Erdős PROBLEM #675, SUBQUESTION (A):

A SUPER-POLYNOMIAL LOWER BOUND ON LOCAL PERIODS OF THE SUMS-OF-TWO-SQUARES SET

YU LEON LIU

ABSTRACT. Let E be the set of sums of two squares. We prove that, for every fixed $0 < c < 1/10$ and all sufficiently large n, every positive integer t satisfying the n-translation property for E (that is, $a \in E \iff a + t \in E$ for all $1 \le a \le n$) must exceed $\exp(n^c)$. We do not address the existence of such t, that is, whether E has the translation property.

Definition 1. For a subset $A \subset \mathbb{N}$ and positive integer n, we say that a positive integer t satisfies the n-translation property for A if

$$a \in A \quad \iff \quad a + t \in A$$

holds for all $1 \le a \le n$. We say that A has the *translation property* if for every $n > 0$ there exists t satisfying the n-translation property for A.

Problem 675 [1] has three parts:

(a) Does the set of sums of two squares have the translation property?
(b) If we partition all primes into $P \sqcup Q$ such that each part contains $\gg x/\log x$ many primes $\le x$ for all large x, does the set of integers only divisible by primes from P have the translation property?
(c) If A is the set of squarefree numbers, how fast does the minimal such t_n satisfying the n-translation property of A grow? Is $t_n > \exp(n^c)$ for some constant $c > 0$?

Here we make the following progress on part (a) concerning sums of two squares:

Theorem 2. *Let E be the set of positive integers expressible as $a^2 + b^2$ with $a, b \in \mathbb{Z}_{\ge 0}$. For every $0 < c < \frac{1}{10}$, there exists N_c such that for all $n \ge N_c$, every t satisfying the n-translation property for E satisfies*

$$t > \exp(n^c).$$

Remark 3. We *do not* prove part (a), i.e., that the set E satisfies the translation property. We do show that if E has the translation property, then t grows faster than $\exp(n^c)$ as in Theorem 2.

Remark 4. We discuss potential improvements on the constant $\frac{1}{10}$ in Remark 12.

First we note that

$$E = \{m \ge 1 \mid v_p(m) \text{ is even for all primes } p \equiv 3 \pmod 4\}. \tag{5}$$

We have the following lemma:

Lemma 6. *Let $p \equiv 3 \pmod 4$ and $n \ge 1$. Suppose t satisfies the n-translation property for E. Then for any $a \in E \cap [1, n]$ with*

$$a \equiv -t \pmod p,$$

we have

$$a \equiv -t \pmod{p^2}.$$

Proof. By construction we have $p \mid a+t$, and the n-translation property implies that $a+t \in E$. It follows from (5) that $p^2 \mid a+t$, and thus

$$a \equiv -t \pmod{p^2}.$$

□

Next, we show that any sufficiently small prime $p \equiv 3 \pmod 4$ must divide t. The idea is to find a, b that are both $\equiv -t \pmod p$ but differ modulo p^2.

Lemma 7. *Let $p \equiv 3 \pmod 4$ be prime. There exists N_p such that, for every $n \geq N_p$ and every $t \geq 1$ satisfying the n-translation property for E, we have $p \mid t$.*

Proof. For each nonzero residue class $r \pmod p$, the residues r and $r+p$ differ modulo p^2. By the Chinese remainder theorem, there are unique classes $u_{r,0}, u_{r,1} \pmod{4p^2}$ satisfying

$$u_{r,0} \equiv 1 \pmod 4, \quad u_{r,0} \equiv r \pmod{p^2},$$
$$u_{r,1} \equiv 1 \pmod 4, \quad u_{r,1} \equiv r+p \pmod{p^2}.$$

Since $r \not\equiv 0 \pmod p$ and each $u_{r,j} \equiv 1 \pmod 4$, both $u_{r,0}$ and $u_{r,1}$ are coprime to $4p^2$. By Dirichlet's theorem on primes in arithmetic progressions, there exist primes $\ell_{r,0}$ and $\ell_{r,1}$ with

$$\ell_{r,0} \equiv u_{r,0} \pmod{4p^2}, \qquad \ell_{r,1} \equiv u_{r,1} \pmod{4p^2}.$$

Each $\ell_{r,j} \equiv 1 \pmod 4$, hence lies in E by (5). Let

$$N_p \coloneqq \max_{\substack{1 \leq r \leq p-1 \\ j \in \{0,1\}}} \ell_{r,j}.$$

Now suppose $n \geq N_p$ and t has the n-translation property for E, and assume for contradiction that $p \nmid t$. Pick $r \in \{1, \dots, p-1\}$ with $r \equiv -t \pmod p$. The witnesses $\ell_{r,0}, \ell_{r,1} \in E \cap [1,n]$ both satisfy $\ell_{r,j} \equiv r \equiv -t \pmod p$, so Lemma 6 forces $\ell_{r,j} \equiv -t \pmod{p^2}$ for $j \in \{0,1\}$. In particular $\ell_{r,0} \equiv \ell_{r,1} \pmod{p^2}$. But by construction $\ell_{r,0} \equiv r \pmod{p^2}$ and $\ell_{r,1} \equiv r+p \pmod{p^2}$, so $\ell_{r,0} \not\equiv \ell_{r,1} \pmod{p^2}$, a contradiction. It follows that $p \mid t$. □

Remark 8. In the proof above we chose $\ell_{r,j}$ to be primes because that guarantees they lie in E. In fact, any choice of $\ell_{r,0}, \ell_{r,1} \in E$ satisfying

$$\ell_{r,0} \equiv r \pmod{p^2}, \qquad \ell_{r,1} \equiv r+p \pmod{p^2}$$

suffices, and a careful choice could yield a better bound.

