ACTA ARITHMETICA
LXVII.4 (1994)

Sums of distinct squares

by

PAUL T. BATEMAN (Urbana, Ill.), ADOLF J. HILDEBRAND (Urbana, Ill.) and GEORGE B. PURDY (Cincinnati, Ohio)

1. Introduction. Throughout this paper we shall suppose that s is an integer ≥ 5. Then order of magnitude considerations show that every sufficiently large integer is expressible as a sum of s distinct non-zero squares. In fact, E. M. Wright [Wr] proved that, if $s \geq 5$, then for large n we can essentially prescribe the ratios of the squares in expressing n as a sum of s squares. Thus, for each $s \geq 5$ there exists a largest integer $N(s)$ which is *not* expressible as a sum of s distinct non-zero squares. In this paper we shall obtain asymptotic estimates for $N(s)$.

In a recent paper [HK], Halter-Koch considered representations of integers as sums of s distinct non-zero *coprime* squares, and he proved among other things the following results.

THEOREM 0 (Halter-Koch). *The largest odd integer not expressible as a sum of* 4 *distinct non-zero squares with greatest common divisor* 1 *is* 157. *Moreover*, *if* $N^*(s)$ *denotes the largest integer not expressible as a sum of* s *distinct non-zero squares with greatest common divisor* 1, *then* $N^*(5) = 245$, $N^*(6) = 333$, $N^*(7) = 330$, $N^*(8) = 462$, $N^*(9) = 539$, $N^*(10) = 647$, $N^*(11) = 888$, *and* $N^*(12) = 1036$.

Halter-Koch also proved a number of related results. For example, he showed that for $s \geq 5$,

$$N^*(s+1) \leq 2(\sqrt{N^*(s)} + 2)^2,$$

which enables one to derive an explicit (but rather crude) bound for $N^*(s)$.

Of the two quantities $N(s)$ and $N^*(s)$, the former is the more natural one, and we shall express our results in terms of $N(s)$. Trivially, we have $N^*(s) \geq N(s)$ for all $s \geq 5$, and we shall show in Theorem 5 that the two functions are in fact identical. Thus, the coprimality condition in the definition of $N^*(s)$ does not affect the results in any way.

Research of the second author supported in part by an NSF Grant.

Since any sum of s distinct positive squares must be greater than or equal to the sum of the first s positive squares, namely

$$P(s) = \sum_{i=1}^{s} i^2 = s(s+1)(2s+1)/6,$$

we have the trivial lower bound $N(s) \geq P(s) - 1$. In fact, $N(s)$ must be strictly larger than $P(s)$ since, for example, $P(s) + 1$ is not expressible as a sum of s distinct squares. Our principal result (Theorem 1) shows among other things that $N(s)$ is asymptotically equal to this lower bound $P(s)$ and gives a fairly precise estimate for the difference

$$R(s) = N(s) - P(s).$$

In order to state this main theorem, we define $\lambda_s \geq 0$ by

$$\lambda_s^2 = 2\max(\|\sqrt{2s}\|, \|\sqrt{2s} - 1/2\|),$$

where $\|\cdot\|$ denotes the distance to the nearest integer. It is easy to see that

$$\lambda_s^2 = 1/2 + \|\sqrt{8s} - 1/2\|. \tag{1.1}$$

We further set, for any non-negative real number x,

$$\mathcal{L}_x = \log\log\max(x, e^e), \quad t_x = \lfloor \mathcal{L}_x/\log 2 \rfloor, \quad f(x) = \sum_{i=0}^{t_x} x^{2^{-i}}.$$

Theorem 1. (i) *We have the asymptotic formula*

$$R(s) = 2s\{\sqrt{2s} + \lambda_s(2s)^{1/4} + O(s^{1/8})\}. \tag{1.2}$$

(ii) *We have the upper estimate*

$$R(s) \leq 2s\{f(\sqrt{2s}) + O(\mathcal{L}_s^2)\}. \tag{1.3}$$

(iii) *The bound* (1.3) *is best possible in the sense that there exists an increasing sequence* $\{s_k\}$ *of positive integers such that*

$$R(s_k) \geq 2s_k\{f(\sqrt{2s_k}) + O(\mathcal{L}_{s_k})\}. \tag{1.4}$$

An example of such a sequence is given by taking $s_1 = 1$ *and* $s_k = 2s_{k-1}^2 + s_{k-1}$ *for* $k \geq 2$.

The estimate (1.2) shows in particular that $R(s) \ll \sqrt{P(s)}$. The second main term on the right-hand side of (1.2) involves the oscillatory quantity λ_s, which depends on how $8s$ is situated relative to the sequence of squares. From the representation (1.1) of λ_s it is clear that $1/\sqrt{2} \leq \lambda_s \leq 1$ and that these bounds are best possible. Specifically, λ_s will be near its maximal value 1 if $8s$ is close to a square; and λ_s will be near its minimal value $1/\sqrt{2}$ when $8s$ is roughly midway between two consecutive squares, for example, when s has the form $m(8m \pm 1)$. Thus, $R(s) = N(s) - P(s)$ oscillates between the limits $(2s)^{3/2} + (2s)^{5/4}/\sqrt{2}$ and $(2s)^{3/2} + (2s)^{5/4}$, up to an error term $O(s^{9/8})$.

The inequality (1.3) gives a universal upper bound for $R(s)$ which sharpens that of (1.2) when $8s$ is close to a square and which by (1.4) is best possible.

The remainder of this paper is organized as follows. In Section 2 we give an explicit polynomial upper bound for $N(s)$, namely $N(s) < (s-1)^5$ for $s \ge 5$ (Theorem 2), which will be needed as a basis for the subsequent arguments. In Section 3 we reformulate the problem of determining $N(s)$ and state a result (Theorem 3) about a related extremal problem. This problem concerns the minimum $Q(m)$ of $\sum_{i=1}^{t} a_i$ for all representations of the integer m in the form $m = \sum_{i=1}^{t} \varepsilon_i a_i^2$, where $\varepsilon_i = \pm 1$ for all i and $a_1, \ldots, a_t$ are distinct positive integers. Theorem 3 gives estimates for $Q(m)$ parallel to those of Theorem 1 and forms the principal ingredient in the proof of that theorem, but is also of some interest for its own sake. In Sections 4 and 5 we prove Theorem 3, and in Sections 6 and 7 we prove Theorem 1. In Section 8, we give the explicit upper bound (Theorem 4)

$$N(s) < P(s) + 2s\sqrt{2s} + 44s^{5/4} + 108s \quad (s \ge 166), \tag{1.5}$$

which is useful for various purposes. In particular, we use (1.5) to show that the function $N(s)$ is monotonic for $s \ge 7$; this answers a question of Erdős. (Note, however, that the function $R(s) = N(s) - P(s)$ is *not* monotonic, since (1.2) gives $R(8m^2) > R(8m^2 + m)$ for all large m.) In Section 9, we prove the above remark that $N(s) = N^*(s)$ for every $s \ge 5$; in fact, we show (Theorem 5) that if a positive integer is expressible as a sum of $s \ge 5$ distinct non-zero squares then it is also expressible as a sum of s distinct non-zero squares with greatest common divisor 1. In Section 10 we make some remarks on the more general problem of expressing an integer as a sum of s distinct positive kth powers. Using the results of Hardy and Littlewood on Waring's problem, we show (Theorem 6) that if $N_k(s)$ denotes the largest integer not expressible in this form, then

$$N_k(s) = \frac{s^{k+1}}{k+1} + O(s^k).$$

In the final section, we discuss the computation of $N(s)$ and we give two tables of numerical data.

2. An initial upper bound. Using the result of Halter-Koch on four squares mentioned in the preceding section, we obtain the rough bound $N(s) < (s-1)^5$, which will be needed later on.

THEOREM 2. *If $s \ge 5$ and if $n \ge (s-1)^5$, then n is expressible as a sum of s distinct non-zero squares.*

Proof. It is convenient to prove the assertion of the theorem under the slightly weaker assumption $n \ge (s-1)^4(s-3)$. For $i = 1, 2, \ldots, s-5$ we put $a_i = \lfloor\sqrt{n/(s-3)}\rfloor + i$; we also put $a_{s-4} = \lfloor\sqrt{n/(s-3)}\rfloor + s - 4 + \delta$, where $\delta \in \{0, 1\}$ is chosen so that $r = n - a_1^2 - a_2^2 - \ldots - a_{s-4}^2$ is odd. (When $s = 5$, only a_{s-4} is needed.) Then $a_i^2 > n/(s-3)$ for each i and thus $r < n/(s-3)$. Moreover,

$$r \ge n - \sum_{i=1}^{s-5}\left(\sqrt{\frac{n}{s-3}} + i\right)^2 - \left(\sqrt{\frac{n}{s-3}} + s - 3\right)^2 = f_s(n),$$

say. A simple calculation gives

$$f_s(n) = \frac{n}{s-3} - (s^2 - 7s + 14)\sqrt{\frac{n}{s-3}} - (2s^3 - 21s^2 + 85s - 126)/6.$$

Clearly $f_s(n)$ is an increasing function of n provided $\sqrt{n/(s-3)} > (s^2 - 7s + 14)/2$. This condition is satisfied if $s \ge 5$ and $n \ge (s-1)^4(s-3)$. Thus, if $n \ge (s-1)^4(s-3)$, we have

$$r \ge f_s(n) \ge f_s((s-1)^4(s-3)) = \frac{14}{3}s^3 - \frac{39}{2}s^2 + \frac{101}{6}s + 8.$$

The polynomial on the right-hand side here is an increasing function of s for $s \ge 5$ and hence

$$r \ge \frac{14}{3}5^3 - \frac{39}{2}5^2 + \frac{101}{6}5 + 8 = 188.$$

Since r is odd and greater than 157, Theorem 0 shows that r is expressible as a sum of four distinct non-zero squares. Since each of these four squares is less than

$$r < n/(s-3) < a_1^2 < a_2^2 < \ldots < a_{s-4}^2$$

and since $n = r + a_1^2 + a_2^2 + \ldots + a_{s-4}^2$, the assertion of the theorem follows.

3. An extremal problem. In this section we rephrase the problem of estimating $N(s)$ in a form which is more suitable when dealing with integers that are close to $P(s)$, and we state a result (Theorem 3), which will form the principal ingredient in the proof of Theorem 1. The underlying idea is that if n is an integer close to $P(s) = \sum_{i=1}^{s} i^2$ which has a representation $n = \sum_{i=1}^{s} a_i^2$ as a sum of s distinct squares, then the set $\{a_i : i \le s\}$ can be expected to be "close" to the set $\{i : i \le s\}$.

To make this idea precise, we note that any set $\{a_i : i \le s\}$ of distinct positive integers can be obtained from the set $\{i : i \le s\}$ by replacing some of the integers $i \le s$, say $s - h_i$, $i \le t$, by distinct integers $> s$, say $s + k_i$,

$i \le t$. The associated representation $n = \sum_{i=1}^s a_i^2$ can then be written as

$$n = \sum_{i=1}^{s} i^2 - \sum_{i=1}^{t} (s-h_i)^2 + \sum_{i=1}^{t} (s+k_i)^2 \tag{3.1}$$
$$= P(s) + 2s \sum_{i=1}^{t} (h_i + k_i) + \sum_{i=1}^{t} (k_i^2 - h_i^2),$$

where the numbers h_i and k_i satisfy

$$h_i \text{ distinct}, \quad 0 \le h_i < s, \tag{3.2}$$

$$k_i \text{ distinct}, \quad k_i \ge 1. \tag{3.3}$$

Conversely, any integer n expressible in the form (3.1) with the conditions (3.2) and (3.3) is a sum of s distinct positive squares. Therefore, $R(s) = N(s) - P(s)$ *is the largest integer* r *not expressible in the form*

$$r = 2s \sum_{i=1}^{t} (h_i + k_i) + \sum_{i=1}^{t} (k_i^2 - h_i^2) \tag{3.4}$$

with integers h_i *and* k_i *satisfying* (3.2) *and* (3.3).

