이학석사 학위논문

A sum of suqares of integers with special property

(특별한 성질을 가지는 제곱수의 합)

2023년 **8**월

서울대학교 대학원

수리과학부

김 기 석

A sum of suqares of integers with special property

(특별한 성질을 가지는 제곱수의 합)

지도교수 오 병 권

이 논문을 이학석사 학위논문으로 제출함

2023년 **4**월

서울대학교 대학원

수리과학부

김 기 석

김 기 석의 이학석사 학위논문을 인준함

2023년 **6**월

위 원 장 ______________________ (인)

부 위 원 장 ______________________ (인)

위 원 ______________________ (인)

A sum of suqares of integers with special property

A dissertation
submitted in partial fulfillment
of the requirements for the degree of
Master of Science
to the faculty of the Graduate School of
Seoul National University

by

Kisuk Kim

Dissertation Director : Professor Byeong-Kweon Oh

Department of Mathematical Sciences
Seoul National University

August 2023

Abstract

In this thesis, we consider two topics about a sum of squares. First, we prove that every natural number can be written as a sum of at most 6 squares of integers not divisible by 3. Second, we study a sum of squares whose domain is the set of all integers except for a fixed integer. For beginning, we check that whether every natural number can be written as a sum of squares except for 1 or 4 and for each case, find the infimum of the number of squares needed to represent every natural number. At the end, we consider the same question for arbitrary positive integer.

Key words: Sums of squares, quadratic forms, representations
Student Number: 2020-21303

Contents

Chapter 1

Introduction

The famous Lagrange's Four Square Theorem says that every natural number n can be written as a sum of four squares of integers. This theorem was generalized in many directions including Waring's problem. In this thesis, we focus on a sum of squares of integers with some special conditions. In fact, Kim and Oh considered in [6] such kind of a problem. They found the smallest integer k such that every natural number is a sum of k squares of integers which are not divisible by a prime p for any prime p. They denote the smallest integer k satisfying above property by $S(p)$ for any prime p.

Theorem 1.1.1. (Kim and Oh, [6]) *Every natural number can be written as a sum of at most* 6 *squares of integers not divisible by* 3*, that is,* $S(3) = 6$.

To prove this, they use Minkowski-Siegel formula. In this thesis, we provide a purely arithmetic proof of this theorem.

Note that if $n = \sum_{i=1}^{k} a_i^2$ for some integer a_i, then clearly, $4^m n = \sum_{i=1}^{k} (2^m a_i)^2$. So, without loss of generality, we may assume that $\mathrm{ord}_2(n) = 0, 1$ to prove the above theorem. In chapter 4, we provide the arithmetic proof of $S(3) = 6$, as mentioned above. To do this, we prove two propositions given below.

Proposition 1.1.2. *Let N be a natural number such that $ord_2(N) = 1$. Then N is a sum of at most 6 squares of integers not divisible by 3.*

Proposition 1.1.3. *Let N be a natural number such that $ord_2(N) = 0$. Then N is a sum of at most 6 squares of integers not divisible by 3.*

Clearly, Theorem 1.1.1 is a direct consequence of these two propositions

For the second problem which we are considering in this thesis, we define for any positive integer ρ,

$$S_\rho := \mathbb{N} - \{\rho\},$$

where $\mathbb{N}$ is the set of positive integers. For any positive integer n, we define

$$k_\rho(n) := \min\{m \mid n = x_1^2 + \cdots + x_m^2,\ x_i \in S_\rho\}.$$

If such a k does not exist for given ρ, n, we define $k_\rho(n) = \infty$. For example, $3 = 1^2 + 1^2 + 1^2$ can be written as a sum of three squares of 1. However we can not write 3 as a sum of squares of integers greater than 1. So in this situation, we can conclude that $k_1(3) = \infty$. We also define

$$I(\rho) := \{n : k_\rho(n) = \infty\} \text{ and } M(\rho) := \max\{k_\rho(n) : n \notin I(\rho)\}.$$

In this thesis, we try to find the integer $M(\rho)$ for various positive integers ρ. For example, we prove that $M(1) = 6$ in Chapter 4.

Chapter 2

Preliminaries

2.1 Basic notations and definitions

Let $\mathbb{Z}$ and $\mathbb{Q}$ denote the ring of integers and the field of rational numbers, respectively. For each finite prime p, we use $\mathbb{Z}_p$, $\mathbb{Q}_p$ to denote their p-adic completion, respectively. Finally, $\mathbb{R} = \mathbb{Q}_\infty$ denotes the field of real numbers.

Let R be the ring of integers $\mathbb{Z}$ or the ring of p-adic integers $\mathbb{Z}_p$. Then, any free R-module of finite rank equipped with a non-degenerate symmetric bilinear form is called a lattice over R or an R-lattice. Let L be a lattice over R equipped with a non-degenerate symmetric bilinear form $B : L \times L \to R$. The corresponding quadratic form Q is defined by

$$Q(x) = B(x, x) \quad \text{for any} \quad x \in L.$$

Let $e_1, e_2 \cdots, e_n$ be a basis for L. Then an $n \times n$ matrix M_L defined by

$$M_L := (B(e_i, e_j))$$

is called the Gram matrix of L, and we write

$$L \cong M_L.$$

For another basis $f_1, f_2 \cdots, f_n$ for L, there is an $n \times n$ matrix $T = (t_{ij})$ with $t_{ij} \in R$ which is called the transition matrix such that $\det T \in R^\times$ and

$$(B(e_i, e_j)) = T^t) B(f_i, f_j))T.$$

The determinant of the Gram matrix, which is unique up to unit squares, is called the discriminant of L. From now on, we fix $\{e_1, e_2, \cdots, e_n\}$ as a basis for L.

