PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 115, Number 4, AUGUST 1992

TRIGONOMETRIC POLYNOMIALS AND LATTICE POINTS

J. CILLERUELO AND A. CORDOBA

(Communicated by J. Marshall Ash)

ABSTRACT. In this paper we study the distribution of lattice points on arcs of circles centered at the origin. We show that on such a circle of radius R, an arc whose length is smaller than $\sqrt{2}R^{1/2-1(4[m/2]+2)}$ contains, at most, m lattice points. We use the same method to obtain sharp L^4-estimates for uncompleted, Gaussian sums

I. Introduction and statement of results

Let us denote by $r(n)$ the number of representations of the integer n as a sum of two squares, i.e., $r(n)$ is the number of lattice points on the circle $x^2 + y^2 = n$. This function plays an important role in the arithmetic of Gaussian integers and it satisfies the relation $r(n) = 4\sum_{d/n} \chi_1(d)$, where χ_1 is the nonprincipal character (mod 4).

It is a well-known fact that $r(n) = O(n^\varepsilon)$ for every $\varepsilon > 0$, and that $r(n)$ is not $O((\log n)^c)$ for any c. However the distribution of values of $r(n)$ is rather irregular. The function $R(n) = \sum_{k \leq n} r(k)$ has also been considered, and it was observed by Gauss that $R(n) = \pi n + E(n)$, with $E(n) = O(n^{1/2})$. To find the true order of magnitude of the error term $E(n)$ is an outstanding problem in the number theory, i.e., the well-known lattice point problem.

There is a result attributed to Heron of Alexandria which says: in any triangle, the product of the lengths of its three sides is equal to four times the area of the triangle multiplied by the radius of the circumscribed circle: $abc = 4\Delta R$. This theorem has the following application: If ν_1, ν_2, ν_3 are three lattice points on the circle $x^2 + y^2 = R^2$, then $\max\{\|\nu_1 - \nu_2\|, \|\nu_1 - \nu_3\|, \|\nu_2 - \nu_3\|\} \geq 2R^{1/3}$. In particular, an arc of length $2R^{1/3}$ contains, at most, two lattice points. This fact was first observed by Schinzel and used by Zygmund [1] to prove a Cantor-Lebesgue theorem in two variables.

Therefore it is a natural question to ask for which exponents α there exists a finite constant N_α satisfying the condition that any arc of length R^α, in a circle centered at the origin and radius R, contains at most N_α points uniformly in R.

Received by the editors December 15, 1989 and, in revised form, June 29, 1990 and January 7, 1991.

1991 *Mathematics Subject Classification*. Primary 10J05, 10G05.

In this paper a new method is introduced to prove that the answer to this question is affirmative for every $\alpha < \frac{1}{2}$. More precisely, we have

Theorem 1. *On a circle of radius R centered at the origin, an arc Γ whose length is not greater than $\sqrt{2}R^{1/2-1/(4[m/2]+2)}$, contains, at most, m lattice points.*

Gaussian sums are an important object in number theory. It is known that

$$\left\| \sum_{N\leq k\leq 2N} e^{2\pi i k^2 x} \right\|_{L^p[0,1]} \simeq N^{1/2} \quad \text{for } 1 \leq p < 4$$

and that the weak-L^4 estimate also holds:

$$\mu\left\{x: \left| \sum_{N\leq k\leq 2N} e^{2\pi i k^2 x} \right| \geq \alpha > 0 \right\} \leq C\frac{N^2}{\alpha^4}$$

where $C < \infty$ is some universal constant and μ denotes Lebesgue measure.

In the other direction, we have the equivalence

$$\left\| \sum_{N\leq k\leq 2N} e^{2\pi i k^2 x} \right\|_{L^4[0,1]} \simeq N^{1/2}(\log N)^{1/4}, \qquad N \to \infty.$$

It is not difficult to observe that

$$\left\| \sum_{N\leq k\leq N+N^{\alpha}} e^{2\pi i k^2 x} \right\|_{L^4[0,1]} = (2N^{2\alpha})^{1/4} + O(1) \quad \text{for every } \alpha \leq \frac{1}{2}.$$

The method introduced in the proof of Theorem 1 allows us to provide estimates of this type for every α, $\frac{1}{2} < \alpha < 1$.

Theorem 2.

$$\int_0^1 \left| \sum_{N\leq k\leq N+N^{\alpha}} e^{2\pi i k^2 x} \right|^4 dx = 2N^{2\alpha} + O(N^{3\alpha-1+\varepsilon})$$

for every $\varepsilon > 0$ and α, $\frac{1}{2} < \alpha < 1$.

