then (since $h(t) \neq t$) we must have $\alpha = -1$, and then the set of roots of f must be of the form $\{\frac{\beta}{2} - a, \frac{\beta}{2}, \frac{\beta}{2} + a\}$ for some nonzero a. But this contradicts the fact that $\mathrm{End}_{\mathbb{C}}(E) \neq \mathbb{Z}[i]$, so h cannot be a linear polynomial. Hence in this case the theorem follows from Propositions 2.9 and 2.7 and Remark 2.12.

Now suppose we are in case (b). Let $\tilde{E}$ be the quotient of E by the given rational subgroup. Then $\tilde{E}$ is an elliptic curve defined over $\mathbb{Q}$ by a Weierstrass model $y^2 = \tilde{f}(x)$, and there is an isogeny $\varphi : \tilde{E} \to E$ of degree p, also defined over $\mathbb{Q}$. Let $h(t) = \varphi_x(\mu(t))$ where φ_x is the x-coordinate of the isogeny φ (as in Remark 2.10) and μ is the the linear fractional transformation which maps the roots of f to the roots of $\tilde{f}$ in the same way as the dual isogeny $\hat{\varphi}$ maps $E[2]$ to $\tilde{E}[2]$. Since $\hat{\varphi}$ is defined over $\mathbb{Q}$, $\mu \in \mathbb{Q}(t)$. If $\mu(t) = \alpha t + \beta$, then after replacing $\tilde{f}(x)$ by $\tilde{f}(x + \beta)$ we may assume that $\beta = 0$. Then multiplication by α sends the roots of f to the roots of $\tilde{f}$, so $\tilde{E}$ is the twist of E by α. Let $\iota : E \to \tilde{E}$ be an isomorphism over $\mathbb{C}$. Then $\varphi \circ \iota \in \mathrm{End}_{\mathbb{C}}(E)$ and $(\varphi \circ \iota)^2 = -p$. This is impossible since we assumed that $\sqrt{-p} \notin \mathrm{End}_{\mathbb{C}}(E)$, so μ cannot be a linear polynomial. Now the theorem follows in this case from Propositions 2.11 and 2.7 and Remark 2.12. □

Remark 3.2. If E has a rational point of order 2 and $j(E) \neq 1728$, then hypothesis (a) of Theorem 3.1 holds.

We illustrate Theorem 3.1 by using the method of Section 2 to construct some explicit families of examples. In Section 5 we will make use of the explicit forms of the polynomials g below.

If E is an elliptic curve over $\mathbb{Q}$ and $E(\mathbb{Q})$ has a point of order 2, we may assume by translating the x-coordinate that $(0,0)$ is a point of order 2, and hence E is of the form $y^2 = x^3 + ax^2 + bx$.

Corollary 3.3. *Suppose that* E *is* $y^2 = x^3 + ax^2 + bx$ *with* $a, b \in \mathbb{Q}$, $ab \neq 0$, $b^2 \neq 4a$. *Let*

$$g(u) = -ab(u^2 + b^2)(u^4 + 2b^2u^2 - a^2bu^2 + b^4).$$

Then $E_{g(u)}$ *is an elliptic curve over* $\mathbb{Q}(u)$ *of rank* 2, *with independent points of infinite order*

$$\left(-\frac{u^2 + b^2}{ab}, \frac{1}{a^2b^2}\right), \quad \left(-\frac{b(u^2 + b^2)}{au^2}, \frac{b}{a^2u^3}\right).$$

Proof. That these points belong to $E_g(\mathbb{Q}(u))$ can be checked directly. Since they are nonconstant, both points have infinite order. The automorphism of $\mathbb{Q}(u)$ which sends u to $-u$ fixes the first point and sends the second point to its inverse, so they are independent in $E_g(\mathbb{Q}(u))$. Since $\deg g = 6$, Remark 2.12 and Lemma 2.5 show that the rank cannot be greater than two. □

Remark 3.4. Corollary 3.3 was obtained through the method of Propositions 2.7 and 2.9 as follows. Set $h(t) = -bt/(at+b)$, the linear fractional transformation that switches the two nonzero roots of f. (This is where we use that f has a rational root; if not, h would not have rational coefficients.) By Propositions 2.7 and 2.9 we see that $E_{f(t)}$ has rank at least 2 over $\mathbb{Q}(t, \sqrt{-b(at+b)}) = \mathbb{Q}(u)$ where we can take $u = \sqrt{-b(at+b)}$. We then have $t = -(u^2+b^2)/(ab)$, and writing the curve $E_{f(t)}$ and the points $(t, 1)$, $(h(t), \sqrt{f(h(t))/f(t)})$ in terms of u we obtain the data in Corollary 3.3.

Suppose now that E has a $\mathbb{Q}$-rational subgroup of order 3. The x-coordinate of the two nonzero points in this subgroup is rational, and after translating we may assume that this x-coordinate is zero. With this normalization one computes that E has a model of the form

$$y^2 = x^3 + (b^2/4c)x^2 + bx + c$$

with $b, c \in \mathbb{Q}$, $c \neq 0$, $b^3 \neq 54c^2$, and conversely every curve defined by such an equation has a $\mathbb{Q}$-rational subgroup $\{O, (0, \sqrt{c}), (0, -\sqrt{c})\}$.

