Sums of integers and sums of their squares

by

DETLEV W. HOFFMANN (Dortmund)

1. Introduction. Let $\mathbb{N}$ (resp. $\mathbb{N}_0$) denote the set of all positive (resp. nonnegative) integers. For $m \in \mathbb{N}$, we define

$$\text{SOS}(m) = \{a_1^2 + \cdots + a_m^2 \mid a_i \in \mathbb{Z} \text{ for } 1 \leq i \leq m\}$$

to be the set of all nonnegative integers that are sums of $m$ integer squares. By Lagrange’s 4-square theorem, we know that $\text{SOS}(m) = \mathbb{N}_0$ for $m \geq 4$. Now let $n \in \mathbb{N}$, $T \in \mathbb{Z}$, and consider the following system of diophantine equations:

\begin{align*}
  x_1 + \cdots + x_m &= T, \\
  x_1^2 + \cdots + x_m^2 &= n.
\end{align*}

For it to have a solution, some necessary conditions must be satisfied by $n$ and $T$:

\begin{enumerate}
  \item $n \in \text{SOS}(m)$,
  \item $n \equiv T \mod 2$,
  \item $T^2 \leq mn$.
\end{enumerate}

Condition (1) is obvious and gives no restriction on $n \in \mathbb{N}$ if $m \geq 4$. Condition (2) follows from the fact that $x^2 \equiv x \mod 2$ for each $x \in \mathbb{Z}$. Condition (3) is a consequence of the Cauchy–Schwarz inequality. Indeed, if $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ is a solution of the above system, and if we put $\mathbf{1} = (1, \ldots, 1) \in \mathbb{Z}^m$, then the Cauchy–Schwarz inequality applied to the usual scalar product (dot product) implies

$$T^2 = (\mathbf{1} \cdot \mathbf{x})^2 \leq (\mathbf{1} \cdot \mathbf{1})(\mathbf{x} \cdot \mathbf{x}) = mn.$$
We now fix \( n \in \text{SOS}(m) \) and define the set of those \( T \) for which the above system has a solution:

\[
\mathcal{I}_m(n) = \{ T \in \mathbb{Z} \mid \text{[1.1] has a solution } x \in \mathbb{Z}^m \}.
\]

Note that \( \mathcal{I}_m(n) \) is symmetric in the sense that \( T \in \mathcal{I}_m(n) \) if and only if \( -T \in \mathcal{I}_m(n) \). Goldmakher and Pollack [3, Th. 2] have determined \( \mathcal{I}_4(n) \):

**Theorem 1.1.** \( \mathcal{I}_4(n) = \{ T \in \mathbb{Z} \mid T \equiv n \mod 2, 4n - T^2 \in \text{SOS}(3) \} \).

In particular, Legendre’s 3-square theorem readily implies that for odd \( n \), one always has \( 1 \in \mathcal{I}_4(n) \), thus giving a new proof of a conjecture of Euler ([1])

The purpose of the present paper is to study the sets \( \mathcal{I}_m(n) \) in more detail also for other values of \( m \). In particular, we get complete descriptions of \( \mathcal{I}_m(n) \) for \( m \leq 11 \): see Proposition 2.1 for the case \( m = 1 \) and the case \( n \leq m \), Theorem 3.1 for the case \( 2 \leq m \leq 7 \), and Theorem 4.1 for the case \( 8 \leq m \leq 11 \). Some further results such as the determination of \( \mathcal{I}_m(n) \) in the case \( 10 \leq m < n \leq m + 6 \) (Corollary 4.12) are also included.

For small values of \( m \) we use classical results by Mordell on representations of integral binary forms as sums of squares of integral linear forms. This approach also allows a new interpretation of Goldmakher and Pollack’s results on \( \mathcal{I}_4(n) \), and it can be applied to variations of the above problem studied by Z.-W. Sun et al. in a series of papers [7]–[10]. There, one considers modified systems of equations for \( m = 4 \) where the first equation in \([1.1]\) is replaced by some other integral polynomial equation, i.e., one looks for solutions of

\[
x_1^2 + x_2^2 + x_3^2 + x_4^2 = n,
\]

\[
P(x_1, x_2, x_3, x_4) = T,
\]

where \( P(x_1, x_2, x_3, x_4) \in \mathbb{Z}[x_1, x_2, x_3, x_4] \). In analogy to the above notation and for given \( n \in \mathbb{N} \), we denote the set of those \( T \in \mathbb{Z} \) for which this new system has a solution \( x \in \mathbb{Z}^4 \) by \( \mathcal{I}_{4,P}(n) \). Using Mordell’s results, we show how several results by Z.-W. Sun et al. concerning \( \mathcal{I}_{4,P}(n) \) for linear polynomials \( P \) can be easily recovered and extended.

**2. General results.** We start with some easy observations.

**Proposition 2.1.** Let \( n, m \in \mathbb{N} \).

1. If \( n = a^2 \) for some \( a \in \mathbb{N} \), then \( \mathcal{I}_1(n) = \{ \pm a \} \); otherwise \( \mathcal{I}_1(n) = \emptyset \).
2. \( \mathcal{I}_m(n) \subseteq \mathcal{I}_{m+1}(n) \).
3. If \( n \leq m \), then \( \mathcal{I}_m(n) = \{ T \in \mathbb{Z} \mid n \equiv T \mod 2, |T| \leq n \} \).

(1) In their paper [3], Goldmakher and Pollack mention Franz Lemmermeyer’s earlier proof of Euler’s conjecture on mathoverflow.net/questions/37278/euler-and-the-four-squares-theorem that also makes use of Legendre’s 3-square theorem.
Proof. (1) is trivial.

(2) Any representation of \( n \) by a sum of \( m \) squares (with corresponding sum \( T \in \mathcal{S}_m(n) \)) becomes a representation by \( m + 1 \) squares by adding \( 0^2 \), hence \( T = T + 0 \in \mathcal{S}_{m+1}(n) \).

(3) It is obvious that if \( n \leq m \), then \( \max(\mathcal{S}_m(n)) = n \) is attained by the representation \( n = \sum_{i=1}^m 1^2 \). So any \( T \in \mathcal{S}_m(n) \) satisfies \( |T| \leq n \). By changing the signs of the 1’s in the above sum as necessary, one finds that each \( T \in \mathbb{Z} \) with \( |T| \leq n \) and \( n \equiv T \mod 2 \) will be in \( \mathcal{S}_m(n) \). □

In view of (1.2), it is a priori possible that \( T \in \mathcal{S}_m(n) \) with \( T^2 = mn \). Of course, since \( T \in \mathbb{Z} \), for this to hold, \( mn \) must be a square. More precisely, we have the following.

**Proposition 2.2.** Let \( m, n \in \mathbb{N} \) and \( T \in \mathbb{Z} \). Then \( T \in \mathcal{S}_m(n) \) with \( T^2 = mn \) if and only if there exists \( a \in \mathbb{N} \) with \( n = ma^2 \), in which case \( T = \pm ma \).

Proof. If \( n = ma^2 \), then \( n = \sum_{i=1}^m a^2 \) and \( T = \sum_{i=1}^m a = ma \in \mathcal{S}_m(n) \). Conversely, if \( T \in \mathcal{S}_m(n) \) with \( T^2 = mn \), then there exists \( x \in \mathbb{Z}^m \) yielding equality in (1.3), which implies that \( x \) and the vector \( 1 \) are linearly dependent, from which it follows that \( x = (x_1, \ldots, x_m) = (a, \ldots, a) \) for some \( a \in \mathbb{Z} \); plugging this into (1.1) implies that \( n = ma^2 \) and \( T^2 = mn = m^2a^2 \). □

Because of this result, it makes sense to focus mainly on those \( T \) in \( \mathcal{S}_m(n) \) with \( T^2 < mn \). For \( n, m \in \mathbb{N} \), we define the following sets of \( T \in \mathbb{Z} \) satisfying (1.2)(2) and strict inequality in (1.2)(3):

\[
\mathcal{S}_m(n) = \{ T \in \mathbb{Z} \mid n \equiv T \mod 2, T^2 < mn \},
\]

\[
\mathcal{S}_m^\prime(n) = \{ T \in \mathcal{S}_m(n) \mid T^2 < mn \}.
\]

We say that \( \mathcal{S}_m(n) \) is full if \( \mathcal{S}_m^\prime(n) = \mathcal{S}_m(n) \). As an immediate consequence of Proposition 2.2(1.2), and the definition of fullness, we get the following.

