MATHEMATICS OF COMPUTATION
VOLUME 46, NUMBER 174
APRIL 1986, PAGES 627-635

Construction of Elliptic Curves with Large Rank

By Thomas J. Kretschmer

Abstract. We describe an algorithm for finding elliptic curves over $\mathbf{Q}$ with large rank and nontrivial torsion group. In particular, an example of a curve of rank exactly 10 with a point of order 2 is given. This method seems to suggest that the rank may be large independently of the torsion group.

1. Introduction. Let K be an algebraic number field and E be an elliptic curve defined over K. Then the set of the K-rational points of E forms an Abelian group and we have the famous theorem of Mordell-Weil stating that

$$E(K) \cong E_{\text{torsion}}(K) \oplus \mathbf{Z}^r \qquad (r \in \mathbf{N}_0).$$

The number r is called the *rank* of E over K.

The rank is a major topic of research since many years. One question related to it is whether there are elliptic curves of arbitrarily large rank over a fixed algebraic number field. Because of the difficulty of this problem, one restricts oneself to the case $K = \mathbf{Q}$. In 1954 Néron [7] succeeded in proving that there exist elliptic curves over $\mathbf{Q}$ with $r \geqslant 11$, but his proof does not yield any explicit examples. The following table gives a survey of examples that have been found up to now.

1948	Wiman	[11]	$r \geqslant 4$
1974	Penney & Pomerance	[8]	$r \geqslant 6$
1975	Penney & Pomerance	[9]	$r \geqslant 7$
1977	Grunewald & Zimmert	[3]	$r \geqslant 8$
1977	Brumer & Kramer	[1]	$r \geqslant 9$
1979	Nakata	[6]	$r \geqslant 9$
1982	Mestre	[5]	$r \geqslant 12$

The exact rank of these curves is not known, except that Mestre's example yields an elliptic curve of exact rank 12, provided the Birch and Swinnerton-Dyer conjecture, the Weil conjecture and the Riemann conjecture generalized to L-series of elliptic curves are true. All the curves with $r \geqslant 8$ have a trivial torsion group. In this paper, an example with $r = 10$ and nontrivial torsion group is given.

2. Results of Tate. In the following section, the main results of Tate from [10] are presented. Let K be an algebraic number field and E an elliptic curve over K with a K-rational point of order 2. E can be given the form:

$$E\colon Y^2 = X^3 + aX^2 + bX \qquad (a, b\ K\text{-integers}),$$

Received January 5, 1984.
1980 *Mathematics Subject Classification.* Primary 14K07, 10-04, 14G25; Secondary 10B10.

where the discriminant $\Delta = b^2(a^2 - 4b)$ is not equal to 0. Write Γ for $E(K)$ and define a homomorphism

$$\alpha\colon \Gamma \to K^*/K^{*2}$$

by

$$\alpha(\mathbf{0}) := \mathbf{1}$$

$$\alpha((0,0)) := bK^{*2}$$

$$\alpha((x,y)) := xK^{*2} \quad \text{for } x \neq 0.$$

Furthermore, define an elliptic curve $\bar{E}$ by

$$\bar{E}\colon Y^2 = X^3 + \bar{a}X^2 + \bar{b}X, \quad \text{where } \bar{a} := -2a,\ \bar{b} := a^2 - 4b.$$

Then $\bar{E}$ is 2-isogeneous to E. $\bar{\Gamma}$ and $\bar{\alpha}$ are defined analogously to Γ and α. In this situation, Tate has proved the fundamental

THEOREM 1.

$$2^r = \frac{|\alpha\Gamma| \cdot |\bar{\alpha}\bar{\Gamma}|}{4},$$

where r is the rank of E over K and $|A|$ denotes the cardinality of a set A.

Hence, the exact rank of E can be calculated if those values modulo squares are known that can occur as x-coordinates of the points on E (resp. $\bar{E}$).

For $K = \mathbf{Q}$, the following theorem yields a great deal of information about $\alpha\Gamma$.

