The exact order of the number of lattice points visible from the origin

Wataru Takeda

Department of Mathematics,
Kyoto University,
Kitashirakawa Oiwake-cho, Sakyo-ku, Kyoto 606-8502, Japan

Abstract

We say a lattice point $X = (x_1, \ldots, x_m)$ is visible from the origin, if $\gcd(x_1, \ldots, x_m) = 1$. In other word, there are no other lattice point on the line segment from the origin $O$ to $X$. From J.E. Nymann’s result [2], we know that the number of lattice point from the origin in $[-r, r]^m$ is $(2r)^m/\zeta(m) + \text{(Error term)}$. We showed that the exact order of the error term is $r^{m-1}$ for $m \geq 3$.

1 Introduction

The counting and probability problem of the visible lattice points is well known. Let $V_m = \{(x_1, \ldots, x_m) \in \mathbb{Z}^m \mid x \text{ is visible from the origin}\}$. It is well known that the cardinality of the set $V_m \cap \{(x_1, \ldots, x_m) \in \mathbb{Z}^m \mid |x_i| \leq r \ (1 \leq i \leq m)\}$ is

$$\frac{2^m}{\zeta(m)} r^m + \begin{cases} O(r \log r) & (m = 2) \\ O(r^{m-1}) & (m \geq 3), \end{cases}$$

where $\zeta$ is the Riemann zeta function. F. Mertens proved the the case of $m = 2$ in 1874 [1] and J. E. Nymann showed the case of $m \geq 3$ in 1972 [2].

In this article, as a generalization of the result of Nymann, we study the number of elements of $V_m \cap \{(x_1, \ldots, x_m) \in \mathbb{Z}^m \mid |x_i| \leq r \ (1 \leq i \leq m)\}$. Let $V_m(r)$ denote $|V_m \cap \{(x_1, \ldots, x_m) \in \mathbb{Z}^m \mid |x_i| \leq r \ (1 \leq i \leq m)\}|$ and let $E_m(x)$ denote the error term, i.e.

$$E_m(r) = V_m(r) - \frac{2^m}{\zeta(m)} r^m.$$

Then we obtain a generating function of $V_m(r)$ and the exact order of $E_m(r)$, where $m \geq 3$. More precisely, we prove
Theorem 1.1. If \( m \geq 3 \),
\[
E_m(r) = \Omega(r^{m-1}).
\]

Combine Nymann’s result [2] with this theorem, the exact order of the magnitude of \( E_m(r) \) is \( r^{m-1} \) for all \( m \geq 3 \).

2 Jordan totient function \( \varphi(n) \)

In [3], it is proved that
\[
V_2(r) = 8 \sum_{n \leq r} \varphi(n).
\]

We follow this way and use the Jordan totient function \( J_m(n) \) to obtain the value of \( V_m(r) \).

Definition 2.1. For \( m \geq 1 \) we define
\[
J_m(n) := |\{(x_1, \ldots, x_m) \in \mathbb{Z}^m \mid \gcd(x_1, \ldots, x_m, n) = 1, 1 \leq x_i \leq n \ (1 \leq i \leq m)\}|.
\]

For \( m = 0 \) we define
\[
J_0(n) := \begin{cases} 1 & (n = 1) \\ 0 & (n \neq 1) \end{cases}
\]

Since \( J_1(n) = |\{x_1 \in \mathbb{Z} \mid \gcd(x_1, n) = 1, 1 \leq x_1 \leq n\}| = \varphi(n) \), we regard \( J_m(n) \) as a generalization of \( \varphi(n) \).

The Euler totient function \( \varphi(n) \) satisfies
\[
\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right),
\]
where \( \mu(d) \) is Möbius function. As well as this, \( J_m(n) \) satisfies following lemma.

Lemma 2.2. \( J_m(n) = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)^m = n^m \prod_{p|n} \left(1 - \frac{1}{p^m}\right) \).