Let $L_1, L_2, \cdots, L_m$ be sublattices of L over R. We define

$$B(L_i, L_j) := \{B(x, y) \mid x \in L_i, \ \ y \in L_j\}.$$

For lattices $L, L_1, L_2, \cdots, L_m$ such that $L = L_1 \oplus L_2 \oplus \cdots \oplus L_m$ with $B(L_i, L_j) = 0$ for any i, j with $i \neq j$, we say that L is the orthogonal sum of $L_1, L_2, \cdots, L_m$ and we write

$$L = L_1 \perp L_2 \perp \cdots \perp L_m.$$

For a subset S of L, we define $S^\perp$, the orthogonal complement of S by

$$S^\perp := \{x \in L \mid B(x, s) = 0 \ \text{ for any } \ s \in S\}.$$

For two lattices L_1, L_2, we say that L_1 is represented by L_2 if there exists a linear map

$$\sigma : L_1 \to L_2 \text{ such that } B(x,y) = B(\sigma(x), \sigma(y)) \text{ for any } x, y \in L_1,$$

and in this case, we write $L_1 \to L_2$. We say that an element $r \in R$ is represented by a lattice L to indicate the existence of a vector $x \in L$ such that $Q(x) = r$. Here we define a special lattice

$$A_3 \cong \begin{bmatrix} 2 & 1 & -1 \\ 1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}$$

for later use.

We may write any nonnegative integer $n = 4^\alpha(8\beta+\gamma)$ for some nonnegative integers α, β, γ. Moreover, we may assume that $0 \le \gamma \le 7$. Throughout this thesis, we always assume that a, b, c are integers. In particular, a, b, c are either 0 or integers not divisible by 3 in Chapter 3.

2.2 Lemmas

In this section, we collect some lemmas which are useful in the sequel. The first lemma is known as Three Square Theorem.

Lemma 2.2.1 (Three Square Theorem). *Let n be a natural number. Then n can be represented as a sum of three squares if and only if*

$$n \ne 4^\alpha(8\beta + 7),$$

where α, β are nonnegative integers.

For the proof of Lemma 2.2.1, one may see [3].

The following second and third lemmas will be used in Chapter 5. In particular, Lemma 2.2.4 is called Cauchy's lemma.

Lemma 2.2.2. *Any even natural number n is represented by the quadratic form A_3 defined above if and only if*

$$n \neq 4^k(8m+7)$$

for nonnegative integers k, m.

Remark 2.2.3. *It is also well-known that any odd natural number can not be represented by A_3. For more information on the quadratic form A_n for a natural number n, one may see [2] and [4].*

Lemma 2.2.4 (Cauchy's Lemma)**.** *Let a and b be odd positive integers such that*

$$b^2 < 4a.$$

Then there exist integers s, t, u, v such that

$$a = s^2 + t^2 + u^2 + v^2 \text{ and } b = s + t + u + v.$$

Remark 2.2.5. *This is actually part of Cauchy's lemma. The original one has additional condition*

$$3a < b^2 + 2b + 4$$

to guarantee non-negativities of s, t, u, v. The proof of this lemma can be found in [3].

Here is one more lemma. This is proved by Kim and Oh in [6].

Lemma 2.2.6. *Let $p \neq 2, 3$ be a prime. Then every natural number n can be written as a sum of at most 4 squares of integers all of which are not divisible by p, except for the case when $p = 5$ and $n = 79$.*

Jacobi's four square theorem is the last lemma which we need in this thesis. One may find this theorem in [7].

Lemma 2.2.7 (Jacobi's Four Square Theorem)**.** *Let $r_4(n)$ denote the number of ways to represent a natural number n as the sum of four squares. Then $r_4(n)$ is eight times the sum of the divisors of n if n is odd and 24 times the sum of the odd divisors of n if n is even. It is also true that $r_4(n)$ is eight times the sum of all divisors which are not divisible by 4.*

Chapter 3

Proof of Theorem 1.1.1

In this chapter, we will prove Theorem 1.1.1. To prove the theorem, we divide it into several cases, and we prove each case separately. In Section 3.1, we will consider the case when n is even. In Sections 3.2 and 3.3, we will consider the case when n is odd.

3.1 Proof of Proposition 1.1.2

In this section, we prove Proposition 1.1.2.

First, assume that $n \equiv 3, 6 \pmod 9$. Here we can write

$$n = 2(8\beta + \gamma) = 8 \times 2\beta + 2\gamma$$

for nonnegative integers β, γ. Note that $\gamma = 1, 3, 5, 7$, for we are assuming that $\mathrm{ord}_2(n) = 1$. Now, n can be written as a sum of three squares by Lemma

2.2.1. Hence we have

$$n = a^2 + b^2 + c^2$$

for some integers a, b, and c. If one of a, b, c is divisible by 3, then $n \not\equiv 3, 6 \pmod 9$. Therefore n is a sum of three squares of integers not divisible by 3, which implies the theorem in this case.

Now, assume that $n \equiv 0 \pmod 9$. Here we can write

$$n = 2(8\beta + \gamma) = 8 \times 2\beta + 2\gamma$$

for nonnegative integers β, γ with $\gamma = 1, 3, 5, 7$. If $\gamma = 1, 5$, then we have $n - 12 \equiv 6 \pmod 9$. At the same time, $n - 12 \equiv 6 \pmod 8$. Furthermore, since $9 = 2^2 + 2^2 + 1$, we may assume that $n \geq 18$. Hence

$$n = 2^2 + 2^2 + 2^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3. If $\gamma = 3, 7$, then $n - 12 \equiv 6 \pmod 9$ and $n - 12 \equiv 2 \pmod 8$. Hence

$$n = 2^2 + 2^2 + 2^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

Suppose that $n \not\equiv 0 \pmod 3$. Now, we consider the case when $n \equiv 1, 2, 4, 5, 7, 8 \pmod 9$. Again we may write

$$n = 8 \times 2\beta + 2\gamma$$

for nonnegative integers β, γ with $\gamma = 1, 3, 5, 7$. First, assume that $n \equiv 1$

