

# GENERALIZED QUATERNION RINGS OVER $\mathbb{Z}/n\mathbb{Z}$ FOR AN ODD $n$

JOSÉ MARÍA GRAU, CELINO MIGUEL, AND ANTONIO M. OLLER-MARCÉN

ABSTRACT. We consider a generalization of the quaternion ring  $\left(\frac{a,b}{R}\right)$  over a commutative unital ring  $R$  that includes the case when  $a$  and  $b$  are not units of  $R$ . In this paper, we focus on the case  $R = \mathbb{Z}/n\mathbb{Z}$  for and odd  $n$ . In particular, for every odd integer  $n$  we compute the number of non-isomorphic generalized quaternion rings  $\left(\frac{a,b}{\mathbb{Z}/n\mathbb{Z}}\right)$ .

AMS 2010 Mathematics Subject Classification 11R52,16-99

Keywords: Quaternion algebra,  $\mathbb{Z}/n\mathbb{Z}$ , Structure

## 1. INTRODUCTION

The origin of quaternions dates back to 1843, when William Rowan Hamilton considered a 4-dimensional vector space over  $\mathbb{R}$  with basis  $\{1, i, j, k\}$  and defined an associative product given by the now classical rules  $i^2 = j^2 = -1$  and  $ij = -ji = k$ . These so-called “Hamilton quaternions” turned out to be the only division algebra over  $\mathbb{R}$  with dimension greater than 2. Later on, this idea was extended to define quaternion algebras over arbitrary fields. Thus, if  $F$  is a field and  $a, b \in F \setminus \{0\}$  we can define a unital, associative, 4-dimensional algebra over  $F$  just considering a basis  $\{1, i, j, k\}$  and the product given by  $i^2 = a$ ,  $j^2 = b$  and  $ij = -ji = k$ . The structure of quaternion algebras over fields of characteristic different from two is well-known. Indeed, such a quaternion algebra is either a division ring or isomorphic to the matrix ring  $\mathbb{M}_2(F)$  [11, p.19]. This is no longer true if  $F$  is of characteristic 2, since quaternions over  $\mathbb{Z}/2\mathbb{Z}$  are not a division ring but they form a commutative ring, while  $\mathbb{M}_2(\mathbb{Z}/2\mathbb{Z})$  is not commutative. Nevertheless, some authors consider a different product in the characteristic 2 case given by  $i^2 + i = a$ ,  $j^2 = b$ , and  $ji = (i + 1)j = k$ . The algebra defined by this product is isomorphic to the corresponding matrix ring.

Generalizations of the notion of quaternion algebra to other commutative base rings  $R$  have been considered by Kanzaki [5], Hahn [4], Knus [6], Gross and Lucianovic [3], Tuganbaev [15], and most recently by John Voight [16, 17]. Quaternions over finite rings have attracted significant attention since they have applications in coding theory see, [9, 10, 14]. In [2] the case  $R = \mathbb{Z}/n\mathbb{Z}$  was studied proving the following result.

**Theorem 1** ([2], Theorem 4). *Let  $n$  be an integer and let  $a, b$  be such that  $\gcd(a, n) = \gcd(b, n) = 1$ . The following hold:*

i) *If  $n$  is odd, then*

$$\left(\frac{a,b}{\mathbb{Z}/n\mathbb{Z}}\right) \cong \mathbb{M}_2(\mathbb{Z}/n\mathbb{Z}).$$

ii) If  $n = 2^s m$  with  $s > 0$  and  $m$  odd, then

$$\left( \frac{a, b}{\mathbb{Z}/n\mathbb{Z}} \right) \cong \begin{cases} \mathbb{M}_2(\mathbb{Z}/m\mathbb{Z}) \times \left( \frac{-1, -1}{\mathbb{Z}/2^s\mathbb{Z}} \right), & \text{if } s = 1 \text{ or } a \equiv b \equiv -1 \pmod{4}; \\ \mathbb{M}_2(\mathbb{Z}/m\mathbb{Z}) \times \left( \frac{1, 1}{\mathbb{Z}/2^s\mathbb{Z}} \right), & \text{otherwise.} \end{cases}$$

In this paper, we extend the concept of quaternion rings over commutative, associative, unital rings to the case when  $i^2$  and  $j^2$  are not necessarily units of the ring  $R$ . In particular, we will focus on the case  $R = \mathbb{Z}/n\mathbb{Z}$  for an odd  $n$ .

## 2. BASIC CONCEPTS

Let  $R$  be a commutative and associative ring with identity and let  $H(R)$  denote the free  $R$ -module of rank 4 with basis  $\{1, i, j, k\}$ . That is,

$$H(R) = \{x_0 + x_1i + x_2j + x_3k : x_0, x_1, x_2, x_3 \in R\}.$$

Now, let  $a, b \in R$  and define an associative multiplication in  $H(R)$  according to the following rules:

$$\begin{aligned} i^2 &= a, \\ j^2 &= b, \\ ij &= -ji = k. \end{aligned}$$

Thus, we obtain an associative, unital ring called a quaternion ring over  $R$  which is denoted by  $\left( \frac{a, b}{R} \right)$ .

**Definition 1.** A *standard basis* of  $\left( \frac{a, b}{R} \right)$  is any base  $\mathcal{B} = \{1, I, J, K\}$  of the free  $R$ -module  $H(R)$  such that

$$\begin{aligned} I^2 &= a, \\ J^2 &= b, \\ IJ &= -JI = K. \end{aligned}$$

Given the standard basis  $\{1, i, j, k\}$ , the elements of the submodule  $R\langle i, j, k \rangle$  are called pure quaternions. Note that the square of a pure quaternion always lays on  $R$ .

