rings. For example if $m = p_1^{n_1} \dots p_r^{n_r}$ is the prime factorization of m, let $GR(p_i^{n_i}, m_i)$ be the Galois ring of order $p_i^{n_i m_i}$, $m_i \geqslant 1$ for $i = 1, \dots, r$. Let S denote the direct product of the Galois rings $GR(p_i^{n_i}, m_i)$, $i = 1, \dots, r$. 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

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York 1976.

[2] P. S. Bremser and J. Gomez-Calderon, *Value sets of Dickson polynomials over Galois rings*, J. Number Theory 38 (1991), 240–250.

[3] W.-S. Chou, J. Gomez-Calderon and G. L. Mullen, *Value sets of Dickson polynomials over finite fields*, J. Number Theory 30 (1988), 334–344.

[4] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory IT-22 (1976), 644–654.

[5] J. Gomez-Calderon, *On the power polynomial x^d over Galois rings*, Rocky Mountain J. Math., to appear.

[6] H. Lausch and W. Nöbauer, *Algebra of Polynomials*, North-Holland, Amsterdam 1973.

[7] H. Lausch, W. Nöbauer und F. Schweiger, *Polynompermutationen auf Gruppen*, Monatsh. Math. 69 (1965), 410–423.

[8] R. Lidl and W. B. Müller, *Permutation polynomials in RSA-cryptosystems*, in *Advances in Cryptology* (ed. D. Chaum), Plenum Publ. Corp., New York 1984, 293–301.

[9] —, —, *A note on polynomials and functions in algebraic cryptography*, Ars Combin. 17 (1984), 223–229.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., Vol. 20, Addison-Wesley, Reading, Mass., 1983 (now distributed by Cambridge Univ. Press).

[11] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York 1974.

[12] W. B. Müller and W. Nöbauer, *Some remarks on public-key cryptosystems*, Studia Sci. Math. Hungar. 16 (1981), 71–76.

[13] R. Nöbauer, *Über die Fixpunkte von durch Dicksonpolynome dargestellten Permutationen*, Acta Arith. 45 (1985), 173–181.

[14] —, *Key distribution systems based on polynomial functions and on Rédei functions*, Problems Control Inform. Theory 15 (1) (1986), 91–100.

[15] —, *Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen*, Monatsh. Math. 69 (1965), 230–238.

[16] R. L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM 21 (1978), 120–126.

[17] V. Varadharajan, *Cryptosystems based on permutation polynomials*, J. Comput. Math. 23 (1988), 237–250.

DEPARTMENT OF MATHEMATICS
NEW KENSINGTON CAMPUS
THE PENNSYLVANIA STATE UNIVERSITY
New Kensington, PA 15068
U.S.A.

DEPARTMENT OF MATHEMATICS
THE PENNSYLVANIA STATE UNIVERSITY
University Park, PA 16802
U.S.A.

Received on 2.5.1990
and in revised form on 23.11.1990 (2039)

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 $x \to \infty$ $A_l(x) \sim V_l(x)$, where $V_l(x)$ is the volume of the sphere. We denote the corresponding error term by

$$P_l(x) = A_l(x) - V_l(x). \tag{1.1}$$

For every $l > 4$ it is known that [14, Satz 2.2.2]

$$P_l(x) = O(x^{l/2-1}) \tag{1.2}$$

and that [14, Sätze 4.4.8 and 4.4.9]

$$P_l(x) = \Omega_{\pm}(x^{l/2-1}). \tag{1.3}$$

In fact, a large part of Walfisz' book [14] (Chapters III through VII) is dedicated to the study of the lim inf and lim sup as $x \to \infty$ of the bounded function $P_l(x)x^{1-l/2}$, which in some cases are determined explicitly or sharply approximated. The main results gathered in that book are due to Landau, Lursmanaschwili, Petersson and Walfisz. When $2 \leqslant l \leqslant 4$, 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 Ω_+, Ω_-, 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

$$P_4(x) = O(x(\log x)^{2/3}). \tag{1.4}$$

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

$$P_4(x) = \Omega_+(x \log\log x) \tag{1.5}$$

by an averaging technique, thus making more precise the estimate of Walfisz [14, Satz 3.1.2],