THEOREM 2. *If $K = \mathbf{Q}$, then $\alpha\Gamma = \{\mathbf{Q}^{*2}, b\mathbf{Q}^{*2}\} \cup \{b_1\mathbf{Q}^{*2} \mid b_1$ divides b, i.e., $b = b_1b_2$ and*

$$(*) \qquad Z^2 = b_1X^4 + aX^2Y^2 + b_2Y^4$$

is solvable in $\mathbf{Z}$ with $XY \neq 0\}$.

Unfortunately, the solvability of equation (*) is not easy to decide. Nevertheless, Theorem 2 may be exploited to find elliptic curves of a large rank. The idea is to choose first some b composed of many distinct prime factors, and then to find a suitable a such that many of the equations (*) will be solvable. This was done in this way by Penney and Pomerance [8], [9]. Here, a significant improvement on the method of Penney and Pomerance will be achieved and applied to obtain some high-ranking curves, the exact rank of which can be determined.

For the rest of this paper we take $K = \mathbf{Q}$.

We now give two applications of the above theorems.

PROPOSITION 1. *Let $p \in \mathbf{P}$, i.e., p a prime, such that $p \equiv 5 \bmod 8$, and let the elliptic curve E be given by*

$$E\colon Y^2 = X^3 + p^2X.$$

Then (i) rank $E(\mathbf{Q}) = 0$, (ii) $E_{\text{tor}}(\mathbf{Q}) = \mathbf{Z}/2\mathbf{Z}$.

PROPOSITION 2. *Let $a^2 - 4b$ be squarefree. Then the torsion group T of E is isomorphic to one of the following groups*:

$$\mathbf{Z}/2\mathbf{Z},\quad \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z},\quad \mathbf{Z}/4\mathbf{Z},\quad \mathbf{Z}/6\mathbf{Z} \quad \text{or} \quad \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}.$$

More precisely:

(i) $a^2 - 4b = 1$.

(a) $(1 - a)/2$ *is a square in* $\mathbf{N}$. *Then* $T \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

(b) $(1 - a)/2$ *is not a square in* $\mathbf{N}$. *Then* $T \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

(ii) $a^2 - 4b \neq 1$.

(a) *If* $b_1 + a + b_2 \neq 1$ *for all factorizations* $b = b_1 b_2$ *of* b, *then* $T \cong \mathbf{Z}/2\mathbf{Z}$.

(b) *There is a divisor* b_1 *of* b *such that* $b_1 + a + b_2 = 1$.

(α) *If* $b_1 = b_2$, *then* $T \cong \mathbf{Z}/4\mathbf{Z}$.

(β) *If* $b_1 \neq b_2$, *then* T *is isomorphic to* $\mathbf{Z}/6\mathbf{Z}$, *provided that* $b_i = 4b/(4b - (a - 1)(a + 3))$ *for* $i = 1$ *or* 2. *Otherwise*, T *is isomorphic to* $\mathbf{Z}/2\mathbf{Z}$.

Proofs. The proofs can be found in [4].

3. Local Considerations. To get some insight into the solvability of the equations (*) appearing in Theorem 2, we consider them locally, that is to say, we investigate the solvability of

$$Y^2 = g(X) := b_1 X^4 + aX^2 + b_2 \quad \text{with } \Delta(g) := 2^4 3^3 b(a^2 - 4b)^2$$

in the p-adic completions $\mathbf{Q}_p$ of $\mathbf{Q}$ ($p \in \mathbf{P}$), $\Delta(g)$ being the discriminant of g.

The following three lemmas are useful in most cases:

LEMMA 1. *If* $p \in \mathbf{P}$ *with* $p \nmid \Delta(g)$, *then* $Y^2 = g(X)$ *is solvable in* $\mathbf{Q}_p$.

LEMMA 2. *Let* $p \in \mathbf{P}$ *with* $\mu := v_p(a^2 - 4b) \geqslant 1$ *and* $p \nmid 6b$. *Then* $Y^2 = g(X)$ *is solvable in* $\mathbf{Q}_p$ *if and only if*

(i) b_1 (*resp.* b_2) *is a quadratic residue* mod p, *or*

(ii) μ *is even and*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 5, 7 \bmod 8, \\ -1 & \text{if } p \equiv 1, 3 \bmod 8. \end{cases}$$

LEMMA 3. *Let* $p \in \mathbf{P}$ *be such that* $p \mid b$ *but* $p \nmid 6a$. *Then* $Y^2 = g(X)$ *is solvable in* $\mathbf{Q}_p$ *if and only if*

(i) $p \nmid \gcd(b_1, b_2)$, *or*

(ii) $p \mid \gcd(b_1, b_2)$ *and* $(\frac{a}{p}) = 1$ *or* $v_p(b_1)$ *or* $v_p(b_2)$ *is even*).