(mod 9). Note that $8 \times 2\beta + 2\gamma \geq 4$ and $n - 4 = 8 \times 2\beta + 2\gamma - 4 \equiv 6 \pmod 9$. At the same time, $8 \times 2\beta + 2\gamma - 4 \equiv 2, 6 \pmod 8$. Hence we can write

$$n = 2^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

Assume that $n \equiv 4 \pmod 9$. Then $n - 1 = 8 \times 2\beta + 2\gamma - 1 \equiv 3 \pmod 9$. Since $\gamma = 1, 3, 5, 7$, we have $2\gamma - 1 = 1, 5 \pmod 8$. Hence we can write

$$n = 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

The case of $n \equiv 7 \pmod 9$ is quite similar to the above. Note that $n - 4 = 8 \times 2\beta + 2\gamma - 4 \equiv 3 \pmod 9$. Since $\gamma = 1, 3, 5, 7$, we have $2\gamma - 4 = 2, 6 \pmod 8$. Hence we can write

$$n = 2^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

Now, consider the case when $n \equiv 2 \pmod 9$. We assume that $n > 5$. Then $n - 5 = 8 \times 2\beta + 2\gamma - 5 \equiv 6 \pmod 9$. Since $2\gamma - 5 \equiv 1, 5 \pmod 8$, we have

$$n = 2^2 + 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3. If $n = 2$, then clearly, $n = 1^2 + 1^2$.

Let $n \equiv 5 \pmod 9$. If $n > 8$, then $n - 8 = 8 \times 2\beta + 2\gamma - 8 \equiv 6 \pmod 9$.

At the same time, $n - 8 \equiv 2, 6 \pmod 8$. Hence we can write

$$n = 2^2 + 2^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3. If $n = 5$, then clearly, $n = 2^2 + 1^2$.

Let $n \equiv 8 \pmod 9$. $n - 5 = 8 \times 2\beta + 2\gamma - 5 \equiv 3 \pmod 9$. Note that $2\gamma - 5 \equiv 1, 5 \pmod 8$. Hence

$$n = 2^2 + 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which are divisible by 3.

3.2 The first part of the proof of Proposition 1.1.3

In Sections 3.2 and 3.3, we prove Proposition 1.1.3. For convenience, we consider the cases when $\gamma = 1, 3,$ and 5 in this section, and the case when $\gamma = 7$ will be considered in the next section.

First, suppose $n \equiv 3, 6 \pmod 9$. Since $\gamma \neq 7$, we can write

$$n = a^2 + b^2 + c^2$$

for some integers $a, b,$ and c. Note that none of a, b, c is divisible by 3 because $n \equiv 3, 6 \pmod 9$.

Now, suppose $n \equiv 0 \pmod 9$. In this case, $n = 8\beta + \gamma \equiv 0 \pmod 9$. If

$\gamma = 1, 5$, then $n - 3 \equiv 6 \pmod 9$ and $n - 3 \equiv 6, 2 \pmod 8$. Hence

$$n = 1^2 + 1^2 + 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3. If $\gamma = 3$, then $n - 6 \equiv 3 \pmod 9$ and $n - 6 \equiv 5 \pmod 8$. Therefore

$$n = 2^2 + 1^2 + 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

Suppose that $n \not\equiv 0 \pmod 3$. Then $n = 8\beta + \gamma \equiv 1, 2, 4, 5, 7, 8 \pmod 9$ with $\gamma = 1, 3, 5$. First, assume that $n \equiv 1 \pmod 9$. If $n \geq 19$, then $n - 4^2 = n - 16 = 8(\beta - 2) + \gamma \equiv 3 \pmod 9$. Hence we have

$$n = 4^2 + a^2 + b^2 + c^2$$

for some integers a, b, and c, none of which is divisible by 3. If $n < 19$, then $n = 1^2$ which is already a square not divisible by 3.

Let $n \equiv 4 \pmod 9$. If $n \geq 31$, then $n - 16 = 8(\beta - 2) + \gamma \equiv 6 \pmod 9$. Hence we have

$$n = 4^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3. If $n < 31$, then $n = 13$ which can be written as $13 = 2^2 + 2^2 + 2^2 + 1^2$.

Let $n \equiv 7 \pmod 9$. If $n \geq 79$, then $n - 64 = 8(\beta - 8) + \gamma \equiv 6 \pmod 9$. Hence we have

$$n = 8^2 + a^2 + b^2 + c^2$$

for some integers a, b, and c, none of which is divisible by 3. If $n < 79$, then $n = 25, 43, 61$. Note that $25 = 4^2 + 2^2 + 2^2 + 1^2$, $43 = 5^2 + 4^2 + 1^2 + 1^2$ and $61 = 7^2 + 2^2 + 2^2 + 2^2$.

Let $n \equiv 2 \pmod 9$. The least n is 11 and so $\beta \geq 1$. Then $n - 8 = 8(\beta - 1) + \gamma \equiv 3 \pmod 9$. Hence we can write

$$n = 2^2 + 2^2 + a^2 + b^2 + c^2$$

for some integer a, b and c, none of which is divisible by 3.

Let $n \equiv 5 \pmod 9$. If $n \geq 41$, then $n - 8 = 8(\beta - 1) + \gamma \equiv 6 \pmod 9$. Hence we have

$$n = 2^2 + 2^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3. If $n < 41$, then $n = 5$ and we have $5 = 2^2 + 1^2$.

Let $n \equiv 8 \pmod 9$. If $\gamma = 3, 5$, then $n - 2 = 8\beta + \gamma - 2 \equiv 6 \pmod 9$. Hence we have

$$n = 1^2 + 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3. Suppose $\gamma = 1$. If $n \geq 89$, then $n - 20 = 8(\beta - 3) + 5 \equiv 6 \pmod 9$. Hence we have

$$n = 4^2 + 2^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3. If $n < 89$, then $n = 17$ and we have $17 = 4^2 + 1^2$.

3.3 The second part of the proof of Proposition 1.1.3

As mentioned above, we will consider the case when $\gamma = 7$. So, we assume that $n = 8\beta + 7$ for some integer β throughout this section.

