LATTICE POINTS ON CIRCLES
OPEN PROBLEMS IN NUMBER THEORY
SPRING 2018, TEL AVIV UNIVERSITY

ZEÉV RUDNICK

Contents

1. Lattice points on circles

We study the distribution of lattice points on circles.

1.1. Fermat's theorem.

We begin with Fermat's work on representing an integer as a sum of two squares.

Theorem 1.1. *A prime p is a sum of two squares if and only if $p \neq 3 \bmod 4$, and in that case the number of representations is 4 if $p = 2$, and 8 if $p = 1 \bmod 4$.*

Proof. We recall a proof of the claim for primes, which is based on unique factorization into irreducibles in the ring $\mathbb{Z}[i]$ of Gaussian integers. We recall that $\mathbb{Z}[i]$ is a Euclidean domain w.r.t. the norm $N(\alpha) = \alpha\bar{\alpha}$, and the units are precisely the elements of norm 1, that is $\pm 1, \pm i$.

We take a prime $p = 1 \bmod 4$ and want to show that it is a sum of two squares: $p = a^2 + b^2$. Firstly, note that this condition is *equivalent* to $p = \alpha\beta$ being reducible in $\mathbb{Z}[i]$, where α, β are not units, i.e. $N(\alpha), N(\beta) > 1$. Clearly if $p = a^2 + b^2 = (a + ib)(a - ib)$ then it is reducible (if $p > 2$). Conversely, if $p = \alpha\beta$, take norms to obtain $p^2 = N(\alpha)N(\beta)$ and since $N(\alpha), N(\beta) > 1$ we must have $N(\alpha) = p = N(\beta)$ by unique factorization in $\mathbb{Z}$, hence $p = N(\alpha) = a^2 + b^2$ if $\alpha = a + ib$.

So we want to show that p is reducible (splits) in $\mathbb{Z}[i]$. Assume by contradiction that p is irreducible, which since $\mathbb{Z}[i]$ is Euclidean, means that p is prime, i.e. if $p \mid \gamma \cdot \delta$ in $\mathbb{Z}[i]$ then $p \mid \gamma$ or $p \mid \delta$.

We use Fermat's theorem, that if $p = 1 \bmod 4$ then -1 is a quadratic residue: $-1 = x^2 \bmod p$. Thus $x^2 + 1 = pn$. Factor this equation in $\mathbb{Z}[i]$ to obtain

$$(x + i)(x - i) = pn$$

Date: May 30, 2018.

and by the above, since we assume p is irreducible, this means that $p \mid x+i$ or $p \mid x-i$ (and in fact both). So

$$x+i = p(m+ni)$$

for some $m+ni \in \mathbb{Z}[i]$. But comparing imaginary parts gives $1 = pm$, which cannot happen.

So we showed that p is reducible, hence a sum of two squares. We claim that there is essentially only one factorization $p = \pi\bar{\pi}$, with π necessarily irreducible (hence prime) in $\mathbb{Z}[i]$. This is because of $N(\pi) = p$ is prime, then if $\pi = \alpha\beta$ then $p = N(\pi) = N(\alpha)N(\beta)$ and since p is prime in $\mathbb{Z}$, we must have $N(\alpha) = 1$ or $N(\beta) = 1$, so that either α or β are units, hence π is irreducible.

Thus we find that if $p = N(\pi) = \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$, so either $\alpha = u\pi$ or $\alpha = u\bar{\pi}$, and taking norms gives $p = N(\alpha) = N(u)N(\pi) = N(u)p$ so that $u = \pm 1, \pm i$ is a unit. This says that either $\alpha = u\pi$ or $\alpha = u\bar{\pi}$, altogether 8 possibilities. □

Theorem 1.2. *A positive integer $n \geq 1$ is a sum of two squares if and only if whenever a prime $p = 3 \bmod 4$ divides n, it necessarily divides n to even order.*

The number of representations of $n = 2^a \prod_{p=1 \bmod 4} p^{b_p} \prod_{p=3 \bmod 4} p^{2c_p}$ as a sum of two squares is

$$r_2(n) = 4 \prod_{p=1 \bmod 4} (b_p + 1)$$

Corollary 1.3. $r_2(n) \leq d(n)/4$.

1.2. **An upper bound for the divisor function.** We saw that the *average* size of the divisor function $d(n)$ is $\log n$. What can we say about the maximum?

Theorem 1.4. $d(n) = O(n^{\varepsilon})$ *for all* $\varepsilon > 0$.