The above formulation leads naturally to the problem of minimizing the sum $\sum_{i=1}^t (h_i + k_i)$, subject to the conditions (3.2) and (3.3), while holding the sum $\sum_{i=1}^t (k_i^2 - h_i^2)$ fixed. However, this extremal problem is somewhat awkward to deal with directly, as the conditions (3.2) and (3.3) are not symmetrical and depend on the parameter s. We therefore consider the following related, but simpler and more natural problem, which is sufficient for the application to the proof of Theorem 1 and also is of some intrinsic interest. For $m \ne 0$ set

$$Q(m) = \min \Big\{ \sum_{i=1}^{t} a_i : \sum_{i=1}^{t} \varepsilon_i a_i^2 = m \Big\}, \tag{3.5}$$

where the minimum is taken over all sets $\{a_i : i \le t\}$ of distinct positive integers satisfying $\sum_{i=1}^t \varepsilon_i a_i^2 = m$ with suitable numbers $\varepsilon_i \in \{\pm 1\}$, and define $Q(0) = 0$. The quantity $Q(m)$ may be viewed as a measure for how "economically" m can be represented as a difference of sums of distinct squares. The following result gives precise upper and lower bounds for $Q(m)$ that are largely parallel to those of Theorem 1. Since $m = ((m+10)/2)^2 - ((m+8)/2)^2 - 3^2$ for even positive integers m and $m = ((m+17)/2)^2 - ((m+15)/2)^2 - 4^2$ for odd positive integers m, every non-zero integer m has indeed a representation $m = \sum_{i=1}^t \varepsilon_i a_i^2$ of the above form, so that $Q(m)$ is well-defined. Halter-Koch's result that $N^*(5) = 245$, along with Schwarz's inequality, shows that trivially $Q(m) \le \sqrt{5m}$ for $m \ge 246$.

THEOREM 3. (i) *We have the asymptotic formula*

$$Q(m) = \sqrt{|m|} + \sqrt{2\theta_{|m|}}\,|m|^{1/4} + O(|m|^{1/8}), \tag{3.6}$$

where $\theta_x = \|\sqrt{x}\|$.

(ii) *We have the upper estimate*

$$Q(m) \le f(\sqrt{|m|}\,) + O(\mathcal{L}_{|m|}), \tag{3.7}$$

where $f(x)$ *and* $\mathcal{L}_x$ *are defined as in Theorem* 1.

(iii) *The inequality* (3.7) *is best possible in the sense that if the sequence* $\{m_k\}$ *is defined by* $m_0 = 1$ *and* $m_k = m_{k-1}^2 + m_{k-1}$ *for* $k \ge 1$, *then we have*

$$Q(m_k) \ge f(\sqrt{m_k}\,) + O(\mathcal{L}_{m_k}). \tag{3.8}$$

(iv) *The upper bounds in* (3.6) *and* (3.7) *remain valid if in the definition* (3.5) *of* $Q(m)$, t *is restricted by the condition*

$$t \le C\mathcal{L}_{|m|}, \tag{3.9}$$

where C *is a suitable absolute constant.*

4. Proof of Theorem 3; upper bounds. Call a representation $m = \sum_{i=1}^{t} \varepsilon_i a_i^2$ *admissible* if $\varepsilon_i \in \{\pm 1\}$ and the numbers a_i are distinct positive integers. To obtain the upper bounds of Theorem 3 (in the stronger form claimed in the last part of Theorem 3), we need to construct an admissible representation with $t \le C\mathcal{L}_{|m|}$ for which the sum $\sum_{i=1}^{t} a_i$ is bounded by the right-hand sides of (3.6) and (3.7). Our construction is essentially that obtained by the greedy algorithm, supplemented by a direct argument for the first few values of m. We first dispose of the case of small m with the following lemma.

LEMMA 4.1. *If* $0 < |m| \le 37$, *then* m *has an admissible representation* $m = \sum_{i=1}^{t} \varepsilon_i a_i^2$ *such that* $a_i \le 5$ *for all* i.

Proof. The identities $1 = 1^2$, $2 = 4^2 - 3^2 - 2^2 - 1^2$, $3 = 2^2 - 1^2$, $4 = 2^2$, $5 = 2^2 + 1^2$, $6 = 3^2 - 2^2 + 1^2$, $7 = 4^2 - 3^2$, $8 = 3^2 - 1^2$, $9 = 3^2$, $10 = 3^2 + 1^2$, $11 = 4^2 - 2^2 - 1^2$, $12 = 4^2 - 2^2$, and $13 = 3^2 + 2^2$ show that every m with $0 < m \le 13$ has a representation of the required form with $a_i \le 4$. Replacing ε_i by $-\varepsilon_i$ in each of these representations, we see that the same is true for $-13 \le m < 0$. In the remaining range $13 < |m| \le 37$ the result follows by writing $m = \varepsilon 5^2 + m'$ with $\varepsilon \in \{\pm 1\}$ and $|m'| \le 12$ and representing m' in the above form using squares a_i^2 with $a_i \le 4$.

The lemma shows that for $0 < |m| \le 37$, $Q(m)$ is well-defined and satisfies the bounds (3.6) and (3.7) trivially, provided the O-constants are suitably chosen. The same is true for $m = 0$, since by definition $Q(0) = 0$. To deal with the general case, we begin with the following observation. Given an arbitrary integer m, let $q = \lfloor \sqrt{|m|} \rfloor$, so that $q^2 \le |m| \le q^2 + 2q$, and set $a = \langle\sqrt{|m|}\rangle$, where $\langle x\rangle$ denotes the nearest integer to x. (Note that, since $\sqrt{|m|}$ cannot be half an odd integer, there is no ambiguity in the definition of $\langle\sqrt{|m|}\rangle$.) Then $a = q$ if $q^2 \le |m| \le q^2 + q$, $a = q + 1$ if $q^2 + q + 1 \le |m| \le q^2 + 2q$, and in either case we have $m = \varepsilon a^2 + r$ with $\varepsilon = \mathrm{sign}(m)$ (with the convention $\mathrm{sign}(0) = 1$) and $|r| \le q = \lfloor\sqrt{|m|}\rfloor$.

Iterating this procedure, we obtain, for any given integer m, sequences of integers $\{a_i\}$ and $\{r_i\}$ defined by

$$r_0 = m,\ a_i = \langle\sqrt{|r_{i-1}|}\rangle,\ \varepsilon_i = \mathrm{sign}(r_{i-1}),\ r_{i-1} = \varepsilon_i a_i^2 + r_i\ (i \ge 1), \tag{4.1}$$

such that

$$|r_i| \le \lfloor\sqrt{|r_{i-1}|}\rfloor \quad (i \ge 1). \tag{4.2}$$

We then have for any $k \ge 1$ the representation

$$m = \sum_{i=1}^{k} \varepsilon_i a_i^2 + r_k. \tag{4.3}$$

In fact, for sufficiently large k we have the exact representation $m = \sum_{i=1}^{k} \varepsilon_i a_i^2$, since it is easily seen that the sequence $\{r_i\}$ must be eventually zero; however, in order to ensure that the numbers a_i are distinct, we need to work with the truncated version (4.3) in which the term r_k is not necessarily 0.

Assume now that $|m| = |r_0| > 37$. Then

$$a_1 = \langle\sqrt{|m|}\rangle \ge \langle\sqrt{37}\rangle \ge 6.$$

Moreover, if $i \ge 2$ and $a_i \ge 3$ then (4.2) and (4.1) imply that

$$3 \le a_i = \langle\sqrt{|r_{i-1}|}\rangle \le \langle|r_{i-2}|^{1/4}\rangle < \langle\sqrt{|r_{i-2}|}\rangle = a_{i-1},$$

since any real number x with $\langle x\rangle \ge 3$ must be at least equal to $5/2$ and hence satisfies $x < x^2 - 1$ and $\langle x\rangle < \langle x^2\rangle$. Therefore, defining k to be the maximal index such that $a_k \ge 6$, we have

$$a_1 > a_2 > \ldots > a_k \ge 6 > a_{k+1}.$$

Furthermore, by (4.1) we have $\langle\sqrt{|r_k|}\rangle = a_{k+1} \le 5$, so that $|r_k| \le (5 + 1/2)^2 < 36$. If $r_k = 0$, then (4.3) gives an admissible representation of m. Otherwise we have $0 < |r_k| < 36$ and we can therefore apply Lemma 4.1 to represent r_k in the form

$$r_k = \sum_{i=k+1}^{t} \varepsilon_i a_i^2, \qquad 5 \ge a_{k+1} > \ldots > a_t \ge 1.$$

Combining this representation with (4.3) we obtain again an admissible representation of m involving $t \le k + 5$ squares. In either case we obtain the inequality

(4.4) $$Q(m) \le \sum_{i=1}^{t} a_i \le \sum_{i=1}^{k} a_i + \sum_{i=1}^{5} i = \sum_{i=1}^{k} a_i + 15.$$

To bound the sum $\sum_{i=1}^{k} a_i$, we first observe that by (4.2) and induction we have for each $i \ge 1$,

$$|r_i| \le |r_0|^{2^{-i}} = |m|^{2^{-i}}.$$

Together with (4.1), this implies

(4.5) $$a_i = \langle \sqrt{|r_{i-1}|} \rangle \le |m|^{2^{-i}} + 1/2$$

and, in particular,

$$6 \le a_k \le |m|^{2^{-k}} + 1/2.$$

The last estimate implies

(4.6) $$k \le \frac{1}{\log 2} \mathcal{L}_{|m|},$$

which in view of the inequality $t \le k + 5$ shows that the representation constructed above satisfies the additional restriction (3.9) stated in part (iv) of the theorem. Moreover, (4.5) and (4.6) yield

$$\sum_{i=1}^{k} a_i \le \sum_{i=1}^{k} (|m|^{2^{-i}} + 1/2) \le f(\sqrt{|m|}) + O(\mathcal{L}_{|m|}).$$

In view of (4.4) this establishes the bound (3.7).

To prove the upper bound in (3.6), we observe that if $\sqrt{|m|} = a + \vartheta$ with $|\vartheta| \le 1/2$, then we have $a = \langle \sqrt{|m|} \rangle$, $|\vartheta| = \theta_{|m|}$ and

$$|r_1| = ||m| - a^2| = |(a+\vartheta)^2 - a^2| = 2a|\vartheta| + O(1) = 2\theta_{|m|}\sqrt{|m|} + O(1).$$

Using this estimate together with (4.4), (4.5), and (4.6), we obtain

$$\begin{aligned} Q(m) &\le \sum_{i=1}^{k} a_i + O(1) \le \sqrt{|r_0|} + \sqrt{|r_1|} + \sum_{i=3}^{k} (|m|^{2^{-i}} + 1/2) + O(1) \\ &= \sqrt{|m|} + \sqrt{2\theta_{|m|}}|m|^{1/4} + O(|m|^{1/8}), \end{aligned}$$

which is the desired estimate.

5. Proof of Theorem 3; lower bounds. We begin with a lemma which supplies the key step in the proof.

LEMMA 5.1. (i) *For any integer m, we have $Q(m) = Q(|m|) \ge \sqrt{|m|}$.*

(ii) *If m is a sufficiently large positive integer, then we have*

(5.1) $$Q(m) = \min\left\{q + Q(m - q^2), q + 1 + Q(m - (q+1)^2)\right\},$$

where $q = \lfloor \sqrt{|m|} \rfloor$.