II. Proof of Theorem 1

A. **Preliminary remarks and notation.** Let us recall the known fact that $r(n) = 4\sum_{d/n}\chi_1(d) = 4\{d_1(n) - d_3(n)\}$, where d_j, $j = 1, 3$, denotes the number of divisors of n which are conjugent with j module 4. The factor 4 takes into account the symmetry of the lattice.

If $n = 2^{\nu}\prod_{p_j\equiv 1(4)} p_j^{\alpha_j}\prod_{q_k\equiv 3(4)} q_k^{\beta_k}$ is the prime factorization of the integer n, then $r(n) = 0$ unless all the exponents β_k are even. In that case we have $r(n) = 4\prod(1+\alpha_j)$.

We also have the composition formula given by multiplication in the ring of Gaussian integers: If $a^2+b^2 = n$ and $c^2+d^2 = m$, then $(ac-bd)^2+(ad+bc)^2 = mn$. That is, in terms of norms we have $N(a+bi) = n$ and $N(c+di) = m$ imply that $N((a+bi)(c+di)) = mn$. Furthermore, if $(m, n) = 1$ then each representation of mn as a sum of two squares arises from decompositions of m and n given by the formula above. Therefore we shall associate lattice points with Gaussian integers: $a^2 + b^2 = n$ determines a Gaussian integer $a + bi = \sqrt{n}e^{2\pi i\Phi}$ for a suitable phase Φ.

We have

(i) $r(2^\nu) = 4$ and there are two possible situations, namely, ν is even, in which case $2^\nu = 0 + (\pm 2^{\nu/2})^2 = (\pm 2^{\nu/2})^2 + 0$ or ν is odd, and then $2^\nu = (\pm 2^{[\nu/2]})^2 + (\pm 2^{[\nu/2]})^2$.

That is, the Gaussian integers corresponding to the four representations of 2^ν as a sum of two squares are the following:

$$2^{\nu/2}e^{2\pi i\{\Phi_0 + t/4\}}, \qquad t = 0, 1, 2, 3, \quad \text{where } \Phi_0 = \begin{cases} 0 & \text{if } \nu \text{ is even}, \\ \frac{1}{8} & \text{if } \nu \text{ is odd}. \end{cases}$$

(ii) If $q \equiv 3(4)$ is a prime number, then $r(q^{2\beta}) = 4$ and the representations are given by

$$q^{2\beta} = 0^2 + (\pm q^\beta)^2 = (\pm q^\beta)^2 + 0^2,$$

i.e., they correspond to the Gaussian integers $q^\beta e^{2\pi i t/4}$, $t = 0, 1, 2, 3$.

(iii) If $p \equiv 1(4)$ is prime, then $r(p^\alpha) = 4(1 + \alpha)$.

Furthermore if $p = a^2 + b^2$, $a + bi = \sqrt{p}e^{2\pi i\Phi}$, $a, b > 0$, then the representations of p^α as a sum of two squares are given by $p^{\alpha/2}e^{2\pi i\{\gamma\Phi + t/4\}}$ where $t = 0, 1, 2, 3$ and γ describes the set $\Lambda_\alpha = \{\gamma \in Z, |\gamma| \le \alpha, \gamma \equiv \alpha \pmod 2\}$.

(iv) We can summarize the previous observations in the following manner. If $n = 2^\nu \prod_{p_j \equiv 1(4)} p_j^{\alpha j} \prod_{q_k \equiv 3(4)} q_k^{2\beta_k}$ then the Gaussian integers corresponding to the $4\prod(1 + \alpha_j)$ representations of n as a sum of two squares are given by the formula

$$(*) \qquad \sqrt{n}e^{2\pi i\{\Phi_0 + \sum_j \gamma_j \Phi_j + t/4\}}, \qquad t = 0, 1, 2, 3,$$

where γ_j describes the set Λ_{α_j} and $\Phi_0 = 0$ or $\frac{1}{8}$ depending upon the parity of ν.

Remark. The angles Φ_j corresponding to different primes $p_j \equiv 1(4)$ are linearly independent over the rationals, i.e., a relation $\sum_{1 \le j \le N} a_j \Phi_j + a_0 = 0$, with coefficients $a_j \in Q$, implies necessarily that $a_0 = a_1 = \cdots = a_N = 0$.

