rings. For example if \( m = p_1^{m_1} \cdots p_r^{m_r} \) is the prime factorization of \( m \), let \( \text{GR}(p_i^{m_i}, m) \) be the Galois ring of order \( p_i^{m_i}, m_i \geq 1 \) for \( i = 1, \ldots, r \). Let \( S \) denote the direct product of the Galois rings \( \text{GR}(p_i^{m_i}, m), i = 1, \ldots, r \). Using the ring \( S \) one can construct various cryptographic systems generalizing those constructed over the residue class ring of integers modulo \( m \). We shall not, however, go into these details here.

Acknowledgement. The authors would like to thank the referee for a number of suggestions that improved an earlier version of the paper.

References


ACTA ARITHMETICA
LIX.4 (1991)

Lattice points in ellipsoids

by

SUKUMAR DAS ADHIKARI (Madras) and Y.-F. S. PÉTERMANN (Genève)

1. Introduction. The main object of this paper is to prove two-sided Omega estimates for the error terms in the classical lattice-points problem for the three- and four-dimensional spheres.

If \( A_l(x) \) is the number of integer lattice-points in an \( l \)-dimensional sphere of radius \( \sqrt{x} \), then as \( x \to \infty \), \( A_l(x) \sim \mathcal{V}_l(x) \), where \( \mathcal{V}_l(x) \) is the volume of the sphere. We denote the corresponding error term by

\[ (1.1) \quad P_l(x) = A_l(x) - \mathcal{V}_l(x). \]

For every \( l > 4 \) it is known that [14, Satz 2.2.2]

\[ (1.2) \quad P_l(x) = O(x^{l/2 - \frac{1}{2}}) \]

and that [14, Sätze 4.4.8 and 4.4.9]

\[ (1.3) \quad P_l(x) = \Omega_l(x^{l/2 - 1}). \]

In fact, a large part of Walfisz' book [14] (Chapters III through VII) is dedicated to the study of the liminf and limsup as \( x \to \infty \) of \( P_l(x) \) for the bounded function \( P_l(x)x^{l/2 - 1} \), which in some cases is determined explicitly or only approximated. The main results gathered in that book is due to Landau, Lursmanaschwill, Petersson and Walfisz. When \( 2 \leq l \leq 4 \), however, the exact order of magnitude of \( P_l(x) \) (in the sense of (1.2) and (1.3)) is not even known. The case \( l = 2 \) is the famous circle problem; to date, the best \( \Omega_2, \Omega_3 \), and \( O \)-estimates are due respectively to Corrádi and Kátai [4], Hafner [5], and Huxley [6].

We first consider the case \( l = 4 \). Walfisz [15] proved that

\[ (1.4) \quad P_4(x) = O(x(\log x)^{2/3}). \]

On the other hand, Adhikari, Balasubramanian and Sankaranarayanan [1] recently obtained the one-sided

\[ (1.5) \quad \Omega_4(x) = \Omega(x \log \log x). \]
by an averaging technique, thus making more precise the estimate of Walfisz [14, Satz 3.1.2].

\[ P_\alpha(x) = \Omega(x \log \log x). \]

Here we prove that

\[ P_\alpha(x) = \Omega_{\alpha}(x \log \log x). \]

In fact, we obtain a more precise and general result. Let \( \bar{n} = (n_1, n_2, n_3, n_4) \in \mathbb{Z}^4 \) and consider the quadratics

\[ Q_k := Q_k(\bar{n}) := n_1^2 + 2^{k/2} n_2^2 + 2^{k/2} n_3^2 + 2^k n_4^2 \]

for \( 0 \leq k \leq 3 \) (where \( \lfloor x \rfloor \) and \( \lceil x \rceil \) denote respectively the largest integer not exceeding \( x \) and the smallest integer not less than \( x \)), the associated four-dimensional ellipsoids

\[ 0 \leq Q_k \leq x \]

of respective volumes

\[ V_{4,k}(x) = \frac{\pi^2}{2^{k+1}} x^2, \]

and the corresponding error terms

\[ R_k(x) := \sum_{n \leq x} r_k(n) - V_{4,k}(x) \]

where

\[ r_k(n) := \sum_{n_k = n} 1. \]

(Thus, \( R_0 \) is \( P_4 \) and \( V_{4,0} \) is \( V_4 \).) We prove in Section 2 below

**Theorem 1.** For \( k = 0, 1, 2, 3 \) and \( \ast = +, - \), we have

\[ \limsup_{x \to \infty} \left( \frac{R_k(x)}{x \log \log x} \right) \geq 2^{1-k} e^{\gamma}, \]

where \( \gamma \) denotes the Euler constant.