(1.6) $$P_4(x) = \Omega(x \log\log x).$$

Here we prove that

(1.7) $$P_4(x) = \Omega_{\pm}(x \log\log x).$$

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

(1.8) $$Q_k := Q_k(\bar{n}) := n_1^2 + 2^{\lfloor k/2 \rfloor} n_2^2 + 2^{\lceil k/2 \rceil} n_3^2 + 2^k n_4^2$$

for $0 \leqslant k \leqslant 3$ (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

$$0 \leqslant Q_k \leqslant x$$

of respective volumes

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

and the corresponding error terms

(1.9) $$R_k(x) := \sum_{n \leqslant x} r_k(n) - V_{4,k}(x)$$

where

$$r_k(n) := \sum_{Q_k = n} 1.$$

(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 $* = +, -$, we have*

(1.10) $$\limsup_{x \to \infty} \left(* \frac{R_k(x)}{x \log\log x} \right) \geqslant 2^{1-k} e^{\gamma},$$

where γ 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

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

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

(1.12) $$P_3(x) = \Omega_{+}(x^{1/2} \log\log x),$$

which – crossing our fingers – we think is new. (The corresponding Ω_{-}-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

(1.13) $$Q_k(\bar{n}) = \sum_{i=1}^{4} a_{ki} n_i^2 \quad (0 \leqslant k \leqslant 3),$$

and we consider the three-dimensional ellipsoids

$$0 \leqslant Q_{kj}(\overline{m_j}) \leqslant x \quad (0 \leqslant k \leqslant 3;\ 1 \leqslant j \leqslant 4),$$

where

(1.14) $$Q_{kj}(\overline{m_j}) = \sum_{\substack{i=1 \\ i \neq j}}^{4} a_{ki} n_i^2,$$

and

$$\overline{m_j} = (n_{i_1}, n_{i_2}, n_{i_3}), \quad 1 \leqslant i_1 < i_2 < i_3 \leqslant 4,\ i_r \neq j,$$

with respective volumes

(1.15) $$W_{kj}(x) = \tfrac{4}{3} \pi \alpha_{kj} x^{3/2},$$

where

$$\alpha_{kj} := \prod_{\substack{i=1 \\ i \neq j}}^{4} (a_{ki})^{-1/2},$$

and the corresponding error terms

(1.16) $$R_{kj}(x) = \sum_{n \leqslant x} r_{kj}(n) - W_{kj}(x),$$

where

$$r_{kj}(n) := \sum_{Q_{kj} = n} 1.$$

(Thus, R_{01} is P_3.) We prove in Section 3

THEOREM 2. *For each R_{kj} defined above and for $* = +, -$ we have*

(1.17) $$\limsup_{x \to \infty} \left(* \frac{R_{kj}(x)}{x^{1/2} \log\log x} \right) \geqslant \alpha_{kj} e^{\gamma}.$$

Remark. The four four-dimensional ellipsoids associated with Q_k ($0 \leqslant k \leqslant 3$) 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 $R_{\mathfrak{g}}$ 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 $r_k(n)$ in terms of the sum-of-divisors function $\sigma(n)$.

LEMMA 1 ([2; pp. 353–354; and Chapter VIII, § 20–22]). *Let* $n = 2^h u$, *where* u *is odd and* $h \geqslant 0$. *Then*

$$r_0(n) = \begin{cases} 8\sigma(u) & \text{if } h = 0, \\ 24\sigma(u) & \text{if } h > 0, \end{cases} \tag{2.1}$$

$$r_1(n) = \begin{cases} 4\sigma(u) & \text{if } h = 0, \\ 8\sigma(u) & \text{if } h = 1, \\ 24\sigma(u) & \text{if } h > 1, \end{cases} \tag{2.2}$$