**Remark 1.** Given  $q \in \left( \frac{a, b}{R} \right)$  and a fixed standard basis, there exist  $x_0 \in R$  and a pure quaternion  $q_0$  such that  $q = x_0 + q_0$ . Observe that both  $x_0$  and  $q_0$  are uniquely determined and also that the only pure quaternion in  $R$  is 0.

The following classical concepts are not altered by the fact that  $a$  and  $b$  are not necessarily units.

**Definition 2.** Consider the standard basis  $\{1, i, j, k\}$  and let  $q \in \left( \frac{a, b}{R} \right)$ . Put  $q = x_0 + q_0$  with  $x_0 \in R$  and  $q_0 = x_1i + x_2j + x_3k$  a pure quaternion. Then,

- i) The conjugate of  $q$  is:  $\bar{q} = x_0 - q_0 = x_0 + x_1i - x_2j - x_3k$ .
- ii) The trace of  $q$  is  $\text{tr}(q) = q + \bar{q} = 2x_0$ .
- iii) The norm of  $q$  is  $n(q) = q\bar{q} = x_0^2 - q_0^2 = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$ .

Note that  $n(q), \text{tr}(q) \in R$  and  $n(q_1q_2) = n(q_1)n(q_2)$ .

**Remark 2.** Observe that, if  $q$  is a pure quaternion, then  $\bar{q} = -q$  and  $\text{tr}(q) = 0$ . The converse also holds only if  $R$  has odd characteristic.

In the following result we will see that isomorphisms preserve conjugation. The classical proof in the case when  $a$  and  $b$  are units (see [1, Theorem 5.6] for instance) is no longer valid in our setting and it must be slightly modified.

**Theorem 2.** *Let  $f : \left(\frac{a,b}{R}\right) \rightarrow \left(\frac{c,d}{R}\right)$  be a ring isomorphism. Then, for every  $q \in \left(\frac{a,b}{R}\right)$  it holds that  $f(\bar{q}) = \overline{f(q)}$ .*

*Proof.* Let  $q \in \left(\frac{a,b}{R}\right)$  and put  $q = x_0 + q_0$  with  $x_0 \in R$  and  $q_0$  a pure quaternion. Then,  $\bar{q} = x_0 - q_0$  and  $f(\bar{q}) = f(x_0) - f(q_0) = x_0 - f(q_0)$ . On the other hand,  $\overline{f(q)} = \overline{f(x_0 + q_0)} = \overline{f(x_0) + f(q_0)} = \overline{x_0 + f(q_0)} = x_0 + \overline{f(q_0)}$ . Hence, in order to prove the result, it is enough to prove that  $\overline{f(q_0)} = -f(q_0)$  for every pure quaternion  $q_0$ .

Let us consider the standard basis  $\{1, i, j, k\}$  of  $\left(\frac{a,b}{R}\right)$ . Then,  $f(i) = \alpha_1 + q_1$  with  $\alpha_1 \in R$  and  $q_1$  a pure quaternion in  $\left(\frac{c,d}{R}\right)$ . Now, since  $i^2 \in R$  and taking into account that  $f$  fixes  $R$ , we have that  $f(i^2) = f(i)^2 = (\alpha_1 + q_1)^2 = \alpha_1^2 + q_1^2 + 2\alpha_1 q_1 \in R$ . Consequently,  $2\alpha_1 q_1 \in R$  (because both  $\alpha_1^2$  and  $q_1^2$  are in  $R$ ) and since  $2\alpha_1 q_1$  is a pure quaternion, it must be  $2\alpha_1 q_1 = 0$ . Thus,  $f(2\alpha_1 i) = 2\alpha_1 f(i) = 2\alpha_1^2$  and, since  $f$  fixes  $R$ , it follows that  $2\alpha_1 i = 0$  and also that  $2\alpha_1 = 0$ . Equivalently,  $\alpha_1 = -\alpha_1$  and then,  $\overline{f(i)} = \alpha_1 - q_1 = -\alpha_1 - q_1 = -f(i)$ .

In the same way, it can be seen that  $\overline{f(j)} = -f(j)$  and  $\overline{f(k)} = -f(k)$ . Thus, if  $q_0 = Ai + Bj + Ck$  is a pure quaternion in  $\left(\frac{a,b}{R}\right)$  we have that:

$$\overline{f(q_0)} = A\overline{f(i)} + B\overline{f(j)} + C\overline{f(k)} = -Af(i) - Bf(j) - Cf(k) = -f(q_0),$$

and the result follows.  $\square$

Since both the trace and the norm are defined in terms of the conjugation, the following result easily follows from Theorem 2.

**Corollary 1.** *Let  $f : \left(\frac{a,b}{R}\right) \rightarrow \left(\frac{c,d}{R}\right)$  be a ring isomorphism. Then, for every  $q \in \left(\frac{a,b}{R}\right)$  the following hold.*

- i)  $\text{tr}(f(q)) = \text{tr}(q)$ .
- ii)  $\text{n}(f(q)) = \text{n}(q)$ .

**Remark 3.** Theorem 2 and Corollary 1 imply in particular that the conjugate, the trace and the norm of an element are independent from the standard basis of  $\left(\frac{a,b}{R}\right)$  used to compute them. Moreover, according to Remark 2, Theorem 2 implies that (in the odd characteristic case) every isomorphism preserves pure quaternions.

**Proposition 1.** *Let  $R$  be a ring with odd characteristic and Let  $f : \left(\frac{a,b}{R}\right) \rightarrow \left(\frac{a,c}{R}\right)$  be a ring isomorphism. Then, for some pair of standard bases the matrix of  $f$  has the form*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha_1 & \alpha_2 \\ 0 & 0 & \beta_1 & \beta_2 \\ 0 & 0 & \gamma_1 & \gamma_2 \end{pmatrix},$$

with  $\alpha_1 a = \alpha_2 a = 0$ .