**Corollary 2.3.** Let \( m, n \in \mathbb{N} \).

\( \mathcal{S}_m(n) \) is full \( \iff \)

\[
\begin{cases}
\mathcal{S}_m(n) = \mathcal{S}_m(n) \cup \{ \pm ma \} & \text{if } \exists a \in \mathbb{N} : n = ma^2, \\
\mathcal{S}_m(n) = \mathcal{S}_m(n) & \text{otherwise.}
\end{cases}
\]

**Corollary 2.4.** Let \( n, m \in \mathbb{N} \) with \( n \leq m \). Then \( \mathcal{S}_m(n) \) is full if and only if \( m \leq n + 4 + 4/n \). In particular, \( \mathcal{S}_m(n) \) is full whenever \( n \leq m \leq 8 \).

Proof. It follows readily from Proposition 2.1(3) and the definition of fullness that \( \mathcal{S}_m(n) \) is full iff \( |T| \leq n \) for all \( T \in \mathbb{Z} \) with \( n \equiv T \mod 2 \) and \( T^2 < mn \), iff \((n + 2)^2 \geq mn \) iff \( m \leq n + 4 + 4/n \). Since \( n + 4 + 4/n \geq 8 \) for all \( n \in \mathbb{N} \), it follows that \( \mathcal{S}_m(n) \) is full whenever \( n \leq m \leq 8 \). □
3. Mordell’s results on sums of squares of linear forms. Let us fix \( n, m \in \mathbb{Z} \). Working in the polynomial ring \( \mathbb{Z}[X,Y] \), one readily finds that \( x = (x_1, \ldots, x_m) \in \mathbb{Z}^m \) being a solution of (1.1) is equivalent to the equality

\[
\sum_{i=1}^{m} (X + x_i Y)^2 = mX^2 + 2TXY + nY^2
\]

in \( \mathbb{Z}[X,Y] \). We will denote the binary integral quadratic form \( mX^2 + 2TXY + nY^2 \) by \([m,T,n]\) for short. Hence, \([m,T,n]\) can be written as a sum of \( m \) squares of integral linear forms. Note that this in turn means that \([m,T,n]\) must be positive semidefinite. We define the determinant \( \Delta \) of \([m,T,n]\) to be

\[
\Delta(m,T,n) = mn - T^2,
\]

the determinant of the Gram matrix \( \begin{pmatrix} m & T \\ T & n \end{pmatrix} \) of the associated bilinear form. By the Hurwitz criterion (and since \( m,n \in \mathbb{N} \)), the form \([m,T,n]\) is positive semidefinite iff \( \Delta(m,T,n) = mn - T^2 \geq 0 \), i.e., \( mn \geq T^2 \), which is a different way of deriving the necessary condition (3) in (1.2).

In \([5], [6]\), Mordell considered the following more general problem. Given \( a,h,b \in \mathbb{Z} \) and \( m \in \mathbb{N} \), what are necessary and sufficient conditions for \([a,h,b]\) to be a sum of \( m \) squares of integral linear forms, i.e., when are there \( a_i, b_i \in \mathbb{Z}, 1 \leq i \leq m \), with

\[
\sum_{i=1}^{m} (a_i X + b_i Y)^2 = aX^2 + 2hXY + bY^2?
\]

The necessary and sufficient criteria found by Mordell for the solvability of (3.2), when applied to \([a,h,b] = [m,T,n]\), thus become necessary conditions for the solvability of (3.1). For \( 2 \leq m \leq 7 \) we can say more (recall that the trivial case \( m = 1 \) has been dealt with in Proposition 2.1).

Proposition 3.1. Let \( m,n \in \mathbb{N} \) and \( T \in \mathbb{Z} \).

(i) If \( m = 2,3 \), then \( T \in \mathcal{J}_m(n) \) if and only if \([m,T,n]\) is a sum of \( m \) squares of integral linear forms.

(ii) If \( 4 \leq m \leq 7 \), then \( T \in \mathcal{J}_m(n) \) if and only if \( T \equiv n \) mod 2 and \([m,T,n]\) is a sum of \( m \) squares of integral linear forms.

Proof. If \( T \in \mathcal{J}_m(n) \), then as remarked above, \([m,T,n]\) is a sum of \( m \) squares of integral linear forms. Note also that \( T \equiv n \) mod 2.

Conversely, suppose that \( 2 \leq m \leq 7 \), and in addition that \( n \equiv T \) mod 2 when \( m \geq 4 \), and assume that

\[
[m,T,n] = \sum_{i=1}^{m} (a_i X + b_i Y)^2
\]

with \( a_i, b_i \in \mathbb{Z} \). We may further assume that \( a_i \geq 0 \) for \( 1 \leq i \leq m \) after changing signs of both \( a_i \) and \( b_i \) whenever necessary. Since \( m = \sum_{i=1}^{m} a_i^2 \), we
see that for \( m = 2, 3 \) the only solution is \( a_1 = \cdots = a_m = 1 \), which means we have a solution of \((3.1)\), hence \( T \in \mathcal{I}_m(n) \).

Now if \( m = 4 \), our solution of \((3.3)\) satisfies in particular \( m = \sum_{i=1}^{m} a_i^2 \), and after permuting the summands if necessary, there are two possibilities: \((a_1, \ldots, a_4) = (1, 1, 1, 1)\) or \((a_1, \ldots, a_4) = (2, 0, 0, 0)\). In the case \((1, 1, 1, 1)\), this again implies that we get a solution of \((3.1)\), hence \( T \in \mathcal{I}_4(n) \).

In the case \((2, 0, 0, 0)\), we get \( 4b_1 = 2T \), which necessarily implies that \( n \equiv T \equiv 0 \mod 2 \). But then \( n = \sum_{i=1}^{4} b_i^2 = \sum_{i=1}^{4} \pm b_i \equiv 0 \mod 2 \). We put

\[
c_1 = \frac{1}{2} (b_1 + b_2 + b_3 + b_4), \quad c_2 = \frac{1}{2} (b_1 + b_2 - b_3 - b_4),
\]

\[
c_3 = \frac{1}{2} (b_1 - b_2 + b_3 - b_4), \quad c_4 = \frac{1}{2} (b_1 - b_2 - b_3 + b_4),
\]

and we have \( c_i \in \mathbb{Z}, \sum_{i=1}^{4} c_i = 2b_1 = T \) and \( \sum_{i=1}^{4} c_i^2 = \sum_{i=1}^{4} b_i^2 = n \), and therefore \( T \in \mathcal{I}_4(n) \).

If \( 5 \leq m \leq 7 \), our solution of \((3.3)\) satisfies in particular \( m = \sum_{i=1}^{m} a_i^2 \), and after permuting the summands if necessary, there are two possibilities: \((a_1, \ldots, a_m) = (1, \ldots, 1)\) or \((a_1, \ldots, a_m) = (2, 0, 0, 0, 1, \ldots, 1)\).

In the case \((1, \ldots, 1)\), we conclude as before that \( T \in \mathcal{I}_m(n) \). Now suppose that we are in the case \((2, 0, 0, 0, 1, \ldots, 1)\). Then \( T = 2b_1 + \sum_{i=5}^{m} b_i \). Now

\[
\sum_{i=5}^{m} b_i \equiv T \equiv n \equiv \sum_{i=1}^{m} b_i^2 \equiv \sum_{i=1}^{m} \pm b_i \mod 2,
\]

which implies that \( \sum_{i=1}^{4} \pm b_i \) is even. Hence, with the same \( c_1, \ldots, c_4 \) as above and with \( c_i = b_i \) for \( 5 \leq i \leq m \), we have \( c_i \in \mathbb{Z}, \sum_{i=1}^{m} c_i = 2b_1 + \sum_{i=5}^{m} b_i = T \) and \( \sum_{i=1}^{m} c_i^2 = \sum_{i=1}^{m} b_i^2 = n \), and therefore \( T \in \mathcal{I}_m(n) \).

We now turn to Mordell’s results on solving \((3.2)\) for given \( aX^2 + 2hXY + bY^2 \in \mathbb{Z}[X,Y] \). Let us first deal with some obvious cases. Recall that the solvability requires \( a, b, \Delta = ab - h^2 \geq 0 \), which we henceforth assume. Also, if we assume in addition \( aX^2 + 2hXY + bY^2 \neq 0 \), then we cannot have \( a = b = 0 \), in which case we may assume \( a > 0 \).

**Proposition 3.2.** Let \( aX^2 + 2hXY + bY^2 \in \mathbb{Z}[X,Y] \setminus \{0\} \) with \( a > 0 \), \( b, \Delta \geq 0 \).

(a) If \( \Delta = 0 \), then the following are equivalent:

(i) \((3.2)\) is solvable;

(ii) \( a \in \text{SOS}(m) \);

(iii) there exist \( r, s, t \in \mathbb{Z} \) with \( 0 < t \in \text{SOS}(m) \) and \( aX^2 + 2hXY + bY^2 = t(rX + sY)^2 \).