B. End of the proof. Let us suppose that for the integer

$$n_0 = 2^\nu \prod_{p_j \equiv 1(4)} p_j^{\alpha_j} \prod_{q_k \equiv 3(4)} q_k^{2\beta_k}$$

there is an arc, in the circle of radius $R_0 = \sqrt{n_0}$ centered at the origin, which contains more than m points and whose length is $\sqrt{2}R_0^\alpha$. Then, formula $(*)$ implies that the same must be true for the circle of radius $R = \sqrt{n}$, where $n = \prod_j p_j^{\alpha_j}$. That is, we may assume the existence of $m+1$ lattice points in such an arc of this circle. They will have representations $\sqrt{n}e^{2\pi i\{\Sigma_j \gamma_j^s \Phi_j + t^s/4\}}$, $s = 1, 2, \ldots, m+1$, $\gamma_j^s \in \{\gamma \in Z, |\gamma| \le \alpha_j, \gamma \equiv \alpha_j(2)\}$, and $t^s \in \{0, 1, 2, 3\}$.

For each pair $s \neq s'$ of such points, let us consider the quantity

$$\begin{aligned}\Psi^{s,s'} &= \sum_j \{\gamma_j^s - \gamma_j^{s'}\} + \frac{t^s - t^{s'}}{4} \\ &= 2\left\{\sum_j \Phi_j \frac{\gamma_j^s - \gamma_j^{s'}}{2} + \frac{t^s - t^{s'}}{8}\right\}\end{aligned}$$

and observe that the $\gamma_j^{s,s'} = (\gamma_j^s - \gamma_j^{s'})/2$ take always integer values.

We have two cases to consider, depending upon the parity of t^s and $t^{s'}$:

(1) if $t^s \equiv t^{s'}(2)$, then $(t^s - t^{s'})/8 = t^{s,s'}/4$ for some integer $t^{s,s'}$;

(2) if $t^s \not\equiv t^{s'}(2)$, then $(t^s - t^{s'})/8 = \frac{1}{8} + t^{s,s'}/4$ for some integer $t^{s,s'}$.

In the first case, formula $(*)$ shows that $\Psi^{s,s'}/2$ is the angle corresponding to a representation of $\prod_j p_j^{|\gamma_j^{s,s'}|}$ as a sum of two squares.

The second case corresponds to a representation of $2\prod_j p_j^{|\gamma_j^{s,s'}|}$.

If $\Psi^{s,s'}/2$ is an integer, then the linear independence of $\{1, \Phi_1, \Phi_2, \ldots\}$ over the rationals, implies that $t^s = t^{s'}$ and $\gamma_j^{s,s'} = 0$ for every j, so that finally $s = s'$. Thus we have the following result. If $s \neq s'$ then $|||\Psi^{s,s'}/2||| > 0$, where $|||\ |||$ denotes distance to the integers.

Our previous considerations show that if $s \neq s'$, then $\Psi^{s,s'}/2$ is the angle of a lattice point not on the x axis, but on the circle of radius

$$2^{\nu/2}\prod_j p_j^{|\gamma_j^{s,s'}|/2} \quad \text{where } \nu = 0 \text{ or } \nu = 1.$$

Therefore we have

$$\left|\left|\left|\frac{\Psi^{s,s'}}{2}\right|\right|\right| > \frac{1}{2\pi\sqrt{2}\prod_j p_j^{|\gamma_j^{s,s'}|/2}}$$

by a simple argument.

On the other hand, our hypothesis on the location of the $m+1$ lattice points on an arc of length $\sqrt{2}R^\alpha$, implies the following inequality:

$$\left|\left|\left|\frac{\Psi^{s,s'}}{2}\right|\right|\right| \leq \frac{1}{2\pi\sqrt{2}}R^{\alpha-1}.$$

We have $m(m+1)/2$ couples s, s'. Multiplying all these inequalities, we get

$$R^{(\alpha-1)m(m+1)/2} > \frac{1}{\prod_{s,s'}\prod_j p_j^{|\gamma_j^{s,s'}|}} = \frac{1}{\left(\prod_j p_j^{\sum_{s,s'}|\gamma_j^{s,s'}|}\right)^{1/2}}.$$

Next we want to estimate the maximum value of the sum

$$\sum_{s,s'}|\gamma_j^{s,s'}| = \frac{1}{2}\sum_{s,s'}|\gamma_j^s - \gamma_j^{s'}|$$

where, as was stated before, γ_j^s takes values in the set $\{\gamma \in Z,\ |\gamma| \leq \alpha_j,\ \gamma \equiv \alpha_j(2)\}$.

If $m+1$ is even, the maximum value is obtained when $(m+1)/2$ of the numbers γ_j^s are equal to α_j and the remaining $(m+1)/2$ are $-\alpha_j$.

