Heegner Point Computations

Noam D. Elkies

Department of Mathematics, Harvard University, Cambridge, MA 02138 USA
elkies@zariski.harvard.edu

Abstract. We discuss the computational application of Heegner points to the study of elliptic curves over $\mathbf{Q}$, concentrating on the curves

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

arising in the "congruent number" problem.[1] We begin by briefly reviewing the cyclotomic construction of units in real quadratic number fields, which is analogous in many ways to the Heegner-point approach to the arithmetic of elliptic curves, and allows us to introduce some of the key ideas in a more familiar setting. We then quote the key results and conjectures that we shall need concerning elliptic curves and Heegner points, and show how they yield practical algorithms for finding rational points on E_D and other properties of such curves. We conclude with a report on more recent work along similar lines on the elliptic curves $x^3 + y^3 = A$.

1 Review: the cyclotomic approach to "Pell's equation"

This classical Diophantine equation[2] asks in effect for nontrivial units u in an order $O = O_D$ in a real quadratic number field K. Here D is the discriminant of O, so $O_D = \mathbf{Z} + \mathbf{Z}w$ where $w = \sqrt{D}/2$ or $(1+\sqrt{D})/2$ according as D is even or odd. It is known that for all D (subject to the usual condition that D is positive, congruent to 0 or 1 mod 4, and not a perfect square), there exists a "fundamental unit" $u_1 = a_1 - b_1 w$ with nonnegative $a, b \in \mathbf{Z}$ such that the group of units in O_D is $\{\pm 1\} \times u_0^{\mathbf{Z}}$. For any unit $u = a - bw$ with $a \geq 0, b > 0$ the rational number a/b approximates w well; indeed $|w - a/b|$ is small enough that all such a/b, and in particular the first one a_1/b_1, are among the rational approximations of w obtained by expanding w in a continued fraction (a.k.a. applying the Euclidean algorithm to 1 and w). Thus the fundamental unit can be readily computed from the continued-fraction expansion of w. At least for

[1] The problem is for which D does E_D have nontrivial rational points, or equivalently positive rank. Such D are called "congruent", because they are precisely the numbers that arise as the common difference ("congruum") of a three-term arithmetic progression of rational squares, namely the squares of $(x^2-2x-1)/2y$, $(x^2+1)/2y$, and $(x^2+2x-1)/2y$. See the Preface and Chapter XVI of [Di] for the early history of this problem, and [Kob] for a contemporary treatment of the curves E_D.

[2] "...the equation $x^2 - Ny^2 = 1$ to which [Pell's] name, because of Euler's mistaken attribution, has remained attached; since its traditional designation as 'Pell's equation' is unambiguous and convenient, we will go on using it, even though it is historically wrong." [We, p.174]

even D, this was first explained by Euler and Lagrange in the late 1760's, though algorithms implementing this method of computing the fundamental unit were known since the age of Fermat in Europe, and centuries earlier in India [We].

Gauss found an alternative construction of units in K. Let ω be a primitive D-th root of unity. Then he showed that K is contained in $\mathbf{Q}(\omega)$, and observed that $(1-\omega^a)/(1-\omega^b)$ is a unit whenever a, b are integers relatively prime to D. A suitable product of these "cyclotomic units" then yields a unit $U \in K$. Such a unit will not in general be fundamental, and indeed it is not a priori obvious that U is not one of the trivial units ± 1; that U is indeed nontrivial was first shown for all D by Dirichlet, who further showed that $U = \pm u_1^{\pm h}$ where $h = h(K)$ is the class number of K by expressing both $h\bigl|\log|u_1|\bigr|$ and $\bigl|\log|U|\bigr|$ in terms of the residue of the zeta function $\zeta_K(s)$ at $s=1$.

This cyclotomic approach, though certainly more circuitous and cumbersome than the usual continued-fraction method, still yields a polynomial-time algorithm for computing both U and u_1. Since the conjugate of U is $\pm U^{-1}$, both $U \pm U^{-1}$ and $(U \mp U^{-1})/\sqrt{D}$ are integers. Thus by merely calculating U *as a real number* to more than $\bigl|\log_{10}|U|\bigr|$ digits we can recognize U as a $\mathbf{Z}$-linear combination of 1 and w. Dirichlet's formula, together with easy upper bounds on $L(1,\chi)$, shows that $\bigl|\log|U|\bigr| \ll D^{1/2+\epsilon}$, so the computation time is dominated by the evaluation of $O(D)$ trigonometric functions to $O(D^{1/2+\epsilon})$ digits and is thus clearly polynomial in D. For instance, if D is prime then we may take

$$U = D^{-1/2}\prod_a (2\sin\frac{a\pi}{D}),$$

the product extending over all positive integers $a < D/2$ that are quadratic residues mod D; e.g. when $D = 1093$ we calculate (in a few CPU seconds on a SUN-4) that

