J. Austral. Math. Soc. **72** (2002), 217–222

LATTICE POINTS ON CIRCLES

JAVIER CILLERUELO

(Received 7 November 2000; revised 15 February 2001)

Communicated by W. W. L. Chen

Abstract

We prove that the lattice points on the circles $x^2 + y^2 = n$ are well distributed for most circles containing lattice points.

2000 *Mathematics subject classification*: primary 11N36.

1. Introduction

The number of lattice points on the circle $x^2 + y^2 = n$ is denoted by $r(n)$. It is known that $r(n)$ is an unbounded function and it is a natural question to ask for the distribution of the $r(n)$ lattice points on the circle $x^2 + y^2 = n$.

In order to give a measure of that distribution, we consider the polygon with vertices at the $r(n)$ lattice points and denote by $S(n)$ the area of such a polygon. If the lattice points are well distributed, the area of the polygon must be close to the area of the circle, that is, $S(n)/\pi n \sim 1$.

If $r(n) > 0$, trivially $2/\pi \le S(n)/\pi n < 1$. In [1] we proved that the set $\{S(n)/\pi n : r(n) > 0\}$ is dense in the interval $[2/\pi, 1]$. We also proved that $|S(n)/\pi n - 1| \ll (\log\log n/\log n)^2$ for infinitely many integers.

In this paper we prove that, in fact, for most integers n such that $r(n) > 0$, the quantity $S(n)/\pi n$ is close to 1.

THEOREM 1.1. *For any $n \le x$ with $r(n) > 0$,*

$$\frac{S(n)}{\pi n} > 1 - \left(\frac{11\log\log\log x}{\log\log x}\right)^2 \tag{1.1}$$

I am indebted to Laura Fainsilber for calling my attention to this problem.

with at most

$$O\left(\frac{x}{(\log x)^{1/2}\log\log x\log\log\log x}\right) \tag{1.2}$$

exceptions.

It should be noted that if we call $B_x = \{n \le x : r(n) > 0\}$, then $|B_x| \sim cx/(\log x)^{1/2}$.

2. Background

In the proof of Theorem 1.1 we will use the prime number theorem for Gaussian primes on angular sectors, and Selberg's sieve. We present them in a suitable form in this section.

THEOREM 2.1. *Let D be an angular sector of the circle $x^2+y^2 \le R^2$ with angle θ. Then*

$$\sum_{\rho\in D} 1 = \frac{\theta R^2}{\pi\log R} + O\left(\frac{R^2}{\log^2 R}\right), \tag{2.1}$$

where $\rho = a+bi$ are primes in $Z[i]$ and the constant in the error term does not depend on θ.

PROOF. Stronger versions of this result can be found in [2] and [3]. □

The sieving function $S(\mathscr{A}, P, z)$ denotes the number of terms of the sequence $\mathscr{A}$ that are not divisible by any prime $p \in P$, $p < z$. We denote by $\pi_P(x)$ the counting function of the sequence P.

THEOREM 2.2. *If P is an infinite subset of primes such that*

$$\pi_P(x) = \alpha x/\log x + O\left(x/\log^2 x\right) \text{ and } \mathscr{A} = \{1,\dots,x\}, \text{ then} \tag{2.2}$$

$$S(\mathscr{A}, P, x) \ll \frac{x}{(\log x)^{\alpha}}. \tag{2.3}$$

PROOF. It will be a consequence of Selberg's sieve. For every square-free positive integer d, let $|A_d|$ denote the number of terms of the sequence $\mathscr{A}$ which are divisible by d. Then $|A_d| = x/d + r_d$, with $|r_d| \le 1$. Let

$$G(z) = \sum_{m<z,\, p|m \text{ implies } p\in P} \frac{1}{m}.$$

Selberg's sieve [4, page 180] implies that

$$S(A, P, z) \le \frac{x}{G(z)} + \sum_{d<z^2, d \text{ square-free}} 3^{\omega(d)}.$$

