RANK OF AN ELLIPTIC CURVE AND 3-RANK OF A QUADRATIC FIELD VIA THE BURGESS BOUNDS

NOAM D. ELKIES

ABSTRACT. For nonzero k let E_k be the "Mordell curve" $y^2 = x^3 + k$. Let

$$D = 725138346538478285394503254 93 = 41p \tag{1}$$

Where p is the prime 17686301135084836229134225 73. Then the elliptic curve E_{16D} has rank $r = 16$ over $\mathbf{Q}$. Because E_k is always 3-isogenous with E_{-27k}, it follows that E_{-432D} has rank 16 as well. This was the first pair of Mordell curves known to have rank at least 16; we now prove that it has rank exactly 16. Having shown $r \geq 16$ by exhibiting 16 independent points, we must prove $r \leq 16$ by descent. This leads us to compute the 3-torsion in the class group of $\mathbf{Q}(\sqrt{-3D})$. The discriminant of this field has absolute value $|\Delta| = 3D > 2 \cdot 10^{29}$, so large that it is not routine to compute the class group without a GRH assumption. We compute it unconditionally using the Burgess bounds on short character sums, which reduce the calculation from $\widetilde{O}(|\Delta|^{1/2})$ to $|\Delta|^{1/4+\epsilon}$, and Treviño and Booker's explicit bounds on the constants in the Burgess bounds, to make the factor $|\Delta|^{\epsilon}$ explicit as well. Along the way we compute unconditionally the class group of $\mathbf{Q}(\sqrt{-3D})$, whose 3-rank of 8 is the current record for the class group of a quadratic number field.

0. INTRODUCTION

The general elliptic curve of j-invariant zero is the "Mordell curve"

$$E_k : y^2 = x^3 + k \tag{2}$$

for nonzero k. The Mordell–Weil ranks of such curves E_k over $\mathbf{Q}$ have long been of interest, both as a natural question in its own right and because of connections to other arithmetic questions and quantities, including the rank of the 3-torsion subgroup of quadratic number fields $\mathbf{Q}(\sqrt{k})$. In [Bhargava–Elkies–Shnidman 2019] the average rank of E_k is shown to be bounded as k varies in $\mathbf{Z}$ (or in any arithmetic progression in $\mathbf{Z}$), but it is not known whether individual curves E_k can have arbitrarily large rank. In [Elkies 2016] we gave the first known examples of a curve E_k of rank at least 16, improving the previous record of 15 [Elkies 2009]. But at the time we could not prove unconditionally that our curve's rank is exactly 16, only that it is at least 16 (by exhibiting 16 rational points and checking their independence). In this paper we give an unconditional proof.

It is well-known (see (5) below) that E_k and E_{-27k} are related by 3-isogenies and thus have the same rank. We prove:

Theorem 1. Let

$$D = 725138346538478285394503254 93 = 41 \cdot 17686301135084836229134225 73. \tag{3}$$

Date: June 2024.
2010 *Mathematics Subject Classification.* 11G05, 11R29, 11L40, 11Y40/11Y50.
NSF grants DMS-1100511 and DMS-1502161; Simons AGNTC Collaboration grant #550031.

Submitted to Algor. Num. Th. Symp.

Then the Mordell–Weil groups $E_{16D}(\mathbf{Q})$ and $E_{-432D}(\mathbf{Q})$ are free abelian groups of rank 16. The 16 points tabulated in (10) are independent in the Mordell–Weil group $E_{16D}(\mathbf{Q})$, and the 16 points tabulated in (9) are independent in the Mordell–Weil group $E_{-432D}(\mathbf{Q})$.

This k, like previous records, was found by applying the Mestre–Nagao heuristic (large partial sums of $-\log L(E,1)$ suggest large rank of E) to a family of curves E_k of moderately large rank, using the sieve technique described in [Elkies–Klagsbrun 2020, §3] to search more efficiently. Further details will appear elsewhere; here we are concerned with proving the rank unconditionally.

Once we had the high-rank candidate k it was not hard to find the 16 points P_i or Q_j and check that they are independent. But to complete the proof of Theorem 1 we must also show that the rank is no larger than 16, and this requires a descent.[1] The difficulty of this descent is intermediate between those of record-rank and near-record-rank curves with nontrivial torsion, such as those of [Elkies–Klagsbrun 2020], and (near-)record curves with trivial torsion and isogeny class, such as those analyzed in [Klagsbrun–Sherman–Weigandt 2016]. If $E/\mathbf{Q}$ has a torsion point P of order l then the descent via l-isogenies between E and $E/\langle P\rangle$ requires only factorization in $\mathbf{Z}$ and $\mathbf{Z}[\boldsymbol{\mu}_l]$, which is routine for all high-rank E seen so far, and is likely to remain routine for the foreseeable future. For unconstrained E, the simplest descent available is a 2-descent, which requires computing the 2-torsion subgroup of the class group of the 2-torsion field $\mathbf{Q}(E[2])$, or of a cubic subfield in the usual case that $\mathrm{Gal}(\mathbf{Q}(E[2])/\mathbf{Q}) \cong S_3$. This is not yet feasible to do unconditionally, and it was already a significant advance when [Klagsbrun–Sherman–Weigandt 2016] could determine the rank assuming the GRH (generalized Riemann hypothesis) "only" for number fields rather than for the elliptic-curve L-function $L(E,s)$.

When E is a Mordell curve E_k, the cubic subfields of $\mathbf{Q}(E[2])$ are isomorphic with the "pure cubic field" $\mathbf{Q}(k^{1/3})$, whose class group is no easier to compute than that of an unconstrained cubic field of the same size; Magma [Bosma–Cannon–Playoust 1997] can already compute the class group under GRH, but this is just because our D is much smaller than the coefficients of the curves analyzed in [Klagsbrun–Sherman–Weigandt 2016]. However, E_k also has a 3-isogenous curve E_{-27k}, which allows a simpler descent involving 3-torsion in the quadratic field $\mathbf{Q}(\sqrt{k})$ and its "mirror field" $\mathbf{Q}(\sqrt{-3k})$. Not only are those fields' class groups much easier to compute under GRH than the class group of $\mathbf{Q}(k^{1/3})$ (seconds rather than hours in Magma); for $k = 16D$ we find that it is even possible, with rather more effort, to *unconditionally* compute the class group, and thus determine the exact rank of E_k. The present paper documents the resulting proof of Theorem 1.

For our curves the descent via isogenies between E_k and E_{-27k} accounts for most of the rank of these curves via the rank of the 3-torsion subgroups of the class groups of $\mathbf{Q}(\sqrt{k})$ and $\mathbf{Q}(\sqrt{-3k})$. We find that these real and imaginary quadratic fields have class groups of 3-rank 7 and 8 respectively, which is the current record. This connection was already used in [Quer 1987], where three curves E_k of rank 12 led to three imaginary quadratic fields $Q(\sqrt{k})$ each of 3-rank 6 and with a mirror field of 3-rank 5.