$$\begin{aligned} U \quad &= \qquad\qquad .000000025435427170067\ldots, \\ U^{-1} &= 39315243.000000025435427170067\ldots, \end{aligned}$$

from which U is the unit $(-39315243 + 1189189\sqrt{1093})/2$ of norm -1. The class number h is then the largest integer such that $|U|^{1/h}$ is a unit in K, which again we detect by the integrality of $|U|^{1/h} \pm |U|^{-1/h}$. It quickly follows that having found U we can also determine h and recover u_1 in polynomial time. Returning to our example of $D = 1093$, we see that h must be odd since U has negative norm (this always happens when D is a prime); for $h=3$ we find

$$U^{1/3} = .002940896\ldots, \quad U^{-1/3} = 340.032416171\ldots$$

whence $\sqrt[3]{U} \notin K$, but for $h=5$

$$U^{1/5} = .030275255\ldots, \quad U^{-1/5} = 33.030275255\ldots$$

indicates that $U = [(-33+\sqrt{1093})/2]^5$, and we soon confirm that K has fundamental unit $(33-\sqrt{1093})/2$ and thus that $h(K) = 5$. Indeed it turns out that the prime ideal $(3, (1+\sqrt{1093})/2)$ generates the class group, and its fifth power is the principal ideal $((11-\sqrt{1093})/2)$.

Our use of "polynomial time" here and later requires some comment, since we mean some power of the input D rather than its size $\log(D)$, so that the running time is actually exponential in the size of the input. But the size $\bigl|\log|U|\bigr|$ of the *output* is heuristically expected, and experimentally observed, to be $D^{1/2\pm\epsilon}$. Since it takes at least $\bigl|\log|U|\bigr|$ time just to write U out in full, no algorithm can be expected to run in time less than polynomial in D, so our designation of $D^{O(1)}$ time as "polynomial" appears reasonable. Moreover it is expected that for most D the class number $h(K)$ is small enough that even the fundamental unit u_1 has at least $D^{1/2-\epsilon}$ digits.[3] Admittedly, when (as with $D = 1093$) the fundamental unit is unusually small, the continued-fraction algorithm will find it quickly, taking time polynomial in its size, whereas the cyclotomic approach cannot exploit a small fundamental unit well enough to reduce the running time below a power of D. More generally, even if U is a fundamental unit and thus is not an exact power of a much smaller unit, it may be possible to write U more compactly as a product than in its explicit $a - bw$ form; for instance the fundamental unit

$$9482010153904475351 + 276383546065778460\sqrt{1177}$$

of the quadratic field $\mathbf{Q}(\sqrt{1177})$ of class number 1 equals

$$2^{-50}3^{-13}(31+\sqrt{1177})^2(35+\sqrt{1177})^{13}(37+\sqrt{1177})^7$$

(cf. [Co, 281–282]). If we accept such representations it becomes reasonable to ask for an algorithm faster than $D^{O(1)}$, and indeed Buchmann [Co, 283–289], adapting ideas of Hafner and McCurley ([HMcC], see also [Co, 247–256]) for imaginary quadratic fields, has a factor-base algorithm that finds both the class number and a product form of the fundamental unit in expected time $D^{o(1)}$ subexponential in the input size. When we later consider elliptic curves depending on a parameter D or A, we again expect that the output often has size proportional to a power of that parameter, and thus use "polynomial time" to mean $|D|^{O(1)}$ or $|A|^{O(1)}$. Our method, analogous to the cyclotomic approach to Pell's equation, will require such running times even when the fundamental solutions are unusually small. There is as yet no elliptic-curve analogue known for the continued-fraction approach to Pell's equation, nor a subexponential factor-base method, nor even a more compact representation of large generators. The analogy between Pell's equation and the congruent number problem suggests that progress in these directions may yield not only faster algorithms but also a better theoretical understanding of the arithmetic of elliptic curves.

[3] See [CL] and [Co, 292–293] for these heuristics on the size of $U, h(K), u_1$.

2 Elliptic curves and Heegner points

Let E be an elliptic curve over $\mathbf{Q}$, with L-series (see [Si, App.C, §16])

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

We assume that E is *modular*, i.e. that there exists a nonconstant map from $X_0(N)$ to E defined over $\mathbf{Q}$, or equivalently that

$$\varphi(\tau) := \sum_{n=1}^{\infty} a_n q^n$$

(with $q = \exp(2\pi i\tau)$ as usual) is a modular form of weight 2 for $\Gamma_0(N)$ for some integer N. A modular parametrization $X_0(N) \to E$ can be constructed from φ as follows: regard $X_0(N)$ over $\mathbf{C}$ as the quotient of the upper half-plane by the fractional linear transformations in $\Gamma_0(N)$; then the function[4]

$$I_\varphi(\tau) := 2\pi i \int_{i\infty}^{\tau} \varphi(z)\, dz$$

on the upper half-plane descends to an analytic map from $X_0(N)$ to $\mathbf{C}/L$ for some lattice $L \subset \mathbf{C}$ such that $\mathbf{C}/L$ is isomorphic with E as a Riemann surface.[5] Elliptic curves with complex multiplication, such as our "congruent number" curves

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

are known to be modular, and it is expected but not yet proved that every $E/\mathbf{Q}$ is modular — a seminal conjecture variously credited to Shimura, Taniyama, and/or Weil.