Observe that

$$G(z) \prod_{p<z, p\notin P} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \ge \sum_{m<z} \frac{1}{m} \gg \log z$$

and

$$\prod_{p<z, p\notin P} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \prod_{p<z, p\notin P} \frac{p}{p-1} \le \prod_{p} \frac{p^2}{p^2-1} \prod_{p<z, p\notin P} \left(1 + \frac{1}{p}\right).$$

The first product is a constant and the second product can be estimated by taking logarithms:

$$\log\left(\prod_{p<z, p\notin P} \left(1 + \frac{1}{p}\right)\right) \le \sum_{p<z, p\notin P} \frac{1}{p} = \sum_{p<z} \frac{1}{p} - \sum_{p<z, p\in P} \frac{1}{p}.$$

The two sums can be handled using Abel's summation together with the formula

$$\pi(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right), \qquad \pi_P(x) = \alpha \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

Then

$$\sum_{p<z} \frac{1}{p} - \sum_{p<z, p\in P} \frac{1}{p} = (1-\alpha) \log\log z + O(1),$$

which yields

$$S(\mathscr{A}, P, z) \ll \frac{x}{(\log z)^\alpha} + \sum_{m<z^2, m \text{ square -free}} 3^{\omega(m)}.$$

Observe that

$$\sum_{m<z^2, m \text{ square-free}} 3^{\omega(m)} = \sum_{m<z^2, m \text{ square-free}} (2^{\omega(m)})^{\log 3/\log 2} \le \sum_{m<z^2, m \text{ square-free}} d^2(m) \ll z^2 \log^3 z.$$

Now if we choose $z = [x^{1/3}]$, we obtain $S(\mathscr{A}, P, x) \le S(\mathscr{A}, P, z) \ll x/(\log x)^\alpha$. □

Next, we will present two proposition needed to prove Theorem 1.1.

PROPOSITION 2.3. *Let $\{x_j\}_{j=1}^{2k}$ be a set of real numbers such that*

$$x_j \in I_j = \left(\frac{j-1}{2k}, \frac{j}{2k}\right], \quad j = 1, \ldots, 2k$$

and for any real ϕ let $S = \left\{\phi + \sum_{j=1}^{2k} \epsilon_j x_j,\ \epsilon_j = \pm 1\right\}$. Then, for any $j = 1, \ldots k$, there exists $s \in S$ such that $\{s/2\} \in J_j = ((j-1)/k, j/k]$, where $\{s/2\}$ denotes the fractional part of $s/2$.

PROOF. Let $\alpha = \phi - \sum_{j=1}^{2k} x_j$. Then we can write

$$S = \left\{ \alpha + \sum_{j=1}^{2k} \gamma_j x_j,\ \gamma_j \in \{0, 2\} \right\}.$$

The numbers $s_i/2 = \alpha/2 + x_i$, satisfy $s_{i+1}/2 - s_i/2 < 1/k$ for $i = 1, \dots, 2k-1$ and $s_1/2 + 1 - s_{2k}/2 < 1/k$. Then, for each interval J_j, there exists $s_i \in S$ such that $\{s_i/2\} \in J_j$. □

PROPOSITION 2.4. *Let $n = n_1 n_2$ such that $n_j = x_j^2 + y_j^2$, $x_j + iy_j = \sqrt{n_j} e^{i\phi_j}$, $j = 1, 2$. Then, the angles $\pm\phi_1 \pm \phi_2$ correspond to lattice points on the circle $x^2 + y^2 = n$.*

PROOF. See [1] for more details. □

3. Proof of Theorem 1.1

For each prime $p = 2$ or $p \equiv 1 \pmod 4$ let $\phi_p = (4/\pi)\tan^{-1}(a/b)$, where a, b are the only integers such that $a^2 + b^2 = p$, $0 < a \le b$. Then $\phi_p \in (0, 1]$.