Corollary 3.5. *Suppose that E is $y^2 = x^3 + (b^2/4c)x^2 + bx + c$ with $b, c \in \mathbb{Q}$, $bc \neq 0$, $b^3 \neq 54c^2$. Let*

$$g(u) = -bc(2u^6 + (18c^2 - b^3)u^4 + (54c^4 + 2b^3c^2)u^2 + 54c^6 - b^3c^4).$$

Then $E_{g(u)}$ is an elliptic curve over $\mathbb{Q}(u)$ of rank 2, with independent points of infinite order

$$\left(-\frac{u^2 + 3c^2}{2bc}, \frac{1}{4b^2c^2}\right),$$
$$\left(\frac{cg(u) - b^4u^2(u^2 - c^2)^2}{4b^2cu^2(u^2 + 3c^2)^2}, \frac{cg(u) + 3b^4u^2(u^2 - c^2)^2}{8b^3cu^3(u^2 + 3c^2)^3}\right).$$

Proof. As with Corollary 3.3, the simplest proof is a direct calculation. □

Remark 3.6. Corollary 3.5 was obtained through the method of Propositions 2.7 and 2.11 as follows. The quotient of E by the subgroup of order 3 generated by $(0, \sqrt{c})$ is the curve $\tilde{E}$ given by $Y^2 = \tilde{f}(X)$ where

$$\tilde{f}(X) = X^3 - \frac{3b^2}{4c}X^2 - \frac{b(b^3 - 54c^2)}{6c^2}X - \frac{(b^3 - 54c^2)^2}{108c^3}.$$

Let $\varphi : \tilde{E} \to E$ be the isogeny given by

$$(\varphi_x(X), Y\varphi_y(X)),$$

where

$$\varphi_x = \frac{-27c^3x^3 + 27b^2c^2x^2 - (9b^4c - 486bc^3)x + b^6 - 108b^3c^2 + 2916c^4}{243c^3x^2},$$

$$\varphi_y = \frac{27c^3x^3 - (9b^4c - 486bc^3)x + 2b^6 - 216b^3c^2 + 5832c^4}{729c^3x^3}.$$

The linear fractional transformation $\mu(t)$ that sends the roots of f to the roots of $\tilde{f}$ in the same way that $\hat{\varphi}$ sends $E[2]$ to $\tilde{E}[2]$ is

$$\mu(t) = \frac{(b^3 - 54c^2)t}{6c(2bt + 3c)}.$$

As in Proposition 2.11 we take $h(t) = \varphi_x(\mu(t))$ and see that $E_{f(t)}$ has rank two over

$$\mathbb{Q}(t, \sqrt{-c(2bt + 3c)}) = \mathbb{Q}(u),$$

where we let $u = \sqrt{-c(2bt + 3c)}$. Then

$$t = -(u^2 + 3c^2)/(2bc),$$

and writing the curve $E_{f(t)}$ and the points $(t, 1)$, $(h(t), \sqrt{f(h(t))/f(t)})$ in terms of u we obtain the data of Corollary 3.5.

The following example is contained in [Mestre 1992, Théorème 1]. We include it here to show how it fits into the framework of this paper. This result includes the families in Corollaries 3.3 and 3.5 above. The advantages of those corollaries is that the polynomials $g(u)$ have smaller degree, which will lead to stronger results in Section 5.

Theorem 3.7 [Mestre 1992]. *Suppose that $E : y^2 = x^3 + ax + b$ is an elliptic curve over $\mathbb{Q}$ with $ab \neq 0$. Let*

$$g(u) = -ab(b^2(u^4 + u^2 + 1)^3 + a^3u^4(u^2 + 1)^2)(u^2 + 1).$$

Then $E_{g(u)}$ has rank at least 2 over $\mathbb{Q}(u)$.

Proof. Let $f(x) = x^3 + ax + b$,

$$h_1(t) = -\frac{b(t^3 - 1)}{a(t^2 - 1)}, \quad \text{and} \quad h_2(t) = -\frac{b(t^3 - 1)}{at(t^2 - 1)},$$

and apply Corollary 2.2 with $g_i = f \circ h_i$ and $u = \sqrt{t}$. □

4. RANK 3

Suppose for this section that $E(\mathbb{Q})$ contains 3 points of order 2, i.e., $f(x)$ has three rational roots. After translating and scaling (scaling corresponds to taking a quadratic twist, which is harmless for our purposes) we may assume that $f(x) = x(x - 1)(x - \lambda)$ with $\lambda \in \mathbb{Q} - \{0, 1\}$.