$$r_2(n) = \begin{cases} 2\sigma(u) & \text{if } h = 0, \\ 4\sigma(u) & \text{if } h = 1, \\ 8\sigma(u) & \text{if } h = 2, \\ 24\sigma(u) & \text{if } h > 2, \end{cases} \tag{2.3}$$

and

$$r_3(n) = \begin{cases} \sigma(u) + j(u) & \text{if } h = 0, \\ 2\sigma(u) & \text{if } h = 1, \\ 4\sigma(u) & \text{if } h = 2, \\ 8\sigma(u) & \text{if } h = 3, \\ 24\sigma(u) & \text{if } h > 3, \end{cases} \tag{2.4}$$

where

$$j(n) = \begin{cases} (-1)^{(n^2-1)/8} \sum\limits_{u = v^2 + 4w^2} (-1)^{(v-1)/2} v & \text{if } n \text{ is odd}, \\ 0 & \text{if } n \text{ is even}. \end{cases}$$

A straightforward calculation then yields

LEMMA 2. *For* $k = 0, 1, 2, 3$ *we have*

$$\frac{r_k(n)}{n} = 2^{3-k} \sum_{d \mid n} \frac{\alpha_k(d)}{d} + \varepsilon_k(n), \tag{2.5}$$

where

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

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 $k = 0, 1, 2, 3$,

$$\mathscr{R}_{0k}(x) = \sum_{n \leqslant x} \left(\sum_{d \mid n} \frac{\alpha_k(d)}{d} + \varepsilon_k(n) \right) - x \sum_{d=1}^{\infty} \frac{\alpha_k(d)}{d^2} \tag{2.6}$$

and

$$\mathscr{R}_{1k}(x) = \sum_{n \leqslant x} n \left(\sum_{d \mid n} \frac{\alpha_k(d)}{d} + \varepsilon_k(n) \right) - \frac{x^2}{2} \sum_{d=1}^{\infty} \frac{\alpha_k(d)}{d^2}. \tag{2.7}$$

It follows from Lemma 2 that

$$R_k(x) = 2^{3-k} \mathscr{R}_{1k}(x). \tag{2.8}$$

Now, from a result of Walfisz [12, Hilfssatz 29], we have

LEMMA 3.

$$\sum_{n \leqslant x} n \varepsilon_3(n) = \sum_{n \leqslant x} j(n) = O(x^{5/6}) \tag{2.9}$$

and

$$\sum_{n \leqslant x} \varepsilon_3(n) = \sum_{n \leqslant x} \frac{j(n)}{n} = O(1). \tag{2.10}$$

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*

$$\sum_{n \leqslant x} \frac{\alpha_k(n)}{n} = \left(2 + \frac{k}{2}\right) \log 2 + O\left(\frac{1}{x}\right). \tag{2.11}$$

LEMMA 5. *For* $k = 0, 1, 2, 3$ *we have*

$$\frac{\mathscr{R}_{1k}(x)}{x} - \mathscr{R}_{0k}(x) = O(1). \tag{2.12}$$

LEMMA 6. *For $k = 0, 1, 2, 3$, uniformly in $x \geqslant 2$ and $y \geqslant \sqrt{x}$, we have (the second equality being a—helpful—triviality in view of Lemma 4)*

$$(2.13)\qquad \mathscr{R}_{0k}(x) = -\sum_{d \leqslant y} \frac{\alpha_k(d)}{d}\left\{\frac{x}{d}\right\} + O(1) = -\sum_{d \leqslant y} \frac{\alpha_k(d)}{d}\psi\left(\frac{x}{d}\right) + O(1),$$

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

$$\sum_{d > y} h(d)\{x/d\} = O(1) \quad \text{for} \quad y \geqslant x/G(x).$$

Then we have

$$R_0(x) = -\sum_{d \leqslant y} h(d)\{x/d\} + O(1) \quad \text{for} \quad y \geqslant x/G(x)."$$

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

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

$$(2.14)\qquad \limsup_{x \to \infty}\left(* \frac{\mathscr{R}_{0k}(x)}{\log\log x}\right) \geqslant \frac{e^{\gamma}}{4}$$

