C. R. Acad. Sci. Paris, Ser. I 349 (2011) 497–500

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number Theory

Sums of distinct integral squares in real quadratic fields

Sommes de carrés distincts dans l'anneau des entiers d'un corps quadratique réel

Byeong Moon Kim [a], Poo-Sung Park [b,1]

[a] *Department of Mathematics, Gangnung-Wonju National University, Gangneung Daehangno 120, Gangneung City, Gangwon Province, 210-702, Republic of Korea*
[b] *Department of Mathematics Education, Kyungnam University, Changwon, 631-701, Republic of Korea*

ARTICLE INFO

Article history:
Received 11 May 2010
Accepted after revision 22 March 2011
Available online 12 April 2011

Presented by Jean-Pierre Serre

ABSTRACT

We show that the elements of the ring of integers of real quadratic fields which are sums of integral squares are in fact sums of *distinct* squares, provided their norm is large enough.

RÉSUMÉ

Nous montrons que les entiers totalement positifs de normes suffisamment grandes sont des sommes de carrés distincts dans l'anneau des entiers des corps réel quadratique.

1. Introduction

In 1948, Sprague [8] showed in a quite elementary way that every integer bigger than 128 can be represented as a sum of distinct integral squares. He also found all 31 positive integers which cannot be represented as sums of distinct squares: 2, 3, 6, 7, 8, 11, 12, 15, 18, 19, 22, 23, 24, 27, 28, 31, 32, 33, 43, 44, 47, 48, 60, 67, 72, 76, 92, 96, 108, 112 and 128.

The second author proved an analogous result for $\mathbb{Q}(\sqrt{5})$ [6]. But, in general, it is not easy to classify all algebraic integers which can be represented as sums of distinct integral squares in number fields. Such a result has recently been obtained for $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$ [4].

Another direction to generalize Sprague's result is to represent n-ary quadratic forms as sums of distinct squares of linear forms. That is, we can regard an integer as a unary quadratic form. Sprague's result is rephrased as follows: $kx^2 = (a_1x)^2 + (a_2x)^2 + \cdots + (a_rx)^2$ with $0 < a_1 < a_2 < \cdots < a_r$ for $k > 128$.

In this article, we find all integral positive definite binary quadratic forms which cannot be represented as sums of distinct squares of linear forms. Moreover, using this result, we show that all totally positive integers of sufficiently large norms are represented as sums of distinct squares in real quadratic fields.

2. Binary forms as sums of distinct squares

We abbreviate a binary form $Q(x, y) = ax^2 + 2bxy + cy^2$ by $[a, b, c]$. We define the discriminant of Q by $dQ = ac - b^2$.

Any positive definite binary form can be reduced to the form $[a, b, c]$ modulo $\mathrm{GL}(2, \mathbb{Z})$ with $0 < a \leqslant c$ and $0 \leqslant b \leqslant a/2$. Suppose that $b = b_1^2 + b_2^2 + \cdots + b_r^2$ with $0 \leqslant b_1 < b_2 < \cdots < b_r$. Then

E-mail addresses: kbm@gwnu.ac.kr (B.M. Kim), pspark@kyungnam.ac.kr (P.-S. Park).

[1] This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0006592).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2011.03.019

$$[a,b,c]-\left[b_1^2,b_1^2,b_1^2\right]-\left[b_2^2,b_2^2,b_2^2\right]-\cdots-\left[b_r^2,b_r^2,b_r^2\right]=[a-b,0,c-b].$$

If both of $a'=a-b$ and $c'=c-b$ can be represented as sums of distinct squares, we are done.

Assume that $a'\geqslant 2$ and cannot be written as a sum of distinct squares. Then, not both $a'-2$ and $a'-3$ are in Sprague's exceptional list. Note that

$$[2,0,8]=[1,2,4]+[1,-2,4],$$
$$[3,0,14]=[1,3,9]+[1,-1,1]+[1,-2,4].$$

If $a\geqslant 4$ and $c>2(128+14)$, then $a'=a-b\geqslant a-\frac{a}{2}\geqslant 2$ and $c'=c-b\geqslant c-\frac{c}{2}>128+14$. Thus $[a',0,c']$, $[a',0,c']-[2,0,8]$ or $[a',0,c']-[3,0,14]$ is represented as a sum of distinct squares.