First, suppose $n \equiv 3, 6 \pmod 9$. Let $n = 8\beta + 7 \equiv 3 \pmod 9$. Then $n - 6 = 8\beta + 1 \equiv 6 \pmod 9$. Hence we have

$$n = 2^2 + 1^2 + 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3. Now, let $n = 8\beta + 7 \equiv 6 \pmod 9$. Then $n - 9 = 8(\beta - 1) + 6 \equiv 6 \pmod 9$. Hence we have

$$n = 2^2 + 2^2 + 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

Now, suppose that $n \equiv 0 \pmod 9$. Let $n = 8\beta + 7 \equiv 0 \pmod 9$. Then $n - 6 = 8\beta + 1 \equiv 3 \pmod 9$. Hence we have

$$n = 2^2 + 1^2 + 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

Suppose that $n \not\equiv 0 \pmod 3$. Then we have $n = 8\beta + 7 \equiv 1, 2, 4, 5, 7, 8 \pmod 9$. First, assume that $n \equiv 1 \pmod 9$. Then $n - 4 = 8\beta + 3 \equiv 6 \pmod 9$. Hence we have

$$n = 2^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

If $n \equiv 2 \pmod 9$, then $n - 5 = 8\beta + 2 \equiv 6 \pmod 9$. Hence we have

$$n = 2^2 + 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

If $n \equiv 4 \pmod 9$, then $n - 1 = 8\beta + 6 \equiv 3 \pmod 9$. Hence we have

$$n = 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

If $n \equiv 5 \pmod 9$, then $n - 2 = 8\beta + 5 \equiv 3 \pmod 9$. Hence we have

$$n = 1^2 + 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

If $n \equiv 7 \pmod 9$, then $n - 1 = 8\beta + 6 \equiv 6 \pmod 9$. Hence we have

$$n = 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

If $n \equiv 8 \pmod 9$, then $n - 2 = 8\beta + 5 \equiv 6 \pmod 9$. Hence we have

$$n = 1^2 + 1^2 + a^2 + b^2 + c^2$$

for some integers a, b and c, none of which is divisible by 3.

Hence every natural number n is a sum of at most six squares of integers not divisible by 3. In fact, one may easily show that 15 is not a sum of five squares of integers not divisible by 3. Note that $15 = 2^2 + 2^2 + 2^2 + 1^2 + 1^2 + 1^2$

is a sum of six squares of integers not divisible by 3.

Chapter 4

$I(1)$ and $M(1)$

Since we define $S_1 = \{2, 3, 4, \ldots\}$, we have $a^2 \geq 4$ for any $a \in S_1$. Hence $1, 2, 3 \in I(1)$, which implies that $I(1)$ is not empty.

Theorem 4.1.1. *There are exactly* 12 *positive integers which are not a sum of squares of integers greater than* 1*. More precisely, we have*

$$I(1) = \{1, 2, 3, 5, 6, 7, 10, 11, 14, 15, 19, 23\}.$$

Theorem 4.1.2. *Any integer which is a sum of squares of integers greater than* 1 *is a sum of at most six squares of integers greater than* 1*. That is,*

$$M(1) = 6.$$

In fact, we will prove that $I(1) = \{1, 2, 3, 5, 6, 7, 10, 11, 14, 15, 19, 23\}$ and $M(1) = 6$ by using Lemmas 2.2.2 and 2.2.4.

If an integer $n = \sum_{i=1}^{k} a_i^2$ for some integers a_i, then we may also write

$4n = \sum_{i=1}^{k} (2a_i)^2$. The following proposition is a key ingredient of the proof.

Proposition 4.1.3. *Let ρ be any positive integer. Then there exists a natural number n_ρ satisfying the following condition: If $n > n_\rho$, then n is a sum of at most four squares of integers all of which are contained in S_ρ.*

Proof. First, assume that $n \equiv 2 \pmod 4$. Choose a nonnegative integer m such that

$$4m^2 \le n < 4(m+1)^2.$$

Since $n - 4m^2 \equiv 2 \pmod 4$, it is represented by the ternary quadratic form A_3 by Lemma 2.2.2. So, there are integers α, β, γ such that

$$n - 4m^2 = \alpha^2 + \beta^2 + \gamma^2 + (\alpha + \beta - \gamma)^2.$$

If we write $\alpha + \beta - \gamma = \delta$, then we have $\alpha + \beta - \gamma - \delta = 0$ so that

$$n = (m+\alpha)^2 + (m+\beta)^2 + (m-\gamma)^2 + (m-\delta)^2.$$

Note that $n - 4m^2 < 8m + 4$. Hence we have

$$-\sqrt{8m+4} < \alpha, \beta, \gamma, \delta < \sqrt{8m+4}.$$

This implies that $n = x^2 + y^2 + z^2 + w^2$ has an integer solution (a, b, c, d) such that $a, b, c, d \in (m - \sqrt{8m+4}, m + \sqrt{8m+4})$. Hence if n is big enough so that $m - \sqrt{8m+4} > \rho$, then all of a, b, c, d are greater than ρ.

Now, assume that $n \equiv 1, 3 \pmod 4$. First, take a nonnegative integer m satisfying

$$4m^2 + 2m \le n < 4(m+1)^2 + 2(m+1).$$

Consider the system of diophantine equations,

$$\begin{cases} n - (4m^2 + 2m) = x^2 + y^2 + z^2 + w^2, \\ 1 = x + y + z + w. \end{cases}$$

If this system of diophantine equations has a solution $(\alpha, \beta, \gamma, \delta)$, then we have four integers $\alpha, \beta, \gamma, \delta$ such that $\alpha + \beta + \gamma + \delta = 1$ and

$$n = (m+\alpha)^2 + (m+\beta)^2 + (m+\gamma)^2 + (m+\delta)^2 = 4m^2 + 2m + \alpha^2 + \beta^2 + \gamma^2 + \delta^2.$$

Since $1 < 4(n - 4m^2 - 2m)$, we may apply Lemma 2.2.4 so that we have an integer solution such an $\alpha, \beta, \gamma, \delta$. Note that

$$n - 4m^2 - 2m < 4(m+1)^2 + 2(m+1) - 4m^2 - 2m = 8m + 6$$

which implies that

$$-\sqrt{8m+6} < \alpha, \beta, \gamma, \delta < \sqrt{8m+6}.$$

Now, we have $n = x^2 + y^2 + z^2 + w^2$ has an integer solution (a, b, c, d) with $a, b, c, d \in (m - \sqrt{8m+6}, m + \sqrt{8m+6})$. Hence if n is big enough so that $m - \sqrt{8m+6} > \rho$, then all of a, b, c, d are greater than ρ.

