Toyama Math. J.
Vol. 39(2017), 9-18

Gausenstein integers

Yoji YOSHII

Abstract. We introduce a beautiful order of the rational quaternion algebra $\left(\frac{-1,-3}{\mathbb{Q}}\right)$, which has an interesting structure like the Hurwitz order. We show that the order is norm euclidean by a geometrical method, which is quite simple. We also show that the quadratic form $x^2+y^2+3z^2+3w^2$ is universal, using this order, in an elementary way.

1. Introduction

We know Fermat's Two Square Theorem: if $p = 4n+1$ is prime, then $p = a^2+b^2$ for some $a, b \in \mathbb{Z}$. This can be shown using a property in the Gaussian integers $\mathbb{Z}[i]$. Namely, such a prime p is not prime in $\mathbb{Z}[i]$. In 1770, Lagrange proved the so-called Four Square Theorm: for any natural number n, there exist some $a, b, c, d \in \mathbb{Z}$ such that $n = a^2+b^2+c^2+d^2$, which is called the **universality** of the quadratic form $a^2+b^2+c^2+d^2$. This is also shown using the ring of **Hurwitz integers**, which is a norm euclidean order of the rational quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ (see [1], [2] and the terminology in [13]). Recall the Hamilton's quaternion algebra

$$\mathbb{H} = \mathbb{R}[i,j] = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}ij \quad (i^2 = j^2 = -1 \text{ and } ij = -ji).$$

The Hurwitz integers are precisely the subring of $\mathbb{H}$, namely,

$$\mathbb{Z}[i,h] \quad \text{where} \quad h = \frac{1+i+j+ij}{2}.$$

2010 *Mathematics Subject Classification.* Primary: 16U30 ; Secondary: 11A05.

Note that $\mathbb{Z}[i,j,h] = \mathbb{Z}[i,h]$ since $hih^5 = j$. The crucial property for the proof of the Four Square Theorem is that a prime in $\mathbb{Z}$ is not prime in $\mathbb{Z}[i,h]$.

On the other hand, we know a theorem: if $p = 3n+1$ is prime, then $p = a^2+3b^2$ for some $a,b \in \mathbb{Z}$. This is shown using the Eisenstein integers $\mathbb{Z}[\omega]$, where $\omega = \frac{-1+\sqrt{3}i}{2}$ is a primitive 3rd root of unity. The crucial property is again that such a prime p is not prime in $\mathbb{Z}[\omega]$.

We introduce a kind of a mixed ring of $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ but not commutative, namely,

$$\mathbb{Z}[\omega, j] = \mathbb{Z} \oplus \mathbb{Z}\omega \oplus \mathbb{Z}j \oplus \mathbb{Z}\omega j$$

the subring of $\mathbb{H}$, which we call the ring of **Gausenstein integers**. (Episode: When Gauss was 75 years old, Eisenstein died at the age of 29. Gauss missed the young genius, and counted the days of his life, which are 10777 days. Note that $10777 = 13 \cdot 829 = 24^2 + 101^2 = 61^2 + 84^2 = 37^2 + 3 \cdot 56^2 = 83^2 + 3 \cdot 36^2$.) We show that it is a norm euclidean order of the rational quaternion algebra $\left(\frac{-1,-3}{\mathbb{Q}}\right)$. Using this order, we prove the universality of the quadratic form $a^2 + b^2 + 3c^2 + 3d^2$. Of course, this is a non-surprising fact for number theorists. In fact, the form is one of the 54 quaternary quadratic forms shown by Ramanujan [12] (see also [5], [9] and [11]).

Moreover, we have found that Deutsch showed the universality of the quadratic form using a different order of the rational quaternion algebra $\left(\frac{-1,-3}{\mathbb{Q}}\right)$ in [3] (see also [4]). Also, Fitzgerald had already shown in [7] that $\mathbb{Z}[\omega, j]$ is in fact isomorphic to the order which Deutsch found (see also [6]). Thus there might be no novelty in our paper anymore. However, we shall give a simple direct proof that $\mathbb{Z}[\omega, j]$ is norm euclidean by a geometrical method (using the Pythagorean Theorem). Since $\mathbb{Z}[\omega, j]$ is quite simple and natural, we think it worth studying this order itself (not only for the universality of the form) in future. So another purpose of this paper is to summarize some fundamental properties of the Gausenstein integers $\mathbb{Z}[\omega, j]$.

