An average upper bound for a divisibility set

Runbo Li

Abstract

For a positive integer n, put

$$S_n = \{(a,b) \in \mathbb{N}^2 : a, b < \sqrt{n},\ n \mid a^2 + b^3 + 1\}.$$

We prove that

$$\sum_{n \leqslant N} |S_n| \ll N.$$

The proof uses the Hasse–Weil bound. We also give an elementary proof of a weaker result

$$\sum_{n \leqslant N} |S_n| \ll N^{1+\varepsilon}.$$

1 Introduction

For a positive integer n, put

$$S_n = \{(a,b) \in \mathbb{N}^2 : a, b < \sqrt{n},\ n \mid a^2 + b^3 + 1\}. \tag{1}$$

It is easy to show that $|S_n| < \sqrt{n}$ for every $n \geqslant 2$: we fix b and suppose that $(a_1, b) \in S_n$ and $(a_2, b) \in S_n$, where $a_1 \leqslant a_2$. Since $a_1^2 \equiv a_2^2 (\mathrm{mod} n)$ and $0 < a_1^2 \leqslant a_2^2 < n$, we must have $a_1^2 = a_2^2$ and $a_1 = a_2$. Thus there is at most one a for every $b < \sqrt{n}$, and $|S_n| < \sqrt{n}$. In 2024, Yuxing Ye proved that for every $n \geqslant 10$, we have

$$|S_n| < n^{\frac{1}{2} - \frac{c}{\log\log n}} \tag{2}$$

with some $c > 0$.

In the present note, we focus on the average upper bound for $|S_n|$. Our main result is the following theorem.

Theorem 1.1. *For every sufficiently large N, we have*

$$\sum_{n \leqslant N} |S_n| \ll N.$$

Put $X = \sqrt{N}$ and

$$F(A, B) = A^2 + B^3 + 1. \tag{3}$$

If $(a, b) \in S_n$, then $n \mid F(a, b)$ and we can define

$$q = \frac{F(a, b)}{n}. \tag{4}$$

The inequalities $a < \sqrt{n}$ and $b < \sqrt{n}$ imply

$$F(a, b) = a^2 + b^3 + 1 < n + bn + 1 = (b + 1)n + 1. \tag{5}$$

Since q is an integer, (5) gives

$$q = \frac{F(a, b)}{n} < b + 1. \tag{6}$$

On the other hand, $n \leqslant N = X^2$ gives

$$q = \frac{a^2 + b^3 + 1}{n} \geqslant \frac{b^3}{X^2}. \tag{7}$$

Since $n = F(a, b)/q$, the map $(n, a, b) \mapsto (a, b, q)$ is injective. Thus, we have

$$\sum_{n \leqslant N} |S_n| \leqslant \sum_{\substack{1 \leqslant a, b \leqslant X \\ b^3 X^{-2} \leqslant q \leqslant b+1 \\ q \mid F(a,b)}} 1. \tag{8}$$

2 The Hasse–Weil bound

For $q \geqslant 1$, define

$$\rho(q) = |\{(u, v) \bmod q : F(u, v) \equiv 0 (\mathrm{mod} q)\}|, \qquad g(q) = \frac{\rho(q)}{q}.$$

The Chinese remainder theorem shows that ρ and g are multiplicative.

Lemma 2.1. *We have, uniformly for $Y \geqslant 2$,*

$$\sum_{q \leqslant Y} g(q) \ll Y,$$

$$\sum_{L < q \leqslant U} \frac{g(q)}{q} \ll 1 + \log \frac{U}{L} \qquad (1 \leqslant L < U),$$

$$\sum_{q \leqslant Y} q g(q) \ll Y^2.$$

Proof. Let

$$C : B^3 + A^2Z + Z^3$$

be the projective closure of $F(A, B) = 0$. For $p > 3$, the partial derivatives are

$$F_A = 2AZ, \qquad F_B = 3B^2, \qquad F_Z = A^2 + 3Z^2.$$

If they vanished simultaneously, then $B = 0$, and either $Z = 0$ or $A = 0$. In the first case $[A : B : Z] = [0 : 0 : 0]$, and in the second case the same conclusion follows from $F_Z = 0$. Thus $C_{\mathbb{F}_p}$ is smooth. A smooth plane cubic is geometrically irreducible and has genus 1. The Hasse–Weil bound in this case is thus

$$|\#C(\mathbb{F}_p) - (p + 1)| \leqslant 2\sqrt{p}.$$

The line at infinity is $Z = 0$, and then $B^3 = 0$, so it consists of the single point $[1 : 0 : 0]$. Therefore,

$$\rho(p) = \#C(\mathbb{F}_p) - 1 = p + O(\sqrt{p}) \qquad (p > 3) \tag{9}$$

with an absolute implied constant.