Assume that $n \equiv 0 \pmod 4$. First, denote $\rho = 2^k \rho'$ with $k \geq 0$ and an odd integer ρ'. We have $n = 4^e l$ with $e \geq 1$ and $l \not\equiv 0 \pmod 4$. By Lagrange's four square theorem, there are nonnegative integers a, b, c, d satisfying

$$l = a^2 + b^2 + c^2 + d^2.$$

Hence we have

$$n = (2^e a)^2 + (2^e b)^2 + (2^e c)^2 + (2^e d)^2.$$

If $k < e$, then $2^e a, 2^e b, 2^e c, 2^e d \neq \rho$. Otherwise, we can find integers a', b', c', d' satisfying

$$l = (a')^2 + (b')^2 + (c')^2 + (d')^2,$$

and $a', b', c', d' > 2^{k-e}\rho'$ since $l \not\equiv 0 \pmod 4$. By multiplying 4^e, we have

$$n = 4^e l = (2^e a')^2 + (2^e b')^2 + (2^e c')^2 + (2^e d')^2.$$

$\square$

Now, we may prove $M(1) = 6$ by using Proposition 4.1.3. Note that if $m \geq 11$, then

$$1 < m - \sqrt{8m+6}.$$

Hence any odd integer greater than 504 is a sum of at most four squares of integers contained in S_1. Assume that n is even. For $n = 4l$, there are some integers a, b, c and d satisfying

$$n = (2a)^2 + (2b)^2 + (2c)^2 + (2d)^2,$$

where

$$l = a^2 + b^2 + c^2 + d^2.$$

Since $2a, 2b, 2c, 2d \neq 1$, the integer n is a sum of at most four squares of integers greater than 1. For $n \equiv 2 \pmod 4$, if $m \geq 11$, then we have

$$1 < m - \sqrt{8m+4}.$$

That is, every $n \geq 484$ is a sum of at most four squares of integers contained in S_1. For any integer less than 506, one may directly compute that any integer not in $I(1)$ is a sum of at most 6 squares of integers greater than 1. Note that any integer in $I(1)$ is not a sum of squares greater than 1. This completes the proofs of Theorems 4.1.1 and 4.1.2.

Chapter 5

$I(\rho)$ for $\rho \geq 2$ and $M(2)$

In this section, we mainly prove the case case when $\rho = 2$. To do this, we first prove the following:

Theorem 5.1.1. *$I(\rho) = \varnothing$ for $\rho \geq 2$.*

Proof. Since $1 \in S_2$ and any integer is a sum of squares of 1, $I(\rho) = \varnothing$ for any integer $\rho \geq 2$. □

Theorem 5.1.2. *We have $M(2) = 8$.*

Proof. First, we apply Proposition 4.1.3. If $m \geq 13$, the we have

$$2 < m - \sqrt{8m+6}.$$

Hence any odd integer greater than 702 is a sum of at most four squares of integers contained in $S(2)$. If $n = 4^2 l$, then we may find integers a, b, c, d such that

$$l = a^2 + b^2 + c^2 + d^2.$$

Hence we have

$$n = (4a)^2 + (4b)^2 + (4c)^2 + (4d)^2.$$

Since $4a, 4b, 4c, 4d \neq 2$, any integer divisible by 16 is a sum of at most 4 squares of integers contained in S_2. If $n = 4l$ with $484 \leq l \equiv 2 \pmod 4$, then l can be written as a sum of four squares contained in S_1 by Proposition 4.1.3. If $n = 4l$ with $506 \leq l \equiv 1 \pmod 2$, then l is a sum of at most four squares greater than 1. Hence n is a sum of at most four squares of integers contained in S_2. Now, for $n \equiv 2 \pmod 4$, if $m \geq 13$, then

$$2 < m - \sqrt{8m+4}.$$

Hence every $n \geq 676$ is a sum of at most four squares of integers contained in S_2. As a result, for any $n \geq 2024$, n is a sum of at most 4 squares of integers contained in S_2. So, the proof follows from direct computation for positive integers less than 2024. $\square$

The following proposition is a slight modification of Proposition 4.1.3, which gives an effective method to determine $M(\rho)$ for any arbitrary integer ρ.

Proposition 5.1.3. *Let ρ be a positive integer. There is a constant c_ρ depending on ρ satisfying the condition: If $n > c_\rho \cdot \rho^2$, then there are integers $a, b, c, d \in S_\rho$ such that $n = a^2 + b^2 + c^2 + d^2$. Here c_ρ is non-increasing and $c_\rho \leq 506$.*

Proof. First assume that $n \equiv 2 \pmod 4$. Then for each natural number n, find a nonnegative integer m such that

$$4m^2 < n < 4(m+1)^2.$$

From the proof of Proposition 4.1.3, there are integers a, b, c and d satisfying

$$n = a^2 + b^2 + c^2 + d^2,$$

and

$$m - \sqrt{8m+4} < a, b, c, d.$$

If

$$\rho < m - \sqrt{8m+4}, \tag{5.1}$$

then we have four integers a, b, c and d in S_ρ satisfying

$$n = a^2 + b^2 + c^2 + d^2.$$

From Equation (5.1), we have

$$m > \rho + 4 + 2\sqrt{2\rho+5}.$$

For every

$$n \geq 4m^2 > 4\rho^2 + 64\rho + (16\rho + 64)\sqrt{2\rho+5} + 144,$$

we can find integers $a, b, c, d \in S_\rho$ such that

$$n = a^2 + b^2 + c^2 + d^2.$$

Assume that $n \equiv 1, 3 \pmod 4$. Then for each natural number n, find a nonnegative integer m such that