We thank Professor Koichi Kawada for helpful suggestions.

2. Preliminary Notes

For $\alpha = a + bi + cj + dk \in \mathbb{H} = \mathbb{R}[i, j]$, where $k := ij$, we define $\bar{\alpha} := a - bi - cj - dk$, $N(\alpha) := \alpha\bar{\alpha} \in \mathbb{R}_{\geq 0}$ (called the norm of α) and $|\alpha| = \sqrt{N(\alpha)}$, as usual. We note that $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$ for all $\alpha, \beta \in \mathbb{H}$, and so $N(\alpha\beta) = N(\alpha)N(\beta)$. We have $\alpha = 0 \Leftrightarrow N(\alpha) = 0$. Thus any $\alpha \neq 0$ is invertible with $\alpha^{-1} = N(\alpha)^{-1}\bar{\alpha}$ (since $\alpha\bar{\alpha} = \bar{\alpha}\alpha$), i.e., $\mathbb{H}$ is a division ring. Also, $\mathbb{H}$ can be identified with a 4-dimensional euclidean space with the inner product

$$(\alpha, \beta) := \mathrm{Re}(\alpha\bar{\beta})$$

(the real part of $\alpha\bar{\beta}$).

We note that $j\omega = \omega^2 j = -j - \omega j$, and so $(j\omega)^2 = -1$. Thus

$$R := \mathbb{Z}[\omega, j] = \mathbb{Z} \oplus \mathbb{Z}\omega \oplus \mathbb{Z}j \oplus \mathbb{Z}\omega j$$

is a subring of $\mathbb{H}$, and we have

$$N(\alpha) = a^2 + b^2 - ab + c^2 + d^2 - cd \in \mathbb{Z}_{\geq 0}$$

for $\alpha = a + b\omega + cj + d\omega j \in R$. Clearly,

$$R' := \mathbb{Z}[\sqrt{-3}i, j] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-3}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\sqrt{-3}ij$$

is a subring $of R$, and we have

$$N(a + bj + c\sqrt{3}i + d\sqrt{3}ij) = a^2 + b^2 + 3c^2 + 3d^2.$$

So, R and R' are both orders of the rational quaternion algebra $\left(\frac{-1,-3}{\mathbb{Q}}\right)$, i.e., they are finitely generated $\mathbb{Z}$-modules such that

$$R \otimes_{\mathbb{Z}} \mathbb{Q} = R' \otimes_{\mathbb{Z}} \mathbb{Q} \cong \left(\frac{-1, -3}{\mathbb{Q}}\right).$$

By the multiplicativity of the norm, we have the identity

$$\begin{aligned} &(a^2 + b^2 + 3c^2 + 3d^2)(x^2 + y^2 + 3z^2 + 3w^2) \\ =&(ax - by - 3cz - 3dw)^2 + (ay + bx - 3cw + 3dz)^2 \\ &+ 3(az + bw + cx - dy)^2 + 3(aw - bz + cy + dx)^2. \end{aligned} \tag{1}$$

For units, we note that $u \in R$ is a unit if and only if $N(u) = 1$.

Lemma 2.1. *The group G of units in R is*

$$G = \{\pm 1, \pm\omega, \pm\omega^2, \pm j, \pm\omega j, \pm\omega^2 j\}.$$

Proof. One can easily check that $\supset$. For the other inclusion, let $\alpha = a + b\omega + cj + d\omega j \in G$. Since $N(\alpha) = 1$, we have $a^2 + b^2 - ab + c^2 + d^2 - cd = 1$, and so $(a - b/2)^2 + 3b^2/4 + (c - d/2)^2 + 3d^2/4 = 1$. Thus, $(b,d) = (0,0)$, $(\pm 1, 0)$ or $(0, \pm 1)$. If $(b,d) = (0,0)$, then $a^2 + c^2 = 1$, and so $a = \pm 1$ or $c = \pm 1$. Hence, $\alpha = \pm 1$ or $\pm j$. If $(b,d) = (\pm 1, 0)$, then $(a \mp 1/2)^2 + c^2 = 1/4$, and so $c = 0$ and $a \mp 1/2 = \pm 1/2$, i.e., $a = 0$ or $a = \pm 1$. Hence, $\alpha = \pm\omega$ or $\pm 1 \pm \omega = \mp\omega^2$. Similarly, if $(b,d) = (0, \pm 1)$, then $\alpha = \pm\omega j$ or $\pm\omega^2 j$. Thus $\subset$ is shown. □

