MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 111-115

THREE POINTS OF GREAT HEIGHT ON ELLIPTIC CURVES

ANDREW BREMNER AND DUNCAN A. BUELL

For D. H. Lehmer, and his love of numbers

ABSTRACT. We give three elliptic curves whose generators have great height, demonstrating along the way a moderately efficient method for finding such points.

1. INTRODUCTION

Let $p \equiv 5 \pmod 8$ be a prime number. Bremner and Cassels have verified that the rank of the Mordell-Weil group of the elliptic curve

$$Y^2 = X(X^2 + p)$$

over $\mathbb{Q}$ is 1, for $p < 1000$ [2], and Bremner has extended this to $p < 20000$ [1]. For all $p < 5000$ except for $p = 3917$, 4157, and 4957, explicit coordinates of a generator are known. In this paper we fill in these gaps by presenting the coordinates of generators for the Mordell-Weil groups of the following curves:

$$\text{For} \quad Y^2 = X(X^2 + 3917)$$

$$X = \frac{\begin{array}{r} 1\ 3191326145\ 6422472921 \\ 5873290251\ 8863871195\ 1947136699\ 2233127128\ 9213974121 \end{array}}{\begin{array}{r} 548834475\ 8892451852 \\ 7451707440\ 2156457012\ 3908977288\ 1880026829\ 0258264900 \end{array}}$$

$$Y = \frac{\begin{array}{r} 422605 \\ 7873470623\ 6958538698\ 4222606144\ 1026117548\ 7546042859 \\ 8908260829\ 3814216233\ 8843167731\ 8301133130\ 4053463581 \end{array}}{\begin{array}{r} 1285 \\ 7664123892\ 6034798978\ 3481163135\ 9345003535\ 1077250240 \\ 1959049281\ 1437042584\ 0089183445\ 3200116260\ 9377357000 \end{array}}$$

$$\text{For} \quad Y^2 = X(X^2 + 4157)$$

$$X = \frac{\begin{array}{r} 5332499248\ 7599063389 \\ 1066356325\ 7642601861\ 0337363601\ 2044939282\ 4882088521 \end{array}}{\begin{array}{r} 44003585\ 6451313819 \\ 9226472581\ 4648511569\ 0449920470\ 8057736801\ 3774720100 \end{array}}$$

Received by the editor July 15, 1991 and, in revised form, April 23, 1992.
1991 *Mathematics Subject Classification*. 11G05, 14H52, 11-04.
Key words and phrases. Elliptic curves, Mordell-Weil group, descent.

$$Y = \frac{\begin{array}{r} 44108 \\ 4155760469\;\; 7993705069\;\; 3168537280\;\; 6635440124\;\; 9847767197 \\ 2013041097\;\; 2556677066\;\; 6836701935\;\; 5981000014\;\; 3598411181 \end{array}}{\begin{array}{r} 29 \\ 1898658996\;\; 7029975275\;\; 2870403348\;\; 9392140054\;\; 6948318468 \\ 1015324839\;\; 9597607540\;\; 4475037731\;\; 3582116884\;\; 4060801000 \end{array}}$$

For $Y^2 = X(X^2 + 4957)$

$$X = \frac{\begin{array}{r} 2578\;\; 6593364983\;\; 8869943482\;\; 2726741534 \\ 8642803837\;\; 2862724530\;\; 1355555758\;\; 7191972747\;\; 6066494521 \end{array}}{\begin{array}{r} 2\;\; 7544734678\;\; 8209581109\;\; 2823066215 \\ 4526375537\;\; 5984629139\;\; 2220985954\;\; 5339442186\;\; 6359716100 \end{array}}$$

$$Y = \frac{\begin{array}{r} 131315\;\; 4053999120\;\; 5952869312 \\ 1641825016\;\; 9330523130\;\; 1417335322\;\; 2596278362\;\; 4828231988 \\ 0210527534\;\; 7918347549\;\; 9579064513\;\; 0766126108\;\; 4369453931 \end{array}}{\begin{array}{r} 4\;\; 5714912217\;\; 3449737242 \\ 8932870955\;\; 5522703332\;\; 6956396590\;\; 2104635417\;\; 4424919684 \\ 8609580514\;\; 6737003842\;\; 7423528188\;\; 6907027288\;\; 7875659000 \end{array}}$$

The respective (canonical) heights of these points [1] are approximately 162.61, 160.83, and 192.10.