Proof. (i) The identity $Q(m) = Q(|m|)$ follows immediately from the definition of $Q(m)$. The bound $Q(m) \geq \sqrt{|m|}$ holds trivially for $m = 0$, since $Q(0) = 0$. If $m \neq 0$, then any representation of the form

$$m = \sum_{i=1}^{t} \varepsilon_i a_i^2, \quad \varepsilon_i \in \{\pm 1\},\ a_1 > a_2 > \ldots > a_t \geq 1, \tag{5.2}$$

satisfies

$$\sum_{i=1}^{t} a_i \geq \Big(\sum_{i=1}^{t} a_i^2\Big)^{1/2} \geq \Big|\sum_{i=1}^{t} \varepsilon_i a_i^2\Big|^{1/2} = \sqrt{|m|}.$$

By the definition of $Q(m)$ this implies $Q(m) \geq \sqrt{|m|}$.

(ii) We first show that $Q(m)$ is bounded from below by the right-hand side of (5.1). Suppose that m is a positive integer and fix a representation of the form (5.2) such that $Q(m) = \sum_{i=1}^{t} a_i$. If $t = 1$ in (5.2), then $|m| = a_1^2 = q^2$, and (5.1) holds trivially. Assume therefore that $t \geq 2$. By (5.2), $\sum_{i=2}^{t} \varepsilon_i a_i^2$ is an admissible representation for the number $m - \varepsilon_1 a_1^2$, and we therefore have $Q(m - \varepsilon_1 a_1^2) \leq \sum_{i=2}^{t} a_i$. It follows that

$$Q(m) = a_1 + \sum_{i=2}^{t} a_i \geq a_1 + Q(m - \varepsilon_1 a_1^2). \tag{5.3}$$

Thus, to obtain the lower bound in (5.1), it suffices to show that $\varepsilon_1 = 1$ and $a_1 = q$ or $a_1 = q + 1$ whenever m is sufficiently large.

Suppose first that $a_1 \leq \sqrt{m/2}$. Then (5.2) implies

$$Q(m) = \sum_{i=1}^{t} a_i \geq \frac{1}{a_1} \sum_{i=1}^{t} a_i^2 \geq \frac{1}{a_1} \Big|\sum_{i=1}^{t} \varepsilon_i a_i^2\Big| = \frac{m}{a_1} \geq \sqrt{2m},$$

which contradicts the upper bound of (3.6) if m is sufficiently large. If $a_1 > \sqrt{m/2}$ and $\varepsilon_1 = -1$, then (5.3) and part (i) of the lemma give

$$Q(m) \geq a_1 + \sqrt{m + a_1^2} \geq \sqrt{m/2} + \sqrt{3m/2},$$

which again yields a contradiction to the upper bound of (3.6).

Finally, suppose that $a_1 > \sqrt{m/2}$, $\varepsilon_1 = 1$, but $a_1 \notin \{q, q+1\}$. In this case we obtain from (5.3) and part (i) of the lemma the bound

$$Q(m) \geq a_1 + \sqrt{|m - a_1^2|}. \tag{5.4}$$

Now, note that the function $x + \sqrt{|m - x^2|}$ is decreasing for $\sqrt{m/2} < x < \sqrt{m}$ and increasing for $x > \sqrt{m}$. Since $q \leq \sqrt{m} < q + 1$, it follows that over the ranges $\sqrt{m/2} < a_1 \leq q - 1$ and $a_1 \geq q + 2$ the right-hand side of (5.4) is minimal when $a_1 = q - 1$ or $a_1 = q + 2$, and in either case is bounded from below by

$$q-1+\min(\sqrt{m-(q-1)^2},\sqrt{(q+2)^2-m})$$
$$\geq q-1+\sqrt{m-(\sqrt{m}-1)^2}=\sqrt{m}+\sqrt{2}m^{1/4}+O(1).$$

Since this bound exceeds the upper bound (3.6) for large enough m, we conclude that for sufficiently large m, a_1 must be equal to either q or $q+1$, as we wanted to show.

To obtain the reverse inequality, it suffices to note that under the conditions $Q(m-q^2)<q$ and $Q(m-(q+1)^2)<q+1$ we obtain admissible representations of m by adding q^2 to any admissible representation of $m-q^2$ or by adding $(q+1)^2$ to any admissible representation of $m-(q+1)^2$ and therefore have $Q(m)\leq\min(q+Q(m-q^2),q+1+Q(m-(q+1)^2))$. In view of the inequalities $0\leq m-q^2\leq 2q$ and $0\leq(q+1)^2-m\leq 2q+1$ and the bound $Q(m)\ll\sqrt{|m|}$, the two conditions are satisfied provided m is sufficiently large.

Remark. The recurrence formula (5.1) could be used in principle to evaluate $Q(m)$ for any m to within an error term $O(1)$, but it is unlikely that it would lead to a simple explicit expression for $Q(m)$ or provide a simple algorithm for computing $Q(m)$ for any particular value of m *without the knowledge of the prior values of the function* Q. The reason for this is that it seems hard to decide *a priori*, which of the two terms on the right of the formula achieves the minimum; in particular, since the function $Q(m)$ is not monotonic, the minimum is not necessarily attained (or even approximately attained) at the term in which the argument of Q (i.e., $m-q^2$ or $m-(q+1)^2$) has smaller absolute value.

Proof of (3.6), lower bound. In view of part (i) of Lemma 5.1 we may assume that m is sufficiently large and positive. Writing $\theta=\theta_m=\|\sqrt{m}\|$ and $q=\lfloor\sqrt{m}\rfloor$, we have $\sqrt{m}=q+\theta$ if $q^2\leq m\leq q^2+q$, $\sqrt{m}=q+1-\theta$ if $q^2+q+1\leq m<(q+1)^2$, and in any case

$$\min(|m-q^2|,|m-(q+1)^2|)\geq 2q\theta+O(1).$$

Applying Lemma 5.1, we therefore obtain

$$Q(m)\geq q+\min(\sqrt{|m-q^2|},\sqrt{|m-(q+1)^2|})$$
$$\geq q+\sqrt{2q\theta+O(1)}\geq\sqrt{m}+\sqrt{2\theta}m^{1/4}+O(1),$$

which proves the lower bound of (3.6).

Proof of (3.8). We first note that the recurrence relation $m_k=m_{k-1}^2+m_{k-1}$ implies $\lfloor\sqrt{m_k}\rfloor=\lfloor\sqrt{m_k+1}\rfloor=m_{k-1}$. Thus, if $m=m_k$ or $m=m_k+1$, then we have, in the notation of Lemma 5.1, $q=m_{k-1}$. Moreover, the numbers $m-q^2$ and $m-(q+1)^2$ are equal to m_{k-1} and

$-(m_{k-1}+1)$, respectively, if $m = m_k$, and to $m_{k-1}+1$ and $-m_{k-1}$ if $m = m_k + 1$. Setting

$$Q_k = \min(Q(m_k), Q(m_k+1))$$

and noting that $Q(m) = Q(-m)$ we therefore obtain from (5.1) the inequality

$$Q_k \ge m_{k-1} + Q_{k-1}$$

for all sufficiently large k, say $k \ge k_0$. Iterating this inequality, we deduce

$$Q(m_k) \ge Q_k \ge \sum_{i=k_0-1}^{k-1} m_i + Q_{k_0-1} = \sum_{i=1}^{k-1} m_{k-i} + O(1) \tag{5.5}$$

for $k \ge k_0$.

To estimate the sum on the right of (5.5), we show by induction that for $0 \le i \le k$

$$m_{k-i} \le m_k^{2^{-i}} \le m_{k-i} + 1 - 2^{-i}. \tag{5.6}$$

For $i = 0$, (5.6) holds trivially. Assuming (5.6) holds for some $i \le k-1$, we deduce

$$m_k \ge m_{k-i}^{2^i} \ge (m_{k-i-1}^2)^{2^i} = m_{k-i-1}^{2^{i+1}}$$

and

$$\begin{aligned} m_k &\le (m_{k-i} + 1 - 2^{-i})^{2^i} = (m_{k-i-1}^2 + m_{k-i-1} + 1 - 2^{-i})^{2^i} \\ &\le (m_{k-i-1}^2 + 2(1 - 2^{-i-1})m_{k-i-1})^{2^i} < (m_{k-i-1} + 1 - 2^{-i-1})^{2^{i+1}}, \end{aligned}$$

which implies (5.6) for $i+1$ and completes the induction.

Applying first (5.6) with $i = k-1$ we obtain

$$2 = m_1 \le m_k^{2^{-k+1}} \le m_1 + 1 - 2^{-k+1} = 3 - 2^{-k+1},$$

which implies $k = \mathcal{L}_{m_k}/\log 2 + O(1) = t_{m_k} + O(1)$. Using this inequality and the upper bound of (5.6) we get

$$\begin{aligned} \sum_{i=1}^{k} m_{k-i} &\ge \sum_{i=1}^{k} (m_k^{2^{-i}} - 1) = \sum_{i=0}^{t_{m_k}} \sqrt{m_k}^{2^{-i}} - k + O(1) \\ &= f(\sqrt{m_k}) - \frac{1}{\log 2}\mathcal{L}_{m_k} + O(1), \end{aligned}$$

since by (5.6) the terms $m_k^{2^{-i}}$ with $i = k + O(1)$ are of order $O(1)$. Combined with (5.5), this gives the desired estimate.

6. Proof of Theorem 1; lower bounds. Recall that $R(s)$ is the largest integer r not expressible in the form (3.4) with integers h_i and k_i satisfying

(3.2) and (3.3). For $0 \le r_0 < 4s$ let $R(s, r_0)$ denote the largest such integer r that lies in the residue class r_0 modulo $4s$. Then clearly

$$R(s) = \max_{0 \le r_0 < 4s} R(s, r_0). \tag{6.1}$$

We shall obtain the lower bounds of Theorem 1 by considering $R(s, r_0)$ for suitable choices of r_0.

We begin with a lemma which gives a bound for $R(s, r_0)$ in terms of the function $Q(m)$ defined in Theorem 3.

Lemma 6.1. *We have*

$$R(s, r_0) \ge 2s \min\{Q(2s - d), Q(2s + d)\} + O(s), \tag{6.2}$$

where $|d| \le 2s$ *is chosen so that*

$$d \equiv \begin{cases} r_0 \bmod 4s & \text{if } r_0 \text{ is odd,} \\ 2s - r_0 \bmod 4s & \text{if } r_0 \text{ is even.} \end{cases} \tag{6.3}$$

Proof. It suffices to show that any integer $r \equiv r_0 \bmod 4s$ which has a representation of the form

$$r = 2s \sum_{i=1}^{t} (h_i + k_i) + \sum_{i=1}^{t} (k_i^2 - h_i^2) = 2s\Sigma_1 + \Sigma_2, \tag{6.4}$$

say, with integers h_i and k_i satisfying (3.2) and (3.3), is bounded from below by the right-hand side of (6.2).

We first observe that, by the upper bound $Q(m) \le \sqrt{|m|} + O(|m|^{1/4})$ of Theorem 3, the right-hand side of (6.2) is bounded from above by

$$2s \min(\sqrt{2s - d}, \sqrt{2s + d}) + O(s^{5/4}) \le 2s\sqrt{2s} + O(s^{5/4}).$$

Thus, if

$$r \ge 4s^{3/2} + O(s), \tag{6.5}$$

then r is bounded from below by the right-hand side of (6.2).