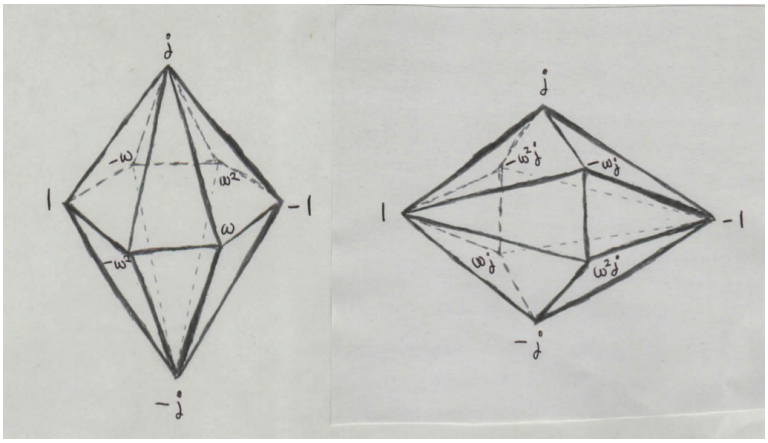
Remark 2.2. A nonabelian group of order 12 is isomorphic to one of D_6 (the dihedral group of a regular hexagon), A_4 (the alternating group of degree 4) and the generalized quaternion $Q_{12} \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_4$. One can check that the unit group G in Lemma 2.1 is isomorphic to Q_{12}. In fact, we have $G = \langle\omega\rangle \rtimes \langle j\rangle$ with $\langle\omega\rangle \cong \mathbb{Z}_3$ and $\langle j\rangle \cong \mathbb{Z}_4$.

We note that the subgroup $S := \{\pm 1, \pm\omega, \pm\omega^2\}$ of G is a regular hexagon in the complex plane. Also, the subset $T := \{\pm j, \pm\omega j, \pm\omega^2 j\}$ of G is a regular hexagon in the plane $\mathbb{R}j \oplus \mathbb{R}\omega j$. Our G is not just $G = S \sqcup T$, but $G = S \perp T$. Intuitively, G consists of two regular hexagons which are orthogonal to each other in a 4-dimensional space. The reason follows from the following lemma:

Lemma 2.3. *Two subspaces $\mathbb{R} \oplus \mathbb{R}\omega = \mathbb{C}$ (which is a subfield) and $\mathbb{R}j \oplus \mathbb{R}\omega j$ of $\mathbb{H}$ are orthogonal. Hence, we have $\mathbb{H} = \mathbb{C} \perp (\mathbb{R}j \oplus \mathbb{R}\omega j)$ and $\mathbb{Z}[\omega, j] = \mathbb{Z}[\omega] \perp (\mathbb{Z}j \oplus \mathbb{Z}\omega j)$.*

Proof. For $\alpha := a + b\omega$, $\beta := cj + d\omega j \in \mathbb{H}$ $(a,b,c,d \in \mathbb{R})$, we have $\alpha\bar{\beta} = -(acj + ad\omega j + bc\omega j + bd\omega^2 j)$, and so $\mathrm{Re}(\alpha\bar{\beta}) = 0$. □

The **pictures** below describe some part of the group G. The left picture is the cross section by the hyperplane $\mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j$. The right picture, which is congruent to the left one, is the cross section by the hyperplane $\mathbb{R} \oplus \mathbb{R}j \oplus \mathbb{R}k$. It is like a hyper-hexagonal diamond.



3. Main Results

We investigate some algebraic properties of the ring R.