Proofs. Lemma 1 is clear. Lemma 2 is easy to prove if one uses that

$$y^2 = b_1 x^4 + ax^2 + b_2$$

is equivalent to

$$(2b_1 x^2 + a)^2 = a^2 - 4b + 4b_1 y^2 \quad \text{for } x, y \in \mathbf{Q}_p.$$

The proof of Lemma 3 involves a standard calculation in p-adic numbers. The details of all this can be found in [4].

Of course, these lemmas cannot always decide the global solvability, but they are a valuable tool in recognizing an equation to be not solvable. Furthermore, we can easily use them to prove (see [4]):

THEOREM 3. *Let* $a, b \in \mathbf{Z}$ *be such that*

(1) $b = 2^{e_2} \cdot 3^{e_3} \cdot p_1 \cdot \cdots \cdot p_n$ *with* $n,\ e_2,\ e_3 \in \mathbf{N},\ p_i \in \mathbf{P} \setminus \{2,3\}$ *and* $e_2 \geqslant 7$, $e_3 \geqslant 3$, $p_i \neq p_j$ *for* $i \neq j$ $(i, j \in \{1, \ldots, n\})$.

(2) $a \equiv 1 \bmod 24$.

(3) $p_i \nmid a$ *for all* $i \in \{1, \ldots, n\}$.

(4) $a^2 - 4b \in \mathbf{P}$.

Then

$$Y^2 = g(X) = b_1 X^4 + aX^2 + b_2 \qquad (b = b_1 b_2)$$

is everywhere locally solvable for all divisors b_1 *of* b.

4. Construction. For the following, $a^2 - 4b$ must not be a square. Let $A := \{b\} \cup \{b_1 \mid b_1 b_2 = b, b_i \in \mathbf{Z}$ and $b_1 + a + b_2$ is an integral square$\}$ and B be the group generated by $A \cdot \mathbf{Q}^{*2}$ in $\mathbf{Q}^*/\mathbf{Q}^{*2}$. Then $|B| = 2^s$ for some integer s, and the rank of E is not less than $s - 1$, as outlined in [8]. All we have to do now in order to find elliptic curves with large rank is to find a and b such that s is large. Of course, there are infinitely many choices for a and b, and so we impose some conditions on a and b:

(i) b satisfies condition (1) of Theorem 3 with large n. n should be greater than or equal to $r - 2$, if we want to find curves of rank $\geqslant r$.

(ii) a satisfies (2) of Theorem 3.

(iii) $0 \leqslant a \leqslant d\sqrt{b}$, where $d = 10$ or so, as suggested by experience.

(iv) For some small primes p, choose a and $b \bmod p$ such that $N_p := |E(\mathbf{F}_p)|$ is maximal. This idea may be found already in the article [2] of Birch and Swinnerton-Dyer on page 7 and, with a more solid foundation, in the article of Mestre [5].

When we have made some choice for b according to (i) and (iv), we let the computer find the best values for a (i.e., the values for which A is maximal) that satisfy (ii), (iii) and (iv). We now describe an algorithm which efficiently performs this task.

Conditions (ii) and (iv) (for a) can be summarized by

$$a \equiv c_1, \ldots, c_k \mod c,$$

where c is the product of 24 and the chosen small primes p of (iv), and $0 < c_1 < c_2 < \cdots < c_k < c$, $c_i \in \mathbf{N}_0$. In the sequel, we consider only one of the c_i:

$$a \equiv a_0 := c_i \mod c.$$

The algorithm then processes the c_i's one after another. Using (iii), we can reformulate the problem:

If $a_k := a_0 + kc$ $(0 \leqslant k \leqslant k_{\max}, k \in \mathbf{N}_0$, $k_{\max}$ depending on d of (iii) and on $c)$ and $M := \{b_1 + b_2 \mid b_1 b_2 = b, b_i \in \mathbf{Z}\}$, the algorithm has to determine for which indices k the set $a_k + M$ contains the most squares.