The rest of the paper proceeds as follows. First we review the 3-isogenies $\varphi, \widehat{\varphi}$ between Mordell curves E_k and E_{-27k}, and exhibit 16 independent points on each of E_{16D} and E_{-432D}. We then carry out the descents via the isogenies $\varphi, \widehat{\varphi}$ and reduce the proof of

[1] And some luck: a descent computes a Selmer group, which gives only an upper bound on the rank, and this bound is not necessarily sharp because the Tate–Šafarevič group might intervene. But for record-rank curves such as our E_{16D} it is rare for the Selmer bound to be even larger than the arithmetic rank.

Theorem 1 to the calculation of 3-ranks of the class groups of the quadratic number fields of discriminants D and $-3D$. We exhibit the structure of these class groups assuming GRH, and then adapt the technique of [Booker 2006] to determine unconditionally the class group of $\mathbf{Q}(\sqrt{D})$ using the explicit constants of [Booker 2006, Treviño 2015] for the bounds of [Burgess 1962] on short character sums. Finally, we note that our curves also yield a pure cubic field $\mathbf{Q}(k^{1/3})$ whose class group has 2-rank at least 15 (and exactly 15 under GRH), and announce a curve E_k of rank 17 to which our analytic technique does not apply because k is the product of two large primes.

Acknowledgement. I am grateful to the referees for their careful reading of the initial manuscript and for their detailed corrections and suggestions.

1. The 3-isogenous curves E_{16D} and E_{-432D}, and the points P_i, Q_j

1.1. **The endomorphism ring; the isogenies $\varphi : E_k \to E_{-27k}$ and $\widehat{\varphi} : E_{-27k} \to E_k$.** We work over an arbitrary field F of characteristic zero. Let ρ be a cube root of unity, and $\bar\rho = \rho^2$ its conjugate, so $\rho - \bar\rho$ is a square root of -3; if $F \subseteq \mathbf{C}$, we may take $\rho = (-1+\sqrt{3}\,i)/2$. Then for every k the endomorphism ring $\mathrm{End}_{\overline{F}}(E_k)$ is isomorphic to $\mathbf{Z}[\rho]$, with ρ acting by $(x,y) \mapsto (\rho x, y)$. It is well-known that if $k \in F^*$ then the curves E_k and E_{-27k}, which are each other's quadratic twist by $F(\rho) = F(\sqrt{-3}\,)$, are also related by 3-isogenies defined over F, each with kernel consisting of the point at infinity together with the two points where $x = 0$. Note that this is the subgroup of $E(\overline{F})$ fixed by ρ, and thus the kernel of $\rho - \bar\rho = \sqrt{-3}$. Using the group law on the elliptic curve E_k, we compute that if $P \in E_k(F)$ has coordinates (x,y) then

$$(\rho - \bar\rho)(P) = (\rho x, y) + (\bar\rho x, -y) = \Big(-\frac{x^3+4k}{3x^2}, \frac{(x^3-8k)y}{(\rho-\bar\rho)^3 x^3}\Big). \tag{4}$$

As expected, this point is in $E_k(F(\rho))$, and its negative can be obtained by switching ρ with $\bar\rho$, which lets us identify (4) with an F-rational point on the quadratic twist. Multiplying x by $-3 = (\rho-\bar\rho)^2$ and y by $(\rho-\bar\rho)^3$ gives the coordinates of this point. We have thus constructed the 3-isogeny

$$\varphi : E_k \to E_{-27k}, \quad (x,y) \mapsto \Big(\frac{x^3+4k}{x^2}, \frac{(x^3-8k)y}{x^3}\Big), \tag{5}$$

whose kernel consists of the origin and the points $(x,y) = (0, \pm\sqrt{k})$. Applying the same formula with k replaced by $-27k$ gives a map from E_{-27k} to E_{729k}. Now E_{729k} is identified with E_k by dividing x by 9 and y by 27; thus we obtain the dual isogeny

$$\widehat{\varphi} : E_{-27k} \to E_k, \quad (x,y) \mapsto \Big(\frac{x^3-108k}{9x^2}, \frac{(x^3+216k)y}{27x^3}\Big), \tag{6}$$

with kernel $\{\mathbf{0}, (0, \pm\sqrt{-27k}\,)\}$. We can check that $\widehat{\varphi}\circ\varphi$ and $\varphi\circ\widehat{\varphi}$ are the multiplication-by-3 maps on E_k and E_{-27k} respectively, for instance by checking that for large x, y (that is, near the origins of E_k and E_{-27k}) these maps $\widehat{\varphi}\circ\varphi$ and $\varphi\circ\widehat{\varphi}$ multiply the local coordinate x/y by $3 + o(1)$.

1.2. **The curves E_{16D} and E_{-432D} and their minimal models.** For any field F not of characteristic 2 or 3, and any $k, k' \in F^*$, the curves E_k and $E_{k'}$ are isomorphic if and only if $k'/k \in F^{*6}$. Thus for $F = \mathbf{Q}$ each Mordell curve is isomorphic to a unique curve E_k with $k \in \mathbf{Z}$ that is free of sixth-power factors. Given such k, the model $y^2 = x^3 + k$ for E_k is minimal unless $k \equiv 16 \bmod 64$, when the minimal model is $y^2 + y = x^3 + (k-16)/64$,

obtained from $E_{k/64}$ by replacing y by $y + 1/2$. This is the case for our $k = 16D$, so the minimal model of E_{16D} is

$$y^2 + y = x^3 + \frac{D-1}{4} = x^3 + 181284586634619571348625813 73. \tag{7}$$

This curve has discriminant $-27D^2$ and conductor $27D^2$; likewise E_{-432D} has minimal model

$$y^2 + y = x^3 - \frac{27D+1}{4} = x^3 - 489468383913472842641289697078, \tag{8}$$

again with conductor $27D^2$ and this time with discriminant -3^9D^2.

We next exhibit 16 independent points on each of these curves. Even with coefficients as large as those of (7,8), it is still feasible to search for integral points with x of size comparable with $|k|^{1/3}$, and this turns out to be sufficient. Curiously such a search succeeds more quickly for the slightly more complicated curve E_{-432D}, even though E_{16D} and E_{-432D} have the same regulator (they are related by 3-isogenies, and each of $E_{16D}(\mathbf{Q})$ and $E_{-432D}(\mathbf{Q})$ contains the image of the other with the same index 3^8). Using Stoll's program `ratpoints` [Stoll 2008], later ported into `gp` [BBBCO 1998–2023] as `ellratpoints` and `hyperellratpoints`, it takes only a minute or so to find all integers $x \in [0, 10^{12}]$ such that $x^3 - 432D$ is a square; this is several thousand times faster than 10^{12} calls to `gp`'s `issquare` command or the corresponding command in a comparable package.[2] We find 31 such x. Using the height pairing on E_{-432D} we compute that these points generate a group of rank 16. We then sort the pairs $(x, \pm y)$ by increasing canonical height and extract the lexicographically first generating set. Choosing from each pair the point with $y > 0$ yields the following 16 independent points Q_j $(1 \le j \le 16)$ on E_{-432D}:

[2] `ratpoints` still takes time $\widetilde{O}(N)$ to find all integer solutions of $P(x) = y^2$ with x in an interval of length N, but with much smaller constants, because most candidates x are excluded with a sieve, without ever testing whether the large integer $P(x)$ is a square. Asymptotically, it is even faster to use lattice reduction techniques as in [Elkies 2000]. In our setting x^3, y^2, and $x^3 - y^2$ are of comparable size, so we cannot use our technique for finding all small nonzero values of $|x^3 - y^2|$ with $x < N$ in time only $\widetilde{O}(N^{1/2})$; but we can at least use linear approximations to $x^{3/2}$ to reduce the runtime to $\widetilde{O}(N^{5/6})$, still using negligible space. But $N = 10^{12}$ is not large enough for this to give much if any improvement compared with `ratpoints/(hyper)ellratpoints`.