Next, note that under the conditions $0 \le h_i < s$ and $k_i > 0$, which are implied by (3.2) and (3.3), the right-hand side of (6.4) is an increasing function of each of the variables h_i and k_i. Hence, for any λ with $0 < \lambda \le 1$, (6.4) implies

$$\begin{aligned} r &\ge 2s \sum_{i=1}^{t} (\lambda h_i + \lambda k_i) + \sum_{i=1}^{t} ((\lambda k_i)^2 - (\lambda h_i)^2) \\ &\ge 2s\lambda\Sigma_1 + \lambda^2\Sigma_2 \ge 2s\lambda\sqrt{|\Sigma_2|} + \lambda^2\Sigma_2, \end{aligned}$$

since trivially

$$\Sigma_1^2 \ge \sum_{i=1}^{t} (h_i^2 + k_i^2) \ge |\Sigma_2|.$$

If now $|\Sigma_2| \geq 4s$, then choosing $\lambda = \sqrt{4s/|\Sigma_2|}$ we obtain $r \geq 4s^{3/2} - 4s$ and hence (6.5). Thus, it remains to consider the case when

$$|\Sigma_2| < 4s. \tag{6.6}$$

Observe that the sums Σ_1 and Σ_2 in (6.4) have the same parity, since $x \equiv \pm x^2 \bmod 2$ for any integer x. Hence, if $r \equiv r_0 \bmod 4s$ with r_0 even, (6.4) implies that both sums are even and that $r_0 \equiv \Sigma_2 \bmod 4s$. If r_0 is odd, both sums are odd, and in this case (6.4) yields $r_0 \equiv \Sigma_2 - 2s \bmod 4s$. In either case we have $|\Sigma_2| \equiv 2s + d$ or $|\Sigma_2| \equiv 2s - d$ with d given by (6.3). In view of (6.6), this implies

$$|\Sigma_2| \in \{2s \pm d\}. \tag{6.7}$$

The conditions (3.2) and (3.3) imply that in the representation $\Sigma_2 = \sum_{i=1}^{t}(k_i^2 - h_i^2)$ the numbers h_i are mutually distinct and non-negative and the numbers k_i are mutually distinct and positive, although the two sets of numbers are not necessarily disjoint. However, by dropping any pairs (h_i, k_j) with $h_i = k_j$ as well as 0 if it occurs among the numbers h_i and relabeling the remaining numbers h_i and k_i we obtain a representation of the form

$$\Sigma_2 = \sum_{i=1}^{t_1} k_i^2 - \sum_{i=1}^{t_2} h_i^2$$

in which the integers h_i and k_j are mutually distinct and strictly positive. The latter representation is an admissible representation in the definition of $Q(\Sigma_2)$, and we therefore have

$$Q(|\Sigma_2|) = Q(\Sigma_2) \leq \sum_{i=1}^{t_1} k_i + \sum_{i=1}^{t_2} h_i \leq \Sigma_1.$$

Combining this inequality with (6.7) and (6.4) yields the desired lower bound for r.

This completes the proof of the lemma.

Proof of (1.2), lower bound. By (6.1) and Lemma 6.1 we have

$$R(s) \geq 2s \max_{|d|\leq\sqrt{2s}} \min\{Q(2s-d), Q(2s+d)\} + O(s). \tag{6.8}$$

To bound the right-hand side, we use the bound of (3.6) of Theorem 3 together with the estimates

$$\sqrt{2s \pm d} = \sqrt{2s} \pm \frac{d}{2\sqrt{2s}} + O(s^{-1/2}) \quad (|d| \leq \sqrt{2s}), \tag{6.9}$$
$$(2s \pm d)^{1/4} = (2s)^{1/4} + O(s^{-1/4}) \quad (|d| \leq \sqrt{2s}).$$

We thus obtain for $|d| \leq \sqrt{2s}$,

$$\min(Q(2s-d), Q(2s+d)) \geq \sqrt{2s} + \sqrt{2\mu}(2s)^{1/4} + O(s^{1/8}), \tag{6.10}$$

where

$$\mu = \mu(s,d) = \min(\|\sqrt{2s+d}\|, \|\sqrt{2s-d}\|).$$

By (6.9) we have

$$\|\sqrt{2s \pm d}\| = \left\| \sqrt{2s} \pm \frac{d}{2\sqrt{2s}} \right\| + O(s^{-1/2})$$

and therefore

$$\max_{|d|\le\sqrt{2s}} \mu(s,d) = \max_{|\delta|\le 1/2} \min\{\|\delta+\sqrt{2s}\|, \|\delta-\sqrt{2s}\|\} + O(s^{-1/2}). \tag{6.11}$$

It is easy to see that the maximum on δ is attained either at $\delta = 0$ or at $\delta = 1/2$ and thus is equal to $\max(\|\sqrt{2s}\|, \|\sqrt{2s}-1/2\|) = \lambda_s^2/2$ by the definition of λ_s. It follows that the left-hand side of (6.11) is equal to $\lambda_s^2/2+O(s^{-1/2})$, which combined with (6.10) and (6.8) proves the lower bound of (1.2).

Proof of (1.4). We set $s_k = m_k/2$ for $k \ge 1$ with m_k defined as in part (iii) of Theorem 3. Clearly $s_1 = 1$ and $s_k = 2s_{k-1}^2 + 1$ for $k \ge 2$, so that s_k is an odd integer. Applying the bound of Lemma 6.1 with $r_0 = 2s_k$ (so that $d = 0$), together with the estimate (3.8) of Theorem 3, we obtain

$$\begin{aligned} R(s_k) &\ge R(s_k, 2s_k) \ge 2s_k Q(2s_k) + O(s_k) \\ &\ge 2s_k\{f(\sqrt{m_k}\,) + O(\mathcal{L}_{m_k})\} + O(s_k) = 2s_k\{f(\sqrt{2s_k}\,) + O(\mathcal{L}_{s_k})\}, \end{aligned}$$

which proves (1.4).

7. Proof of Theorem 1; upper bounds. To obtain the upper bounds (1.2) and (1.3) for $R(s)$, we need to show that if r is greater than the right-hand side of (1.2) or (1.3) then r is expressible in the form (3.4), i.e.,

$$r = 2s\sum_{i=1}^{t}(h_i + k_i) + \sum_{i=1}^{t}(k_i^2 - h_i^2), \tag{7.1}$$

with integers h_i and k_i satisfying (3.2) and (3.3). In fact, it will be convenient to also consider such representations with (3.2) and (3.3) replaced by the slightly stronger conditions

$$1 \le h_i \le s-1, \qquad h_i \text{ distinct}, \tag{7.2}$$

$$1 \le k_i \le s-1, \qquad k_i \text{ distinct}, \tag{7.3}$$

which have the advantage of being symmetric in h_i and k_i. We denote by $\mathcal{R}_t(s)$ the set of integers r expressible in the form (3.2)–(3.4), and by $\mathcal{R}_t^*(s)$ the set of integers expressible in the form (7.1)–(7.3). Needless to say, empty sums are to be interpreted as zero, so that $\mathcal{R}_0(s) = \mathcal{R}_0^*(s) = \{0\}$. We further set $\mathcal{R}(s) = \bigcup_{t\ge0}\mathcal{R}_t(s)$, $\mathcal{R}^*(s) = \bigcup_{t\ge0}\mathcal{R}_t^*(s)$, and for any residue class $r_0 \bmod 4s$ we put

$$\mathcal{R}_t(s, r_0) = \{r \in \mathcal{R}_t(s) : r \equiv r_0 \bmod 4s\},$$

and define $\mathcal{R}_t^*(s, r_0)$, $\mathcal{R}(s, r_0)$, and $\mathcal{R}^*(s, r_0)$ analogously. Note that $\mathcal{R}^*(s) \subset \mathcal{R}(s)$.

The following three propositions contain the key steps of the proof and will be proved in turn in the remainder of this section. The second and third of these propositions will be used again in Section 9 to obtain an explicit numerical bound.

Proposition 7.1. *For any residue class* $r_0 \bmod 4s$ *there exists a non-negative integer* $r \in \mathcal{R}_t^*(s, r_0)$ *for some* $t \ll \mathcal{L}_s$ *satisfying*

$$r \le 2s\{\sqrt{2s} + \lambda_s (2s)^{1/4} + O(s^{1/8})\}, \tag{7.4}$$

$$r \le 2s\{f(\sqrt{2s}) + O(\mathcal{L}_s^2)\}. \tag{7.5}$$

Proposition 7.2. *If* $s \ge 150$ *and* $r \in \mathcal{R}_t^*(s)$ *for some* $t \le s/25$, *then* $r + 4sq \in \mathcal{R}^*(s)$ *for every* q *satisfying*

$$4t + 3 \le q \le \lfloor (s+5)/6 \rfloor s. \tag{7.6}$$

Proposition 7.3. *Suppose that* $s \ge 50$ *and that* $\mathcal{R}^*(s-1)$ *contains every integer in the interval* $[(s-1)^3/6, (s-1)^3/2]$. *Then* $\mathcal{R}(s)$ *contains every integer* $\ge 2s^3/3$.

Proof of Theorem 1; upper bounds. We may clearly assume that s is sufficiently large. The first two propositions imply that $\mathcal{R}^*(s)$, and hence also $\mathcal{R}(s)$, contains every integer r in the ranges

$$2s\{\sqrt{2s} + \lambda_s (2s)^{1/4} + c_1 s^{1/8}\} \le r \le 4\lfloor (s+5)/6 \rfloor s^2, \tag{7.7}$$

$$2s\{f(\sqrt{2s}) + c_2 \mathcal{L}_s^2\} \le r \le 4\lfloor (s+5)/6 \rfloor s^2, \tag{7.8}$$

provided c_1 and c_2 are sufficiently large absolute constants. Since for large s the ranges (7.7) and (7.8) contain the interval $[s^3/6, 2s^3/3]$, it follows by the third proposition that, if s is sufficiently large, then $\mathcal{R}(s)$ also contains every integer $\ge 2s^3/3$. Therefore, $R(s) = \max\{r : r \notin \mathcal{R}(s)\}$ is bounded by the left-hand sides of (7.7) and (7.8), and we obtain the upper bounds of (1.2) and (1.3).

Proof of Proposition 7.1. In the case $r_0 \equiv 0 \bmod 4s$, $r = 0$ belongs to $\mathcal{R}_0^*(s, 0)$ and (7.4) and (7.5) are trivially satisfied. We can therefore assume that $r_0 \not\equiv 0 \bmod 4s$.

As a first step, we show that for sufficiently large s and every integer m with $0 < m < 4s$ there exist integers h_i and k_i $(1 \le i \le t)$ satisfying (7.2) and (7.3) with

$$t \ll \mathcal{L}_m, \tag{7.9}$$

such that

$$m = \sum_{i=1}^{t} (k_i^2 - h_i^2) \tag{7.10}$$

and

$$\sum_{i=1}^{t} (h_i + k_i) \le \begin{cases} \sqrt{m} + \sqrt{2\theta_m} m^{1/4} + O(m^{1/8}), \\ f(\sqrt{m}) + O(\mathcal{L}_m^2), \end{cases} \tag{7.11}$$

where θ_m is defined as in Theorem 3.

An application of Theorem 3 yields a representation

$$m = \sum_{i=1}^{t_1} h_i^2 - \sum_{i=1}^{t_2} k_i^2 \tag{7.12}$$

with distinct positive integers h_i, $1 \le i \le t_1$, and k_i, $1 \le i \le t_2$, whose sum is bounded by the right-hand side of (7.11) and such that

$$t_1 + t_2 \le C\mathcal{L}_m, \tag{7.13}$$

where C is the constant in (3.9). The bound (7.11) implies that the integers h_i and k_i are bounded by $\ll \sqrt{m} < \sqrt{4s}$, and hence are $\le s - 1$ if s is sufficiently large. The conditions (7.2) and (7.3) are therefore satisfied for these integers, and if $t_1 = t_2$ then (7.9)–(7.11) follow immediately with $t = t_1 = t_2$.

If $t_1 \ne t_2$, we will obtain (7.9)–(7.11) by suitably enlarging the sets $\{h_i\}$ and $\{k_i\}$ to two sets having the same cardinality t, while leaving the value of $\sum_i h_i^2 - \sum_i k_i^2$ unchanged. Without loss of generality, assume that $t_1 > t_2$ and set

$$l = t_1 - t_2, \quad t = t_1 + l = t_2 + 2l.$$

By (7.13) we have $t \le t_1 + l \le 2t_1 \le 2C\mathcal{L}_m$, so that (7.9) is satisfied. We define additional integers h_i and k_i by setting

$$h_{t_1+i} = 5a_i, \quad k_{t_2+i} = 3a_i, \quad k_{t_2+l+i} = 4a_i \quad (1 \le i \le l) \tag{7.14}$$

with distinct positive integers a_i to be chosen later. This definition ensures that

$$\sum_{i=1}^{t} (k_i^2 - h_i^2) = \sum_{i=1}^{t_1} k_i^2 - \sum_{i=1}^{t_2} h_i^2,$$

which in view of (7.12) yields (7.10). Moreover, if we restrict the integers a_i to the residue class 1 modulo 3, then the sets $\{3a_i\}$, $\{4a_i\}$, and $\{5a_i\}$ are pairwise disjoint, and the numbers defined in (7.14) are therefore mutually distinct positive integers. Thus, in order to satisfy the conditions (7.2) and (7.3), it remains to ensure that these numbers are distinct from the numbers h_i, $1 \le i \le t_1$, and k_i, $1 \le i \le t_2$, and are bounded by $s - 1$.