Every affine solution modulo $p > 3$ has at least one of $2A$ and $3B^2$ nonzero. The multivariable Hensel lemma therefore says that each solution modulo p^r has exactly p lifts modulo p^{r+1}: one coordinate is uniquely determined modulo p^{r+1} after the other coordinate is chosen arbitrarily modulo p^{r+1}. Hence

$$\rho(p^r) = p^{r-1}\rho(p) \qquad (p > 3, r \geqslant 1) \tag{10}$$

and

$$g(p^r) = g(p) = 1 + O(p^{-\frac{1}{2}}) \qquad (p > 3, r \geqslant 1). \tag{11}$$

It remains to control the two "bad" primes 2 and 3. We first prove an elementary estimate.

Lemma 2.2. *For a fixed p, $r \geqslant 1$ and $c \in \mathbb{Z}$, we have*

$$|\{x \bmod p^r : x^2 \equiv c (\mathrm{mod} p^r)\}| \ll p^{\frac{1}{2}\min(v_p(c), r)}.$$

Proof. Suppose first that $v_p(c) < r$. Solutions can occur only when $v = 2s$ is even. Writing $x = p^s y$ reduces the equation to a unit square congruence modulo p^{r-2s}. Such a congruence has at most two roots for odd p and at most four roots for $p = 2$; the free higher digits contribute p^s.

If $v_p(c) \geqslant r$, the congruence $x^2 \equiv 0 (\mathrm{mod} p^r)$ has $p^{r-\lceil \frac{r}{2} \rceil} \leqslant p^{\frac{r}{2}}$ roots. □

We have

$$B^3 + 1 = (B + 1)(B^2 - B + 1).$$

For $p = 2$, the factor $B^2 - B + 1$ is always odd, and hence

$$v_2(B^3 + 1) = v_2(B + 1).$$

Among the B modulo 2^r, at most 2^{r-j} satisfy $v_2(B+1)=j$ for $0\leqslant j<r$, and one class has valuation at least r. Now Lemma 2.2 and summing over B gives

$$\rho(2^r)\ll\sum_{0\leqslant j<r}(2^{r-j}2^{\frac{j}{2}})+2^{\frac{r}{2}}\ll 2^r.$$

Write $T=B+1$, then

$$B^3+1=T(T^2-3T+3).$$

we have $v_3(B^3+1)=0$ if $3\nmid T$, while

$$v_3(B^3+1)=v_3(T)+1$$

if $3\mid T$. Thus the number of $B \bmod 3^r$ for which $\min(v_3(B^3+1),r)=j$ is $O(3^{r-j+1})$. Similarly, Lemma 2.2 gives

$$\rho(3^r)\ll\sum_{0\leqslant j\leqslant r}(3^{r-j+1}3^{\frac{j}{2}})\ll 3^r.$$

We have therefore proved

$$g(2^r)+g(3^r)\ll 1\qquad(r\geqslant 1).\tag{12}$$

Define the Dirichlet convolution $h=g*\mu$, where μ is the Möbius function. Since g and μ are multiplicative, h is also multiplicative. We also have

$$h(p^r)=g(p^r)-g(p^{r-1})\qquad(r\geqslant 1).$$

Since $g(1)=1$, we have $h(p)=g(p)-1$. By (11) and (12), we have

$$\sum_p\sum_{r\geqslant 1}\frac{|h(p^r)|}{p^r}<\infty.$$

The Euler product gives

$$\sum_{m=1}^{\infty}\frac{|h(m)|}{m}=\prod_p\left(1+\sum_{r\geqslant 1}\frac{|h(p^r)|}{p^r}\right)<\infty.$$

Using $g(n)=\sum_{d|n}h(d)$ (the Möbius inversion formula), we get

$$\sum_{n\leqslant Y}g(n)\leqslant\sum_{n\leqslant Y}\sum_{d|n}|h(d)|=\sum_{d\leqslant Y}|h(d)|\left\lfloor\frac{Y}{d}\right\rfloor\leqslant Y\sum_{d=1}^{\infty}\frac{|h(d)|}{d}\ll Y.$$

