A FUNCTION RELATED TO THE MORDELL-WEIL RANK OF ELLIPTIC CURVES

ANUP B. DIXIT, M. RAM MURTY, AND SIDDHI S. PATHAK

ABSTRACT. Let p be a prime number. For each natural number n, we study the behaviour of the function $f_p(n)$ which enumerates the number of factorizations $ab = n$ with $a + b$ a perfect square (mod p). The study of this function is inspired by the cognate function $f(n)$ which enumerates the number of factorizations $ab = n$ with $a + b$ a perfect square. The descent theory of elliptic curves would show that if $f(n)$ is unbounded for squarefree values of n, then there are elliptic curves over the rational number field with arbitrarily large rank. In this note, we show for every prime p, $f_p(n)$ is unbounded as n ranges over squarefree values, thus providing some evidence for the conjecture that $f(n)$ is unbounded for squarefree n.

1. Introduction

For a natural number n, let

$$f(n) := \# \{1 \leq a,\, b \leq n \,:\, ab = n,\, a + b \text{ is a perfect square}\}.$$

The unboundedness of $f(n)$ for n squarefree has a connection to the unbounded rank conjecture of elliptic curves which we will describe in section 2 below.

For a fixed prime p, let

$$f_p(n) := \# \left\{1 \leq a,\, b \leq n \,:\, ab = n,\, \left(\frac{a+b}{p}\right) = 1\right\},$$

where $\left(\frac{a}{p}\right)$ denotes the Legendre symbol. In this paper, we show that for any fixed prime number p, the function $f_p(n)$ is unbounded as n ranges over squarefree numbers. The study of this function is inspired by the cognate function $f(n)$ defined above. The descent theory of elliptic curves (see section 2) would show that if $f(n)$ is unbounded as a function of n, then there are elliptic curves over the rational number field with arbitrarily large rank. If $f(n)$ is unbounded, then so is $f_p(n)$ for every prime p. We show the following.

Theorem 1. *Let p be a prime number. Then,*

$$\sum_{\substack{n \leq x \\ n \text{ squarefree}}} f_p(n) \gg x \log x,$$

with the implied constant dependent on the prime p. Consequently, $f_p(n)$ is unbounded as n varies over squarefree positive integers.

2020 *Mathematics Subject Classification.* 11G05, 11L40.

Key words and phrases. rank of an elliptic curve, character sums, Tauberian theorem.

Research of the first and the third authors was partially supported by the INSPIRE Faculty Fellowship. Research of the second author was partially supported by an NSERC Discovery grant.

2. Two descent via a 2-isogeny

In his famous 1961 Haverford lectures, Tate [5] (see also the appendix in [2]) described a simple algorithm for determining the Mordell-Weil rank of elliptic curves of the form

$$E: \qquad y^2 = x^3 + ax^2 + bx, \qquad a, b \in \mathbb{Z}.$$

We let $W = (0,0)$ and observe that it is a rational point on $E(\mathbb{Q})$ of order 2. Now define the curve E' as:

$$E': \qquad y^2 = x^3 + a'x^2 + b'x.$$

with $a' = -2a$ and $b' = a^2 - 4b$. Denoting by $\mathcal{O}$ the identity element of $E(\mathbb{Q})$, we define the map

$$\alpha_E : E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

by $\alpha(\mathcal{O}) = 1 \mod \mathbb{Q}^{\times 2}$, $\alpha_E(W) = b \mod \mathbb{Q}^{\times 2}$ and for $x \neq 0$,

$$\alpha_E(x, y) = x \mod \mathbb{Q}^{\times 2}.$$

The definition of $\alpha_{E'}$ is analogous. The image of α_E and $\alpha_{E'}$ are then shown to be finite. If r denotes the rank of $E(\mathbb{Q})$, Tate [5] proves that

$$2^{r+2} = |\mathrm{Im}(\alpha_E)| \, |\mathrm{Im}(\alpha_{E'})| \, .$$

Thus, to determine the rank r, one needs to determine the size of the images of α_E and $\alpha_{E'}$.

