MATHEMATICS OF COMPUTATION
Volume 88, Number 316, March 2019, Pages 837–846
http://dx.doi.org/10.1090/mcom/3348
Article electronically published on May 17, 2018

THE ELKIES CURVE HAS RANK 28 SUBJECT ONLY TO GRH

ZEV KLAGSBRUN, TRAVIS SHERMAN, AND JAMES WEIGANDT

Abstract. In 2006, Elkies presented an elliptic curve with 28 independent rational points. We prove that subject to GRH, this curve has Mordell-Weil rank equal to 28. We prove a similar result for a previously unpublished curve of Elkies having rank 27 as well.

Our work complements work of Bober and Booker and Dwyer that can be used to obtain these same results subject to both GRH and the BSD conjecture. This provides new evidence that the rank portion of the BSD conjecture holds for elliptic curves over $\mathbb{Q}$ of very high rank.

Our results about Mordell-Weil ranks are proven by computing the 2-ranks of class groups of cubic fields associated to these elliptic curves. As a consequence, we also succeed in proving that, subject to GRH, the class group of a particular cubic field has 2-rank equal to 22 and that the class group of a particular totally real cubic field has 2-rank equal to 20.

1. Introduction

The celebrated Mordell-Weil theorem asserts that the group $E(\mathbb{Q})$ of rational points on an elliptic curve E defined over $\mathbb{Q}$ is finitely generated. It remains unknown, however, whether the ranks of elliptic curves over $\mathbb{Q}$ are uniformly bounded. As of this writing, the elliptic curve defined over $\mathbb{Q}$ with the largest number of known independent points is the curve E_{28},

$$y^2+xy+y=x^3-x^2-2006776241557552658503320820933854275093023031217895650 2x + 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9, \tag{1}$$

discovered by Elkies [11] which has at least 28 independent rational points. Our main result is the following.

Theorem 1. *Assuming the Generalized Riemann Hypothesis (GRH), $E_{28}(\mathbb{Q})$ has rank 28.*

Building on work of Mestre [14], Booker and Dwyer have previously proved that E_{28} has analytic rank at most 28, conditional on GRH for the L-function of E_{28} (see Remark 1.2 in [3]). It follows that E_{28} has rank 28 conditional on both GRH and the Birch and Swinnerton-Dyer conjecture (BSD).

In contrast, Theorem 1 is proved using the classical method of 2-descent. We show that GRH implies that the dimension of the 2-Selmer group $\mathrm{Sel}_2(E_{28}/\mathbb{Q})$ is exactly 28. This is a consequence of the following.

Theorem 2. *Let K_{28} be the cubic subfield of the 2-division field of E_{28}. Then:*

(i) *The 2-rank of the ideal class group $\mathrm{Cl}(K_{28})$ is at least 20.*

Received by the editor June 23, 2017, and, in revised form, November 6, 2017, and December 5, 2017.

2010 *Mathematics Subject Classification.* Primary 11-04, 11G05, 11Y40, 14G05, 14M52.

(ii) *If GRH holds, then the* 2*-rank of* $\mathrm{Cl}(K_{28})$ *is exactly* 20.

Part (i) is obtained by applying a result of Brumer and Kramer (see Proposition 2.1), together with the lower bound on the rank of $E_{28}(\mathbb{Q})$ coming from the independent points. Part (ii) is the result of a large class group computation described in Sections 3 and 4.

In addition to E_{28}, Elkies also shared with us the previously unpublished curve E_{27},

$$y^2 + xy = x^3 - 5567114686524440191611777302029661007975401550097 0x$$
$$+161981895322788558220906653027519611838007321625214218991719656790551905956,$$

which has rank at least 27. Using similar machinery as for E_{28}, we prove the following.

Theorem 3. *Assuming GRH,* $E_{27}(\mathbb{Q})$ *has rank 27.*

Theorem 3 is a consequence of the following.

Theorem 4. *Let* K_{27} *be the cubic subfield of the* 2*-division field of* E_{27}*.*

(i) *The* 2*-rank of the ideal class group* $\mathrm{Cl}(K_{27})$ *is at least* 22*.*

(ii) *If GRH holds, then the* 2*-rank of* $\mathrm{Cl}(K_{27})$ *is exactly* 22*.*

To our knowledge, the 2-rank of $\mathrm{Cl}(K_{27})$ is the largest known for a cubic field to have been proven under standard hypotheses. Similarly, the 2-rank of $\mathrm{Cl}(K_{28})$ is the largest known for a totally real cubic field proven under standard hypotheses.