*Proof.* Let  $\{1, i, j, k\}$  be any standard basis in  $\left(\frac{a, b}{R}\right)$ . Since  $f(i)^2 = f(i^2) = a$ , let us consider  $S$  the subring of  $\left(\frac{a, c}{R}\right)$  generated by  $\{1, f(i)\}$ . Now, we apply the Cayley-Dickson process [13] to  $S$  and  $c$  so that we extend  $\{1, f(i)\}$  to an standard basis  $\{1, I := f(i), J, K\}$  of  $\left(\frac{a, c}{R}\right)$ .

Now, since  $R$  has odd characteristic,  $f$  preserves pure quaternions. Thus,  $f(j) = \alpha_1 I + \beta_1 J + \gamma_1 K$  and  $f(k) = \alpha_2 I + \beta_2 J + \gamma_2 K$ .

Finally,  $f(k) = f(ij) = f(i)f(j) = I(\alpha_1 I + \beta_1 J + \gamma_1 K) = \alpha_1 a + \beta_1 K + \gamma_1 a J$  must be a pure quaternion and hence  $\alpha_1 a = 0$ . In the same way it can be seen that  $\alpha_2 a = 0$  and the result follows.  $\square$

In what follows, we will be interested in determining whether two different quaternion rings are isomorphic or not. The following isomorphism, which is well-known if  $a$  and  $b$  are units, also holds in our setting. The proof is straightforward.

**Lemma 1.** *Let  $a, b \in R$ . Then,*

$$\left(\frac{a, b}{R}\right) \cong \left(\frac{b, a}{R}\right).$$

Nevertheless, some other easy isomorphisms that hold in the case when  $a$  and  $b$  are units, like

$$(1) \quad \left(\frac{a, b}{R}\right) \cong \left(\frac{a, -ab}{R}\right) \cong \left(\frac{b, -ab}{R}\right)$$

are, as we will see, no longer generally true in our setting.

### 3. SOME RESULTS REGARDING $\left(\frac{a, b}{\mathbb{Z}/p^k\mathbb{Z}}\right)$ FOR A PRIME $p$

Throughout this section  $p$  will denote any prime. The next two results present some isomorphisms that will be useful in forthcoming sections. The first one (Lemma 2) is, in some sense, an analogue to the classical isomorphism (1). The second one (Lemma 3) presents some kind of descent principle.

**Lemma 2.** *Let  $a$  and  $b$  be integers with  $\gcd(a, p) = 1$ . Then,*

$$\left(\frac{a, bp^s}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \left(\frac{a, -abp^s}{\mathbb{Z}/p^k\mathbb{Z}}\right).$$

*Proof.* Let us consider standard bases  $\{1, i, j, k\}$  and  $\{1, I, J, K\}$  of  $\left(\frac{a, bp^s}{\mathbb{Z}/p^k\mathbb{Z}}\right)$  and  $\left(\frac{a, -abp^s}{\mathbb{Z}/p^k\mathbb{Z}}\right)$ , respectively. Then it is enough to consider the ring homomorphism  $f$  induced by  $f(1) = 1$ ,  $f(I) = i$ ,  $f(J) = k$  and  $f(K) = aj$ ; which is bijective because its coordinate matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & a \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

is regular over  $\mathbb{Z}/p^k\mathbb{Z}$ .  $\square$

**Lemma 3.** Let  $a_i$  ( $1 \leq i \leq 4$ ) and  $k \geq 1$  be integers such that

$$\left( \frac{a_1, a_2}{\mathbb{Z}/p^k\mathbb{Z}} \right) \cong \left( \frac{a_3, a_4}{\mathbb{Z}/p^k\mathbb{Z}} \right)$$

and let  $s \leq k$ . If  $a_i \equiv a'_i \pmod{p^s}$  for every  $1 \leq i \leq 4$ , then

$$\left( \frac{a'_1, a'_2}{\mathbb{Z}/p^s\mathbb{Z}} \right) \cong \left( \frac{a'_3, a'_4}{\mathbb{Z}/p^s\mathbb{Z}} \right)$$

*Proof.* Let  $f$  be an isomorphism between  $\left( \frac{a_1, a_2}{\mathbb{Z}/p^k\mathbb{Z}} \right)$  and  $\left( \frac{a_3, a_4}{\mathbb{Z}/p^k\mathbb{Z}} \right)$ . If  $A$  is the coordinate matrix of  $f$  with respect to some standard bases, it is obvious that  $A$  is regular over  $\mathbb{Z}/p^k\mathbb{Z}$  and, consequently, also over  $\mathbb{Z}/p^s\mathbb{Z}$ .

Then, the linear map  $g$  between  $\left( \frac{a'_1, a'_2}{\mathbb{Z}/p^s\mathbb{Z}} \right)$  and  $\left( \frac{a'_3, a'_4}{\mathbb{Z}/p^s\mathbb{Z}} \right)$  defined by the matrix  $A$  with respect to some standard bases, induces an ring isomorphism because  $a_i \equiv a'_i \pmod{p^s}$  for every  $i$ .  $\square$

It is also interesting, and often harder, to determine whether two quaternion rings are not isomorphic. The following results go in this direction.