The L-series of a modular elliptic curve can be expressed as a Mellin transform

$$L(E,s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty \varphi(it) t^s \frac{dt}{t}$$

of φ, giving an analytic continuation of $L(E,s)$ to an entire function of s with a functional equation relating $L(E,s)$ and $L(E,2-s)$. The *Birch and Swinnerton-Dyer (BSD) Conjecture* relates the behavior of $L(E,s)$ at the fixed point $s=1$ of the involution $s \leftrightarrow 2-s$ with the arithmetic of $E/\mathbf{Q}$. Let $r = r(E)$ be the rank of the abelian group $E(\mathbf{Q})$ of rational points of E; Mordell showed that this group is finitely generated, so r, the *(arithmetic) rank* of E, is a finite nonnegative integer. The BSD conjecture asserts that r equals the order of vanishing of $L(E,s)$

4 We insert the factor $2\pi i$ because $2\pi i\, dz = dq/q$.

5 Note that L contains, but might be strictly larger than, the period lattice of ϕ; thus it is not claimed that E is the strong Weil curve associated with ϕ, only that it is isogenous to that curve. This requires the isogeny theorem, which for general E is a difficult theorem (due to Faltings) even if we assume the Eichler-Shimura modular theory, but is much easier for curves with complex multiplication such as our E_D.

at $s=1$; that order of vanishing is thus known as the *analytic rank* $r_{\text{an}} = r_{\text{an}}(E)$ of E. The conjecture also expresses the "leading term" $\lim_{s\to 1}(s-1)^{-r_{\text{an}}}L(E,s)$ as a product of invariants of the curve, including notably the *regulator* of $E(\mathbf{Q})$ and the order of the conjecturally finite *Tate-Šafarevič group* $\text{Ш} = \text{Ш}(E)$, analogous to the factors of the regulator and class number in Dirichlet's formula for $L(1,\chi)$. (Unlike the class group, though, Ш is known to have square order if it is finite, because then it carries a nondegenerate alternating pairing.) The parity of r_{an}, and thus conjecturally also of r, depends only on the sign of the functional equation for $L(E,s)$. For the curves E_D, where we may assume that D is a squarefree integer because square factors may be absorbed into y^2, it is known that r_{an} is odd if and only if $|D| \bmod 8$ is 5, 6, or 7. Thus for such D, the arithmetic rank of E_D is conjecturally odd, so in particular positive, whence the Diophantine equation $Dy^2 = x^3 - x$ is expected to have infinitely many nontrivial solutions in rational x, y. The BSD conjecture has almost been proved for modular elliptic curves of analytic rank 0 or 1: it is now known [Kol] that for such curves the arithmetic and analytic ranks are equal, Ш is finite, and the conjectured leading term of $L(E,s)$ at $s=1$ is correct except perhaps for "small" prime factors.

A crucial ingredient in the proof is the construction of a non-torsion point in $E(\mathbf{Q})$ when $r_{\text{an}} = 1$. Recall that $X_0(N) - \{\text{cusps}\}$ parametrizes elliptic curves C with a cyclic subgroup G of order N; over $\mathbf{C}$, the image in $X_0(N)$ of any τ in the upper half-plane corresponds to $C = \mathbf{C}/(\mathbf{Z}+\mathbf{Z}\tau)$ with the cyclic subgroup G generated by $1/N$. A *Heegner point* is a point of $X_0(N)$ parametrizing (C,G) such that C and the quotient elliptic curve C/G are curves with complex multiplication *of the same discriminant*. Let the "CM field" of such a point be the fraction field of the endomorphism ring of C. A Heegner point, and thus also its image $P \in E(\mathbf{C})$, must be defined over some number field (described in detail by the arithmetic theory of complex multiplication); the sum in the group law of E of all the conjugates[6] of P is then a rational point ΣP on E. If $X_0(N_1) \to E_1$ is a modular parametrization of some elliptic curve E_1 of analytic rank 0 which becomes isomorphic with E over some imaginary quadratic field K (so E is a quadratic twist of E_1), then it is sometimes possible to construct a rational point on E from the image $P_1 \in E_1$ of a Heegner point of $X_0(N_1)$ with CM field K: the sum of the $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-conjugates of P_1 will be a torsion point on E_1, but the conjugates *over* K sum to a K-rational point on E_1 which yields a $\mathbf{Q}$-rational point $\Sigma_1 P_1$ on E. For our curves E_D of odd analytic rank this happens when D is odd using $N_1 = 32$ and

$$E_1 : y^2 = x^3 - x$$

and $K = \mathbf{Q}(\sqrt{-|D|})$ [note that in our family E_D and E_{-D} are isomorphic elliptic curves over $\mathbf{Q}$, since $(x,y) \leftrightarrow (-x,y)$ maps one to the other — in general any CM

