Curves $Dy^2 = x^3 - x$

of odd analytic rank

Noam D. Elkies
Harvard University

1. Introduction: Review of the arithmetic of the "congruent number" curves

$$E_D : Dy^2 = x^3 - x;$$

statement of new results.

2. Proof of: $D \equiv 5, 6, 7 \bmod 8 \Rightarrow r(E_D) > 0$ if $0 < D < 10^6$ (previous bound [ANTS-I]: $2 \cdot 10^5$)

3. Rank 3 curves with $D < 10^7$ in the same congruence classes

1. Introduction.

Recall (e.g. from ANTS-I paper): for nonzero $D \in \mathbf{Q}$ let E_D be the elliptic curve $Dy^2 = x^3 - x$ (or in Weierstrass form $y^2 = x^3 - D^2x$) over $\mathbf{Q}$. May assume $D \in \mathbf{Z}$ squarefree since $E_{c^2D} \cong E_D$. For this family also $E_{-D} \cong E_D$.

Classical interest: The arith. rank $r(E_D/\mathbf{Q})$ is positive $\Longleftrightarrow$ D is area of a rational right triangle $\Longleftrightarrow$ D is common difference (**congruum**) of a 3-term arith. prog. of rational squares (i.e., D is a "congruent number").

Modern interest: $\{E_D\}$ is a family of quadratic twists of E_1; since $r(E_1/\mathbf{Q}) = 0$ [Fermat], $r(E_D/\mathbf{Q}) > 0 \Longleftrightarrow r(E_1/\mathbf{Q}(\sqrt{D})) > 0$; the E_D are a paradigmatic example and test case for elliptic-curve ideas in general, sometimes easier because CM.

Conductor of E_D is $16D^2$ or $32D^2$ for D even or odd. Functional equation of $L(E_D/\mathbf{Q}, s)$ has sign $+1$ for $|D|$ in $\{1, 2, 3\}$ mod 8, and -1 for $|D|$ in $\{5, 6, 7\}$ mod 8. Thus we expect [Birch and Swinnerton-Dyer] that $r(E_D/\mathbf{Q})$ is even in the $+1$ case, odd in the -1 case. We consider the odd case: $|D| = 8k+5$, $8k+6$, or $8k+7$. [NB: if this holds for c^2D then it holds for D, since c is odd so $c^2 \equiv 1 \bmod 8$. Hence we needn't officially require D squarefree, but can still assume it in practice.]

If r is odd then $r > 0$; hence we expect all such $|D|$ to be "congruent numbers". In [ANTS-I] we proved this for $|D| < 2 \cdot 10^5$. New software and faster hardware lets us obtain:

Theorem. *Let D be an integer such that $|D| \equiv 5$, 6, or 7 mod 8 and $|D| < 10^6$. Then E_D has positive analytic rank over $\mathbf{Q}$.*

The computations that establish this result also yield the conjectural value of $r(E_D/\mathbf{Q})$ for all $|D|$ in those mod-8 congruence classes up to 10^6, and indeed 10^7. As expected, the rank is usually 1. But we have no heuristic for the frequence of rank 3 and higher. The experimental tables of rank-3 values of $|D|$ are the most extensive ones so far of rank-3 quadratic twists of any elliptic curve, and might be used to suggest or test frequency heuristics for such twists. They already point to unexpected and mysterious biases: some congruence classes are significantly richer in rank-3 twists.

The tables can be accessed on the Web by following links from

<www.math.harvard.edu/~elkies/compnt.html>.

2. Proof of Theorem 1.

Approach is same as in [ANTS-I]. Don't actually look for rational (x, y) on E_D! Smallest height is often $|D|^{(1/2r)\pm\epsilon}$ where $r = r(E_D/\mathbf{Q})$; usually $r = 1$, and $|D|^{(1/2)\pm\epsilon}$ quickly becomes hopelessly large. Fortunately rank 1 can be recognized indirectly in time $|D|^{O(1)}$. For the few remaining cases we can try to find a point of height $< |D|^{(1/6)+\epsilon}$. This is feasible now for larger $|D|$ thanks to better software (Cremona's MWRANK — not available in 1994 — exploiting full 2-torsion on $E_D(\mathbf{Q})$) and faster computers.

How to prove $r > 0$ without exhibiting x, y? Thanks to the Heegner-Birch construction of rational points on E_D from complex multiplication (CM) points on modular curves.

Let K_D be the following imaginary quadratic field: $K_D = \mathbf{Q}(\sqrt{-|D|})$ if D odd, $\mathbf{Q}(\sqrt{-|D/2|})$ if D is even. The modular parametrization $X_0(32) \to E_1$ (for D odd) or $X_0(64) \to E_2$ (for D even), and CM points on $X_0(2^\bullet)$, yield $P_D \in E_D(\mathbf{Q})$ via points of E_1 or E_2 defined over K_D. If P_D is not in $(E_D(\mathbf{Q}))_{\text{tors}} = E_D[2]$ then $r > 0$.