We pass to the case \( l = 3 \). To our knowledge the best \( O \)-estimate known to date is due to Vinogradov [11]. On the other hand, Szegö [10] proved in 1926 that

\[ P_3(x) = \Omega_{-}(x^{1/2} \log x^{1/2}). \]

In 1965, unaware of Szegö's result (as all their reviewers!), Bleicher and Knopp [3] derived the weaker and less precise

\[ P_3(x) = \Omega(x^{1/2} \log \log x) \]

from Walfisz' result (1.6). But now, by using their ingenious technique we can derive from (1.5) the estimate

\[ P_3(x) = \Omega_{\alpha}(x^{1/2} \log \log x), \]

which—crossing our fingers—we think is new. (The corresponding \( \Omega_{-} \)-result which follows from (1.7) is again weaker than (1.11).) Here again we prove a result more precise and general. We rewrite (1.8) under the form

\[ Q_k(\bar{n}) = \sum_{i=1}^{4} a_{i_k} n_i^2 \quad (0 \leq k \leq 3), \]

and we consider the three-dimensional ellipsoids

\[ 0 \leq Q_{3,j}(\bar{m}) \leq x \quad (0 \leq k \leq 3; 1 \leq j \leq 4), \]

where

\[ Q_{3,j}(\bar{m}) := \sum_{i=1}^{4} a_{i_k} n_i^2, \]

and

\[ \bar{m}_j = (n_{i_1}, n_{i_2}, n_{i_3}), \quad 1 \leq i_1 < i_2 < i_3 \leq 4, \quad i, \neq j, \]

with respective volumes

\[ W_{3,j}(x) = \frac{3}{3} \pi^{3/2}, \]

where

\[ u_{a_{i_k}} := \prod_{i \neq j} (a_{i_k})^{-1/2}, \]

and the corresponding error terms

\[ R_{3,j}(x) := \sum_{n \leq x} r_{3,j}(n) - W_{3,j}(x), \]

where

\[ r_{3,j}(n) := \sum_{n_{a_{i_k} = n}} 1. \]

(Thus, \( R_{3,0} \) is \( P_3 \).) We prove in Section 3

**Theorem 2.** For each \( R_{3,j} \) defined above and for \( \ast = +, - \), we have

\[ \limsup_{x \to \infty} \left( \frac{R_{3,j}(x)}{x^{3/2} \log \log x} \right) \geq a_{3,j} e^{\gamma}. \]

**Remark.** The four four-dimensional ellipsoids associated with \( Q_k \), \( 0 \leq k \leq 3 \) are considered by Walfisz in [12] and [13], where he studies the asymptotic square mean of \( R_k \). \( O \)-results for the \( R_k \) can be derived from [15, Chapter III].
Estimates for the number of changes in sign of \( R_s \) in the interval \([1, x]\) can be found in [7].

**Acknowledgments.** The two authors were able to meet and complete the present work, at the Tata Institute of Fundamental Research in Bombay, and then in Europe, owing to financial supports granted to them by the International Centre for Theoretical Physics in Trieste (first author) and by the Fond national suisse pour la recherche scientifique (second author). They are grateful to these institutions.

2. **Proof of Theorem 1.** We first recall formulae of Jacobi and Liouville expressing \( r_s(n) \) in terms of the sum-of-divisors function \( \sigma(n) \).