Note that one cannot do much better, since there are arbitrarily large n for which $d(n) > n^{(1-o(1))\log 2/\log\log n}$. To see this, take $n_K = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p_K$, the product of the first K primes. Then $d(n_K) = 2^K$ and we want to express 2^k in terms of n. By the Prime Number Theorem,

$$\log n_K = \sum_{p \leq p_K} \log p \sim p_K$$

and again using the Prime Number Theorem, $p_K \sim K \log K$ and so

$$\log n_K \sim K \log K$$

which gives

$$K \sim \log n_K / \log\log n_K$$

so that

$$d(n_K) = 2^K \approx 2^{\log n/\log\log n} = n^{\log 2/\log\log n}.$$

Proposition 1.5. *if $f(n)$ is a multiplicative function, such that for all prime powers,*

$$f(p^k) \to 0, \quad p^k \to \infty \tag{1.1}$$

then $\lim_{n\to\infty} f(n) = 0$.

If we take $f(n) = d(n)/n^\varepsilon$ then clearly

$$f(p^k) = \frac{d(p^k)}{p^{k\varepsilon}} = \frac{k+1}{p^{k\varepsilon}} \to 0,$$

as $k \to \infty$ so that $d(n)/n^\varepsilon \to 0$ by (1.1).

Proof. Let

$$S := \{q = p^k : |f(q)| > 1\}$$

Note that S is a finite set because we assume that $f(p^k) \to 0$ as $p^k \to \infty$ and therefore

$$A = A_f := \prod_{p^k \in S} |f(p^k)| < \infty.$$

Fix $\epsilon > 0$. Then there is some $Q \geq 1$ so that $p^k > Q$ implies $|f(p^k)| < \epsilon$. Divide the prime powers into three disjoint subsets:

$$\mathcal{Q}_1 := \{q = p^k \leq Q : |f(q)| \leq 1\}$$

$$\mathcal{Q}_2 := \{q = p^k \leq Q : |f(q)| > 1\}$$

in particular $\mathcal{Q}_2 \subseteq \{q = p^k : |f(q)| > 1\} =: S$.

$$\mathcal{Q}_3 := \{q = p^k > Q\}$$

We may uniquely decompose each integer $n = n_1 n_2 n_3$ with n_j being a product of prime powers all lying in $\mathcal{Q}_j$: We write $n = \prod p_p^k$ as a product of powers of distinct primes, and separate these into one of the three sets $\mathcal{Q}_j$. In particular, n_j are pairwise coprime. Hence $f(n) = \prod_{j=1}^3 f(n_j)$.

We may assume that $n \gg 1$ is sufficiently large, so that it is not just a product $N = n_1 n_2$, that is that $n_3 \neq 1$. Then

- $|f(n_1)| \leq 1$
- $$|f(n_2)| = \prod_{p^k || n_2} |f(p^k)| \leq \prod_{p^k \in S} |f(p^k)| = A < \infty$$
- Since $n_3 \neq 1$
  $$|f(n_3)| = \prod_{p^k || n_3} |f(p^k)| \leq \epsilon$$
  as there is at least one factor $f(p^k)$ with $p^k \in \mathcal{Q}_3$.

Altogether we obtain

$$|f(n)| = |f(n_1)| \cdot |f(n_2)| \cdot |f(n_3)| \leq 1 \cdot A \cdot \epsilon = A\epsilon$$

Thus we showed that given any $\epsilon > 0$, there is some $N_\epsilon > 1$ so that for all $n > N_\epsilon$, $|f(n)| \leq A\epsilon$ (with $A = A_f$ an absolute constant). Thus $f(n) \to 0$ as $n \to \infty$. □

Since $r_2(n) \leq d(n)/4$, we deduce:

Corollary 1.6. *$r_2(n) = O(n^\varepsilon)$ for all $\varepsilon > 0$.*

We saw that the divisor function $d(n)$ has mean value $\log n$. What about $r_2(n)$? The naive answer is π, because we know that

$$\sum_{n \leq N} r_2(n) = \#\{(x, y) \in \mathbb{Z}^2 : x^2 + y^2 = n\} \sim \pi N.$$

so that

$$\frac{1}{N}\sum_{n\leq N} r_2(n) \sim \pi$$

However, it turns out that most of the terms are actually zero. Landau (1909) showed that

$$\#\{n \leq N : n = a^2 + b^2\} \sim K\frac{N}{\sqrt{\log N}}$$

where

$$K = \frac{1}{\sqrt{2}}\prod_{\substack{q=3 \bmod 4\\ \text{prime}}}(1-\frac{1}{q^2})^{-1/2} = \frac{\pi}{4}\prod_{\substack{p=1 \bmod 4\\ \text{prime}}}(1-\frac{1}{p^2})^{1/2} = 0.764\ldots$$

