LATTICE POINTS ON CIRCLES

JAVIER CILLERUELO

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

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 the distribution of the lattice points, we consider the polygon with vertices on the $r(n)$ lattice points and we denote by $S(n)$ the area of such polygon. When the lattice points are well distributed, the area of the polygon will be close to the area of the circle, i.e. $\frac{S(n)}{\pi n} \sim 1$.

If $r(n) > 0$, trivially $\frac{2}{\pi} \leq \frac{S(n)}{\pi n} < 1$. In [1] we proved that the set $\left\{ \frac{S(n)}{\pi n} : r(n) > 0 \right\}$ is dense in the interval $[\frac{2}{\pi}, 1]$. In this paper we prove that for most integer n, $r(n) > 0$, the quantity $\frac{S(n)}{\pi n}$ is close to 1.

Theorem 1.1. *Let $x \geq 10^{10^{30}}$. Then, for any $n \leq x$ with $r(n) \neq 0$,*

$$\frac{S(n)}{\pi n} > 1 - \left(\frac{12 \log \log \log x}{\log \log x} \right)^2 \tag{1.1}$$

with at most $$O\left(\frac{x}{(\log x)^{1/2} \log \log x \log \log \log x} \right)$$ *exceptions.*

It should be noted [2] that if we call $R_x = \{n \leq x : r(n) \neq 0\}$, then $|R_x| \sim c \frac{x}{(\log x)^{1/2}}$

2. Background

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

Theorem 2.1. *Let D a 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] $\square$

The sieving function $S(\mathcal{A},P,z)$ denotes the number of terms of the sequence $\mathcal{A}$ that are not divisible by any prime $p\in P$ such that $p<z$.

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

$$\pi_P(x)=\alpha\frac{x}{\log x}+O\left(\frac{x}{\log^2 x}\right) \tag{2.2}$$

and $\mathcal{A}=\{1,\dots,x\}$, then

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

Proof. It will be a consequence of the Selberg sieve.

For every square-free positive integer d, let $|A_d|$ denote the number of terms of the sequence $\mathcal{A}$ that are divisible by d. Then $|A_d|=\frac{1}{d}x+r(d)$, with $|r(d)|\le 1$.

Let

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

Selberg sieve ([4], pg 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

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

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

The first product is a constant and the second product can be estimated 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 estimated using the Abel summation and the formulas

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

Then

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

and we have

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

Observe that

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

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

Now if we choose $z=[x^{1/3}]$ we obtain

$$S(\mathcal{A},P,x)\le S(\mathcal{A},P,z)\ll\frac{x}{(\log x)^\alpha}$$

$\square$

Also we present in this section two easy propositions that we will need in the proof of theorem 1.1.

Proposition 2.3. *Let* $\{x_j\}_{j=0}^{2k-1}$ *be a set of real numbers such that*

$$x_j\in I_j=\left(\frac{j}{2k},\frac{j+1}{2k}\right],\qquad j=0,\dots,2k-1$$

and for any real ϕ *let* $S=\left\{\phi+\sum_{j=0}^{2k-1}\epsilon_j x_j,\quad \epsilon_j=\pm1\right\}$. *Then, for any* $j=0,\dots k-1$, *there exist* $s\in S$ *such that*

$$\left(\frac{s}{2}\right)\in J_j=\left(\frac{j}{k},\frac{j+1}{k}\right],$$

where $(\frac{s}{2})$ *denotes the fractional part of* $\frac{s}{2}$.

Proof. Let $\alpha = \phi - \sum_{j=0}^{2k-1} x_j$. Then we can write

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

The elements $\frac{s_i}{2} = \frac{\alpha}{2} + x_i$, $i = 0, \dots, 2k-1$ satisfy $\frac{s_{i+1}}{2} - \frac{s_i}{2} < \frac{1}{k}$ and $\frac{s_0}{2} + 1 - \frac{s_{2k-1}}{2} < \frac{1}{k}$. Then, for each interval J_j there exist a $\frac{s_i}{2}$ such that $\left(\frac{s_i}{2}\right) \in J_j$. □

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. Obvious. See [1] for more details. □

3. Proof of Theorem 1.1

For each prime $p = 2$ or $p \equiv 1 \pmod 4$ let $\phi_p = \frac{4}{\pi}\tan^{-1}(a/b)$ 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 $I_j = (\frac{j}{2k}, \frac{j+1}{2k}]$, $j = 0, 1, \dots, 2k-1$ and we define

$$G_k(x) = \left\{ n \in R_x; n = p_0 p_1 \cdots p_{2k-1} m, \text{ with } \phi_{p_j} \in I_j \right\} \tag{3.1}$$

In proposition 3.1 we will prove that if $n \in G_k(x)$ the lattice points on the circle $x2 + y^2 = n$ are well distributed, and in proposition 3.2 we will estimate the cardinality of $B_k(x) = R_x \setminus G_k(x)$. Theorem 1.1 will be a consequence of these propositions for a suitable k.

Proposition 3.1. *If $n \in G_k(x)$ then*

$$\frac{S(n)}{\pi n} > 1 - \frac{13\pi^2}{24k^2} \tag{3.2}$$

Proof. We can write $n = p_0 \cdots p_{2k-1} n'$. Obviously, n' has, at least, a representation as a sum of two squares, $n' = x'^2 + y'^2$, $x' + iy' = \sqrt{n'} \exp\left(i\frac{\pi}{4}\phi'\right)$.

