

Adv. Appl. Clifford Algebras (2018) 28:17 © 2018 Springer International Publishing AG, part of Springer Nature 0188-7009/010001-14 published online February 7, 2018 https://doi.org/10.1007/s00006-018-0839-x

Advances in Applied Clifford Algebras



Generalized Quaternion Rings over $\mathbb{Z}/n\mathbb{Z}$ for an Odd n

José María Grau, Celino Miguel and Antonio M. Oller-Marcén*

Communicated by Rafał Abłamowicz

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 R-isomorphic generalized quaternion rings $\left(\frac{a,b}{\mathbb{Z}/n\mathbb{Z}}\right)$.

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 i = (i+1)i = k. The algebra defined by this product is isomorphic to the corresponding matrix ring.

^{*}Corresponding author.

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 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

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

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:

$$i^{2} = a,$$

$$j^{2} = b,$$

$$ij = -ji = k.$$

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 basis $\mathcal{B} = \{1, I, J, K\}$ of the free *R*-module H(R) such that

$$I^{2} = a,$$

$$J^{2} = b,$$

$$IJ = -JI = K.$$

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 $q_0 = x_1 i + x_2 j + x_3 k$ a pure quaternion. Then,

- (i) The conjugate of q is: $\overline{q} = x_0 q_0 = x_0 x_1 i x_2 j x_3 k$.
- (ii) The trace of q is $tr(q) = q + \overline{q} = 2x_0$.
- (iii) The norm of q is $n(q) = q\overline{q} = x_0^2 q_0^2 = x_0^2 ax_1^2 bx_2^2 + abx_3^2$.

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

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

In what follows, we assume that an homomorphism f between two quaternion algebras over a ring R is also a R-module homomorphism. Hence, f(1) = 1 and it fixes every element of the base ring R. For the sake of simplicity we will call them R-homomorphisms and an R-isomorphism is just a bijective R-homomorphism. Now, let $f: \left(\frac{a,b}{R}\right) \to \left(\frac{c,d}{R}\right)$ be a linear map and let us consider standard basis $\{1, i, j, k\}$ and $\{1, I, J, K\}$ of $\left(\frac{a, b}{R}\right)$ and $\left(\frac{c,d}{R}\right)$, respectively. It is clear that if f(1) = 1, $f(i^2) = a$, $f(j^2) = b$ and f(ij) = -f(ji) = f(k), then f induces a well-defined R-homomorphism between both quaternion rings. We will make extensive use of this fact in many subsequent results.

In the following result we will see that R-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 $f: \left(\frac{a,b}{R}\right) \to \left(\frac{c,d}{R}\right)$ be an *R*-isomorphism. Then, for every $q \in \left(\frac{a,b}{R}\right)$ it holds that $f(\overline{q}) = \overline{f(q)}$.

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, $\overline{q} = x_0 - q_0$ and $f(\overline{q}) = f(x_0) - f(q_0) = x_0 - f(q_0)$. On the other hand, $\overline{f(q)} = \overline{f(x_0 + q_0)} = \overline{f(x_0) + f(q_0)} = x_0 + \overline{f(q_0)} = x_0 + \overline{f(q_0)}$. 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 $a = f(a) = f(i^2) =$

 $f(i)^2 = (\alpha_1 + q_1)^2 = \alpha_1^2 + q_1^2 + 2\alpha_1 q_1 \in R$. Consequently, $2\alpha_1 q_1 \in R$ (because both α_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.

and the result follows.

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 $f:\left(\frac{a,b}{R}\right) \to \left(\frac{c,d}{R}\right)$ be a ring isomorphism. Then, for every $q \in \left(\frac{a,b}{R}\right)$ the following hold. (i) $\operatorname{tr}(f(q)) = \operatorname{tr}(q).$ (ii) n(f(q)) = 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 R-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 an R-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 subalgebra of $\left(\frac{a,c}{R}\right)$ generated by $\{1, f(i)\}$ which is a Cayley-Dickson algebra of dimension 2 [13]. To apply the Cayley-Dickson process to S and c we consider the vector space $C = S \oplus S$ with a new product defined by [13, p. 45]:

$$(s_1, s_2)(s_3, s_4) = (s_1s_3 + cs_4\overline{s}_2, \overline{s}_1s_4 + s_3s_2).$$

With this product, is is easily seen that C is R-isomorphic to $\left(\frac{a,c}{R}\right)$. Moreover, the set $\{(1,0), (f(i),0), (0,1), (0, f(i))\}$ is a standard basis of C. With this,

we have seen that we can extend the set $\{1, f(i)\}$ to a 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 $\alpha_2 a =$ and the result follows.