[6] More precisely, the sum of the images of conjugates of the Heegner point: it is conceivable that P might be defined over a smaller number field, and thus have fewer conjugates, but then each one is counted several times in the sum. Likewise for the variant construction using quadratic twists, and the computations described in the next section.

elliptic curve over $\mathbf{Q}$ is isogenous with its twist by the CM field]; this indeed was the original setting for Heegner's construction [He], later amplified and extended by Birch [Bi1, Bi2]. When $D \equiv 6 \bmod 8$ a similar construction [Mo] works with E_1 replaced by E_2 and $N_1 = 64$ instead of 32.

Our rational point ΣP or $\Sigma_1 P_1$ on E need not in general be a generator of $E(\mathbf{Q})$ mod torsion, and indeed our construction does not preclude the possibility of finding only a trivial (torsion) point. Occasionally (e.g. for $\Sigma_1 P_1$ on E_D with $D \equiv 7 \bmod 8$ prime) triviality may be ruled out by a parity argument, analogous to the observation that when a cyclotomic unit has norm -1 it cannot be a root of unity. A more powerful tool is Gross and Zagier's result [GrZ], analogous to but much harder than Dirichlet's class number formula, which shows that the canonical height of this point is proportional to $L'(E,1)$. Thus the Heegner-Birch construction, which can be applied to any modular elliptic curve of odd analytic rank, yields a nontorsion point only when $L'(E,1) \neq 0$, i.e. when $r_{\mathrm{an}} = 1$. Comparing the Gross-Zagier formula with the BSD conjecture one further finds[7] that when $r_{\mathrm{an}} = 1$ the height of that point should be $|Ш|$ times the height of a generator of $E(\mathbf{Q})$ mod torsion, which means that the Heegner-point construction yields the $\pm\sqrt{|Ш|}$ multiple of the generator up to torsion.

3 Heegner-point computations for E_D

As was true for the cyclotomic and fundamental units of a real quadratic field, we can compute, in time polynomial in $|D|$, the point $\Sigma_1 P_1$ on E_D, and (provided $\Sigma_1 P_1$ is not a torsion point) also a fundamental solution and thus the conjectural size of Ш. Here "computing" a rational point means exhibiting its coordinates as rational numbers. Nevertheless, as in the computation of U, it will be enough to compute those coordinates as real numbers to sufficient accuracy: $O(H+1)$ digits, where H is either the naïve or the canonical logarithmic height of $\Sigma_1 P_1$, determine the numerators and denominators via the Euclidean algorithm. By the Gross-Zagier formula, the canonical height of $\Sigma_1 P_1$ is proportional to $\sqrt{|D|} \cdot L'(E_D, 1)$; one readily shows that $L'(E_D, 1)$, and thus also H, is bounded by a power of D, so we need only compute $\Sigma_1 P_1$ to $|D|^{O(1)}$ digits. One expects that $L'(E_D, 1)$ (and indeed the r-th derivative of $L(E_D, s)$ at $s = 1$ for any fixed r) is actually bounded by $O_\epsilon(|D|^\epsilon)$ for all $\epsilon > 0$, as was true for the residue at $s=1$ of $\zeta_K(s)$ with $K = \mathbf{Q}(\sqrt{+|D|})$, and thus that $H \ll_\epsilon |D|^{1/2+\epsilon}$, but this has not yet been proved.

Let $K = \mathbf{Q}(\sqrt{-|D|})$ as before, with D odd. The prime 2 splits or ramifies in K according as $|D| \equiv 7$ or $|D| \equiv 5 \bmod 8$. We shall henceforth assume that $|D| \equiv 7 \bmod 8$, the other case being similar but somewhat more delicate. Then the number of conjugates of P_1 over K is the class number of K, and is thus

[7] At least for the curves E_D with D prime; for general E, the factor $\sqrt{|Ш(E)|}$ must be multiplied by $\sqrt{|Ш(E_1)|}$ and perhaps by products of small primes. With our $E_1 : y^2 = x^3 - x$ the BSD conjecture predicts that $|Ш(E_1)| = 1$; this was proved by Rubin [Ru].