Definition 3.1. A subring A of $\mathbb{H}$ is said to be **norm euclidean** if for any $\alpha, \beta \in A$ with $\beta \neq 0$, there exist some $q, r \in A$ such that $\alpha = q\beta + r$ with $N(r) < N(\beta)$.

Theorem 3.2. *$R = \mathbb{Z}[\omega, j]$ is norm euclidean.*

Proof. Note that for any $\alpha, \beta \in R$ with $\beta \neq 0$, we have $\gamma := \alpha\beta^{-1} = \alpha\bar{\beta}/N(\beta) \in \mathbb{Q}[\omega, j]$. Thus it is enough to show that there exists some $q \in R$ such that $N(\gamma - q) < 1$. In fact, for $r := \alpha - q\beta$, we havet $N(r) = N(\gamma\beta - q\beta) = N(\gamma - q)N(\beta) < N(\beta)$.

Let $\gamma = z_1 + z_2\omega + z_3 j + z_4\omega j \in \mathbb{Q}[\omega, j]$. We know that there exist some $a, b \in \mathbb{Z}$ such that $|(z_1 + z_2\omega) - (a + b\omega)| \leq 1/\sqrt{3}$. (Recall that $\mathbb{Z}[\omega]$ is norm euclidean.) Similarly, there exist some $c, d \in \mathbb{Z}$ such that $|(z_2 j + z_4\omega j) - (cj + d\omega j)| \leq 1/\sqrt{3}$.

Now, by Lemma 2.3, $x := (z_1 + z_2\omega) - (a + b\omega)$ and $y := (z_2 j + z_4\omega j) - (cj + d\omega j)$ are orthogonal. Therefore, by the Pythagorean Theorem, letting $q := a + b\omega + cj + d\omega j$, we have

$$N(\gamma - q) = |x + y|^2 = |x|^2 + |y|^2 \leq 1/3 + 1/3 = 2/3 < 1.$$

Hence we have obtained $N(\gamma - q) < 1$. □

Lemma 3.3. *Suppose that I is a left ideal of R. Then there exists some $\beta \in R$ such that $I = R\beta$.*

Proof. Fix $\beta \in I$ so that $N(\beta)$ is the smallest number among $N(\alpha)$ for $\alpha \in I$. Then for any $\alpha \in I$, we have $\alpha = q\beta \in R\beta$ by Theorem 3.2. □

Remark 3.4. We say that R is a **left principal ideal domain** for the property in Lemma 3.3 (see [8]). One can similarly show that R is a **right principal ideal domain**.

Lemma 3.5. *For any odd prime p and any $a \in \mathbb{Z}$, there exist some $x, y \in \mathbb{Z}$ such that $x^2 + y^2 \equiv a \mod p$.*

Proof. Let $p = 2n+1$. Then the set $\{0, \pm 1, \pm 2, \ldots, \pm n\}$ is a representative of $\mathbb{Z}_p$. Since $i^2 \equiv j^2 \mod p \Leftrightarrow i \equiv \pm j \mod p$, the range of x^2 as a function of x, say $\{0^2, 1^2, 2^2, \ldots, n^2\}$, has $n+1$ elements (all are distinct). Similarly, the range of $a - y^2$ as a function of y has $n+1$ elements. Since there are only $2n+1$ elements in $\mathbb{Z}_p$, there exist some $x, y \in \mathbb{Z}$ such that $x^2 \equiv a - y^2 \mod p$, by the Pigeonhole Principle. □

Lemma 3.6. *For any odd prime p, there exist $x, y \in \mathbb{Z}$ such that*

$$x^2 - x + y^2 + 1 \equiv 0 \mod p.$$

Hence, $p \mid N(x + yj + \omega)$.

Proof. Since $x^2 - x \equiv (x - 2^{-1})^2 - 2^{-2} \mod p$, the required equation is $X^2 + y^2 \equiv a \mod p$, where $X := x - 2^{-1}$ and $a := 2^{-2} - 1$. Thus the statement follows from Lemma 3.5. The second statement follows from the identity $N(x + yj + \omega) = (x + yj + \omega)(x - yj + \omega^2) = x^2 - x + y^2 + 1$. □

A non-unit $\alpha \in R$ is said to be **prime** if α satisfies the following:

$$\alpha = \beta\gamma \text{ for some } \beta, \gamma \in R \implies \beta \text{ or } \gamma \text{ is a unit in } R.$$

We show the following by the same way as in [1].