If $a<4$ and $c>128+5$, then $b=0,1$ and each form $[a,b,c]$ is a sum of distinct squares as follows:

$$[1,0,c]=[1,0,0]+[0,0,c],$$
$$[2,0,c]=[1,1,1]+[1,-1,1]+[0,0,c-2],$$
$$[2,1,c]=[1,0,0]+[1,1,1]+[0,0,c-1],$$
$$[3,0,c]=[1,0,0]+[1,1,1]+[1,-1,1]+[0,0,c-2],$$
$$[3,1,c]=[1,0,0]+[1,-1,1]+[1,2,4]+[0,0,c-5].$$

Now, suppose that b cannot be represented as a sum of distinct squares. Then $a\geqslant 2b\geqslant 4$. Note that $b-2$ or $b-4$ is a sum of distinct squares. Thus from the equalities

$$[a,b,c]=[4,2,1]+[a-4,b-2,c-1]=[1,2,4]+[4,2,1]+[a-5,b-4,c-5]$$

the problem reduces to the previous case if $a\geqslant 5$. But, the form $[1,2,4]$ might already be used, so that we would use the following equalities selectively when $a'=a-b$ cannot be written as a sum of distinct squares:

$$[2,0,8]=[1,2,4]+[1,-2,4],$$
$$[2,0,18]=[1,3,9]+[1,-3,9],$$
$$[3,0,14]=[1,3,9]+[1,-1,1]+[1,-2,4].$$

For example, $[7,4,151]=[1,2,4]+[4,2,1]+[2,0,146]$. But, we cannot use $[2,0,8]$ to reduce $[2,0,146]$ because $[1,2,4]$ was already used. So we should use $[2,0,18]$ instead of $[2,0,8]$.

Thus if $a\geqslant 4+5$ and $c>2(128+18)+5$, then $[a,b,c]$ is represented as a sum of distinct squares.

If $a<9$, then $b=2,3$ and forms $[a,b,c]$ are verified to be sums of distinct squares for $c>128+10$.

$$[4,2,c]=[4,2,1]+[0,0,c-1],$$
$$[5,2,c]=[1,0,0]+[4,2,1]+[0,0,c-1],$$
$$[6,2,c]=[1,1,1]+[1,-1,1]+[4,2,1]+[0,0,c-3],$$
$$[6,3,c]=[1,0,0]+[1,1,1]+[4,2,1]+[0,0,c-2],$$
$$[7,2,c]=[1,0,0]+[1,1,1]+[1,-1,1]+[4,2,1]+[0,0,c-3],$$
$$[7,3,c]=[1,0,0]+[1,1,1]+[1,2,4]+[4,0,0]+[0,0,c-5],$$
$$[8,2,c]=[4,0,0]+[4,2,1]+[0,0,c-1],$$
$$[8,3,c]=[1,0,0]+[1,1,1]+[1,2,4]+[1,-2,4]+[4,2,1]+[0,0,c-10].$$

Hence finitely many forms remain unchecked. That is, $[a,b,c]$ with $0\leqslant 2b\leqslant a\leqslant c\leqslant 2(128+18)+5$.

Table 1 lists all 105 binary forms which cannot be represented as sums of distinct squares. The maximal discriminant is 160 for $[13,3,13]$ and $[5,0,32]$. Thus if a binary form has discriminant >160, then it can be represented as a sum of distinct squares of linear forms.

3. Algebraic integers as sums of distinct squares

Using the previous result, we characterize algebraic integers of real quadratic fields which can be represented as sums of distinct squares.

Let $D>1$ be a square-free positive integer. Denote the ring of integers in the real quadratic field $\mathbb{Q}(\sqrt{D})$ by $\mathcal{O}$. If $D\not\equiv 1 \pmod 4$, then $\mathcal{O}=\mathbb{Z}[\sqrt{D}]$. If $D\equiv 1 \pmod 4$, then $\mathcal{O}=\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$.

Table 1
Binary forms which cannot be represented as a sum of distinct squares of linear forms.

