Adv. Appl. Clifford Algebras 25 (2015), 875–887
© 2015 Springer Basel
0188-7009/040875-13
published online April 18, 2015
DOI 10.1007/s00006-015-0544-y

Advances in
Applied Clifford Algebras

On the Structure of Quaternion Rings Over $\mathbb{Z}/n\mathbb{Z}$

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

Abstract. In this paper we investigate the structure of $\left(\frac{a,b}{\mathbb{Z}/n\mathbb{Z}}\right)$, the quaternion rings over $\mathbb{Z}/n\mathbb{Z}$. It is proved that these rings are isomorphic to $\left(\frac{-1,-1}{\mathbb{Z}/n\mathbb{Z}}\right)$ if $a \equiv b \equiv -1 \pmod 4$ or to $\left(\frac{1,1}{\mathbb{Z}/n\mathbb{Z}}\right)$ otherwise. We also prove that the ring $\left(\frac{a,b}{\mathbb{Z}/n\mathbb{Z}}\right)$ is isomorphic to $\mathbb{M}_2(\mathbb{Z}/n\mathbb{Z})$ if and only if n is odd and that all quaternion algebras defined over $\mathbb{Z}/n\mathbb{Z}$ are isomorphic if and only if $n \not\equiv 0 \pmod 4$.

Mathematics Subject Classification. 11R52, 16-99.

Keywords. Quaternion ring, Modular integers, Structure.

1. Introduction

The origin of quaternions dates back to 1843, when Hamilton considered a four-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 "Hamilton quaternions" turned out to be the only associative division algebra over $\mathbb{R}$ with dimension >2. Later on, this idea was extended to define quaternion algebras over arbitrary fields. Thus, if F is a field and $a, b \in F\backslash\{0\}$ we can define a unital, associative, four-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 $\mathbb{M}_2(F)$ [9, 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.

*Corresponding author.

Celino Miguel was supported by FCT project UID/EEA/50008/2013

Birkhäuser

Generalizations of the notion of quaternion algebra to other commutative base rings R have been considered by Kanzaki [3], Hahn [2], Knus [4], Gross and Lucianovic [1], Tuganbaev [12], and most recently by Voight [13,14]. On the other hand, quaternions over finite rings have attracted significant attention since they have applications in coding theory see [7,8,11].

In particular, we will define quaternion rings over commutative, associative, unital rings. Some authors consider a different definition in the case that the element 2 is not invertible in the base ring R (for fields this corresponds to the case of characteristic 2). However, following Tuganbaev, we make no distinction between the case where 2 is invertible and the case where 2 is not invertible in the base ring. Our definition is as follows

Definition 1. 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,

$$H(R) = \{x_0 + x_1 i + x_2 j + x_3 k \colon x_0, x_1, x_2, x_3 \in R\}.$$

Now, let $a, b \in R$ be units 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 $\left(\frac{a,b}{R}\right)$.

Remark. If $a = b = -1$, the corresponding quaternion ring in called the ring of Hamilton quaternions over R and it is denoted by $\mathbb{H}(R)$.

Remark. Note that, over a field F of characteristic not 2, quaternions form a central simple algebra. This is no longer true if the field F has characteristic 2. This is one of the reasons that lead some authors to consider a different definition in the case of a field of characteristic 2.

Definition 2. Let $z = x_0 + x_1 i + x_2 j + x_3 k \in \left(\frac{a,b}{R}\right)$.

(i) The conjugate of z is $\bar{z} = x_0 - x_1 i - x_2 j - x_3 k$.
(ii) The norm of z is $\mathrm{n}(z) = z\bar{z} = x_0^2 - a x_1^2 - b x_2^2 + ab x_3^2$.
(iii) The trace of z is $\mathrm{tr}(z) = z + \bar{z} = 2x_0$.

Note that $\mathrm{n}(z), \mathrm{tr}(z) \in R$.

The correspondence between quaternion algebras over a field and quadratic forms is a classic result, see for instance [6]. Roughly speaking, quaternion algebras over a field F are the same as ternary quadratic forms over F. Recently, this correspondence was extended by Voight [13] to quaternion algebras over an arbitrary commutative and associative ring with identity. Therefore, the structure of quaternion rings can be deduced from the theory of quadratic forms. However, the proofs in this paper are elementary, in the sense that we use only the simplest properties of congruences (except the basic Taylor theorem in the proof of Lemma 1).