We split the interval $(0, 1]$ in the $2k$ intervals $I_j = ((j-1)/2k,\ j/2k]$, $j = 1, \dots, 2k$ and we define the good numbers as

$$G_x^k = \left\{ n \in B_x; n = p_1 \cdots p_{2k} m,\ \text{with } \phi_{p_j} \in I_j \right\}, \tag{3.1}$$

where we recall $B_x = \{n \le x : \quad r(n) > 0\}$.

In Proposition 3.1 we will prove that if $n \in G_x^k$, the lattice points on the circle $x^2 + y^2 = n$ are well distributed, and in Proposition 3.2 we will estimate the cardinality of the bad numbers, $B_x^k = B_x \setminus G_x^k$. Theorem 1.1 will be a consequence of these propositions for a suitable value of k.

PROPOSITION 3.1. *If $n \in G_x^k$, then*

$$S(n)/\pi n > 1 - \pi^2/6k^2. \tag{3.2}$$

PROOF. We can write $n = p_1 \cdots p_{2k} m$.

Obviously, m has, at least, a representation as a sum of two squares, $m = a^2 + b^2$, $a + ib = \sqrt{m}\exp(i(\pi/4)\phi)$.

Proposition 2.4 implies that the angles $(\pi/4)\big(\phi + \sum_{j=1}^{2k-1} \epsilon_j \phi_{p_j}\big)$, $\epsilon_j = \pm 1$ correspond to lattice points on the circle $x^2 + y^2 = n$.

Suppose that $(\pi/4)s$ is one of these angles. Then, due to the symmetry of the lattice, the angle $(\pi/4)s - (\pi/2)[s/2] = (\pi/2)\{s/2\}$ also corresponds to a lattice point.

Now we apply Proposition 2.3 to conclude that for every $j = 1, \dots, k$ there exists an angle s such that $\{s/2\} \in J_j = ((j-1)/k, j/k]$. In other words, for every $j = 1, \dots, k$ there exists a lattice point on the arc $\sqrt{n}\exp(\pi\theta i/2)$, $\theta \in J_j$.

Again, due to the symmetry of the lattice we can find, for every $j = 1, \dots, k$ and for $r = 0, 1, 2, 3$, a lattice point on the arc $\sqrt{n}\exp(\pi(\theta + r)i/2)$, $\theta \in J_j$.

Now let us choose a lattice point for each arc. Let P_0 be the polygon with vertices in these $4k$ lattice points. Obviously, $S_0(n) \le S(n)$, where $S_0(n) = \text{Area}(P_0)$. Now we denote by $\theta_1, \dots \theta_{4k}$ the angles between each pair of two consecutive lattice points.

If we consider a sector with angle θ_j and radius $\sqrt{n}$, an easy geometric argument prove that the area of the part of the sector outside the triangle is $n(\theta_j - \sin\theta_j)/2 \le n\theta_j^3/12$. Then $\pi n - S_0(n) \le (n/12)\sum_{j=1}^{4k}\theta_j^3$. We know that $\theta_j \le \pi/k$ and that $\sum_{j=1}^{4k}\theta_j = 2\pi$. Therefore, the maximum happens when the half of the angles are 0 and the other half are π/k. That is, $\pi n - S(n) \le \pi n - S_0(n) \le n\pi^3/6k^2$. □

PROPOSITION 3.2. $|B_x^k| \ll kx/(\log^{1/2+1/4k} x) + kx^{3/4}$.

PROOF. If we apply Theorem 2.1 to the region

$$D_j = \left\{(a,b) : a^2 + b^2 \le x,\ 0 < a \le b,\ (4/\pi)\tan^{-1}(a/b) \in I_j\right\}$$

we obtain

$$\pi_{P_j}(x) = \frac{x}{4k\log x} + O\left(\frac{x}{\log^2 x}\right), \tag{3.3}$$

where $P_j = \{p \not\equiv 3 \pmod 4 : \phi_p \in I_j\}$.

