MATHEMATICS OF COMPUTATION, VOLUME 28, NUMBER 127, JULY 1974, PAGES 851-853

A Search for Elliptic Curves With Large Rank

By David E. Penney and Carl Pomerance

Abstract. A search procedure is described for finding elliptic curves with rational coefficients for which the group of rational points has large rank. Specific examples are given of elliptic curves with rank $\geqq 6$.

We recall Mordell's famous theorem that the set of rational points on a genus 1 curve with rational coefficients forms a finitely generated abelian group. The rank of such a curve is defined to be the number of free generators of this group. Wiman [3] gave the curve

$$y^2 = x^3 + 338x^2 + 13432x \tag{1}$$

as an example of a rank 4 elliptic curve. (Wiman claims the curve (1) has rank 6, but this is because his definition of rank is the minimum number of generators of the group of rational points, including points of finite order.)

Néron [1] proved that rank 10 elliptic curves exist, but gave no examples. In fact, no specific examples of elliptic curves of rank exceeding 4 have been published.

In this paper, we describe a procedure which computerizes a search for large rank elliptic curves. In particular, we give several examples of curves with rank $\geqq 6$. In a future paper, we hope to give examples with even larger rank.

We restrict our attention to curves of the form

$$y^2 = x^3 + ax^2 + bx \tag{2}$$

where $a, b \in \mathbf{Z}$ and $a^2 - 4b$ is not a square. (We note that Wiman's example (1) is not in this form, since $338^2 - 4 \cdot 13432 = 246^2$.) Let Γ be the group of rational points on (2), where the identity of Γ is 0, the point at infinity.

Since Γ is a finitely generated abelian group, we write $\Gamma \cong \mathbf{Z}^r \oplus \mathbf{Z}_{p_1^{a_1}} \oplus \cdots \oplus \mathbf{Z}_{p_k^{a_k}}$ where $p_1, \ldots, p_k$ are primes and r is the rank of Γ. Since $a^2 - 4b$ in (2) is not a square, there is only one rational root to $x^3 + ax^2 + bx$; so Γ has precisely one rational point of order 2, namely (0,0). Hence, precisely one of $p_1, \ldots, p_k$ is 2. Then $\Gamma/2\Gamma \cong \mathbf{Z}_2^{r+1}$.

Now it is easy to show from the definition of doubling a point on Γ, that if $(x,y) \in 2\Gamma$, then $x \in Q^2$; that is, x is the square of a rational number. Denote by Q^* the group of nonzero rationals, and let $\alpha\colon \Gamma \to Q^*/Q^{*2}$ where $\alpha(x,y) = xQ^{*2}$ if $x \neq 0$, $\alpha(0,0) = bQ^{*2}$, and $\alpha(0) = Q^{*2}$. It follows that α is a group homomorphism (for example, see Tate [2]) and that $2\Gamma \subset \ker \alpha$.

Summing up, we have $2^{r+1} = o(\mathbf{Z}_2^{r+1}) = o(\Gamma/2\Gamma) \geqq o(\Gamma/\ker \alpha) = o(\text{im } \alpha)$. Hence, if we could compute $o(\text{im } \alpha)$,we would have a lower bound for the rank r of Γ. A proof of the following theorem may be found in Tate [2].

Received October 4, 1973.

AMS (MOS) subject classifications (1970). Primary 10B10; Secondary 14G25, 14H30.

Key words and phrases. The rank of an elliptic curve.

THEOREM. im $\alpha = \{bQ^{*2}\} \cup \{nQ^{*2}: n \in \mathbf{Z}, n|b, \text{and } nu^4 + bv^4/n + au^2v^2 = w^2 \text{ has a solution } (u, v, w) \text{ in pairwise prime nonzero integers}\}$.

The quartic mentioned in the theorem is often difficult to analyze, so we restrict our attention to those quartics which allow a solution with $u = v = 1$. Namely, we study

$$A = \{bQ^{*2}\} \cup \{nQ^{*2}: n \in \mathbf{Z}, n|b, n + b/n + a \text{ is a nonzero square}\}. \tag{3}$$

Let $B =$ the subgroup of im α generated by A. Then B is isomorphic to a subgroup of $\mathbf{Z}_2^{r+1}$ and hence $B \cong \mathbf{Z}_2^s$ for some $s \leqq r + 1$. Hence, if we can compute $o(B)$ for a given choice of a and b in (2), we will have computed a lower bound for the rank r of Γ.

For a given choice of a and b in (2), we ask the computer to determine the members of

$$A' = \{n: n \in \mathbf{Z}, n|b, n + b/n + a \text{ is a square}\}. \tag{4}$$

By examining this set, it is not hard to compute A and then proceed to compute $o(B)$.