Proof. It suffices to show that \( n^m = \sum_{d|n} J_m(d) \), because the Möbius inversion formula gives the assertion. Let \( S \) denote \( \{(x_1, \ldots, x_m) \in \mathbb{Z}^m \mid 1 \leq x_i \leq n \ (1 \leq i \leq m)\} \). Let \( S(d) \) be \( \{(x_1, \ldots, x_m) \in \mathbb{Z}^m \mid \gcd(x_1, \ldots, x_m, n) = d, 1 \leq x_i \leq n \ (1 \leq i \leq m)\} \), where \( d \) divides \( n \). Then \( S \) is the disjoint union \( S = \bigcup_{d|n} S(d) \).

\[
\gcd(x_1, \ldots, x_m, n) = d \text{ if and only if } \gcd\left(\frac{x_1}{d}, \ldots, \frac{x_m}{d}, \frac{n}{d}\right) = 1, \text{ so } |S(d)| = J_m\left(\frac{n}{d}\right).
\]

Hence we can write
\[
n^m = |S| = \sum_{d|n} |S(d)| = \sum_{d|n} J_m\left(\frac{n}{d}\right) = \sum_{d|n} J_m(d).
\]
The equality on the left in Lemma follows.

Let us prove the other equality. If \( n = 1 \) the product is empty and assigned to be the value 1.

And if \( n \geq 2 \), we can observe that

\[
\sum_{d \mid n} \frac{\mu(d)}{q^m} = \prod_{\substack{p \mid n \ \text{p-prime}}} \left(1 - \frac{1}{p^m}\right).
\]

Thus the other equality in Lemma also follows. \( \square \)

3 Generating function of \( V_m(r) \)

**Theorem 3.1.** Generating function of \( V_m(r) \) is the following.

\[
\sum_{m=0}^{\infty} \frac{u^m}{m!} V_m(r) = \frac{1}{2u} (e^{(2X+1)u} - e^{(2X-1)u})
\]

and

\[
\sum_{m=0}^{\infty} u^{m+1} V_m(r) = \frac{1}{2} \log \frac{1 - (2X-1)u}{1 - (2X+1)u},
\]

where \( i \sum_{n \leq r} J_{i-1}(n) \) is replaced by \( X^i \) when \( i \geq 1 \), and \( X^0 \) are assigned to be the value 0.

**Proof.** It suffices to show that

\[
V_m(r) = \frac{1}{2(m+1)} ((2X+1)^{m+1} - (2X-1)^{m+1}).
\]

Let \( V_m^+(r) \) denote \( |V^m \cap \{ (x_1, \ldots, x_m) \mid 0 < x_i \leq r \ (1 \leq i \leq m) \}| \) for \( m \geq 1 \).

Considering the sign of component, we have

\[
V_m(r) = \sum_{i=0}^{m-1} \binom{m}{i} 2^{m-i} V_{m-i}^+(r).
\]

Let \( A_m^+(n) = V_m^+(n) - V_m^+(n-1) \), then

\[
V_m^+(r) = \sum_{2 \leq n \leq r} A_m^+(n) + 1.
\]

We compute \( A_m^+(n) \) in a combinatorial way as follows.
Fix $i$ with $0 \leq i < m$. Fix $I \subset \{1, \ldots, m\}$ such that $|I| = m - i$, and let 

\[ V = \{(x_1, \ldots, x_m) \in \mathbb{V}^m \mid x_j = n \text{ for all } j \in I, 0 < x_j < n \text{ for all } j \not\in I\}. \]

Then $|V| = J_i(n)$. There are \( \binom{m}{m-i} \) ways to choose $I \subset \{1, \ldots, m\}$ with $|I| = m - i$. So the number of points $(x_1, \ldots, x_m) \in \mathbb{V}$ such that $|\{i \mid x_i = n\}| \geq m - i$ is \( \binom{m}{m-i} J_i(n) \).

But we count same point $(x_1, \ldots, x_m) \in \mathbb{V}$ such that $|\{i \mid x_i = n\}| = k$, \( \binom{k}{m-i} \) times each $i$ ($m-k \leq i \leq m-1$).