Partial summation then gives

$$\sum_{L<q\leqslant U}\frac{g(q)}{q}=\frac{G(U)}{U}-\frac{G(L)}{L}+\int_L^U\frac{G(t)}{t^2}dt\ll 1+\log\frac{U}{L},\qquad G(t)=\sum_{q\leqslant t}g(q)$$

since $G(t)\ll t$. Finally,

$$\sum_{q\leqslant Y}qg(q)\leqslant Y\sum_{q\leqslant Y}g(q)\ll Y^2.$$

Now Lemma 2.1 is proved. □

3 Proof of Theorem 1.1

Now we want to give an upper bound for the sum

$$\sum_{\substack{1\leqslant a,b\leqslant X\\ b^3X^{-2}\leqslant q\leqslant b+1\\ q|F(a,b)}} 1. \tag{13}$$

We first split the summation range of b into dyadic intervals $B < b \leqslant 2B$, where $1 \leqslant B \leqslant X$. In one such interval, every q occurring in (13) satisfies

$$L_B \leqslant q \leqslant 3B, \qquad L_B := \max\left(1, \frac{B^3}{X^2}\right).$$

For a fixed q, each residue class modulo q occurs at most $\frac{X}{q}+1$ times among $1 \leqslant a \leqslant X$ and at most $\frac{B}{q}+1$ times among $B < b \leqslant 2B$. Therefore

$$\begin{aligned}|\{1 \leqslant a \leqslant X,\ B < b \leqslant 2B : q \mid F(a,b)\}| &\leqslant \rho(q)\left(\frac{X}{q}+1\right)\left(\frac{B}{q}+1\right)\\ &= \frac{XB}{q}g(q) + Xg(q) + Bg(q) + qg(q). \end{aligned}\tag{14}$$

Summing over $L_B \leqslant q \leqslant 3B$ and by Lemma 2.1, we have

$$\sum_{\substack{1\leqslant a\leqslant X\\ B<b\leqslant 2B\\ L_B\leqslant q\leqslant 3B\\ q|F(a,b)}} 1 \ll XB\left(1+\log\frac{3B}{L_B}\right) + B^2. \tag{15}$$

If $B \leqslant X^{\frac{2}{3}}$, then $L_B = 1$. A dyadic summation gives

$$\sum_{B\leqslant X^{\frac{2}{3}}} XB\left(1+\log(3B)\right) + \sum_{B\leqslant X^{\frac{2}{3}}} B^2 \ll X^{\frac{5}{3}}\log(2X) + X^{\frac{4}{3}} \ll X^2 = N. \tag{16}$$

If $X^{\frac{2}{3}} < B \leqslant X$, then $L_B = B^3X^{-2}$. Writing $B \asymp X2^{-j}$, we have

$$\log\frac{3B}{L_B} = \log\frac{3X^2}{B^2} \ll 1 + j. \tag{17}$$

Hence

$$\sum_j XB(1+j) \ll X^2\sum_{j\geqslant 0} 2^{-j}(1+j) \ll X^2 = N, \tag{18}$$

$$\sum_j B^2 \ll X^2 = N. \tag{19}$$

Combining (8), (16), (18) and (19), Theorem 1.1 is proved.

4 An elementary argument

In this section we use an elementary method to prove a weaker result

$$\sum_{n\leqslant N}|S_n|\ll N^{1+\varepsilon}.$$

By exchanging the order of summation, we get

$$\sum_{n\leqslant N}|S_n|=\sum_{n\leqslant N}\sum_{\substack{1\leqslant a,b\leqslant\sqrt{n}\\ n|F(a,b)}}1=\sum_{a,b\geqslant 1}\sum_{\substack{\max(a^2,b^2)\leqslant n\leqslant N\\ n|F(a,b)}}1\leqslant\sum_{1\leqslant a,b\leqslant X}\tau(F(a,b)),\tag{20}$$

where τ is the divisor function. The classical bound for the divisor function gives $\tau(m)\ll m^{\varepsilon_1}$ for every $\varepsilon_1>0$. Let $\varepsilon_1=\frac{2}{3}\varepsilon$, by (20) we have

$$\sum_{n\leqslant N}|S_n|\leqslant\sum_{1\leqslant a,b\leqslant X}\tau(F(a,b))\ll\sum_{1\leqslant a,b\leqslant X}(a^2+b^3+1)^{\frac{2}{3}\varepsilon}\ll N\cdot N^{\varepsilon}=N^{1+\varepsilon}.\tag{21}$$

The proof is now completed.

Email address: runbo.li.carey@gmail.com