Next, we bound N_p as a function of p:

Theorem 9 (Linnik [4])**.** *There exist constants $C > 0$ and $L > 0$ such that for any modulus $q \geq 2$ and any residue class a with $1 \leq a \leq q-1$ and $\gcd(a,q) = 1$, the smallest prime $p_0 \equiv a \pmod q$ satisfies $p_0 \leq Cq^L$.*

The best current unconditional value is $L \leq 5$, due to Xylouris [5].

Proof of Theorem 2. Let $p \equiv 3 \pmod 4$ be a prime. Applying Theorem 9 with $q = 4p^2$, we see that we can choose primes $\ell_{r,j}$ with

$$\ell_{r,j} \leq C(4p^2)^L.$$

Thus, with $A = 4^L C$, we have

$$N_p \leq Ap^{2L}.$$

In particular, if $p \le (n/A)^{1/(2L)}$, then $n \ge N_p$, so any t satisfying the n-translation property for E has $p \mid t$ by Lemma 7.

Let $y := (n/A)^{1/(2L)}$. It follows that

$$\prod_{\substack{p \le y \\ p \equiv 3 \pmod 4}} p \,\Big|\, t.$$

By the prime number theorem in arithmetic progressions (see e.g. Davenport [3]), the primes $\equiv 3 \pmod 4$ have density $\frac{1}{2}$ among the odd primes, so

$$\sum_{\substack{p \le y \\ p \equiv 3 \pmod 4}} \log p \;\sim\; \frac{y}{2} \qquad \text{as } y \to \infty. \tag{10}$$

Fix a constant $c_1 \in (0, \frac{1}{2})$, say $c_1 = \frac{1}{4}$. By (10), there exists a threshold $y_0 = y_0(c_1)$ such that for all $y \ge y_0$,

$$\sum_{\substack{p \le y \\ p \equiv 3 \pmod 4}} \log p \;\ge\; c_1 y. \tag{11}$$

Set $N_1 := A \cdot y_0^{2L}$, so that $n \ge N_1$ guarantees $y = (n/A)^{1/(2L)} \ge y_0$. For all such n, combining the divisibility above with (11) gives

$$\log t \;\ge \sum_{\substack{p \le y \\ p \equiv 3 \pmod 4}} \log p \;\ge\; c_1 y \;=\; K n^{1/(2L)},$$

where $K := c_1 A^{-1/(2L)}$.

Now fix any $0 < c < 1/(2L)$; since $L \le 5$, every $0 < c < 1/10$ satisfies this. Since the exponent gap $1/(2L) - c$ is positive, the inequality $K n^{1/(2L)} > n^c$, equivalently $n^{1/(2L)-c} > K^{-1}$, holds for all $n \ge N_2(c) := \lfloor K^{-2L/(1-2Lc)} \rfloor + 1$. Setting

$$N_c := \max\big(\lceil N_1 \rceil,\; N_2(c)\big),$$

we conclude that for every $n \ge N_c$,

$$\log t \;\ge\; K n^{1/(2L)} \;>\; n^c, \qquad \text{i.e., } t > \exp(n^c). \qquad \square$$

Remark 12. The constant $\frac{1}{10}$ in Theorem 2 arose as $\frac{1}{2L}$ with $L \le 5$ from [5]. There are two potential ways to improve it.

First, by improving Linnik's constant. Under the Generalized Riemann Hypothesis, one has $p_{\min}(a, q) \ll \varphi(q)^2 (\log q)^2$, which sets Linnik's constant to $L \le 2 + \epsilon$ in Theorem 9. This pushes the conclusion of Theorem 2 to $t > \exp(n^c)$ with $0 < c < \frac{1}{4}$. The Linnik conjecture, $p_{\min}(a, q) \ll_\varepsilon q^{1+\varepsilon}$ for every $\varepsilon > 0$, would further yield $t > \exp(n^c)$ for every $0 < c < \frac{1}{2}$.

Second, by relaxing the choice of witnesses. As noted in the remark following Lemma 7, we never used that the witnesses $\ell_{r,j}$ are prime; any $\ell_{r,j} \in E$ with the prescribed residue $\pmod{p^2}$ suffices. Bounding the smallest such $\ell_{r,j}$ is a question about E in arithmetic progressions; sharp bounds here would likely improve the constant further.

Acknowledgements

The proof in this note was discovered with the assistance of OpenAI's Codex together with the Rethlas open-source agentic mathematics-research pipeline. The strategy is directly inspired by Ho Boon Suan's proof of the analogous super-polynomial lower bound for the squarefree subquestion

(c) of Erdős Problem 675 [2]. All mathematical arguments and claims in the final manuscript were independently verified by the author, who takes full responsibility for the paper.

References

[1] T. F. Bloom, *Erdős Problem #675*, https://www.erdosproblems.com/675, accessed 10 May 2026. 1

[2] Ho Boon Suan, *A squarefree lower bound for Erdős Problem 675*, note, 18 April 2026, https://boonsuan.github.io/erdos675_squarefree.pdf. 4

[3] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000. Revised and with a preface by Hugh L. Montgomery. 3

[4] U. V. Linnik, *On the least prime in an arithmetic progression. I. The basic theorem*, Rec. Math. [Mat. Sbornik] N.S. **15(57)** (1944), no. 2, 139–178. 2

[5] T. Xylouris, *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*, PhD thesis, Rheinische Friedrich-Wilhelms-Universität Bonn, 2011; also published as *Bonner Mathematische Schriften* **404**, Universität Bonn, Mathematisches Institut, Bonn, 2011. 2, 3

1 Oxford St, Cambridge, MA 02139

Email address: yuleonliu@math.harvard.edu