(b) \((3.2)\) is solvable for \( m = 1 \) if \( \Delta = 0 \) and \( a \in \text{SOS}(1) \).

**Proof.** In (a), the implications (i)\( \Rightarrow\) (ii) and (iii)\( \Rightarrow\) (i) are trivial. If (ii) holds, then \( ab = h^2 \) implies that we can find \( r, t \in \mathbb{N}, s \in \mathbb{N}_0 \) with \( a = r^2t \),
b = s^2t and h = \pm rst, and thus \( aX^2 + 2hXY + bY^2 = t(rX \pm sY)^2 \). But then it is well known (or easy to check) that \( 0 < a \in \text{SOS}(m) \) iff \( 0 < t \in \text{SOS}(m) \), which yields (iii).

If (3.2) is solvable for \( m = 1 \), then \( aX^2 + 2hXY + bY^2 = (rX + sY)^2 \) for some \( r, s \in \mathbb{Z} \). Hence \( \Delta = ab - h^2 = r^2s^2 - (rs)^2 = 0 \). Now (b) follows readily from (a).

Before we state Mordell’s results, we introduce some further notations. For \( n \in \mathbb{Z} \setminus \{0\} \) and any prime number \( p \), we denote by \( v_p(n) \in \mathbb{N}_0 \) the usual \( p \)-adic value of \( n \), and by \( n_p \) the \( p \)-free part of \( n \), so that \( n = p^{v_p(n)}n_p \) where \( n_p \in \mathbb{Z} \) with \( \gcd(p, n_p) = 1 \). If \( p \) does not divide \( n \), then \( (n_p) \) denotes the usual Legendre symbol:

\[
\left( \frac{n}{p} \right) = \begin{cases} 
1 & \text{if } n \text{ is a quadratic residue modulo } p, \\
-1 & \text{otherwise}.
\end{cases}
\]

Let now \( aX^2 + 2hXY + bY^2 \in \mathbb{Z}[X,Y] \) with \( a, b, \Delta = ab - h^2 > 0 \). Let \( d = \gcd(a, h, b) \) and \( \tilde{d} = \gcd(a, 2h, b) \). Then \( \tilde{d} \in \{d, 2d\} \).

**Theorem 3.3** (Mordell [5], [6]). Let \( aX^2 + 2hXY + bY^2 \in \mathbb{Z}[X,Y] \) with \( a, b, \Delta = ab - h^2 > 0 \).

(i) (3.2) is solvable for \( m = 2 \) iff \( \Delta \in \text{SOS}(1) \) and \( d \in \text{SOS}(2) \).

(ii) (3.2) is solvable for \( m = 3 \) iff all of the following conditions are satisfied:

(\( \alpha \)) for any odd prime \( p \) with \( v_p(\Delta) \) odd and \( v_p(a) \) even, one has

\[
\left( \frac{-a_p}{p} \right) = 1;
\]

(\( \beta \)) for any odd prime \( p \) with \( v_p(\Delta) \) odd and \( v_p(a) \) odd, one has

\[
\left( \frac{-a_p\Delta_p}{p} \right) = 1;
\]

(\( \gamma \)) for any odd prime \( p \) with \( v_p(\Delta) \) even and \( v_p(d) \) odd, one has

\[
\left( \frac{-\Delta_p}{p} \right) = 1.
\]

(iii) (3.2) is solvable for \( m = 4 \) iff \( \Delta \in \text{SOS}(3) \).

(iv) (3.2) is solvable for \( m = 5 \) (and thus for all \( m \geq 5 \)).

Note that our formulation of the results in the case \( m = 3 \) is a somewhat streamlined version of the one given by Mordell in his original article [6].

We now apply Mordell’s results to determine \( \mathcal{S}_m(n) \) for \( 2 \leq m \leq 7 \).

**Theorem 3.4.** Let \( n \in \mathbb{N} \) and \( T \in \mathbb{Z} \).

(i) \( T \in \mathcal{S}_2(n) \) if and only if \( 2n - T^2 \in \text{SOS}(1) \).
(ii) $T \in \mathcal{S}_3(n)$ if and only if either

- $T = \pm 3t$ and $n = 3t^2$ for some $t \in \mathbb{N}$, or
- $3n - T^2 > 0$ and the following holds: Write $3n - T^2 = D_0D_1^2$ with $D_0, D_1 \in \mathbb{N}$ and $D_0$ squarefree, say, $D_0 = 2^{k_0}q_1 \ldots q_r$ where $k, \ell \in \{0, 1\}$ and $q_1, \ldots, q_r$ ($r \geq 0$) are pairwise different primes with $q_i \notin \{2, 3\}$. Then
  (a) $q_i \equiv 1 \mod 6$ for all $1 \leq i \leq r$, and
  (b) if $\ell = 1$ or $\gcd(3, T, n) = 3$, then $k = 1$.

(iii) (Goldmakher and Pollack [3]) $T \in \mathcal{S}_4(n)$ if and only if $n \equiv T \mod 2$ and $4n - T^2 \in \text{SOS}(3)$. In particular, $\mathcal{S}_4'(n) = \{T \in \mathcal{S}_m(n) \mid 4n - T^2 \in \text{SOS}(3)\}$.

(iv) $T \in \mathcal{S}_m(n)$ for $5 \leq m \leq 7$ if and only if $n \equiv T \mod 2$ and $mn - T^2 \geq 0$. In particular, $\mathcal{S}_m(n)$ is full for $5 \leq m \leq 7$.

Proof. (i) By Proposition 3.1, $T \in \mathcal{S}_2(n)$ if and only if $[2, T, n]$ is a sum of two squares of integral linear forms. Now $d = \gcd(2, T, n) \in \{1, 2\}$, so $d \in \text{SOS}(2)$. By Theorem 3.3(ii) and Proposition 3.2 it follows that $T \in \mathcal{S}_2(n)$ if and only if $2n - T^2 \in \text{SOS}(1)$.

(ii) It is certainly necessary to have $3n - T^2 \geq 0$ by (1.2). By Proposition 2.2, $T \in \mathcal{S}_3(n)$ with $3n - T^2 = 0$ if and only if $T = \pm 3t$ and $n = 3t^2$ for some $t \in \mathbb{N}$. So assume from now on $3n - T^2 > 0$. In view of Proposition 3.1 it suffices to apply the conditions ($\alpha$)–($\gamma$) of Theorem 3.3(ii) to the binary form $3X^2 + 2TXY + nY^2$, for which $a = 3$, $d = \gcd(3, T, n) = \gcd(3, 2T, n) = \tilde{d} \in \{1, 3\}$ and $\Delta = 3n - T^2$. As for ($\alpha$) and ($\beta$), the only odd primes $p$ with $v_p(\Delta)$ odd are the $q_i$’s, and $3$ if $\ell = 1$. Since $v_{q_i}(a) = v_{q_i}(3) = 0$, condition ($\alpha$) applies to these primes, and in view of $a_{q_i} = 3_{q_i} = 3$ and quadratic reciprocity, it translates into

\[(3.4) \quad \left(\frac{-3}{q_i}\right) = \left(\frac{q_i}{3}\right) = 1,
\]

or equivalently $q_i \equiv 1 \mod 3$, and therefore, since the $q_i$ are odd, $q_i \equiv 1 \mod 6$.

If $\ell = 0$, no further odd prime has to be considered in ($\alpha$) and ($\beta$). If $\ell = 1$, then the odd prime $p = 3$ has to be considered as well, but then we are in the situation of ($\beta$) since $v_3(a) = v_3(3) = 1$. Here, $a_3 = 1$, and the squarefree part of $\Delta_3$ is $2^kq_1 \cdots q_r$. Hence, in view of (3.4), condition ($\beta$) becomes

\[(3.5) \quad \left(\frac{-2^kq_1 \cdots q_r}{3}\right) = \left(\frac{-2^k}{3}\right) = \left(\frac{2^k+1}{3}\right) = 1,
\]

from which we find that if $\ell = 1$, then $k = 1$. 

As for condition \((\gamma)\), the odd primes \(p\) with \(v_p(\Delta)\) even are all odd primes \(p \notin \{3, q_1, \ldots, q_r\}\), and \(p = 3\) if \(\ell = 0\), but we have \(v_p(d)\) odd iff \(d = p = 3\). Thus, \((\gamma)\) boils down to the condition that if \(d = 3\) and \(\ell = 0\), then again \(k = 1\) (note that \(-a_3\Delta_3 = -\Delta_3\)).

Thus, the previous two conditions can be summarized: if \(d = 3\) or \(\ell = 1\), then \(k = 1\).

(iii) and (iv) follow directly from Theorem 3.3(iii, iv) together with Proposition 3.1(ii).