$O(|D|^{1/2}\log|D|)$. These conjugates may be exhibited explicitly as follows: let O be the ring of integers of K, and $I \subset O$ the fifth power of one of the two ideals of O lying above 2; thus $O/I \cong \mathbf{Z}/32$. For each ideal class of K choose a representative ideal J. Fix an imbedding of K in $\mathbf{C}$; then each J is a lattice in $\mathbf{C}$ determined up to homothecy, and IJ is a sublattice with $J/IJ \cong O/I \cong \mathbf{Z}/32$. For each J we regard $\mathbf{C}/J$ and $\mathbf{C}/IJ$ as elliptic curves with complex multiplication of discriminant $-|D|$, and J/IJ as a cyclic subgroup of $\mathbf{C}/IJ$, whence $(\mathbf{C}/IJ, J/IJ)$ yields a Heegner point on $X_0(32)$. The images of these points under the modular parametrization $X_0(32) \to E_1$ are then the conjugates of P_1. It is easy to compute in polynomial time the ideal I and representatives J of all ideal classes, and thus also the Heegner points as points $\tau \in K$ in the upper half-plane. Thus it remains only to compute for each such τ the image on E_1 of the corresponding point on $X_0(32)$.

We may compute these images either as complex solutions (x, y) of the cubic equation $y^2 = x^3 - x$, or as points on the complex torus $\mathbf{C}/L$. The latter approach is more convenient since we will have to sum many such points and adding complex numbers mod L is easier than the addition law on E_1; also the $\mathbf{C}/L$ approach directly generalizes to quadratic twists of other modular elliptic curves. At any rate the generators of L and the elliptic functions giving (x, y) as functions on $\mathbf{C}/L$ can be easily computed to arbitrary precision in polynomial time, so we may compute on $\mathbf{C}/L$ and recover (x, y) at the end. We noted already that the image of τ on $\mathbf{C}/L$ is $I_\varphi(\tau) \bmod L$. We integrate φ termwise to find

$$I_\varphi(\tau) = \sum_{n=1}^{\infty} \frac{a_n}{n} q^n = q - \frac{2}{5}q^5 - \frac{3}{9}q^9 + \frac{6}{13}q^{13} \cdots .$$

For our curve E_1 the coefficients a_n can be rapidly computed from either a product or a sum expansion of φ:

$$\varphi = \eta_4^2 \eta_8^2 = q \prod_{m=1}^{\infty} \left[(1 - q^{4m})(1 - q^{8m})\right]^2 = \sum_{m_1, m_2} m_1 q^{m_1^2 + m_2^2},$$

where the sum runs over all $m_1, m_2 \in \mathbf{Z}$ such that m_1 is odd, m_2 is even, and $m_1 \equiv m_2 + 1 \bmod 4$. Each of the coefficients a_n/n in the expansion of $I_\varphi(\tau)$ is of absolute value at most 1 (indeed $a_n \ll_\epsilon n^{1/2+\epsilon}$), so the sum of the first $O(H/\log(|q|^{-1})) = O(H/\mathrm{Im}(\tau))$ terms $(a_n/n)q^n$ already gives $I_\varphi(\tau)$ to the required precision $\exp(-O(H))$. Thus we conclude that the entire computation can be done in polynomial time provided we have a polynomial upper bound on $1/\mathrm{Im}(\tau)$.

Now τ is only defined up to a fractional linear transformation in $\Gamma_0(32)$, corresponding to a choice of generators for the lattice IJ. It is not hard to choose these generators to make $\mathrm{Im}(\tau) \gg |D|^{-1/2}$, which is enough to compute $\Sigma_1 P_1$ in polynomial time; but in fact we can always choose an equivalent τ with imaginary part $> 1/8$. This is because in addition to the invariance of $\varphi(z)\,dz$ under $\Gamma_0(32)$ the modular form φ also satisfies

$$\varphi\left(z + \frac{1}{4}\right) = i\varphi(z), \qquad \varphi\left(-\frac{1}{32z}\right) = -\frac{1}{32z^2}\varphi(z),$$

whence I_φ satisfies the identities

$$I_\varphi\left(\tau+\frac{1}{4}\right)=iI_\varphi(\tau), \qquad I_\varphi\left(-\frac{1}{32\tau}\right)=2I_\varphi(\frac{i}{\sqrt{32}})-I_\varphi(\tau),$$

and the transformations $\tau\mapsto\tau+1/4$ and $\tau\mapsto -1/32\tau$ generate an arithmetic subgroup of $\mathrm{PSL}_2(\mathbf{Q})$ with fundamental domain

$$\{z:|\mathrm{Re}(z)|\leq\frac{1}{8},\,|z|^2\geq\frac{1}{32}\}\,.$$

(For a general modular elliptic curve of conductor N_1 such a trick is not available, but could still find an image of any τ under $\Gamma_0(N_1)$ that is close enough to some cusp to compute $I_\varphi(\tau)$ by one of a finite list of q-expansions with $\log|1/q|\gg 1/N_1$, the implied constant not depending on D.) So the computation of $\Sigma_1 P_1$ takes time polynomial in $|D|$ as claimed.