To this end, we consider every possible factorization $b = b_1 b_2$ with $b_1, b_2 \in \mathbb{Z}$. For each such factorization, we examine the Diophantine equation involving the variables M, N and e:

$$N^2 = b_1 M^4 + aM^2e^2 + b_2 e^4. \tag{1}$$

If (1) has a solution in non-zero integers M, N, e with $e > 0$, then a routine verification shows that

$$x = \frac{b_1 M^2}{e^2}, \quad y = \frac{b_1 MN}{e^3}$$

gives a rational point $P = (x, y)$ on E so that $\alpha_E(P) = b_1 \mod \mathbb{Q}^{\times 2}$.

For curves with $a = 0$, we now see the connection to the function $f(n)$. For n squarefree, consider the family of curves

$$E_n: \qquad\qquad y^2 = x^3 + nx.$$

The algorithm for the rank of this curve derived by Tate would imply $2^{r+2} \geq f(n)$. Thus, if $f(n)$ is unbounded, then the Mordell-Weil ranks of $E_n(\mathbb{Q})$ would be unbounded. This is the motivation for studying $f(n)$ and $f_p(n)$.

In his MSc thesis (written under the direction of the senior author), David Clark [1] proved that $f(n)$ is unbounded if we remove the restriction that n is squarefree. In this paper, we study $f_p(n)$ for n squarefree so as to elucidate the more difficult study of $f(n)$ when n is squarefree.

3. Preliminary lemmas

In the proof of our theorem, we need various results that we collect in this section for ease of reference.

The first is a Tauberian theorem. We use the classical version as stated below. See Exercise 4.4.17 in [4] for a reference.

Lemma 2. *Let $f(s) = \sum_{n=1}^{\infty} a_n/n^s$ with $a_n = O(n^{\epsilon})$. Suppose that*

$$f(s) = \zeta(s)^k g(s),$$

where k is a natural number and $g(s)$ is a Dirichlet series absolutely convergent in $\Re(s) > 1 - \delta$ for some $0 < \delta < 1$. Then we have

$$\sum_{n \le x} a_n \sim \frac{g(1)}{(k-1)!} x \left(\log x\right)^{k-1}$$

as $x \to \infty$.

The following result is due to Hooley [3].

Lemma 3 (Hooley, 1975)**.** *Let $R(x; a, q)$ be the number of squarefree numbers in the arithmetic progression a mod q with $(a, q) = 1$. For any $\epsilon > 0$, we have*

$$R(x; a, q) = \frac{1}{\zeta(2)} \prod_{\substack{p \mid q \\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right)^{-1} \frac{x}{q} + O_{\epsilon}\left(\left(\frac{x}{q}\right)^{1/2} + q^{1/2+\epsilon}\right). \tag{2}$$

Lemma 4.

$$\sum_{n \le x} \mu^2(n)\, d(n) = Cx \log x + o(x \log x)$$

where

$$C = \prod_p \left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right) = 0.33...$$

Proof. This is a simple application of Lemma 2. Here are the relevant details. We have

$$\sum_{n=1}^{\infty} \frac{\mu^2(n) d(n)}{n^s} = \prod_p \left(1 + \frac{2}{p^s}\right).$$

The infinite product can be re-written as

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-2} \prod_p \left(1 - \frac{1}{p^s}\right)^2 \left(1 + \frac{2}{p^s}\right) = \zeta(s)^2 g(s) \quad \text{(say)}.$$

An application of the Tauberian theorem gives

$$\sum_{n \le x} \mu^2(n) d(n) = Cx \log x + o(x \log x)$$

with

$$C = \prod_p \left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right) = \prod_p \left(\frac{p^3 - 3p + 2}{p^3}\right)$$

Since each factor in the absolutely convergent product is non-zero, we deduce $C \neq 0$, as desired. □

Remark 3.1. *We remark that it is possible to refine the lemma to give constants C, D such that*

$$\sum_{n \le x} \mu^2(n) d(n) = Cx \log x + Dx + O(x^{1/2}),$$

using the technique of contour integration as discussed in Chapter 4 of [4].