Let us illustrate the rather technical conditions in Theorem 3.4(ii) with three examples.

**Example 3.5.** Let us determine \(\mathcal{J}_3(n)\) for \(n = 42\). The \(T \geq 0\) satisfying \(3n - T^2 = 126 - T^2 \geq 0\) and \(T \equiv n \mod 2\) are \(T = 0, 2, 4, 6, 8, 10\). Using the notations from Theorem 3.4(ii) and its proof and checking the criteria (a) and (b) there, we get the following table:

<table>
<thead>
<tr>
<th>(T)</th>
<th>(\Delta = 3n - T^2)</th>
<th>(D_0)</th>
<th>(k)</th>
<th>(\ell)</th>
<th>(d = \gcd(3, n, T))</th>
<th>(T \in \mathcal{J}_3(n))?</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>126</td>
<td>2 \cdot 7</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>yes</td>
</tr>
<tr>
<td>2</td>
<td>122</td>
<td>2 \cdot 61</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>yes</td>
</tr>
<tr>
<td>4</td>
<td>110</td>
<td>2 \cdot 5 \cdot 11</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>no: 5, 11 (\not\equiv) 1 mod 6</td>
</tr>
<tr>
<td>6</td>
<td>90</td>
<td>2 \cdot 5</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>no: 5 (\not\equiv) 1 mod 6</td>
</tr>
<tr>
<td>8</td>
<td>62</td>
<td>2 \cdot 31</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>yes</td>
</tr>
<tr>
<td>10</td>
<td>26</td>
<td>2 \cdot 13</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>yes</td>
</tr>
</tbody>
</table>

Indeed, the only representation of 42 as a sum of three squares of positive integers is \(42 = 5^2 + 4^2 + 1^2\) (cf. Theorem 5.2(3)), from which we easily see that \(\mathcal{J}_3(42) = \{\pm 10, \pm 8, \pm 2, 0\}\).

**Example 3.6.** We now determine \(\mathcal{J}_3(n)\) for \(n = 43\). The \(T \geq 0\) satisfying \(3n - T^2 = 129 - T^2 \geq 0\) and \(T \equiv n \mod 2\) are \(T = 1, 3, 5, 7, 9, 11\). Similarly to the previous example, we now get the following table:

<table>
<thead>
<tr>
<th>(T)</th>
<th>(\Delta = 3n - T^2)</th>
<th>(D_0)</th>
<th>(k)</th>
<th>(\ell)</th>
<th>(d = \gcd(3, n, T))</th>
<th>(T \in \mathcal{J}_3(n))?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>128</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>yes</td>
</tr>
<tr>
<td>3</td>
<td>120</td>
<td>2 \cdot 3 \cdot 5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>no: 5 (\not\equiv) 1 mod 6</td>
</tr>
<tr>
<td>5</td>
<td>104</td>
<td>2 \cdot 13</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>yes</td>
</tr>
<tr>
<td>7</td>
<td>80</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>no: 5 (\not\equiv) 1 mod 6</td>
</tr>
<tr>
<td>9</td>
<td>48</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>no: ((k, \ell) = (0, 1))</td>
</tr>
<tr>
<td>11</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>yes</td>
</tr>
</tbody>
</table>

Indeed, the only representation of 43 as a sum of three squares of positive integers is \(43 = 5^2 + 3^2 + 3^2\) (cf. Theorem 5.2(3)), from which we also easily get \(\mathcal{J}_3(43) = \{\pm 11, \pm 5, \pm 1\}\).
EXAMPLE 3.7. Let us finally determine \( \mathcal{S}_3(n) \) for \( n = 75 \). Note that here \( n = 3a^2 \) for \( t = 5 \), from which it follows by Proposition 2.2 that \( T = \pm 3t = \pm 15 \in \mathcal{S}_3(75) \). Thus, the interesting cases are the \( T \geq 0 \) satisfying \( 3n - T^2 = 225 - T^2 > 0 \) and \( T \equiv n \mod 2 \), which are \( T = 1, 3, 5, 7, 9, 11, 13 \). Using the notations from Theorem 3.4(ii) and its proof, we now get the following table:

<table>
<thead>
<tr>
<th>( T )</th>
<th>( \Delta = 3n - T^2 )</th>
<th>( D_0 )</th>
<th>( k )</th>
<th>( \ell )</th>
<th>( d = \gcd(3, n, T) )</th>
<th>( T \in \mathcal{S}_3(n) )?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>224</td>
<td>2 \cdot 7</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>yes</td>
</tr>
<tr>
<td>3</td>
<td>216</td>
<td>2 \cdot 3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>yes</td>
</tr>
<tr>
<td>5</td>
<td>200</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>yes</td>
</tr>
<tr>
<td>7</td>
<td>176</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>no: ( 11 \not\equiv 1 \mod 6 )</td>
</tr>
<tr>
<td>9</td>
<td>144</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>no: ( (k, d) = (0, 3) )</td>
</tr>
<tr>
<td>11</td>
<td>104</td>
<td>2 \cdot 13</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>yes</td>
</tr>
<tr>
<td>13</td>
<td>56</td>
<td>2 \cdot 7</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>yes</td>
</tr>
</tbody>
</table>

Indeed, the only representations of 75 as a sum of three squares of positive integers are \( 75 = 7^2 + 5^2 + 1^2 = 5^2 + 5^2 + 5^2 \), from which we easily get \( \mathcal{S}_3(75) = \{ \pm 15, \pm 13, \pm 11, \pm 5, \pm 3, \pm 1 \} \).

4. Further results on \( \mathcal{I}_m(n) \) for \( m \geq 8 \). For \( m \geq 5 \), it turns out that \( \mathcal{I}_m(n) \) only depends on the maximal value in this set. So we define

\[
T_m^*(n) = \max(\mathcal{I}_m(n)).
\]

**Proposition 4.1.** Let \( n, m \in \mathbb{N} \) with \( m \geq 5 \). If \( 0 < T \in \mathcal{I}_m(n) \), then \( T - 2 \in \mathcal{I}_m(n) \). In particular,

\[
\mathcal{I}_m(n) = \{ T \in \mathbb{Z} \mid T \equiv n \mod 2, |T| \leq T_m^*(n) \}.
\]

**Proof.** If \( T = 1 \in \mathcal{I}_m(n) \), then by symmetry \( -1 = -T = T - 2 \in \mathcal{I}_m(n) \). Hence, it suffices to consider the case \( T \geq 2 \). We use induction on \( m \). If \( m = 5 \), then the fullness of \( \mathcal{I}_m(n) \) (Theorem 3.4) implies the result. So suppose the result holds for a given \( m \geq 5 \), and let \( 2 \leq T \in \mathcal{I}_{m+1}(n) \). Then there exist \( a_i \in \mathbb{Z}, 0 \leq i \leq m \), with \( \sum_{i=0}^{m} a_i = T \geq 2 \) and \( \sum_{i=0}^{m} a_i^2 = n \).

Suppose there exists some \( i \in \{0, \ldots, m\} \) with \( a_i \leq 0 \), say \( a_0 \leq 0 \). Then \( \sum_{i=1}^{m} a_i = T - a_0 \geq T \geq 2 \). On the other hand, if \( a_i \geq 1 \) for each \( i \), then \( \sum_{i=1}^{m} a_i \geq m > 4 \). Thus, we may assume that for \( T' = \sum_{i=1}^{m} a_i \) and with \( n' = \sum_{i=1}^{m} a_i^2 \), we have \( 2 \leq T' \in \mathcal{I}_m(n') \), and by the induction hypothesis we have \( T' - 2 \in \mathcal{I}_m(n') \). So there exist \( b_i \in \mathbb{Z}, 1 \leq i \leq m \), with \( T' - 2 = \sum_{i=1}^{m} b_i \) and \( n' = \sum_{i=1}^{m} b_i^2 \), from which we get

\[
T' - 2 = a_0 + T' - 2 = a_0 + \sum_{i=1}^{m} b_i \quad \text{and} \quad n = a_0^2 + n' = a_0^2 + \sum_{i=1}^{m} b_i^2,
\]

which shows that \( T - 2 \in \mathcal{I}_{m+1}(n) \). □
Corollary 4.2. Let \( n, m \in \mathbb{N} \) with \( m \geq 5 \). Then \( \mathcal{J}_m(n) \) is full iff

\[
T_m^*(n) = \begin{cases} 
\lfloor \sqrt{mn} \rfloor & \text{if } n \equiv \lfloor \sqrt{mn} \rfloor \mod 2, \\
\lfloor \sqrt{mn} \rfloor - 1 & \text{if } n \not\equiv \lfloor \sqrt{mn} \rfloor \mod 2.
\end{cases}
\]

Proposition 4.3. Let \( m, n \in \mathbb{N} \). If \( T \in \mathcal{J}_m'(n) \), then \( T^2 \leq m(n-1)+1 \).