We give the following numerical example to illustrate the above process. Let Γ be the group of rational points on $y^2 = x^3 + 17x^2 - 105x$. It is a simple matter to compute A', the set defined in (4). Namely, $A' = \{-21, -15, -7, -3, -1, 5, 7, 15, 35, 105\}$. Then the subgroup B of im α is $\{nQ^{*2}: n \in \mathbf{Z}, n|105\}$ and $o(B) = 16$. Hence, $y^2 = x^3 + 17x^2 - 105x$ has rank $\geqq 3$.

In practice, we make a choice for b in (2) and let the computer search for a "good" choice for a. Indeed, for a given b, the computer has the set $\{n + b/n: n|b\}$ stored as an increasing sequence. For each choice of a, the computer forms the set $\{n + b/n + a: n|b, n + b/n + a \geqq 0\}$. This last set is searched for squares. If we have hit upon a good choice for a, i.e., there are many (say $\geqq 4$) squares in the set, then the computer prints out n, b/n, $n + b/n + a$ whenever $n + b/n + a$ is a square. The computer identifies an integer $x \geqq 0$ as a square by first verifying that x is a square for various small moduli, and if x passes these tests, $[x^{1/2}]$ is found by Newton's method written in integer programming for speed. Then x is a square if and only if $[x^{1/2}]^2 = x$.

In (2), we specify that $a^2 - 4b$ is not a square. However, for a given b, the computer might well choose an a such that $a^2 - 4b$ is a square. It is not necessary to patch up this "flaw" since $a^2 - 4b$ is a square if and only if $x^2 + ax + b = 0$ has an integral root if and only if for some divisor n of b, $n + b/n + a = 0$. Hence, the square 0 appears on our printout if and only if $a^2 - 4b$ is a square. Thus, we merely ignore those choices for a and b where the square 0 appears.

There are infinitely many ways of choosing a and b in (2). We need, therefore, a method of deciding which choices should be tried. Experience and a few elementary considerations, most of which we omit here, have led us to make the following restrictions on the choices for a and b.

First, we assume b is odd and square-free.

For a given b, we choose a so that $0 < a < f(b) < |b|$ where $f(b)$ is an arbitrarily chosen bound that increases with $|b|$. Furthermore, we take $a \equiv 2 \pmod 3$ and $a \equiv 0, 2,$ or $3 \pmod 5$. If $b \equiv 3 \pmod 8$, we choose $a \equiv 5 \pmod 8$. If $b \equiv 7 \pmod 8$, we choose $a \equiv 1 \pmod 8$. If $b \equiv 1 \pmod 4$, we

choose a in a few (possibly 1) congruence classes mod 64. The following lemmas provide some explanation.

LEMMA 1. *If* $b \equiv 3 \pmod 4$, *then* $x + bx^{-1} \equiv 1 + b \pmod 8$ *for every odd* x.

Proof. If x is odd, then $x \equiv x^{-1} \pmod 8$, so $x + bx^{-1} \equiv x + bx \equiv x(1 + b) \equiv 1 + b \pmod 8$ (since $1 + b \equiv 0 \pmod 4$).

LEMMA 2. *If* $b \equiv 1 \pmod 4$, *then* $x + bx^{-1}$ *has precisely* 4 *values as* x *ranges over the* 32 *odd congruence classes* mod 64.

Proof. This lemma is easily verified by proving that for each odd x mod 64, there are precisely 8 odd y's mod 64 such that $x + bx^{-1} \equiv y + by^{-1} \pmod{64}$. In fact, this last congruence holds if and only if $(x - y)(b - xy) \equiv 0 \pmod{64}$ if and only if

(1) if $b \equiv 1 \pmod 8$, then $y \equiv x \pmod 8$,

(2) if $b \equiv 5 \pmod 8$, then $y \equiv x \pmod{16}$ or $y \equiv x^2 + bx - 1 \pmod{16}$.

The following table sums up the highlights of what we found:

TABLE

b	a	*rank*
$3 \cdot 5 \cdot 13 \cdot 17 \cdot 29$	1217	$\geqslant 5$
$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	5513	$\geqslant 5$
$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	7265	$\geqslant 5$
$-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	29162	$\geqslant 5$
$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	53213	$\geqslant 6$
$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	80885	$\geqslant 6$
$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	100757	$\geqslant 6$
$-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	5858	$\geqslant 6$
$-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	47138	$\geqslant 6$
$-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	68258	$\geqslant 6$
$-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	74882	$\geqslant 6$
$-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	82658	$\geqslant 6$
$-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	93122	$\geqslant 6$

Department of Mathematics
University of Georgia
Athens, Georgia 30602

1. A. NÉRON, "Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps," *Bull. Soc. Math. France*, v. 80, 1952, pp. 101-166. MR **15**,151.

2. J. TATE, *Rational Points on Elliptic Curves*, Philips Lectures, Haverford College, 1961.

3. A. WIMAN, "Über rationale Punkte auf Kurven dritter Ordnung vom Geschlechte Eins," *Acta Math.*, v. 80, 1948, pp. 223-257. MR **10**,472.