Remark 1.1. A method similar to Booker and Dwyer's for bounding the analytic rank of an elliptic curve was independently developed by Bober [3]. The implementation of his method in **Sage** (due to Spicer) can be used to prove that the analytic rank of E_{27} is at most 27, conditional on GRH for the L-function of E_{27} [17].

Remark 1.2. Prior to the discovery of E_{28}, the record for largest known rank had successively been held by curves of ranks at least 20, 21, 22 ,23, and 24 [10]. Unlike previous record holding curves, the exact ranks of these curves had only been proven subject to both GRH and BSD [3]. We were able to use the methods described in this paper to confirm these curves did indeed have the suspected ranks, subject only to GRH. Since these computations were small enough to complete using the number field sieve machinery implemented in **magma** [4] under the `NFSProcess` command, we have omitted the details for the sake of brevity.

Remark 1.3. Whereas bounding the analytic rank of a curve using the methods of Bober and Booker and Dwyer requires assuming GRH for the L-function of a single elliptic curve, we use GRH as described in Section 3.2 to assert that $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$ is generated by primes below a particular bound. We therefore need to rely on GRH for the zeta functions of a large but finite number of unramified quadratic extensions of K.

1.1. **Data.** Our computations use a variant of Buchmann's algorithm which is similar to the number field sieve. As detailed in Section 3, this algorithm proceeds by collecting relations for $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$ supported on primes below a certain bound. We have made these relations available at `https://github.com/zevklagsbrun/ElkiesCurve` so that the enterprising reader can verify our results. In addition, the relations obtained for the curves referenced in Remark 1.2, the set of large primes

at which each curve has bad reduction (originally obtained by Dodson for the curve E_{28} [9]), and a list of 27 independent points on the curve E_{27} (provided by Elkies) are all available at the same url.

2. The 2-Selmer group

One of the most common methods for obtaining an upper bound on the Mordell-Weil rank of E is studying the 2-Selmer group $\mathrm{Sel}_2(E/\mathbb{Q})$ of E. We briefly recall the definition and some important properties here and refer the reader to Chapter X of [16] for more details.

If E is an elliptic curve defined over $\mathbb{Q}$, then $E(\mathbb{Q})/2E(\mathbb{Q})$ maps into $H^1(\mathbb{Q}, E[2])$ via the Kummer map δ. The following diagram commutes for every place v of $\mathbb{Q}$, where δ_v is the local Kummer map:

$$\begin{array}{ccc} E(\mathbb{Q})/2E(\mathbb{Q}) & \xrightarrow{\delta} & H^1(\mathbb{Q}, E[2]) \\ \downarrow & & \downarrow \mathrm{Res}_v \\ E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) & \xrightarrow{\delta_v} & H^1(\mathbb{Q}_v, E[2]). \end{array}$$

For each place v of $\mathbb{Q}$, let $H^1_f(\mathbb{Q}_v, E[2])$ denote the image of $E(\mathbb{Q}_v)/2E(\mathbb{Q}_v)$ in $H^1(\mathbb{Q}_v, E[2])$. The **2-Selmer group** of $E/\mathbb{Q}$, denoted $\mathrm{Sel}_2(E/\mathbb{Q})$, is then defined as

$$\mathrm{Sel}_2(E/\mathbb{Q}) = \left\{ c \in H^1(\mathbb{Q}, E[2]) : \mathrm{Res}_v(c) \in H^1_f(\mathbb{Q}_v, E[2]) \text{ for all } v \text{ of } \mathbb{Q} \right\}.$$

The group $\mathrm{Sel}_2(E/\mathbb{Q})$ is a finite dimensional $\mathbb{F}_2$ vector space and sits in the exact sequence

$$0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathrm{Sel}_2(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[2] \longrightarrow 0,$$

where $Ш(E/\mathbb{Q})$ is the Tate-Shafarevich group of E. It follows that the rank of $E(\mathbb{Q})$ is at most $\dim_{\mathbb{F}_2}\mathrm{Sel}_2(E/\mathbb{Q}) - \dim_{\mathbb{F}_2}E(\mathbb{Q})[2]$. Computing $\mathrm{Sel}_2(E/\mathbb{Q})$ is usually the easiest way to obtain an upper bound on the rank of $E(\mathbb{Q})$; when $Ш(E/\mathbb{Q})[2]$ is trivial, this bound is sharp.