$d=2$:	[1, 0, 2]					
$d=3$:	[1, 0, 3]					
$d=5$:	[2, 1, 3]					
$d=6$:	[1, 0, 6]					
$d=7$:	[2, 1, 4],	[1, 0, 7]				
$d=8$:	[3, 1, 3],	[2, 0, 4],	[1, 0, 8]			
$d=10$:	[2, 0, 5]					
$d=11$:	[3, 1, 4],	[1, 0, 11]				
$d=12$:	[3, 0, 4],	[4, 2, 4],	[1, 0, 12]			
$d=13$:	[2, 1, 7]					
$d=15$:	[4, 1, 4],	[3, 0, 5],	[2, 1, 8],	[1, 0, 15]		
$d=18$:	[1, 0, 18]					
$d=19$:	[4, 1, 5],	[1, 0, 19]				
$d=20$:	[3, 1, 7],	[2, 0, 10]				
$d=22$:	[1, 0, 22]					
$d=23$:	[4, 1, 6],	[3, 1, 8],	[2, 1, 12],	[1, 0, 23]		
$d=24$:	[4, 0, 6],	[1, 0, 24]				
$d=27$:	[4, 1, 7],	[1, 0, 27]				
$d=28$:	[4, 0, 7],	[4, 2, 8],	[2, 0, 14],	[1, 0, 28]		
$d=30$:	[3, 0, 10]					
$d=31$:	[5, 2, 7],	[4, 1, 8],	[2, 1, 16],	[1, 0, 31]		
$d=32$:	[6, 2, 6],	[4, 0, 8],	[4, 2, 9],	[3, 1, 11],	[1, 0, 32]	
$d=33$:	[1, 0, 33]					
$d=35$:	[5, 0, 7],	[3, 1, 12]				
$d=39$:	[5, 1, 8],	[6, 3, 8],	[2, 1, 20]			
$d=40$:	[5, 0, 8],	[2, 0, 20]				
$d=43$:	[4, 1, 11],	[1, 0, 43]				
$d=44$:	[5, 1, 9],	[4, 2, 12],	[1, 0, 44]			
$d=47$:	[6, 1, 8],	[7, 3, 8],	[4, 1, 12],	[3, 1, 16],	[2, 1, 24],	[1, 0, 47]
$d=48$:	[4, 0, 12],	[4, 2, 13],	[1, 0, 48]			
$d=52$:	[2, 0, 26]					
$d=55$:	[7, 1, 8],	[8, 3, 8],	[2, 1, 28]			
$d=60$:	[8, 2, 8],	[5, 0, 12],	[3, 0, 20],	[2, 0, 30],	[1, 0, 60]	
$d=63$:	[8, 1, 8],	[8, 3, 9],	[2, 1, 32]			
$d=67$:	[4, 1, 17],	[1, 0, 67]				
$d=70$:	[7, 0, 10]					
$d=72$:	[1, 0, 72]					
$d=76$:	[5, 2, 16],	[1, 0, 76]				
$d=88$:	[4, 0, 22]					
$d=92$:	[9, 4, 12],	[1, 0, 92]				
$d=96$:	[4, 2, 25],	[1, 0, 96]				
$d=108$:	[9, 3, 13],	[1, 0, 108]				
$d=112$:	[4, 2, 29],	[1, 0, 112]				
$d=128$:	[9, 4, 16],	[4, 0, 32],	[4, 2, 33],	[1, 0, 128]		
$d=140$:	[12, 4, 13],	[5, 0, 28]				
$d=160$:	[13, 3, 13],	[5, 0, 32]				

The ring $\mathcal{O}$ has a canonical involution $\bar{\cdot}$ sending $\sqrt{D}$ to $-\sqrt{D}$. If $\alpha > 0$ and $\bar{\alpha} > 0$ for an integer $\alpha \in \mathcal{O}$, α is said to be *totally positive*. Obviously, if a number can be represented as a sum of squares, it is totally positive. We denote the set of totally positive integers by $\mathcal{O}^+$.

Theorem 1. *Let $D \not\equiv 1 \pmod 4$. If $\alpha = a + 2b\sqrt{D} \in \mathcal{O}^+$ satisfies $N(\alpha) = \alpha\bar{\alpha} = a^2 - 4b^2D > 160 \cdot 4D + D^2$, then α is represented as a sum of distinct squares.*

Proof. Note that if an algebraic integer is represented as a sum of squares, the coefficient of $\sqrt{D}$ is even.

We choose a suitable integer $t \in [-(D-1), D]$ such that $2D|(a+t)$. Then $a-t$ is positive and even.

Consider the binary quadratic form

$$Q(x, y) = \frac{a+t}{2D}x^2 + 2bxy + \frac{a-t}{2}y^2$$

with discriminant

$$dQ = \frac{a+t}{2D} \cdot \frac{a-t}{2} - b^2 = \frac{a^2 - t^2 - 4b^2D}{4D} = \frac{N(\alpha) - t^2}{4D} > 160.$$

Since Q is represented as a sum of distinct squares of linear forms, $\alpha = Q(\sqrt{D}, 1)$ is represented as a sum of distinct squares. □

Every positive definite binary form is represented as a sum of five squares of linear forms [5]. Thus if $\alpha = a+2b\sqrt{D} \in \mathcal{O}^+$ satisfies $N(\alpha) > D^2$, then α can be represented as a sum of five squares by using the same construction as in the above proof.