We consider the set of positive integers $a \le 12C\mathcal{L}_m + 3$, where C is the constant in (7.13). Clearly, at least $4C\mathcal{L}_m$ of these integers satisfy the congruence $a \equiv 1 \bmod 3$, and at most $3(t_1+t_2)$ integers can be of the form λh_i, $1 \le i \le t_1$, or λk_i, $1 \le i \le t_2$, with $\lambda = 1/3$, $1/4$, or $1/5$. Since by (7.13), $4C\mathcal{L}_m - 3(t_1+t_2) \ge t_1+t_2 \ge l$, there exist l of these integers, say $a_1, \ldots, a_l$, with $a_i \equiv 1 \bmod 3$, such that none of the integers (7.14) is equal to one of the numbers h_i, $1 \le i \le t_1$, or k_i, $1 \le i \le t_2$. Moreover, since $l \le t_1 \le C\mathcal{L}_m$ and $a_i \le 12C\mathcal{L}_m + 3$, the integers in (7.14) are bounded by $\ll \mathcal{L}_m \le \mathcal{L}_{4s}$ (and thus are $\le s-1$ for large enough s), and we have

$$\sum_{i=t_1+1}^{t} h_i + \sum_{i=t_2+1}^{t} k_i \ll \sum_{i=1}^{l} a_i \ll \mathcal{L}_m^2.$$

Thus, extending the summation in $\sum_{i=1}^{t_1} h_i$ and $\sum_{i=1}^{t_2} k_i$ to the full range $1 \le i \le t$ increases the two sums by at most $O(\mathcal{L}_m^2)$, and therefore does not affect the upper bound (7.11). Hence (7.9)–(7.11) hold in any case.

Now, let $r_0 \bmod 4s$ be a given non-zero residue class and define $|d| < 2s$ by the congruence

$$d \equiv \begin{cases} r_0 \bmod 4s & (r_0 \text{ odd}), \\ 2s + r_0 & (r_0 \text{ even}). \end{cases} \tag{7.15}$$

We apply the above construction with $m = m_\pm = 2s \pm d$ to obtain integers $h_i^\pm$ and $k_i^\pm$ $(1 \le i \le t_\pm)$ satisfying (7.2), (7.3), and (7.9)–(7.11), and set for $\varepsilon = \pm$

$$r_\varepsilon = 2s\Sigma_\varepsilon + \varepsilon m_\varepsilon, \tag{7.16}$$

where $\Sigma_\varepsilon = \sum_{i=1}^{t_\varepsilon}(h_i^\varepsilon + k_i^\varepsilon)$. We shall show that at least one of the integers $r_\pm$ has the properties claimed in the proposition.

First note that the numbers $r_\pm$ are both non-negative, since $0 < m_\pm < 4s$ and $\Sigma_\pm \ge 2$. Also, both numbers lie in the residue class $r_0 \bmod 4s$, since by (7.10), $\Sigma_\varepsilon \equiv m_\varepsilon \equiv d \bmod 2$ and therefore

$$r_\varepsilon \equiv 2sd + \varepsilon(2s + \varepsilon d) \equiv 2s(d+1) + d \equiv r_0 \bmod 4s.$$

Moreover, by (7.16) and (7.10), r_+ has a representation of the required form (7.1) with $t_+ \ll \mathcal{L}_s$ terms, and interchanging the roles of h_i^- and k_i^- in (7.16) shows that the same is true for r_-. Therefore, we have $r_\varepsilon \in \mathcal{R}^*_{t_\varepsilon}(s, r_0)$ with $t_\varepsilon \ll \mathcal{L}_s$, and it remains to show that at least one of the integers $r_\pm$ is bounded by the right-hand sides of (7.4) and (7.5).

By (7.11) and (7.16) we have

$$r_\varepsilon \le \begin{cases} 2s\{M_\varepsilon(d) + O(s^{1/8})\}, \\ 2s\{f(\sqrt{2s+\varepsilon d}) + O(\mathcal{L}_s^2)\}, \end{cases} \tag{7.17}$$

where

$$M_\varepsilon(d) = \sqrt{2s+\varepsilon d} + \sqrt{2\theta_{2s+\varepsilon d}}\,(2s+\varepsilon d)^{1/4}.$$

The second estimate in (7.17) together with the monotonicity of the function $f(x)$ immediately gives the upper bound

$$\min(r_+, r_-) \le 2s\{f(\sqrt{2s}) + O(\mathcal{L}_s^2)\},$$

and hence the estimate (7.5) for one of the integers $r = r_\pm$.

The proof of (7.4) is more involved. By (7.17) it suffices to show that for any d with $|d| < 2s$,

$$\min\{M_+(d), M_-(d)\} \le \sqrt{2s} + \lambda_s(2s)^{1/4} + O(s^{1/8}). \tag{7.18}$$

To prove this estimate, we may clearly assume that $d \ge 0$. If $d > (2s)^{3/4}$, then we have

$$\sqrt{2s-d} \le \sqrt{2s} - \frac{d}{2\sqrt{2s}} \le \sqrt{2s} - \tfrac{1}{2}(2s)^{1/4},$$

and therefore

$$M_-(d) \le \sqrt{2s} + \tfrac{1}{2}(2s)^{1/4},$$

which implies (7.18) since $\lambda_s \ge 1/\sqrt{2}$ for all s. Thus it remains to consider the case when $0 \le d \le (2s)^{3/4}$. Setting

$$\delta = d(2s)^{-3/4}, \qquad \mu = \delta(2s)^{1/4} = d(2s)^{-1/2},$$

we have $0 \le \delta \le 1$ and hence obtain by Taylor's formula

$$\begin{aligned}\sqrt{2s+\varepsilon d} &= \sqrt{2s} + \frac{\varepsilon d}{2\sqrt{2s}} - \frac{d^2}{8(2s)^{3/2}} + O(s^{-1/4})\\ &= \sqrt{2s} + \varepsilon\mu/2 - \delta^2/8 + O(s^{-1/4})\end{aligned}$$

and

$$(2s+\varepsilon d)^{1/4} = (2s)^{1/4} + O(1).$$

Thus,

$$M_\varepsilon(d) = \sqrt{2s} + (2s)^{1/4}\{\varepsilon\delta/2 + \sqrt{2\|\sqrt{2s}+\varepsilon\mu/2-\delta^2/8\|}\} + O(s^{1/8}),$$

and to prove (7.18) it suffices to show that the coefficient of $(2s)^{1/4}$ here is at most λ_s for at least one of the choices of $\varepsilon = \pm$. This is a consequence of the following lemma.

LEMMA 7.4. *For $\varepsilon = \pm$ and real numbers θ, δ, and μ, let*

$$\lambda_\varepsilon(\theta,\delta,\mu) = \varepsilon\delta/2 + \sqrt{2\|\theta+\varepsilon\mu/2-\delta^2/8\|}$$

and put

$$\lambda(\theta,\delta,\mu) = \min\{\lambda_+(\theta,\delta,\mu), \lambda_-(\theta,\delta,\mu)\}.$$

Then

$$\max_{\mu\in\mathbb{R},\delta\ge0}\lambda(\theta,\delta,\mu)=\sqrt{2\max(\|\theta\|,\|\theta+1/2\|)}.$$

Proof. Clearly

$$\max_{\mu\in\mathbb{R},\delta\ge0}\lambda(\theta,\delta,\mu)\ge\max(\lambda(\theta,0,0),\lambda(\theta,0,1))=\sqrt{2\max(\|\theta\|,\|\theta+1/2\|)}.$$

To obtain the inequality in the reverse direction, write

$$\eta_\varepsilon=\eta_\varepsilon(\theta,\delta,\mu)=\sqrt{2\|\theta+\varepsilon\mu/2-\delta^2/8\|},$$

so that

$$\lambda(\theta,\delta,\mu)=\min\{\delta/2+\eta_+,-\delta/2+\eta_-\}.$$

We begin by considering $\eta_+^2+\eta_-^2$. Clearly

$$\eta_+^2+\eta_-^2=2(\|\theta_\delta+\mu/2\|+\|\theta_\delta-\mu/2\|),$$

where $\theta_\delta=\theta-\delta^2/8$. The right-hand expression is maximal as a function of μ when the two terms $\|\theta_\delta+\mu/2\|$ and $\|\theta_\delta-\mu/2\|$ are equal, which is the case if and only if μ is an integer. Thus, for all real μ we have

$$\eta_+^2(\theta,\delta,\mu)+\eta_-^2(\theta,\delta,\mu)\le4\max(\|\theta_\delta\|,\|\theta_\delta-1/2\|)=\varrho^2,$$

say, where $\varrho=\varrho(\theta,\delta)$ satisfies $0\le\varrho\le\sqrt2$. It follows that $\eta_+\le\sqrt{\varrho^2-\eta_-^2}$, and taking the maximum over all values of η_- in the range $0\le\eta_-\le\varrho$, we see that

$$\lambda(\theta,\delta,\mu)\le\max_{0\le v\le\varrho}\min(\delta/2+\sqrt{\varrho^2-v^2},-\delta/2+v).$$

If $\delta\ge\varrho$, then for any v in the interval $[0,\varrho]$ we have

$$v-\delta/2\le\varrho-\delta/2\le\delta/2\le\delta/2+\sqrt{\varrho^2-v^2},$$

so that the maximum over v occurs at $v=\varrho$ and

$$\lambda(\theta,\delta,\mu)=\varrho-\delta/2\le\varrho/2\le1/\sqrt2\le\sqrt{2\max(\|\theta\|,\|\theta+1/2\|)}.$$

If $\delta<\varrho$, the maximum occurs when

$$\delta/2+\sqrt{\varrho^2-v^2}=-\delta/2+v,$$

i.e., when $v=v_\pm=\delta/2\pm\sqrt{(\varrho^2-\delta^2/2)/2}$. Since $v_-<0<v_+\le\varrho$ for $\delta<\varrho$, the maximum over $0\le v\le\varrho$ is attained at $v=v_+$ and is equal to $-\delta/2+v_+=\sqrt{(\varrho^2-\delta^2/2)/2}$. Since

$$\varrho^2/2=2\max(\|\theta-\delta^2/8\|,\|\theta+1/2-\delta^2/8\|)\le2\max(\|\theta\|,\|\theta+1/2\|)+\delta^2/4,$$

we obtain

$$\lambda(\theta,\delta,\mu)\le\sqrt{\varrho^2/2-\delta^2/4}\le\sqrt{2\max(\|\theta\|,\|\theta+1/2\|)}.$$

Thus Lemma 7.4 is proved, and the proof of Proposition 7.1 is complete.