In what follows, we will be interested in determining whether two different quaternion rings are R-isomorphic or not. The following R-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,

$$\Bigl(\frac{a,b}{R}\Bigr)\cong\Bigl(\frac{b,a}{R}\Bigr).$$

Nevertheless, some other easy $R\mbox{-}\mathrm{isomorphisms}$ that hold in the case when a and b are units, like

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

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

3. Some Results Regarding $\left(rac{a,b}{\mathbb{Z}/p^k \mathbb{Z}} ight)$ for a Prime p

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

Lemma 2. Let s, k be such that $0 \le s \le k$ with $1 \le k$ and 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, the linear map f defined by f(1) = 1, f(I) = i, f(J) = k and f(K) = aj clearly induces a well-defined R-homomorphism; 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 $\mathbb{Z}/p^k\mathbb{Z}$.

Lemma 3. Let a_i $(1 \le i \le 4)$ and $k \ge 1$ 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 $0 < s \le k$. If $a_i \equiv a'_i \pmod{p^s}$ for every $1 \le i \le 4$, 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 R-isomorphism between $\begin{pmatrix} a_1, a_2 \\ \mathbb{Z}/p^k \mathbb{Z} \end{pmatrix}$ and $\begin{pmatrix} a_3, a_4 \\ \mathbb{Z}/p^k \mathbb{Z} \end{pmatrix}$. 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 $\begin{pmatrix} a'_1, a'_2 \\ \mathbb{Z}/p^s \mathbb{Z} \end{pmatrix}$ and $\begin{pmatrix} a'_3, a'_4 \\ \mathbb{Z}/p^s \mathbb{Z} \end{pmatrix}$ defined by the matrix A with respect to some standard bases, induces an R-isomorphism because $a_i \equiv a'_i \pmod{p^s}$ for every i.

It is also interesting, and often harder, to determine whether two quaternion rings are not *R*-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 $0 \le s \le r < k$. Then, the quaternion rings R_1 , R_2 and R_3 defined by

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

are pairwise non R-isomorphic.

Proof. For each $i \in \{1, 2, 3\}$ let us define the set $\mathbb{P}_i := \{q \in R_i : \operatorname{tr}(q) = 0\}$. Due to Corollary 1 i), these sets are preserved by *R*-isomorphisms so, in order to show that R_1 , R_2 and R_3 are pairwise non *R*-isomorphic, we will look for differences between the sets \mathbb{P}_i .

We begin by the odd p case. In this case the sets \mathbb{P}_i are precisely the sets of pure quaternions. First, we observe that for every element $q \in \mathbb{P}_3$ it holds that $q^2 = 0$, while \mathbb{P}_1 and \mathbb{P}_2 both clearly contain elements whose square is non-zero. This implies that R_3 is not R-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 R-isomorphic.

In the p = 2 case, the sets \mathbb{P}_i are no longer the sets of pure quaternions. Instead, we have that $\mathbb{P}_i = \{\alpha 2^{k-1} + q_0 : q_0 \text{ is a pure quaternion}\}$ but we can reason in the exact same way.

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

$$\left(\frac{ap^{s_1}, bp^{s_2}}{\mathbb{Z}/p^k\mathbb{Z}}\right) \ncong \left(\frac{cp^{s_3}, dp^{s_4}}{\mathbb{Z}/p^k\mathbb{Z}}\right)$$

Proof. Let us assume that both rings are *R*-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 $s_1 < s_3 \le s_2$, 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.

4. Quaternions over $\mathbb{Z}/p^k\mathbb{Z}$ for an Odd Prime p

This section is devoted to determine the number of different generalized quaternion rings over $\mathbb{Z}/p^k\mathbb{Z}$ for an odd prime p, up to R-isomorphism. 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 $r \ge 0$,

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

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 $f : R \to S$ whose matrix with respect to these bases is

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

clearly induces a well-defined *R*-homomorphism because $f(i^2) = f(i)^2 = (xI)^2 = x^2I^2 \equiv ts^{-1}sp^r \equiv tp^r \pmod{p^k}$, $f(j^2) = f(j)^2 = J^2 = m$, f(ij) = f(i)f(j) = xIJ = xK = f(k) and f(ji) = f(j)f(i) = J(xI) = xJI = xJI

-xK = -f(k). Moreover, since A is regular over $\mathbb{Z}/p^k\mathbb{Z}$, it is in fact an R-isomorphism and the result follows.