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

$$(2.15)\qquad h_k(x) := \sum_{n \leqslant x} \frac{\alpha_k(d)}{d}\psi\left(\frac{x}{d}\right)$$

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 $B = B(x) \geqslant 0$ 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 $x > 1$,*

$$(2.16)\qquad g(x) = \sum_{n \leqslant x} \frac{\alpha(n)}{n} f\left(\frac{x}{n}\right) = \sum_{n \leqslant z} \frac{\alpha(n)}{n} f\left(\frac{x}{n}\right) + O(1),$$

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

$$(2.17)\qquad \frac{1}{x}\sum_{n \leqslant x} g(An + B) = \sum_{l \leqslant u} \frac{\alpha(l)}{l}\left(\frac{1}{l^*}\sum_{n \leqslant l^*} f\left(\frac{n}{l^*} + \frac{B}{l}\right)\right) + O(1),$$

where l^* 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, (1.6.1)], noting that $\psi(x) = B_1(\{x\})$, where B_1 is the first Bernoulli polynomial.

LEMMA 8. *With the notation of Lemma 7 we have*

$$(2.18)\qquad \frac{1}{l^*}\sum_{n \leqslant l^*} \psi\left(\frac{n}{l^*} + \frac{B}{l}\right) = \frac{1}{l^*}\psi\left(\frac{B}{(A, l)}\right).$$

Consequently, if $A = m!/2^r = x^{1/4}$, where $2^r \| m!$, and if $B = 0$, respectively $B = A - 1$, we have, for some u with $x^{15/16} \ll u \ll x^{15/16}$,

$$(2.19)\qquad \frac{1}{x}\sum_{n \leqslant x} h_k(An + B) = \sum_{l \leqslant u} \frac{\alpha_k(l)}{l^2}(A, l)\psi\left(\frac{B}{(A, l)}\right) + O(1)$$

$$= *\sum_{n|A} \frac{\alpha_k(n)}{2n} C(n) + O(1),$$

where

$$(2.20)\qquad C(n) = \sum_{\substack{l \leqslant u/n \\ p|l \text{ and } p^{\alpha} \| A \text{ then } p^{\alpha} \| n}} \alpha_k(l)/l^2,$$

and where $*$ denotes $-$, respectively $+$.

Now we have, as $m \to \infty$,

$$(2.21)\qquad \sum_{n|A} \frac{\alpha_k(n)}{n} = \prod_{p^{\alpha_p} \| A}\left(1 + \frac{1}{p} + \ldots + \frac{1}{p^{\alpha_p}}\right) \sim \frac{e^{\gamma}}{2}\log m;$$

and, with the equality

$$(2.22)\qquad \frac{1}{r^2}\left(1 + \frac{2^k}{2^{2(k+1)}} - 3 \cdot 2^k\left(\frac{1}{2^{2(k+2)}} + \frac{1}{2^{2(k+3)}} + \ldots\right)\right) = \frac{1}{r^2},$$

we see from (2.20), the definition (2.5) of α_k, and the fact that $A \leqslant u$, that

$$(2.23)\qquad C(n) \geqslant \sum_{\substack{r \equiv 1\,(2) \text{ and } r \leqslant u/n; \\ p|r \text{ and } p^{\alpha} \| A \text{ then } p^{\alpha} \| n}} \frac{1}{r^2} \geqslant 1$$

for every n. Thus, as $m \to \infty$,

$$(2.24)\qquad *\frac{1}{x}\sum_{n \leqslant x} h_k(An + B) \geqslant \frac{e^{\gamma}}{4}\log m(1 + o(1)).$$

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 $j = 1, 2, 3, 4$,

(3.1) $$M_k(x) := \sum_{n \leqslant x} r_k(n) \quad \text{and} \quad M_{kj}(x) := \sum_{n \leqslant x} r_{kj}(n).$$

(Thus, $M_0(x) = A_4(x)$ and $M_{0j}(x) = A_3(x)$.) We have, if a_{kj} and α_{kj} are as in (1.13) and (1.15),