It is easy to see that the known characterization for quaternion rings over fields of characteristic different from two is no longer true in this general setting. For instance, consider the ring of Hamilton quaternions over $\mathbb{Z}$. Clearly, the corresponding quaternion ring $\mathbb{H}(\mathbb{Z})$ is not a division ring. On the other hand, we see that this ring is not isomorphic to the matrix ring $\mathbb{M}_2(\mathbb{Z})$. To see this, let us consider $z \in \mathbb{H}(\mathbb{Z})$ such that $z^2 = 0$. Then $n(z) = 0$ and it follows that $z = 0$. Since this property ($z^2 = 0 \to z = 0$) does not hold in $\mathbb{M}_2(\mathbb{Z})$, these two rings are not isomorphic, as claimed.

The question naturally arises as to whether a quaternion ring over an associative and commutative ring with identity R that is not a division ring is isomorphic to the matrix ring $\mathbb{M}_2(R)$. In this paper we consider the case $R = \mathbb{Z}/n\mathbb{Z}$. In particular we prove that, given $n \in \mathbb{N}$, there exist at most two quaternion rings over $\mathbb{Z}/n\mathbb{Z}$ up to isomorphism: $\mathbb{H}(\mathbb{Z}/n\mathbb{Z})$ and $\left(\frac{1,1}{\mathbb{Z}/n\mathbb{Z}}\right)$. Moreover, we will see that $\mathbb{H}(\mathbb{Z}/n\mathbb{Z}) \cong \left(\frac{1,1}{\mathbb{Z}/n\mathbb{Z}}\right) \cong \mathbb{M}_2(\mathbb{Z}/n\mathbb{Z})$ if and only if n is odd.

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

$$\mathbb{Z}_n \cong \mathbb{Z}/\mathbb{Z}p_1^{r_1} \oplus \cdots \oplus \mathbb{Z}/\mathbb{Z}p_k^{r_k}. \tag{1}$$

Decomposition (1) induces a natural isomorphism

$$\left(\frac{a,b}{\mathbb{Z}/n\mathbb{Z}}\right) \cong \left(\frac{a,b}{\mathbb{Z}/p_1^{r_1}\mathbb{Z}}\right) \oplus \cdots \oplus \left(\frac{a,b}{\mathbb{Z}/p_k^{r_k}\mathbb{Z}}\right). \tag{2}$$

Consequently, it suffices to study the case when n is a prime-power.

This fact strongly determines the structure of the paper. In Sect. 5 we focus on the case when n is a power of two, while Sect. 4 is devoted to the odd prime-power case. Before them, Sect. 2 presents some auxiliary results from elementary number theory that are useful in the sequel and in Sect. 3 we study Hamilton quaternions over $\mathbb{Z}/n\mathbb{Z}$ and $\left(\frac{1,1}{\mathbb{Z}/n\mathbb{Z}}\right)$ due to the main role that these particular cases will play in our classification.

2. Some Number-Theoretical Auxiliary Results

In this section we collect some results that will be useful in forthcoming sections. They are mainly related to finding solutions to quadratic polynomial congruences in two variables modulo a prime-power.

When we deal with polynomial congruences in one variable, Hensel's lemma plays a key role. The simplest form of Hensel's lemma [10, p. 170] states that, under certain regularity conditions, a solution of a polynomial with integer coefficients modulo a prime number p can be lifted to a solution modulo p^j for $j > 1$. The following lemma generalizes this result to polynomials in two variables.

Lemma 1. *Let $f(x_1, x_2)$ be a polynomial in two variables with integer coefficients. let p be a prime number, and let $A = (a_1, a_2) \in \mathbb{Z}^2$ be such that*

$$f(a_1, a_2) = 0 \quad mod\, p^j.$$

If at least one of the partial derivatives $\frac{\partial f}{\partial x_i}$ *is nonzero at* (a_1, a_2) *modulo* p, *then there exist integers* t_1, t_2 *such that*

$$f(a_1 + t_1 p^j, a_2 + t_2 p^j) = 0 \quad mod\, p^{j+1}.$$

Proof. Let n be the degree of the polynomial f. Using Taylor's theorem for functions of two independent variables we get