We also use the following estimates. Let $R(x)$ denote the number of squarefree numbers $n \leq x$. It is well-known that (see for example, Exercise 1.4.4 of [4])

$$R(x) = \frac{x}{\zeta(2)} + O(\sqrt{x}).$$

By partial summation,

$$\sum_{\substack{n \leq x \\ n \text{ squarefree}}} \frac{1}{n} = \sum_{n \leq x} \frac{\mu^2(n)}{n} = \int_1^x \frac{R(t)}{t^2}\, dt + O(1) = \frac{\log x}{\zeta(2)} + O(1). \tag{3}$$

Similarly, we can deduce

$$\sum_{\substack{n \leq x \\ n \text{ squarefree}}} \frac{1}{\sqrt{n}} = \frac{2\sqrt{x}}{\zeta(2)} + O(\log x). \tag{4}$$

Using these, we prove the crucial lemma below.

Lemma 5. *For a prime p,*

$$\left| \sum_{\substack{ab \leq x, \\ a,b \text{ squarefree}}} \left(\frac{a+b}{p}\right) \right| \leq \frac{1}{\sqrt{p}\,(p+1)\,\zeta(2)^2}\, x \log x + O\left(x\right).$$

Proof. Recall that the Legendre symbol can be written using the Gauss sum as

$$\left(\frac{a}{p}\right) = \frac{1}{\tau} \sum_{c \neq 0} \left(\frac{c}{p}\right) e\left(\frac{ca}{p}\right),$$

where $e(t) = e^{2\pi i t}$ and

$$\tau = \sum_{b=1}^{p-1} \left(\frac{b}{p}\right) e\left(\frac{b}{p}\right)$$

is the Gauss sum. Hence, we have

$$\left(\frac{a+b}{p}\right) = \frac{1}{\tau} \sum_{c \neq 0} \left(\frac{c}{p}\right) e\left(\frac{c(a+b)}{p}\right).$$

Therefore,

$$\sum_{\substack{ab \leq x, \\ a,b \text{ squarefree}}} \left(\frac{a+b}{p}\right) = \frac{1}{\tau} \sum_{c \neq 0} \left(\frac{c}{p}\right) \sum_{\substack{ab \leq x, \\ a,b \text{ squarefree}}} e\left(\frac{c(a+b)}{p}\right),$$

and the innermost sum can be written as

$$\sum_{\substack{a \leq x, \\ a, \text{ squarefree}}} e\left(\frac{ca}{p}\right) \sum_{\substack{b \leq x/a, \\ b \text{ squarefree}}} e\left(\frac{cb}{p}\right). \tag{5}$$

This motivates us to consider

$$\sum_{\substack{b \leq Y, \\ b \text{ squarefree}}} e\left(\frac{cb}{p}\right).$$

Again, using the Möbius function to sift out non-squarefree numbers, we have

$$\sum_{\substack{b\le Y,\\ b \text{ squarefree}}} e\left(\frac{cb}{p}\right) = \sum_{b\le Y} e\left(\frac{cb}{p}\right)\sum_{t^2|b}\mu(t) = \sum_{t\le\sqrt{Y}}\mu(t)\sum_{s\le Y/t^2} e\left(\frac{ct^2s}{p}\right).$$

If t is not divisible by p, the inner sum is bounded giving a final contribution of $O(\sqrt{Y})$ in this case. Inserting this into (5) gives an estimate of $O(x)$, where the constant depends on p. If t is divisible by p, the contribution is

$$\sum_{\substack{t\le\sqrt{Y}\\ p|t}}\mu(t)\left[\frac{Y}{t^2}\right].$$

Note that

$$\sum_{\substack{t=1\\ p|t}}^{\infty}\frac{\mu(t)}{t^2} = \frac{-1}{p^2}\prod_{\substack{l \text{ prime}\\ l\neq p}}\left(1-\frac{1}{l^2}\right) = \frac{-1}{p^2}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{l \text{ prime}}\left(1-\frac{1}{l^2}\right) = \frac{-1}{(p^2-1)\zeta(2)}.$$