Proof. We may assume \( T \geq 0 \). Suppose \( T \in \mathcal{J}_m'(n) \) with \( T^2 > m(n-1)+1 \). Since by assumption \( T^2 < mn \), there exist \( \ell, k, s \in \mathbb{N}_0 \) with \( 0 \leq s \leq m-1 \) and \( 2 \leq \ell \leq m-1 \) (which forces \( m \geq 3 \)) such that

\[
T = mk + s, \quad T^2 = m(n-1) + \ell.
\]

Then

\[
T^2 = (mk + s)^2 = m^2k^2 + 2mks + s^2 \equiv s^2 \equiv \ell \mod m,
\]

and since \( \ell \not\equiv 0, 1 \mod m \), we must have \( s \not\equiv 0, \pm 1 \mod m \), so \( 2 \leq s \leq m-2 \). Note that this cannot happen for \( m \leq 3 \), so assume \( m \geq 4 \). We will show by induction that for each \( n \) we get a contradiction.

If \( n = 1 \), then \( T^2 > m(n-1)+1 = 1 \) implies \( T \geq 2 \), but \( T \in \mathcal{J}_m'(1) = \{ \pm 1 \} \), a contradiction. If \( n = 2 \), then \( T^2 > m(n-1)+1 = m+1 \geq 5 \), hence \( T \geq 3 \), but \( T \in \mathcal{J}_m'(2) = \{ 0, \pm 2 \} \), a contradiction.

So suppose \( n \geq 3 \). By assumption, \( T \in \mathcal{J}_m'(n) \), so we can find \( a_i \in \mathbb{Z} \), \( 1 \leq i \leq m \), such that

\[
T = \sum_{i=1}^{m} (k + a_i) = mk + \sum_{i=1}^{m} a_i = mk + s,
\]

(4.1)

\[
n = \sum_{i=1}^{m} (k + a_i)^2 = m^2k^2 + 2 mk \sum_{i=1}^{m} a_i + \sum_{i=1}^{m} a_i^2.
\]

From this, we get \( \sum_{i=1}^{m} a_i = s \geq 2 \) and therefore \( n \geq n' = \sum_{i=1}^{m} a_i^2 \geq 2 \) as well. In particular, \( s \in \mathcal{J}_m(n') \). Furthermore,

\[
m^2k^2 + 2mks + s^2 = T^2 = mn - m + \ell
\]

\[
= m^2k^2 + 2mks + m \sum_{i=1}^{m} a_i^2 - m + \ell,
\]

which implies

\[
s^2 = m \sum_{i=1}^{m} a_i^2 - m + \ell = m(n' - 1) + \ell
\]

and thus \( s \in \mathcal{J}_m(n') \) with \( m(n' - 1) + 1 < s^2 < mn' \). Now if \( n' < n \), this leads to a contradiction by induction (where \( T \) is replaced by \( s \)). If \( n' = n \), then (4.1) implies that necessarily \( k = 0 \) and thus \( 2 \leq T = s \leq m-2 \). If \( n \geq m-1 \), then \( T^2 \leq (m-2)(n-1) = m(n-1) - 2(n-1) < m(n-1) + \ell \), a contradiction.
If \( n \leq m - 2 \), then since \( T \in \mathcal{I}_m^l(n) \), we deduce by Proposition 2.1(iii) that \( T \leq n \), hence
\[
n^2 \geq T^2 \geq m(n - 1) + 2 \geq (n + 2)(n - 1) + 2 = n^2 + n > n^2,
\]
again a contradiction. \( \blacksquare \)

**Corollary 4.4.** Let \( m, n \in \mathbb{N} \) and \( T^* = T^*_m(n) \).

(i) \( T^{*2} = mn \) if and only if there exists an \( a \in \mathbb{N} \) with \( n = ma^2 \). In this case, if \( m \geq 5 \), then \( \mathcal{I}_m(n) = \mathcal{I}_m(ma^2) \) is full. In particular, there exist infinitely many values \( n \in \mathbb{N} \) for which \( \mathcal{I}_m(n) \) is full.

(ii) If there is no \( a \in \mathbb{N} \) with \( n = ma^2 \), then \( T^{*2} \leq m(n - 1) + 1 \).

**Remark 4.5.** Consider \( n = ma^2 \) in (i) above for \( m \geq 5 \); then \( T^*_m(n) = T^* = ma \). In this case, the maximal value in \( \mathcal{I}_m(ma^2) \) is \( ma - 2 \) by Proposition 4.4. Now obviously \( m(4a - 1) \geq 3 \), which implies that
\[
(ma - 2)^2 = m^2a^2 - 4ma + 4 \leq m^2a^2 - m + 1 = m(n - 1) + 1;
\]
this of course would also follow from Proposition 4.3.

Having dealt with those \( \mathcal{I}_m(n) \) where \( n \leq m \) or \( m \leq 7 \) in Proposition 2.1 and Theorem 3.4 respectively, we now focus on the case \( n > m \geq 8 \). We need the following technical lemma.

**Lemma 4.6.** Let \( m, n, \ell, r, s \in \mathbb{N} \) and \( s \in \mathbb{N}_0 \). Suppose that
\[
m > \ell, \quad mn > r, \quad 4((m - \ell)r - ms) > \ell m^2,
\]
and
\[
T \in \mathbb{Z} \quad | \quad T' \equiv n' \mod 2, \quad T'^2 < (m - \ell)n' - s \} \subseteq \mathcal{I}_{m-\ell}(n')
\]
for all \( n' \in \mathbb{N} \) of the shape \( n' = n - \ell k^2 \) for some \( k \in \mathbb{N} \). Then
\[
\{ T \in \mathbb{Z} \mid T \equiv n \mod 2, \quad T^2 \leq mn - r \} \subseteq \mathcal{I}_m(n).
\]

**Proof.** Let \( T \in \mathbb{N} \) with \( T \equiv n \mod 2 \) and \( T^2 \leq mn - r \). If we can find \( k \in \mathbb{Z} \) such that for \( T' = T - \ell k \) and \( n' = n - \ell k^2 \) we have \( T'^2 < (m - \ell)n' - s \) (which necessarily forces \( n' > 0 \)), then by assumption and since \( k \equiv k^2 \mod 2 \), we have \( T' \equiv n' \mod 2 \) and thus \( T' \in \mathcal{I}_{m-\ell}(n') \), i.e., there exist \( a_i \in \mathbb{Z}, 1 \leq i \leq m - 2 \), such that
\[
T' = \sum_{i=1}^{m-\ell} a_i \quad \text{and} \quad n' = \sum_{i=1}^{m-\ell} a_i^2
\]
and therefore
\[
T = \sum_{i=1}^{m-\ell} a_i + \ell \times k \quad \text{and} \quad n = \sum_{i=1}^{m-\ell} a_i^2 + \ell \times k^2,
\]
which in turn implies that \( T \in \mathcal{I}_m(n) \).
Now $T'^2 < (m - \ell)n' - s$ translates into

$$(T - \ell k)^2 < (m - \ell)(n - \ell k^2) - s,$$

or equivalently

$$mlk^2 - 2T\ell k + T^2 - n(m - \ell) + s < 0.$$ 

We can find a $k \in \mathbb{Z}$ that satisfies this inequality iff the polynomial $P(X) = mlX^2 - 2T\ell X + T^2 - n(m - \ell) + s \in \mathbb{R}[X]$ has two roots $\rho_1 < \rho_2$ in $\mathbb{R}$ and there is an integer $k$ in the open interval $][\rho_1, \rho_2[$. Now the roots are

$$\rho_{1,2} = \frac{T\ell \pm \sqrt{(m - \ell)\ell(mn - T^2) - m\ell s}}{ml},$$

and they are real and distinct if and only if $(m - \ell)(mn - T^2) - ms > 0$, in which case we have $][\rho_1, \rho_2[ \cap \mathbb{Z} \neq \emptyset$ if $\rho_2 - \rho_1 > 1$, i.e.,

$$2\sqrt{(m - \ell)\ell(mn - T^2) - m\ell s} > ml.$$

Hence, the existence of real roots $\rho_1 < \rho_2$ with $][\rho_1, \rho_2[ \cap \mathbb{Z} \neq \emptyset$ follows from (4.4)

$$4((m - \ell)(mn - T^2) - ms) > \ell m^2.$$

Now by assumption $r \leq mn - T^2$. Hence, (4.4) is certainly satisfied if

$$4((m - \ell)r - ms) > \ell m^2,$$

but this holds by our assumptions in (4.2).