We further find that the most time-consuming part of the computation is the calculation of $O(|D|^{1/2}\log|D|)$ values of I_φ, each of which requires on the order of H arithmetic operations to as many digits of precision; if $H\ll_\epsilon |D|^{1/2+\epsilon}$ as expected then the entire computation takes time $O_\epsilon|D|^{2+\epsilon}$, or $O_\epsilon|D|^{3/2+\epsilon}$ with fast multiplication and division. Moreover, the space requirement is only a constant multiple of the $\max(H,\log|D|)$ needed just to write down D and the digits of $\Sigma_1 P_1$. It may seem that we must know H in advance to achieve this, but we can get around this as follows: perform the computation assuming $H<2$; if it fails (as it most likely will unless $r_{\mathrm{an}}>1$), start anew with the assumption $H<4$; then try $H<8$, $H<16$, etc. until the first success. In practice we initially assume that H is less than a small multiple of $\sqrt{|D|}$, set the precision accordingly, and increase it (or check for bugs!) if no suitable rational approximation to the coordinates of $\Sigma_1 P_1$ is found.

If $r_{\mathrm{an}}=1$, i.e. if $\Sigma_1 P_1$ is not a torsion point, then we can find a fundamental solution, and thus the conjectural $|Ш|$, by trying to divide $\Sigma_1 P_1$ by $S=2,3,\cdots$ in $E_D(\mathbf{Q})$. For each S there are at most $2S$ points $(\Sigma_1 P_1)/S$ on $E_D(\mathbf{R})$, which we can conveniently calculate from our $\mathbf{C}/L$ representation of $\Sigma_1 P_1$. If one of them is rational it has height $\ll H/S^2$; thus it is enough to try all $S\ll\sqrt{H}$, and we find that the recovery of the generator takes less time than the computation of $\Sigma_1 P_1$. For instance when $|D|$ is the prime 751 we compute $\Sigma_1 P_1$ in less than one SUN-4 CPU minute, and in a few more seconds find that $S=3$ and that $751y^2=x^3-x$ has fundamental solution

$$(x,y)=(\frac{323761}{17^2 751},\frac{136696560}{17^3 751^2}).$$

It is actually quite rare to find D such that $\Sigma_1 P_1$ is not the fundamental solution or its 2^s-th multiple for small s: usually (assuming the BSD conjecture) Ш is either trivial or a 2-group accounted for entirely by the 2-descent. For instance, of the 565 curves E_D with $|D|<20000$ a prime congruent to 7 mod 8 (such for such D it is known that the 2-part of $Ш(E_D)$ is trivial), only 24 have $S=3$, of which 751 is the first example; in that range there are no instances of $S=5$ or greater, the first one occurring at $|D| = 26423$. (For $|D| \equiv 5 \bmod 8$, the smallest primes with $S = 3$, $S = 5$ are 1493, 12269.) When $r_{\text{an}} = 1$, the generator typically has about $\sqrt{|D|}$ digits, and then the algorithm outlined above is the fastest known for computing it: as noted already, there is as yet no known analogue for E_D to the continued-fraction approach to Pell's equation (for which again the class number is usually 1 or a small power of 2, and fundamental units often have about $\sqrt{D}$ digits), and the traditional approach of making a few 2-descents and then searching exhaustively takes time exponential in $\sqrt{|D|}$. In practice the 2-descents also significantly streamline the computation of $\Sigma_1 P_1$ by reducing the precision required; e.g. if $|D| \equiv 7 \bmod 8$ is prime then the x-coordinate of $\Sigma_1 P_1$ must be of the form $x = (D^2 X^4 + 1)/(2DX^2)$ for some rational X which has only about $1/4$ as many digits as x. This allowed us to compute that the x-coordinate of a generator of $E_{1063}(\mathbf{Q})$ mod torsion is $(1063^2 X^4 + 1)/(2 \cdot 1063 X^2)$ where

$$X = \frac{11091863741829769675047021635712281767382339667434645}{317342657544772180735207977320900012522807936777887},$$

a solution so large that to date it could not have been computed except by Heegner-point methods.

