Canad. Math. Bull. Vol. **34** (2), 1991 pp. 181–185

AN ARITHMETICAL FUNCTION ASSOCIATED WITH THE RANK OF ELLIPTIC CURVES

DAVID CLARK

ABSTRACT. We define an arithmetical function, $f(n)$, which gives a lower bound for the rank of elliptic curves, $y^2 = x^3 + nx$, n square-free. Thus, if $f(n)$ is unbounded for square-free values of n, then there are elliptic curves of arbitrarily large rank. We show that $f(n)$ is unbounded as n ranges over all integers.

1. **Introduction.** The set $E(Q)$ of rational points of an elliptic curve over Q is the set of solutions

$$\{(x, y) \in Q \times Q : y^2 = x^3 + ax + b\},$$

together with ∞, the point at infinity, where $a, b \in Q$ and the discriminant of $x^3 + ax + b$, $-4a^3 - 27b^2$, is nonzero. Poincaré noticed that an addition law could be defined on this set using secants and tangents. Mordell [6] showed that $E(Q)$ is a finitely generated group under this addition law. From this result it follows that

$$E(Q) \cong E(Q)_{\text{tors}} \times Z^r,$$

where $E(Q)_{\text{tors}}$ is the set of elements of finite order. The integer r is called the rank of the elliptic curve over Q. The theorems of Lutz [3], Nagell [7], and Mazur [4] give a complete characterization of the torsion part of elliptic curves over Q. However, the rank of elliptic curves over Q remains very poorly understood. In the case of elliptic curves over function fields Shafarevich and Tate [8] showed that there exist elliptic curves with arbitrarily large rank. Naturally, it is conjectured that the same result holds for elliptic curves over the rational numbers. Using a specialization argument, Néron [8] proved the existence of an infinite family of elliptic curves over Q with rank greater than ten, but his method yields no explicit examples. Mestre [5] found an elliptic curve of rank at least fourteen using an algorithm based on the Birch and Swinnerton-Dyer Conjecture; unfortunately, his method is not suited to finding infinite families of such curves.

This paper investigates an arithmetical function,

$$f(n) = \#\{(a, b) \in Z \times Z : ab = n,\ a + b = \square\},$$

which gives a lower bound for the rank of elliptic curves, $y^2 = x^3 + nx$, for n square-free. The definition of this function is motivated by the Tate algorithm for computing the rank of an elliptic curve over Q.

Received by the editors July 18, 1990.
AMS subject classification: 11G05, 11D85.

THEOREM 1. *If E: $y^2 = x^3 + nx$ is an elliptic curve of rank r over Q, with $n \in Z$ square-free, then* $f(n) \leqq 2^{r+2}$.

Thus, if

$$\limsup_{n \text{ squarefree}} f(n) = +\infty, \tag{1}$$

then there exist elliptic curves of arbitrarily large rank. Although this conjecture remains unproved, the following holds.

THEOREM 2. $\limsup_{n\to\infty} f(n) = +\infty$.

Section 2 outlines the Tate algorithm and proves these two theorems. Section 3 determines the average order of $f(n)$. The final section gives some numerical observations which support conjecture (1).

2. **Tate Algorithm and the Arithmetical Function.** Tate formulated an algorithm for determining the rank of elliptic curves of the form

$$E\colon y^2 = x^3 + ax^2 + bx, \quad a,\ b \in Q.$$

For a detailed exposition of this algorithm, see Appendix 1 of Coates [2]. An outline of the algorithm follows. Consider the mapping

$$\alpha_E\colon E(Q) \longrightarrow Q^\times / Q^{\times 2},$$

defined by

$$\alpha_E(\infty) = 1 \,(\text{mod } Q^{\times 2}),\ \ \alpha_E(0,\ 0) = b\,(\text{mod } Q^{\times 2}),\ \text{ and }\ \alpha_E(x,\ y) = x\,(\text{mod } Q^{\times 2}),\ x \neq 0,$$

where $Q^\times$ is the multiplicative group of the rational numbers. If r_E is the rank of $E(Q)$, then

$$2^{r_E} = \frac{1}{4}\,|\text{Image }(\alpha_E)|\,|\text{Image }(\alpha_{E'})|, \tag{2}$$

where E': $y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. An integer b_1 is in the image of α_E if

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4,\ b_1b_2 = b, \tag{3}$$

has a nontrivial integer solution. However, this algorithm is theoretically ineffective since there is no known method for deciding if (3) has a solution.