On the other hand, if we denote by $Q = \{q \equiv 3 \pmod 4 : q \text{ primes}\}$, the prime number theorem for arithmetic progressions says that $\pi_Q(x) = x/(2\log x) + O(x/\log^2 x)$. Then, if $Q_j = Q \cup P_j$ we obtain

$$\pi_{Q_j}(x) = \left(\frac{1}{2} + \frac{1}{4k}\right)\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right). \tag{3.4}$$

We define, for any $1 \le l \le \sqrt{x}$, $\mathscr{A}_l = \{m \le x/l^2\}$ and $\mathscr{A}_l^* = \{m \le x/l^2 : m \text{ square free}\}$. Now, suppose that $n \in B_x^k$ with $n = l^2 m$, m square free. Because $r(n) > 0$, then m has not prime divisors $q \equiv 3 \pmod 4$. Since $n \notin G_x^k$, then there exists an integer j such that m has no prime divisors p with $\phi_p \in I_j$. Then, that integer n is shifted in $S(\mathscr{A}_l^*, Q_j, x/l^2)$. Thus,

$$|B_x^k| \le \sum_{1\le l\le\sqrt{x}}\sum_{j=1}^{2k} S(\mathscr{A}_l^*, Q_j, x/l^2) \le \sum_{1\le l\le\sqrt{x}}\sum_{j=1}^{2k} S(\mathscr{A}_l, Q_j, x/l^2). \tag{3.5}$$

For $l < x^{1/4}$ we apply Theorem 2.2 to each $S(\mathscr{A}_l, Q_j, x/l^2)$,

$$S(\mathscr{A}_l, Q_j, x/l^2) \ll \frac{x}{l^2(\log(x/l^2))^{1/2+1/4k}} \ll \frac{x}{l^2(\log x)^{1/2+1/4k}}$$

and then

$$\sum_{1\le l\le x^{1/4}} \sum_{j=1}^{2k} S(\mathscr{A}_l, Q_j, x/l^2) \ll \frac{kx}{(\log x)^{1/2+1/4k}}.$$

For $l \ge x^{1/4}$ we use the trivial estimate $S(\mathscr{A}_l, Q_j, x/l^2) \le x/l^2$ and we obtain $\sum_{x^{1/4}\le l} \sum_{j=1}^{2k} S(\mathscr{A}_l, Q_j, x/l^2) \ll kx^{3/4}$. □

To conclude Theorem 1.1 we apply Proposition 3.1 and Proposition 3.2 with $k = [\log\log x/(8\log\log\log x)]$. Observe that if x is large enough, then

$$k = [\log\log x/(8\log\log\log x)] > \log\log x/((8.5)\log\log\log x).$$

Thus, for $n \in G_x^k$ and x large enough,

$$\frac{S(n)}{\pi n} > 1 - \frac{\pi^2}{6}\left(\frac{(8.5)\log\log\log x}{\log\log x}\right)^2 > 1 - \left(\frac{11\log\log\log x}{\log\log x}\right)^2. \tag{3.6}$$

On the other hand,

$$\begin{aligned} |B_k(x)| &\ll \frac{\log\log x}{\log\log\log x}\,\frac{x}{(\log x)^{1/2}(\log x)^{(2\log\log\log x)/(\log\log x)}} \\ &\ll \frac{x}{(\log x)^{1/2}\log\log x\log\log\log x}. \end{aligned} \tag{3.7}$$

References

[1] J. Cilleruelo, 'The distribution of the lattice points on circles', *J. Number Theory* **43** (1993), 198–202.
[2] I. Kubilyus, 'The distribution of Gaussian primes in sectors and contours', *Leningrad. Gos. Univ. Uchen. Zap. Ser. Mat. Nauk* **137** (1950), 40–52.
[3] T. Mitsui, 'Generalized prime number theorem', *Japan J. Math.* **26** (1956), 1–42.
[4] M. Nathanson, *Additive number theory: the classical bases* (Springer, New York, 1996).

Departamento de Matemáticas
Universidad Autónoma de Madrid
28049 Madrid
Spain
e-mail: franciscojavier.cilleruelo@uam.es