2.1. **The Brumer-Kramer bound.** We now assume that $E(\mathbb{Q})[2] = 0$. Define Φ_a to be the set of primes where E has additive reduction. Define Φ_m to be the set of primes p where E has multiplicative reduction and $\mathrm{ord}_p\Delta$ is even, where Δ is the discriminant of E. For each prime p, let n_p be the number of primes of K lying above p, where K is the cubic subfield of the 2-division field of E. Finally, set $u(E) = 1$ if $\Delta < 0$ and $u(E) = 2$ if $\Delta > 0$. Brumer and Kramer then show:

Proposition 2.1 (Proposition 7.1 in [5])**.** *With notation as above, we have*

$$\dim_{\mathbb{F}_2}\mathrm{Sel}_2(E/\mathbb{Q}) \leq \dim_{\mathbb{F}_2}\mathrm{Cl}(K)[2] + u(E) + |\Phi_m| + \sum_{p\in\Phi_a}(n_p - 1). \tag{3}$$

Proposition 2.1 is proved by analyzing the structure of $H^1(\mathbb{Q}, E[2])$ and of $H^1_f(\mathbb{Q}_v, E[2])$ when $E(\mathbb{Q})[2] = 0$. Additional information about $H^1_f(\mathbb{Q}_v, E[2])$ at the primes where E has bad reduction can be used to obtain more refined bounds such as the following.

Proposition 2.2. *If E has split multiplicative reduction at $p = 2$, $\mathrm{ord}_2\Delta$ is even, and 2 ramifies in $K/\mathbb{Q}$, then (3) may be improved to*

$$\dim_{\mathbb{F}_2}\mathrm{Sel}_2(E/\mathbb{Q}) \leq \dim_{\mathbb{F}_2}\mathrm{Cl}(K)[2] + u(E) + |\Phi_m| - 1 + \sum_{p\in\Phi_a}(n_p - 1), \tag{4}$$

We now describe the details from [5] necessary to prove Proposition 2.2.

When $E(\mathbb{Q})[2] = 0$, the norm $N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ induces a map $N : K^\times/(K^\times)^2 \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. The cohomology group $H^1(\mathbb{Q}, E[2])$ is then given by $\ker(N)$.

For each place v of $\mathbb{Q}$, the algebra $A_v = K \otimes \mathbb{Q}_v$ decomposes as $A_v = \bigoplus_{w|v} K_w$. The norm $\mathbf{N}_{A_v/\mathbb{Q}_v} : A_v \to \mathbb{Q}_v$ defined by the product of local field norms $\mathbf{N}_{A_v/\mathbb{Q}_v} = \prod_{w|v} N_{K_w/\mathbb{Q}_v}$ induces a map $N_v : A_v^\times/(A_v^\times)^2 \to \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2$. The group $H^1(\mathbb{Q}_v, E[2])$ is then given by $\ker(N_v)$.

Using this identification, we define a subgroup $U_p \subset H^1(\mathbb{Q}_p, E[2])$ for each prime p as the intersection of the image of $\bigoplus_{w|p}\mathcal{O}_{K_w}^\times$ in $A_p^\times/(A_p^\times)^2$ with $H_f^1(\mathbb{Q}_p, E[2]) \subset \ker(N_p)$. In the proof of Proposition 2.1, Brumer and Kramer then show that

$$\dim_{\mathbb{F}_2}\mathrm{Sel}_2(E/\mathbb{Q}) \leq \dim_{\mathbb{F}_2}\mathrm{Cl}(K)[2] + u(E) + \sum_{p \text{ prime}} \dim_{\mathbb{F}_2} H_f^1(\mathbb{Q}_p, E[2])/U_p. \tag{5}$$

To complete the proof of Proposition 2.1, they then show that $\dim_{\mathbb{F}_2} H_f^1(\mathbb{Q}_p, E[2])/U_p$ is at most $n_p - 1$ if $p \in \Phi_a$, at most 1 if $p \in \Phi_m$, and 0 otherwise. We now prove Proposition 2.2.

Proof of Proposition 2.2. Based on the above, it suffices to show that if E has split multiplicative reduction at $p = 2$, $\mathrm{ord}_2\Delta$ is even, and 2 ramifies in $K/\mathbb{Q}$, then $U_2 = H_f^1(\mathbb{Q}_2, E[2])$.

Since E has split multiplicative reduction at $p = 2$, Proposition 4.1 in [5] tells us that $A_2 = K \otimes \mathbb{Q}_2$ has at least one component equal to $\mathbb{Q}_2$. Since K is ramified at 2, we therefore get that $A_2 \simeq \mathbb{Q}_2 \times L$, where $L/\mathbb{Q}_2$ is a ramified quadratic extension.