**Lemma 4.** Let  $p$  be a prime and consider integers  $a, b$  and  $c$  coprime to  $p$ . Also, let  $0 \leq s \leq r < k$ . Then, the quaternion rings  $R_1, R_2$  and  $R_3$  defined by

$$R_1 = \left( \frac{ap^s, bp^r}{\mathbb{Z}/p^k\mathbb{Z}} \right), \quad R_2 = \left( \frac{cp^s, 0}{\mathbb{Z}/p^k\mathbb{Z}} \right), \quad R_3 = \left( \frac{0, 0}{\mathbb{Z}/p^k\mathbb{Z}} \right)$$

are pairwise non-isomorphic.

*Proof.* For each  $i \in \{1, 2, 3\}$  let us define the set  $\mathbb{P}_i := \{q \in R_i : \text{tr}(q) = 0\}$ .

Note that, if  $p$  is odd, then  $\mathbb{P}_i$  is precisely the set of pure quaternions and is hence preserved by isomorphisms. Now, for every element  $q \in \mathbb{P}_3$  it holds that  $q^2 = 0$ , while  $\mathbb{P}_1$  and  $\mathbb{P}_2$  contain elements whose square is non-zero. This implies that  $R_3$  is not isomorphic to  $R_1$  or  $R_2$ . On the other hand, the set  $\mathbb{P}_2 \setminus p\mathbb{P}_2$  contains elements with zero square while this is not the case for  $\mathbb{P}_1 \setminus p\mathbb{P}_1$ . This implies that  $R_1$  and  $R_2$  are not isomorphic.

Finally, if  $p = 2$ , then  $\mathbb{P}_i = \{\alpha 2^{k-1} + q_0 : \alpha \text{ is odd and } q_0 \text{ is a pure quaternion}\}$  and we can reason in the same way.  $\square$

**Lemma 5.** Let  $p$  be a prime and consider integers  $a, b, c$  and  $d$  coprime to  $p$ . Also, let  $s_1 \leq s_2 \leq k$  and  $s_3 \leq s_4 \leq k$  and assume that either  $s_1 \neq s_3$  or  $s_2 \neq s_4$ . Then

$$\left( \frac{ap^{s_1}, bp^{s_2}}{\mathbb{Z}/p^k\mathbb{Z}} \right) \not\cong \left( \frac{cp^{s_3}, dp^{s_4}}{\mathbb{Z}/p^k\mathbb{Z}} \right)$$

*Proof.* Let us assume that both rings are isomorphic. Without loss of generality, we can also assume that  $s_1 \leq s_3$ . Five different situations arise:

i) If  $s_1 = s_3 = s_2 < s_4$ , then Lemma 3 implies that

$$\left( \frac{ap^{s_1}, bp^{s_1}}{\mathbb{Z}/p^{s_4}\mathbb{Z}} \right) \cong \left( \frac{cp^{s_1}, 0}{\mathbb{Z}/p^{s_4}\mathbb{Z}} \right),$$

which contradicts Lemma 4.

ii) If  $s_1 = s_3 < s_2 < s_4$ , then due to Lemma 3 we have that

$$\left( \frac{ap^{s_1}, bp^{s_2}}{\mathbb{Z}/p^{s_4}\mathbb{Z}} \right) \cong \left( \frac{cp^{s_1}, 0}{\mathbb{Z}/p^{s_4}\mathbb{Z}} \right),$$

which contradicts Lemma 4.

iii) If  $s_1 = s_2 < s_3$ , by Lemma 3 we have that

$$\left( \frac{ap^{s_1}, bp^{s_1}}{\mathbb{Z}/p^{s_3}\mathbb{Z}} \right) \cong \left( \frac{0, 0}{\mathbb{Z}/p^{s_3}\mathbb{Z}} \right),$$

which contradicts Lemma 4 again.

iv) If  $s_1 < s_2 \leq s_3$ , Lemma 3 implies that

$$\left( \frac{ap^{s_1}, 0}{\mathbb{Z}/p^{s_2}\mathbb{Z}} \right) \cong \left( \frac{0, 0}{\mathbb{Z}/p^{s_2}\mathbb{Z}} \right),$$

contradicting Lemma 4.

v) If  $s_1 < s_3 \leq s_2$ , Lemma 3 leads to

$$\left( \frac{ap^{s_1}, 0}{\mathbb{Z}/p^{s_3}\mathbb{Z}} \right) \cong \left( \frac{0, 0}{\mathbb{Z}/p^{s_3}\mathbb{Z}} \right),$$

which is a contradiction due to Lemma 4.

Hence, in any case we reach a contradiction and the result follows.  $\square$

#### 4. QUATERNIONS OVER $\mathbb{Z}/p^k\mathbb{Z}$ FOR AN ODD PRIME $p$

This section is devoted to determine the number of non-isomorphic generalized quaternion rings over  $\mathbb{Z}/p^k\mathbb{Z}$  for an odd prime  $p$ . Hence, throughout this section  $p$  will be assumed to be an odd prime.

**Lemma 6.** *Let  $s$  and  $t$  be integers coprime to  $p$  such that  $st$  is a quadratic residue modulo  $p$  and let  $m$  be any integer. Then, for every  $r \geq 0$ ,*

$$R = \left( \frac{tp^r, m}{\mathbb{Z}/p^k\mathbb{Z}} \right) \cong \left( \frac{sp^r, m}{\mathbb{Z}/p^k\mathbb{Z}} \right) = S.$$

*Proof.* Since  $\gcd(st, p) = 1$ , it follows that  $st$  is also a quadratic residue modulo  $p^k$  so let  $x$  be an integer such that  $x^2 \equiv ts^{-1} \pmod{p^k}$ . Let us consider  $\{1, i, j, k\}$  and  $\{1, I, J, K\}$  standard bases of  $R$  and  $S$ , respectively. Then, the linear map whose matrix with respect to these bases is