(9)

j	$x(Q_j)$	$y(Q_j)$	$\hat{h}(Q_j)$
1	7902580710	63670717606558	21.874
2	9243066342	547910842668385	21.962
3	9384872862	580613609811649	21.971
4	10588813590	835332795310558	22.044
5	11276039694	971735349657982	22.083
6	14415958344	1583178444925222	22.248
7	14600918460	1619646563246566	22.257
8	38242987644	7445931730687462	23.028
9	31840756833/4	977373412490165/8	23.264
10	32498192145/4	1731017073186653/8	23.275
11	7916896660	82103281566566	23.339
12	8045520694	176978571769182	23.348
13	8702884360	411934199691558	23.392
14	12861701800	1279905353076441	23.635
15	22606480144	3326205023518937	24.051
16	202406423745/4	90889676714539589/8	24.664

For E_{16D} we could proceed in the same way, though it is somewhat harder than the computation for E_{-432D}, even though we find a Mordell–Weil subgroup of the same regulator. Alternatively, having found a rank-16 subgroup of $E_{-432D}(\mathbf{Q})$, we can compute its preimage under φ in $E_{16D}(\mathbf{Q})$. Either way we find a rank-16 group whose lexicographically first generating set comprises the following points P_i $(1 \le i \le 16)$:

(10)

i	$x(P_i)$	$y(P_i)$	$\hat{h}(P_i)$
1	1061832153	139016765771325	22.181
2	−2069581821	96250143600728	22.212
3	2323084809	175115687339501	22.303
4	2437726383	180595326275964	22.318
5	3097225419	218722516138736	22.407
6	7619958189	678654480211793	22.970
7	13493940633	1573274288396285	23.446
8	15245095569	1887136964766261	23.554
9	6376192377/4	1191407043318535/8	23.609
10	17844824169	2387591696553138	23.696
11	5948344741/9	3664166411156266/27	24.359
12	7271819311/9	3687841575833417/27	24.365
13	−11236359299/9	3434674826973187/27	24.375
14	31140274567/9	6588845927720308/27	24.655
15	−26120241831/16	7512202525369347/64	24.965
16	−1185892731/25	16830196043015853/125	25.370

2. The and φ- and $\widehat{\varphi}$-descents; the class groups of $\mathbf{Q}(\sqrt{D}\,)$ and $\mathbf{Q}(\sqrt{-3D}\,)$

2.1. From φ- and $\widehat{\varphi}$-descents to 3-torsion in class groups of $\mathbf{Q}(\sqrt{D}\,)$ and $\mathbf{Q}(\sqrt{-3D}\,)$.

Suppose in general that D is an integer such that $D \equiv 1 \bmod 4$, so the minimal model of

E_{16D} is $y^2 + y = x^3 + (D-1)/4$ as in (7), and that D is not a square. Working in the $E_{16D}[\varphi]$-torsion field $\mathbf{Q}(\sqrt{D})$, we have the factorization

$$x^3 = y^2 + y - \frac{D-1}{4} = \Big(y + \frac{1+\sqrt{D}}{2}\Big)\Big(y + \frac{1-\sqrt{D}}{2}\Big), \tag{11}$$

with each factor $y + (1 \pm \sqrt{D})/2$ being a Weil function on E_{16D}. Thus we have a homomorphism $\delta : E_{16D}(\mathbf{Q}) \to \mathbf{Q}(\sqrt{D})^\times/(\mathbf{Q}(\sqrt{D})^\times)^3$ that takes any nonzero (x, y) to the class of $y + (1 + \sqrt{D})/2$, with $\ker\delta = \widehat{\varphi}(E_{-432D}(\mathbf{Q}))$. We claim:

Lemma 1. Suppose the integer D is squarefree, congruent to $1 \bmod 4$, and not equal to 1 or -3. Then the image of δ is contained in the subgroup of $\mathbf{Q}(\sqrt{D})^\times/(\mathbf{Q}(\sqrt{D})^\times)^3$ consisting of cosets $[a]$ such that $3|v_{\mathfrak{q}}(a)$ for all primes $\mathfrak{q}$ of $\mathbf{Q}(\sqrt{D})$.

Note that the rank of this subgroup is the sum of the ranks of the unit group and the 3-torsion of the class group of $\mathbf{Q}(\sqrt{D}\,)$.

Proof. Write x, y in lowest terms as $(x, y) = (m/d^2, n/d^3)$ for some integers m, n, d with $d > 0$, and multiply the factorization (11) by d^6 to obtain a factorization

$$m^3 = \Big(n + \frac{1+\sqrt{D}}{2}d^3\Big)\Big(n + \frac{1-\sqrt{D}}{2}d^3\Big) \tag{12}$$

in the ring of integers O_D of $\mathbf{Q}(\sqrt{D})$. We claim that the two factors are relatively prime. Indeed, suppose both factors are contained in some prime ideal $\mathfrak{q}$ of O_D. Then so is their sum $\sqrt{D}\,d^3$, so either $\mathfrak{q}|d$ or $\mathfrak{q}|\sqrt{D}$. If $\mathfrak{q}|d$ then $\mathfrak{q}|n$, so $y = n/d^3$ is not in lowest terms (if two rational integers are coprime in $\mathbf{Z}$ then they remain coprime in O_D). If $\mathfrak{q}$ does not divide d then $\mathfrak{q}$ is odd and contains $2n + d^3$, so $\gcd(2n + d^3, D) \neq 1$ in $\mathbf{Z}$. Letting q be a common prime factor of $2n + d^3$ and D, we observe that $(2n + d^3)^2 = 4m^3 + Dd^6$ so $q|m$ and $v_q(D) \geq 2$, contradicting our hypothesis that D be squarefree. Thus the factors $n + (1 \pm \sqrt{D})/2$ are relatively prime as claimed. Therefore

$$3 \mid v_{\mathfrak{q}}\Big(n + \frac{1 \pm \sqrt{D}}{2}d^3\Big) \tag{13}$$

for all primes $\mathfrak{q}$ of O_D. Since also $3|v_{\mathfrak{q}}(d^3)$, the lemma is proved. □

For E_{-432D}, we likewise define a homomorphism $\hat{\delta} : E_{-432}(\mathbf{Q}) \to \mathbf{Q}(\sqrt{-3D})^\times/(\mathbf{Q}(\sqrt{-3D})^\times)^3$ that takes any nonzero (x, y) to the class of $y + (1 + \sqrt{-3D})/2$, with $\ker\hat{\delta} = \varphi(E_{16D}(\mathbf{Q}))$. As with δ, we have:

Lemma 2. Suppose the integer D is squarefree, congruent to $1 \bmod 4$, and is neither a multiple of 3 nor equal to 1. Then the image of $\hat{\delta}$ is contained in the subgroup of $\mathbf{Q}(\sqrt{-3D})^\times/(\mathbf{Q}(\sqrt{-3D})^\times)^3$ consisting of cosets $[a]$ such that $3|v_{\mathfrak{q}}(a)$ for all primes $\mathfrak{q}$ of $\mathbf{Q}(\sqrt{-3D})$.