Temptation: use Gross-Zagier: $\hat{h}(P_D)$ equals $* L'(E_D/\mathbf{Q}, 1)$. Problem: not known for all D, only those D for which 2 splits in K_D, that is, $D \equiv 7 \bmod 8$ and $D \equiv 14 \bmod 16$. Anyway, it takes $|N|^{(1/2)+\epsilon} = |D|^{1+\epsilon}$ time to prove $L'(E_D/\mathbf{Q}, 1) \neq 0$ by direct computation; while $|D|^{1+\epsilon}$ is poly($|D|$), that's still too long.

Fortunately P_D comes from a sum of $h(K_D)$ CM points on E_1 or E_2, and on average $h(K_D)$ grows only as $\sqrt{|D|}$. We regard E_1 and E_2 as complex tori, and use the $\int_\infty^\tau \phi\, dq/q$ formula to approximate each of the $h(K_D)$ points to within say 10^{-25} in time $|D|^\epsilon$. So, on average, we need only $|D|^{(1/2)+\epsilon}$ time to compute P_D to enough precision to prove that it is nontorsion — if it is indeed nontorsion.

If $P_D \in E_D[2]$, this approach fails. But that's exactly when $r > 1$! So, for such D, we revert to the elementary method of proving $r > 0$: we find a rational solution of $Dy^2 = x^3 - x$ with $y \neq 0$.

[To be honest, there are several caveats to our claim that $P_D \in E_D[2] \Longleftrightarrow r > 1$. But to establish Thm.1 we don't actually need to prove this, just to find a single nontorsion point on $E_D(\mathbf{Q})$.

The details: (i) If 2 splits in K_D then not only do we get $\hat{h}(P_D) = 0 \Rightarrow L'(E_D(\mathbf{Q}), 1) = 0 \Rightarrow r_{\text{an}}(E_D/\mathbf{Q}) > 1$ from Gross-Zagier — when we still need BSD to get to $r > 1$ — but we can cite Kolyvagin for the "$\Leftarrow$" direction: if P_D is nontorsion then $r = 1$. If 2 doesn't split, P_D comes from a "mock-Heegner" construction, for which neither G-Z nor Kolyvagin are known but both still seem to hold experimentally.

ii) Conceivably P_D might not really be a torsion point, just very close numerically to a 2-torsion point. Then we could really be sunk. But if $P_D \notin (E_D(\mathbf{Q}))_{\text{tors}}$, we expect P_D's location on $E_D(\mathbf{R})$ to be "random". So, it would take considerable bad luck to have P_D numerically indistinguishable from a 2-torsion point, and we have yet to come close to such misfortune.

Another encouraging sign: in each case where P_D seems to be torsion, $|D|$ is among the minority of $|D|$ values for which the Selmer 2-groups are large enough to allow $r \geq 3$.]

Of the 303979 $\simeq (3\pi^2/8)10^6$ squarefree values of $|D|$ in our range, all but 1375 had P_D at distance at least 10^{-8} from the nearest 2-torsion point. We thus obtain $r > 0$ in each of these $303979 - 1375$ cases.

For each of the remaining 1375 values of $|D|$, there is a 2-torsion point at distance at most 10^{-20} — usually much less — from P_D. We found a nontorsion point on $E_D(\mathbf{Q})$ (exhibited at the abovementioned web pages) for each of these $|D|$, thus completing the proof of Theorem 1.

These rational points were computed as follows. We first found all $x = r/s$ with small $H = \max(|r|, |s|)$ such that $s^4 x = rs(r^2 - s^2)$ is Dz^2 for some $D, z \in \mathbf{Z}$ with $|D| < 10^6$. We can search as far as $H < 5 \cdot 10^7$ in a few hours, because at least two of $r, s, r \pm s$ must have very small squarefree parts: one less than $(4 \cdot 10^6)^{1/4} < 45$, the next less than $(4 \cdot 10^6/f)^{1/3} \leq (4 \cdot 10^6)^{1/3} < 160$.

The resulting list of D's included all but 70 of our 1375 targets. MWRANK disposed of the remaining 70 in a few more hours.

Why stop at 10^6?

The P_D computation can be taken much further. The problem is the rank-3 curves. We can find points of height $|D|^{(1/6)+\epsilon}$ for much larger $|D|$ than points of height $|D|^{(1/2)+\epsilon}$, it still takes time exponential in $|D|^{1/6}$, which does seem prohibitive if we're to reach 10^7.

[The corresponding difficulty in the even-rank case is why Tunnell's conjecture in that case is not yet known even up to 10^5: we can't find rational points of height $|D|^{(1/4)+\epsilon}$ on the curves E_D of rank 2.]