The following algorithm for solving this problem works substantially faster than the one used by Penney and Pomerance.*

ALGORITHM.

(0) *Associate with each* k $(0 \leqslant k \leqslant k_{\max})$ *a counter* Z_k *which at the end contains the number of squares in the set* $a_k + M$.

(1) *Set all counters* Z_k *to* 0.

(2) *For each divisor of* b *consider the sequence* $\tilde{a}_k := b_1 + b_2 + a_k$ $(0 \leqslant k \leqslant k_{\max})$ *(without loss of generality* $\tilde{a}_0 > 0$*), determine all indices* $k_1, \ldots, k_{e(b_1)}$ $(e(b_1) \in \mathbf{N}_0)$ *such that* $\tilde{a}_{k_i}$ *is a square* $(1 \leqslant i \leqslant e(b_1))$*, and increment the associated counters by* 1.

(3) *Print all the* a_k *for which* Z_k *is large.*

The disadvantage of this algorithm is step (0), because the counters are represented by an array of integers, the length of which is limited by the memory of the computer (this means, e.g., on our Siemens 7.561 that $k_{\max} \leqslant 500{,}000$). We will now explain how to execute in an efficient manner step (2), which at first sight looks relatively unfeasible.

Let $x_1, \ldots, x_s \in \mathbf{Z}$ be the solutions of

$$x^2 \equiv \tilde{a}_0 \mod c,$$

where the x_i are chosen from a fixed full system of residues mod c. The x_i can be computed fast, if at the very beginning of the program (i.e., after the input of a, b, c) a table of square roots mod c (or mod some factors of c, if c is too large) is computed and stored.

Define $y_i \in \mathbf{N}_0$ $(1 \leqslant i \leqslant s)$ by

y_i is minimal such that

(i) $y_i \equiv x_i \mod c$,

(ii) $y_i^2 \geqslant \tilde{a}_0$.

Then we have

$\tilde{a}_k$ is a square $\Leftrightarrow \exists i \in \{1, \ldots, s\}$, $l \in \mathbf{N}_0$: $\tilde{a}_k = (y_i + lc)^2$.

Proof.

" $\Leftarrow$ " trivial, but one remark: i and l given, there indeed exists a $k \in \mathbf{N}_0$ such that $\tilde{a}_k = (y_i + lc)^2$, because $(y_i + lc)^2 \geqslant y_i^2 \geqslant \tilde{a}_0$ and $(y_i + lc)^2 \equiv y_i^2 \equiv x_i^2 \equiv \tilde{a}_0 \mod c$.

" $\Rightarrow$ " If $\tilde{a}_k = e^2$ for some $e \in \mathbf{N}_0$ then $e^2 \equiv \tilde{a}_k \equiv \tilde{a}_0 \mod c$. Hence, there exists an $i \in \{1, \ldots, s\}$ such that $e \equiv x_i \mod c$. Because $e^2 \geqslant \tilde{a}_0$, and because of the definition of y_i, there exists $l \in \mathbf{N}_0$ such that $e = y_i + lc$.

Define now $k_{l,i} \in \mathbf{N}_0$ by

$$\tilde{a}_{k_{l,i}} = (y_i + lc)^2 \qquad (l \in \mathbf{N}_0, 1 \leqslant i \leqslant s).$$

Then the indices looked for in step (2) of the algorithm are given by

$$\{k_{l,i} | l \in \mathbf{N}_0, 1 \leqslant i \leqslant s\} \cap \{x \in \mathbf{N}_0 | x \leqslant k_{\max}\}.$$

---

*The curves of [9, Chapter 2], were found in 5 seconds, whereas 10 minutes were needed before.

