Bull. Korean Math. Soc. **51** (2014), No. 5, pp. 1369–1374
http://dx.doi.org/10.4134/BKMS.2014.51.5.1369

SOLVABILITY OF SOME ENTANGLED DIOPHANTINE EQUATIONS

Poo-Sung Park

Abstract. We show that the Diophantine equation

$$a\,Q(x_1,x_2)+b\,Q(x_3,x_4)+c\,Q(x_5,x_6)=abc$$

has integral solutions for arbitrary positive integers a,b,c when $Q(x,y)$ is a norm form for some imaginary quadratic fields.

1. Introduction

The study on Diophantine equations is to find out whether $f(x_1,x_2,\dots,x_n)=k$ has an integral solution, where f is a specific polynomial and k is an integer. But little has been known the situation about f and k varying together, that is, $f(x_1,x_2,\dots,x_n)=N_f$, where N_f is an integer determined by f. Let us call such equations *entangled*.

For example, the family of Diophantine equations of the form

$$ax_1^2+bx_2^2+cx_3^2+dx_4^2=abcd$$

is entangled. If RHS is, for example, a instead of $abcd$, the problem is trivial. The equation is not always solvable for integers a,b,c,d. It has no solution for $a=b=3$ and $c=d=7$. That is,

$$3x_1^2+3x_2^2+7x_3^2+7x_4^2\neq 3\cdot 3\cdot 7\cdot 7$$

for all integers x_i.

Based on some numerical results using computers, the author conjectures that the entangled Diophantine equation

$$a_1x_1^2+a_2x_2^2+a_3x_3^2+a_4x_4^2+a_5x_5^2=a_1a_2a_3a_4a_5$$

has an integral solution for arbitrary positive integers a_1,a_2,a_3,a_4,a_5.

We may consider this Diophantine equation as a sumset problem. That is, if S is the set of squares of integers, it is a problem asking whether the weighted sumset $\sum_{i=1}^5 a_i\cdot S$ contains $\prod_{i=1}^5 a_i$ or not, where $a_i\cdot S=\{a_is\,|\,s\in S\}$.

Received February 5, 2013; Revised April 2, 2014.
2010 *Mathematics Subject Classification.* Primary 11D09; Secondary 11E39.
Key words and phrases. Diophantine equations, quadratic forms, Hermitian lattices.
This work was supported by Kyungnam University Foundation Grant, 2011.

In the present article we will show that the sumset problems are solvable for $S = \{x^2 + ky^2 \mid x, y \in \mathbb{Z}\}$ and $S = \{x^2 + xy + ky^2 \mid x, y \in \mathbb{Z}\}$ with $k = 1, 2, 3$: For example, if S is the set of sums of two squares, then $a \cdot S + b \cdot S + c \cdot S$ contains abc. Thus,

$$a(x_1^2 + x_2^2) + b(x_3^2 + x_4^2) + c(x_5^2 + x_6^2) = abc$$

has an integral solution for arbitrary positive integers a, b, c.

To prove these problems we use the unique factorization property of rings of algebraic integers of some quadratic fields and representation theory of local lattices. Another proof for $S = \{x^2 + y^2 \mid x, y \in \mathbb{Z}\}$ was given by Coppersmith [1]. His elegant proof uses minimal vectors.

2. Preliminaries

Note that $x_1^2 + Dx_2^2 = (x_1 + x_2\sqrt{-D})(x_1 - x_2\sqrt{-D})$ corresponds to a unary Hermitian form $x\overline{x}$ defined over $\mathbb{Q}(\sqrt{-D})$. So we can use representation theory of Hermitian lattices.

Let E be an imaginary quadratic field and let D be a positive squarefree integer for which $E = \mathbb{Q}(\sqrt{-D})$. The ring $\mathcal{O}_E$ of algebraic integers of E is generated by 1 and ω_D, where $\omega_D = \sqrt{-D}$ if $D \equiv 1, 2 \pmod 4$ or $D = \frac{1+\sqrt{-D}}{2}$ if $D \equiv 3 \pmod 4$.