**Lemma 1** ([2; pp. 353–354; and Chapter VIII, §20–22]). Let \( n = 2^su \), where \( u \) is odd and \( k \geq 0 \). Then

\[
\begin{align*}
  r_0(n) &= \begin{cases} 
    8\sigma(u) & \text{if } h = 0, \\
    24\sigma(u) & \text{if } h > 0,
  \end{cases} \\
  r_1(n) &= \begin{cases} 
    4\sigma(u) & \text{if } h = 0, \\
    8\sigma(u) & \text{if } h = 1, \\
    24\sigma(u) & \text{if } h > 1,
  \end{cases} \\
  r_2(n) &= \begin{cases} 
    2\sigma(u) & \text{if } h = 0, \\
    4\sigma(u) & \text{if } h = 1, \\
    8\sigma(u) & \text{if } h = 2, \\
    24\sigma(u) & \text{if } h > 2,
  \end{cases}
\end{align*}
\]

and

\[
\begin{align*}
  r_3(n) &= \begin{cases} 
    \sigma(u) + j(u) & \text{if } h = 0, \\
    2\sigma(u) & \text{if } h = 1, \\
    4\sigma(u) & \text{if } h = 2, \\
    8\sigma(u) & \text{if } h = 3, \\
    24\sigma(u) & \text{if } h > 3,
  \end{cases}
\end{align*}
\]

where

\[
j(n) = \begin{cases} 
    (-1)^{n^2-1/8} \sum_{u=\sqrt{u}+4w} (-1)^{n-1/2} & \text{if } n \text{ is odd}, \\
    0 & \text{if } n \text{ is even}.
  \end{cases}
\]

A straightforward calculation then yields

**Lemma 2.** For \( k = 0, 1, 2, 3 \) we have

\[
\frac{r_k(n)}{n} = 2^{3-k} \sum_{d \mid n} \frac{\alpha_k(d)}{d^2} + \sum_{d \mid n} \frac{\varepsilon_k(n)}{d^2},
\]

where

\[
\alpha_k(d) = \begin{cases} 
    1 & \text{if } d \text{ is odd}, \\
    0 & \text{if } \exists ! d \text{ and } 2^{k+1} \mid d \ (k > 0), \\
    2^k & \text{if } 2^{k+1} \mid d, \\
    -3 \cdot 2^k & \text{if } 2^{k+2} \mid d,
  \end{cases}
\]

and

\[
\varepsilon_k(n) = \begin{cases} 
    0 & \text{if } k = 0, 1 \text{ or } 2, \\
    j(n)/n & \text{if } k = 3.
  \end{cases}
\]

Further, similarly to [1] we set, for \( k = 0, 1, 2, 3 \),

\[
\mathcal{R}_{0k}(x) = \sum_{n \leq x} \left( \sum_{d \mid n} \frac{\alpha_k(d)}{d^2} + \varepsilon_k(n) \right) - \frac{1}{x} \sum_{d=1}^{\infty} \frac{\alpha_k(d)}{d^2}
\]

and

\[
\mathcal{R}_{1k}(x) = \sum_{n \leq x} \left( \sum_{d \mid n} \frac{\alpha_k(d)}{d^2} + \varepsilon_k(n) \right) - \frac{1}{x} \sum_{d=1}^{\infty} \frac{\alpha_k(d)}{d^2}.
\]

It follows from Lemma 2 that

\[
\mathcal{R}_{1k}(x) = 2^{3-k} \mathcal{R}_{0k}(x).
\]

Now, from a result of Walisz [12, Hilfsatz 29], we have

**Lemma 3.**

\[
\sum_{n \leq x} \varepsilon_3(n) = \sum_{n \leq x} j(n) = O(x^{5/6})
\]

and

\[
\sum_{n \leq x} \varepsilon_5(n) = \sum_{n \leq x} j(n)/n = O(1).
\]

The three intermediate results we state below are, with the help of Lemma 3, straightforward generalizations of Lemmata 3.7, 3.8, and 3.9 of [1].