The additional assumption that D is not a multiple of 3 still holds for our $D = 41p$.

Proof. We proceed as in the proof of Lemma 1, starting with the factorization

$$m^3 = \Big(n + \frac{1+\sqrt{-27D}}{2}d^3\Big)\Big(n + \frac{1-\sqrt{-27D}}{2}d^3\Big). \tag{14}$$

The only change occurs when $\mathfrak{q}$ is the prime of O_{-3D} above the ramified rational prime 3, and $\mathfrak{q}$ does not divide d. In this case $v_q(D) = 3$, so $(2n + d^3)^2 = 4x^3 + Dd^6$ is possible; but then $v_q(2n + d^3) \geq 2$, so each of the factors in (14) has the same $\mathfrak{q}$-valuation as $\sqrt{-27D}$, which is 3. Thus even in this new case the valuation is a multiple of 3 and we are done. □

Combining these two lemmas, we find:

Proposition 2. Suppose the integer D is squarefree, congruent to 1 mod 4, and is neither a multiple of 3 nor equal 1. Then the rank of E_{16D} is at most the sum of 1 and the 3-ranks of the class groups of $\mathbf{Q}(\sqrt{D})$ and $\mathbf{Q}(\sqrt{-3D})$.

Proof. Let r be the rank of E_{16D}. Under our hypotheses, E_{16D} has trivial torsion, so

$$\begin{aligned} 3^r &= [E_{16D}(\mathbf{Q}) : 3E_{16D}(\mathbf{Q})] \\ &= [\widehat{\varphi}(E_{-432D}(\mathbf{Q})) : 3E_{16D}(\mathbf{Q})]\,[E_{16D}(\mathbf{Q}) : \widehat{\varphi}(E_{-432D}(\mathbf{Q}))], \end{aligned} \tag{15}$$

and the first factor is $[E_{-432D}(\mathbf{Q}) : \varphi(E_{16D}(\mathbf{Q}))]$. Thus our two lemmas bound r by the sum of unit ranks and class-group 3-ranks of $\mathbf{Q}(\sqrt{D})$ and $\mathbf{Q}(\sqrt{-3D})$. The unit ranks are either $0+1$ (for $D>0$) or $1+0$ (for $D<0$) by Dirichlet, so in either case we deduce the claimed bound. □

Thus for our $D = 41p$ the 3-ranks must sum to at least $16-1=15$, so by the reflection theorem the class groups of $\mathbf{Q}(\sqrt{D})$ and $\mathbf{Q}(\sqrt{-3D})$ must have 3-ranks at least 7 and 8 respectively. We shall see that in fact these 3-ranks are exactly 7 and 8, which will prove that E_{16D} and E_{-432D} have rank 16.

2.2. **The class groups of $\mathbf{Q}(\sqrt{D})$ and $\mathbf{Q}(\sqrt{-3D})$.** For a fundamental discriminant Δ, let H_Δ be the class group of the quadratic field $\mathbf{Q}(\sqrt{\Delta})$ of that discriminant, and let $h_\Delta = |H_\Delta|$ be the class number. Thus we want to show that H_{-3D} has 3-rank 8, and H_D has 3-rank 7. Now Magma takes only a few seconds to compute both class groups assuming the GRH:

$$H_{-3D} \overset{\text{GRH}}{\cong} (\mathbf{Z}/2\mathbf{Z})^2 \times (\mathbf{Z}/3\mathbf{Z})^8 \times (\mathbf{Z}/77681\mathbf{Z}) \times (\mathbf{Z}/139939\mathbf{Z}), \tag{16}$$

$$H_D \overset{\text{GRH}}{\cong} (\mathbf{Z}/2\mathbf{Z})^2 \times (\mathbf{Z}/3\mathbf{Z})^7. \tag{17}$$

We shall remove the GRH hypothesis from (16) (Proposition 3 below). This will imply in particular that H_{-3D} indeed has 3-rank 8. We do *not* claim to prove (17) unconditionally, but once we know that $r_3(H_{-3D}) = 8$ the Scholz reflection theorem [Scholz 1932] gives $r_3(H_D) = 7$, which is all we need to establish that E_{16D} and E_{-432D} have rank 16.

For each of H_{-3D} and H_D, Magma computes ideals the rings of integers in $\mathbf{Q}(\sqrt{-3D})$ or $\mathbf{Q}(\sqrt{D})$ whose classes generate the conjectural class groups. In the case of H_{-3D}, we denote by H_0 the subgroup of H_{-3D} generated by those ideal classes. It is easy to check unconditionally that each generator has the claimed order and that they are independent in H_{-3D}.[3] Thus we have an injection $H_0 \hookrightarrow H_{-3D}$. We shall show:

Proposition 3. The injection $H_0 \hookrightarrow H_{-3D}$ is an isomorphism; that is, (16) is true unconditionally.

We begin the proof by checking that $[H_{-3D} : H_0]$ is odd. Indeed $H_{-3D}[2] \cong (\mathbf{Z}/2\mathbf{Z})^2$ by genus theory, so there is no missing 2-torsion; and using [Rédei 1934] we check that $H_{-3D}[4] = H_{-3D}[2]$, so H_0 also accounts for all the 4-torsion in H_{-3D}. Therefore Proposition 3 will follow once we prove that $h_{-3D} < 3|H_0|$; we do this in the next section. (If H_{-3D} did have elements of order 4 then proving $h_{-3D} < 3|H_0|$ would not suffice to prove

[3] For the eight 3-torsion classes, we just reduced all $3^8 - 1 = 6560$ nontrivial combinations and checked that none of them is principal. This was fast enough that there was no need to split the 3-torsion generators into two subsets of four, reduce each of the $2(3^4-1) = 160$ nontrivial combinations of each subset, and check that none is principal and no two match.

Proposition 3, but it would still establish that H_{-3D} and H_0 have the same 3-rank, which is all that we need to prove our main theorem; we could also still prove Proposition 3 by computing longer partial sums of the relevant L-function, as can be seen by taking $N = 2^{45}$ instead of $N = 2^{43}$ in (38).)