Proof of Proposition 7.2. Let $u = \lceil q/s \rceil$ so that $(u-1)s < q \le us$. The bound $1 \le q \le \lfloor (s+5)/6 \rfloor s$ implies $1 \le u \le (s+5)/6$. We shall use the identity (cf. [PS, Problem VIII.9])

$$q = \sum_{i=1}^{u} q_i, \qquad q_i = \lfloor (q+i-1)/u \rfloor.$$

Since $q_u < q/u + 1 \le s + 1$ and $q_1 \ge q/u - 1 > (1 - 1/u)s - 1$, we have

$$\left(1 - \frac{1}{u}\right)s - 1 < q_1 \le q_2 \le \ldots \le q_u \le s.$$

We seek to express $r + 4sq$ in the form (7.1) with t replaced by $t + 2u$. For $i = 1, \ldots, u$ we take

$$h_{t+2i-1} = k_{t+2i-1} = m_i, \qquad h_{t+2i} = k_{t+2i} = q_i - m_i$$

for some m_i satisfying $1 \le m_i \le q_i - 1$ and $m_i \ne q_i/2$. In order to ensure that the numbers $h_1, \ldots, h_{t+2u}$ are distinct and the numbers $k_1, \ldots, k_{t+2u}$ are distinct, we choose $m_1, \ldots, m_u$ in succession so that $1 \le m_i \le q_i - 1$, $m_i \ne q_i/2$, and both m_i and $q_i - m_i$ are distinct from the $2t + 2(i-1)$ values $h_1, \ldots, h_t$, $k_1, \ldots, k_t$, $m_1, \ldots, m_{i-1}$, $q_1 - m_1, \ldots, q_{i-1} - m_{i-1}$. A suitable choice of m_i is possible, provided

$$q_i - 2 > 4t + 4(i-1) \qquad (1 \le i \le u). \tag{7.19}$$

We are going to show that, under the hypotheses of the proposition, this condition is always satisfied.

Suppose first that $u = 1$, i.e., $4t + 3 \le q \le s$. Then the assumption $q \ge 4t + 3$ guarantees that $q - 2 > 4t$, so that (7.19) holds.

Next, suppose that $2 \le u < s/15$. In view of the hypothesis $t \le s/25$ we then have

$$4t + 4(i-1) \le 4t - 4 + 4u < 4s/25 + 4s/15 < 4s/9$$

and

$$q_i - 2 > (1 - 1/u)s - 3 \ge s/2 - 3 > 4s/9$$

for $i = 1, \ldots, u$, which gives again (7.19).

Finally, suppose that $s/15 \le u \le (s+5)/6$. Since by hypothesis $s \ge 150$, we have $u \ge 10$. Thus, in this case

$$q_i - 2 > (1 - 1/u)s - 3 \ge 9s/10 - 3 > 5s/6$$

and

$$4t + 4(i-1) \le 4t + 4u - 4 < 4s/25 + 4s/6 < 5s/6,$$

and (7.19) follows.

With $m_1,\ldots,m_u$ chosen as above, we have

$$\begin{aligned} r+4sq &= 2s\sum_{i=1}^{t}(h_i+k_i)+\sum_{i=1}^{t}(k_i^2-h_i^2)+4s\sum_{i=1}^{u}q_i \\ &= 2s\sum_{i=1}^{t+2u}(h_i+k_i)+\sum_{i=1}^{t+2u}(k_i^2-h_i^2), \end{aligned}$$

so that $r+4sq\in\mathcal{R}^*(s)$ as asserted.

Proof of Proposition 7.3. Suppose $s\ge 50$ and that every integer in the interval $[(s-1)^3/6,(s-1)^3/2]$ belongs to $\mathcal{R}^*(s-1)$. Let $r\ge 2s^3/3$ be given and set $n=r+P(s)$. If $n\ge s^5$ then $n>N(s)$ by Theorem 2 and therefore $r>R(s)$, i.e., $r\in\mathcal{R}(s)$. We may therefore assume that $P(s)+2s^3/3\le n<s^5$. Now choose a positive integer a so that $n_1=n-a^2$ satisfies

$$P(s-1)+(s-1)^3/6\le n_1\le P(s-1)+(s-1)^3/2. \tag{7.20}$$

This is possible, since the maximum difference between consecutive squares less than n is less than $2\sqrt{n}<2s^{5/2}<(s-1)^3/3$ for $s\ge 50$. Moreover, the bounds on n and n_1 imply that

$$a^2=n-n_1\ge P(s)+2s^3/3-(P(s-1)+(s-1)^3/2)>s^3/6>(2s)^2.$$

By (7.20) we have $n_1-P(s-1)\in[(s-1)^3/6,(s-1)^3/2]$ and hence $n_1-P(s-1)\in\mathcal{R}^*(s-1)$. By the definition of $\mathcal{R}^*(s-1)$ (see (3.1), (3.4), (7.2) and (7.3)) this means that n_1 is expressible as a sum of $s-1$ squares of distinct positive integers a_i, $i=1,\ldots,s-1$, which satisfy either $1\le a_i\le s-1$ or $1\le a_i-(s-1)\le s-1$ and thus in any case are bounded by $2(s-1)$. Since $a>2s$, $n=n_1+a^2$ is a sum of s distinct non-zero squares, i.e., $r=n-P(s)$ belongs to the set $\mathcal{R}(s)$. This proves Proposition 7.3.

8. An explicit upper bound for $N(s)$. In this section we will prove the following result, which gives an explicit upper bound for $N(s)$ for $s\ge 166$. While this bound is weaker asymptotically than the bounds of Theorem 1, such a specific upper bound is needed in order to show that $N(s)$ is strictly increasing for $s\ge 7$ and in proving the "redundancy of coprimality" in the next section. It is also useful for computing the values of $N(s)$, as it substantially reduces the number of cases that have to be checked in determining $N(s)$.

THEOREM 4. *For $s\ge 166$ we have*

$$N(s)<P(s)+2s\sqrt{2s}+44s^{5/4}+108s.$$

COROLLARY 1. *For $s\ge 166$ we have $N(s)<1.033P(s)$.*

Proof. If $s \geq 166$, then

$$\begin{aligned}2s\sqrt{2s} + 44s^{5/4} + 108s &\leq s^3\{2\sqrt{2} \cdot 166^{-3/2} + 44 \cdot 166^{-7/4} + 108 \cdot 166^{-2}\} \\ &< 0.011s^3 < 0.033P(s).\end{aligned}$$

The result now follows from Theorem 4.

COROLLARY 2. *If* $s \geq 7$, *then* $N(s) < N(s+1)$.

Proof. For $s \geq 360$, Theorem 4 gives

$$\begin{aligned}N(s) &\leq P(s) + s^2\{2\sqrt{2} \cdot 360^{-1/2} + 44 \cdot 360^{-3/4} + 108 \cdot 360^{-1}\} \\ &< P(s) + s^2 < P(s+1) < N(s+1).\end{aligned}$$

For the range $7 \leq s \leq 359$, the monotonicity of $N(s)$ follows from the table in Section 11 (which also shows that the inequality $N(s) < N(s+1)$ fails at $s = 6$).

To prove Theorem 4, we shall use Propositions 7.2 and 7.3, as well as the following explicit version of Proposition 7.1.

PROPOSITION 8.1. *If* $s \geq 165$, *then for any residue class* r_0 *modulo* $4s$ *there exists a positive integer* $r \in \mathcal{R}_t^*(s, r_0)$ *for some* $t \leq 6$ *satisfying*

$$r \leq 2s\sqrt{2s} + 44s^{5/4}. \tag{8.1}$$

Proof. We will show that for any integer m with $|m| \leq 2s$ there exist positive integers h_i and k_i $(1 \leq i \leq t)$ with $t = 5$ or $t = 6$ satisfying (7.2) and (7.3), such that

$$\sum_{i=1}^{t}(h_i + k_i) \leq \sqrt{2s} + 21s^{1/4} \tag{8.2}$$

and

$$\sum_{i=1}^{t}(k_i^2 - h_i^2) = m. \tag{8.3}$$

The integer

$$r = 2s\sum_{i=1}^{t}(h_i + k_i) + \sum_{i=1}^{t}(k_i^2 - h_i^2)$$

then belongs to $\mathcal{R}_t^*(s)$ and satisfies (8.1). Moreover, if $r_0 \bmod 4s$ is a given residue class, then choosing m so that $m \equiv r_0 \bmod 4s$ if r_0 is even and $m \equiv r_0 + 2s \bmod 4s$ if r_0 is odd, we have $r \equiv r_0 \bmod 4s$ and therefore $r \in \mathcal{R}_t^*(s, r_0)$. Thus it remains to prove the above claim.

By interchanging the roles of h_i and k_i, we see that it suffices to consider the case when $0 \leq m \leq 2s$.

Suppose first that $0 \le m \le 25\sqrt{s}$. We then take $h_1 = 4$ and $h_i = i + 4$ for $i = 2, 3, 4, 5$. The integers h_i clearly satisfy (7.2) if $s \ge 10$. Moreover, since by Theorem 0

$$m + \sum_{i=1}^{5} h_i^2 \ge \sum_{i=1}^{5} h_i^2 = 246 > N^*(5),$$

we may choose distinct positive integers $k_1, \ldots, k_5$ such that

$$\sum_{i=1}^{5} k_i^2 = m + \sum_{i=1}^{5} h_i^2.$$

Our assumptions $m \le 25\sqrt{s}$ and $s \ge 165$ imply

$$\sum_{i=1}^{5} k_i^2 \le 25\sqrt{s} + 246 \le \sqrt{s}\{25 + 246 \cdot 165^{-1/2}\} < 45\sqrt{s},$$

so that $k_1, \ldots, k_5$ are positive integers less than $\sqrt{45}s^{1/4} < s$ and therefore satisfy (7.3). Moreover,

$$\begin{aligned}\sum_{i=1}^{5}(h_i + k_i) &\le 4 + \sum_{i=2}^{5}(i+4) + \sqrt{5\sum_{i=1}^{5} k_i^2}\\ &\le 34 + \sqrt{5 \cdot 45\sqrt{s}} = 34 + 15s^{1/4},\end{aligned}$$

which implies the bound (8.2) with $t = 5$.

Now suppose that $25\sqrt{s} < m \le 2s$. In this case we take $h_1 = 1$ and $k_1 = \lfloor \sqrt{m} \rfloor$, so that

$$(\sqrt{m} - 1)^2 = m - 2\sqrt{m} + 1 < k_1^2 \le m \le 2s,$$

and, in particular, $k_1 \le \sqrt{2s} < s$. Setting $d = m - (k_1^2 - h_1^2) = m + 1 - k_1^2$, we have

$$1 \le d < 2\sqrt{m} \le 2\sqrt{2s}.$$

The assumptions $m > 25\sqrt{s}$ and $s \ge 165$ give

$$k_1^2 > m - 2\sqrt{m} = m\left(1 - \frac{2}{\sqrt{m}}\right) > 25\sqrt{s}\left(1 - \frac{2}{5 \cdot 165^{1/4}}\right) > 22\sqrt{s}. \tag{8.4}$$

Next, we take $h_2 = 4$ and $h_i = 3 + i$ for $3 \le i \le 6$, so that

$$\sum_{i=2}^{6} h_i = 34, \qquad \sum_{i=2}^{6} h_i^2 = 246.$$

Applying again Theorem 0, we obtain distinct positive integers $k_2, \ldots, k_6$ such that

$$\sum_{i=2}^{6} k_i^2 = d + \sum_{i=2}^{6} h_i^2,$$

that is

$$\sum_{i=1}^{6} k_i^2 = m + \sum_{i=1}^{6} h_i^2.$$

Clearly,

$$\sum_{i=2}^{6} k_i^2 \le 2\sqrt{2s} + 246 \le \sqrt{s}\{2\sqrt{2} + 246 \cdot 165^{-1/2}\} < 22\sqrt{s},$$

which by (8.4) implies that the integers $k_2, \ldots, k_6$ are less than k_1 and hence also less than s. The integers h_i and k_i therefore satisfy (7.2) and (7.3). Moreover, we have

$$\sum_{i=1}^{6}(h_i + k_i) = k_1 + \sum_{i=2}^{6} k_i + 35 \le k_1 + \sqrt{5\sum_{i=2}^{6} k_i^2} + 35$$
$$\le \sqrt{m} + \sqrt{5 \cdot 22\sqrt{s}} + 35 \le \sqrt{2s} + s^{1/4}\{\sqrt{110} + 35 \cdot 165^{-1/4}\},$$

which again gives (8.2).