Suppose σ is a permutation of the roots $\{0, 1, \lambda\}$ of f. There is a unique linear fractional transformation $h_\sigma(t) \in \mathbb{Q}(t)$ which acts on $\{0, 1, \lambda\}$ as σ does. By Proposition 2.9, as long as $h_\sigma(t)$ is not linear there are $j_\sigma \in \mathbb{Q}(t)$ and $k_\sigma \in \mathbb{Q}[t]$ such that $f \circ h_\sigma = k_\sigma f j_\sigma^2$.

In order to use these h_σ in Proposition 2.8, we will need to find σ_1, σ_2 such that the curve defined by $r^2 = k_{\sigma_1}(t)$, $s^2 = k_{\sigma_2}(t)$ has a rational point.

Theorem 4.1. *Suppose that E is an elliptic curve of the form $y^2 = x(x - 1)(x - \lambda)$ where $\lambda = -2a^2$ with $a \in \mathbb{Q}^\times$. Let $g(u)$ be the polynomial of degree 12 in u given by*

$$g(u) = 2N(N - 2D^2)(N - 2\lambda D^2),$$

where $D = \lambda(2\lambda - 1)u^2 + 2 - \lambda$ and

$$N = \lambda^2(\lambda+1)(2\lambda-1)^2u^4 - 4\lambda^2(\lambda-1)(2\lambda-1)u^3 + 2\lambda(\lambda+1)(2\lambda^2-3\lambda+2)u^2 - 4\lambda(\lambda-1)(\lambda-2)u + (\lambda-2)^2(\lambda+1).$$

Then $E_{g(u)}$ has rank at least 3 over $\mathbb{Q}(u)$, with independent points

$$P_1 = \left(\frac{N}{2D^2}, \frac{1}{4D^3}\right),$$

$$P_2 = \left(\frac{\lambda^2(D^2 - 4\lambda u(u-1)(\lambda(2\lambda-1)u+2-\lambda))}{(\lambda(2\lambda-1)u^2 - 2\lambda(2\lambda-1)u + \lambda - 2)^2}, \frac{a\lambda}{(\lambda(2\lambda-1)u^2 - 2\lambda(2\lambda-1)u + \lambda - 2)^3}\right),$$

$$P_3 = \left(\frac{D^2 + 4\lambda u(u-1)(\lambda(2\lambda-1)u+2-\lambda)}{\lambda(\lambda(2\lambda-1)u^2 - (2\lambda-4)u + \lambda - 2)^2}, -\frac{a}{\lambda^2(\lambda(2\lambda-1)u^2 - (2\lambda-4)u + \lambda - 2)^3}\right).$$

Proof. Take σ_1 to be the permutation of $\{0,1,\lambda\}$ which switches 0 and 1, and σ_2 to be the permutation which switches 0 and λ. Then the linear fractional transformations

$$h_1(t) = \frac{\lambda^2 t - \lambda^2}{(2\lambda-1)t - \lambda^2}, \qquad h_2(t) = \frac{-t+\lambda}{(\lambda-2)t+1}$$

act on $\{0,1,\lambda\}$ as σ_1 and σ_2 do, respectively. One computes in Propositions 2.9 that $f \circ h_1 = k_1 f j_1^2$ and $f \circ h_2 = k_2 f j_2^2$ where

$$k_1(t) = (1-\lambda)((\lambda-2)t+1),$$
$$k_2(t) = \lambda(1-\lambda)((2\lambda-1)t - \lambda^2).$$

If $a \neq 0$, then k_1 and k_2 are $\mathbb{Q}$-linearly independent. Setting $t_0 = (\lambda+1)/2$, and using that $\lambda = -2a^2$, one obtains

$$k_1(t_0) = k_2(t_0) = a^2(\lambda-1)^2.$$

These formulas give us a rational point on the curve of genus zero defined by $r^2 = k_1(t), s^2 = k_2(t)$. Using this point one computes that $\mathbb{Q}(t, \sqrt{k_1(t)}, \sqrt{k_2(t)}) = \mathbb{Q}(u)$, where

$$u = \frac{\sqrt{k_2(t)} - a(\lambda-1)}{\sqrt{k_1(t)} - a(\lambda-1)},$$

and then $t = N/2D^2$ (where N, D are defined in terms of λ, u in the statement of the theorem). Thus, if $g(u)$ is as in the statement of the theorem, we obtain $f(t) = g(u)/(4D^3)^2$ and the theorem follows from Proposition 2.8. The 3 points of infinite order are computed by taking points with x-coordinates t, $h_1(t)$, and $h_2(t)$, and expressing t in terms of u. □

Theorem 4.2. *Let E be given by $y^2 = x(x-1)(x-\lambda)$, where either*

(a) $\lambda = (1-a^2)/(a^2+2)$ *with* $a \in \mathbb{Q} - \{0, \pm 1\}$, *or*
(b) $\lambda = a(a-2)/(a^2+1)$ *with* $a \in \mathbb{Q} - \{0, 2\}$.

Then there is a squarefree polynomial $g(u) \in \mathbb{Q}[u]$ of degree 12 in u, which factors into a product of three quartic polynomials, such that $E_{g(u)}$ has rank at least 3 over $\mathbb{Q}(u)$. (See the electronic files associated with this paper for the polynomials $g(u)$ and independent points of infinite order.)