Thus, we have

$$\left|\sum_{\substack{t\le\sqrt{Y}\\ p|t}}\mu(t)\left[\frac{Y}{t^2}\right]\right| \le \frac{Y}{(p^2-1)\,\zeta(2)} + O\left(\sqrt{Y}\right).$$

Putting everything together along with the fact that $|\tau| = \sqrt{p}$, we get the lemma. □

4. **Proof of the main theorem**

When $p = 2$, note that $f_2(n) = \#\{1 \le a, b \le n : ab = n\} = d(n)$, the divisor function. It has already been established in Lemma 4 that

$$\sum_{\substack{n\le x\\ n \text{ squarefree}}} d(n) = Cx\log x + o(x\log x).$$

This proves the theorem for $p = 2$.

Henceforth, let $p \ge 3$ be a fixed prime and $f_p(n)$ be as above. Note that

$$2f_p(n) = \sum_{\substack{1\le a,b\le n\\ ab=n}}\left(\left(\frac{a+b}{p}\right)+1\right) - \sum_{\substack{1\le a,b\le n,\\ ab=n,\, p|a+b}} 1.$$

Let

$$S(x) = 2\sum_{\substack{n\le x\\ n \text{ squarefree}}} f_p(n).$$

Then

$$S(x) = \sum_{\substack{n\le x\\ n \text{ squarefree}}}\sum_{ab=n}\left(\frac{a+b}{p}\right) + \sum_{\substack{n\le x\\ n \text{ squarefree}}}\sum_{ab=n} 1 - \sum_{\substack{n\le x\\ n \text{ squarefree}}}\sum_{ab=n,\, p|a+b} 1.$$

Let us denote the three summations over $n \le x$ on the right hand side as S_1, S_2 and S_3 respectively.

We first obtain an upper bound on S_3. Observe that in S_3, we have that a and b are coprime for otherwise, n would not be squarefree. Therefore,

$$\begin{aligned} S_3 = \sum_{\substack{n \le x \\ n \text{ squarefree}}} \sum_{ab=n,\, p|a+b} 1 &= \sum_{\substack{a \le x \\ a \text{ squarefree}}} \sum_{\substack{b \le \frac{x}{a},\, p|a+b \\ (a,b)=1 \\ b \text{ squarefree}}} 1 \\ &\le \sum_{\substack{a \le x \\ a \text{ squarefree}}} \sum_{\substack{b \le \frac{x}{a},\, p|a+b \\ b \text{ squarefree}}} 1. \end{aligned}$$

The inner sum above is counting squarefree $b \le x/a$ which are congruent to $-a \pmod p$. Therefore, using (2) in Lemma 3 with $\epsilon = 1/4$, we get

$$\sum_{\substack{b \le \frac{x}{a},\, p|a+b \\ b \text{ squarefree}}} 1 = \frac{1}{\zeta(2)} \frac{p}{(p^2-1)} \frac{x}{a} + O\left(\left(\frac{x}{ap}\right)^{1/2} + p^{3/4}\right).$$

Inserting this estimate in the upper bound for S_3, together with (3) and (4), gives

$$\begin{aligned} S_3 &\le \frac{1}{\zeta(2)} \frac{p}{(p^2-1)} \sum_{\substack{a \le x \\ a \text{ squarefree}}} \frac{x}{a} + \sqrt{x}\, O\left(\sum_{\substack{a \le x \\ a \text{ squarefree}}} \frac{1}{\sqrt{a}}\right) + O(x) \\ &= \frac{1}{\zeta(2)^2} \frac{p}{(p^2-1)} x \log x + O(x), \end{aligned} \tag{6}$$

where the implied constant in the O-term depends on p.