2. Computation

The method of descent outlined in [1] leads us to search for simultaneous solutions r, s, t, u to pairs of equations.

For $p = 3917$:

(2.1) $2(r^2 - s^2) - 10rs - 3(ru + st) + 10(rt - su) + 3(t^2 - u^2) + 2tu = 0,$

(2.2) $7(r^2 - s^2) - \; 2rs + 2(ru + st) - \; (t^2 - u^2) = 0.$

For $p = 4157$:

(2.3) $32(r^2 - s^2) - 382rs - 27(ru + st) - 12(rt - su) - (t^2 - u^2) - 2tu = 0,$

(2.4) $203(r^2 - s^2) + \; 26rs + \; 2(ru + st) - (t^2 - u^2) = 0.$

For $p = 4957$:

(2.5) $16rs - 3(ru + st) - 4(rt - su) + (t^2 - u^2) = 0,$

(2.6) $4(r^2 - s^2) + \; 6rs + 2(ru + st) - (t^2 - u^2) + 2tu = 0.$

We will illustrate the computational method using $p = 3917$ as an example.

For $p = 3917$ we are searching for simultaneous solutions r, s, t, u to the pair of equations (2.1) and (2.2). From the known height of the generator (see [1]) we expect a solution to exist in the approximate range

$$0 \le |r|, |s|, |t|, |u| \le 17000.$$

A brute force search over $34^4 \cdot 10^{12} \approx 1.3 \cdot 10^{18}$ possible quadruples would be infeasible, so it is fortunate that it is not necessary.

We rewrite (2.2) in a manner more amenable to computation:

(2.7) $$(t - s)^2 = (u + r)^2 + 6(r^2 - s^2) - 2rs = (u + r)^2 + K.$$

Simplification 1: Symmetry. *We need only search over* $r \geq 0$, $s \geq 0$.

This is because under $(r, s) \to (-r, -s)$ we have $K \to K$, and under $(r, s) \to (s, -r)$ or $(r, s) \to (-s, r)$ we have $K \to -K$. We will search only over nonnegative r and s and then solve (2.7) as $N^2 = M^2 + |K|$. We will then let $u + r = \pm M$ and $t - s = \pm N$ or the reverse, whichever is appropriate.

Simplification 2: Congruences. *Most* r, s *pairs can be eliminated by congruence conditions.*

By analysis or simply by enumeration, we find that only 9 of the 25 possible pairs (r, s) modulo 5 can be completed to a quadruple (r, s, t, u) which solves both (2.1) and (2.2) when treated as congruences and not equations. Further, only 13 of 49 pairs modulo 7, 73 of 169 pairs modulo 13, and 129 of 289 pairs modulo 17 can be completed. Working modulo 8, we find also that r and s must both be even.

In fact, we can sieve out the impossible (r, s) pairs for primes q as high as we wish, provided we can store and access a $q \times q$ bit matrix to determine by table lookup whether a pair is possible. Using the primes through 47, we find that of the 289 million potential pairs (r, s) only 25153, or 87 per million, pass all the sieve tests to generate values of K for which $N^2 = M^2 + |K|$ need be solved. Our experience on these three curves is that, for most of the small primes, between 30% and 60% of the potential pairs are impossible for each prime. Even with bad luck, then, for every two primes used in the sieve, the number of possible pairs is reduced at least by half.

A search for solutions to $N^2 = M^2 + |K|$ is especially simple. Given $|K|$, the smallest choice of N is $[\sqrt{|K|}] + 1$, and we compute N^2 by multiplication only for this smallest N. As we loop on M from 1 to some limit, then, we can update the values of the right- and left-hand sides without multiplying, using the standard formula $(x + 1)^2 = x^2 + x + x + 1$. When we update M and the right-hand side, if this is larger than the current left-hand side, we simply update the left-hand side until it is no longer smaller. For large M and N these will be alternating operations and thus will be very efficient. For two of the three curves here, it can also be determined that M is even and N odd. This further limits the search.

With these simplifications, a C program running on the CRAY 2 at SRC tests r in a block of 1000 integers and all s from 0 through 17000 in about 80 seconds of CPU time (on one head of the CRAY 2). Our program was moderately efficient but not extraordinarily so, and improvements in speed certainly could have been made. Using this program, we find that

$$(r, s, t, u) = (2684, 7586, 5487, -21317)$$

is the desired solution.