This completes the proof of Proposition 8.1.

Proof of Theorem 4. First suppose that $s \ge 165$. By Proposition 8.1, for any residue class r_0 mod $4s$ there exists an integer $r \le 2s\sqrt{2s}+44s^{5/4}$ which belongs to $\mathcal{R}_t^*(s, r_0)$ for some $t \le 6$. By Proposition 7.2, it follows that $r + 4sq \in \mathcal{R}^*(s)$ for any q satisfying

$$4 \cdot 6 + 3 \le q \le \lfloor (s+5)/6 \rfloor s.$$

Since $r + 4\lfloor (s+5)/6 \rfloor s^2 \ge 2s^3/3$ and

$$r + (4 \cdot 6 + 3)4s \le 2s\sqrt{2s} + 44s^{5/4} + 108s,$$

we conclude that every integer in the interval $[2s\sqrt{2s} + 44s^{5/4} + 108s, 2s^3/3]$ belongs to $\mathcal{R}^*(s)$. Furthermore, since for $s \ge 165$,

$$2s\sqrt{2s}+44s^{5/4}+108s \le s^3\{2\sqrt{2}\cdot 165^{-3/2}+44\cdot 165^{-7/4}+108\cdot 165^{-2}\} < s^3/6,$$

this interval contains the interval $[s^3/6, 2s^3/3]$ and we can apply Proposition 7.3 to deduce that for $s \ge 165+1 = 166$, $\mathcal{R}(s)$ contains every integer $\ge 2s^3/3$. Hence, for $s \ge 166$, we have

$$R(s) = \max\{r : r \notin \mathcal{R}(s)\} < 2s\sqrt{2s} + 44s^{5/4} + 108s,$$

as claimed.

9. Redundancy of coprimality. We have stated and proved our main results in terms of the function $N(s)$, whereas Halter-Koch stated his results (as quoted in Theorem 0) in terms of the function $N^*(s)$. (Recall that $N^*(s)$ is defined like $N(s)$, except that only representations by sums of coprime squares are to be considered.) In this section we show that the two functions are identical. In fact, we prove the following more precise result.

THEOREM 5. *If $s \geq 5$ and if n is expressible as a sum of s distinct non-zero squares, then n is also expressible as a sum of s distinct non-zero squares having no non-trivial common factor.*

Remark. The same result holds for $s = 4$ if we restrict attention to the positive integers not divisible by 8. It also holds for $s = 3$ if we restrict attention to the positive integers not divisible by 4 (cf. [Ka], Satz 9).

Proof of Theorem 5. For $s = 5$ the assertion of the theorem follows easily from Halter-Koch's result that $N^*(5) = 245$ (see Theorem 0). For, since $2^2 + 4^2 + 6^2 + 8^2 + 12^2 > 245$, the only integer not exceeding 245 which is expressible as a sum of 5 distinct non-zero squares having a non-trivial common factor is $220 = 2^2 + 4^2 + 6^2 + 8^2 + 10^2$, which has also the coprime representation $220 = 1^2 + 3^2 + 5^2 + 8^2 + 11^2$.

Theorem 0 also shows that $N^*(s) < 4P(s)$ for $6 \leq s \leq 12$. Thus every integer $\geq 4P(s) = \sum_{i=1}^{s}(2i)^2$ is expressible as a sum of s distinct non-zero squares having no non-trivial common factor. If an integer less than $4P(s)$ is expressible as a sum of s distinct non-zero squares, these squares necessarily have g.c.d. 1. Indeed, otherwise the common factor of these squares would be at least 2^2, and dividing each term by this factor would yield a representation of an integer less than $P(s) = \sum_{i=1}^{s} i^2$ as a sum of s distinct squares, which is impossible. Thus the assertion of the theorem holds for $6 \leq s \leq 12$.

Now suppose that $s > 12$. As before, if $n < 4P(s)$ and if n is expressible as a sum of s distinct non-zero squares, then these squares necessarily have g.c.d. 1. On the other hand, if $n > 3(3 + \sqrt{N(s-2) + 14})^2$, we claim that n is always expressible as a sum of s distinct non-zero squares having no non-trivial common factor. For if $a = \lfloor \sqrt{n/3} + 1 \rfloor$ and if $n_1 = n - a^2 - (a+1)^2$, then

$$n_1 \geq n - (\sqrt{n/3} + 1)^2 - (\sqrt{n/3} + 2)^2 = (\sqrt{n/3} - 3)^2 - 14 > N(s-2),$$

and so n_1 is expressible as a sum of $s - 2$ distinct non-zero squares. Since a and $a + 1$ are coprime and $a > \sqrt{n/3} > \sqrt{n_1}$, it follows that n is expressible as a sum of s distinct non-zero squares having no non-trivial common factor.

To complete the proof it suffices to observe that

$$3(3 + \sqrt{N(s-2) + 14})^2 < 4P(s)$$

for $s > 12$. For $12 < s \leq 168$ this follows from the computed values of $N(s)$ (see Section 11). For $s \geq 168$ we have by the first corollary to Theorem 4

$$N(s-2) < 1.033P(s-2) < 0.35(s-1)^3,$$

and hence

$$\begin{aligned}3(3+\sqrt{N(s-2)+14})^2 &= 3N(s-2)+69+18\sqrt{N(s-2)+14}\\ &< 4P(s-2)+4(s-1)^2+18\sqrt{4(s-1)^3/9}\\ &< 4P(s-2)+4(s-1)^2+4s^2 = 4P(s).\end{aligned}$$

Thus the theorem is proved.

10. A result for kth powers. Throughout this section, k will be a fixed positive integer greater than 1. Let $R_s(n)$ denote the number of solutions to $x_1^k + x_2^k + \ldots + x_s^k = n$ in non-negative integers $x_1, \ldots, x_k$. Hardy and Littlewood proved that there is a positive integer $s_0 = s_0(k)$ depending only on k such that if $s \geq s_0$ and n is any positive integer, then

$$b_s n^{s/k-1} < R_s(n) < B_s n^{s/k-1},$$

where b_s and B_s are positive numbers depending only on s and k (see, e.g., Chapter 2 in [Va]).

LEMMA 10.1. *There exist positive constants C and D (depending on k) such that if m is a given positive integer and n is a positive integer greater than $(Cm+D)^k$, then n is expressible as a sum of $s_0(k)+2$ distinct k-th powers each of which is $\geq m^k$.*

Proof. Let $F(n)$ denote the number of solutions of $x_1^k + \ldots + x_{s_0+2}^k = n$ in integers $x_1, \ldots, x_{s_0+2}$ such that $x_i \geq m$ for each i and $x_i \neq x_j$ for $i \neq j$. Then

$$\begin{aligned}F(n) &\geq R_{s_0+2}(n) - (s_0+2)\sum_{i=0}^{m-1} R_{s_0+1}(n-i^k)\\ &\quad - \binom{s_0+2}{2}\sum_{i=m}^{\lfloor (n/2)^{1/k}\rfloor} R_{s_0}(n-2i^k)\\ &> b_{s_0+2}n^{(s_0+2)/k-1} - (s_0+2)mB_{s_0+1}n^{(s_0+1)/k-1}\\ &\quad - \binom{s_0+2}{2}\left(\frac{n}{2}\right)^{1/k} B_{s_0}n^{s_0/k-1} > 0,\end{aligned}$$

provided

$$b_{s_0+2}n^{1/k} > (s_0+2)B_{s_0+1}m + (s_0+2)(s_0+1)2^{-1-1/k}B_{s_0}.$$

Since the latter condition holds if $n^{1/k} > Cm + D$ with suitable constants C and D depending on k, the assertion of the lemma follows.

Let $N_k(s)$ denote the largest positive integer *not* expressible as a sum of s distinct kth powers of positive integers. The preceding lemma (with $m = 1$) shows that $N_k(s)$ exists for $s \geq s_0(k) + 2$.

THEOREM 6. *$N_k(s) = s^{k+1}/(k+1) + O(s^k)$ for $s \geq s_0(k) + 2$.*

Proof. First we note that $1 + \sum_{i=1}^{s} i^k$ cannot be expressed as a sum of s distinct positive kth powers, so that

$$N_k(s) > \sum_{i=1}^{s} i^k = \frac{s^{k+1}}{k+1} + O(s^k).$$

On the other hand, we show that if $s \geq s_0(k) + 2$ and if

$$n > (s - s_0 - 1)^{k+1}/(k+1) + (C(s - s_0 - 1) + D)^k,$$

where C and D are as in the lemma, then n is expressible as a sum of s distinct positive kth powers. For then

$$n > \sum_{i=1}^{s-s_0-2} i^k + (C(s - s_0 - 1) + D)^k$$

and so by the lemma with $m = s - s_0 - 1$ we obtain that $n - \sum_{i=1}^{s-s_0-2} i^k$ is expressible as a sum of $s_0(k) + 2$ distinct positive kth powers each of which is greater than $(s - s_0 - 2)^k$.

11. Numerical data. We have calculated $N(s)$ for $5 \leq s \leq 400$ and for some isolated values greater than 400. In order to carry out these computations we needed some a priori bound $L(s)$ for $N(s)$, so that it suffices to test the integers in the interval $[P(s), L(s)]$ for expressibility as a sum of s distinct non-zero squares. (Recall that $P(s) = 1^2 + 2^2 + \ldots + s^2$ is the smallest integer expressible as a sum of s distinct non-zero squares.) Given such a bound $L(s)$, we used the following algorithm: First, an array $a[P(s)], a[P(s) + 1], \ldots, a[L(s)]$ is initialized to zero and a variable L is set to $L(s)$. Then s-tuples $(x_1, \ldots, x_s)$ of integers such that $0 < x_1 < \ldots < x_s$ and $x_1^2 + \ldots + x_s^2 \leq L$ are generated, and the value of $a[x_1^2 + \ldots + x_s^2]$ is set to 1. Whenever it occurs that $x_1^2 + \ldots + x_s^2 = L$ exactly, then we replace L by the largest integer L' such that $a[L'] = 0$. This device results in a dramatic reduction of the number of cases to be investigated compared to a brute force approach. The algorithm terminates when there is no tuple $(x_1, \ldots, x_s)$ left satisfying $0 < x_1 < \ldots < x_s$ and $x_1^2 + \ldots + x_s^2 \leq L$. The number $N(s)$ is then equal to the current value of L.

The efficiency of this algorithm clearly depends on the length of the array $a[n]$ and it is therefore desirable to have a numerical bound $L(s)$ which is as close to $P(s)$ as possible. For our computations of $N(s)$ for $5 \leq s \leq 400$ we used the bound given by the following proposition. While this bound is inferior asymptotically to the bound given by Theorem 4, it is better numerically for values of s less than 8000, say, as a result of the large size of the coefficients on the right-hand side of the inequality of Theorem 4. The inequality of Proposition 11.1 has the disadvantage that it requires a knowledge of $N(s-1)$ and so is useful primarily for calculating a complete table of values of $N(s)$ up to some point. For calculating an isolated value of $N(s)$ we must use the bound of either Theorem 4 or Corollary 1.

Proposition 11.1. *For* $s \geq 6$, *we have* $N(s) \leq L(s)$, *where*

$$L(s) = 2N(s-1) - P(s-2) + 6 + 4\sqrt{N(s-1) - P(s-2) + 2}.$$

Remark. From (1.2) it follows that

$$\begin{aligned} L(s) &= 2P(s-1) - P(s-2) + 2(2(s-1))^{3/2} + O(s^{5/4}) \\ &\quad + 4\sqrt{P(s-1) - P(s-2) + O(s^{3/2})} \\ &= P(s) + 2(2s)^{3/2} + O(s^{5/4}). \end{aligned}$$

On the other hand, we have

$$N(s) = P(s) + (2s)^{3/2} + O(s^{5/4}).$$

Thus, $N(s)$ lies near the midpoint of the interval $[P(s), L(s)]$ for large s.