Now there remains the question of how to determine the $k_{l,i}$. To settle this, we fix an $i \in \{1, \ldots, s\}$ and abbreviate $k_l := k_{l,i}$. First compute k_0 and, to this end, compute y_i:

Let $y_i = x_i + l_i c$. Without loss of generality, the full system of residues may be chosen so that always $l_i \in \mathbf{N}_0$. According to the definition of y_i, l_i is minimal such that $(x_i + l_i c)^2 \geqslant \tilde{a}_0$. Therefore,

$$l_i = \text{entier}\left(\frac{\sqrt{\tilde{a}_0} - x_i}{c}\right).$$

By this formula, l_i, and consequently y_i, can be computed. We get for k_0:

$$k_0 = \frac{y_i^2 - \tilde{a}_0}{c}.$$

To compute k_l ($l \geqslant 0$), we define

$$d_l := k_{l+1} - k_l = 2y_i + (2l + 1)c.$$

Then $d_{l+1} - d_l = 2c$.

Summarizing: Compute k_0 as before and set $d_0 := 2y_i + c$. Then,

$$\begin{aligned} k_{l+1} &= k_l + d_l \\ d_{l+1} &= d_l + 2c \end{aligned} \qquad (l \in \mathbf{N}_0).$$

This shows that the computation of k_{l+1} from k_l requires only two additions and is therefore very fast. Repeat all this for each $i \in \{1, \ldots, s\}$.

5. Examples. Using an implementation of the above algorithm on the Siemens 7.561, running the SAC2/Aldes system, the following curve was found:

THEOREM 4. *Let* $a = 12{,}273{,}038{,}545$ *and* $b = 2^{10} \cdot 3^6 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 53 = 17{,}236{,}434{,}803{,}911{,}308{,}288$. *Then the elliptic curve* E: $Y^2 = X^3 + aX^2 + bX$ *has rank* 10 *over* $\mathbf{Q}$.

Proof. $\bar{E}$ is given by $\bar{E}$: $Y^2 = X^3 + \bar{a}X^2 + \bar{b}X$, where $\bar{a} := -2a = -24{,}546{,}077{,}090$ and $\bar{b} := a^2 - 4b = 47^2 \cdot 53 \cdot q = 81{,}681{,}735{,}911{,}410{,}483{,}873$, with $q := 697{,}675{,}341{,}112{,}349$ prime. Define

$$r_1 := \log_2|\alpha\Gamma| - 1, \qquad r_2 := \log_2|\bar{\alpha}\bar{\Gamma}| - 1.$$

We will show that $r_1 = 10$ and $r_2 = 0$. Theorem 1 then implies that $r = r_1 + r_2 = 10$. As to r_1, we know from the computer output that $B = \langle 2 \cdot 41, 3 \cdot 41, 17, 19 \cdot 41, 23 \cdot 41, 29, 31 \cdot 41, 37, 43, 53, -1\rangle \mathbf{Q}^{*2}$. Therefore, $r_1 \geqslant 10$. Assuming $r_1 = 11$, we would have $B = \alpha\Gamma$, and $Y^2 = 41X^4 + aX^2 + b/41$ would be solvable in $\mathbf{Q}_q$. Because $(\frac{41}{q}) = -1$, this is a contradiction to Lemma 2.

With regard to r_2, we show that $\bar{\alpha}\bar{\Gamma} = \{\mathbf{Q}^{*2}, \bar{b}\mathbf{Q}^{*2}\}$. Let $\bar{b}_1\mathbf{Q}^{*2} \in \bar{\alpha}\bar{\Gamma}$ with $\bar{b}_1\bar{b}_2 = \bar{b}$.

(i) $\bar{b}_1 < 0$ implies that

$$(*) \qquad Y^2 = \bar{b}_1 X^4 + \bar{a} X^2 + \bar{b}_2$$

is not solvable in $\mathbf{R}$, a contradiction to $\bar{b}_1 \mathbf{Q}^{*2} \in \bar{\alpha}\bar{\Gamma}$.

(ii) $\bar{b}_1 > 0$. By using Lemma 2, one can show that equation $(*)$ is not solvable in $\mathbf{Q}_{19}$ or in $\mathbf{Q}_{29}$.