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & x \end{pmatrix}$$

induces an isomorphism because  $(xI)^2 = x^2I^2 \equiv ts^{-1}sp^r \equiv tp^r \pmod{p^k}$  and  $A$  is regular over  $\mathbb{Z}/p^k\mathbb{Z}$ .  $\square$

**Lemma 7.** *Let  $s$  be an integer such that  $\gcd(p, s) = 1$ . Then, for every  $r \geq 0$ ,*

$$R = \left( \frac{p^r, p^r}{\mathbb{Z}/p^k\mathbb{Z}} \right) \cong \left( \frac{sp^r, sp^r}{\mathbb{Z}/p^k\mathbb{Z}} \right) = S$$

*Proof.* Let  $x, y \in \mathbb{Z}/p^k\mathbb{Z}^*$  such that  $x^2 + y^2 \equiv s^{-1} \pmod{p^k}$  (the exist due to [2, Proposition 1]). Now let us consider  $\{1, i, j, k\}$  and  $\{1, I, J, K\}$  standard bases of  $R$  and  $S$ , respectively. Then, the linear map whose matrix with respect to these bases is

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x & -y & 0 \\ 0 & y & x & 0 \\ 0 & 0 & 0 & s^{-1} \end{pmatrix}$$

induces an isomorphism because

$$\begin{aligned}(xI + yJ)^2 &= (x^2 + y^2)sp^r \equiv p^r \pmod{p^k}, \\ (-yI + xJ)^2 &= (x^2 + y^2)sp^r \equiv p^r \pmod{p^k}, \\ (xI + yJ)(-yI + xJ) &\equiv (x^2 + y^2)K \equiv s^{-1}K \pmod{p^k}\end{aligned}$$

and  $A$  is regular over  $\mathbb{Z}/p^k\mathbb{Z}$ .  $\square$

**Lemma 8.** *Let  $u$  be a quadratic nonresidue modulo  $p$  with  $p \nmid u$  and consider integers  $a$  and  $b$  coprime to  $p$  and let  $0 \leq s$ . Then,*

i)

$$\left(\frac{1, ap^s}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \left(\frac{1, p^s}{\mathbb{Z}/p^k\mathbb{Z}}\right) \text{ and } \left(\frac{u, p^s}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \left(\frac{u, bp^s}{\mathbb{Z}/p^k\mathbb{Z}}\right)$$

ii) *The isomorphism*

$$\left(\frac{1, p^s}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \left(\frac{u, p^s}{\mathbb{Z}/p^k\mathbb{Z}}\right)$$

*holds if and only if  $s = 0$ .*

*Proof.* i) To see that  $R = \left(\frac{1, p^s}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \left(\frac{1, ap^s}{\mathbb{Z}/p^k\mathbb{Z}}\right) = S$ , let us consider  $\{1, i, j, k\}$  and  $\{1, I, J, K\}$  standard bases of  $R$  and  $S$ , respectively. It is obvious that there exist  $x, y \in \mathbb{Z}/p^k\mathbb{Z}$  with  $\gcd(p, y) = 1$  such that  $x^2 - y^2 \equiv a^{-1} \pmod{p^k}$ . Then, the linear map whose matrix with respect to these bases is

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x & y \\ 0 & 0 & y & x \end{pmatrix}$$

induces an isomorphism because

$$(xj + yk)^2 = x^2j^2 + y^2k^2 = x^2ap^s - y^2ap^s = ap^s(x^2 - y^2) \equiv p^s \pmod{p^k}$$

and  $A$  is regular over  $\mathbb{Z}/p^k\mathbb{Z}$ .

The remaining isomorphism can be proved in a similar way.

ii) Assume that  $s > 0$ . To see that  $\left(\frac{1, p^s}{\mathbb{Z}/p^k\mathbb{Z}}\right) \not\cong \left(\frac{u, p^s}{\mathbb{Z}/p^k\mathbb{Z}}\right)$  it is enough to

observe that  $\left(\frac{1, p^s}{\mathbb{Z}/p^k\mathbb{Z}}\right)$  does not contain any pure quaternion  $q$  with  $q^2 = u$ . In fact, if  $\{1, i, j, k\}$  is a standard basis,  $q = ai + bj + ck$  and  $q^2 = a^2 + (b^2 - c^2)p^s$ . Hence, if  $q^2 \equiv u \pmod{p^k}$  it follows that  $u$  is a quadratic residue modulo  $p$ , which is a contradiction.

On the other hand, if  $s = 0$ , we know that  $\left(\frac{1, 1}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \left(\frac{u, 1}{\mathbb{Z}/p^k\mathbb{Z}}\right)$  using [2, Theorem 4].  $\square$

**Lemma 9.** *Let  $u$  be a quadratic nonresidue modulo  $p$  with  $p \nmid u$  and let  $0 < s < k$ . Then,*

$$\text{i) } R_1 = \left(\frac{up^s, p^s}{\mathbb{Z}_{p^k}}\right) \not\cong \left(\frac{p^s, p^s}{\mathbb{Z}_{p^k}}\right) = R_2.$$

$$\text{ii) } S_1 = \left(\frac{up^s, 0}{\mathbb{Z}_{p^k}}\right) \not\cong \left(\frac{p^s, 0}{\mathbb{Z}_{p^k}}\right) = S_2.$$

*Proof.* i) Let us consider the following sets:

$$N_1 := \{q \in R_1 : q \text{ is a pure quaternion, } n(q) = 0, pq \neq 0\},$$

$$N_2 := \{q \in R_2 : q \text{ is a pure quaternion, } n(q) = 0, pq \neq 0\}.$$

In order to prove that  $R_1 \not\cong R_2$  we will see that  $\text{card}(N_1) \neq \text{card}(N_2)$ .