Again by Proposition 4.1 in [5], we see that the image of $\delta_2(E(\mathbb{Q}_2))$ is contained in the intersection of $\ker(N_2)$ with the image of $(1, \mathbb{Q}_2^\times)$ in $A_2^\times/(A_2^\times)^2 = \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \times L^\times/(L^\times)^2$. As the image of $\mathbb{Q}_2^\times$ in $L^\times/(L^\times)^2$ is generated by $\mathbb{Z}_2^\times$, we in fact, have $U_2 = H_f^1(\mathbb{Q}_2, E[2])$. □

As a consequence of Propositions 2.1 and 2.2, we get the following.

Corollary 2.3. *We have*

$$28 \leq \dim_{\mathbb{F}_2}\mathrm{Sel}_2(E_{28}/\mathbb{Q}) \leq \dim_{\mathbb{F}_2}\mathrm{Cl}(K_{28})[2] + 8 \quad \textit{and} \tag{6}$$

$$27 \leq \dim_{\mathbb{F}_2}\mathrm{Sel}_2(E_{27}/\mathbb{Q}) \leq \dim_{\mathbb{F}_2}\mathrm{Cl}(K_{27})[2] + 5. \tag{7}$$

Proof. The left-hand inequalities come from the known rational points on $E_n(\mathbb{Q})$. The right-hand inequalities in (6) and (7) follow by direct calculation from Propositions 2.1 and 2.2, respectively. □

Parts (i) of Theorems 2 and 4 now follow directly from Corollary 2.3.

Remark 2.4. As we will see, for both E_{27} and E_{28} the bound in Corollary 2.3 is equal to the suspected rank, allowing us to conclude that $Ш(E)[2] = 0$. This is in line with the Delaunay heuristics, which predict that once E attains even mildly high rank, the probability that $Ш(E)$ is non-trivial is very small [8]. The bounds obtained from Propositions 2.1 and 2.2 are generally not expected to be so tight. We suspect that its accuracy here is a result of these curves having such high rank.

3. An algorithm for computing $\dim_{\mathbb{F}_2}\mathrm{Cl}(K)[2]$

To compute an upper bound on $\dim_{\mathbb{F}_2}\mathrm{Sel}_2(E_{28}/\mathbb{Q})$, we need to bound $\dim_{\mathbb{F}_2}\mathrm{Cl}(K_{28})[2]$. Our method for doing so is based on an algorithm of Buchmann et al. [6] inspired by the number field sieve. While Buchmann's algorithm is able to compute the exact structure of $\mathrm{Cl}(K)$ subject to GRH for a general number field K, we are able to take a few shortcuts that simplify the algorithm since K_{28} is a cubic field and because we are only concerned with obtaining an upper bound on $\dim_{\mathbb{F}_2}\mathrm{Cl}(K_{28})[2]$. We describe our variant of Buchmann's algorithm below.

3.1. **A presentation for** $\mathrm{Cl}(K)$**.** We start with a factor base $\mathcal{P}$ of degree one prime ideals of $\mathcal{O}_K$ (including ramified prime ideals with residue class field degree one) with norm less than a bound $\mathcal{B}$. The factor base $\mathcal{P}$ will serve as a generating set for the class group $\mathrm{Cl}(K)$.

To compute a presentation for $\mathrm{Cl}(K)$, we need relations supported on $\mathcal{P}$. Relations are given by principal ideals (β) such that $\mathbf{N}_{K/\mathbb{Q}}\beta$ is $\mathcal{B}$-smooth and (β) factors as a product of primes in $\mathcal{P}$. Factoring these relations as

$$(\beta) = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\beta)},$$

we obtain a matrix M with entries in $\mathbb{Z}$. If $\mathcal{P}$ is large enough and M contains enough relations, the structure of $\mathrm{Cl}(K)$ can be deduced from the Hermite normal form (HNF) of M.

Computing the HNF of a large matrix is difficult because it requires doing an integral linear algebra computation. However, since we are only interested in computing the rank of $\mathrm{Cl}(K)[2] \simeq \mathrm{Cl}(K)/\mathrm{Cl}(K)^2$, we can take the coefficients of this matrix to be in $\mathbb{F}_2$ instead. In this case, the dimension of the right nullspace of this $\mathbb{F}_2$ matrix is an upper bound for the dimension of the subspace of $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$ generated by the primes in $\mathcal{P}$.

3.2. **The size of the factor base** $\mathcal{P}$**.** By a result of Bach [1], if GRH holds, then $\mathrm{Cl}(K)$ is generated by the primes of K with norm less than $12(\log\mathfrak{d}(K))^2$ (the "Bach bound"), where $\mathfrak{d}(K)$ is the discriminant of $\mathcal{O}_K$. Subsequent work by Belabas, Diaz y Diaz, and Friedman [2] gives an alternative and less explicit bound B_K (the "Belabas bound") such that if GRH holds, then $\mathrm{Cl}(K)$ is generated by the primes of K with norm less than B_K.