A Hermitian space (V, H) is a vector space over E equipped with a Hermitian map $H\colon V \times V \to E$. A Hermitian lattice L is a finitely generated $\mathcal{O}_E$-module in the Hermitian space (V, H).

Assume that a Hermitian lattice L is free. That is, L has a basis $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ as a module. Then the $n \times n$-matrix

$$\mathcal{G}_L = [H(\mathbf{v}_i, \mathbf{v}_j)]_{1 \le i,j \le n}$$

is called the Gram matrix of L. We identify a lattice L and its Gram matrix $\mathcal{G}_L$. We define the discriminant of L by $dL = \det \mathcal{G}_L$.

If $\mathcal{G}_L$ is diagonal, we use the brief notation

$$\langle H(\mathbf{v}_1), H(\mathbf{v}_2), \ldots, H(\mathbf{v}_n) \rangle .$$

If $L = L_1 \oplus L_2$ and $H(\mathbf{v}_1, \mathbf{v}_2) = 0$ for all $\mathbf{v}_i \in L_i$, then we write

$$L = L_1 \perp L_2 \quad \text{and} \quad \mathcal{G}_L = \mathcal{G}_{L_1} \perp \mathcal{G}_{L_2}.$$

We say that a number a is represented by L and denote it by $a \to L$ if there exists a vector $\mathbf{v} \in L$ such that $H(\mathbf{v}) := H(\mathbf{v}, \mathbf{v}) = \mathbf{v}^* \mathcal{G}_L \mathbf{v} = a$, where $*$ means conjugate transpose. Let ℓ be a Hermitian lattice of rank m. If there exists a matrix $X \in \mathrm{Mat}_{n \times m}(\mathcal{O}_E)$ such that $\mathcal{G}_\ell = X^* \mathcal{G}_L X$, then we say that ℓ is represented by L and denote it by $\ell \to L$. If two nondegenerate lattices ℓ and L satisfy $\ell \to L$ and $L \to \ell$, we say that ℓ is isometric to L and denote it by $\ell \cong L$.

Let p be a prime spot (possibly, ∞). Define E_p by $E \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and $\mathcal{O}_{E_p}$ by $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for each p. Note that E_p has a unique involution (see [3], [13]).

Thus we can define Hermitian lattices over E_p. We call $L_p = \mathcal{O}_{E_p} \otimes_{\mathcal{O}_E} L$ a localization of L. We define the class of L by

$$\operatorname{cls} L = \{M \mid M \cong L\}$$

and the genus of L by

$$\operatorname{gen} L = \{M \mid M_p \cong L_p \text{ for all } p\}.$$

It is known that $\operatorname{gen} L$ is the union of the finite number of classes of lattices. That is,

$$\operatorname{gen} L = \operatorname{cls} L_1 \cup \operatorname{cls} L_2 \cup \cdots \cup \operatorname{cls} L_n$$

for some $L_1, L_2, \ldots, L_n \in \operatorname{gen}(L)$. If $\ell_p \to L_p$ for all prime spots p, then $\ell \to L_i$ for some $L_i \in \operatorname{gen} L$. There is a systematic method [3], [6] to check whether $\ell_p \to L_p$ for each prime p.

If $H(\mathbf{v}) > 0$ for all $\mathbf{v}(\neq 0) \in L$ over E, we call L positive definite. If a positive definite Hermitian lattice L represents all positive integers, we say that L is universal. Similarly, if L represents all positive definite m-ary Hermitian lattice, we say that L is m-universal.

The universal Hermitian lattices were studied by many mathematicians [2], [5], [8], [11]. A criterion for universality was obtained by the author and his colleagues [7].

All the ternary and quaternary 2-universal Hermitian lattices were found by the author and M.-H. Kim (see Table 1) [9].