Hence if we condition on $r_2(n) > 0$, that is on $n = \square + \square$ being a sum of two squares, then the mean value is

$$\frac{1}{\#\{n \leq N : n = \square + \square\}}\sum_{\substack{n\leq N\\ n=\square+\square}} r_2(n) \sim \frac{\pi N}{KN/\sqrt{\log N}} = \frac{\pi}{K}\sqrt{\log N}$$

This is still significantly smaller than the mean value of the divisor function, which is $\log N$.

1.3. **Jarnik's theorem (1926)** [J].

Theorem 1.7. *An arc on the circle of length $r \ll R^{1/3}$ contains at most two lattice points.*

We begin with a simple proof which uses a classical result of Euclidean geometry:

Proof. There is a result attributed to Heron of Alexandria which says: in any triangle, the product of the lengths of its three sides a, b, c is equal to four times the area A of the triangle multiplied by the radius R of the circumscribed circle:

$$abc = 4AR.$$

This theorem has the following application: If P_1, P_2, P_3 are three lattice points on the circle $x^2 + y^2 = R^2$, then being a lattice triangle, its area $A \geq 1/2$. Moreover, the lengths of the sides, being lengths of integer vectors, are at least 1. Thus if $a = \max(||P_i - P_j||)$, then

$$a^3 \geq abc = 4AR \geq 4 \cdot \frac{1}{2} R = 2R$$

and so $\max ||P_i - P_j|| \geq (2R)^{1/3}$. In particular, an arc of length $(2R)^{1/3}$ contains, at most, two lattice points.

To prove Heron's formula: Let the point O be the center of the circumscribed circle, as in Figure 1 The area of the triangle is $A = \frac{1}{2} bc \sin \alpha$. We also know that

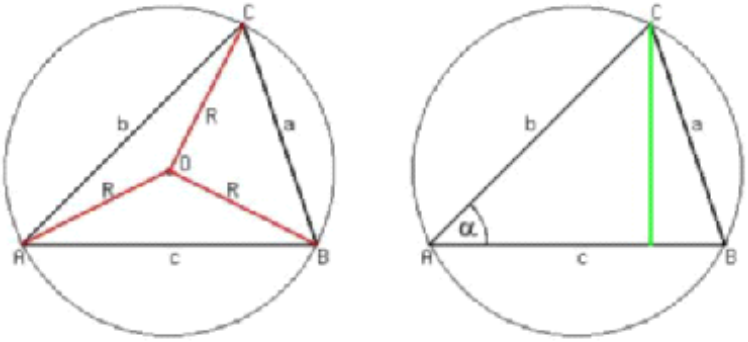

FIGURE 1

$\angle BPC = 2\angle BAC = 2\alpha$ and that $a = BC = 2R \sin \alpha$. Substituting we obtain $4AR = abc$. □

Here is a second (related) proof, with less reliance on classical geometry, which has the benefit of being extendable to higher dimensions:

Proof. Suppose we have three lattice points in the arc, which has length $r = o(R)$. We may assume that two of the lattice points are the boundary points of the arc, and the third lattice point lies somewhere in the middle, as in Figure 2. Let A be the area of the triangle formed by these three lattice points. Since the circle

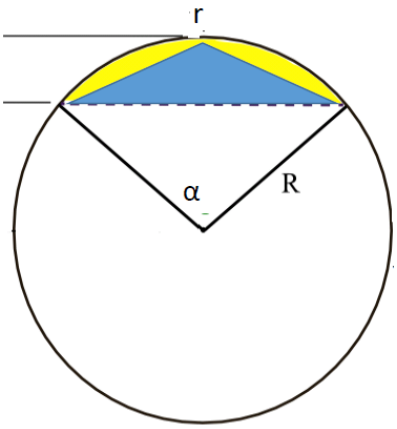

FIGURE 2

is convex, these lattice point cannot be co-linear, so that $A \neq 0$. we can compute the area of the triangle as $1/2$ times the cross product of the vectors forming sides of the triangle, and since these are integer vectors, their cross product (which is non-zero) has length ≥ 1, and so we find

$$A \geq 1/2.$$

On the other hand, the triangle is contained in the circular cap bounded by the two lattice points, and hence A bounded above by the area of this cap. We will show that this area is $\sim \frac{1}{12}\frac{r^3}{R}$, and hence we will obtain

$$\frac{1}{2} \leq \frac{1}{12}\frac{r^3}{R}\Big(1+o(1)\Big)$$

which gives $r \gg R^{1/3}$ as claimed.