We can show that $(-1)^m \sum_{i=m-k}^{m-1} (-1)^i \binom{k}{m-i} = 1$, so we can count all points in $\mathbb{V}$ without repetition and obtain that $A_m^+(n) = \sum_{j=0}^{m-1} (-1)^{m-1-j} \binom{m}{j} J_j(n)$.

Thus we get

\[ V_m^+(r) = \sum_{2 \leq n \leq r} \sum_{j=0}^{m-i-1} (-1)^{m-i-1-j} \binom{m-i}{j} J_j(n) + 1, \]

and

\[ V_m(r) = \sum_{i=0}^{m-1} \binom{m}{i} 2^{m-i} \left( \sum_{2 \leq n \leq r} \sum_{j=0}^{m-i-1} (-1)^{m-i-1-j} \binom{m-i}{j} J_j(n) + 1 \right). \]

For $j \geq 1$, $X_j$ is defined by $j \sum_{n \leq r} J_{j-1}(n)$. To use this notation, we add the term $n = 1$ to above sum. By the definition of $J_j(n)$, we get $J_j(1) = 1$ for all $j$. And we get $\sum_{j=0}^{m-i-1} (-1)^{m-i-1-j} \binom{m-i}{j} = 1$ by applying the binomial theorem. Using this we have

\[ V_m(r) = \sum_{i=0}^{m-1} \binom{m}{i} 2^{m-i} \left( \sum_{n \leq r} \sum_{j=0}^{m-i-1} (-1)^{m-i-1-j} \binom{m-i}{j} J_j(n) \right). \]

\[ = \sum_{i=0}^{m-1} \binom{m}{i} 2^{m-i} \left( \sum_{j=0}^{m-i-1} (-1)^{m-i-1-j} \binom{m-i}{j} \sum_{n \leq r} J_j(n) \right). \]
By the definition of \( X^j \), we find
\[
\binom{m-i}{j} \sum_{n \leq r} J_j(n) = \frac{1}{m-i+1} \binom{m-i+1}{j+1} X^{j+1},
\]
this gives
\[
= \sum_{i=0}^{m-1} \binom{m-i}{i} 2^{m-i} \frac{1}{m-i+1} \sum_{j=0}^{m-i-1} (-1)^{m-i-j} \binom{m-i+1}{j} X^{j+1}.\]

Replacing the index \( j + 1 \) by \( j \), we obtain
\[
= \sum_{i=0}^{m-1} \binom{m-i}{i} 2^{m-i} \frac{1}{m-i+1} \sum_{j=1}^{m-i} (-1)^{m-i-j} \binom{m-i+1}{j} X^{j}.\]

Because the term \( i = m \) and \( m+1 \) and \( j = 0 \) of above sum are a constant times \( X^0 \), we get
\[
V_m(r) = \sum_{i=0}^{m+1} \binom{m-i}{i} 2^{m-i} \frac{1}{m-i+1} \left( X^{m-i+1} - \sum_{j=0}^{m-i+1} (-1)^{m-i+1-j} \binom{m-i+1}{j} X^{j} \right).
\]

Applying the binomial theorem by repetition, we get
\[
= \sum_{i=0}^{m+1} \binom{m-i}{i} 2^{m-i} \frac{1}{m-i+1} \left( X^{m-i+1} - (X-1)^{m-i+1} \right),
\]
\[
= \frac{1}{2(m+1)} \sum_{i=0}^{m+1} \binom{m+1}{i} \left( (2X)^{m+1} + (2X-2)^{m+1} \right),
\]
\[
= \frac{1}{2(m+1)} \left( (2X+1)^{m+1} + (2X-1)^{m+1} \right).
\]

This proves the theorem. \( \square \)

4 The value of \( \sum_{n \leq r} J_{i-1}(n) \)

In this paper, we use the \( \Omega \) simbol introduced by G.H. Hardy and J.E. Littlewood. This simbol is defined as follows:
\[
f(x) = \Omega(g(x)) \iff \limsup_{x \to \infty} \left| \frac{f(x)}{g(x)} \right| > 0
\]

If there exists a function \( g(x) \) such that \( f(x) = O(g(x)) \) and \( f(x) = \Omega(g(x)) \) then the exact order of \( f(x) \) is \( g(x) \).