TABLE 1. 2-universal Hermitian lattices of rank 3 and 4

$$\begin{aligned}
&\mathbb{Q}(\sqrt{-1}): \quad \langle 1,1,1\rangle, \quad \langle 1,1\rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \\
&\mathbb{Q}(\sqrt{-2}): \quad \langle 1,1\rangle \perp \begin{bmatrix} 2 & -1+\omega_2 \\ -1-\omega_2 & 2 \end{bmatrix} \\
&\mathbb{Q}(\sqrt{-3}): \quad \langle 1,1,1\rangle, \quad \langle 1,1,2\rangle \\
&\mathbb{Q}(\sqrt{-7}): \quad \langle 1,1,1\rangle \\
&\mathbb{Q}(\sqrt{-11}): \quad \langle 1,1\rangle \perp \begin{bmatrix} 2 & \omega_{11} \\ \overline{\omega}_{11} & 2 \end{bmatrix}
\end{aligned}$$

Refer [4] or [10] for unexplained notations and terminology.

3. Main results

Now we show that the Diophantine equation

$$a\,Q(x_1, x_2) + b\,Q(x_3, x_4) + c\,Q(x_5, x_6) = abc$$

is solvable for some norm forms $Q(x, y) = x^2 + ky^2$ or $Q(x, y) = x^2 + xy + ky^2$.

Lemma 3.1. *Let $E = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field with $D = 1, 2, 3, 7,$ or 11. If a positive definite binary Hermitian lattice ℓ is given, then $\langle 1\rangle \perp \ell$ represents $d\ell$.*

Proof. Since the class number of $E = \mathbb{Q}(\sqrt{-D})$ is 1 for $D = 1, 2, 3, 7, 11$, all Hermitian lattices over E are free.

Note that $\langle 1, 1, 1\rangle$ is 2-universal over $\mathbb{Q}(\sqrt{-D})$ with $D = 1, 3, 7$. We postpone the case of $D = 2, 11$.

Let $\ell = \left[\begin{smallmatrix} a & b \\ \overline{b} & c \end{smallmatrix}\right]$ be a positive definite binary Hermitian lattice. Then

$$a\, s\overline{s} + b\, s\overline{t} + \overline{b}\, \overline{s}t + c\, t\overline{t} = x\overline{x} + y\overline{y} + z\overline{z}$$

for some linear forms $x, y, z \in \mathcal{O}_E[s, t]$. If we set $x = \alpha s + \beta t$, then

$$\begin{bmatrix} a & b \\ \overline{b} & c \end{bmatrix} - \begin{bmatrix} \alpha\overline{\alpha} & \alpha\overline{\beta} \\ \overline{\alpha}\beta & \beta\overline{\beta} \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus,

$$\begin{bmatrix} a - \alpha\overline{\alpha} & b - \alpha\overline{\beta} \\ \overline{b} - \overline{\alpha}\beta & c - \beta\overline{\beta} \end{bmatrix} = X^* \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} X$$

for some $X \in \mathrm{Mat}_{2\times 2}(\mathcal{O}_E)$.

Comparing determinants of both sides, we obtain that

$$\det \begin{bmatrix} a - \alpha\overline{\alpha} & b - \alpha\overline{\beta} \\ \overline{b} - \overline{\alpha}\beta & c - \beta\overline{\beta} \end{bmatrix} = \gamma\overline{\gamma}$$

for $\gamma = \det(X)$. Rearranging the equality, we obtain that

$$ac - b\overline{b} = \begin{bmatrix} \gamma & \beta & -\alpha \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & \overline{b} & c \end{bmatrix} \begin{bmatrix} \overline{\gamma} \\ \overline{\beta} \\ -\overline{\alpha} \end{bmatrix}.$$