Let $\alpha = r/R$ be the opening angle of the sector subtended by the arc. Then the area of the sector is $\pi R^2(\alpha/2\pi) = Rr/2$. The area of the cap is the difference between the area of the sector and the area of the triangle formed by the center of the circle and the two endpoints of the arc. The height of the triangle is $R\cos(\alpha/2)$, and its base is $2R\sin(\alpha/2)$, and hence its area is $R^2\sin\alpha/2\cos\alpha/2 = \frac{1}{2}R^2\sin(\alpha) = \frac{1}{2}R^2\sin(r/R)$. Thus

$$\text{area(cap)} = \frac{r}{2R} - \frac{1}{2}R^2\sin(r/R) \sim \frac{1}{2}\Big(\frac{r}{R} - (\frac{r}{R} - \frac{1}{3!}(\frac{r}{R})^3\Big) \sim \frac{1}{2\cdot 6}(\frac{r}{R})^3$$

as claimed. □

Exercise 1. *Show that the three lattice points*

$$(4n^3-1, 2n^2+2n), \quad (4n^3, 2n^2+1), \quad (4n^3+1, 2n^2-2n)$$

all lie on the circle $x^2+y^2 = R_n^2$, *with* $R_n^2 = 16n^6+4n^4+4n^2+1$, *and are contained in an arc of length* $(16R_n)^{1/3}+o(1)$. *Hence the exponent* $1/3$ *in Jarnik's theorem is sharp.*

Exercise 2. *Show that there is some $c > 0$ so that all lattice points in a cap of diameter $cR^{1/4}$ on the sphere $x^2 + y^2 + z^2 = R^2$ are co-planar.*

The following construction shows that we can have unbounded number of lattice points in very small caps in 3 dimensions: Given $K > 1$, find an integer n which has $r_2(n) = 4 \cdot 2^K$, e.g. $n = p_1 \cdot \cdots \cdot p_K$ where p_j are distinct primes $p_j = 1 \bmod 4$, and take $R^2 = N^2 + n$. Then for all solutions of $x_j^2 + y_j^2 = n$, we get a point (x_j, y_j, N) on the sphere of radius R, contained in the cap around the "north pole" of diameter $\approx \sqrt{n}$ if $N \gg 1$, which can be made arbitrarily small in terms of R.

1.4. **The Theorem of Cilleruelo and Cordoba.** Cilleruelo-Cordoba [C-C] (1992) went beyond Jarnik's theorem, showing that we cannot have m lattice points on an arc of size $> R^{b(m)}$.

Lemma 1.8. *Let $P_1, \dots, P_m$ be distinct lattice points on the circle $|x| = R$. Then*

$$\prod_{1 \le i < j \le m} |P_i - P_j| \ge R^{e(m)}, \qquad e(m) = \begin{cases} \frac{m}{2}(\frac{m}{2} - 1), & m \text{ even} \\ \\ \frac{1}{4}(m-1)^2, & m \text{ odd.} \end{cases}$$

Taking $m = 2$ in Lemma 1.8, it follows that

$$|P_0 - P_1| \, |P_1 - P_2| \, |P_2 - P_0| \ge R$$

and we recover Jarnik's theorem.

More generally, since there are $\binom{m}{2}$ pairs $\{P_i, P_j\}$, we obtain

$$\Big(\max_{1 \le i \ne j \le m} |P_i - P_j| \Big)^{\binom{m}{2}} \ge R^{e(m)}$$

or

$$\max_{1 \le i \ne j \le m} |P_i - P_j| \ge R^{\eta(m)}$$

with $\eta(m) = e(m)/\binom{m}{2}$.

m	3	4	5	6
$e(m)$	1	2	4	6
$\eta(m)$	1/3	1/3	2/5	2/5

Lemma 1.8 implies a uniform bound $B(\varepsilon)$ on the number of lattice points on an arc $C \subset \{|x| = R\}$ of size $r < R^{\frac{1}{2} - \varepsilon}$. More precisely