Proof. Take σ_1 to be the permutation of $\{0,1,\lambda\}$ which switches 0 and 1, σ_2 to be the permutation which switches 1 and λ, and σ_3 to be the cyclic permutation $0 \mapsto \lambda \mapsto 1 \mapsto 0$. Let $h_i \in \mathbb{Q}(t)$ be the corresponding linear fractional transformation. Then in Propositions 2.9 we have $f \circ h_i = k_i f j_i^2$ where

$$k_1(t) = (1-\lambda)((\lambda-2)t+1),$$
$$k_2(t) = (1-\lambda)\lambda((\lambda^2-\lambda+1)t - \lambda),$$
$$k_3(t) = \lambda((\lambda+1)t - \lambda).$$

Now suppose $\lambda = (1-a^2)/(a^2+2)$ with $a \in \mathbb{Q} - \{0, \pm 1\}$. Then k_1 and k_2 are $\mathbb{Q}$-linearly independent, and setting $t_0 = 2\lambda/(\lambda+1)$ we find

$$k_1(t_0) = a^2(\lambda-1)^2, \quad k_2(t_0) = a^2\lambda^2(\lambda-1)^2.$$

These formulas give us a rational point on the curve $r^2 = k_1(t), s^2 = k_2(t)$.

If $\lambda = a(a-2)/(a^2+1)$ with $a \in \mathbb{Q} - \{0, 2\}$, then k_2 and k_3 are $\mathbb{Q}$-linearly independent, and setting $t_0 = 1/\lambda$ we find

$$k_2(t_0) = (\lambda-1)^2, \quad k_3(t_0) = \left(\frac{a^2+a-1}{a^2+1}\right)^2.$$

These formulas give us a rational point on the curve $r^2 = k_2(t), s^2 = k_3(t)$.

The theorem now follows from Proposition 2.8. □

The next example applies to essentially the same curves as [Mestre 1998, Théorème 2].

Theorem 4.3. *Suppose $E[2] \subseteq E(\mathbb{Q})$ and E has a rational cyclic subgroup of order 4. Then E has a model*

$$y^2 = x(x-b)(x-a^2b)$$

where $a, b \in \mathbb{Q}^\times$ and $a \neq 1$. Let $g(u)$ be the polynomial of degree 11 given by

$$\begin{aligned} g(u) = -4bu\big((a-1)^2u - a\big) \\ \times \big(a^2(a^2-3a+4)u - (a^2+1)(a-1)\big) \\ \times \big(a(a^2-3a+4)u^2 - 2a(a-1)u + a + 1\big) \\ \times \big(a(a+1)(a-1)^2(a^2-3a+4)u^2 \\ - 2a(a-1)^2(a^2+1)u + (a^2+1)^2\big) \\ \times \big(a^2(a-1)^2(a^2-3a+4)^2u^4 \\ - 4a^2(a-1)^3(a^2-3a+4)u^3 \\ + 2(a-1)^2(3a^4-6a^3+5a^2+2)u^2 \\ - 4a(a-1)^2(a^2+1)u + (a^2+1)^2\big). \end{aligned}$$

Then $E_{g(u)}$ has rank at least 3 over $\mathbb{Q}(u)$. (See the associated electronic files for 3 independent points of infinite order.)

Proof. We may write E as $y^2 = f(x)$, where f has 3 rational roots. If C_4 denotes the rational cyclic subgroup of order 4, then $2C_4$ contains a rational point, and we may choose our model so that this point is $(0,0)$. Denote the other roots of f by b and $b\lambda$. If Q is a generator of C_4 and $x(Q)$ is its x-coordinate, then $x(Q) \in \mathbb{Q}$ and a computation gives $x(Q)^2 = \lambda b^2$. Hence λ is a square, and we write $\lambda = a^2$ with $a \in \mathbb{Q}^\times$. Thus E is given by $y^2 = f(x) := x(x-b)(x-a^2b)$.

The quotient of E by the group generated by $(0,0)$ is

$$\tilde{E} : Y^2 = \tilde{f}(X) := X(X+(a-1)^2b)(X+(a+1)^2b).$$

The isogeny from $\tilde{E}$ to E is

$$\varphi(X,Y) = (\varphi_x(X), Y\varphi_y(X)),$$

where

$$\varphi_x(X) = \frac{(X+(a-1)^2b)(X+(a+1)^2b)}{4X},$$

$$\varphi_y(X) = \frac{X^2-(a^2-1)^2b^2}{8X^2}.$$

The linear fractional transformation

$$\mu(t) = \frac{a(a+1)(a-1)^2b(t-b)}{-(a^2-3a+4)t + a(a+1)b}$$

sends the roots of f to the roots of $\tilde{f}$. Set $h_1(t) = \varphi_x(\mu(t)) \in \mathbb{Q}(t)$.