Lemma 3.7. *Any rational prime p is not prime in R.*

Proof. First, we have $2 = (1 + j)(1 - j)$, and hence 2 is not prime even in $\mathbb{Z}[j] \subset R$. If p is an odd rational prime, then by Lemma 3.6, we have $p \mid N(x + yj + \omega)$ for some $x, y \in \mathbb{Z}$. Let $\alpha := x + yj + \omega$. We claim that

$$Rp \subsetneq Rp + R\alpha \subsetneq R.$$

In fact, if $\alpha \in Rp$, then $x+yj+\omega = (a+b\omega+cj+d\omega j)p$ for some $a,b,c,d \in \mathbb{Z}$. Hence, in particular, we have $\sqrt{3}i = bp\sqrt{3}i$, which implies that p is a unit. This is a contradiction. Thus the first inclusion is proper. For the second inclusion, suppose that $\beta p+\gamma\alpha = 1$ for some $\beta,\gamma \in R$. Then we have $N(\gamma\alpha) = N(1-\beta p)$. The left hand side is equal to $N(\gamma)N(\alpha)$ which is a multiple of p. On the other hand, the right hand side is equal to $(1-\beta p)(1-\bar{\beta}p) = 1-(\beta+\bar{\beta})p+N(\beta)p^2 \equiv 1 \mod p$. This is a contradiction. Hence we have shown our claim.

By Lemma 3.3, we have $Rp+R\alpha = R\delta$ for some $\delta \in R$, and so $p = \xi\delta$ for some $\xi \in R$. By our claim above, δ and ξ are non-units. Therefore, p is not a prime in R. □

Lemma 3.8. *For any rational prime p, there exists some $\alpha \in R$ such that $p = N(\alpha)$.*

Proof. Since p is not prime (by Lemma 3.7), we have $p = \alpha\beta$ for some non-units $\alpha,\beta \in R$. Since $p^2 = N(p) = N(\alpha)N(\beta)$, we obtain $p = N(\alpha)$. □

Theorem 3.9. *For any rational prime p, there exist some $a,b,c,d \in \mathbb{Z}$ such that $p = a^2+b^2+3c^2+3d^2$.*

Proof. By Lemma 3.8, let $p = N(\alpha)$ for some $\alpha \in R$. We claim that there exists some $\beta \in R' = \mathbb{Z}[\sqrt{3}i, j]$ such that $p = N(\beta)$.

First, note that $\alpha = 2\ell_1+2\ell_2\omega+2\ell_3 j+2\ell_4\omega j+\varepsilon_1+\varepsilon_2\omega+\varepsilon_3 j+\varepsilon_4\omega j$ for some $\ell_j \in \mathbb{Z}$ and $\varepsilon_i = 0,1$. If $\varepsilon_2 = \varepsilon_4 = 0$, then $\alpha \in R'$. Thus we investigate the other 12 cases, i.e., $\varepsilon_1+\varepsilon_2\omega+\varepsilon_3 j+\varepsilon_4\omega j =$ (i) ω, (ii) ωj, (iii) $1+\omega$, (iv) $1+\omega j$, (v) $\omega+j$, (vi) $\omega+\omega j$, (vii) $j+\omega j$, (viii) $1+\omega+j$ (ix) $1+\omega+\omega j$, (x) $1+j+\omega j$, (xi) $\omega+j+\omega j$, (xii) $1+\omega+j+\omega j$.