If $m+1$ is odd, then the maximum takes place when $(m+2)/2$ of the γ_j^s are equal to α_j and the remaining $m/2$ are $-\alpha_j$. Therefore,

$$\sum_{s,s'} |\gamma_j^{s,s'}| \le \alpha_j \frac{(m+1)^2 - \delta(m)}{4},$$

where

$$\delta(m) = \begin{cases} 0 & \text{if } m \text{ is odd}, \\ 1 & \text{if } m \text{ is even}. \end{cases}$$

We obtain

$$R^{(\alpha-1)m(m+1)/2} > \left(\prod_j p_j^{\alpha_j((m+1)^2-\delta(m))/4}\right)^{-1/2} = R^{-((m+1)^2-\delta(m))/4}$$

which yields

$$\alpha > 1 - \frac{(m+1)^2 - \delta(m)}{2m(m+1)} = \frac{1}{2} - \frac{1}{4[m/2]+2}$$

and this completes the proof of Theorem 1.

Here, as in the rest of the paper, we have used the standard notation $[x]$ to denote the integer part of the real number x.

III. Proof of Theorem 2

Let $r_\alpha(n) = \operatorname{Card}\{(h,k) \in Z^2 : n = k^2 + h^2,\ N \le k, h \le N + N^\alpha\}$. Let $C_j = \{n : r_\alpha(n) = j\}$. Then

$$\int_0^1 \left| \sum_{N \le k \le N+N^\alpha} e^{2\pi i k^2 x} \right|^4 dx = \sum_n r_\alpha^2(n) = \sum_j j^2 \operatorname{Card}(C_j)$$
$$= \operatorname{Card}(C_1) + 4\operatorname{Card}(C_2) + \sum_{j\ge 3} j^2 \operatorname{Card}(C_j).$$

Observe that $\operatorname{Card}(C_1) \le [N^\alpha]$, because the lattice points corresponding to points of C_1 necessarily lie on the diagonal, i.e., $h = k$.

Our next step is to compute $\sum_{j\ge 3} j^2 \operatorname{Card}(C_j)$.

Let $n \in \bigcup_{j\ge 3} C_j$. Then n admits two different representations as a sum of two squares which are not placed symmetrically with respect to the diagonal of the first quadrant.

Let $\sqrt{n} e^{2\pi i \Phi^1}$, $\sqrt{n} e^{2\pi i \Phi^2}$ be the Gaussian integers corresponding to such points, where

$$\Phi^s = \sum_j \gamma_j^s \Phi_j + \frac{t^s}{4}, \qquad s = 1, 2,$$

and we have used the notation of the previous theorem.

We have

$$\frac{(\Phi^1 \pm \Phi^2)}{2} = \sum_j \Phi_j \frac{(\gamma_j^1 \pm \gamma_j^2)}{2} + \frac{(t^1 \pm t^2)}{8},$$

$$\left|\frac{\Phi^1 - \Phi^2}{2}\right| < \frac{1}{4\pi}\left\{\operatorname{arctg}\frac{N+N^\alpha}{N} - \operatorname{arctg}\frac{N}{N+N^\alpha}\right\} < \frac{1}{2\pi}N^{\alpha-1},$$

$$\left|\frac{(\Phi^1 + \Phi^2)}{2} - \frac{1}{8}\right| < \frac{1}{4\pi}\left\{\operatorname{arctg}\frac{N+N^\alpha}{N} - \operatorname{arctg}\frac{N}{N+N^\alpha}\right\} < \frac{1}{2\pi}N^{\alpha-1}.$$

(i) If $t^1 - t^2$ is even, then $(\Phi^1 - \Phi^2)/2$ and $(\Phi^1 + \Phi^2)/2$ are angles corresponding to representations of integers d_1, d_2, respectively, such that $d_1 d_2 = n$,

$$d_1 = a_1^2 + b_1^2, \qquad 0 < b_1 < N^{\alpha-1}a_1,$$
$$d_2 = a_2^2 + b_2^2, \qquad 0 < |a_2 - b_2| < N^{\alpha-1}a_2.$$

Observe that $a_2 = b_2$ implies $(\Phi^1 + \Phi^2)/2 - \frac{1}{8} = 0$, i.e., the two representations of n are symmetric with respect to the diagonal; $b_1 = 0$ implies $(\Phi^1 + \Phi^2)/2 = 0$, i.e., the two representations of n are the same.