Let σ be the permutation of $\{0, b, a^2b\}$ that interchanges b and a^2b, and let $h_2 \in \mathbb{Q}(t)$ be the corresponding linear fractional transformation. One computes in Propositions 2.11 and 2.9 that $f \circ h_1 = k_1 f j_1^2$ and $f \circ h_2 = k_2 f j_2^2$ where

$$k_1(t) = (a-1)ab((a^2-3a+4)t - a(a+1)b),$$
$$k_2(t) = b((a^2+1)t - a^2b).$$

Setting $t_0 = a^2b$ we find

$$k_1(t_0) = (a-1)^4a^2b^2, \quad k_2(t_0) = a^4b^2.$$

These formulas give us a rational point on the curve defined by $r^2 = k_1(t), s^2 = k_2(t)$. Using this point one computes that

$$\mathbb{Q}(t, \sqrt{k(t)}, \sqrt{k_\sigma(t)}) = \mathbb{Q}(u),$$

where

$$u = \frac{\sqrt{k_1(t)} - (a-1)^2ab}{\sqrt{k_2(t)} - a^2b}.$$

We can solve for t in terms of u (see the associated electronic files). The theorem then follows from Proposition 2.8. □

Remark 4.4. The theorems above give certain infinite families of curves which have twists of rank (at least) 3 over $\mathbb{Q}(u)$. The restriction to these families makes it possible to find rational points on the genus zero curves $r^2 = k_1(t), s^2 = k_2(t)$ which arise in the construction. It is possible to carry out the construction for many curves not in these families. We give one example in the next theorem.

Theorem 4.5. *The elliptic curve*

$$6(u^{12} - 33u^8 - 33u^4 + 1)y^2 = x^3 - x$$

has rank at least 3 over $\mathbb{Q}(u)$, with independent points

$$P_1 = \left(-\frac{u^4-6u^2+1}{3(u^2+1)^2}, \frac{2}{9(u^2+1)^3}\right),$$

$$P_2 = \left(-\frac{u^4+6u^2+1}{3(u^2-1)^2}, \frac{2}{9(u^2-1)^3}\right),$$

$$P_3 = \left(\frac{u^4+1}{6u^2}, \frac{1}{36u^3}\right).$$

Proof. The simplest proof is a direct computation. To construct this example one takes E to be $y^2 = x^3 - x$ and proceeds exactly as in the proofs of Theorems 4.1 and 4.2, with $h_1(t) = (t+1)/(3t-1)$ and $h_2(t) = (-t+1)/(3t+1)$, which gives

$$k_1(t) = -6t + 2, \quad k_2(t) = 6t + 2.$$

The curve defined by $r^2 = k_1(t), s^2 = k_2(t)$ has a rational point $(r, s, t) = (2, 0, -\frac{1}{3})$, and using this one computes that

$$\mathbb{Q}(t, \sqrt{k_1}, \sqrt{k_2}) = \mathbb{Q}(u),$$

where

$$t = -\frac{u^4 - 6u^2 + 1}{3(u^2+1)^2}.$$

Proposition 2.8 with this input leads to the data above. □

Remark 4.6. Let $g(u) = 6(u^3 - 33u^2 - 33u + 1)$. Over $\mathbb{Q}(u)$, the rank of E_g is 1, that of $E_{g(u^2)}$ is 2, and that of $E_{g(u^4)}$ is 3. Unfortunately this pattern does not continue; the rank of $E_{g(u^8)}$ is 3. Replacing u by $\sqrt{u}$ in P_1 and P_2 above gives two independent points on $E_{g(u^2)}$.

5. DENSITIES

Recall the definitions of $r_E(D)$ and

$$N_r(E, x) \geq N_r^+(E, x)$$

from the introduction. In this section we use results of Stewart and Top [1995] to obtain lower bounds for $N_r(E, x)$ (and, subject to the Parity Conjecture, for $N_r^+(E, x)$, as in [Gouvêa and Mazur 1991]), with E and r provided by the examples of the previous sections. The first two assertions of the following theorem are immediate from [Stewart and Top 1995, Theorems 2 and 1], and were used in that paper in several families of examples. What is new here is that by using the examples of the previous sections we have more curves to which we can apply these results. In addition, we show in Theorem 5.1(iii) how to use [Stewart and Top 1995, Theorem 1] along with the Parity Conjecture to obtain results for higher rank. See also [Gouvêa and Mazur 1991; Stewart and Top 1995, § 12].

If A is an elliptic curve over $\mathbb{Q}$, let $w(A) \in \{\pm 1\}$ denote the root number in the functional equation of the L-function $L(A, s)$. The Parity Conjecture asserts that $w(A) = (-1)^{\operatorname{rank} A(\mathbb{Q})}$.

Theorem 5.1. *Suppose that E is an elliptic curve over $\mathbb{Q}$, and $g \in \mathbb{Q}[u]$ is nonconstant and squarefree. Let $r = \operatorname{rank} E_g(\mathbb{Q}(u))$ and $k = \left[\frac{1}{2}(\deg g + 1)\right]$.*

(i) *For $x \gg 1$,*

$$N_r(E, x) \gg x^{1/k} / \log^2(x).$$

Suppose further that the irreducible factors of g all have degree at most 6.