**Lemma 4.** For \( k = 0, 1, 2, 3 \) we have

\[
\sum_{n \leq x} \frac{\alpha_k(n)}{n} = \left( 2^{1-k} + \frac{k}{2} \right) \log 2 + O \left( \frac{1}{x} \right)
\]

and

\[
\sum_{n \leq x} \frac{\alpha_4(n)}{n} = \left( 2^{1-4} + \frac{4}{2} \right) \log 2 + O \left( \frac{1}{x} \right).
\]

**Lemma 5.** For \( k = 0, 1, 2, 3 \) we have

\[
\frac{\mathcal{R}_{1k}(x)}{x} - \mathcal{R}_{0k}(x) = O(1).
\]
Lemma 6. For \( k = 0, 1, 2, 3 \), uniformly in \( x \geq 2 \) and \( y \geq \sqrt{x} \), we have (the second equality being a helpful triviality in view of Lemma 4)

\[
\mathcal{R}_n(x) = -\sum_{d \leq y} \frac{\alpha(d)}{d} \left\{ \frac{x}{d} \right\} + O(1) = -\sum_{d \leq y} \frac{\alpha(d)}{d} \psi\left(\frac{x}{d}\right) + O(1),
\]

where \( \psi(z) := [z] - 1/2 \).

Remark. A typographical accident has made the statement of Lemma 3.5 in [1] incomprehensible. Although we do not appeal to that particular result in the present paper, the fact that we heavily refer to [1] requires an emendation: Lemma 3.5 should read as follows.

"Let \( G(x) \) and \( x/G(x) \) be positive, increasing functions such that

\[
\sum_{d \leq y} h(d)\{x/d\} = O(1) \text{ for } y \gg x/G(x).
\]

Then we have

\[
R_n(x) = -\sum_{d \leq y} h(d)\{x/d\} + O(1) \text{ for } y \gg x/G(x).
\]

We also point out a misprint in the proof of Theorem 1 of [1]: the product in line (4.3) should be on \( p \times q \) (instead of the \( p \times d \)).

From (2.8) and Lemma 5 we see that Theorem 1 is equivalent to the assertion

\[
\limsup_{x \to \infty} \left( \frac{\sigma \mathcal{R}_n(x)}{\log \log x} \right) \geq \frac{e^\gamma}{4}
\]

for \( k = 0, 1, 2, 3 \) and \( * = +, - \). To prove (2.14) we apply to the expression (2.13) of \( \mathcal{R}_n \) the averaging technique of [8]. The function

\[
h_k(x) := \sum_{n \leq x} \frac{\alpha_k(n)}{n} \psi\left(\frac{x}{n}\right)
\]

satisfies the conditions of Theorem 1 in that paper, from which we state here the simplified version we need as

Lemma 7. Let \( A = A(x) > 0 \) and \( B = B(x) \geq 0 \) be integer valued functions, and \( z = z(x) \) be a positive, strictly increasing, continuous and unbounded function. Suppose that \( z \) is regularly \( O \)-varying, i.e. \( \limsup_{x \to \infty} z(2x)/z(x) < \infty \), and that \( u(x) := z(Ax + B) = o(x) \) as \( x \to \infty \). Suppose further that the real function \( g \) satisfies, for \( x > 1 \),

\[
g(x) = \sum_{n \leq x} \frac{\alpha(n)}{n} f\left(\frac{x}{n}\right) = \sum_{n \leq x} \frac{\alpha(n)}{n} f\left(\frac{x}{n}\right) + O(1),
\]

where \( \alpha(n) \) is a sequence of real numbers with a finite asymptotic mean and with \( \sum_{n \leq x} \alpha(n) = O(x) \), and where \( f \) is a periodic function of period 1, of bounded variation and with mean 0. Then

\[
\frac{1}{x} \sum_{n \leq x} g(A_n + B) = \sum_{\lambda \in \mathbb{G}} \frac{\alpha(\lambda)}{1} \sum_{n \in \mathbb{G}} f\left(\frac{n}{1} + B\right) + O(1),
\]

where \( \mathbb{G} \) denotes \( l'(A, l) \).