For the case (i), let $\beta = \alpha\omega^2 = 2\ell_1\omega^2+2\ell_2+2\ell_3 j\omega^2+2\ell_4\omega^2 j+1 \in R'$ (note $\omega j\omega^2 = \omega^2 j$), and then $N(\beta) = \beta\bar{\beta} = \alpha\omega^2\omega\bar{\alpha} = N(\alpha) = p$. For the case (ii), let $\beta = \omega^2\alpha = 2\ell_1\omega^2+2\ell_2+2\ell_3\omega^2 j+2\ell_4 j+j \in R'$ and then $N(\beta) = \beta\bar{\beta} = \omega^2\alpha\bar{\alpha}\omega = N(\alpha) = p$. For the case (iii), since $1+\omega = -\omega^2$, we let $\beta = \alpha\omega = 2\ell_1\omega+2\ell_2\omega^2+2\ell_3 j\omega+2\ell_4\omega j\omega-1 \in R'$ (note $\omega j\omega = j$). For the case (iv), let

$$\beta = \omega\alpha\omega^2 = 2\ell_1+2\ell_2\omega+2\ell_3\omega^2 j+2\ell_4 j+1+j \in R',$$

and then $N(\beta) = \beta\bar{\beta} = \omega\alpha\omega^2\omega\bar{\alpha}\omega^2 = \omega N(\alpha)\omega^2 = p$. For the case (v), let

$$\beta = \omega\alpha\omega = 2\ell_1\omega^2+2\ell_2+2\ell_3 j+2\ell_4\omega j+1+j \in R',$$

and then $N(\beta) = \beta\bar{\beta} = \omega\alpha\omega\omega^2\bar{\alpha}\omega^2 = \omega N(\alpha)\omega^2 = p$. For the case (vi), let

$$\beta = \omega^2\alpha = 2\ell_1\omega^2 + 2\ell_2 + 2\ell_3\omega^2 j + 2\ell_4 j + 1 + j \in R',$$

and then $N(\beta) = \beta\bar{\beta} = \omega^2\alpha\bar{\alpha}\omega = \omega^2 N(\alpha)\omega = p$. For the case (vii), since $j + \omega j = -\omega^2 j$, we let $\beta = \omega\alpha = 2\ell_1\omega + 2\ell_2\omega^2 + 2\ell_3\omega j + 2\ell_4\omega^2 j - j \in R'$, and get $N(\beta) = \beta\bar{\beta} = \omega\alpha\bar{\alpha}\omega^2 = \omega N(\alpha)\omega^2 = p$. For the case (viii), note that $1 + \omega + j = -\omega^2 + j$. Let

$$\beta = \omega^2\alpha\omega^2 = 2\ell_1\omega + 2\ell_2\omega^2 + 2\ell_3 j + 2\ell_4\omega j - 1 + j \in R',$$

and then $N(\beta) = \beta\bar{\beta} = \omega^2\alpha\omega^2\omega\bar{\alpha}\omega = \omega^2 N(\alpha)\omega = p$. For the case (ix), note that $1 + \omega + \omega j = -\omega^2 + \omega j = -\omega^2 + j\omega^2 = (j-1)\omega^2$. Thus it works as (iii), letting

$$\beta = \alpha\omega = 2\ell_1\omega + 2\ell_2\omega^2 + 2\ell_3 j\omega + 2\ell_4 j + j - 1 \in R'.$$

For the case (x), note that $1 + j + \omega j = 1 - \omega^2 j$. Let

$$\beta = \omega^2\alpha\omega = 2\ell_1 + 2\ell_2\omega + 2\ell_3\omega j + 2\ell_4 j\omega + 1 - j \in R',$$

and then $N(\beta) = \beta\bar{\beta} = \omega^2\alpha\omega\omega^2\omega\bar{\alpha}\omega = \omega^2 N(\alpha)\omega = p$. For the case (xi), note that $\omega + j + \omega j = \omega - \omega^2 j = (1-j)\omega$. Thus it works as (i), letting

$$\beta = \alpha\omega^2 = 2\ell_1\omega^2 + 2\ell_2 + 2\ell_3 j\omega^2 + 2\ell_4\omega^2 j + 1 - j \in R'.$$

For the last case (xii), note that $1 + \omega + j + \omega j = -\omega^2 + (1+\omega)j = -\omega^2(1 + j)$. Thus it works as (vii), letting

$$\beta = \omega\alpha = 2\ell_1\omega + 2\ell_2\omega^2 + 2\ell_3\omega j + 2\ell_4\omega^2 j - 1 - j \in R'.$$