Now consider the cases of $D = 2, 11$. Let $\ell = \left[\begin{smallmatrix} a & b \\ \overline{b} & c \end{smallmatrix}\right]$ be a positive definite binary Hermitian lattice. We know that $\ell_p \to \langle 1, 1, 1\rangle_p$ for all prime spots p. However, $\langle 1, 1, 1\rangle$ is not 2-universal. So we need more steps. By [12] we have that each genus of $\langle 1, 1, 1\rangle$ is composed of two classes of

$$\begin{aligned} \mathbb{Q}(\sqrt{-2}): &\quad I = \langle 1, 1, 1\rangle \quad \text{and} \quad J = \langle 1\rangle \perp \begin{bmatrix} 2 & 1 + \omega_2 \\ 1 - \omega_2 & 2 \end{bmatrix}, \\ \mathbb{Q}(\sqrt{-11}): &\quad I = \langle 1, 1, 1\rangle \quad \text{and} \quad J = \langle 1\rangle \perp \begin{bmatrix} 2 & \omega_{11} \\ \overline{\omega}_{11} & 2 \end{bmatrix}. \end{aligned}$$

Thus we can guarantee that $\ell \to I$ or $\ell \to J$.

Since both of I and J can be written as $\langle 1\rangle \perp N$ with $dN = 1$,

$$\begin{bmatrix} a & b \\ \overline{b} & c \end{bmatrix} - \begin{bmatrix} \alpha\overline{\alpha} & \alpha\overline{\beta} \\ \overline{\alpha}\beta & \beta\overline{\beta} \end{bmatrix} \to N$$

for some $\alpha, \beta \in \mathcal{O}_E$.

Comparing determinants of both sides, we obtain the required result. □

Lemma 3.2. *Let k be 1 or 2. If a prime p is not of the form a^2+kb^2 and p divides a number x^2+ky^2, then p divides both x and y.*

Proof. Suppose, to the contrary, that p does not divide x or y.

Since $\mathbb{Z}[\sqrt{-k}]$ is a UFD, $x^2+ky^2=(x+\sqrt{-k}y)(x-\sqrt{-k}y)$ is a unique factorization. If p is an irreducible element in $\mathbb{Z}[\sqrt{-k}]$, then p divides both x and y. Thus, p should be a product of non-units in $\mathbb{Z}[\sqrt{-k}]$. Assume that $p=(a+\sqrt{-k}b)(c+\sqrt{-k}d)$ for some $a,b,c,d\in\mathbb{Z}$. Comparing norms of both sides, we obtain

$$p^2=(a^2+kb^2)(c^2+kd^2).$$

Thus, p is of the form a^2+kb^2, since p is a prime in $\mathbb{Z}$. It contradicts the assumption. □

Lemma 3.3. *Let k be $1,2$ or 3. If a prime p is not of the form $a^2+ab+kb^2$ and p divides a number $x^2+xy+ky^2$, then p divides both x and y.*

Proof. Since $\mathbb{Z}[\frac{1+\sqrt{1-4k}}{2}]$ is a UFD, the proof is almost identical to Lemma 3.2. □

Theorem 3.4. *Let k be 1, 2, or 3. Each of the following Diophantine equations has integral solutions for any positive integers a, b and c.*

$$a(x_1^2+kx_2^2)+b(x_3^2+kx_4^2)+c(x_5^2+kx_6^2)=abc,$$
$$a(x_1^2+x_1x_2+kx_2^2)+b(x_3^2+x_3x_4+kx_4^2)+c(x_5^2+x_5x_6+kx_6^2)=abc.$$

Proof. We will give a proof for the first equation only for $k=1$ because the proofs for other cases are similar. We may assume that c is not divisible by any prime p of the form $\alpha^2+\beta^2$. If such a prime $p=\alpha^2+\beta^2$ exists, then solutions y_i's of the following equation

$$a(y_1^2+y_2^2)+b(y_3^2+y_4^2)+\frac{c}{p}(y_5^2+y_6^2)=ab\,\frac{c}{p}$$

yield solutions to the original equation by equality

$$x_i^2+x_j^2=(\alpha^2+\beta^2)(y_i^2+y_j^2)=(\alpha y_i+\beta y_j)^2+(\alpha y_j-\beta y_i)^2.$$

Let $\ell=\left[\begin{smallmatrix}ac & 0\\ 0 & bc\end{smallmatrix}\right]$. Considering ℓ as a Hermitian lattice over $\mathbb{Q}(\sqrt{-1})$, we conclude that the Diophantine equation

$$x_1^2+x_2^2+ac(x_3^2+x_4^2)+bc(x_5^2+x_6^2)=abc^2$$

has an integral solution by Lemma 3.1. Then $c\mid x_1^2+x_2^2$. Since every prime factor of c is not sum of two squares, we conclude that $c\mid x_1$ and $c\mid x_2$ by Lemma 3.2. Now canceling c from both sides, we obtain the required result.