Before we apply Lemma 7 to \( g = h_k \), with \( z(x) = x^{3/4} \) (and \( \alpha = \alpha_k \), \( f = \psi \)), we state the following particular case of a well-known property of the Bernoulli polynomials \([9, \{1,6\}])

\[
\psi(x) = B_1(x), \text{ where } B_1 \text{ is the first Bernoulli polynomial.}
\]

Lemma 8. With the notation of Lemma 7 we have

\[
\frac{1}{|e^\gamma|} \sum_{n \in \mathbb{G}} \psi\left(\frac{n}{1} + B\right) = \frac{1}{|e^\gamma|} \psi\left(\frac{B}{(A, l)}\right).
\]

Consequently, if \( A = m'!/m = x^{1/4} \), where \( 2^r \| m! \), and if \( B = 0 \), respectively \( B = A - 1 \), we have, for some \( u \) with \( x^{3/4} \ll u \ll \sqrt{x/16} \),

\[
\frac{1}{x} \sum_{n \leq x} h_k(A_n + B) = \sum_{\lambda \in \mathbb{G}} \frac{\alpha_k(\lambda)}{1} \psi\left(\frac{B}{(A, l)}\right) + O(1)
\]

\[
= \sum_{\lambda \in \mathbb{G}} \frac{\alpha_k(\lambda)}{2n} C(n) + O(1),
\]

where

\[
C(n) = \sum_{\lambda \in \mathbb{G}} \frac{\alpha_k(\lambda)}{l^2},
\]

and where \( * denotes - , \text{ respectively } + . \)

Now we have, as \( m \to \infty \),

\[
\sum_{\lambda \in \mathbb{G}} \alpha_k(n) = \prod_{\lambda \in \mathbb{G}} \left(1 + \frac{1}{p^m} + \frac{1}{p^{2m}} + \frac{1}{p^{4m}} + \cdots\right) \sim e^{\gamma} \log m;
\]

and, with the equality

\[
\frac{1}{r^2} \left(1 + 2 + 3 + 4 + \cdots\right) = \frac{1}{r^2},
\]

we see from (2.20), the definition (2.5) of \( \alpha_k \), and the fact that \( A \leq u \), that

\[
C(n) \geq \sum_{\lambda \in \mathbb{G}} \frac{1}{r^2} \geq 1
\]

for every \( n \). Thus, as \( m \to \infty \),

\[
\frac{1}{x} \sum_{n \leq x} h_k(A_n + B) \geq \frac{e^{\gamma}}{4} \log m(1 + o(1)).
\]
Finally, since \( \log \log x \sim \log \log A \sim \log m \), the proof of (2.14) is complete in view of Lemma 6 and definition (2.15).

3. Proof of Theorem 2. We let, for \( k = 0, 1, 2, 3 \) and \( j = 1, 2, 3, 4 \),
\[
M_k(x) := \sum_{n \leq x} r_k(n) \quad \text{and} \quad M_k(x) := \sum_{n \leq x} r_k(n).
\]
(Thus, \( M_0(x) = A_4(x) \) and \( M_0(x) = A_3(x) \).) We have, if \( a_k \) and \( \alpha_k \) are as in (1.13) and (1.15),
\[
M_k(x) = \sum_{m \leq x^{1/2}} M_k(x-a_km^2) = \frac{4}{3} \pi \alpha_k \sum (x-a_km^2)^2 + \sum R_k(x-a_km^2),
\]
where the three sums run over the integers \( m \) with \( |m| \leq (x/a_k)^{1/2} \). Let us suppose that
\[
\limsup_{x \to \infty} \frac{R_k(x)}{x^{1/2} \log \log x} < a_k e^{\eta}.
\]
Then, there are numbers \( \varepsilon > 0 \) and \( N > 3 \) such that if \( x > N \), then
\[
R_k(x) < (a_k e^{\eta} - \varepsilon)x^{1/2} \log \log x.
\]
Also, for any \( x > 3 \), we have
\[
R_k(x) < K x^{1/2} \log \log x
\]
for some \( K \) independent of \( x \). Now, assuming that \( x > N \) and setting \( x_k := x/a_k \), we have
\[
\sum_{-\sqrt{x_k} \leq m \leq \sqrt{x_k}} R_k(x-a_km^2) \leq \sum_{-\sqrt{x_k} \leq N \leq \sqrt{x_k}} R_k(x-a_km^2) + \sum_{N < m \leq \sqrt{x_k}} R_k(x-a_km^2) \leq 2(a_k e^{\eta} - \varepsilon)(x_k-N)^{1/2} x^{1/2} \log \log x + \frac{a_k^{1/2} N x^{1/2} \log \log x}{(x-k_N)^{1/2}} + O(1),
\]
since the number of integers \( m \) with \( \sqrt{x_k-N} \leq |m| \leq \sqrt{x_k} \) is at most
\[
N(a_k/(x-a_k N))^{1/2}.
\]
Thus
\[
\limsup_{x \to \infty} \left( \sum_{-\sqrt{x_k} \leq m \leq \sqrt{x_k}} \frac{R_k(x-a_km^2)}{x^{1/2} \log \log x} \right) \leq 2a_k e^{\eta} - \varepsilon \frac{2e}{\sqrt{a_k}} = 2^{1-k} e^{\eta} - \frac{2e}{\sqrt{a_k}},
\]
since
\[
\left( \prod_{i=1}^{4} a_k \right)^{1/2} = 2^k.
\]
Hence, from (3.2) and Lemma 9 below, we have
\[
M_k(x) = \frac{4}{3} \pi a_k a_k^{1/2} \sum_{-\sqrt{x_k} \leq m \leq \sqrt{x_k}} (x_k-m^2)^{1/2} + S(x)
\]
\[
= \frac{4}{3} \pi a_k a_k^{1/2} \left( \sum_{N \leq x \leq k_N} x \right) + S(x) + O(x) = \frac{\pi^2}{2a_k} x^{1/2} + S(x) + O(x),
\]
where
\[
\limsup_{x \to \infty} \frac{S(x)}{x \log \log x} \leq 2^{1-k} e^{\eta} - \frac{2e}{\sqrt{a_k}},
\]
and this is in contradiction with Theorem 1. Thus (3.3) cannot be true and the proof of Theorem 2 with \(* = +\) is complete. The case \(* = -\) is treated similarly.

