MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 131
JULY 1975, PAGES 965–967

Three Elliptic Curves with Rank at Least Seven

By David E. Penney and Carl Pomerance

Abstract. Three rational elliptic curves whose ranks are at least 7 are exhibited. The arithmetical details are given for one of the curves, namely $y^2 = x^3 + 1692602x^2 - 530052723915x$.

1. Introduction. In [2], we demonstrated a computer search procedure for finding rational elliptic curves with large rank. In particular, we demonstrated nine elliptic curves with rank at least 6. Previously, the elliptic curve with the highest known rank was a rank 4 curve demonstrated by Wiman [3]. It is not known if elliptic curves with arbitrarily large rank exist, but Néron [1] was able to show that rank 10 curves do exist. However, Néron gave no examples. In this paper, we present three elliptic curves with rank at least 7.

Our method is essentially the same as that described in [2]. Namely, we consider the group Γ of rational points on

$$y^2 = x^3 + ax^2 + bx \tag{1}$$

where $a, b \in \mathbf{Z}$ and $a^2 - 4b$ is not a square. Let

$$A = \{n \in \mathbf{Z}: |n| \leqslant |b|^{1/2} \text{ and } n + b/n + a \text{ is an integral square}\} \cup \{b\}.$$

We let B be the group generated by the image of A under the projection $\mathbf{Q}^* \to \mathbf{Q}^*/\mathbf{Q}^{*2}$, where $\mathbf{Q}^*$ is the group of nonzero rationals and $\mathbf{Q}^{*2}$ is the subgroup of squares in $\mathbf{Q}^*$. Then $o(B) = 2^s$ for some integer s. Let r be the rank of Γ. In [2], we outlined the proof that

$$r \geqslant s - 1. \tag{2}$$

2. The Three Curves. The three elliptic curves found with rank at least 7 all have

$$b = -530052723915 = -3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37.$$

For this value of b, the CDC 6400 searched over the approximately 1800 values of a satisfying

$$0 < a < 3000000$$
$$a \equiv 26 \text{ or } 58 \ (64)$$
$$a \equiv 2 \ (3)$$
$$a \equiv 2 \text{ or } 3 \ (5)$$
$$a \equiv 2 \ (7).$$

Received February 28, 1974.
AMS (MOS) subject classifications (1970). Primary 10B10; Secondary 14G25, 14H30.
Key words and phrases. The rank of an elliptic curve.

For each value of a for which the set A had at least 5 elements, the members of A were printed out. The running time was approximately 10 minutes. Examining the printout by hand, three choices for a were found for which $s = 8$, and hence by (2), for which the rank r is at least 7. These values of a are

$$a = 1692602, 2843738, \text{ and } 2877338.$$

3. The Curve Γ: $y^2 = x^3 + 1692602x^2 - 530052723915x$. In this section, we detail the arithmetical information which proves that the rank of Γ is at least 7. We let $a = 1692602$, $b = -530052723915$. In Table 1, the 16 members n of $A \sim \{b\}$ are enumerated together with $(n + b/n + a)^{1/2}$.

We must show that the group B generated by the image of A in $\mathbf{Q}^*/\mathbf{Q}^{*2}$ has order $256 = 2^8$. In fact, we show that B has the eight independent generators

$$B' = \{b, 5 \cdot 13, 13 \cdot 23, -23 \cdot 31, 31 \cdot 37, -19 \cdot 37, -17 \cdot 29, -3 \cdot 5 \cdot 29\}.$$

We must check three points:

1. the members of B' are multiplicatively independent mod $\mathbf{Q}^{*2}$;
2. the members of B' are in the group generated by A;
3. the members of A are in the group generated by B'.

Now 1 is immediately verified since $5 \cdot 13$, $13 \cdot 23$, $-23 \cdot 31$, $31 \cdot 37$, $-19 \cdot 37$ are clearly independent and involve only six of the ten primes dividing b. The data needed to verify points 2 and 3 are collected in Tables 2 and 3 respectively. The equations in these two tables are actually congruences mod $\mathbf{Q}^{*2}$.

TABLE 1

n	$(n + b/n + a)^{1/2}$	n	$(n + b/n + a)^{1/2}$
$n_1 = 5 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	276	$n_9 = -3 \cdot 5 \cdot 29 \cdot 31 \cdot 37$	1502
$n_2 = 13 \cdot 19 \cdot 31 \cdot 37$	324	$n_{10} = -5 \cdot 11 \cdot 13 \cdot 17 \cdot 31$	1650
$n_3 = 3 \cdot 5 \cdot 23 \cdot 29 \cdot 31$	542	$n_{11} = -3 \cdot 5 \cdot 17 \cdot 19 \cdot 31$	2252
$n_4 = 13 \cdot 23 \cdot 31 \cdot 37$	700	$n_{12} = -5 \cdot 19 \cdot 23 \cdot 37$	2858
$n_5 = 17 \cdot 19 \cdot 29 \cdot 37$	714	$n_{13} = -3 \cdot 11 \cdot 23 \cdot 37$	4532
$n_6 = 19 \cdot 23 \cdot 31 \cdot 37$	1066	$n_{14} = -3 \cdot 11 \cdot 13 \cdot 37$	5922
$n_7 = -3 \cdot 17 \cdot 19 \cdot 23 \cdot 31$	1330	$n_{15} = -11 \cdot 17 \cdot 31$	9650
$n_8 = -3 \cdot 13 \cdot 17 \cdot 23 \cdot 37$	1438	$n_{16} = -11 \cdot 13 \cdot 29$	11380

TABLE 2

$$5 \cdot 13 = n_{10}n_{15} \qquad -19 \cdot 37 = (5 \cdot 13)(13 \cdot 23)n_{12}$$
$$13 \cdot 23 = n_{13}n_{14} \qquad -17 \cdot 29 = (-19 \cdot 37)n_5$$
$$-23 \cdot 31 = n_1n_{10} \qquad -3 \cdot 5 \cdot 29 = (-23 \cdot 31)n_3$$
$$31 \cdot 37 = (13 \cdot 23)n_4$$

TABLE 3

$$n_2 = (13 \cdot 23)(-23 \cdot 31)(-19 \cdot 37) \qquad n_7 = (-17 \cdot 29)n_9 n_{12}$$
$$n_3 = (-23 \cdot 31)(-3 \cdot 5 \cdot 29) \qquad n_8 = (13 \cdot 23)n_6 n_7$$
$$n_4 = (13 \cdot 23)(31 \cdot 37) \qquad n_{10} = (-23 \cdot 31)n_1$$
$$n_5 = (-19 \cdot 37)(-17 \cdot 29) \qquad n_{11} = (5 \cdot 13)(13 \cdot 23)n_7$$
$$n_6 = (-23 \cdot 31)(-19 \cdot 37) \qquad n_{14} = b(-3 \cdot 5 \cdot 29)n_7$$
$$n_9 = (31 \cdot 37)(-3 \cdot 5 \cdot 29) \qquad n_{13} = (13 \cdot 23)n_{14}$$
$$n_{12} = (5 \cdot 13)(13 \cdot 23)(-19 \cdot 37) \qquad n_{15} = (5 \cdot 13)n_{10}$$
$$n_1 = bn_3 n_{12} \qquad n_{16} = n_2 n_5 n_{15}$$

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. D. E. PENNEY & C. POMERANCE, "A search for elliptic curves with large rank," *Math. Comp.*, v. 28, 1974, pp. 851–853.

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