Lemma 1.9 ([C-C])**.** *Let $\delta(m) = \frac{1}{4\lfloor \frac{m}{2} \rfloor + 2}$. If $C \subset \{|x| = R\}$ is an arc of length $r < \sqrt{2} R^{\frac{1}{2} - \delta(m)}$, then C contains at most m lattice points.*

Cilleruello and Granville (2007) conjectured a uniform bound on the number of lattice points on any arc of length $\lambda^{1-\epsilon}$:

Conjecture 1. [C-G, Conjecture 14] *Let $0 < \epsilon < 1$. Then there is some $B_\epsilon > 0$ so that the number of lattice points on any arc $C \subset \{|x| = R\}$ of length $r < R^{1-\epsilon}$ is at most B_ϵ.*

Proof. The argument in [C-C] is arithmetic and based on factorization of $E = R^2$ in Gaussian primes. The following elegant and much simpler argument was given by Ramana [Ra] (2007): We identify the standard lattice $\mathbb{Z}^2 \subset \mathbb{R}^2$ with the Gaussian

integers $\mathbb{Z}[\sqrt{-1}] \subset \mathbb{C}$. If $\overline{P}$ denotes the complex conjugate of P, then our condition on the lattice points being on one circle says that

$$P_j \overline{P_j} = R^2, \quad j = 1, \dots, m$$

Ramana observed that for any $0 \le k \le m-1$, we have an identity

$$R^{k(k+1)} \prod_{1 \le i < j \le m} (P_j - P_i) = \Big(\prod_{i=1}^{m} P_i^k \Big) \cdot \det V_{k,m} \tag{1.2}$$

where $V_{k,m}$ is the following Vandermonde type matrix

$$V_{k,m} = \begin{pmatrix} \overline{P_1}^k & \overline{P_2}^k & \dots & \overline{P_m}^k \\ \overline{P_1}^{k-1} & \overline{P_2}^{k-1} & \dots & \overline{P_m}^{k-1} \\ \vdots & & & \\ 1 & 1 & \dots & 1 \\ P_1 & P_2 & \dots & P_m \\ \vdots & & & \\ P_1^{m-1-k} & P_2^{m-1-k} & \dots & P_m^{m-1-k} \end{pmatrix}$$

Once (1.2) is established, we take absolute values and noting that $|\det V_{k,m}|^2 \ge 1$ since it is a nonzero integer (!), we get

$$R^{k(k+1)} \prod_{1 \le i < j \le m} |P_j - P_i| \ge R^{km}$$

Taking $k = \lfloor \frac{m}{2} \rfloor$ gives Lemma 1.8. □

To see (1.2) , we compute the RHS of (1.2) by noting that $P_i^k \det V_{k,m}$ is the determinant of the matrix resulting from multiplying the i-th column of $V_{k,m}$ by P_i^k, and using $P_j \overline{P_j} = R^2$ one is reduced to computing an ordinary Vandermonde determinant, yielding the LHS of (1.2). □

1.5. **An almost everywhere result** [1]**.** We can show that Conjecture 1 is true for most $E = R^2 \in \mathbb{Z}_+$, in fact we have the stronger statement that all lattice points on the circle of radius $\sqrt{E}$ are well separated.

We will show that for all but $O(N^{1-\varepsilon})$ of the squared radii $E = R^2 \leq N$, the distance between any two lattice points is $\gg R^{1-\varepsilon/3}$, so that any arc of length $\gg R^{1-\varepsilon}$ contains a bounded number of lattice points. Since the total number of squared radii $E \leq N$ which are sums of two squares is $\approx N/\sqrt{\log N}$ (Landau's theorem), we deduce that "almost all" admissible radii are such that all lattice points on the circle of radius R= $\sqrt{E}$ are well-separated, in the sense that their minimal spacing is close to the average spacing.

Lemma 1.10. *Let $0 \neq z \in \mathbb{Z}^2$, and write $z = d\hat{z}$ with $d \geq 1$ and $\hat{z} \in \mathbb{Z}^2$ primitive, that is with coprime coordinates. Let $b \in \mathbb{Z}$. Then*

$$\#\{x \in \mathbb{Z}^2 : |x| \leq R, \quad x \cdot z = b\} \ll \frac{R}{|\hat{z}|} + 1$$