For elliptic curves of the form E: $y^2 = x^3 + nx, n \in Z$, equation (3) simplifies to $N^2 = b_1M^4 + b_2e^4, b_1b_2 = n$. Thus, factorization of $n = ab$ with, $a + b = \square$ ($a + b$ a square), give nontrivial elements of the image of α_E. Call such factorizations of n good. For n square-free, the magnitude of the arithmetical function $f(n)$ gives a lower bound for the rank of $E(Q)$.

PROOF OF THEOREM 1. Since n is not a square, every factorization $n = ab, a+b = \square$, gives rise to two elements of the image of α_E, and since n is square-free, the elements from all such factorizations are distinct. ∎

PROOF OF THEOREM 2. Choose an elliptic curve $y^2 = x^3 + Dx$ with rank greater than or equal to one, for example $y^2 = x^3 + 2x$. An integer point (x, y) on the curve such that $x|y$ and $x \neq 0$ gives rise to a desired factorization of D,

$$\frac{y^2}{x^2} = x + \frac{D}{x}.$$

Given any positive integer m, choose m rational points on the elliptic curve,

$$\left(\frac{p_1}{s_1^2}, \frac{r_1}{s_1^3}\right); \left(\frac{p_2}{s_2^2}, \frac{r_2}{s_2^3}\right); \ldots; \left(\frac{p_m}{s_m^2}, \frac{r_m}{s_m^3}\right),$$

with the property

$$\frac{p_i}{s_i^2}\frac{p_j}{s_j^2} \neq D, \tag{4}$$

for all i and j. Let $R = \prod_{i=1}^m r_i$ $S = \prod_{i=1}^m s_i$, and consider the elliptic curve

$$y^2 = x^3 + DR^4S^4x. \tag{5}$$

From

$$\left(\frac{r_i}{s_i^3}\right)^2 = \left(\frac{p_i}{s_i^2}\right)^3 + D\left(\frac{p_i}{s_i^2}\right) \text{ or } r_i^2 = p_i^3 + Dp_is_i^4,$$

it is clear that $p_i | r_i^2$. Observe that $(R^2S^2p_i/s_i^2, \; R^3S^3r_i/s_i^3)$ are distinct integer points on the curve (5) and that $R^2S^2p_i/s_i^2 | R^3S^3r_i/s_i^3$, which follows immediately from $p_i|r_i^2$. The property (4) ensures that the representations are distinct. Thus, $f(DR^4S^4) \geqq 2m$. ∎

3. **Average Order Estimate.** There are the following estimates of the average order of $f(n)$. The proof uses the fact that for a and c nonnegative the inequalities $a \leqq \sqrt{x}$ and $c \leqq \sqrt{(x+a^2)/a}$ are equivalent to the inequality $a(c^2 - a) \leqq x$.

THEOREM 3.

$$x^{3/4} \ll \sum_{n \leqq x} f(n) \ll x^{3/4}.$$

PROOF. First, notice that,

$$\begin{aligned}
\sum_{1 \leqq n \leqq x} f(n) &= \sum_{1 \leqq a \leqq \sqrt{x}} \left[\sqrt{\frac{x+a^2}{a}}\right] \leqq \sum_{1 \leqq a \leqq \sqrt{x}} \sqrt{\frac{x+a^2}{a}} \\
&\leqq \sqrt{x+1} + \int_1^{\sqrt{x}} \sqrt{\frac{x}{a} + a}\, da \leqq \sqrt{x+1} + \int_1^{\sqrt{x}} \left(\sqrt{\frac{x}{a}} + \sqrt{a}\right) da \\
&\leqq \sqrt{x+1} + 2\sqrt{x}(x^{1/4} - 1) + \frac{2}{3}(x^{3/4} - 1) \\
&\ll x^{3/4}.
\end{aligned}$$