Moreover, if $D = 2$ or 3, then every totally positive integer of the form $a + 2b\sqrt{D}$ can be represented as a sum of three squares [1,7].

Theorem 2. *Let $D \equiv 1 \pmod 4$. If $\alpha = a + \frac{1+\sqrt{D}}{2}b \in \mathcal{O}^+$ satisfies*

$$N(\alpha) = \alpha\bar{\alpha} = \frac{(2a+b)^2 - b^2D}{4} > 160D + \frac{D^2}{4},$$

then α is represented as a sum of distinct squares.

Proof. We choose an integer $t \in [-(D-1), D]$ such that $D|(2a+b+t)$ and $b - \frac{2a+b+t}{D}$ is even.

Let $f(b) = (b^2D + 160 \cdot 4D + D^2) - (2b+D)^2 = (D-4)b^2 - 4Db + 640D$.

This function f has a minimum $\frac{D(636D-4\cdot 640)}{D-4}$ at $b = \frac{2D}{D-4}$. Since $D \geqslant 5$, $f(b) > 0$. From the norm condition,

$$(2a+b)^2 > b^2D + 160 \cdot 4D + D^2 > (2b+D)^2.$$

Thus $2a > b + D \geqslant b + t$ and $a > \frac{2a+b+t}{4}$.

Let $A = 2a + b + t$. Note that all the coefficients are integers and

$$a - \frac{A(D-1)}{4D} > a - \frac{A}{4} = a - \frac{2a+b+t}{4} > 0.$$

Consider the binary quadratic form

$$Q(x, y) = \frac{A}{D}x^2 + \left(b - \frac{A}{D}\right)xy + \left(a - \frac{A(D-1)}{4D}\right)y^2$$

with discriminant

$$dQ = \frac{A}{D}\left(a - \frac{A(D-1)}{4D}\right) - \frac{1}{4}\left(b - \frac{A}{D}\right)^2 = \frac{(2a+b)^2 - b^2D - t^2}{4D}$$
$$= \frac{4N(\alpha) - t^2}{4D} > 160.$$

Since Q is represented as a sum of distinct squares of linear forms, $\alpha = Q(\frac{1+\sqrt{D}}{2}, 1)$ is represented as a sum of distinct squares. □

If $\alpha \in \mathcal{O}^+$ satisfies $N(\alpha) \geqslant \frac{D^2}{D-4} + \frac{D^2}{4}$, then

$$f(b) = \left(b^2D + \frac{4D^2}{D-4} + D^2\right) - (2b+D)^2 = (D-4)b^2 - 4Db + \frac{4D^2}{D-4} > 0$$

for every $b \in \mathbb{Z}$. Hence the $Q(x, y)$ is positive definite and α can be represented as a sum of five squares.

Moreover, if $D = 5$, every totally positive integer can be represented as a sum of three squares [3]. If $D > 12$, then there exists a totally positive integer of arbitrarily large norm which cannot be represented as a sum of four squares [2].

Acknowledgement

This work was supported by academic research development grant of Gangneung-Wonju National University (2007).

References

[1] H. Cohn, Calculation of class numbers by decomposition into three integral squares in the field of $2^{1/2}$ and $3^{1/2}$, Amer. J. Math. 83 (1961) 33–56.
[2] H. Cohn, G. Pall, Sums of four squares in a quadratic ring, Trans. Amer. Math. Soc. 105 (1962) 536–556.
[3] F. Götzky, Über eine zahlentheoretische Anwendung von Modulfunktionen zweier Veränderlicher, Math. Ann. 100 (1) (1928) 411–437.
[4] J.Y. Kim, Y.M. Lee, Sums of distinct integral squares in $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$, preprint.
[5] L. Mordell, On the representation of a binary quadratic form as a sum of squares of linear forms, Math. Z. 35 (1) (1932) 1–15.
[6] P.-S. Park, Sums of distinct integral squares in $\mathbb{Q}(\sqrt{5})$, C. R. Acad. Sci. Paris, Sér. I 346 (13–14) (2008) 723–725.
[7] R. Scharlau, Zur Darstellbarkeit von totalreellen ganzen algebraischen Zahlen durch Summen von Quadraten, Dissertation, Bielefeld, 1979.
[8] R. Sprague, Über Zerlegungen in ungleiche Quadratzahlen, Math. Z. 51 (1948) 289–290.