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

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

Proof. Let $x, y \in \mathbb{Z}/p^k\mathbb{Z}^*$ such that $x^2 + y^2 \equiv s^{-1} \pmod{p^k}$ (such x, y 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 a well-defined R-homomorphism because

$$\begin{split} f(i^2) &= f(i)^2 = (xI + yJ)^2 = (x^2 + y^2)sp^r \equiv p^r \pmod{p^k},\\ f(j^2) &= f(j)^2 = (-yI + xJ)^2 = (x^2 + y^2)sp^r \equiv p^r \pmod{p^k},\\ f(ij) &= f(i)f(j) = (xI + yJ)(-yI + xJ) \equiv (x^2 + y^2)K\\ &\equiv s^{-1}K = f(k) \pmod{p^k},\\ f(ji) &= f(j)f(i) = (-yI + xJ)(xI + yJ) \equiv -(x^2 + y^2)K\\ &\equiv -s^{-1}K = -f(k) \pmod{p^k}. \end{split}$$

Since, in addition, A is regular over $\mathbb{Z}/p^k\mathbb{Z}$ it is an R-isomorphism and the proof is complete.

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. Consider $x, y \in \mathbb{Z}/p^k\mathbb{Z}$ such that $x^2 - y^2 \equiv a^{-1} \pmod{p^k}$ (such x, y exist because it is enough to consider $x + y \equiv a^{-1}$ and $x - y \equiv 1$ and, since

p is odd, we can solve this system of equations). 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 a well-defined R-homomorphism because

$$\begin{split} f(i^2) &= f(i)^2 = I^2 = 1, \\ f(j^2) &= (xJ + yK)^2 = x^2J^2 + y^2K^2 = x^2ap^s - y^2ap^s = ap^s(x^2 - y^2) \\ &\equiv p^s \pmod{p^k}, \\ f(ij) &= f(i)f(j) = I(xJ + yK) = yJ + xK = f(k), \\ f(ji) &= f(j)f(i) = (xJ + yK)I = -(yJ + xK) = -f(k). \end{split}$$

The fact that it is an R-isomorphism follows because A is regular over $\mathbb{Z}/p^k\mathbb{Z}$.

The remaining R-isomorphisms 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 $q^2 \equiv u \pmod{p^k}$ if 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].

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

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

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

Proof. (i) Let us consider

 $N_i := \{q \in R_i : q \text{ is a pure quaternion}, n(q) = 0\}.$

Since *R*-isomorphisms preserve norms and pure quaternions, in order to prove that $R_1 \not\cong R_2$ we will see that $\operatorname{card}(N_1) \neq \operatorname{card}(N_2)$. 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 $x_1^2up^s + x_2^2p^s - x_3^2up^{2s} \equiv 0 \pmod{p^k}$. On the other hand, if $q_2 \in N_2$, it must be $q_2 = y_1I + y_2J + y_3K$ with $y_1^2p^s + y_2^2p^s - y_3^2p^{2s} \equiv 0 \pmod{p^k}$.

Now, let $(a_1, a_2, a_3) \in (\mathbb{Z}/p^{k-s}\mathbb{Z})^3$ be a solution of the congruence $x_1^2 u + x_2^2 - x_3^2 u p^s \equiv 0 \pmod{p^{k-s}}$ and let us define $b_i = a_i + l_i p^{k-s}$ with $0 \leq l_i < p^s$. Then, it is straightforward that $(b_1, b_2, b_3) \in (\mathbb{Z}/p^k\mathbb{Z})^3$ is a

solution of the congruence $x_1^2 u p^s + x_2^2 p^s - x_3^2 u p^{2s} \equiv 0 \pmod{p^k}$. This implies that $\operatorname{card}(N_1)/p^{3s}$ is the number of solutions of the congruence

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

while it can be seen in the same way that $\operatorname{card}(N_2)/p^{3s}$ is the number of solutions of the congruence

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

Now, reducing modulo p, we can see that:

- If -1 is a quadratic residue modulo 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 not a quadratic residue modulo 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 $\operatorname{card}(N_1) \neq \operatorname{card}(N_2)$ 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 $x^2p^s \equiv up^s \pmod{p^k}$ ha no solutions because u is a quadratic nonresidue modulo p.

Lemma 10. Let u be a quadratic nonresidue (mod 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 *R*-isomorphic.

Proof. Let us see that $R_1 \ncong R_2$, $R_1 \ncong R_4$, $R_2 \ncong R_3$ and $R_3 \ncong R_4$. If they were *R*-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 $R_1 \cong R_3$. 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 *R*-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 $\alpha_1 u p^s = 0$.

In particular, $up^r = j^2 = f(j^2) = f(j)^2 = (\alpha_1 I + \beta_1 J + \gamma_1 K)^2 = \alpha_1^2 up^s + \beta_1^2 p^r - \gamma_1^2 up^{r+s} = \beta_1^2 p^r - \gamma_1^2 u^2 p^{r+s}$. In other words, $\beta_1^2 p^r - \gamma_1^2 up^{r+s} \equiv up^r \pmod{p^k}$ 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 non-residue.