$$4m^2 + 2m < n < 4(m+1)^2 + 2(m+1).$$

Again from the proof of Proposition 4.1.3, there are integers a, b, c and d satisfying

$$n = a^2 + b^2 + c^2 + d^2,$$

and

$$m - \sqrt{8m+6} < a, b, c, d.$$

If

$$\rho < m - \sqrt{8m+6}, \tag{5.2}$$

then we have four integers a, b, c and d in S_ρ satisfying

$$n = a^2 + b^2 + c^2 + d^2.$$

From Equation (5.2), we have

$$m > \rho + 4 + \sqrt{8\rho + 22}.$$

For every

$$n \geq 4m^2 + 2m > 4\rho^2 + 66\rho + 160 + 34\sqrt{8\rho + 22} + 8\rho\sqrt{8\rho + 22},$$

we can find integers $a, b, c, d \in S_\rho$ such that

$$n = a^2 + b^2 + c^2 + d^2.$$

Assume that $n \equiv 0 \pmod 4$. Denote $\rho = 2^k \rho'$ with a nonnegative integer k and an odd integer ρ'. Since $n \equiv 0 \pmod 4$, we can write $n = 4^e l$ for some positive integers $l \not\equiv 0 \pmod 4$ and e. If we have integers $\alpha, \beta, \gamma, \delta$ satisfying

$$l = \alpha^2 + \beta^2 + \gamma^2 + \delta^2,$$

then we can write

$$n = (2^e\alpha)^2 + (2^e\beta)^2 + (2^e\gamma)^2 + (2^e\delta)^2.$$

If $e > k$, then we can take $a = 2^e\alpha, b = 2^e\beta, c = 2^e\gamma, d = 2^e\delta$.

So, assume that $e \leq k$. Now the original problem is equivalent to the same problem of replacing n, ρ with $l, 2^{k-e}\rho'$ respectively. Since $l \neq 0 \pmod 4$, this case can be proved by above methods.

By equation (5.1) and (5.2), we can denote n as

$$n = c_\rho \rho^2.$$

Note that we can take c_ρ as the greatest value among the cases treated above.

From equation (5.1) we have

$$2m > 2\rho + 4 + 2\sqrt{2\rho + 5}$$

and from equation (5.2) we have

$$2m > 2\rho + 4 + \sqrt{8\rho + 22}.$$

Similarly, we can find that

$$2q\rho + 4 + 2\sqrt{q\rho + 5} < \frac{q}{p}(2p\rho + 4 + 2\sqrt{p\rho + 5})$$

and

$$2q\rho + 4 + \sqrt{8q\rho + 22} < \frac{q}{p}(2p\rho + 4 + \sqrt{8p\rho + 22})$$

for positive integers p, q with $p < q$. This means that c_ρ is actually decreasing. So, $\sup_\rho(c_\rho) = 506 = c_1$. $\square$

Chapter 6

Value of $M(\rho)$

In the previous chapters, We have proved

$$M(1) = 6 \quad \text{and} \quad M(2) = 8.$$

By using a similar method, one may prove that

$$M(3) = 6, \quad M(4) = 5, \quad \text{and} \quad M(5) = 5.$$

Theorem 6.0.1. *For any integer ρ which is not of the form $2^a \cdot 3^b$ for some nonnegative integers a, b, and $\rho \neq 5$, then $M(\rho) = 4$. Hence, if there is a prime $p \geq 7$ dividing ρ, then $M(\rho) = 4$.*

Proof. It was proved in [6] that any integer is a sum of at most 4 squares of integers not divisible by p for ant prime $p \geq 7$. Now, assume that $\rho \neq 5$ is divisible by 5. Since any integer which is not equal to 79 is a sum of at most

4 squares of integers not divisible by 5, and

$$79 = 1^2 + 2^2 + 5^2 + 7^2 = 2^2 + 5^2 + 5^2 + 5^2,$$

we have $M(\rho) = 4$. $\square$

6.1 $M(\rho)$ for $\rho = 2^s$

In this section, we consider the case when $\rho = 2^s$ for some positive integer s. Since we prove that $M(2) = 8$ and $M(4) = 5$, we may assume that $\rho = 2^s$ for $s \geq 3$. The following theorem claims that $M(\rho) = 5$ in this case.

Theorem 6.1.1. *We have $M(2^s) = 5$ for any $s \geq 2$.*

Proof. Take $\rho = 2^s$ for some positive integer $s \geq 2$. By Proposition 5.1.3, we have four integers $a, b, c, d \neq \rho$ such that

$$n = a^2 + b^2 + c^2 + d^2$$

for every positive integer $n > 506\rho^2$.

Suppose that $n \leq 506\rho^2$. Now take a positive integer m such that

$$(m-1)^2 \leq n < m^2.$$

Then we have

$$n - (m-1)^2 < 2m - 1.$$

If $2m-1 \leq 4^s$, then

$$n-(m-1)^2 = a^2+b^2+c^2+d^2$$

for some integers $a,b,c,d \neq \rho$. Note that $2m-1 \leq 4^s$ holds for $m \leq \frac{4^s}{2}$. This means that for $n < 4^{2s-1}$, n can be written as

$$n = (m-1)^2+a^2+b^2+c^2+d^2.$$

So, if $506 \times 4^s < 4^{2s-1}$, equivalently $s \geq 6$, every n is a sum of at most five squares of integers in S_{2^s}.

The only matter is that the case of $m-1 = 2^s$. In that case, we can substitute $m-1$ with $m-2$. We have $n-(m-2)^2 < 4m-4 = 4(2^s+1)-4 = 2^{s+2} \leq 4^s$ for $s \geq 2$. One can find that $M(8) = M(16) = M(32) = 5$ by direct computations.