If $r_{\text{an}} > 1$ then $H = 0$ and $\Sigma_1 P_1$ is a torsion point. This can be detected by computing $\Sigma_1 P_1$ to low precision (in practice 19 digits, and a threshold of 10^{-12}, are more than enough) because there are only four rational torsion points on E_D. This is a very fast computation, requiring time only $O_\epsilon(|D|^{1/2+\epsilon})$, much less than the $O_\epsilon(|D|^{1+\epsilon})$ required to calculate $L'(E_D, 1)$ directly as in [BGZ]. We were thus able screen all squarefree $|D| < 2 \cdot 10^5$ congruent to 7 mod 8, and found that only 75 had $r_{\text{an}} \geq 3$, of which the smallest are

$$4199 = 13 \cdot 17 \cdot 19, \quad 4895 = 5 \cdot 11 \cdot 89, \quad \text{and} \quad 6671 = 7 \cdot 953.$$

For $|D| \equiv 5 \bmod 8$ we find 89 examples in the same range, beginning with

$$2605 = 5 \cdot 521, \quad 4669 = 7 \cdot 23 \cdot 29, \quad \text{and} \quad 8005 = 5 \cdot 1601;$$

and there are 173 examples with $|D| \equiv 6 \bmod 8$, starting with

$$1254 = 2 \cdot 3 \cdot 11 \cdot 19, \quad 2774 = 2 \cdot 19 \cdot 73, \quad 3502 = 2 \cdot 17 \cdot 13.$$

We have checked that in the first few cases the curve E_D has arithmetic rank 3. (See also [GeZ, p. 81].) The heuristics used above to surmise $H \ll_\epsilon |D|^{1/2+\epsilon}$ when $r(E_D) = 1$ indicate that if $r(E_D) \geq 3$ then E_D should have a nontorsion point of height $O_\epsilon(|D|^{1/6+\epsilon})$, considerably smaller than in the rank-1 case. Indeed on each of our $75 + 89 + 173$ curves E_D with analytic rank at least 3 we were able to find at least one nontorsion point by a rather simple-minded numerical search. Having already computed a nontorsion point such as $\Sigma_1 P_1$ on E_D for all other $|D| < 2 \cdot 10^5$ congruent to 5, 6, or 7 mod 8, we deduce that E_D has positive rank for all $|D| < 2 \cdot 10^5$ such that the functional equation of $L(E_D, \cdot)$ has sign -1.

4 The twisted Fermat cubics $x^3 + y^3 = A$

The question of which numbers can be written as the sum of two rational cubes leads to the family of elliptic curves

$$\mathsf{E}_A : x^3 + y^3 = A.$$

We take the point at infinity as the origin of the curve. By absorbing cubic factors in A into x, y we may assume that A is a positive cube-free integer; we also assume that $A \geq 3$, since it is well known that other than the point at infinity $(1,1)$ is the only rational point on E_2, and $(1,0)$, $(0,1)$ the only rational points on E_1, the latter being of course the exponent-3 case of Fermat's "Last Theorem". For $A \geq 3$ the torsion group of E_A is trivial ([Se, p.212], attributed to A. Hurwitz), so A is the sum of two rational cubes if and only if E_A has positive arithmetic rank.

The family of curves E_A recalls in many ways the family of curves E_D of the last two sections; each E_A is an elliptic curve with complex multiplication and a twist (cubic, not quadratic) of a curve E_1 admitting a simple modular parametrization, this time by $X_0(27)$. The parity of $r_{\text{an}}(\mathsf{E}_A)$ was computed by Birch and Stephens [BS]; in particular if $A > 3$ is prime, $r_{\text{an}}(\mathsf{E}_A)$ is odd precisely when A is congruent to 4, 7, or 8 mod 9, and the same is true of $r_{\text{an}}(\mathsf{E}_{A^2})$. Thus Birch and Stephens conjectured that every prime $p \equiv 4$, 7, or 8 mod 9 can be written as a sum of two rational cubes, a conjecture prefigured by Selmer [Se] and traditionally ascribed to Sylvester. We have proved this conjecture for the first two cases $p \equiv 4, 7 \bmod 9$, and also shown that p^2 is a sum of two cubes for any such p; e.g. for $p = 337$ the smallest solution is