Lemma 4.1. Let \( \{x\} \) be the fractional part of \( x \). If \( m \geq 2 \),
\[
\sum_{d \leq r} \mu(d) \left( \frac{r}{d} \right)^m \left\{ \frac{r}{d} \right\} = \Omega(r^m).
\]
Proof. It suffices to show that $\sum_{d \leq r} \frac{\mu(d)}{d^m} \left\{ \frac{r}{d} \right\} \leq M < 0$ for infinity many values of $r$ and some negative $M$.

If $m \geq 4$ and $r$ is odd integer and greater than or equal to 3,

$$
\sum_{d \leq r} \frac{\mu(d)}{d^m} \left\{ \frac{r}{d} \right\} = -\frac{1}{2^{m+1}} + \sum_{3 \leq d \leq r} \frac{\mu(d)}{d^m} \left\{ \frac{r}{d} \right\}.
$$

Since $\mu(d) = 1.0 - 1$ and $\left\{ \frac{r}{d} \right\} \leq 1$,

$$
\leq -\frac{1}{2^{m+1}} + \sum_{3 \leq d \leq r} \frac{1}{d^m},
$$

$$
= -\frac{1}{2^{m+1}} + \zeta(m) - 1 - \frac{1}{2m} < 0,
$$

since when $m \geq 4$, $\zeta(m) - 1 - \frac{1}{2m} < 0$.

So for $m \geq 4$ the lemma follows.

Suppose that $m = 2$ or $m = 3$ and $r = k \prod_{p \leq 100} p$, where the product is extended over all odd primes less than 100 and $k$ isn’t a multiple of 2 and $p$.

Then,

$$
\sum_{d \leq r} \frac{\mu(d)}{d^m} \left\{ \frac{r}{d} \right\} \leq \sum_{d=1}^{100} \frac{\mu(d)}{d^m} \left\{ \frac{r}{d} \right\} + \sum_{d=101}^{\infty} \frac{\mu(d)}{d^m} \left\{ \frac{r}{d} \right\}.
$$

Since $\mu(d) = 1.0 - 1$ and $\left\{ \frac{r}{d} \right\} \leq 1$,

$$
\leq -\frac{1}{2^{m+1}} + \sum_{d=3}^{100} \frac{\mu(d)}{d^m} \left\{ \frac{r}{d} \right\} + \sum_{d=101}^{\infty} \frac{1}{d^m}.
$$

Because we defined $r = k \prod_{p \leq 100} p$, we obtain

$$
\sum_{d=3}^{100} \frac{\mu(d)}{d^m} \left\{ \frac{r}{d} \right\} = \sum_{p=prime}^{47} \frac{1}{(2p)^m} \left( \frac{1}{30^m} + \frac{1}{42^m} + \frac{1}{66^m} + \frac{1}{78^m} + \frac{1}{70^m} \right) < \frac{2}{5} \times \frac{1}{10^{m-1}}
$$
From this result and \( \sum_{d=101}^{\infty} \frac{1}{d^m} \leq \frac{1}{100^{m-1}} \), we find
\[
\sum_{d \leq r} \mu(d) \frac{1}{d^m} \left( \frac{r}{d} \right) \leq -\frac{1}{2^{m+1}} + \frac{2}{5} \times \frac{1}{10^{m-1}} + \frac{1}{100^{m-1}} < \frac{1}{20},
\]
so for \( m = 2 \) or \( m = 3 \) the lemma follows. This completes the proof of the lemma.

Lemma 4.2. If \( i \geq 3 \), \( X^i = \frac{1}{\zeta(i)} r^i + \Omega(r^{i-1}) \)

Proof. For \( i \geq 3 \), \( X^i \) is defined by \( i \sum_{n \leq r} J_{i-1}(n) \).