We estimate S_2 using Lemma 4:

$$S_2 = Cx \log x + o(x \log x). \tag{7}$$

Finally, we estimate S_1 as follows. The condition that $n = ab$ is squarefree can be re-written using the Möbius function.

$$\begin{aligned} S_1 = \sum_{\substack{n \le x \\ n \text{ squarefree}}} \sum_{ab=n} \left(\frac{a+b}{p}\right) &= \sum_{\substack{ab \le x \\ a,b \text{ squarefree}}} \left(\frac{a+b}{p}\right) \sum_{\substack{d|a \\ d|b}} \mu(d) \\ &= \sum_{d \le x} \mu(d) \left(\frac{d}{p}\right) \sum_{\substack{ab \le x/d^2 \\ a,b \text{ squarefree}}} \left(\frac{a+b}{p}\right). \end{aligned}$$

By Lemma 5, we deduce

$$|S_1| \le \frac{1}{\sqrt{p}(p+1)\zeta(2)^2} \left(\sum_{d \le x} \frac{x}{d^2} \log\left(\frac{x}{d^2}\right)\right) + O(x) = \frac{1}{\sqrt{p}\,(p+1)\,\zeta(2)} x \log x + O(x). \tag{8}$$

Putting everything together, for a fixed prime p, we have

$$S(x) = S_1 + S_2 - S_3,$$

Now by (6), (7) and (8), we get that

$$S(x) \geq \left[C - \frac{1}{\sqrt{p}(p+1)\zeta(2)} - \frac{p}{(p^2-1)\zeta(2)^2}\right] x\log x + o_p(x\log x).$$

Since the constant in brackets above is minimized when $p = 3$,

$$C - \frac{1}{\sqrt{p}\,(p+1)\,\zeta(2)} - \frac{p}{(p^2-1)\,\zeta(2)^2} > C - \frac{1}{4\sqrt{3}\,\zeta(2)} - \frac{3}{8\,\zeta(2)^2} = 0.10\ldots > 0.$$

The above inequality implies that $S(x) \gg x\log x$, thus establishing that $f_p(n)$ is unbounded as n ranges over squarefree numbers.

□

5. **Concluding remarks**

An examination of the algorithm described in Section 2 shows that we can consider the more general function $f(n; A)$ for squarefree n which counts the number of factorizations $ab = n$ such that $a+b+A$ is a perfect square. The function $f(n)$ corresponds to the case $A = 0$. Our analysis can be extended to study $f_p(n; A)$ which counts the number of factorizations such that $a+b+A$ is a square mod p. This may be of some help in our search for elliptic curves of unbounded Mordell-Weil rank.

Acknowledgements

We thank the referee for a careful reading and helpful comments on an earlier version of the paper.

References

[1] D. Clark, An arithmetical function associated with the rank of elliptic curves, *Canadian Math. Bulletin,* **34** (2) (1991), 181-185.

[2] J. Coates, Elliptic curves and Iwasawa theory, pp. 51-74 in Modular Forms, edited by Robert A. Rankin, Ellis Horwood Limited, 1984.

[3] C. Hooley, A note on square-free numbers in arithmetic progressions, *Bull. London Math. Soc.*, **7**, (1975), 133–138.

[4] M. Ram Murty, Problems in Analytic Number Theory, Second Edition, Graduate Texts in Mathematics 206, Springer, 2008.

[5] J. Silverman and J. Tate, Rational Points on Elliptic Curves, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

Institute of Mathematical Sciences (HBNI), CIT Campus Taramani, Chennai, Tamil Nadu, India 600113

Department of Mathematics and Statistics, Queen's University, Kingston, Canada, ON K7L 3N6.

Chennai Mathematical Institute, H-1 SIPCOT IT Park, Siruseri, Kelambakkam, Tamil Nadu, India 603103.

Email address: anupdixit@imsc.res.in
Email address: murty@queensu.ca
Email address: siddhi@cmi.ac.in