While the Belabas bound is asymptotically worse than the Bach bound, it is often quite a bit smaller than the Bach bound for fields of interest. We will therefore use the term "GRH bound" to refer to the smaller of the Bach bound and the Belabas bound for a particular field K. If $\mathcal{P}$ contains all the primes of K with norm less than the GRH bound, the rank of the right nullspace of the relation matrix is an upper bound for $\dim_{\mathbb{F}_2}\mathrm{Cl}(K)[2]$ under GRH.

It is easy to see that if K is a cubic field, then the same result holds if $\mathcal{P}$ only contains all degree one primes of norm less than the GRH bound. If $\mathfrak{p}$ is a degree 3 prime, then $\mathfrak{p}$ is principal and need not be included in $\mathcal{P}$. If $\mathfrak{p}$ is a degree two prime of $\mathcal{O}_K$ lying above a rational prime p, then there is a degree one prime $\mathfrak{p}'$ such that $\mathfrak{p}\mathfrak{p}' = (p)$. Since the ideal classes $[\mathfrak{p}]$ and $[\mathfrak{p}']$ are inverses of each other in $\mathrm{Cl}(K)$, it suffices to include only $\mathfrak{p}'$ in $\mathcal{P}$.

Remark 3.1. Both the Bach and Belabas bounds require GRH to hold for the zeta functions of all unramified abelian extensions of K. However, since we are only

concerned with $\mathrm{Cl}(K)[2]$, it suffices to assume GRH only for those of unramified quadratic extensions of K.

3.3. **Constructing relations.** While the smooth relations (β) described in Section 3.1 need not be constructed in any particular way, there is a computationally efficient method for constructing them based on the number field sieve factoring algorithm [13]. We now describe the basic idea behind sieving.

Letting $f(x)$ be any defining polynomial for K and α be a root of $f(x)$. Suppose that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ given by a rational prime p and a root r of $f(x) \pmod p$. We can then see that $\mathfrak{p}$ divides $a + b\alpha$ if $r \equiv -ab^{-1} \pmod p$. Therefore, we may identify all $a + b\alpha$ in a large range $-A \leq a \leq A$ and $1 \leq b \leq B$ such that $\mathfrak{p}$ divides $a + b\alpha$.

Doing this for all of the primes $\mathfrak{p} \in \mathcal{P}$, we may identify all coprime (a, b) with $-A \leq a \leq A$ and $1 \leq b \leq B$ such that $a + b\alpha$ is divisible by many different primes $\mathfrak{p}$ in $\mathcal{P}$ and therefore more likely to factor completely in terms of primes in $\mathcal{P}$. After identifying many candidates $a+b\alpha$, we may apply trial division (or any other factoring algorithm) to discover which $(a + b\alpha)$ factor entirely in $\mathcal{P}$.

4. Choosing parameters

Constructing relations requires choosing three parameters: the polynomial $f(x)$ defining K, a factor base bound $\mathcal{B}$, and a sieve region $[-A, A] \times [1, B]$. We now describe how to choose these parameters with a focus on the field K_{28}.

4.1. **Choosing the polynomial.** If K is a cubic field, then we can always find a defining polynomial $f(x)$ for K (unique up to the action of $\mathrm{GL}_2(\mathbb{Z})$) such that the discriminant of $f(x)$ is equal to the discriminant of $\mathcal{O}_K$. By applying Julia reduction to $f(x)$ (see Algorithm 1 in [7], for example), we can obtain what is in some sense the smallest polynomial defining K. For the field K_{28}, this reduced polynomial is given by

$$\begin{aligned} f(x) = {} & 64023127168000x^3 + 10309553525987840512490787747x^2 \\ & - 385887800226533264569886106608158518260 8x \\ & - 690432957144021383533767485102108376768946894343026 74. \end{aligned} \tag{8}$$

4.2. **Choosing the factor base bound.** Section 3.2 addresses how small the factor base bound $\mathcal{B}$ may be. However, choosing the smallest possible $\mathcal{B}$ makes it less likely that an element $a + b\alpha$ of a given size will be smooth. While choosing a larger bound $\mathcal{B}$ will make it easier to find relations, it will make the follow-on linear algebra work harder since the size of the matrix M will increase. Our primary goal in choosing a factor base bound was that the resulting matrix could be processed in **magma**. For K_{28}, a natural touchstone was the Bach bound of $1,202,639$, which gave us a factor base $\mathcal{P}$ containing $92,945$ primes.