**Theorem 4.7.**

(i) $\mathcal{S}_8(n)$ is full for all $n \in \mathbb{N}$.
(ii) Let $n > m \in \{9,10,11\}$. Then

$$\mathcal{S}'_m(n) = \{T \in \mathbb{Z} \mid T^2 \leq m(n - 1) + 1, T \equiv n \mod 2\}.$$

**Proof.** We apply Lemma 4.6

(i) In the case $m = 8$, we put $\ell = 1$, $s = 0$. Note that if $T \in \mathcal{S}_8(n)$ then $0 < mn - T^2 = 8n - T^2$ and $n \equiv T \mod 2$, from which we conclude by working modulo 8 that $mn - T^2 \geq 4$. So it suffices to show that we can choose $r = 4$ in the lemma in order to conclude the fullness of $\mathcal{S}_8(n)$. Now $\mathcal{S}_7(n')$ is full for all $n' \in \mathbb{N}$ by Theorem 3.4, therefore (4.3) in the lemma is satisfied, and so also is (4.2) because

$$112 = 4((m - \ell)r - ms) > \ell m^2 = 64.$$

(ii) In the case $m = 9$ we choose $\ell = 1$, and in the case $m = 10$ we choose $\ell = 2$. In both cases we put $s = 0$ and we see that (4.3) is satisfied because of the fullness of $\mathcal{S}_8(n')$ that has been established in part (i). Since $m(n - 1) + 1 = mn - (m - 1)$, we put $r = m - 1$. We then find that for $m = 9, \ell = 1, r = 8$ and $s = 0$, (4.2) is satisfied because

$$256 = 4((m - \ell)r - ms) > \ell m^2 = 81,$$
and for \( m = 10, \ell = 2, r = 9 \) and \( s = 0 \), \((4.2)\) is also satisfied because
\[
288 = 4((m - \ell)r - ms) > \ell m^2 = 200.
\]
The lemma together with Proposition \([4.3]\) then implies the result.

Let now \( m = 11 \). As before, to determine \( \mathcal{I}_1(n) \), because of Proposition \([4.3]\) we only have to check for which \( T \geq 0 \) with \( T^2 \leq m(n - 1) + 1 = 11n - 10 \) with \( T \equiv n \mod 2 \), we have \( T \in \mathcal{I}_1(n) \). But then, for parity reasons, we have either \( T^2 = 11n - 10 \) or \( T^2 \leq 11n - 12 \). Consider first the case \( T^2 = 11n - 10 \). Then \( T^2 \equiv 1 \mod 11 \), which implies that \( T \equiv \pm 1 \mod 11 \), so this case can only occur if there is a \( k \in \mathbb{N} \) with \( T = 11k \pm 1 \) (note that \( k \geq 1 \) since we assumed \( n > m \geq 11 \)). But then necessarily
\[
T^2 = 11^2k^2 \pm 2 \cdot 11k + 1 = 11n - 10
\]
and therefore \( n = 11k^2 \pm 2k + 1 \), and we get the following representations of \( n \) by sums of eleven squares:

- \( n = 11k^2 + 2k + 1 = 10 \times k^2 + (k + 1)^2 \), \( T = 11k + 1 = 10 \times k + (k + 1) \);
- \( n = 11k^2 - 2k + 1 = 10 \times k^2 + (k - 1)^2 \), \( T = 11k - 1 = 10 \times k + (k - 1) \).

So indeed, if \( T \) is such that \( T^2 = 11n - 10 \), then \( T \in \mathcal{I}_1(n) \).

Finally, consider the case where \( T^2 \leq 11n - 12 \). Here, we can argue as in the cases \( m = 8, 9, 10 \) but now with \( r = 12, \ell = 3, s = 0 \) to conclude as before:

\[
384 = 4((m - \ell)r - ms) > \ell m^2 = 363. \quad \blacksquare
\]

**Corollary 4.8.** Let \( n \in \mathbb{N} \) and \( n > m \in \{9, 10, 11\} \).

(i) If \( m = 9 \), then \( \mathcal{I}_9(n) \) is full iff \( 9n - 2 \notin \text{SOS}(1) \).

(ii) If \( m = 10 \), then \( \mathcal{I}_{10}(n) \) is full iff either \( n \) is odd and \( 10n - 1, 10n - 5 \notin \text{SOS}(1) \), or \( n \) is even and \( 10n - 4 \notin \text{SOS}(1) \).

(iii) If \( m = 11 \), then \( \mathcal{I}_{11}(n) \) is full iff \( 11n - 2, 11n - 6, 11n - 8 \notin \text{SOS}(1) \).

**Proof.** By Proposition \([4.3]\) and Theorem \([4.7]\), \( \mathcal{I}_m(n) \) not being full is equivalent to the existence of some \( T \in \mathbb{N} \) with \( m(n - 1) + 1 < T^2 < mn \) and \( T^2 \equiv T \equiv n \mod 2 \). For example, in (iii), this is equivalent to the existence of some \( T \in \mathbb{N} \) with \( 11n - 9 < T^2 < 11n - 1 \) and \( T^2 \equiv T \equiv n \equiv 11 \mod 2 \), and since \( T^2 \equiv 0, 1, 3, 4, 5, 9 \mod 11 \), this is equivalent to having some \( T \in \mathbb{N} \) with \( T^2 \in \{11n - 2, 11n - 6, 11n - 8\} \).

(i) and (ii) can be shown by similar arguments; we leave the details to the reader. \( \blacksquare \)

**Example 4.9.** Corollary \([4.8]\) states that if \( n \geq 10 \), then \( \mathcal{I}_9(n) \) not being full is equivalent to \( 9n - 2 \) being a square. The smallest such \( n \) is 19: we have \( 9 \cdot 19 - 2 = 13^2 \). One could also easily check directly that \( 13 \notin \mathcal{I}_9(19) \). But we know by Theorem \([4.7]\) that \( 11 \in \mathcal{I}_9(19) \). Indeed,
\[
19 = 4 \times 2^2 + 3 \times 1^2 = 3^2 + 2^2 + 6 \times 1^2.
\]
We easily see that we get all odd numbers $T$ between $-11$ and $11$ by suitably changing the signs of the coefficients that are being squared in these representations. Of course, this also follows from Proposition 4.7. In particular,

$$\mathcal{I}_9(19) = \{T \in \mathbb{Z} \mid T \equiv 1 \mod 2, |T| \leq 11\}.$$ 

The above also shows that $\mathcal{I}_9(n)$ is full for all $9 < n \leq 18$.

**Example 4.10.** Similarly, we find that if $n \geq 11$, then $\mathcal{I}_{10}(n)$ not being full is equivalent to the existence of some $T \in \mathbb{N}$ with $T \equiv n \mod 2$ and $T^2 \in \{10n - 1, 10n - 4, 10n - 5\}$. The smallest such $n$ is $17: 10 \cdot 17 - 1 = 13^2$. As in the previous example, we know that $11 \in \mathcal{I}_{10}(17)$: indeed,

$$17 = 3 \times 2^2 + 5 \times 1^2 = 3^2 + 8 \times 1^2$$

and hence

$$\mathcal{I}_{10}(17) = \{T \in \mathbb{Z} \mid T \equiv 1 \mod 2, |T| \leq 11\}.$$ 

The smallest such $n$ with $n$ even is $n = 20: 10 \cdot 20 - 4 = 14^2$. We observe that $12 \in \mathcal{I}_{10}(20)$:

$$20 = 4 \times 2^2 + 4 \times 1^2 = 3^2 + 2^2 + 7 \times 1^2$$

and hence

$$\mathcal{I}_{10}(20) = \{T \in \mathbb{Z} \mid T \equiv 0 \mod 2, |T| \leq 12\}.$$ 

**Example 4.11.** Similarly, we find that the smallest $n > 11$ for which $\mathcal{I}_{11}(n)$ is not full is given by $n = 18: 14^2 = 11 \cdot 18 - 2$. But we know that $12 \in \mathcal{I}_{11}(18)$. Indeed,

$$18 = 3 \times 2^2 + 6 \times 1^2 = 3^2 + 9 \times 1^2.$$ 

Hence,

$$\mathcal{I}_{11}(18) = \{T \in \mathbb{Z} \mid T \equiv 0 \mod 2, |T| \leq 12\}.$$ 

If $n \leq m$, then fullness of $\mathcal{I}_m(n)$ is dealt with in Corollary 2.4. In view of the above examples, if $n > m$ we can still expect fullness provided $n$ is ‘close’ to $m$. The following corollary also explains the above examples in more generality.

**Corollary 4.12.** Let $n, m \in \mathbb{N}$.

(i) If $10 \leq n \leq 18$, then $\mathcal{I}_9(n)$ is full. $\mathcal{I}_9(19)$ is not full.