For complete proof, let $\rho = 2^s$. here $s \geq 2$. Then $n = 3 \times 2^{2s-1} = 6 \times \left(\frac{\rho}{2}\right)^2$ needs 5 squares. By Lemma 2.2.7, $r_4(3 \times 2^{2s-1}) = 96$. But $n = (\pm\rho)^2 + (\pm\frac{\rho}{2})^2 + (\pm\frac{\rho}{2})^2 + 0$ is the only way since the number of arraying the order and sign is $\frac{4!}{2!} \times 2^3 = 96$. Hence this n can not be a sum of four squares. $\square$

6.2 $M(\rho)$ for $\rho = 3^t$

Now let $\rho = 3^t$. Since we have $M(3)$, consider that $t \geq 2$. Then we can prove that $M(\rho) \leq 6$ by direct computations.

Theorem 6.2.1. *We have $M(3^t) \leq 6$ for $t \geq 2$*

Proof. Fix a natural number $t \geq 2$. For a natural number n, we can write

$$n = a^2 + b^2 + c^2 + d^2$$

for some integers a, b, c, d. If $a = b = c = d = 3^t$, then

$$n = 4 \times 9^t = (2 \times 3^t)^2.$$

If $a = b = c = 3^t$, but $d \neq 3^t$, then

$$n = 3 \times 9^t + d^2 = 27 \times 3^{t-1} + d^2 = (5 \times 3^{t-1})^2 + (3^{t-1})^2 + (3^{t-1})^2 + d^2.$$

If $a = b = 3^t$, but $c, d \neq 3^t$, then

$$n = 2 \times 9^t + c^2 + d^2 = (4 \times 3^{t-1})^2 + (3^{t-1})^2 + (3^{t-1})^2 + c^2 + d^2.$$

If $a = 3^t$, but $b, c, d \neq 3^t$, then

$$n = 9^t + b^2 + c^2 + d^2 = (2 \times 3^{t-1})^2 + (2 \times 3^{t-1})^2 + (3^{t-1})^2 + b^2 + c^2 + d^2.$$

$\square$

By Proposition 5.1.3, we can also deduce that $M(\rho) \leq 5$.

Theorem 6.2.2. *We have $M(3^t) \leq 5$ for $t \geq 2$*

Proof. Take $\rho = 3^t$ for some positive integer $t \geq 2$. By Proposition 5.1.3, we have four integers $a, b, c, d \neq \rho$ such that

$$n = a^2 + b^2 + c^2 + d^2$$

for every positive integer $n > 506\rho^2$.

Suppose that $n \leq 506\rho^2$. Now take a positive integer m such that

$$(m-1)^2 \leq n < m^2.$$

Then we have

$$n - (m-1)^2 < 2m - 1.$$

If $2m - 1 \leq 9^t$, then

$$n - (m-1)^2 = a^2 + b^2 + c^2 + d^2$$

for some integers $a, b, c, d \neq \rho$. Note that $2m - 1 \leq 9^t$ holds when $m \leq \frac{9^t+1}{2}$. This means that for $n < \left(\frac{9^t+1}{2}\right)^2$, n can be written as

$$n = (m-1)^2 + a^2 + b^2 + c^2 + d^2.$$

So, if $2024 \times 9^t < 9^{2t} + 2 \times 9^t + 1$, then every n is a sum of at most five squares of integers in S_ρ. Note that

$$2022 \times 9^t < 9^{2t} < 9^{2t} + 1$$

holds when $t \geq 4$.

The only matter is that the case of $m - 1 = 3^t$. In that case, we can substitute $m-1$ with $m-2$. We have $n - (m-2)^2 < 4m - 4 = 4(3^t + 1) - 4 = 4 \times 3^t \leq 9^t$ for all $t \geq 2$. One can find that $M(9) = M(27) = 4$ by direct computations. $\square$

If $n \not\equiv 2 \pmod 3$, we can write n as a sum of at most four squares of integers in S_ρ.

Theorem 6.2.3. *Let $\rho = 3^t$ for $t \geq 2$. Suppose that $n \not\equiv 2 \pmod 3$. Then n is a sum of at most four squares of integers in S_ρ.*

Proof. First suppose that n is not of the form $4^\alpha(8\beta+7)$. Let $n \equiv 0 \pmod 3$. Then $n = a^2 + b^2 + c^2$ and a, b, c should be divisible by 3 or none of them should be divisible by 3. Suppose a, b, c are divisible by 3. Without loss of generality, we can write

$$a = 3^e a_0, \quad b = 3^f b_0, \quad c = 3^g c_0 \quad (1 \leq e \leq f \leq g)$$

for integers a_0, b_0, c_0, e, f, g so that a_0, b_0, c_0 are not divisible by 3. Let

$$M = \frac{a+b+c}{3} = 3^{e-1}a_0 + 3^{f-1}b_0 + 3^{g-1}c_0.$$

Then

$$\begin{aligned} &(2M-a)^2 + (2M-b)^2 + (2M-c)^2 \\ &= 12M^2 - 4M(a+b+c) + a^2 + b^2 + c^2 = a^2 + b^2 + c^2 = n^2 \end{aligned}$$

and

$$\mathrm{ord}_3(2M-a) = \mathrm{ord}_3(2M-b) = \mathrm{ord}_3(2M-c) = e-1$$

unless $e = f = g$. In this case, we can write n as a sum of three squares none of them is divisible by 3 by using induction on e. Let $e = f = g$. If $a, b, c \neq 3^t$, then it is over. So we suppose $a = 3^t$. Now we have $M = 3^{t-1}(1 + b_0 + c_0)$.

Then

$$2M - a = 3^{t-1}(b_0 + c_0 - 2),$$
$$2M - b = 3^{t-1}(1 + c_0 - 2b_0),$$
$$2M - c = 3^{t-1}(1 + b_0 - 2c_0).$$

Since $b_0, c_0 \equiv 1, 2 \pmod 3$, $2M - a$ is divisible by 3^t if and only if $b_0, c_0 \equiv 1 \pmod 3$. Moreover $2M - b, 2M - c$ are also divisible by 3^t if and only if $b_0, c_0 \equiv 1 \pmod 3$ respectively. If we substitute b by $-b$, $2M-a, 2M-b, 2M-c$ can not be divisible by 3^t. Hence we can write $n = a^2+b^2+c^2$ with $a, b, c \neq 3^t$.