3. The Dirichlet formula and the Burgess–Treviño–Booker bounds

The Dirichlet class number formula gives

$$h_{-3D} = \frac{\sqrt{3D}}{\pi} L(1, \chi_{3D}) = \frac{\sqrt{3D}}{\pi} \sum_{n=1}^{\infty} \frac{\chi_{3D}(n)}{n} \tag{18}$$

where $\chi_{3D} = \left(\frac{-3D}{\cdot}\right)$ is the quadratic character of conductor $3D$ associated to the imaginary quadratic field $\mathbf{Q}(\sqrt{-3D}\,)$. Since h_{-3D} is an integer, this formula determines its value once the sum is computed to within $\pi/(2\sqrt{3D})$. Our D is much too large for such accuracy (to within about $3.4 \cdot 10^{-15}$) to be feasible. But we already have an odd-index subgroup H_0 of the class group of $\mathbf{Q}(\sqrt{-3D}\,)$. Therefore, to prove that $h = |H_0|$ it is enough to bound $L(1, \chi_{3D})$ by $3\pi|H_0|/\sqrt{3D}$. This requires much less accuracy: using (16) we compute

$$\begin{aligned} |H_0| &= 2^2\, 3^8\, 77681 \cdot 139939 = 285288064689996, \\ \pi|H_0|/\sqrt{3D} &= 1.92159744340\ldots. \end{aligned} \tag{19}$$

But even this accuracy is not easy to achieve, because the sum $\sum_{n=1}^{\infty} \chi_{3D}(n)/n$ that defines $L(1, \chi_{3D})$ does not converge absolutely, and we need to compute a long partial sum, say

$$L_{(N)}(1, \chi_{3D}) := \sum_{n=1}^{N} \frac{\chi_{3D}(n)}{n}, \tag{20}$$

to guarantee that $L(1, \chi_{3D})$ does not exceed 5.7.

The length N of the partial sum that we need depends on how well we can estimate the remainder, call it

$$R(\chi_{3D}, N) := L(1, \chi_{3D}) - L_{(N)}(1, \chi_{3D}) = \sum_{n=N+1}^{\infty} \frac{\chi_{3D}(n)}{n}. \tag{21}$$

We expect $R(\chi_{3D}, N)$ to decay roughly as $N^{-1/2}$: when $\gcd(n, 3D) = 1$, the signs $\chi_{-3D}(n) = \pm 1$ should behave almost like independent coin flips, which makes $\sum_{n>N}(\chi_{3D}(n)/n)$ a random variable with variance about $2/(3N)$. In fact the signs are not quite independent, because for each m, knowing $\chi_{3D}(n)$ determines $\chi_{3D}(mn)$; and the numerical plot below might hint at subtler correlations. The light blue plot shows the remainder

$$R(\chi_D, N) := \sum_{n=N+1}^{\infty} \frac{\chi_D(n)}{n}. \tag{22}$$

in the sum for $L(1, \chi_D)$, scaled by the same factor of $N^{1/2}$, and shows a similar bias for positive values but not an oscillation as prominent as the one for $R(\chi_{3D}, N)$. Here $\chi_D = \left(\frac{D}{\cdot}\right)$ is the quadratic character of conductor D associated to $\mathbf{Q}(\sqrt{D})$.

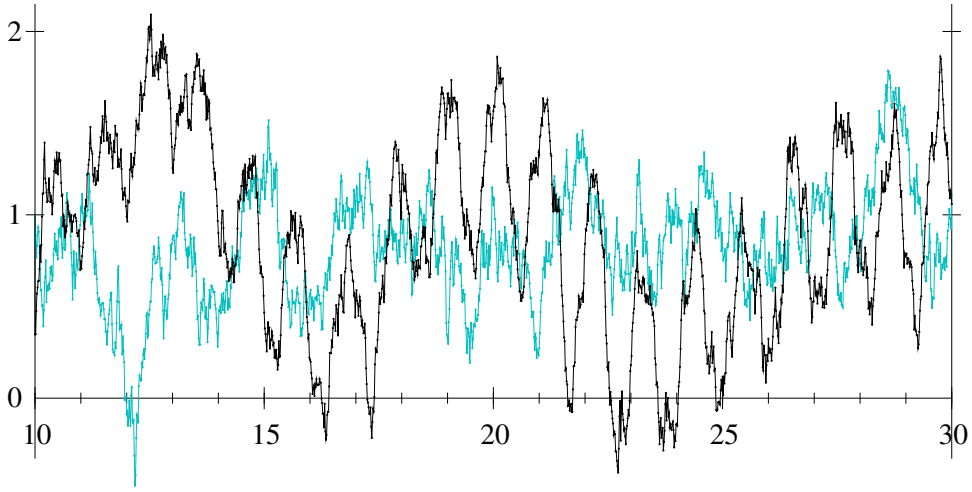

Figure 1: $N^{1/2}R(\chi_{3D}, N)$ and $N^{1/2}R(\chi_D, N)$ for $N = 2^x$, $10 \le x \le 30$

It takes rather more work to *prove* that $L(1, \chi_{3D})$, and thus H_{-3D}, is given by (19) as expected. We begin with the standard device of writing $R(\chi_{3D}, N)$ as a Riemann-Stieltjes integral involving

$$S(x) := \sum_{1 \le n \le x} \chi_{3D}(n) \tag{23}$$

and integrating by parts:

$$\begin{aligned} R(\chi_{3D}, N) &= \int_{N+\frac{1}{2}}^{\infty} \frac{1}{x}\, d\big(S(x) - S(N)\big) \\ &= \left[\frac{S(x) - S(N)}{x}\right]_{x=N}^{\infty} - \int_{N+\frac{1}{2}}^{\infty} \big(S(x) - S(N)\big)\, d(1/x) \\ &= \int_{N+\frac{1}{2}}^{\infty} \big(S(x) - S(N)\big)\, \frac{dx}{x^2}\,. \end{aligned} \tag{24}$$

Now $S(x)$ is bounded, because χ_{3D} is periodic with period $3D$ and $\sum_{n=1}^{3D} \chi_{3D}(n) = 0$; this proves that indeed $R(\chi_{3D}, N) \to 0$ as $N \to \infty$. But the convergence is too slow for our purpose: it is known (Pólya–Vinogradov 1918) that for any primitive Dirichlet character χ of conductor q, all sums $\sum_{n=N}^{N'} \chi(n)$ are $O(q^{1/2} \log q)$, with an effective implied constant (that can be easily taken less than 1); and conversely such sums are $\gg q^{1/2}$ in mean square, so $q^{1/2}$ is the best estimate possible up to log factors. But then (24) yields an upper bound of order $q^{1/2}/N$ on $R(\chi_{3D}, N)$, which means we would have to take N of size about $q^{1/2}$ to be able to prove $R(\chi_{3D}, N) \ll 1$. Since $q^{1/2} > 4.6 \cdot 10^{14}$ for our $q = 3D$, such a calculation might be feasible, but only at an exorbitant computational cost.

3.1. **The Burgess bounds on short character sums.** Fix a nontrivial character χ modulo a prime p, and again define $S(N) = \sum_{n=1}^{N} \chi(N)$. Burgess [Burgess 1962] found a series of upper bounds on character sums

$$S_\chi(N, H) := S(N + H) - S(N) = \sum_{h=1}^{H} \chi(N + h) \tag{25}$$

that, for certain ranges of H, improve on both the trivial bound $|S_\chi(N,H)| \le H$ and the Pólya–Vinogradov bound $S_\chi(N,H) \ll p^{1/2}\log p$. Namely, for each positive integer r Burgess shows

$$S_\chi(N,H) \ll_r (\log p)^{1/r} H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}}. \tag{26}$$

For $r = 1$ this coincides with the Pólya–Vinogradov bound. For each $r > 1$, the bound improves on Pólya–Vinogradov for $H < p^{\frac{2r+1}{4r}+o(1)}$, and on the trivial bound for $H > p^{\frac{r+1}{4r}+o(1)}$.