4.3. **Choosing a sieve region.** In order to choose a sieve region $\mathcal{A} = [-A, A] \times [1, B]$, we need to consider two things: how large our sieve region should be (that is, $2 \cdot A \cdot B$) and how skew that region should be (that is, A/B).

4.3.1. *Skewness.* Let $F(X,Y)$ be the homogenization of $f(x)$. The norm $\mathbf{Norm}(a+b\alpha)$ is given by $\mathbf{Norm}(a+b\alpha) = N_{K/\mathbb{Q}}(a+b\alpha) = F(a,-b)/c_3(f)$, where $c_3(f)$ is the leading coefficient of $f(x)$. Assuming that all primes dividing $c_3(f)$ are in $\mathcal{P}$, $\mathcal{P}$ contains all of the primes dividing (α), and a is coprime to b, then $(a+b\alpha)$ factors completely in $\mathcal{P}$ if and only if $F(a,-b)$ is $\mathcal{B}$-smooth. Therefore, the likelihood that the ideal generated by $a+b\alpha$ for a random (a,b) in $\mathcal{A}$ factors completely in $\mathcal{P}$ is given by the probability that $F(a,-b)$ is $\mathcal{B}$-smooth for a random $(a,b) \in \mathcal{A}$. To first order approximation, this probability is determined by the size of $|F(a,-b)|$.

Rather than attempt to understand how the size of $|F(a,-b)|$ is distributed on $\mathcal{A}$, we may simply consider the maximum of $|F(a,-b)|$ on the boundary of $\mathcal{A}$. To do so, we consider the individual terms of $F(X,Y)$, which attain their maximum (in absolute value) of $|c_i|A^iB^{3-i}$ at the point (A,B), where c_i is the coefficient of x^i in $f(x)$. An ideal skewness would have A/B chosen so that each $|c_i|A^iB^{3-i}$ is of roughly equal size.

The polynomial $F(X,Y)$ does not admit a skewness such that each $|c_i|A^iB^{3-i}$ is of roughly equal size. We may, however, choose a skewness so that the largest two values of $|c_i|A^iB^{3-i}$ are roughly the same. For our polynomial $F(X,Y)$, this suggests a skewness of $s = 2^{41.25}$.

If $\mathcal{A}$ has skewness $s = 2^{41.25}$, then $\mathcal{A}$ must have an area of at least $S = 42.25$ bits in order to have integral points with $b \neq 0$. We will therefore assume that S is at least 42.25 bits. In this case, we find that the two largest values of $|c_i|A^iB^{3-i}$ are $|c_2|A^2B$ and $|c_0|B^3$, which both have size $175.5 + \frac{3}{2}(S-42.25)$ bits. As the values of $|c_1|AB^2$ and $|c_3|A^3$ are substantially smaller, we may approximate the maximum of $|F(X,-Y)|$ on $\mathcal{A}$ as $|c_2|A^2B + |c_0|B^3$ which is roughly $176.5 + \frac{3}{2}(S-42.25)$ bits in size.

4.3.2. *Smoothness probabilities.* We now must consider how large of a sieve region to use. In order to produce enough relations, we need

$$\frac{1}{\zeta(2)} 2 \cdot A \cdot B \cdot \mathrm{Prob}\big(F(a,-b) \text{ is } \mathcal{B}\text{-smooth } \mid (a,b) \in \mathcal{A}\big) \geq |\mathcal{P}|.$$

We therefore need to estimate the probability that $F(a,-b)$ is $\mathcal{B}$-smooth when (a,b) is chosen randomly from $\mathcal{A}$.

Let $\rho(u)$ denote Dickman's rho function. If n is a random number of size C, then standard results tell us that the probability that n is $\mathcal{B}$-smooth can be approximated by $\rho\left(\frac{\log C}{\log \mathcal{B}}\right)$ as long as $\mathcal{B} \geq (\log C)^{2+\epsilon}$ (assuming GRH) [12]. However, if $n = F(a,-b)$ is a random value of $F(X,Y)$, then the probability that n is $\mathcal{B}$-smooth is affected by a parameter known as $\alpha = \alpha(F)$ which takes into account the modular root properties of $F(X,Y)$ [15]. Assuming that n has size C, the probability that n is $\mathcal{B}$-smooth is equal to the probability that a random number of size $C\alpha$ is smooth. We may therefore approximate the probability that n is smooth by $\rho\left(\frac{\log C + \log \alpha}{\log \mathcal{B}}\right)$. An approximation of α may be computed in **magma** using the command `MurphyAlphaApproximation`. For the polynomial $F(X,Y)$, we have $\alpha \approx 2^{-1.9}$.