**Lemma 9** [3, Lemma 3 for \( k = 3 \)]. We have, as \( x \to \infty \),
\[
\sum_{-\sqrt{x} \leq m \leq \sqrt{x}} (x-m^2)^{1/2} = \frac{4}{3} \pi x^2 + O(x).
\]

References


On some sums involving the largest prime divisor of $n$

by

E. J. SCOURFIELD (London)

1. Introduction. Using analytic methods, R. Balasubramanian and K. Ramachandra proved in [1] that

\[ \sum_{\nu(n) \leq x} 1 \sim C x (\log x)^{\lambda - 1} \quad \text{as } x \to \infty \]

(1.1)

for a class of positive multiplicative functions $g$ satisfying

\[ \begin{align*} 
    g(p) &= \frac{1}{\lambda} & \text{for all primes } p, \\
    g(n) &\gg n^{-1/16} & \text{for all positive integers } n.
\end{align*} \]

(1.2)

In fact they obtained an asymptotic expansion of the form

\[ \sum_{\nu(n) \leq x} 1 = x (\log x)^{\lambda - 1} \sum_{n \leq m \leq \log x} A_m x^{-1} + O(x \exp(-A(\log x)^{3/2}(\log \log x)^{-1/5})). \]

(1.3)

This class of functions $g$ includes the divisor function $d(n)$, when $\lambda = 1/2$, and its reciprocal, when $\lambda = 2$. In the final section of their paper, they remark that a similar result, but with a weaker exponential error term in some cases, can be obtained when the first condition in (1.2) is relaxed to

\[ g(p) = 1/\lambda + O(\exp(-c(\log p)^a)), \]

$c > 0$ and $a \geq 1$ being constants. They asserted that, to establish this when $1 \leq n \leq 3/2$, the contour used to derive (1.3) should be replaced by a modification of the one used by P. T. Bateman, in his method C of [3], to prove that for any fixed $\varepsilon > 0$

\[ \sum_{\nu(n) \leq x} 1 = \frac{\zeta(2)\zeta(3)}{\zeta(6)} x + O(x \exp(-(1-\varepsilon)(\frac{1}{2} \log x \log \log x)^{1/2}))), \]

(1.4)

where $\phi$ denotes Euler's function; an elementary proof of (1.4) has been given recently in [2], and similar sums for other multiplicative functions in a certain class are considered in [17]. When $\lambda = 1$, method C in [3] can be applied directly to estimate $\Sigma_\nu(x)$; see Theorem 7 in Section 8 below.