(ii) If $t^1 - t^2$ is odd, then $(\Phi^1 - \Phi^2)/2 + \frac{1}{8}$, $(\Phi^1 + \Phi^2)/2 + \frac{1}{8}$ are angles corresponding to representations of d_1, d_2 such that $d_1 d_2 = n$,

$$d_1 = a_1^2 + b_1^2, \qquad 0 < |a_1 - b_1| < N^{\alpha-1}a_1,$$
$$d_2 = a_1^2 + b_2^2, \qquad 0 < b_2 < N^{\alpha-1}a_2.$$

In any case, given $n \in \bigcup_{j\geq 3} C_j$, we have a decomposition $n = d_1 d_2$ such that

$$d_1 = a_1^2 + b_1^2, \quad 0 < b_1 < N^{\alpha-1}a_1,$$
$$d_2 = a_2^2 + b_2^2, \quad 0 < |a_2 - b_2| < N^{\alpha-1}a_2.$$

The number of pairs d_1, d_2 satisfying the conditions above gives an upper bound for $\operatorname{Card}(\bigcup_{j\geq 3} C_j)$.

With d_1 fixed we estimate the cardinality of the set of numbers d_2 such that

$$d_2 = a_2^2 + b_2^2, \qquad 0 < |a_2 - b_2| < N^{\alpha-1}a_2, \qquad \sqrt{2}N < \sqrt{d_1 d_2} < \sqrt{2}(N + N^\alpha),$$

i.e.,

$$\frac{\sqrt{2}N}{\sqrt{d_1}} < \sqrt{a_2^2 + b_2^2} < \frac{\sqrt{2}N}{\sqrt{d_1}}(N + N^\alpha).$$

To do it we observe that if we fix a_2, then there are $O(N^{\alpha-1}a_2)$ integers b_2 such that $|a_2 - b_2| < N^{\alpha-1}a_2$ and since $\sqrt{a_2^2 + b_2^2} \simeq \sqrt{2}a_2 \simeq \sqrt{2}N/\sqrt{d_1}$, we have that for d_1 fixed, there are at most $N^{\alpha-1}(N/\sqrt{d_1})(N^\alpha/\sqrt{d_1}) = N^{2\alpha}/d_1$ integers d_2 satisfying that set of inequalities. Therefore,

$$\operatorname{Card}\left\{\bigcup_{j\geq 3} C_j\right\} < \sum_{a_1 < N}\ \sum_{0 < b_1 < N^{\alpha-1}a_2} \frac{N^{2\alpha}}{a_1^2 + b_1^2} < N^{3\alpha-1}\log N.$$

On the other hand, clearly

$$\sum_n r_\alpha(n) = \operatorname{Card}\{(k, h) \colon N \leq k, h \leq N + N^\alpha\} = N^{2\alpha} + O(N^\alpha)$$

and

$$\sum_n r_\alpha(n) = \sum_j \operatorname{Card}(C_j) = \operatorname{Card}(C_1) + 2\operatorname{Card}(C_2) + O\left(N^\varepsilon \operatorname{Card}\left(\bigcup_{j\geq 3} C_j\right)\right)$$

for every $\varepsilon > 0$.

Thus

$$\operatorname{Card}(C_2) = \frac{N^{2\alpha}}{2} + O(N^\alpha + N^{3\alpha-1+\varepsilon}) \quad \text{for every } \varepsilon > 0$$

which yields the theorem. □

Remarks. Theorem 1 was motivated by the search for a direct connection between the restriction properties of Fourier integrals and those of Fourier series coefficients to circles. We have some evidence that $\alpha = \frac{1}{2}$ is sharp, but we have no proof.

It would be interesting to obtain a version of Theorem 2 with coefficients: is

$$\left\| \sum_{N\leq k\leq N+N^\alpha} a_k e^{2\pi i k^2 x} \right\|_4 \simeq \left(\sum |a_n|^2\right)^{1/2}$$

uniformly in N?

Acknowledgment

We would like to thank the referee for his comments, which helped us to improve the quality of the presentation of this paper.

References

1. A. Zygmund, *A Cantor-Lebesgue theorem for double trigonometric series*, Studia Math. **64** (1972), 189–202.
2. G. H. Hardy and E. M. Wright, *Introduction to the theory of numbers*, 4th ed., Clarendon Press, Oxford, 1960.
3. W. B. Jurkat, *The proof of the central limit theorem for theta sums*, Duke Math. J. **48** (1981), 873–885.
4. Z. Zalcwasser, *Sur les pôlynomes associes aux fonctions modulaires θ*, Studia Math. **7** (1937), 16–35.

Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049–Madrid, España