Similarly,

$$
\begin{aligned}
\sum_{1\leqq n\leqq x} f(n) = \sum_{1\leqq a\leqq\sqrt{x}} \left[\sqrt{\frac{x+a^2}{a}}\right] &\geqq \sum_{1\leqq a\leqq\sqrt{x}} \sqrt{\frac{x+a^2}{a}} - \sqrt{x} \\
&\geqq \int_1^{\sqrt{x}} \sqrt{\frac{x}{a}+a}\, da - \sqrt{x} \leqq \int_1^{\sqrt{x}} \frac{1}{\sqrt{2}} \left(\sqrt{\frac{x}{a}} + \sqrt{a}\right) da - \sqrt{x} \\
&\geqq \sqrt{2x}(x^{1/4}-1) + \frac{\sqrt{2}}{3}(x^{3/4}-1) - \sqrt{x} \\
&\gg x^{3/4}.
\end{aligned}
$$

■

4. **Numerical Observations.** A computer search produced the following examples of integers n with a large number of good representations.

n	factorization	$f(n)$
828	$2^2 \cdot 3^2 \cdot 23$	6
8,820	$2^2 \cdot 3^2 \cdot 5 \cdot 7$	8
26,100	$2^2 \cdot 3^2 \cdot 5^2 \cdot 29$	10
92,400	$2^4 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11$	10
153,648	$2^4 \cdot 3^2 \cdot 11 \cdot 97$	10
417,600	$2^6 \cdot 3^2 \cdot 5^2 \cdot 29$	12
2,458,368	$2^{10} \cdot 3^2 \cdot 11 \cdot 19$	14
3,009,600	$2^6 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 19$	16
541,209,600	$2^{10} \cdot 3^6 \cdot 5^2 \cdot 29$	20

To give some evidence for the validity of the conjecture (1), a search was also made for square-free integers with many good representations.

n	factorization	$f(n)$
547,230	$2 \cdot 3 \cdot 5 \cdot 17 \cdot 29 \cdot 37$	8
613,263	$3 \cdot 7 \cdot 19 \cdot 29 \cdot 53$	6
86,129,043	$3 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29 \cdot 43$	6
121,706,970	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 47 \cdot 59$	8
209,323,023	$3 \cdot 7 \cdot 13 \cdot 17 \cdot 23 \cdot 37 \cdot 53$	6
27,522,144,195	$3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 43$	6
55,639,361,778	$2 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 43$	8

ACKNOWLEDGEMENTS. I would like to thank Ram Murty for introducing me to elliptic curves, and I would like to thank the referee for his detailed comments on the first draft of this paper. The results of this paper formed part of the last chapter of the author's M.Sc. thesis [1].

REFERENCES

1. D. Clark, "L-series and Ranks of Elliptic Curves," M. Sc. Thesis, McGill University, Montréal, Québec, 1988.

2. J. Coates, *Elliptic Curves and Iwasawa Theory*, in "Modular Forms," R. Rankin ed., Halsted Press, New York, 1984.

3. E. Lutz, *Sur l'equation* $y^2 = x^3 - Ax - B$ *dans le corps p-adic*, J. Reine Angew. Math. **177** (1937), 237–247.

4. B. Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math. **47** (1977), 33–186.

5. J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Comp. Math. **58** (1986), 209–232.

6. L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Camb. Phil. Soc. **21** (1922), 179–192.

7. T. Nagell, *Solution de quelque problémes dans la théorie arithmétique des cubiques planes du premier genre*, Wid. Akad. Skrifter Oslo I (1935), Nr. 1.

8. A. Néron, *Problémes arithemétiques et géométriques rattachés a la notion de rang d'une courbe algégbrique dans un corps*, Bull. Soc. Math. France **80** (1952), 101–166.

9. I. R. Shafarevich and J. Tate, *The rank of elliptic curves*, A.M.S. Transl. **8** (1967), 917–920.

Department of Mathematics and Statistics
McGill University
Montréal, Quebec, H3A 2K6

https://doi.org/10.4153/CMB-1991-029-4 Published online by Cambridge University Press