$$337^2 = \frac{7773971682119096^3 - 5751462787384249^3}{135022593649447^3}.$$

One might try to construct points on E_p by mimicking the Heegner-Birch approach to E_D: find a combination of CM points on $X_0(27)$ that sum to a point on E_1 defined over $\mathbf{Q}(\sqrt[3]{p})$. Indeed a similar construction starting from the parametrization $X_0(36) \to \mathsf{E}_2$ yields non-torsion points on E_{2p} for certain primes p [Sa]. But all attempts to construct rational points on E_p along similar lines have produced only the zero point, a fact Gross can now predict from a conjectured generalization of the Gross-Zagier formula. This generalization also suggested how to modify the CM construction to obtain nontrivial points on E_p. Let ϖ be one of the prime factors of p in $\mathbf{Z}[e^{2\pi i/3}]$, chosen so that $\varpi \equiv 1 \bmod 3$. Then the curve E_ϖ has a modular parametrization by $X_1(9p)$ or $X_1(27p)$ defined over $\mathbf{Q}(e^{2\pi i/3})$. We find a point on the modular curve parametrizing a cyclic isogeny between elliptic curves with complex multiplication of discriminant -27, and show that the image of this point on E_ϖ is a nontorsion point defined over $\mathbf{Q}(e^{2\pi i/3}, \sqrt[3]{\bar{\varpi}})$ which yields a nontrivial point of $\mathsf{E}_{\varpi\bar{\varpi}} = \mathsf{E}_p$ defined over $\mathbf{Q}$. Likewise we construct a nontrivial point of $\mathsf{E}_{p^2}(\mathbf{Q})$ from a modular parametrization of E_{ϖ^2}. As in the previous section we find that this yields a practical algorithm with running time polynomial in p, dominated this time by

$O(pH)$ arithmetic operations to $O(H)$-digit precision, where H is the height of the constructed point, expected to be $O_\epsilon(p^{1/3+\epsilon})$ or $O_\epsilon(p^{2/3+\epsilon})$ for E_p, E_{p^2} respectively. This point should again be the $S = \pm\sqrt{|Ш|}$ multiple of the generator of $\mathsf{E}_p(\mathbf{Q})$ or $\mathsf{E}_{p^2}(\mathbf{Q})$, where S is usually 1 but occasionally larger: on E_{547} and E_{229^2} (the smallest instances) our construction gives not the generators

$$547 = 14^3 - 13^3, \quad 229^2 = \frac{154699^3 - 69515^3}{4004^3},$$

but twice those points, so we guess that $|Ш| = 4$ in these cases. So far no higher multiples have been observed, though presumably S and $|Ш|$ can be arbitrarily large.

Acknowledgements

Thanks to Benedict Gross for introducing me to the arithmetic of elliptic and modular curves and for many enlightening conversations on the Heegner-point construction and its variations. This work was made possible in part by funding from the Harvard Society of Fellows, the National Science Foundation, and the Packard Foundation; some of the computations were carried out using the GP/PARI and MACSYMA packages.

References

[Bi1] Birch, B.J.: Elliptic curves and modular functions. *Symp. Math.* **4** (1970), 27–37.

[Bi2] Birch, B.J.: Heegner points of elliptic curves. *Symp. Math.* **15** (1975), 441–445.

[BS] Birch, J., Stephens, N.M.: The parity of the rank of the Mordell-Weil group. *Topology* **5**, 295–299 (1966).

[BGZ] Buhler, J.P., Gross, B.H., Zagier, D.: On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3. *Math. of Computation* **44** (1985) #175, 473–481.

[Co] Cohen, H.: *A course in computational algebraic number theory.* Berlin: Springer 1993.

[CL] Cohen, H., Lenstra, H.W.: Heuristics on class groups of number fields. Lect. Notes in Math. **1068** (1984: Proceedings of Journées Arithmétiques 1983 at Noordwijkerhout), 33–62.

[Di] Dickson, L.E.: *History of the Theory of Numbers, Vol. II: Diophantine Analysis.* New York: Stechert 1934.

[GeZ] Gebel, J., Zimmer, H.G.: Computing the Mordell-Weil Group of an Elliptic Curve over **Q**. *CRM Proc. & Lect. Notes* **4** (1994), 61–83.

[GrZ] Gross, B.H., Zagier, D.: Heegner points and derivatives of L-series. *Invent. Math.* **84** (1986), 225–320.

[HMcC] Hafner, J., McCurley, K.: A rigorous subexponential algorithm for computation of class groups. *J. AMS* **2** (1989), 837–850.

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

[Kob] Koblitz, N.: *Introduction to elliptic curves and modular forms.* New York: Springer 1984.

[Kol] Kolyvagin, V.A.: Euler systems. Pages 435–483 of *The Grothendieck Festscrhift* Vol. II, Birkhäuser: Boston 1990.

[Mo] Monsky, P.: Mock Heegner points and congruent numbers. *Math. Z.* **204** (1990) #1, 45–67.

[Ru] Rubin, K.: Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. *Invent. Math.* **89** (1987), 527–560

[Sa] Satgé, Ph.: Un analogue du calcul de Heegner. *Invent. Math.* **87**, 425–439 (1987).

[Se] Selmer, E.S.: The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.* **85**, 203–362 (1951).

[Si] Silverman, J.H.: *The Arithmetic of Elliptic Curves.* New York: Springer 1986.

[We] Weil, A.: *Number theory: An approach through history; From Hammurapi to Legendre.* Boston: Birkhäuser, 1983.

This article was processed using the LaTeX macro package with LLNCS style