(3.2) $$\begin{aligned} M_k(x) &= \sum M_{kj}(x - a_{kj}m^2) \\ &= \tfrac{4}{3}\pi\alpha_{kj} \sum (x - a_{kj}m^2)^{3/2} + \sum R_{kj}(x - a_{kj}m^2), \end{aligned}$$

where the three sums run over the integers m with $|m| \leqslant (x/a_{kj})^{1/2}$. Let us suppose that

(3.3) $$\limsup_{x \to \infty} \frac{R_{kj}}{x^{1/2} \log\log x} < \alpha_{kj} e^{\gamma}.$$

Then, there are numbers $\varepsilon > 0$ and $N > 3$ such that if $x > N$, then

(3.4) $$R_{kj}(x) < (\alpha_{kj} e^{\gamma} - \varepsilon) x^{1/2} \log\log x.$$

Also, for any $x > 3$, we have

(3.5) $$R_{kj}(x) < K x^{1/2} \log\log x$$

for some K independent of x. Now, assuming that $x > N$ and setting $x_{kj} := x/a_{kj}$, we have

$$\begin{aligned} &\sum_{-\sqrt{x_{kj}} \leqslant m \leqslant \sqrt{x_{kj}}} R_{kj}(x - a_{kj}m^2) \\ &= \sum_{-\sqrt{x_{kj} - N} < m < \sqrt{x_{kj} - N}} R_{kj}(x - a_{kj}m^2) + \sum_{\sqrt{x_{kj} - N} \leqslant |m| \leqslant \sqrt{x_{kj}}} R_{kj}(x - a_{kj}m^2) \\ &\leqslant 2(\alpha_{kj} e^{\gamma} - \varepsilon)(x_{kj} - N)^{1/2} x^{1/2} \log\log x + \frac{a_{kj}^{1/2} K N x^{1/2} \log\log x}{(x - a_{kj}N)^{1/2}} + O(1), \end{aligned}$$

since the number of integers m with $\sqrt{x_{kj} - N} \leqslant |m| \leqslant \sqrt{x_{kj}}$ is at most

$$N\big(a_{kj}/(x - a_{kj}N)\big)^{1/2}.$$

Thus

$$\limsup_{x \to \infty} \left(\frac{\sum_{-\sqrt{x_{kj}} \leqslant m \leqslant \sqrt{x_{kj}}} R_{kj}(x - a_{kj}m^2)}{x^{1/2} \log\log x} \right) \leqslant \frac{2\alpha_{kj} e^{\gamma} - 2\varepsilon}{\sqrt{a_{kj}}} = 2^{1-k} e^{\gamma} - \frac{2\varepsilon}{\sqrt{a_{kj}}},$$

since

$$\Big(\prod_{i=1}^{4} a_{ki}\Big)^{1/2} = 2^k.$$

Hence, from (3.2) and Lemma 9 below, we have

$$\begin{aligned} M_k(x) &= \tfrac{4}{3}\pi\alpha_{kj} a_{kj}^{3/2} \sum_{-\sqrt{x_{kj}} \leqslant m \leqslant \sqrt{x_{kj}}} (x_{kj} - m^2)^{3/2} + S(x) \\ &= \tfrac{4}{3}\pi\alpha_{kj} a_{kj}^{3/2} (\tfrac{3}{8}\pi x_{kj}^2) + S(x) + O(x) = \frac{\pi^2}{2^{k+1}} x^2 + S(x) + O(x), \end{aligned}$$

where

$$\limsup_{x \to \infty} \frac{S(x)}{x \log\log x} \leqslant 2^{1-k} e^{\gamma} - \frac{2\varepsilon}{\sqrt{a_{kj}}},$$

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* $x \to \infty$,

$$\sum_{-\sqrt{x} \leqslant m \leqslant \sqrt{x}} (x - m^2)^{3/2} = \tfrac{3}{8}\pi x^2 + O(x).$$

References

[1] S. D. Adhikari, R. Balasubramanian and A. Sankaranarayanan, *An Ω-result related to $r_4(n)$*, Hardy–Ramanujan J. 12 (1989), 20–30.