(ii) *For $x \gg 1$,*

$$N_r(E, x) \gg x^{1/k}.$$

(iii) *Suppose that the Parity Conjecture holds for all twists of E, and that there is a rational number c such that $g(c) \neq 0$ and $w(E_{g(c)}) = (-1)^{r+1}$. Then for $x \gg 1$,*

$$N_{r+1}^+(E, x) \gg x^{1/k}.$$

Proof. Without loss of generality we may assume that $\deg g \geq 3$, since if not, $r = 0$ by Remark 2.12 and there is nothing to prove.

Let $F(X, Y) = Y^{2k} g(X/Y)$, a homogeneous polynomial of degree $2k$. Assertions (i) and (ii) are immediate from Theorems 2 and 1 of [Stewart and Top 1995], respectively, applied to F.

Suppose now that the Parity Conjecture holds, the irreducible factors of g all have degree at most 6, and $c \in \mathbb{Q}$ is such that $g(c) \neq 0$ and $w(E_{g(c)}) = (-1)^{r+1}$. Choose a closed interval $I \subset \mathbb{R}$ with rational endpoints that contains c but no roots of g, and let $\mu(u) = (\alpha u + \beta)/(\gamma u + \delta) \in \mathbb{Q}(u)$ be a linear fractional transformation which maps $[0, \infty]$ onto I and (for simplicity) such that $\mu(1) = c$. Replace g by the polynomial $(\gamma u + \delta)^{2k}(g \circ \mu)$ of degree at most $2k$. Then we still have that $r = \operatorname{rank} E_g(\mathbb{Q}(u))$, and our construction guarantees that this new polynomial g also satisfies:

(a) the constant term of g and the coefficient of u^{2k} are both nonzero,
(b) the irreducible factors of g have degree at most 6,
(c) $g(1) \neq 0$ and $w(E_{g(1)}) = (-1)^{r+1}$,
(d) $g(u)/g(1)$ is positive if $u \geq 0$.

Further, multiply g by the square of an integer to clear denominators of the coefficients. If A is an elliptic curve over $\mathbb{Q}$, write $\operatorname{cond}(A)$ for its conductor. If further $D \in \mathbb{Q}^\times$ and $\operatorname{cond}(A)$ is relatively prime to the conductor of the character χ_D associated to the quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$, then $w(A_D) = \chi_D(-\operatorname{cond}(A))w(A)$. Applying this with $A = E_{g(1)}$ and $D = g(a/b)/g(1)$ for a and b positive integers congruent to 1 modulo an integer M sufficiently divisible by the prime divisors of $2\operatorname{cond}(E_{g(1)})$, and using (c) and (d) above, gives that

$$w(E_{g(a/b)}) = w(E_{g(1)}) = (-1)^{r+1}. \qquad (5\text{–}1)$$

Let S be the set of squarefree integers D such that $D = F(a,b)/v^2$ for some $a, b, v \in \mathbb{Z}^+$ with $a, b \le x$, $a \equiv b \equiv 1 \bmod M$; then define

$$S(x) = \{D \in S : |D| < x\}.$$

By [Stewart and Top 1995, Theorem 1], for $x \gg 1$,

$$\#(S(x)) \gg x^{1/k}. \tag{5–2}$$

(Note that as stated, the theorem cited does not include the restriction $a, b > 0$ present in our definition of $S(x)$. However, the proof given there does restrict to positive a, b.)

It follows from [Silverman 1983, Theorem C] that $r_E(D) \ge r$ for all but finitely many $D \in S$. However, by (5–1), if $D \in S$ then $w(E_D) = (-1)^{r+1}$ so the Parity Conjecture tells us that $r_E(D) \ne r$. Hence $r_E(D) \ge r+1$ for all but finitely many $D \in S$, and so assertion (iii) of the theorem follows from the Stewart–Top bound (5–2). □

Corollary 5.2. *Suppose that E is an elliptic curve over $\mathbb{Q}$, and $g \in \mathbb{Q}[u]$ is a nonconstant squarefree polynomial whose irreducible factors have degree at most 6. Let $r = \operatorname{rank} E_g(\mathbb{Q}(u))$ and $k = \left[\frac{1}{2}(\deg g + 1)\right]$. If the Parity Conjecture holds for all twists of E, and g has at least one real root, then for $x \gg 1$,*

$$N^+_{r+1}(E, x) \gg x^{1/k}.$$

Proof. If g has a real root then $g(\mathbb{Q})$ contains both positive and negative values (g has no multiple roots because it was assumed to be squarefree). Thus by a result of Rohrlich [1993, Theorem 2] we have

$$\{w(E_{g(a)}) : a \in \mathbb{Q},\ g(a) \ne 0\} = \{1, -1\}.$$

Now the corollary follows immediately from Theorem 5.1(iii). □

We now give some applications of Theorem 5.1 and Corollary 5.2.