Our χ_{3D} has modulus $123p$, which is not quite prime. But if χ has modulus ap for some small a (so in particular $a \not\equiv 0 \bmod p$), then we can still improve on both the trivial and Pólya–Vinogradov estimates on $S_\chi(N,H)$ by factoring $\chi = \chi_a\chi_p$ for some characters $\chi_a \bmod a$ and $\chi_p \bmod p$, and writing

$$S_\chi(N,H) = \sum_{b \bmod a} \chi_a(b) \left(\sum_{\substack{0<h\le H \\ N+h\equiv b \bmod a}} \chi_p(N+h) \right). \tag{27}$$

There are $\phi(a)$ choices of b for which $\chi_a(b) \ne 0$; for each of these, $|\chi_a(b)| = 1$, and the inner sum in (27) is the sum of χ_p over an arithmetic progression of length $\lfloor H/a \rfloor$ or $\lceil H/a \rceil$. Since χ_p is multiplicative, this sum is $\chi_p(a)S_{\chi_p}(N', N'+H')$ for some $N' \bmod p$ and $H' = H/a + O(1)$, and we can apply a Burgess bound to $S_{\chi_p}(N', N'+H')$. This yields the estimate

$$S_\chi(N,H) \ll_r \frac{\phi(a)}{a^{1-\frac{1}{r}}} (\log p)^{1/r} H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}}, \tag{28}$$

uniformly in a for $H \ge a$ (which will always be true in practice). The factor $\phi(a)/a^{1-\frac{1}{r}} < a^{1/r}$ is small enough that (28) can still be a substantial improvement over both the trivial and Pólya–Vinogradov bounds, all the more so since the Pólya–Vinogradov bound on S_χ includes a factor $a^{1/2}$ that does not appear in (28).

Putting this into the estimate into (24) we find a bound on $|R(\chi_{3D}, N)|$ proportional to

$$\frac{\phi(a)}{a^{1-\frac{1}{r}}} (\log p)^{1/r} \int_N^\infty x^{1-\frac{1}{r}} \frac{dx}{x^2} = r \frac{\phi(a)}{a^{1-\frac{1}{r}}} (\log p)^{1/r} p^{\frac{r+1}{4r^2}} N^{-1/r}. \tag{29}$$

Thus the remainder $|R(\chi_{3D}, N)|$ will be small once N exceeds a large enough multiple of

$$\frac{\phi(a)^r}{a^{r-1}} (\log p) p^{\frac{r+1}{4r}}, \tag{30}$$

same as the threshold for the Burgess bound to be nontrivial. As r grows, this threshold is $O(p^{\frac{1}{4}+o(1)})$. For our p, the factor $p^{1/4}$ is less than 10^7, so we expect to be able to compute the partial sum $L_{(N)}(1, \chi_{3D})$ of (20) even if the constants implied in "$\ll_r$" are substantial.

3.2. **Booker's explicit bound.** The proof of the Burgess bounds is complicated enough that it takes some work to extract explicit constants. Fortunately ours is not the first computational application, so this work has already been done in several different ways, starting with [Grosswald 1981, Theorem 1]. In fact Booker did this in 2006 for the very similar problem of computing $L(1, \chi_p)$ to enough precision to certify the class group of a real quadratic field, giving the following bound:[4]

[4]We reproduce the phrasing verbatim, except that we change Booker's d, M, N to p, N, H for consistency with our notations, and reproduce only the $r = 2$ row of his Table 1. Note that the exponent of $\log p$ in

Proposition 4. [Booker 2006, Proposition 2] Let $p > 10^{20}$ be a prime number $\equiv 1 \pmod 4$, $r \in \{2, \dots, 15\}$, and N, H integers with $0 < N, H < 2\sqrt{p}$. Then

$$\left| \sum_{N \le n < N+H} \chi_p(n) \right| \le \alpha(r) p^{\frac{r+1}{4r^2}} (\log p + \beta(r))^{\frac{1}{2r}} H^{1-\frac{1}{r}} \tag{31}$$

where $\alpha(r), \beta(r)$ are given in Table 1.

Here χ_p is the quadratic character mod p. Instead of reproducing the entire table from [Booker 2006], we copy only the values for the exponent $r = 2$ that we shall use:

$$\alpha(2) = 1.8221, \quad \beta(2) = 8.9077. \tag{32}$$

As r grows from 2 to 15, the $\alpha(r)$ slowly decrease to $\alpha(15) = 1.3164$, while the $\beta(r)$ decrease more rapidly, reaching $\beta(1) = -1.9808$.

Our p does exceed 10^{20}, and happily satisfies $p \equiv 1 \bmod 4$. Our N do not all satisfy $0 < N < 2\sqrt{p}$; but Booker's proof does not use this hypothesis, and indeed the proof needs to show (31) for all N because (as Booker notes at the start) it proceeds by an induction on H that requires that (31) hold for smaller H and all $N \bmod p$. The proof does use the condition $H \le 2\sqrt{p}$; Booker remarks that arbitrary H could be allowed "at the expense of slightly worse constants", but does not quantify how much worse.[5] Recall that we have written a sum of H consecutive values of χ_{3D} as a sum of $\phi(123) = 80$ sums $S_{\chi_p}(N, H')$ with $H' < (H/123) + 1$, so we can apply Booker's bound for $x \le 246p^{1/2}$. For $H > 2p^{1/2}$ we use [Treviño 2015, Corollary 1], which has a larger power of $\log p$ but applies to all primes $p \ge 10^7$, any non-principal character $\chi \bmod p$, and all N, H and positive integers r:

$$|S_\chi(N, H)| < 2.74 H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{1/2}. \tag{33}$$

We now substitute these bounds into (29). In Booker's bound (31), the factor

$$(\phi(123)/\sqrt{123})\, \alpha(2)\, (\log p + \beta(2))^{1/4} p^{3/16} \tag{34}$$

is less than $5 \cdot 10^6$. Estimating the integral more carefully than in (29), we obtain

$$\int_N^{2\sqrt{p}} (x-N)^{1/2} \frac{dx}{x^2} = \frac{\pi}{2\sqrt{N}} \,. < \int_N^{\infty} (x-N)^{1/2} \frac{dx}{x^2} = \frac{\pi}{2\sqrt{N}} < \frac{1.6}{\sqrt{N}} \,. \tag{35}$$

For $x > 246\sqrt{p}$ we use the Treviño bound 33 with $r = 2$, getting

$$\int_{2\sqrt{p}}^{\infty} \big(S(x) - S(N)\big) \frac{dx}{x^2} \; < 2.74 \frac{\phi(123)}{\sqrt{123}} p^{3/16} (\log p)^{1/2} \int_{246p^{1/2}}^{\infty} x^{1/2} \frac{dx}{x^2} \tag{36}$$

which is

$$2.74 \frac{80}{123} (\log p)^{1/2} \sqrt{2} / p^{1/16} < 0.4. \tag{37}$$

We conclude that the remainder $R(\chi_{3D}, N)$ of (21) satisfies

$$\big|R(\chi_{3D}, N)\big| < \frac{8 \cdot 10^6}{\sqrt{N}} + 0.4 \,. \tag{38}$$

---

(31) is $1/2r$, so Booker's estimate actually improves on [Burgess 1962] by a factor that grows to infinity as $p \to \infty$.