[2] P. Bachmann, *Niedere Zahlentheorie*, vol. II, Leipzig 1910, repr. by Chelsea, New York 1968.

[3] M. N. Bleicher and M. I. Knopp, *Lattice points in a sphere*, Acta Arith. 10 (1965), 369–376.

[4] K. Corrádi and I. Kátai, *A comment on K. S. Gangadharan's paper entitled "Two classical lattice point problems"*, Magyar Tud. Akad. Mat. Fiz. Oszt. Közl. 17 (1967), 89–97.

[5] J. Hafner, *New omega-theorems for two classical lattice point problems*, Invent. Math. 63 (1981), 181–186.

[6] M. N. Huxley, *Exponential sums and lattice points*, Proc. London Math. Soc. 60 (1990), 471–502.

[7] Y.-F. S. Pétermann, *Changes of sign of error terms related to Euler's function and to divisor functions*, Comment. Math. Helv. 61 (1986), 84–101.

[8] —, *About a theorem of Paolo Codecà's and Ω-estimates for arithmetical convolutions*, J. Number Theory 30 (1988), 71–85.

[9] H. Rademacher, *Topics in Analytic Number Theory*, Springer, Berlin 1973.

[10] G. Szegö, *Beiträge zur Theorie der Laguerreschen Polynome II, Zahlentheoretische Anwendungen*, Math. Z. 25 (1926), 388–404.

[11] I. M. Vinogradov, *On the number of integral points in a given domain* (in Russian), Izv. Akad. Nauk. SSSR Ser. Mat. 24 (1960), 777–786.

[12] A. Walfisz, *Über Gitterpunkte in mehrdimensionalen Ellipsoiden. Fünfte Abhandlung*, Acta Arith. 1 (1936), 222–283.
[13] —, *Teilerprobleme. Fünfte Abhandlung*, ibid. 2 (1937), 80–133.
[14] —, *Gitterpunkte in mehrdimensionalen Kugeln*, PWN, Warszawa 1957.
[15] —, *Weylsche Exponentialsummen in der neueren Zahlentheorie*, Deutscher Verlag der Wissenschaften, Berlin 1963.

THE INSTITUTE OF MATHEMATICAL SCIENCES
Madras 600113, India

UNIVERSITÉ DE GENÈVE
SECTION DE MATHÉMATIQUES
2-4, rue du Lievre, C.P. 240
Ch-1211 Genève

Received on 21.8.1990
and in revised form on 17.12.1990 (2068)

ACTA ARITHMETICA
LIX.4 (1991)

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

$$(1.1)\qquad \Sigma_g(x) = \sum_{ng(n)\leqslant x} 1 \sim Cx(\log x)^{\lambda-1} \quad \text{as } x\to\infty$$

for a class of positive multiplicative functions g satisfying

$$(1.2)\qquad \begin{cases} g(p) = 1/\lambda & \text{for all primes } p,\\ g(n) \gg n^{-1/16} & \text{for all positive integers } n. \end{cases}$$

In fact they obtained an asymptotic expansion of the form

$$(1.3)\qquad \Sigma_g(x) = x(\log x)^{\lambda-1} \sum_{n\leqslant m\leqslant(\log x)^{4/5}} A_{m,n}(\log x)^{-m}(\log\log x)^n + O\big(x\exp(-A(\log x)^{3/5}(\log\log x)^{-1/5})\big).$$

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

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

$c > 0$ and $a \geqslant 1$ being constants. They asserted that, to establish this when $1 \leqslant a \leqslant 3/2$, 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 $\varepsilon > 0$

$$(1.4)\qquad \sum_{\varphi(n)\leqslant x} 1 = \frac{\zeta(2)\zeta(3)}{\zeta(6)}x + O\big(x\exp(-(1-\varepsilon)(\tfrac{1}{2}\log x\log\log x)^{1/2})\big),$$

where φ 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 $\Sigma_g(x)$; see Theorem 7 in Section 8 below.