Proposition 2.4 implies that the angles $\frac{\pi}{4}\left(\phi' + \sum_{j=0}^{2k-1} \epsilon_j \phi_{p_j}\right)$, $\epsilon_j = \pm 1$ correspond to lattice points on the circle $x^2 + y^2 = n$.

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

Now we apply proposition 2.3 to conclude that for every $j = 0, \dots, k-1$ there exists an angle s such that $(\frac{s}{2}) \in J_j = (\frac{j}{k}, \frac{j+1}{k}]$. In other words, for every $j = 0, \dots, k-1$ there exists a lattice point on the arc

$$\sqrt{n} \exp{(\frac{\pi}{2}\theta i)} \qquad \theta \in J_j.$$

Again, due to the symmetry of the lattice points we can find, for every $j = 0, \dots, k-1$, for $r = 0, 1, 2, 3$ a lattice point on the arc

$$\sqrt{n} \exp{(\frac{\pi}{2}(\theta + r)i)} \qquad \theta \in J_j.$$

Now we choose a lattice point for each arc. Let P_0 be the polygon with vertices in these $4k$ lattice points. Obviously $S_0(n) \leq S(n)$, where $S_0(n) =$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 and radius $\sqrt{n}$, an easy geometric argument prove that the part of the sector outside the triangle is less than $\frac{13}{48}n\theta^3$.

Then

$$\pi n - S_0(n) \leq \frac{13}{48} n \sum_{j=1}^{4k} \theta_j^3$$

We know that $\theta_j \leq \frac{\pi}{k}$ and that $\sum_{j=1}^{4k} \theta_j = 2\pi$. Then the maximum happens when the half of the angles are 0 and the other half are $\frac{\pi}{k}$. Then

$$\pi n - S(n) \leq \pi n - S_0(n) \leq n \frac{13\pi^3}{24k^2}$$

$\square$

Proposition 3.2.

$$|B_k(x)| \ll \frac{kx}{\log^{\frac{1}{2}+\frac{1}{4k}} x} + kx^{3/4} \tag{3.3}$$

Proof. If we apply theorem 2.1 to the region

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

we obtain

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

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 $\pi_Q(x) = \frac{x}{2\log x} + O\left(\frac{x}{\log^2 x}\right)$. Then, if $Q_j = Q \cup P_j$ we obtain

$$\pi_{Q_j}(x) = \left(\frac{1}{2} + \frac{1}{4k}\right)\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right) \tag{3.5}$$

We define, for any $1 \le l \le \sqrt{x}$, $\mathcal{A}_l^* = \{m \le x/l^2 : m \text{ squarefree }\}$ and $\mathcal{A}_l = \{m \le x/l^2\}$.

Now, suppose that $n \in B_k(x)$ with $n = l^2 m$, m squarefree.

Because $n \in R_x$ then m has not prime divisors $q \equiv 3 \pmod 4$.

Because $n \notin G_x$, then there exists an integer j such that m has not prime divisors p with $\phi_p \in I_j$

Then, that integer n is shifted in $S(\mathcal{A}_l^*, Q_j, x/l^2)$. Then

$$|B_k(x)| \le \sum_{1\le l\le\sqrt{x}}\sum_{j=0}^{2k-1} S(\mathcal{A}_l^*, Q_j, x/l^2) \le \sum_{1\le l\le\sqrt{x}}\sum_{j=0}^{2k-1} S(\mathcal{A}_l, Q_j, x/l^2) \tag{3.6}$$

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

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

and then

$$\sum_{1\le l\le x^{1/4}}\sum_{j=0}^{2k-1} S(\mathcal{A}_l, Q_j, x/l^2) \ll \frac{kx}{(\log x)^{1/2+1/4k}}.$$

For $l \ge x^{1/4}$ we use the trivial estimate $S(\mathcal{A}_l, Q_j, x/l^2) \le x/l^2$

Then

$$\sum_{x^{1/4}\le l}\sum_{j=0}^{2k-1} S(\mathcal{A}_l, Q_j, x/l^2) \ll kx^{3/4}$$

and we finish the proof. □

We finish the proof of theorem 1.1 taking $k = \left[\frac{\log\log x}{8\log\log\log x}\right]$.

Observe that if $x \ge 10^{10^{30}}$, then $k = [\frac{\log\log x}{8\log\log\log x}] > \frac{\log\log x}{16\log\log\log x}$ and then

$$\frac{S(n)}{\pi n} > 1 - \frac{13}{24}\left(\frac{16\log\log\log x}{\log\log x}\right)^2 > 1 - \left(\frac{12\log\log\log x}{\log\log x}\right)^2 \tag{3.7}$$

and

$$|B_k(x)| \ll \frac{\log\log x}{8\log\log\log x}\frac{x}{(\log x)^{1/2}(\log x)^{\frac{2\log\log\log x}{\log\log x}}} \tag{3.8}$$

$$(3.9) \qquad = \frac{x}{(\log x)^{1/2} \log\log x \log\log\log x}$$

References.

[1] Javier Cilleruelo, "The distribution of the lattice points on circles". *Journal of Number theory,* Vol. 43, No. 2, Febrery 1993, 198-202.

[2] I. Kubilyus, "The distribution of Gaussian primes in sectors and contours". *Leningrad. Gos. Univ. Uc. Zap. Ser. Mat. Nauk* **137 (19)** (1950), 40-52.

[3] T. Mitsui, "Generalized prime number theorem", *Jap. J. Math.* **26** (1956), 1-42.

[4] M. Nathanson, "Additive number theory: The classical bases." Springer,174 (1996).