Similar arguments can be applied to $\mathbb{Q}(\sqrt{-D})$ when $D=2,3,7$, and 11. Thus, other equations are verified to be solvable except for x^2+3y^2.

We conclude that two quadratic forms x^2+3y^2 and x^2+xy+y^2 represent all the same numbers. So we are done. □

Remark 3.5. The author conjectures that the Diophantine equation

$$a_1(x_1^2 + kx_2^2) + a_2(x_3^2 + kx_4^2) + a_3(x_5^2 + kx_6^2) = a_1a_2a_3$$

has an integral solution for arbitrary positive integers a_1, a_2, a_3 and $k = 4, 5, 6, 7, 8$, and 10.

Remark 3.6. The author also conjectures that the Diophantine equation

$$a_1(x_1^2 + x_1x_2 + kx_2^2) + a_2(x_3^2 + x_3x_4 + kx_4^2) + a_3(x_5^2 + x_5x_6 + kx_6^2) = a_1a_2a_3$$

has an integral solution for arbitrary positive integers a_1, a_2, a_3 and $k = 4, 5, 6$, and 8.

Acknowledgements. The author would like to thank Andrew Earnest for his helpful comments and encouragements. He also would like to thank anonymous referees for their helpful comments and corrections. He also would like to thank KIAS (Korea Institute for Advanced Study) for all the support.

References

[1] D. Coppersmith, *Newsgroup:sci.math.research*, private communications.
[2] A. Earnest and A. Khosravani, *Universal binary Hermitian forms*, Math. Comp. **66** (1997), no. 219, 1161–1168.
[3] L. J. Gerstein, *Integral decomposition of Hermitian forms*, Amer. J. Math. **92** (1970), 398–418.
[4] ———, *Basic Quadratic Forms*, Graduate Studies in Mathematics 90, American Mathematical Society, 2008.
[5] H. Iwabuchi, *Universal binary positive definite Hermitian lattices*, Rocky Mountain J. Math. **30** (2000) no. 3, 951–959.
[6] A. A. Johnson, *Integral representation of hermitian forms over local fields*, J. Reine Angew. Math. **229** (1968), 57–80.
[7] B. M. Kim, J. Y. Kim, and P.-S. Park, *The fifteen theorem for universal Hermitian lattices over imaginary quadratic fields*, Math. Comp. **79** (2010), no. 270, 1123–1144.
[8] J.-H. Kim and P.-S. Park, *A few uncaught universal Hermitian forms*, Proc. Amer. Math. Soc. **135** (2007), no. 1, 47–49.
[9] M.-H. Kim and P.-S. Park, *2-universal Hermitian lattices over imaginary quadratic fields*, Ramanujan J. **22** (2010), no. 2, 139–151.
[10] O. T. O'Meara, *Introduction to Quadratic Forms*, Spinger-Verlag, New York, 1973.
[11] P.-S. Park, *Simple proofs for universal binary Hermitian lattices*, Bull. Aust. Math. Soc. **81** (2010), no. 2, 274–280.
[12] A. Schiemann, *Classification of Hermitian forms with the neighbour method*, J. Symbolic Comput. **26** (1998) no. 4, 487–508.
[13] G. Shimura, *Arithmetic of unitary groups*, Ann. Math. **79** (1964), 369–409.

Department of Mathematics Education
Kyungnam University
Changwon-si 631-701, Korea
E-mail address: pspark@kyungnam.ac.kr