To do so, let  $\{1, i, j, k\}$  and  $\{1, I, J, K\}$  be standard bases of  $R_1$  and  $R_2$ , respectively. Then, if  $q_1 \in N_1$ , it must be  $q_1 = x_1i + x_2j + x_3k$  with  $x_1^2up^s + x_2^2p^s - x_3^2up^{2s} \equiv 0 \pmod{p^k}$  and  $p \nmid x_l$  for some  $l \in \{1, 2, 3\}$ . On the other hand, if  $q_2 \in N_2$ , it must be  $q_2 = y_1I + y_2J + y_3K$  with  $y_1^2p^s + y_2^2p^s - y_3^2p^{2s} \equiv 0 \pmod{p^k}$  and  $p \nmid y_l$  for some  $l \in \{1, 2, 3\}$ .

Thus,  $\text{card}(R_1)$  is the number of non-zero solutions of the congruence

$$(2) \quad x_1^2u + x_2^2 - x_3^2up^s \equiv 0 \pmod{p^{k-s}},$$

while  $\text{card}(R_2)$  is the number of non-zero solutions of the congruence

$$(3) \quad y_1^2 + y_2^2 - y_3^2p^s \equiv 0 \pmod{p^{k-s}}.$$

Now, reducing modulo  $p$ , we can see that:

- If  $-1$  is a quadratic residue  $\pmod{p}$  (i.e., if  $p \equiv 1 \pmod{4}$ ), then the congruence (3) has non-zero solutions while the congruence (2) has not.
- If  $-1$  is a quadratic nonresidue  $\pmod{p}$  (i.e., if  $p \equiv 3 \pmod{4}$ ), then the congruence (2) has non-zero solutions while the congruence (3) has not.

In any case, it follows that  $\text{card}(N_1) \neq \text{card}(N_2)$  as claimed.

- ii) For this case, it is enough to observe that  $S_2$  does not contain pure quaternions  $q$  such that  $q^2 = up^s$ , while  $S_1$  obviously does contain such type of elements. To do so, just note that the congruence  $x^2p^s \equiv up^s \pmod{p^k}$  has no solutions because  $u$  is a quadratic nonresidue modulo  $p$ . □

**Lemma 10.** *Let  $u$  be a quadratic nonresidue  $\pmod{p}$  with  $p \nmid u$  and let  $0 < s < r < k$ . Then, the quaternion rings  $R_1 = \left(\frac{up^s, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right)$ ,  $R_2 = \left(\frac{p^s, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right)$ ,  $R_3 = \left(\frac{up^s, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right)$  and  $R_4 = \left(\frac{p^s, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right)$  are pairwise non-isomorphic.*

*Proof.* Let us see that  $R_1 \not\cong R_2$ ,  $R_1 \not\cong R_4$ ,  $R_2 \not\cong R_3$  and  $R_3 \not\cong R_4$ . If they were isomorphic, the due to Lemma 3 we would have (reducing modulo  $p^r$ ) that  $\left(\frac{up^s, 0}{\mathbb{Z}/p^r\mathbb{Z}}\right) \cong \left(\frac{p^s, 0}{\mathbb{Z}/p^r\mathbb{Z}}\right)$ , which contradicts Lemma 9.

Now, let us see that  $R_1 \not\cong R_3$ . Assume that  $R_1 \cong R_3$ . Then, due to Proposition 1, we can consider  $\{1, i, j, k\}$  and  $\{1, I, J, K\}$  standard bases of  $R_1$  and  $R_3$ , respectively such that the matrix of the isomorphism with respect to these bases is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha_1 & \alpha_2 \\ 0 & 0 & \beta_1 & \beta_2 \\ 0 & 0 & \gamma_1 & \gamma_2 \end{pmatrix},$$

with  $\alpha_1up^s = 0$ .

In particular,  $up^r = j^2 = f(j^2) = f(j)^2 = (\alpha_1I + \beta_1J + \gamma_1K)^2 = \alpha_1^2up^s + \beta_1^2p^r - \gamma_1^2up^{r+s} = \beta_1^2p^r - \gamma_1^2u^2p^{r+s}$ . In other words,  $\beta_1^2p^r - \gamma_1^2up^{r+s} \equiv up^r \pmod{p^k}$



but this implies that  $\beta_1^2 - \gamma_1^2 up^s \equiv u \pmod{p^{k-r}}$  and, consequently, that  $\beta_1^2 \equiv u \pmod{p}$  which is a contradiction because  $u$  is a quadratic nonresidue.

The remaining case, namely  $R_2 \not\cong R_4$  can be proved in the exact same way.  $\square$

**Corollary 2.** *Let  $u$  be a quadratic nonresidue modulo  $p$  with  $p \nmid u$ . Consider integers  $a$  and  $b$  coprime to  $p$  and let  $0 < r$ . Then,*

$$\left(\frac{a, bp^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \begin{cases} \left(\frac{u, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), & \text{if } a \text{ is a quadratic nonresidue modulo } p; \\ \left(\frac{1, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), & \text{if } a \text{ is a quadratic residue modulo } p. \end{cases}$$

*Proof.* If  $a$  is a quadratic nonresidue:

$$\left(\frac{a, bp^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \stackrel{\text{Lem. 8}}{\cong} \left(\frac{a, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \stackrel{\text{Lem. 6}}{\cong} \left(\frac{u, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right).$$

Now, if  $a$  is a quadratic residue:

$$\left(\frac{a, bp^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \stackrel{\text{Lem. 6}}{\cong} \left(\frac{1, bp^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \stackrel{\text{Lem. 8}}{\cong} \left(\frac{1, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right).$$