The computation for $p = 4157$ is entirely similar, and we obtain the solution

$$(r, s, t, u) = (9940, 1222, -140939, -25343).$$

In this case, there were 68013 pairs (r, s) which passed the sieve, and the program ran about 50% slower than for $p = 3917$.

For $p = 4957$ rewrite (2.6) as

$$(2t + r - s)^2 = 2 \cdot (u + t + r)^2 + 7(r^2 - s^2) + 10rs.$$

A first search, with r and s bounded above in absolute value by 17000 as with the previous two curves, failed to find a point. We therefore increased the bounds to 25000, and the bounds on N and M to 300000. At this point, only 92417 pairs (r, s) pass through the sieve, and we find the solution

$$(r, s, t, u) = (20147, 7406, 43588, -8808).$$

3. A general method, and the "next" case

The general method we have employed should be apparent. By manipulating or combining the two quadratic polynomials in four variables, we create a single equation of the form

$$AN^2 = BM^2 + K. \tag{3.1}$$

In this equation, we have made K a function of only two of the variables and arranged it so that the other two do not both appear in N and M. This allows us, having solved (3.1), to extract the third and fourth variables without further search. With a judicious choice of A and B in (3.1) ($A = B = 1$ is clearly best possible), the search for solutions to (3.1) can be made very efficient.

The limitations of our method become apparent, however, when we apply it to the "next" hard curve, $Y^2 = X(X^2 + 17477)$; see [1].

The descent argument leads to the pair of equations

$$r^2 - s^2 + 11(ru + st) - 3(rt - su) - 2(t^2 - u^2) - 2tu = 0, \tag{3.2}$$

$$r^2 - s^2 + 6rs + \ t^2 - u^2 + 2tu = 0, \tag{3.3}$$

and (3.3) diagonalizes to the very simple

$$(t + u)^2 = 2u^2 + s^2 - 6rs - r^2. \tag{3.4}$$

However, the estimated bounds on the variables are now on the order of 10^{10}. Sieving with the 25 primes less than 100, we find that about 1.75 pairs (r, s) per million pass through the sieve. If each of the next 75 primes had a (pessimistic) sieve success fraction of .7, and we use exactly 10^{10} as a loop bound, we would need to test only 422 pairs in the inner loop. This number of pairs is not extraordinary, although the enumeration of the pairs could not be done simply by counting but would require incorporating the sieve into the loops. With the inner loop, however, now on the order of 10^{10} instead of 10^4, the feasibility of this computation would depend very much on the number of pairs to be tested staying small. The sieving can be expected to be more successful, so that the estimate of 422 pairs is no doubt high, but this gain could be offset if the estimate of 10^{10} for the loop bound is low by one or two orders of magnitude in each variable. We strongly suspect that finding a solution this way is out of reach, certainly without the expenditure of an estimated three years of CPU time, which is clearly unwarranted.

With sufficient courage, a further descent could be carried out on the pair of equations (3.2, 3.3) by looking for a linear combination of the two quadrics which is singular (singular combinations in fact exist over the field $\mathbb{Q}(\sqrt{106 - 79i})$). However, the details are sufficiently laborious that we have not attempted to carry them through.

The referee has convincingly pointed out to us the merits of calculation using Heegner points, where finding a point on a curve of rank 1 can be expected to be an operation which is polynomial in the conductor, as opposed to exhaustive search, which can be exponential. For the family of curves $Y^2 = X(X^2 + p)$ it seems to be that the limits for exhaustive search are reached essentially by the examples of this paper, and the only sensible way to search for a generator on the curve $Y^2 = X(X^2 + 17477)$ would be by means of Heegner points.

Bibliography

1. A. Bremner, *On the equation* $Y^2 = X(X^2 + p)$, Number Theory and Applications (R. A. Mollin, ed.), Kluwer, Dordrecht, 1989, pp. 3-23.
2. A. Bremner and J. W. S. Cassels, *On the equation* $Y^2 = X(X^2 + p)$, Math. Comp. **42** (1984), 257-264.

Department of Mathematics, Arizona State University, Tempe, Arizona 85287
E-mail address: andrew@math.la.asu.edu

Supercomputing Research Center, 17100 Science Drive, Bowie, Maryland 20715
E-mail address: duncan@super.org