Consequently, we have $p = N(\beta)$ for some $\beta = a + bj + c\sqrt{3}i + d\sqrt{3}ij \in R'$, and hence $p = N(a + b\sqrt{3}i + cj + d\sqrt{3}ij) = a^2 + b^2 + 3c^2 + 3d^2$. □

Since the norm N is multiplicative (see the identity (1)), we also have the following:

Corollary 3.10. *For any natural number n, there exist some $a, b, c, d \in \mathbb{Z}$ such that $n = a^2 + b^2 + 3c^2 + 3d^2$.*

Proof. Let $n = p_1^{m_1} \cdots p_r^{m_r}$ be a prime factorization of n in $\mathbb{N}$. By Lemma 3.8, we have $p_i = N(\beta_i)$ for some $\beta_i \in R'$. Hence, $n = N(\beta_1)^{m_1} \cdots N(\beta_r)^{m_r} = N(\beta_1^{m_1} \cdots \beta_r^{m_r})$, and we are done since $\beta_1^{m_1} \cdots \beta_r^{m_r} \in R'$. □

Remark 3.11. As Legendre's three-square theorem:

$$n = a^2 + b^2 + c^2 \quad \Longleftrightarrow \quad n \neq 4^r(8k+7) \quad \text{for } r,\ k \geq 0$$

(the proof was completed by Gauss), we want to know whether the four terms of $a^2 + b^2 + 3c^2 + 3d^2$ are actually needed to express n. My colleague, Professor Koichi Kawada, answered this question. Namely,

$$n = a^2 + b^2 + 3c^2 \quad \Longleftrightarrow \quad n \neq 3^{2r+1}(3k+2) \quad \text{for } r,\ k \geq 0, \quad \text{and also,}$$

$$n = a^2 + 3b^2 + 3c^2 \quad \Longleftrightarrow \quad n \neq 9^r(3k+2) \quad \text{for } r,\ k \geq 0.$$

These results may be obtained within the classical theory on positive definite ternary quadratic forms (see [10, 1.4-1.5] for instance), so that they had most likely been known already by the end of the 19th century. The author could not find any explicit reference, but observed a proof in an unpublished lecture note of Koichi Kawada.

References

[1] B. Coan and C. Perng, *Factorization of Hurwitz quaternions*, Int. Math. Forum **7**(43) (2012), 2143–2156.

[2] J. Conway and D. Smith, *On quaternions and octonions*, A K Peters, Ltd, 2003.

[3] J. Deutsch, *A quaternionic proof of the universality of some quadratic forms*, Integers, E. J. Comb. Num. Theory **8**(2) A3 (2008); Proc. CANT 2005.

[4] J. Deutsch, *A quaternionic proof of the representation formula of a quaternary quadratic form*, J. Num. Theory **13** (2005), 149–179.

[5] W. Duke, *Some old problems and new results about quadratic forms*, Notices of the AMS **44**(2) (1997), 190–196.

[6] D. Estes and G. Nipp, *Factorization in quaternion orders*, J. Num. Theory **33** (1989), 224–236.

[7] R. Fitzgerald, *Norm euclidean quaternionic orders*, Integers, **11** A58 (2011).

[8] A. Jategaonkar, *Left principal ideal domains*, J. Alg. **8** (1968), 148–155.

[9] J. Liouville, *Sur la forme* $x^2+2y^2+2z^2+4t^2$, J. math. pure appl. **7**, (1862), 1–4.

[10] M. Nathanson, *Additive number theory, the classical bases*, GTM 164, Springer-Verlag, New York (1996).

[11] T. Pepin, *Sur quelques formes quadratiques quaternaires*, J. math. pure appl. **6**, (1890), 5–67.

[12] S. Ramanujan, *On the expression of a number in the form* $ax^2+by^2+cz^2+du^2$, Proc. Cambridge Phil. Soc. **19**, no. I (1917), 11–21.

[13] M.-F. Vingéras, *Arithmétique des algèbres de quaternions*, Springer-Verlag, Berlin, 1980.

Yoji Yoshii
Iwate University
3-18-33 Ueda, Morioka, Iwate, Japan 020-8550
e-mail: yoshii@iwate-u.ac.jp

(Received March 10, 2017)