From Lemma 2.2 we know that \( J_{i-1}(n) = \sum_{d|n} \mu(d) \left( \frac{n}{d} \right)^{i-1} \),
\[
X^i = i \sum_{n \leq r} \mu(d) \left( \frac{n}{d} \right)^{i-1}.
\]

We write \( n = dq \) and sum over all pair of positive integers \( d, q \) with \( dq \leq r \), thus
\[
X^i = i \sum_{dq \leq r} \mu(d) q^{i-1}.
\]

Changing the order of summation,
\[
X^i = i \sum_{d \leq r} \mu(d) \sum_{q \leq \frac{r}{d}} q^{i-1}
\]

Applying the relationship between Bernoulli numbers \( B_0, B_1(= \frac{1}{2}), B_2, \ldots \) and
a sum \( 1^k + 2^k + \cdots + n^k \), that is, \( \sum_{q=1}^{n} q^{i-1} = \frac{1}{i} \sum_{j=0}^{i-1} \left( \begin{array}{c} i \\ j \end{array} \right) B_j n^{i-j} \),
\[
X^i = i \sum_{d \leq r} \mu(d) \sum_{j=0}^{i-1} \left( \begin{array}{c} i \\ j \end{array} \right) B_j \left( \frac{r}{d} \right)^{i-j},
\]
where \( [x] \) is the greatest integer less than or equal to \( x \). Now we use a relation
\[
X^i = \sum_{d \leq r} \mu(d) \sum_{j=0}^{i-1} \left( \begin{array}{c} i \\ j \end{array} \right) B_j \left( \frac{r}{d} - \left\{ \frac{r}{d} \right\} \right)^{i-j}.
\]
We note that
\[ \sum_{d \leq r} \frac{\mu(d)}{d^m} \left( \frac{r}{d} \right)^k \leq \sum_{d \leq r} \frac{1}{d^m} = \begin{cases} \zeta(m) + O(r^{1-m}) & (m \geq 2) \\ \log(r) + \gamma + o(1) & (m = 1), \end{cases} \]
where \( \gamma \) is Euler’s constant, defined by the equation
\[ \gamma = \lim_{n \to \infty} \left( \sum_{k=1}^{n} \frac{1}{k} - \log n \right). \]
Combining this result with Lemma 4.1 and \( \sum_{d \leq r} \frac{\mu(d)}{d^i} = \frac{1}{\zeta(i)} + O \left( \frac{1}{r^{i-1}} \right) \), where \( i > 1 \), we get
\[ X^i = r^i \sum_{d \leq r} \frac{\mu(d)}{d^i} + \Omega(r^{i-1}). \]
This proved the lemma.

5 The exact order of magnitude of \( E_m(r) \)

By using lemmas in last section with Theorem 3.1 we prove following theorem about the exact order of magnitude of \( E_m(r) \).

**Theorem 5.1.** If \( m \geq 3 \),
\[ E_m(r) = \Omega(r^{m-1}). \]

**Proof.**

From Theorem 3.1,
\[ V_m(r) = \frac{1}{2(m+1)} \left( (2X+1)^m - (2X-1)^m \right), \]
\[ = (2X)^m + O(X^{m-2}). \]
Applying Lemma 4.1 and 4.2 we find
\[ V_m(r) = \frac{2^m}{\zeta(m)} r^m + \Omega(r^{m-1}). \]

Combine Nymann’s result [2] with this theorem, the exact order of the magnitude of \( E_m(r) \) is \( r^{m-1} \) for all \( m \geq 3 \).
References

[1] F. Mertens. Ueber einige asymptotische Gesetze der Zahlentheorie. J. Reine Angew. Math, 77 (1874) 289-338.

[2] J. E. Nymann, On the probability that $k$ positive integers are relatively prime, J. Number Theory 4 (1972) 469-473.

[3] T. M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York, 1976.