4.3.3. *Relation estimates.* The size of $|F(a,-b)|$ for $(a,b) \in \mathcal{A}$ may vary considerably. A crude estimate for a representative value of $|F(a,-b)|$ would be the maximum of $|F(X,Y)|$ on the boundary of $\mathcal{A}$ (calculated to be $176.5 + \frac{3}{2}(S-42.25)$ bits at the end of Section 4.3.1).

We obtain a less crude estimate by decomposing $\mathcal{A}$ into shells and taking the maximum of $|F(X,Y)|$ on each shell to be representative of the values of $|F(X,Y)|$ on that shell. Assuming that $S = 42.25 + 0.25 \cdot k$, then using shells of radius 0.25, we estimate that the number of relations for a sieve region of size S is given by

$$\frac{1}{\zeta(2)} \sum_{i=0}^{k} \beta(k)\rho\left(\frac{176.5 + \log_2 \alpha + \frac{3}{2}(0.25k)}{\log_2 \mathcal{B}}\right) = \frac{1}{\zeta(2)} \sum_{i=0}^{k} \beta(k)\rho\left(\frac{174.6 + \frac{3k}{8}}{20.2}\right),$$

where $\beta(k) = \begin{cases} 2^{42.25} & \text{if } k = 0, \\ 2^{42.25+0.25k} - 2^{42.25+0.25(k-1)} & \text{if } k > 0. \end{cases}$

Estimates for several values of S are given Table 1. Since $\mathcal{P}$ consists of 92,945 primes, Table 1 suggests that $\mathcal{A}$ should have size somewhere between 2^{46} and $2^{46.5}$.

TABLE 1. Estimated numbers of relations for different sieve regions

S	Estimated number of relations
45	51,394
45.5	65,320
46	82,602
46.5	104,046
47	130,648
47.5	163,641

4.4. **The computation for K_{28}.** We chose to sieve the region $[-2^{43.75}, 2^{43.75}] \times [1,5]$, which has size roughly 2^{47}. We found 133,637 relations, which is in line with the prediction in Table 1. We were able to augment these with 15,518 relations coming from rational primes p that split completely in $\mathcal{O}_K$ (that is, relations of the form $p + 0 \cdot \alpha$).

Unsurprisingly, a small number of primes in $\mathcal{P}$ did not appear in any relation. However, these primes all had norm greater than the Belabas bound of 200,439, allowing us to safely remove them from $\mathcal{P}$.

However, when we reduced the entries of the relation matrix into $\mathbb{F}_2$, we discovered that the columns for the degree one primes $\mathfrak{p}_7$ and $\mathfrak{p}_{13}$ above 7 and 13 were identically zero. Further inspection revealed that since $\mathrm{ord}_{\mathfrak{p}_7}\alpha = -2$, we had $\mathrm{ord}_{\mathfrak{p}_7} a + b\alpha = -2$ for all relations $a + b\alpha$. The same held true for $\mathfrak{p}_{13}$. We remedied this by including a small number of relations of the form $a + 7\alpha$ and $a + 13\alpha$ (found via sieving). (A degree one prime above 17 would have exhibited the same phenomenon had we not included the rational relation $17 + 0 \cdot \alpha$.)

After computing the nullspace of our relation matrix, we discovered a small number of low-weight nullvectors that appeared spurious. These corresponded to primes (all above the Belabas bound) not appearing in enough relations. By removing the relations incident on these primes, we were able to remove these primes from $\mathcal{P}$. A second nullspace computation showed that the right nullspace of the modified relation matrix had rank 20, proving part (ii) of Theorem 2.

The dominant portion of the computation was the sieving step. Since the NFS functionality built into **magma** did not support our chosen sieve region, we wrote

speciality C code to handle the sieving. The sieve portion of the computation took roughly 14.5 core days on a cluster composed of Intel 2.6 GHz processors. The linear algebra portion of the computation was completed in **magma**, taking roughly 15 minutes on a single desktop processor and using under 16 GB of memory.

Proof of Theorem 1. Combining Corollary 2.3 with part (ii) of Theorem 2, we get that $\dim_{\mathbb{F}_2}\mathrm{Sel}_2(E_{28}/\mathbb{Q}) = 28$, conditional on GRH. The result follows since E_{28} has at least 28 independent points. □

4.5. **Computation for K_{27}.** We used the same considerations described in Sections 4.1–4.3 to choose parameters for K_{27}.