We now list the x-coordinates of 10 independent points defined over $\mathbf{Z}$. The computer output for this example yields 92 integer points on E.

$$x_1 = 3^6 \cdot 17 \cdot 43 \cdot 53$$

$$x_2 = 2^4 \cdot 3^5 \cdot 19 \cdot 43$$

$$x_3 = 2^3 \cdot 3^4 \cdot 29 \cdot 31 \cdot 37$$

$$x_4 = 2^7 \cdot 3^5 \cdot 17 \cdot 19 \cdot 23$$

$$x_5 = 2^7 \cdot 3^5 \cdot 29 \cdot 31 \cdot 41$$

$$x_6 = 2^6 \cdot 3^5 \cdot 19 \cdot 43 \cdot 53$$

$$x_7 = 2^6 \cdot 3^5 \cdot 17 \cdot 23 \cdot 43$$

$$x_8 = 2^5 \cdot 3^5 \cdot 17 \cdot 19 \cdot 41$$

$$x_9 = 2^7 \cdot 3^4 \cdot 17 \cdot 23 \cdot 29 \cdot 53$$

$$x_{10} = -2^5 \cdot 3^5 \cdot 17 \cdot 23 \cdot 31 \cdot 37$$

The following tables contain further examples.

TABLE 1

r	b	a
1	2	7
2	$2^7 \cdot 3^3$	169
3	$2^7 \cdot 3^3 \cdot 7$	997
4	$2^7 \cdot 3^4 \cdot 7 \cdot 13$	6,865
5	$2^8 \cdot 3^3 \cdot 7 \cdot 11 \cdot 17$	17,905
6	$2^7 \cdot 3^4 \cdot 13 \cdot 23 \cdot 29 \cdot 31$	154,465
7	$2^8 \cdot 3^8 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	3,065,905
8	$2^7 \cdot 3^4 \cdot 7 \cdot 11 \cdot 29 \cdot 31 \cdot 41 \cdot 47$	16,835,185
9	$2^9 \cdot 3^6 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 59$	76,171,105

Here $a^2 - 4b$ is always a prime. This fact leads to the following

CONJECTURE. *Let n be a positive integer. Then there exists a set $S = \{p_1, \ldots, p_{n+1}\}$ of primes and an elliptic curve E defined over $\mathbf{Q}$ such that*