Finally,  $\left(\frac{u, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right)$  and  $\left(\frac{1, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right)$  are not isomorphic due to Lemma 8.  $\square$

**Corollary 3.** *Let  $u$  be a quadratic nonresidue modulo  $p$  with  $p \nmid u$ . Consider integers  $a$  and  $b$  coprime to  $p$  and let  $0 < r$ . Then,*

$$\left(\frac{ap^r, bp^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \begin{cases} \left(\frac{up^r, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), & \text{if } ab \text{ is a quadratic nonresidue modulo } p; \\ \left(\frac{p^r, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), & \text{if } ab \text{ is a quadratic residue modulo } p. \end{cases}$$

*Proof.* If  $ab$  is a quadratic nonresidue, only one among  $a$  and  $b$  is a quadratic residue. We can assume without loss of generality that  $a$  is a quadratic residue and that  $b$  is a quadratic nonresidue (so  $ub$  is a quadratic residue) and then:

$$\left(\frac{ap^r, bp^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \stackrel{\text{Lem. 6}}{\cong} \left(\frac{ap^r, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \stackrel{\text{Lem. 6}}{\cong} \left(\frac{p^r, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right).$$

Now, if  $ab$  is a quadratic residue:

$$\left(\frac{ap^r, bp^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \stackrel{\text{Lem. 6}}{\cong} \left(\frac{bp^r, bp^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \stackrel{\text{Lem. 7}}{\cong} \left(\frac{p^r, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right).$$

Finally,  $\left(\frac{p^r, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right)$  and  $\left(\frac{up^r, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right)$  are not isomorphic due to Lemma 9.  $\square$

**Corollary 4.** *Let  $u$  be a quadratic nonresidue modulo  $p$  with  $p \nmid u$ . Consider integers  $a$  and  $b$  coprime to  $p$  and let  $0 < s < r$ . Then,*

$$\left(\frac{ap^s, bp^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \begin{cases} \left(\frac{up^s, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), & \text{if only } b \text{ is a quadratic residue modulo } p; \\ \left(\frac{p^s, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), & \text{if only } a \text{ is a quadratic residue } \pmod{p}; \\ \left(\frac{p^s, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), & \text{if both } a \text{ and } b \text{ are quadratic residues modulo } p. \\ \left(\frac{up^s, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), & \text{if both } a \text{ and } b \text{ are quadratic nonresidues modulo } p. \end{cases}$$

*Proof.* Like in the previous results, it is enough to apply Lemma 6 repeatedly. The four different cases that arise are non-isomorphic due to Lemma 10.  $\square$

Now, we can prove the main result of this section.

**Theorem 1.** *Let  $p$  be an odd prime and let  $k$  be a positive integer. Then, there exist exactly  $2k^2 + 2$  non-isomorphic generalized quaternion rings over  $\mathbb{Z}/p^k\mathbb{Z}$ .*

*Proof.* Taking into account the previous results, any generalized quaternion ring over  $\mathbb{Z}/p^k\mathbb{Z}$  is isomorphic to one of the following:

$$\left(\frac{up^s, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), \left(\frac{p^s, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), \left(\frac{up^s, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), \left(\frac{p^s, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right),$$

where  $u$  is a quadratic nonresidue (mod  $p$ ) with  $p \nmid u$  and  $0 \leq s \leq r \leq k$ .

- If  $0 = s = r$ , due to Lemmata 1, 7 and 8, there is only one ring to consider, namely  $\left(\frac{1, 1}{\mathbb{Z}/p^k\mathbb{Z}}\right)$ .
- If  $0 = s < r < k$ , we must consider the rings

$$\left(\frac{u, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), \left(\frac{1, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), \left(\frac{u, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), \left(\frac{1, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right).$$

Due to Lemma 8 we know that  $\left(\frac{u, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \left(\frac{u, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right)$ ,  $\left(\frac{1, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \left(\frac{1, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right)$  and  $\left(\frac{u, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \not\cong \left(\frac{1, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right)$ . Hence, in this case we have 2 non-isomorphic generalized quaternion rings for each  $1 \leq r \leq k - 1$ . A total of  $2(k - 1)$ .

- If  $0 = s$  and  $k = r$  we must only consider the rings

$$\left(\frac{u, 0}{\mathbb{Z}/p^k\mathbb{Z}}\right), \left(\frac{1, 0}{\mathbb{Z}/p^k\mathbb{Z}}\right)$$

which are non-isomorphic due to Lemma 8. Thus, in this case we have 2 non-isomorphic generalized quaternion rings.

- If  $0 < s = r < k$ , we must consider the rings

$$\left(\frac{up^r, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), \left(\frac{p^r, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), \left(\frac{up^r, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right), \left(\frac{p^r, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right).$$

Using Lemma 1, Lemma 7 and Lemma 9 we know that  $\left(\frac{up^r, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \left(\frac{p^r, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \not\cong \left(\frac{up^r, p^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong \left(\frac{p^r, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right)$ . Hence, in this case we have 2 non-isomorphic generalized quaternion rings for each  $1 \leq r \leq k - 1$  for a total of  $2(k - 1)$ .

- If  $0 < s < r < k$ , Lemma 10 implies that the four rings are non-isomorphic. Hence, in this case we have 2 non-isomorphic generalized quaternion rings for each  $1 \leq s \leq k - 2$  and each  $s + 1 \leq r \leq k - 1$ . A total of  $2(k - 2)(k - 1)$ .
- If  $0 < s < r = k$ , we must only consider the rings

$$\left(\frac{up^s, 0}{\mathbb{Z}/p^k\mathbb{Z}}\right), \left(\frac{p^s, 0}{\mathbb{Z}/p^k\mathbb{Z}}\right)$$

which are non-isomorphic due to Lemma 9. Thus, in this case we have 2 non-isomorphic generalized quaternion rings for each  $1 \leq s \leq k - 1$ . A total of  $2(k - 1)$ .