[5] Booker avoided $H > 2\sqrt{p}$ by using an approximate functional equation to replace the partial sums $L_{(N)}(1, \chi_p)$ by a more refined estimate which however is somewhat more complicated to compute.

3.3. **Computational conclusion and details.** Taking $N = 2^{43}$ in (38) gives a bound of $10^6/2^{18.5} + 0.4 < 3.1$. Since we expect that in fact $\sum_{n=1}^{N} \chi_{3D}(n)/n$ will be very close to $L(1, \chi_{3D})$, this should be more than enough to prove that our subgroup H_0 of the class group H_{-3D} is in fact the full class group.

We computed $S(2^{43})$ numerically; our C code took about a day to run on 16 heads each summing 1/16 of the terms. (See the next two paragraphs for more details about this computation.) The result of $1.92159704\ldots$ was very close to the value $1.92159744\ldots$ of (19), as expected. Thus H_0 has index less than 3 in H_{-3D}. Since we already know that the index is odd, this completes the proof of (16), which we asserted as Proposition 3. Theorem 1 then follows via φ- and $\widehat{\varphi}$-descents. □

We compute character values $\chi_{3D}(n)$ using Quadratic Reciprocity. This is the most time-consuming part of the computation of $S(2^{43})$. We halve the number of character evaluations by writing each $n \le 2^{43}$ as $2^e n_1$ for some odd n_1 and nonnegative integer $e \le 43$. Then

$$S(2^{43}) = \sum_{\substack{0<n_1<2^{43} \\ n_1 \text{ odd}}} \left(\sum_{2^e n_1 \le 2^{43}} \frac{\chi_{3D}(2^e)}{2^e} \right) \frac{\chi_{3D}(n_1)}{n_1}, \tag{39}$$

so we need only evaluate $\chi_{3D}(n_1)$ at odd $n_1 < 2^{43}$. Moreover, the inner sum over e is constant on dyadic intervals $2^f \le n_1 < 2^{f+1}$, so we can rewrite (39) as

$$S(2^{43}) = \sum_{f=0}^{42} \left(\sum_{e=0}^{f-1} \frac{\chi_{3D}(2^e)}{2^e} \right) \left(\sum_{\substack{2^f \le n_1 < 2^{f+1} \\ n_1 \text{ odd}}} \frac{\chi_{3D}(n_1)}{n_1} \right). \tag{40}$$

Then the multiplication by $\sum_e \chi_{3D}(2^e)/2^e$ need only be done 43 times instead of 2^{42}. Since $\chi_{3D}(3) = 0$, we save a further factor of 2/3 by skipping all $n_1 \equiv 0 \bmod 3$. For each of the 16 positive odd $n_0 < 32$, we restrict the last sum in (40) odd $n \equiv n_0 \bmod 32$ that are not multiples of 3, and evaluate these 16 subsums in parallel.

We first did this in floating-point arithmetic, summing over each congruence class mod 32 in reverse order (from $f = 42$ to $f = 0$) to reduce precision loss. Since floating-point arithmetic makes it messy to prove rigorous error bounds, we checked our calculation using only integer arithmetic, as follows. Fix a large integer M, and compute an integer approximation to

$$MS(2^{43}) = \sum_{\substack{0<n_0<32 \\ n_0 \text{ odd}}} \sum_{f=0}^{42} \left(\sum_{e=0}^{f-1} \frac{\chi_{3D}(2^e)}{2^e} \right) \left(\sum_{\substack{2^f \le n_1 < 2^{f+1} \\ n_1 \equiv n_0 \bmod 32}} \chi_{3D}(n_1) \frac{M}{n_1} \right) \tag{41}$$

by replacing each M/n_1 by $\lfloor M/n_1 \rfloor$ (which is what `M/n1` means in C when `M` and `n1` are positive integers). The resulting integer, call it

$$\Sigma_{n_0,f} := \sum_{\substack{2^f \le n_1 < 2^{f+1} \\ n_1 \equiv n_0 \bmod 32}} \chi_{3D}(n_1) \left\lfloor \frac{M}{n_1} \right\rfloor, \tag{42}$$

then differs from the actual sum over n_1 in (41) by an error whose absolute value is at most the length of the sum. Then approximate each term $\pm\Sigma_{n_0,f}/2^e$ in the expansion of $\left(\sum_{e=0}^{f-1} \chi_{3D}(2^e)/2^e\right)\Sigma_{n_0,f}$ by $\pm\lfloor \Sigma_{n_0,f}/2^e \rfloor$. This at most doubles the error. Our final integer estimate for $MS(2^{43})$ is thus within 2^{43} of its actual value, so we recover a rational

approximation of $S(2^{43})$ itself that is within $2^{43}/M$ of its correct value. We chose $M = 2^{61}$ so that we could carry out the entire computation in signed 64-bit arithmetic without running into the overflow threshold at $\pm 2^{63}$. The result agreed with the floating-point answer of $1.92159704\ldots$ (and for several more digits). The error bound of $2^{43}/M = 2^{-18} < 0.000004$ does not even prove that $S(2^{43}) < 1.9216$, but it does easily give $S(2^{43}) < 1.922$, which is still much closer than we need to prove that $[H_{-3D} : H_0] < 3$ and thus that $H_{-3D} = H_0$.

3.4. **More on H_{-3D} and H_D.** We noted already that $r_3(H_{-3D}) = 8$ is the current record for the 3-rank of a quadratic number field. The Cohen–Lenstra heuristics suggest that it might be one of the first examples of $r_3(H_\Delta) = 8$, which should happen for about one of every $3^{8^2} = 3^{64}$ imaginary quadratic number fields, while $3D < 3^{61.5}$, and only $3/\pi^2 < 1/3$ of integers are fundamental discriminants.

We did not attempt to remove the GRH hypothesis from the determination of the class group of H_D (17). This would be possible but would require more work. One difficulty is the fundamental unit; even with a class group of size $2{\cdot}3^7 = 4374$, the regulator exceeds $2.88{\cdot}10^{10}$ under GRH. A greater difficulty is that (still under GRH) we have $L(1, \chi_D) = 0.93602\ldots$, which is about half of $L(1, \chi_{3D})$; this means that we would have to use an even larger N to prove that $\left|R(\chi_D, N)\right| < 2L(1, \chi_D)$.