(ii) Let $m \geq 10$. If $m < n \leq m + 6$, then $\mathcal{I}_m(n)$ is full; and $\mathcal{I}_m(m + 7)$ is not full.

**Proof.** (i) follows from the arguments in Example 4.9.

(ii) Write $T^* = T^*_m(n)$, $m < n \leq m + 7$. Under the assumptions, $n$ is not of the shape $ma^2$ for any $a \in \mathbb{N}$. Thus, for parity reasons, in order to have fullness, it is necessary and sufficient that if $c \in \mathbb{N}$ with $c = n \mod 2$, $c^2 < mn$, $(c + 2)^2 \geq mn$, then $c \in \mathcal{I}_m(n)$, in which case $T^* = c$. 


Let $n = m + k$. For $1 \leq k \leq 3$, the only $c$ satisfying these conditions is $c = n - 2 = m + k - 2$. But then we can write $n$ as a sum of $m - 3 + k \leq m$ squares as follows:

$$n = (m - 4 + k) \times 1^2 + 2^2 \quad \text{with} \quad c = m + k - 2 = (m - 4 + k) \times 1 + 2.$$  
For $4 \leq k \leq 6$, the only $c$ satisfying these conditions is $c = n - 4 = m + k - 4$. But then we can write $n$ as a sum of $m - 6 + k \leq m$ squares as follows:

$$n = (m - 8 + k) \times 1^2 + 2 \times 2^2 \quad \text{with} \quad c = m + k - 4 = (m - 8 + k) \times 1 + 2 \times 2.$$  
This shows that in all these cases, we have indeed $c \in \mathcal{I}_m(n)$, implying fullness.

Now if $n = m + 7$, then $c = m + 3$ satisfies the above conditions. But then $m(n - 1) + 1 = m^2 + 6m + 1 < c^2 = (m + 3)^2$, so $c \notin \mathcal{I}_m'(m + 7)$ by Proposition 4.3, hence $\mathcal{I}_m(m + 7)$ is not full. □

Example 4.13. For each $m \geq 9$, there exist infinitely many $n > m$ for which $\mathcal{I}_m(n)$ is not full. To show this, we just have to find $n$ and $T$ with $T \equiv n \mod 2$ and $m(n - 1) + 1 \leq T^2 < mn$.

If $m \geq 10$, let $r \in \mathbb{N}$ and put $T = 2mr + 3$ and $n = 4mr^2 + 12r + 1$. Both $n$ and $T$ are odd, and we have

$$m(n - 1) + 1 < T^2 = 4m^2 + 12mr + 9 = m(n - 1) + 9 < mn = m(n - 1) + m.$$  
Then $T \in \mathcal{I}_m(n)$ but by Proposition 4.3, $T \notin \mathcal{I}_m'(n)$.

If $m = 9$, let $r \in \mathbb{N}$ and put $T = 18r - 5$ and $n = 36r^2 - 20r + 3$. Both $n$ and $T$ are odd, and we get

$$9(n - 1) + 1 = T^2 - 6 < T^2 < T^2 + 2 = 9n.$$  
Again $T \in \mathcal{I}_m(n)$ but by Proposition 4.3, $T \notin \mathcal{I}_m'(n)$. Note that for $r = 1$, we recover the case $n = 19$ and $T = 13$ from Example 4.9.

Example 4.14. Let $n > m = 12$ and let $T \in \mathbb{N}_0$ with $T \equiv n \mod 2$. Proposition 4.3 shows that if $T^2 < mn$, then a necessary condition for $T \in \mathcal{I}_{12}(n)$ is that $T^2 \leq 12(n - 1) + 1$. However, this is in general not sufficient. Take $T = 17$ and $n = 25$. Then $17^2 = 289 = 12 \cdot 24 + 1$. One easily checks that $17 \notin \mathcal{I}_{12}(25)$. Indeed, $\mathcal{I}_{12}(25) = \{T \in \mathbb{Z} \mid T \equiv 1 \mod 2, |T| \leq 15\}$. The value 15 can be obtained from the representations

$$25 = 5 \times 2^2 + 5 \times 1^2 = 3^2 + 2 \times 2^2 + 8 \times 1^2.$$  

Problem 4.15. If $m \geq 5$, then knowing $T_m^*(n)$ yields a full description of $\mathcal{I}_m(n)$ by Proposition 4.1. Thus, we obtain the following rather natural problem: Find an explicit description or formula for $T_m^*(n)$ in terms of (properties of) $m$ and $n$.

5. Variations of the problem. In this section we consider a variation of the original problem concerning sums of four squares. This problem has
been studied by Z.-W. Sun et al. in a series of papers [7–10]. The purpose of this section is to show how our methods, in particular Mordell’s results on sums of squares of linear forms, can be used to recover and extend some of the results by Z.-W. Sun et al.

First, we generalize some of the problems they consider to \( m \) squares for \( m \in \mathbb{N} \). Let \((a_1, \ldots, a_m) \in \mathbb{Z}^m \setminus \{(0, \ldots, 0)\}\) and \( n \in \mathbb{N} \). This time, we ask for which \( T \in \mathbb{Z} \) the following system of diophantine equations has a solution \((x_1, \ldots, x_m) \in \mathbb{Z}^m:\)

\[
\begin{align*}
    a_1 x_1 + a_2 x_2 + \cdots + a_m x_m &= T, \\
    x_1^2 + x_2^2 + \cdots + x_m^2 &= n.
\end{align*}
\]

(5.1)

Note that the solvability of (5.1) with \( x_i \in \mathbb{Z} \) is invariant under sign changes of the \( a_i \) (just change the signs of the corresponding \( x_i \)) and permutation of the indices, so that we may assume from now on that

\[
a_1 \geq \cdots \geq a_m \geq 0, \quad a_1 \geq 1.
\]

We define

\[
A(x_1, \ldots, x_m) = \sum_{i=1}^{m} a_i x_i \in \mathbb{Z}[x_1, \ldots, x_m] \quad \text{and} \quad a = \sum_{i=1}^{m} a_i^2.
\]

In analogy to what was done before, we define

\[
\mathcal{S}_{m,A}(n) = \{ T \in \mathbb{Z} \mid \text{ (5.1) has a solution } x \in \mathbb{Z}^m \}.
\]

**Proposition 5.1.** Let \( n, m, a, A \) be as above, and let \( T \in \mathbb{Z} \). Let \( d = \gcd(a_1, \ldots, a_m) \in \mathbb{N} \) and let \( a_i = d a_i' \). Put \( a' = \sum_{i=1}^{m} a_i'^2 \), so in particular \( a = d^2 a' \).

(i) If \( T \in \mathcal{S}_{m,A}(n) \), then \( T^2 \leq an \).

(ii) \( T \in \mathcal{S}_{m,A}(n) \) with \( T^2 = an \) if and only if there exists \( b \in \mathbb{N} \) with \( n = a'b^2 \), in which case \( T \in \{ \pm a'bd \} \).

**Proof.**

(i) follows from the Cauchy–Schwarz inequality as in (1.3) with 1 replaced by \( a = (a_1, \ldots, a_m) \) and \( m \) replaced by \( a \).

(ii) Put \( a' = (a_1', \ldots, a_m') \), so that \( a = d(a_1', \ldots, a_m') \). If \( n = a'b^2 \), then \( an = a'^2 b^2 d^2 = (a'bd)^2 \). For \( x = \pm (ba_1', \ldots, ba_m') \) we then have \( x \cdot x = n \) and \( A(x) = a \cdot x = \pm a'bd \in \mathcal{S}_{m,A}(n) \).