Theorem 5.3. *Suppose that either*

(a) *$E[2]$ has a nontrivial Galois-equivariant automorphism and $\operatorname{End}_{\mathbb{C}}(E) \ne \mathbb{Z}[i]$, or*
(b) *E has a rational subgroup of odd prime order p and $\operatorname{End}_{\mathbb{C}}(E) \not\supset \mathbb{Z}[\sqrt{-p}]$.*

Then for $x \gg 1$,

$$N_2(E, x) \gg x^{1/3}.$$

Proof. This is immediate from Theorems 3.1 and 5.1(ii). □

Theorem 5.4. *Suppose that $E[2] \subset E(\mathbb{R})$ and either*

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

If the Parity Conjecture holds for all twists of E then for $x \gg 1$,

$$N_3^+(E, x) \gg x^{1/3}.$$

Proof. Suppose first that we are in case (a). Translating the given rational root of f we may assume that $f(x) = x^3 + ax^2 + bx$ with $b > 0$. Since f has 3 real roots we also have $a^2 - 2b > a^2 - 4b > 0$. In particular, $b(a^2 - 2b) > 0$. Let $g(u)$ be as in Corollary 3.3. Then g is divisible by $g_1(u) = u^4 - b(a^2-2b)u^2 + b^4$. We compute that

$$g_1\big(\sqrt{b(a^2-2b)}\big) = -\tfrac{1}{4}a^2b^2(a^2-4b) < 0,$$

but $g_1(u)$ is positive for large u, so g_1, and hence g, has real roots. Hence the Corollary in this case follows from Corollaries 5.2 and 3.3.

Similarly, suppose we are in case (b). Then as discussed before Corollary 3.5, E has a model $y^2 = x^3 + (b^2/4c)x^2 + bx + c$ with $b, c \in \mathbb{Q}$, $c \ne 0$. The discriminant of this model is $\Delta(E) = 8(b^3 - 54c^2)$. Since all the 2-torsion on E is defined over $\mathbb{R}$, we have $\Delta(E) > 0$. Let $g(u)$ be as in Corollary 3.5. Then $g(u)/(-bc)$ is positive for large u, but $g(0)/(-bc) = -c^4(b^3 - 54c^2) = -\frac{1}{8}c^4\Delta(E) < 0$. Hence g has real roots, so the Corollary in this case follows from Corollaries 5.2 and 3.5. □

Theorem 5.5. *Suppose E is defined by*

$$y^2 = x(x-1)(x-\lambda)$$

where either $\lambda = -2a^2$, or $\lambda = (1-a^2)/(a^2+2)$, or $\lambda = a(a-2)/(a^2+1)$, with $a \in \mathbb{Q}$ and $\lambda \ne 0$. Then for $x \gg 1$,

$$N_3(x) \gg x^{1/6}.$$

Proof. This is immediate from Theorems 5.1(ii), 4.1, 4.2, and 4.5 (the last to handle the excluded value $a = 0$ in Theorem 4.2(a)). □

Theorem 5.6. *Suppose $E[2] \subseteq E(\mathbb{Q})$ and E has a rational cyclic subgroup of order 4. Then:*

(i) *for $x \gg 1$,*

$$N_3(x) \gg x^{1/6},$$

(ii) *if the Parity Conjecture holds for all twists of* E, *then for* $x \gg 1$,

$$N_4^+(x) \gg x^{1/6}.$$

Proof. Assertion (i) follows directly from Theorems 5.1(ii) and 4.3. The polynomial g of Theorem 4.3 has degree 11, and hence it has a real root, so (ii) follows from Corollary 5.2 and Theorem 4.3. □

Remark 5.7. The conclusions of Theorems 5.3, 5.4, 5.5, and 5.6 hold when E is $y^2 = x^3 - x$, by Remark 4.6, Theorem 5.1, and Corollary 5.2.

6. REMARKS AND QUESTIONS

Problem 6.1. Find a hyperelliptic curve C of the form $s^2 = g(u)$ with $g(u) \in \mathbb{Q}[u]$ such that the jacobian of C is isogenous over $\mathbb{Q}$ to $E^r \times B$ for some elliptic curve E and abelian variety B, either with $r \geq 4$, or with both $r = 3$ and $\dim B \leq 1$.

Remark 6.2. A solution (C, E, r, B) to Problem 6.1 would imply, by Theorem 5.1(i) and the equality in Remark 2.12, that

$$N_r(E, x) \gg \frac{x^{1/(1+\text{genus } C)}}{\log^2(x)} = \frac{x^{1/(1+r+\dim B)}}{\log^2(x)}.$$

Remark 6.3. The reason for the restriction on r in Problem 6.1 is that we already have examples when $r \leq 3$. Theorem 3.1 gives numerous examples with $r = 2$ and $\dim B = 0$, and Theorems 4.1, 4.2, 4.3, and 4.5 provide numerous examples with $r = 3$ and $\dim B = 2$.