Let $n \equiv 1 \pmod 3$. Since $n - 1 \equiv 0 \pmod 3$, we can write $n = 1 + a^2 + b^2 + c^2$ for some integers $a, b, c \neq 3^t$.

Now suppose that $n = 4^\alpha(8\beta+7)$. Let $n \equiv 0 \pmod 3$. Then $n = a^2+b^2+c^2+d^2$ and a, b, c, d should be divisible by 3 or exactly one of them should be divisible by 3. If $a = b = c = d = 3^t$, we can write $n = (2 \times 3^t)^2$. So suppose that at least one of them is not 3^t. Without loss of generality, we may assume that $a \neq 3^t$. Then $n - a^2 = b^2 + c^2 + d^2$ is not of the form $4^\alpha(8\beta + 7)$ since it is a sum of three squares and all b, c, d should be divisible by 3. By the same logic, we can write $n = a^2 + (b')^2 + (c')^2 + (d')^2$ with $a, b', c', d' \neq 3^t$.

Let $n \equiv 1 \pmod 3$. Then there are integers a, b, c and d such that $n = a^2 + b^2 + c^2 + d^2$ and all of them are divisible by 3 except for one. Again we may assume a is not divisible by 3. Then $n - a^2 = b^2 + c^2 + d^2$ and all a, b, c should be divisible by 3. So we can write $n = a^2 + (b')^2 + (c')^2 + (d')^2$ with $a, b', c', d' \neq 3^t$. $\square$

It seems that $M(\rho) = 4$ if $\rho = 3^t$ with $t \geq 2$.

Conjectrue 6.2.4. *$M(3^t) = 4$ for $t \geq 2$.*

6.3 $M(\rho)$ for $\rho = 2^s 3^t$

Now we consider the more general and the last one. Let $\rho = 2^s 3^t$. Here we only consider $s, t \geq 1$. Then we have $M(\rho) = 5$ if $t = 1$.

Theorem 6.3.1. *Let $\rho = 2^s 3^t$ for natural numbers s, t. Then we have $M(\rho) = 5$ if $t = 1$.*

Proof. Let $\rho = 3 \times 2^s$ for some positive integer s. By Proposition 5.1.3, we have four integers $a, b, c, d \neq \rho$ such that

$$n = a^2 + b^2 + c^2 + d^2$$

for every positive integer $n > 506\rho^2$.

Suppose that $n \leq 506\rho^2$. Now take a positive integer m such that

$$(m-1)^2 \leq n < m^2.$$

Then we have

$$n - (m-1)^2 < 2m - 1.$$

If $2m - 1 \leq 9 \times 4^s$, then

$$n - (m-1)^2 = a^2 + b^2 + c^2 + d^2$$

for some integers $a, b, c, d \neq \rho$. Note that $2m - 1 \leq 9 \times 4^s$ holds for $m \leq 9 \times \frac{4^s}{2}$.

This means that for $n < 81 \times 4^{2s-1}$, n can be written as

$$n = (m-1)^2 + a^2 + b^2 + c^2 + d^2.$$

So, if $506 \times 9 \times 4^s < 81 \times 4^{2s-1}$, equivalently $s \geq 5$, every n is a sum of at most five squares of integers in S_ρ.

The only matter is that the case of $m - 1 = 3 \times 2^s$. In that case, we can substitute $m-1$ with $m-2$. We have $n-(m-2)^2 < 4m-4 = 4(3\times 2^s+1)-4 = 3 \times 2^{s+2} \leq 9 \times 4^s$ for $s \geq 1$. One can find that $M(6) = M(12) = M(24) = M(48) = M(96) = 5$ by direct computations.

Now we have to show that there exists a natural number n which can not be a sum of at most four squares. Let $N = \frac{14}{9} \times \rho^2 = 14 \times 2^{2s}$. By Lemma 2.2.7, $r_4(7 \times 2^{2s+1}) = 192$. But $n = (\pm\rho)^2 + (\pm\frac{2\rho}{3})^2 + (\pm\frac{\rho}{3})^2 + 0$ is the only way since the number of arraying the order and sign is $4! \times 2^3 = 192$. Hence this n can not be a sum of at most four squares. $\square$

It seems that $M(\rho) = 4$ if $\rho = 2^s 3^t$ for $t > 1$.

Conjectrue 6.3.2. $M(\rho) = 4$ *if* $\rho = 2^s 3^t$ *with* $t > 1$.

Bibliography

[1] O. T. O'Meara, Introduction to quadratic forms, Springer-Verlag, New York, 1963.

[2] Y. Kitaoka, Arithmetic of quadratic forms, Cambridge University Press, 1993.

[3] M. V. Nathanson, Additive number theory the classical bases, Springer, 1996.

[4] J. H. Conway, N. J. A. Sloane, Sphere packings, lattices and groups, third edition, Springer, 1999.

[5] O. T. O'Meara, The integral representations of quadratic forms over local fields, Amer. J. Math 80(1958), 843-878.

[6] K. Kim, B.-K Oh, A sum of squares not divisible by a prime, Ramanujan J. 59(2022), 653-670.

[7] M. D. Hirschhorn, A simple proof of Jacobi's four-square theorem, J. Aust. Math. Soc. 32(1982), 61–67.

국문초록

본 논문에서는 제곱수의 합에 관한 두 가지 주제를 생각한다. 첫째로, 모든 자연수는 3으로 나누어 떨어지지 않는 최대 6개의 정수들의 제곱의 합으로 쓰여질 수 있음을 증명한다. 둘째로, 정수의 집합에서 정해진 수를 제외한 수들의 제곱의 합을 연구한다. 그 시작으로 모든 자연수가 1, 또는 4를 제외한 제곱수들의 합으로 쓰여질 수 있는지를 확인하고, 각각의 모든 자연수를 나타내기 위해 필요한 제곱수들의 최소 갯수를 찾는다. 마지막으로, 해당 주제를 임의의 양수에 대하여 고려한다.

주요어휘: 제곱수의 합, 이차 형식, 표현
학번: 2020-21303