Conversely, if \( T \in \mathcal{S}_{m,A}(n) \) with \( T^2 = an \), then there exists \( x \in \mathbb{Z}^m \) with \( n = x \cdot x \) and \( an = (a \cdot x)^2 \). Since \( a \cdot a = a \), we have equality in the Cauchy–Schwarz inequality, which implies that \( x \) depends linearly on \( a \) and hence on \( a' \). Since \( x, a' \) have coefficients in \( \mathbb{Z} \) and because \( \gcd(a_1', \ldots, a_m') = 1 \), there exists \( b \in \mathbb{Z} \) such that \( x = ba' \), hence \( n = x \cdot x = a'b^2 \) and \( T = A(x) = a \cdot x = a'bd \). □
Similarly to what we did in Section 2, we define
\[ \mathcal{S}'_{m,A}(n) = \{ T \in \mathcal{S}_{m,A}(n) \mid T^2 < an \}. \]
Note that \( T \in \mathcal{S}_{m,A}(n) \) if and only if there exists \( (x_1, \ldots, x_m) \in \mathbb{Z}^m \) such that
\[ aX^2 + 2TXY + nY^2 = \sum_{i=1}^{m} (a_i X + x_i Y)^2 \in \mathbb{Z}[X,Y]. \]
Thus, a necessary condition for \( T \in \mathcal{S}_{m,A}(n) \) is that one can find \( \alpha_i, \beta_i \in \mathbb{Z} \) such that
\[ aX^2 + 2TXY + nY^2 = \sum_{i=1}^{m} (\alpha_i X + \beta_i Y)^2 \in \mathbb{Z}[X,Y]. \]

Proposition 3.2 and Theorem 3.3 tell us exactly when this necessary condition is satisfied. However, this condition is generally not sufficient. But there are cases where sufficiency also holds. Note first that in (5.2), we may again assume (after permuting the summands and changing signs if necessary) that \( \alpha_1 \geq \cdots \geq \alpha_m \geq 0 \). If \( a = \sum_{i=1}^{m} a_i^2 \) is essentially the only decomposition of \( a \) into a sum of \( m \) squares, i.e., if for any other decomposition \( a = \sum_{i=1}^{m} \alpha_i^2 \) with \( \alpha_i \in \mathbb{Z} \) and \( \alpha_1 \geq \cdots \geq \alpha_m \geq 0 \), we have \( a_i = \alpha_i, 1 \leq i \leq m \), then the solvability of (5.2) will be equivalent to the solvability of (5.1).

This leads to the definition of the partition number \( P_m(n) \) for \( n, m \in \mathbb{N} \):
\[ P_m(n) = \left| \left\{ (a_1, \ldots, a_m) \in \mathbb{N}_0^m \mid a_1 \geq \cdots \geq a_m, \sum_{i=1}^{m} a_i^2 = n \right\} \right|, \]
the number of essentially different partitions of \( n \) into \( m \) integer squares.

D. H. Lehmer [4] studied the question for which \( n \) one has \( P_m(n) = 1 \). He gave a full solution for \( m \neq 3 \), and he provided a conjecture for \( m = 3 \). This conjecture was later confirmed (albeit with a correction) by Bateman and Grosswald [2]. Their proof uses the classification of discriminants of binary quadratic forms of class number \( \leq 4 \), which was itself a conjecture at the time and was fully established only later by Arno [1]. Here is the complete result.

**Theorem 5.2.** Let \( n, m \in \mathbb{N} \).

(1) \( P_1(n) = 1 \) iff \( n \in \text{SOS}(1) \).
(2) \( P_2(n) = 1 \) iff \( n = 2^k q^2, \ 2^k q^2 p \) where \( k \in \mathbb{N}_0, q \in \mathbb{N} \) is an odd integer having only prime factors \( \equiv 3 \) mod 4, and \( p \) is a prime with \( p \equiv 1 \) mod 4.
(3) \( P_3(n) = 1 \) iff \( n = 4^c k \) with \( k \in \mathbb{N}_0 \) and \( c = 1, 2, 3, 5, 6, 10, 11, 13, 14, 19, 21, 22, 30, 35, 37, 42, 43, 46, 58, 67, 70, 78, 91, 93, 115, 133, 142, 163, 190, 235, 253, 403, 427 \).
(4) \( P_4(n) = 1 \) iff \( n = 1, 3, 5, 7, 11, 15, 23, 2 \cdot 4^k, 6 \cdot 4^k, 14 \cdot 4^k \) with \( k \in \mathbb{N}_0 \).
(5) \( P_5(n) = 1 \) iff \( n = 1, 2, 3, 6, 7, 15 \).
(6) \( P_6(n) = 1 \) iff \( n = 1, 2, 3, 7 \).
(7) Let \( m \geq 7 \). Then \( P_m(n) = 1 \) iff \( n = 1, 2, 3 \).
Back to our original problem, let

- \( a_i \in \mathbb{N}_0, 1 \leq i \leq m, \) with \( 0 \neq a_1 \geq \cdots \geq a_m, \)
- \( (5.3) \) \( A(x_1, \ldots, x_m) = \sum_{i=1}^{m} a_i x_i, \)
- \( a = \sum_{i=1}^{m} a_i^2. \)

Together with the preceding remarks, we have now established the following.

**Proposition 5.3.** Let \( n, m \in \mathbb{N} \) and let \( a_i, A \) be as in \((5.3)\). If \( T \in \mathcal{J}_{m,A}(n) \), then there exist \( \alpha_i, \beta_i \in \mathbb{Z}, 1 \leq i \leq m \), that satisfy \((5.2)\). The converse holds if in addition \( P_m(a) = 1. \)

In [7]–[10], the authors study the sets \( \mathcal{J}_{n,A}(n) \) for certain linear polynomials \( A \in \mathbb{Z}[x_1, x_2, x_3, x_4] \) as above. They give (partial) results on the existence of certain types of elements contained in \( \mathcal{J}_{n,A}(n) \). The following corollary allows one to easily recover and to extend their results in that context.

**Corollary 5.4.** Let \( n \in \mathbb{N} \) and let \( a_i, A \) be as in \((5.3)\) with \( m = 4. \) Assume \( P_4(a) = 1. \) Then

\[
\mathcal{J}_{4,A}(n) = \{ T \in \mathbb{Z} \mid 0 < an - T^2 \in \text{SOS}(3) \}.
\]

If \( \gcd(a_1, a_2, a_3, a_4) = d \in \mathbb{N} \) and there exists \( b \in \mathbb{N} \) with \( n = ab^2d^{-2}, \) then \( \mathcal{J}_{4,A}(n) = \mathcal{J}_{4,A}(n) \cup \{ \pm abd^{-1} \} \). Otherwise, \( \mathcal{J}_{4,A}(n) = \mathcal{J}_{4,A}(n). \)

**Proof.** This follows readily from Propositions 5.1 and 5.3 together with Theorem 3.3(iii).}

**Example 5.5.** Sun et al. studied polynomials of the type \( A(x_1, x_2, x_3, x_4) = \sum_{i=1}^{4} a_ix_i \) with \( P_4(\sum_{i=1}^{4} a_i^2) = 1, \) for example \( (a_1, a_2, a_3, a_4) = (1, 1, 0, 0) \) ([8, Th. 1.2(i)]), \( (2, 1, 0, 0) \) ([8, Th. 1.2(iii)]), \( (3, 2, 1, 1) \) ([7, Th. 1.5]), \( (2, 1, 1, 1) \) ([7, Th. 1.7(ii)]), \( (3, 2, 1, 0) \) ([7, Th. 1.7(iv)]), \( (2, 1, 1, 0) \) ([9, Th. 1.4(i)]). They proved various results of the type that \( \mathcal{J}_{4,A}(n) \) contains a square, or twice a square, or a cube, or twice a cube, or a power of 4, or a power of 8, etc. We refrain from presenting their results in detail. Suffice it to say that all these types of results for the above mentioned polynomials can now be readily checked or recovered using our explicit and complete description of \( \mathcal{J}_{4,A}(n) \) in all these cases by Corollary 5.4.

Just as an illustration, let us consider the case \( (3, 1, 1, 0) \). We will show that \( \mathcal{J}_{4,A}(n) \) always contains a power of 4. By Corollary 5.4 it suffices to show that \( 11n - (4^m)^2 \in \text{SOS}(3) \) for some \( m \in \mathbb{N}_0 \) to conclude that \( 4^m \in \mathcal{J}_{4,A}(n). \)

Below is a list of such elements \( T = 4^m, \) where \( 11n = 4^{2t+r}(8k+s) \) with \( t, k \in \mathbb{N}_0, r \in \{0, 1\}, s \in \{1, 2, 3, 5, 6, 7\}. \) Note that then 11 must divide \( 8k + s, \) so \( 8k + s \geq 11, \) hence \( 8k + s - 2^\ell > 0 \) for \( \ell \leq 3, \) and if \( s \neq 3, \) then \( 8k + s \geq 22, \) in which case \( 8k + s - 2^\ell > 0 \) for \( \ell \leq 4. \)
For example, if $11n = 4^{2t+1}(8k + s)$ with $s \neq 2, 6$, then $11n - (4^t)^2 = 4^{2t}(32k + 4s - 1)$ with $32k + 4s - 1 \equiv 3 \mod 8$, which shows that indeed $11n - (4^t)^2 \in \text{SOS}(3)$.

Acknowledgments. I am grateful to Professor Zhi-Wei Sun for pointing out an error in an earlier version of this article.

I also thank an anonymous referee for the careful reading of the article and for useful suggestions and corrections.

The author is supported in part by DFG grant HO 4784/2-1 Quadratic forms, quadrics, sums of squares and Kato’s cohomology in positive characteristic.

References


Detlev W. Hoffmann
Fakultät für Mathematik
Technische Universität Dortmund
D-44221 Dortmund, Germany
E-mail: detlev.hoffmann@math.tu-dortmund.de