(i) rank $E(\mathbf{Q}) = n$,

(ii) $E_{\text{torsion}}(\mathbf{Q}) \neq (0)$,

(iii) *E has good reduction outside S.*

TABLE 2

$r \geqslant$	b	a
7	$2^7 \cdot 3^4 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41$	49,555,705
7	$2^7 \cdot 3^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 43$	25,045,585
7	$2^8 \cdot 3^4 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 37 \cdot 41$	14,853,985
7	$2^8 \cdot 3^4 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 47$	6,796,345
7	$2^8 \cdot 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 43 \cdot 47$	39,554,665
8	$2^9 \cdot 3^5 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 41 \cdot 47$	95,560,825
8	$2^8 \cdot 3^4 \cdot 13 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 47 \cdot 53$	104,228,785
8	$2^9 \cdot 3^3 \cdot 19 \cdot 23 \cdot 31 \cdot 37 \cdot 47 \cdot 59 \cdot 61$	203,231,185
8	$2^8 \cdot 3^4 \cdot 19 \cdot 23 \cdot 31 \cdot 43 \cdot 47 \cdot 59 \cdot 61$	1,495,599,625
8	$2^8 \cdot 3^3 \cdot 19 \cdot 23 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59$	269,152,585
8	$2^7 \cdot 3^4 \cdot 19 \cdot 23 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 61$	173,919,265
8	$2^8 \cdot 3^3 \cdot 19 \cdot 29 \cdot 37 \cdot 43 \cdot 47 \cdot 53 \cdot 59$	217,040,785
8	$2^8 \cdot 3^4 \cdot 19 \cdot 29 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 61$	2,178,863,185
8	$2^9 \cdot 3^4 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 47 \cdot 53 \cdot 61$	853,117,945
8	$2^9 \cdot 3^4 \cdot 23 \cdot 29 \cdot 31 \cdot 43 \cdot 47 \cdot 53 \cdot 59$	968,820,385
8	$2^8 \cdot 3^3 \cdot 23 \cdot 29 \cdot 37 \cdot 43 \cdot 53 \cdot 59 \cdot 61$	219,001,225
8	$2^8 \cdot 3^3 \cdot 23 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 59 \cdot 61$	314,984,905
8	$2^8 \cdot 3^3 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53$	945,830,785
8	$2^9 \cdot 3^4 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59$	1,478,670,625
9	$2^9 \cdot 3^4 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 53 \cdot 61$	397,532,305
9	$2^{12} \cdot 3^6 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37$	3,565,004,785
9	$2^{10} \cdot 3^8 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37$	3,104,006,785
9	$2^{10} \cdot 3^8 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37$	6,689,571,985
9	$2^{10} \cdot 3^8 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37$	7,762,474,585
9	$2^9 \cdot 3^7 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 47 \cdot 101$	3,462,137,425
9	$2^9 \cdot 3^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 73$	539,827,945
9	$2^8 \cdot 3^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 67 \cdot 73 \cdot 79$	3,240,270,025
9	$2^9 \cdot 3^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 67 \cdot 79$	1,882,513,345
9	$2^9 \cdot 3^6 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 71$	2,015,170,225
9	$2^9 \cdot 3^6 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 71$	1,912,672,825
9	$2^{10} \cdot 3^6 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 59$	2,305,197,625
9	$2^9 \cdot 3^6 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	1,418,295,385
9	$2^8 \cdot 3^5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 53$	1,021,882,585
9	$2^9 \cdot 3^5 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	992,038,825
9	$2^8 \cdot 3^6 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41$	2,792,554,705
9	$2^8 \cdot 3^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 73$	2,921,371,705
9	$2^9 \cdot 3^4 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 67$	2,583,197,545
9	$2^8 \cdot 3^5 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 47 \cdot 53 \cdot 61$	30,661,587,025
9	$2^9 \cdot 3^4 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 47 \cdot 53 \cdot 59$	21,052,338,745
10	$2^{10} \cdot 3^6 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 53$	12,273,038,545
10	$2^9 \cdot 3^4 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 47 \cdot 53 \cdot 59$	18,926,510,425

This table is an excerpt from what the computer found during my work.

Acknowledgment. I am greatly indebted to Professor H. G. Zimmer for drawing my attention to this problem and for guiding my work on it.

Fachbereich Mathematik
Universität des Saarlandes
D-6600 Saarbrücken, West Germany

1. A. BRUMER & K. KRAMER, "The rank of elliptic curves," *Duke Math. J.*, v. 44, 1977, pp. 715–743.

2. B. J. BIRCH & H. P. F. SWINNERTON-DYER, "Notes on elliptic curves. I," *J. Reine Angew. Math.*, v. 212, 1963, pp. 7–25.

3. F. J. GRUNEWALD & R. ZIMMERT, "Über einige rationale elliptische Kurven mit freiem Rang $\geqslant 8$," *J. Reine Angew. Math.*, v. 296, 1977, pp. 100–107.

4. T. J. KRETSCHMER, *Konstruktion elliptischer Kurven von hohem Rang*, Diploma thesis, Saarbrücken, 1983.

5. J. F. MESTRE, "Construction d'une courbe elliptique de rang $\geqslant 12$," *C. R. Acad. Sci. Paris*, v. 295, 1982, pp. 643–644.

6. K. NAKATA, "On some elliptic curves defined over $\mathbf{Q}$ of free rank $\geqslant 9$," *Manuscripta Math*, v. 29, 1979, pp. 183–194.

7. A. NÉRON, *Propriétés Arithmétiques de Certaines Familles de Courbes Algébriques*, Proc. Internat. Congress, Amsterdam, 1954, III, pp. 481–488.

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

9. D. E. PENNEY & C. POMERANCE, "Three elliptic curves with rank at least seven," *Math. Comp.*, v. 29, 1975, pp. 965–968.

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

11. A. WIMAN, "Über rationale Punkte auf Kurven dritter Ordnung vom Geschlechte eins," *Acta Math.*, v. 80, 1948, pp. 223–257.