4. Further results

4.1. **A pure cubic field of 2-rank (at least) 15.** A 2-torsion point on either of our rank-16 curves E_{16D} and E_{-432D} generates an extension of $\mathbf{Q}$ isomorphic with the "pure cubic field" $\mathbf{Q}((2D)^{1/3})$. A 2-descent on either curve shows that the curve's rank is at most 1 more than the 2-rank of the class group of $\mathbf{Q}((2D)^{1/3})$. Assuming the GRH, Magma takes about 70 minutes to compute that this class group is $\cong (\mathbf{Z}/2\mathbf{Z})^{15} \oplus (\mathbf{Z}/3\mathbf{Z})^2$, so in particular its 2-rank is exactly 15. This is currently the highest 2-rank known for a pure cubic field. (For unrestricted cubic fields the records are 20 in the totally real case and 22 in the mixed case, coming from 2-torsion points on elliptic curves of ranks 28 and 27 respectively; see the paragraph following [Klagsbrun–Sherman–Weigandt 2016, Theorem 4].)

4.2. **A curve E_k of rank (at least) 17.** As far as we know, the current rank record for curves E_k is 17, attained a few weeks after the discovery of E_{16D} and announced in [Elkies 2016a] (and recently exhibited on MathOverflow [Elkies 2023]), but not previously published:

$$\begin{aligned} k &= -90880073662995252611677228364836 3 \\ &= -2195745961 \cdot 41389156704451409263768 3. \end{aligned} \tag{43}$$

This curve certainly has rank at least 17 (and thus larger than the rank of E_{16D}); for example, the isogenous curve E_{-27k} has 17 independent points with x-coordinates

$$\begin{aligned} &-110315760690, -218829008658, 194693247690, -12083686365, 179588218407, \\ &660796972800, 481938369495, 532637728899, 891937317975, 1556910033324, \\ &1369152212199, -249954149276, 527526224524, 2095375244992, 3020920353232, \\ &45908680009155, 209109621212430 \end{aligned}$$

— these are somewhat simpler than for E_k because here E_{-27k} has regulator 1/3 times that of E_k. The rank is exactly 17 assuming the Generalized Riemann Hypothesis holds for $\mathbf{Q}(\sqrt{k})$ or $\mathbf{Q}(\sqrt{-3k})$. (We do not get new 3-rank records for $\mathbf{Q}(\sqrt{k})$ or $\mathbf{Q}(\sqrt{-3k})$,

whose class groups still have 3-rank 8 and 7 respectively, again assuming the relevant GRH; likewise the class group of $\mathbf{Q}(k^{1/3})$ has 2-rank 15 under GRH, and as it happens is again $\cong (\mathbf{Z}/2\mathbf{Z})^{15} \oplus (\mathbf{Z}/3\mathbf{Z})^2$.) But here we cannot remove the hypothesis. This is not because k is too large: it exceeds $16D$ by a factor of about 800, so one might expect the computation to take at most 10 times longer, which would still have been feasible. The real difficulty is that the Burgess bounds are known only for characters of prime conductor: k, unlike D, is not prime or even nearly prime. When and if the Burgess bounds are extended to characters of composite conductor, it may become feasible to prove unconditionally that this curve indeed has rank 17.

References

[BBBCO 1998–2023] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier: *User's Guide to PARI-GP*, available from http://megrez.math.u-bordeaux.fr/pub/pari .

[Bhargava–Elkies–Shnidman 2019] Manjul Bhargava, Noam Elkies, and Ari Shnidman: The average size of the 3-isogeny Selmer groups of elliptic curves $y^2 = x^3 + k$. *J. London Math. Soc.* **101** #1 (Feb. 2020), 299–327. (Published online on 12 Aug. 2019; https://doi.org/10.1112/jlms.12271; arXiv: 1610.05759)

[Booker 2006] Andrew R. Booker: Quadratic class numbers and character sums. *Math. of Computation* **75** (#255, July 2006), 1481–1492; article electronically published on March 21, 2006. https://www.jstor.org/stable/4100285

[Bosma–Cannon–Playoust 1997] Wieb Bosma, John Cannon, and Catherine Playoust: The Magma algebra system. I. The user language. *J. Symbolic Computation* **24** #3–4 (1997), 235–265.

[Burgess 1962] D. A. Burgess: On character sums and primitive roots. *Proc. London Math. Soc.* (3) **12** (1962), 179–192. https://doi.org/10.1112/plms/s3-12.1.193

[Elkies 2000] Noam D. Elkies: Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction, pages 33–63 in *Lecture Notes in Computer Science* **1838** (Proceedings of ANTS-4, 2000; W. Bosma, ed.). arXiv: math.NT/0005139

[Elkies 2009] Noam D. Elkies: "$j = 0$, rank 15; also 3-rank 6 and 7 in real and imaginary quadratic fields", NMBRTHRY post, 30 December 2009. Archived at https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;6a3fad67.0912&S=

[Elkies 2016] Noam D. Elkies: "$j = 0$, rank 16; also 3-rank 7 and 8 in real and imaginary quadratic fields", NMBRTHRY post, 6 February 2016. Archived at https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;fc0d1ed0.1602&S=

[Elkies 2016a] Noam D. Elkies: "$j = 0$, rank 17", e-mail broadcast, 23 February 2016.

[Elkies 2023] Noam D. Elkies: Answer to Stanley Yao Xiao's Question 442468 "Mordell curves with large rank", 11 March 2023. https://mathoverflow.net/questions/442468/mordell-curves-with-large-rank/442487#442487

[Elkies–Klagsbrun 2020] Noam D. Elkies and Zev Klagsbrun: New rank records for elliptic curves having rational torsion. In: Proceeedings of the Fourteeneth Algorithmic Number Theory Symposium (ANTS-14), 2020; https://msp.org/obs/2020/4-1/obs-v4-n1-p15-s.pdf, arXiv: 2003.00077.

[Grosswald 1981] E. Grosswald: On Burgess' bound for primitive roots modulo primes and an application to $\Gamma(p)$. *Amer. J. Math.* **103** #6 (1981), 1171–1183.

[Klagsbrun–Sherman–Weigandt 2016] Zev Klagsbrun, Travis Sherman, and James Weigandt: The Elkies Curve has Rank 28 Subject only to GRH. *Math. of Computation* **88** (#316, March 2019), 837–846. (Published online on May 17, 2018; http://dx.doi.org/10.1090/mcom/3348; arXiv: 1606.07178)

[Quer 1987] Jordi Quer: Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12, *C. R. Acad. Sc. Paris I* **305** (1987), 215–218.

[Rédei 1934] L. Rédei: Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *J. reine angew. Math.* **171** (1934), 55–60.

[Scholz 1932] A. Scholz: Über die Beziehung der Klassenzahlen quadratischer Körper zueinander, *J. reine angew. Math.* **166** (1932), 201–203.

[Stoll 2008] Michael Stoll: The `ratpoints-2.1.3` package, available at http://www.mathe2.uni-bayreuth.de/stoll/programs/ratpoints-2.1.3.tar.gz ; Documentation for the `ratpoints` program, arXiv:0803.3165

[Treviño 2015] Enrique Treviño: The Burgess inequality and the least k-th power non-residue. *International J. Number Theory* **11** #5, 1653–1678 (Published 3 August 2015; arXiv: 1412.3062)

Department of Mathematics, Harvard University, Cambridge MA 02138 USA

Email address: elkies@math.harvard.edu

Submitted to Algor. Num. Th. Symp.