Proof of Proposition 11.1. Replacing s by $s+1$, we see that it suffices to show that if $s \geq 5$ and

$$n > 2N(s) - P(s-1) + 6 + 4\sqrt{N(s) - P(s-1) + 2}, \tag{11.1}$$

then n is a sum of $s+1$ distinct positive squares. We first note that (11.1) implies

$$n > 2N(s) - P(s-1) > 2P(s) - P(s-1) > P(s-1)$$

and so $n - P(s-1) > 0$. Let $g_s(n)$ denote the smallest integer strictly greater than $\sqrt{(n-P(s-1))/2}$. To prove that n is a sum of $s+1$ distinct non-zero squares it suffices to show that

$$n - g_s^2(n) > N(s). \tag{11.2}$$

For if (11.2) holds, then

$$n - g_s^2(n) = x_1^2 + \ldots + x_s^2,$$

for integers $0 < x_1 < \ldots < x_s$ and further

$$x_s^2 = n - g_s^2(n) - x_1^2 - \ldots - x_{s-1}^2 \leq n - g_s^2(n) - P(s-1) < g_s^2(n),$$

the last step resulting from the definition of $g_s(n)$. Now

$$g_s(n) \le 1 + \sqrt{(n - P(s-1))/2},$$

and so to prove (11.2) it suffices to show that (11.1) implies

$$n - \{1 + \sqrt{(n - P(s-1))/2}\}^2 > N(s),$$

that is,

$$\frac{n}{2} + \frac{P(s-1)}{2} - 1 - N(s) > 2\sqrt{(n - P(s-1))/2}$$

or

$$t > 2\sqrt{t - P(s-1) + 1 + N(s)}, \tag{11.3}$$

where

$$t = \frac{n}{2} + \frac{P(s-1)}{2} - 1 - N(s). \tag{11.4}$$

Now (11.1) implies that certainly $t > 2$. Hence (11.3) is equivalent to

$$t^2 > 4(t - P(s-1) + 1 + N(s))$$

or to

$$t^2 - 4t + 4 > 4(N(s) - P(s-1) + 2)$$

or to

$$t - 2 > 2\sqrt{N(s) - P(s-1) + 2}. \tag{11.5}$$

But, in view of (11.4), (11.5) is equivalent to (11.1), and hence (11.3) and (11.2) hold. This completes the proof of Proposition 11.1.

We conclude with two tables of numerical values for $N(s)$. Table I lists all values of $N(s)$ up to $s = 400$ and substantially extends the table given in [HK]. Table II gives the values for $N(s)$ for $s = 20, 40, \ldots, 1000$, along with the polynomial approximation $P(s)$, the difference $R(s) = N(s) - P(s)$, and the approximation $R_0(s) = 2s(\sqrt{2s} + \lambda_s(2s)^{1/4})$ to $R(s)$ given by formula (1.2) of Theorem 1. It is apparent from this table that $P(s)$ is very close to $N(s)$, the difference $R(s) = N(s) - P(s)$ being roughly of size $\sqrt{N(s)}$. On the other hand, the agreement between $R(s)$ and $R_0(s)$ is rather poor. The ratio $R(s)/R_0(s)$ between the two quantities, which by (1.2) is asymptotically equal to 1, falls roughly between 1.15 and 1.4 for the computed values with $180 \le s \le 1000$. This, however, is not surprising, since the error term in (1.2) is only by a factor $O(s^{-1/8})$ smaller than the main term. In fact, a careful analysis of the proof reveals that this error term oscillates in a manner similar to the term $\lambda_s(2s)^{1/4}$, with amplitudes of size $O(s^{-1/8})$ relative to the main term.

Table I. Values of $N(s)$ for $5 \le s \le 400$

s	$N(s)$	$N(s+50)$	$N(s+100)$	$N(s+150)$	$N(s+200)$	$N(s+250)$	$N(s+300)$	$N(s+350)$
1		47668	353301	1167858	2739627	5319763	9157781	14503694
2		50373	364021	1191142	2780495	5384828	9249353	14629010
3		53097	374678	1214987	2821768	5447969	9342342	14752167
4		56253	385598	1238763	2864188	5512557	9433610	14877763
5	245	59522	396675	1261760	2906277	5577097	9527815	15003868
6	333	62502	407899	1286868	2948021	5643262	9620543	15130352
7	330	65842	419464	1311577	2990934	5709383	9714648	15258213
8	462	69203	431180	1336601	3035034	5776983	9809808	15386457
9	539	72944	443298	1362318	3078779	5843172	9905365	15516778
10	647	76356	455265	1387602	3122187	5910676	10001541	15646462
11	888	80337	467574	1413583	3167131	5979037	10098102	15776703
12	1036	84025	480234	1439887	3212141	6047753	10196742	15907827
13	1177	88073	492983	1466892	3257508	6116994	10294787	16038472
14	1445	92211	506103	1493472	3303853	6187750	10392475	16172428
15	1722	96663	519304	1521133	3350142	6257059	10491524	16305557
16	1990	101047	533848	1548373	3396371	6327887	10591708	16438389
17	2311	105604	546629	1576322	3444923	6398667	10693257	16573002
18	2672	110048	560553	1604486	3492519	6471144	10793473	16709866
19	3047	114876	574818	1633723	3539648	6543577	10895090	16844903
20	3492	120057	589270	1662187	3588112	6617561	11000162	16983287
21	4093	125146	604963	1691864	3636957	6690062	11100903	17119604
22	4613	130334	619907	1721508	3686305	6764463	11204407	17257940
23	5138	135755	634512	1751617	3735729	6840727	11310052	17397277
24	5718	141003	650532	1781833	3786418	6914895	11414120	17538653
25	6379	146872	665338	1812662	3837542	6989564	11519601	17679362
26	7123	152752	681113	1843178	3888183	7066848	11626173	17820822
27	7952	158753	697473	1874567	3939399	7142517	11734378	17961603
28	8676	164793	714162	1906687	3993688	7219969	11842042	18104567
29	9537	171150	730855	1938932	4044409	7298930	11950139	18249728
30	10393	177622	748447	1971412	4097381	7376258	12058131	18394212
31	11558	184231	765020	2004237	4150806	7455387	12167768	18538009
32	12602	190959	782064	2036877	4204630	7536043	12279288	18683837
33	13743	197940	800901	2070922	4258959	7616208	12390257	18832238
34	14863	205288	818048	2104898	4314847	7696940	12500665	18978927
35	16252	212317	836570	2139171	4370144	7777169	12614070	19128087
36	17528	219737	855758	2173283	4424940	7859037	12727174	19277167
37	18957	227354	874587	2208688	4481632	7942558	12840823	19426163
38	20481	235170	893691	2244272	4537885	8025578	12955147	19577648
39	22042	243139	913448	2280073	4596062	8108466	13069884	19728777
40	23678	251555	932732	2316237	4652746	8193351	13185828	19880957
41	25347	259616	952017	2352742	4711887	8278108	13301917	20032714
42	27207	268233	972897	2389498	4770523	8363192	13419077	20187950
43	29092	276777	993782	2427007	4828644	8449113	13536802	20342319
44	31228	285685	1014202	2464707	4889252	8535765	13654110	20497803
45	33297	295070	1034591	2502812	4949349	8622718	13774483	20653912

Table I (cont.)

s	$N(s)$	$N(s+50)$	$N(s{+}100)$	$N(s{+}150)$	$N(s{+}200)$	$N(s{+}250)$	$N(s{+}300)$	$N(s{+}350)$
46	35289	304338	1056663	2541621	5009368	8710678	13894279	20810636
47	37653	313747	1078332	2579933	5070898	8798963	14014592	20968325
48	40042	323272	1099592	2619433	5132474	8887116	14135652	21126114
49	42487	333123	1122933	2659421	5194122	8977320	14256960	21284758
50	45023	343296	1145117	2699146	5256211	9067396	14379001	21446362

Table II. Comparison between $R(s) = N(s) - P(s)$ and $R_0(s) = 2s(\sqrt{2s} + \lambda_s(2s)^{1/4})$

s	$N(s)$	$P(s)$	$R(s)$	$R_0(s)$	$R(s)/R_0(s)$
20	3492	2870	622	334.029	1.86212
40	23678	22140	1538	941.071	1.63431
60	76356	73810	2546	1693.18	1.50368
80	177622	173880	3742	2500.56	1.49646
100	343296	338350	4946	3464.73	1.42753
120	589270	583220	6050	4655.05	1.29966
140	932732	924490	8242	5521.97	1.49258
160	1387602	1378160	9442	6917.42	1.36496
180	1971412	1960230	11182	8356.78	1.33807
200	2699146	2686700	12446	9788.85	1.27145
220	3588112	3573570	14542	11196.1	1.29884
240	4652746	4636840	15906	12548.1	1.26761
260	5910676	5892510	18166	13792.5	1.31709
280	7376258	7356580	19678	15484.1	1.27085
300	9067396	9045050	22346	17651.3	1.26597
320	11000162	10973920	26242	18676.9	1.40505
340	13185828	13159190	26638	20926.8	1.27291
360	15646462	15616860	29602	22362.5	1.32373
380	18394212	18362930	31282	24660.5	1.26851
400	21446362	21413400	32962	25835.5	1.27584
420	24820272	24784270	36002	28789	1.25055
440	28527862	28491540	36322	30029.4	1.20955
460	32590736	32551210	39526	32030.6	1.23401
480	37020622	36979280	41342	35001.3	1.18116
500	41836864	41791750	45114	36507.2	1.23576
520	47051574	47004620	46954	37723.2	1.24470
540	52686788	52633890	52898	40770.3	1.29746
560	58748358	58695560	52798	43740.1	1.20708
580	65260300	65205630	54670	45867.6	1.19191
600	72238998	72180100	58898	47553.7	1.23856
620	79695548	79634970	60578	49233.6	1.23042
640	87651558	87586240	65318	51494.2	1.26845
660	96114808	96049910	64898	54439.4	1.19211

Table II (cont.)

s	$N(s)$	$P(s)$	$R(s)$	$R_0(s)$	$R(s)/R_0(s)$
680	105111458	105041980	69478	57337	1.21175
700	114650008	114578450	71558	60199.9	1.18867
720	124748958	124675320	73638	63034.6	1.16822
740	135427128	135348590	78538	65844	1.19279
760	146694958	146614260	80698	68628.9	1.17586
780	158574168	158488330	85838	71388	1.20241
800	171074942	170986800	88142	74119.3	1.18919
820	184215972	184125670	90302	76819.2	1.17551
840	198016654	197920940	95714	79483.2	1.20420
860	212483472	212388610	94862	82105.5	1.15537
880	227644810	227544680	100130	84679	1.18247
900	243507824	243405150	102674	87194.8	1.17752
920	260091014	259986020	104994	89641.3	1.17127
940	277414216	277303290	110926	92004	1.20567
960	295486262	295372960	113302	94262.8	1.20198
980	314326668	314211030	115638	96389.7	1.19969
1000	333951594	333833500	118094	99427.2	1.18774

References

[HK] F. Halter-Koch, *Darstellung natürlicher Zahlen als Summe von Quadraten*, Acta Arith. 42 (1982), 11–20.

[Ka] M. Kassner, *Darstellungen mit Nebenbedingungen durch quadratische Formen*, J. Reine Angew. Math. 331 (1982), 151–161.

[PS] G. Pólya and G. Szegö, *Problems and Theorems in Analysis*, Vol. II, Springer, Berlin, 1978.

[Va] R. C. Vaughan, *The Hardy–Littlewood Method*, Cambridge University Press, Cambridge, 1981.

[Wr] E. M. Wright, *The representation of a number as a sum of five or more squares*, Quart. J. Math. Oxford Ser. 4 (1933), 37–51.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS 61801
U.S.A.

DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF CINCINNATI
CINCINNATI, OHIO 45221
U.S.A.

Received on 19.10.1993 (2502)