Proof. We recall that the linear Diophantine equation

$$ax + by = c$$

has integer solutions if and only if $\gcd(a, b) \mid c$, and in that case all integer solutions are generated from a particular one v_0 by the recipe

$$v_k = v_0 + k\frac{1}{\gcd(a, b)}(-b, a), \quad k \in \mathbb{Z}.$$

Thus writing $z = (a, b) \in \mathbb{Z}^2$, $d = \gcd(a, b)$, $\hat{z} = \frac{1}{d}(a, b)$ and $w = \frac{1}{d}(-b, a)$, we need to count the number of $k \in \mathbb{Z}$ for which

$$|v_0 + kw| \leq R$$

that is points on the line $v_0 + kw$ lying in a ball of radius R. The distance between successive points v_k is $|w|$, and so the worst case scenario is that the line is a diameter of the ball, hence of length $2R$, and then the number of such points on it is at most $2R/|w| + O(1)$. Note that this is just an upper bound; there could be no points if $b \gg R$. Since $|w| = |\hat{z}| = |z|/d$ we conclude the claim. □

Theorem 1.11. *Fix $\epsilon > 0$. Then for all but $O(N^{1-\epsilon/3})$ integers $E \leq N$, one has*

$$\min_{\substack{x \neq y \in \mathbb{Z}^2 \\ |x|^2 = |y|^2 = E}} |x - y| > (\sqrt{E})^{1-\epsilon}$$

Proof. We will say that $E \leq N$ is "exceptional" if there is a pair of close points $|x|^2 = |y|^2 = E$, $0 < |x - y| < \sqrt{E}^{1-\epsilon}$. Writing $z = x - y$, we see that the number of exceptional E's is bounded by the number of pairs of integer vectors $x \in \mathbb{Z}^2$, $0 \neq z \in \mathbb{Z}^2$ with

$$|x|^2 \leq N, \quad 0 < |z| < \sqrt{N}^{1-\epsilon}$$

and satisfying

$$2x \cdot z = |z|^2 \tag{1.3}$$

Writing $z = d\hat{z}$ with $d \geq 1$ and $\hat{z} \in \mathbb{Z}^2$ primitive, we use Lemma 1.10 to see that the number of $x < \sqrt{N}$ lying on the line (1.3) is $O(\sqrt{N}/|\hat{z}|)$ (We can dispense

with the $O(1)$ term since $|\hat{z}| \leq |z| < N^{1/2-\delta}$) and hence the number of exceptional $E \leq N$ is dominated by

$$\sum_{|z|<N^{1/2(1-\epsilon)}} \frac{\sqrt{N}}{|\hat{z}|} = \sum_{1\leq d\leq \sqrt{N}^{1-\epsilon}} \sum_{\substack{\hat{z}\in\mathbb{Z}^2 \text{ primitive} \\ |\hat{z}|\leq(\sqrt{N})^{1-\epsilon}/d}} \frac{\sqrt{N}}{|\hat{z}|}$$

Now

$$\sum_{\substack{\hat{z}\in\mathbb{Z}^2 \text{ primitive} \\ |\hat{z}|\leq Y}} \frac{1}{|\hat{z}|} \leq \sum_{0<|z|\leq Y} \frac{1}{|z|} \approx \int_{1\leq|z|\leq Y} \frac{1}{|z|} dz \approx Y$$

so that

$$\sum_{1\leq d\leq \sqrt{N}^{1-\epsilon}} \sum_{\substack{z'\in\mathbb{Z}^2 \text{ primitive} \\ |z'|\leq(\sqrt{N})^{1-\epsilon}/d}} \frac{\sqrt{N}}{|z'|} \ll \sqrt{N} \sum_{1\leq d\leq \sqrt{N}^{1-\epsilon}} \frac{(\sqrt{N})^{1-\epsilon}}{d} \ll N^{1-\epsilon/2}\log N$$

which proves our claim. □

References

[1] J. Bourgain and Z. Rudnick On the geometry of the nodal lines of eigenfunctions on the two-dimensional torus , Ann. Henri Poincare 12 (2011), no. 6, 1027–1053.

[C-C] J. Cilleruelo, A. Cordoba *Trigonometric polynomials and lattice points*, Proc. AMS, 115 (4) (1992), 899–905.

[C-G] J. Cilleruelo, A. Granville *Lattice points on circles, squares in arithmetic progressions and sumsets of squares*, CRM Proc. LN, Vol. 43, AMS 2007, 241–262.

[J] V. Jarnik *Uber die Gitterpunkte auf konvexen Kurven*, Math. Z. 24 (1) (1926), 500–518.

[Ra] D. S. Ramana *Arithmetical applications of an identity for the Vandermonde determinant.* Acta Arith. 130 (2007), no. 4, 351–359.