Remark 6.4. The results of Stewart and Top [1995] would not be needed in the arguments of Section 5 if the following conjecture of Caporaso, Harris, and Mazur were known to hold. More precisely, Proposition 6.6 shows that (5–2) above follows easily from this conjecture.

Conjecture 6.5 [Caporaso et al. 1995]. *Fix an integer* $h \geq 2$. *Then there is a constant* $B(h)$ *such that for every curve* C *of genus* h *defined over* $\mathbb{Q}$, $\#(C(\mathbb{Q})) < B(h)$.

Proposition 6.6. *Suppose* $g(u) \in \mathbb{Z}[u]$ *is a squarefree polynomial, and let* $k = \left[\frac{1}{2}(\deg g + 1)\right]$ *and* $F(X, Y) = Y^{2k} g(X/Y)$. *Fix a positive integer* M *and define* $S(x)$ *as in the proof of Theorem* 5.1(iii), *with this* M. *If Conjecture* 6.5 *is true and* $k \geq 3$, *then for* $x \gg 1$,

$$\#(S(x)) \gg x^{1/k}.$$

Proof. If $a, b \in \mathbb{Z}$ and $F(a, b) \neq 0$, let $s(F(a, b))$ denote the squarefree part of $F(a, b)$, i.e., the unique squarefree integer D such that $F(a, b) = Dn^2$ for some integer n. For every squarefree integer D let A_D denote the hyperelliptic curve $Dv^2 = g(u)$ of genus $k - 1 \geq 2$. The map

$$(a, b) \mapsto (a/b, \pm b^{-k}\sqrt{F(a, b)/D})$$

defines an injection

$$\{(a, b) \in \mathbb{Z}^2 : (a, b) = 1,\ s(F(a, b)) = D\} \hookrightarrow A_D(\mathbb{Q})/\{\pm 1\}$$

(where -1 denotes the hyperelliptic involution on A_D). Thus by Conjecture 6.5 the order of the set on the left is bounded by $B(k - 1)$. Let

$$R(x) = \{(a, b) \in \mathbb{Z}^2 : 1 \leq a, b \leq x,\ (a, b) = 1, F(a, b) \neq 0,\ a \equiv b \equiv 1 \bmod M\}.$$

There is a constant $K = K(g)$ such that $|F(a, b)| < Kx^{2k}$ if $(a, b) \in R(x)$. It follows that

$$\#(S(x)) \geq \frac{\#(R((x/K)^{1/2k}))}{B(k - 1)}$$

for $x \gg 1$. But showing that $\#(R(x)) \gg x^2/M^2$ for $x \gg 1$ is standard; the proposition follows. □

ACKNOWLEDGEMENTS

We would like to thank Jean-François Mestre for pointing out that the curves with $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z})$-torsion are isogenous to twists of the curves in Theorem 6 of [Stewart and Top 1995], and Brian Conrey for telling us about connections between rank heuristics coming from Random Matrix Theory and Theorems 5.3 and 5.4.

ELECTRONIC AVAILABILITY

Two useful electronic files are companions to this article and can be found at http://www.expmath.org/extra/10.4 and at http://www.math.ohio-state.edu/~silver/bibliography/. One contains several of the formulas in the paper (including those omitted from the statements of Theorems 4.2 and 4.3) in a form suitable for input into PARI. Another contains the

same information in the form of a Mathematica notebook.

REFERENCES

[Caporaso et al. 1995] L. Caporaso, J. Harris, and B. Mazur, "How many rational points can a curve have?", pp. 13–31 in *The moduli space of curves* (Texel Island, 1994), edited by R. Dijkgraaf et al., Prog. Math. **129**, Birkhäuser, Boston, 1995.

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

[Howe et al. 2000] E. W. Howe, F. Leprévost, and B. Poonen, "Large torsion subgroups of split Jacobians of curves of genus two or three", *Forum Math.* **12**:3 (2000), 315–364.

[Mestre 1992] J.-F. Mestre, "Rang de courbes elliptiques d'invariant donné", *C. R. Acad. Sci. Paris Sér. I Math.* **314**:12 (1992), 919–922.

[Mestre 1998] J.-F. Mestre, "Rang de certaines familles de courbes elliptiques d'invariant donné", *C. R. Acad. Sci. Paris Sér. I Math.* **327**:8 (1998), 763–764.

[Rohrlich 1993] D. E. Rohrlich, "Variation of the root number in families of elliptic curves", *Compositio Math.* **87**:2 (1993), 119–151.

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

[Stewart and Top 1995] C. L. Stewart and J. Top, "On ranks of twists of elliptic curves and power-free values of binary forms", *J. Amer. Math. Soc.* **8**:4 (1995), 943–973.

Karl Rubin, Department of Mathematics, Stanford University, Stanford, CA 94305, United States (rubin@math.stanford.edu)

Alice Silverberg, Department of Mathematics, Ohio State University, Columbus, Ohio 43210, United States (silver@math.ohio-state.edu)

Received November 30, 2000; accepted May 15, 2001