- If  $s = r = k$  there is only one ring to consider, namely  $\left(\frac{0, 0}{\mathbb{Z}/p^k\mathbb{Z}}\right)$ .

Finally, taking into consideration all the previous information, we conclude that there exist

$$1 + 2(k - 1) + 2 + 2(k - 1) + 2(k - 2)(k - 1) + 2(k - 1) + 1 = 2k^2 + 2$$

non-isomorphic generalized quaternion rings over  $\mathbb{Z}/p^k\mathbb{Z}$ .  $\square$

**Remark 4.** The sequence  $a_k = 2k^2 + 2$  is sequence A005893 in the OEIS.

5. QUATERNIONS OVER  $\mathbb{Z}/n\mathbb{Z}$  FOR AN ODD  $n$ 

Note that if  $n = p_1^{r_1} \dots p_k^{r_k}$  is the prime factorization of  $n$ , then by the Chinese Remainder Theorem we have that

$$(4) \quad \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_k^{r_k}\mathbb{Z}.$$

Decomposition (4) induces a natural isomorphism

$$(5) \quad \left( \frac{a, b}{\mathbb{Z}/n\mathbb{Z}} \right) \cong \left( \frac{a, b}{\mathbb{Z}/p_1^{r_1}\mathbb{Z}} \right) \oplus \dots \oplus \left( \frac{a, b}{\mathbb{Z}/p_k^{r_k}\mathbb{Z}} \right).$$

Consequently, if we denote by  $\omega(n)$  the number of different primes dividing  $n$  and by  $\nu_p(n)$  the  $p$ -adic order of  $n$  we obtain the following corollary to Theorem 1.

**Corollary 5.** *Let  $n$  be an odd integer. Then, the number of non-isomorphic generalized quaternion rings over  $\mathbb{Z}/n\mathbb{Z}$  is*

$$2^{\omega(n)} \prod_{p|n} (\nu_p(n)^2 + 1).$$

## REFERENCES

- [1] Conrad, K. Quaternion algebras. [www.math.uconn.edu/~kconrad/blurbs/ringtheory/quaternionalg.pdf](http://www.math.uconn.edu/~kconrad/blurbs/ringtheory/quaternionalg.pdf), 2016.
- [2] Grau, J.M.; Miguel, C.J. and Oller-Marcén A.M. On the structure of quaternion rings over  $\mathbb{Z}/n\mathbb{Z}$  *Advances in Applied Clifford Algebras*, 25(4): 875-887, 2015
- [3] Gross, B.H. and Lucianovic, M.W. On cubic rings and quaternion rings. *J. Number Theory*, 129(6):1468–1478, 2009.
- [4] Hahn, A.J. *Quadratic algebras, Clifford algebras, and arithmetic Witt groups*. Universitext. Springer-Verlag, New York, 1994.
- [5] Kanzaki, T. On non-commutative quadratic extensions of a commutative ring. *Osaka J. Math.*, 10:597–605, 1973.
- [6] Knus, M-A. *Quadratic and Hermitian forms over rings*, volume 294 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1991.
- [7] Miguel, C.J. and Serôdio, R. On the structure of quaternion rings over  $\mathbb{Z}_p$ . *Int. J. Algebra*, 5(25-28):1313–1325, 2011.
- [8] O’Meara, T. *Introduction to quadratic forms*. Classics in Mathematics. Springer-Verlag, Berlin, 2000.
- [9] Özdemir, M. The roots of a split quaternion. *Appl. Math. Lett.*, 22(2):258–263, 2009.
- [10] Özen, M. and Güzeltepe, M. Cyclic codes over some finite quaternion integer rings. *J. Franklin Inst.*, 348(7):1312–1317, 2011.
- [11] Pierce, R.S. *Associative algebras*. Springer-Verlag, New York, 1982.
- [12] Rosen, K.H. *Elementary number theory and its applications*. Addison-Wesley, Reading, MA, 2000.
- [13] Schafer, R.D. *An introduction to nonassociative algebras*. Dover Publications, New York, 1995.
- [14] Tariq Shah and Summera Said Rasool. On codes over quaternion integers. *Appl. Algebra Engng. Comm. Comput.*, 24(6):477–496, 2013.
- [15] Tuganbaev, A. A. Quaternion algebras over commutative rings. (Russian). *Math. Notes*, 53(1-2):204–207, 1993.
- [16] Voight, J. Characterizing quaternion rings over an arbitrary base. *J. Reine Angew. Math.*, 657:113–134, 2011.
- [17] Voight, J. Identifying the matrix ring: Algorithms for quaternion algebras and quadratic forms. In K.Alladi, M.Bhargava, D.Savitt, and P.H. Tiep (Eds.) *Quadratic and Higher Degree Forms* (255–298). Springer New York, 2013.

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DE OVIEDO, AVDA. CALVO SOTELO s/N,  
33007 OVIEDO, SPAIN

*E-mail address:* [grau@uniovi.es](mailto:grau@uniovi.es)

INSTITUTO DE TELECOMUNICAÇÕES, POLO DE COVILHA

*E-mail address:* [celino@ubi.pt](mailto:celino@ubi.pt)

CENTRO UNIVERSITARIO DE LA DEFENSA DE ZARAGOZA, CTRA. HUESCA s/N, 50090 ZARAGOZA,  
SPAIN

*E-mail address:* [oller@unizar.es](mailto:oller@unizar.es)