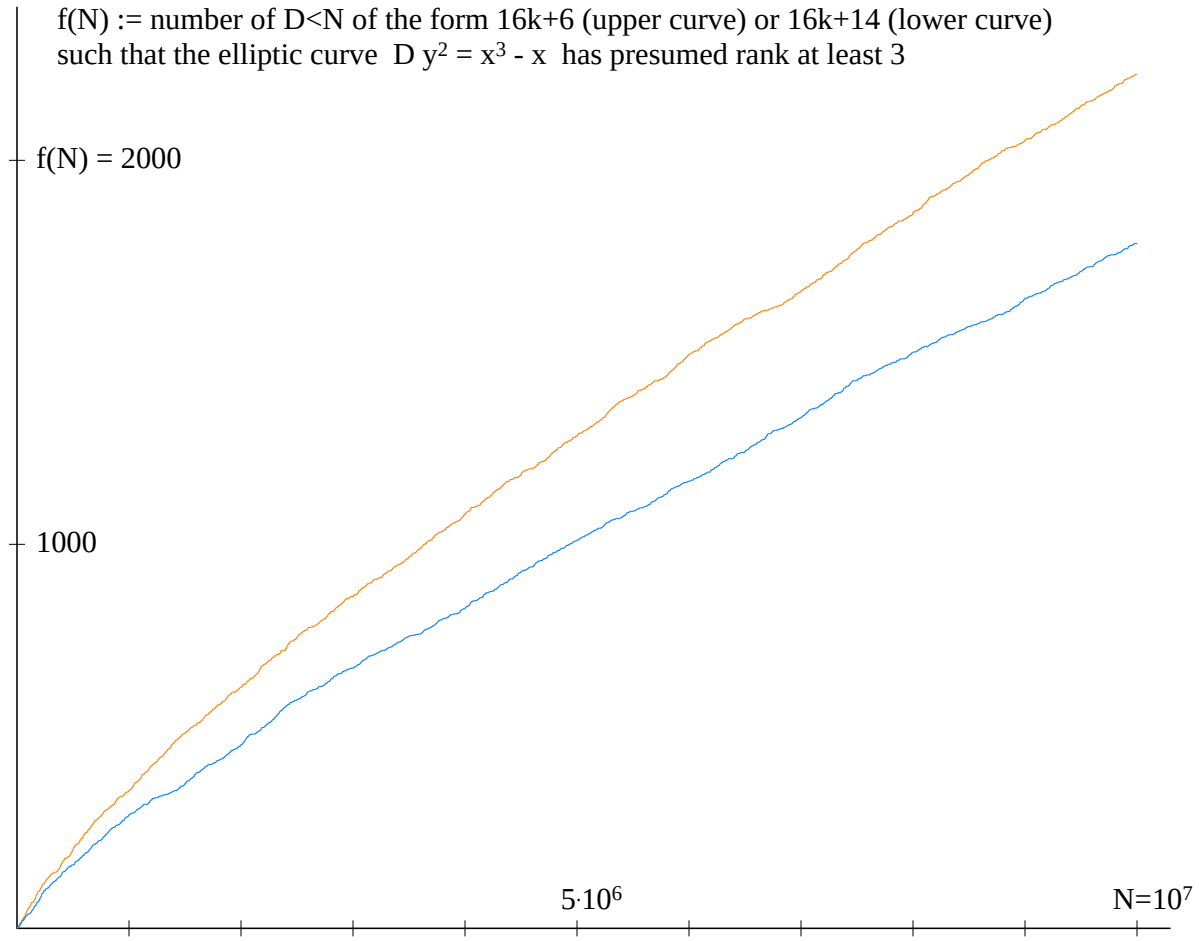
3. Curves E_D of rank 3.

We can still extend to 10^7 the list of $|D|$ for which E_D has conjectural rank at least 3. This requires only the numerical computation of P_D. Moreover, since we no longer care about curves of rank 1, we exclude them a priori by requiring Selmer groups large enough to accommodate a Mordell-Weil group of rank 3. For really large $|D|$, it is known that almost 100% pass this test; but going only through 10^7, only a minority survive. We tabulate their proportions, and the number of $|D|$ of each kind for which the P_D computation indicates rank 3 (total 8740):

$\|D\|$ mod 16	14	6	5, 13	7, 15
survivors	35%	32.1%	21.6%	16.2%
rank 3	2225	1785	2338	2392

Why the disparities? The Selmer bias can be explained by the special role of $2 \in \mathbf{Q}^*/\mathbf{Q}^{*2}$ in the 2-descents; but in the case of odd $|D|$ both residue classes mod 8 have much the same number of rank-3 twists, while in the even case the Selmer bias does not fully account for the preference for twists of rank 3 to have $D \equiv 14 \bmod 16$ rather than 6 mod 16. Please explain!

[We write "rank 3" rather than "$r \geq 3$" because in each case we used the descents-only mode of MWRANK to check that none of these E_D can have rank 5 or greater. The smallest known instance of $r = 5$ has $|D| > 4 \cdot 10^9$ [N.Rogers 2000]. But there are many cases where E_D or one of its three 2-isogenous curves has $r = 3$ and $|Ш[2]| > 1$.]


f(N) := number of D<N of the form 16k+6 (upper curve) or 16k+14 (lower curve)
such that the elliptic curve D y^2 = x^3 - x has presumed rank at least 3
f(N) = 2000
1000
5·10^6
N=10^7