The appropriately minimized and reduced polynomial for K_{27} is given by

$$\begin{aligned} f(x) = {} & 15560036076469248x^3 + 5146844140746931983614347 3x^2 \\ & - 4973122278025054077694001656870 28x \\ & + 5568846122535578469536281311952727406 23601. \end{aligned} \tag{9}$$

The relative size of the coefficients of $f(x)$ suggest that we should use a skewness of $s = 2^{26.625}$.

To choose the factor base bound $\mathcal{B}$, we first considered the Belabas bound $\mathcal{B}_B$ which **magma** says is equal to $143,829$. However, a back of the envelope calculation showed that finding relations with this bound would be particularly difficult, and that choosing $\mathcal{B} = 4 \cdot \mathcal{B}_B$ would be more effective. This resulted in a factor base with $47,063$ primes.

Using the method described in Section 4.3.3 for estimating relations, we chose the sieve region $[-2^{34}, 2^{34}] \times [1, 166]$ which has size roughly $2^{42.375}$. Sieving this region yielded $54,597$ relations which we augmented with an additional $7,817$ relations coming from rational primes.

As was the case for K_{28}, the initial right nullspace computation produced a small number of low-weight vectors. After removing the corresponding columns and the rows incident on them (as well as the empty columns), we were left with a $62,370 \times 46,513$ matrix M. As all of the columns removed corresponded to primes above the Belabas bound, this did not affect the integrity of our computation. A computation in **magma** then showed that the right nullspace of M had dimension 22. As a result, $\mathrm{Cl}(K_{27})$ has 2-rank at most 22, subject to GRH, proving part (ii) of Theorem 4.

Proof of Theorem 3. Combining Corollary 2.3 with part (ii) of Theorem 4, we get that $\dim_{\mathbb{F}_2}\mathrm{Sel}_2(E_{27}/\mathbb{Q}) = 27$, conditional on GRH. The result follows since E_{27} has at least 27 independent points. □

Acknowledgments

We would like to express our thanks to Noam Elkies for sharing the curve E_{27} with us and for providing a number of helpful suggestions along the way. We would also like to thank Jonathan Bober for sharing Booker and Dwyer's results with us. Additionally, we would like to thank the referee for suggesting the refinement of the Brumer-Kramer bound that appears as Proposition 2.2.

References

[1] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380. MR1023756

[2] K. Belabas, F. Diaz y Diaz, and E. Friedman, *Small generators of the ideal class group*, Math. Comp. **77** (2008), no. 262, 1185–1197. MR2373197

[3] J. W. Bober, *Conditionally bounding analytic ranks of elliptic curves*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 135–144. MR3207411

[4] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR1484478

[5] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), no. 4, 715–743. MR0457453

[6] J. Buchmann, M. J. Jacobson Jr., S. Neis, P. Theobald, and D. Weber, *Sieving methods for class group computation*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 3–10. MR1672089

[7] J. E. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2** (1999), 64–94. MR1693411

[8] C. Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbb{Q}$, Experiment. Math. **10** (2001), no. 2, 191–196. MR1837670

[9] B. Dodson. *Re:* $\mathbb{Z}^{28}$ *in* $E(\mathbb{Q})$*, etc.* Listserv. 4 May 2006. NmbrThry.

[10] A. Dujella. *History of elliptic curves rank records.* 2015, `https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`.

[11] N.D. Elkies. $R\mathbb{Z}^{28}$ *in* $E(\mathbb{Q})$*, etc.* Listserv. 3 Apr. 2006. NmbrThry.

[12] A. Hildebrand, *Integers free of large prime factors and the Riemann hypothesis*, Mathematika **31** (1984), no. 2, 258–271 (1985). MR804201

[13] A. Lenstra and H. W. Lenstra Jr., *The development of the number field sieve*, Springer, 1993.

[14] J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques* (French), Compositio Math. **58** (1986), no. 2, 209–232. MR844410

[15] B. Murphy, *Modelling the yield of number field sieve polynomials*, Algorithmic number theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, pp. 137–150. MR1726067

[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094

[17] Sage Mathematics Software (Version 7.1), The Sage Developers, 2016, `http://www.sagemath.org`.

Center for Communications Research, 4320 Westerra Court, San Diego, California 92121

Email address: `zdklags@ccrwest.org`

3208 Riva Ridge Ct, Bowie, Maryland 20721

Email address: `glaisher@hotmail.com`

ICERM, Brown University, Providence, Rhode Island 02903

Current address: P.O. Box 4671, Sidney, Ohio 45365

Email address: `havepenwillfigure@gmail.com`