The remaining case, namely $R_2 \ncong R_4$ can be proved in the exact same way. \Box

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,

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

Proof. If a is a quadratic nonresidue:

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

Now, if a is a quadratic residue:

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

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.

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,

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

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:

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

Now, if ab is a quadratic residue:

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

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.

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,

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

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. \Box

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

Adv. Appl. Clifford Algebras

Theorem 3. Let p be an odd prime and let k be a positive integer. Then, there exist exactly $2k^2 + 2$ non R-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 *R*-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 $\begin{pmatrix} u, up^r \\ \overline{\mathbb{Z}/p^k\mathbb{Z}} \end{pmatrix} \cong \begin{pmatrix} u, p^r \\ \overline{\mathbb{Z}/p^k\mathbb{Z}} \end{pmatrix}, \begin{pmatrix} \underline{1}, up^r \\ \overline{\mathbb{Z}/p^k\mathbb{Z}} \end{pmatrix} \cong \begin{pmatrix} \underline{1, p^r} \\ \overline{\mathbb{Z}/p^k\mathbb{Z}} \end{pmatrix}$ and $\begin{pmatrix} u, p^r \\ \overline{\mathbb{Z}/p^k \mathbb{Z}} \end{pmatrix} \ncong \begin{pmatrix} 1, p^r \\ \overline{\mathbb{Z}/p^k \mathbb{Z}} \end{pmatrix}$. Hence, in this case we have 2 non *R*-isomorphic generalized quaternion rings for each $1 \le r \le k-1$. 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 *R*-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 $\left(\frac{up^r, up^r}{\mathbb{Z}/p^k\mathbb{Z}}\right) \cong$ $\begin{pmatrix} p^r, p^r \\ \overline{\mathbb{Z}/p^k \mathbb{Z}} \end{pmatrix} \ncong \begin{pmatrix} up^r, p^r \\ \overline{\mathbb{Z}/p^k \mathbb{Z}} \end{pmatrix} \cong \begin{pmatrix} p^r, up^r \\ \overline{\mathbb{Z}/p^k \mathbb{Z}} \end{pmatrix}$. Hence, in this case we have 2 non *R*-isomorphic generalized quaternion rings for each $1 \le r \le k-1$ for a total of 2(k-1).

- If 0 < s < r < k, Lemma 10 implies that the four rings are non Risomorphic. Hence, in this case we have 2 non R-isomorphic generalized quaternion rings for each $1 \le s \le k-2$ and each $s+1 \le r \le k-1$. 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 R-isomorphic due to Lemma 9. Thus, in this case we have 2 non *R*-isomorphic generalized quaternion rings for each $1 \le s \le k-1$. A total of 2(k-1).

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

 \square

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

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

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

Decomposition (4) induces a natural *R*-isomorphism

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

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 3.

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

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

References

- Conrad, K. Quaternion algebras. http://www.math.uconn.edu/~kconrad/ blurbs/ringtheory/quaternionalg.pdf (2016). Accessed 25 May 2017
- [2] Grau, J.M., Miguel, C.J., Oller-Marcén, A.M.: On the structure of quaternion rings over Z/nZ. Adv. Appl. Clifford Algebras 25(4), 875–887 (2015)
- [3] Gross, B.H., 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, 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, vol. 294. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer, Berlin (1991)
- [7] Miguel, C.J., 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, Berlin (2000)
- [9] Ozdemir, M.: The roots of a split quaternion. Appl. Math. Lett. 22(2), 258–263 (2009)

- [10] Özen, M., Güzeltepe, M.: Cyclic codes over some finite quaternion integer rings. J. Frankl. Inst. 348(7), 1312–1317 (2011)
- [11] Pierce, R.S.: Associative Algebras. Springer, New York (1982)
- [12] Rosen, K.H.: Elementary Number Theory and Its Applications. Addison-Wesley, Reading (2000)
- [13] Schafer, R.D.: An Introduction to Nonassociative Algebras. Dover Publications, New York (1995)
- [14] Shah, T., Rasool, S.S.: On codes over quaternion integers. Appl. Algebra Eng. Commun. 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: Alladi, K., Bhargava, M., Savitt, D., Tiep, P.H. (eds.) Quadratic and Higher Degree Forms, pp. 255–298. Springer, New York (2013)

José María Grau Departamento de Matemáticas Universidad de Oviedo Avda. Calvo Sotelo s/n 33007 Oviedo Spain e-mail: grau@uniovi.es

Celino Miguel Instituto de Telecomunicaçoes Universidade de Beira Interior Polo de Covilha Portugal e-mail: celino@ubi.pt

Antonio M. Oller-Marcén Centro Universitario de la Defensa de Zaragoza Ctra. Huesca s/n 50090 Saragossa Spain e-mail: oller@unizar.es

Received: May 31, 2017. Accepted: January 23, 2018.