$$\begin{aligned} f(a_1 + t_1 p^j, a_2 + t_2 p^j) &= f(a_1, a_2) + t_1 p^j \frac{\partial f}{\partial x_1}(a_1, a_2) + t_2 p^j \frac{\partial f}{\partial x_2}(a_1, a_2) \\ &+ \frac{1}{2!}\left(t_1^2 p^{2j} \frac{\partial^2 f}{\partial x_1^2}(a_1, a_2) + 2t_1 t_2 p^{2j} \frac{\partial^2 f}{\partial x_2 x_1}(a_1, a_2) \right. \\ &\left. + t_2^2 p^{2j} \frac{\partial^2 f}{\partial x_2^2}(a_1, a_2)\right) + \cdots + \frac{1}{n!}\left(t_1^n p^{nj} \frac{\partial^n f}{\partial x_1^n}(a_1, a_2) \right. \\ &+ \binom{n}{1} t_1^{n-1} p^{(n-1)j} t_2 p^j \frac{\partial^n f}{\partial x_2 x_1^{n-1}}(a_1, a_2) \\ &\left. + \cdots\ t_2^n p^{nj} \frac{\partial^n f}{\partial x_2^n}(a_1, a_2)\right). \end{aligned}$$

It is easy to check that each derivative $\frac{\partial^s f}{\partial x_2^{s-r} x_1^r}$ is divisible by $r!(s-r)!$. That is, $\frac{\partial^s f}{\partial x_2^{s-r} x_1^r} = r!(s-r)!g(x, y)$ for some polynomial g. Therefore,

$$\binom{s}{r} \frac{\partial^s f}{\partial x_2^{s-r} x_1^r} = \binom{s}{r} r!(s-r)!g(x, y) = s!g(x, y).$$

It follows that modulo p^{j+1} the Taylor expansion reduces to

$$f(a_1 + t_1 p^j, a_2 + t_2 p^j) = f(a_1, a_2) + t_1 p^j \frac{\partial f}{\partial x_1}(a_1, a_2) + t_2 p^j \frac{\partial f}{\partial x_1}(a_1, a_2). \quad (3)$$

Finally, we observe that the assumption that at least one of the partial derivatives $\frac{\partial f}{\partial x_i}$ is nonzero at (a_1, a_2) modulo p imply that we can choose t_1 and t_2 satisfying $t_1 p^j \frac{\partial f}{\partial x_1}(a_1, a_2) + t_2 p^j \frac{\partial f}{\partial x_1}(a_1, a_2) = -f(a_1, a_2)$. This completes the proof. □

It is well-known that every element in a finite field can be expressed as a sum of two squares. The following result is a slight variation of this fact and the proof is almost identical. In particular, we use the fact that if A and B are subsets of a finite group G where $|A| + |B| > |G|$, then $G = AB$.

Lemma 2. *Let* p *be an odd prime and let* a, b *be integers such that* $\gcd(p, a) = \gcd(p, b) = 1$. *Then, the equation*

$$ax^2 + by^2 \equiv \alpha \pmod p$$

has solutions for every $\alpha \in \mathbb{Z}$.

Proof. Note that since p is prime it follows that $\mathbb{Z}_p$ is a field. Using the well-known fact that the multiplicative group of a finite field is cyclic it is easy to check that there are $\frac{p+1}{2}$ squares in $\mathbb{Z}_p$.

Now, denote by S the set (in fact it is a subgroup of the multiplicative group) of squares in $\mathbb{Z}_p$. Since $\gcd(p, a) = \gcd(p, b) = 1$, the elements a and

b are non-zero in the field $\mathbb{Z}_p$. Therefore, $|S| = |aS| = |bS| = \frac{p+1}{2}$. Hence, looking at the additive group of the field $\mathbb{Z}_p$ we find that $aS + bS = \mathbb{Z}_p$. This completes the proof. □

We can combine the previous results in the following proposition.

Proposition 1. *Let p be an odd prime number and let $a, b, c \in \mathbb{Z}$ be coprime to p. Then, the congruence*

$$ax^2 + by^2 \equiv c \pmod{p^s}$$

has a solution for every $s \geq 1$.

Proof. Lemma 2 determines that there exists (a_1, a_2) a solution to the congruences for $s = 1$. Moreover, since $p \nmid c$ either a_1 or a_2 is coprime to p. Hence, Lemma 1 applies. □

Unfortunately, when $p = 2$ we can never apply Lemma 2. Consequently we can no longer provide a unified approach. The following results deal with some congruences that we will need to solve (in fact we will just need to know that they have a solution) in the sequel.

Proposition 2. *Let $a, b \in \mathbb{Z}$ be odd integers with $a \equiv b \pmod 8$. Then the congruence*

$$ax^2 \equiv b \pmod{2^s}$$

has a solution for every $s \geq 1$.

Proof. If $1 \leq s \leq 2$ the result follows by direct inspection. Now, let us assume that $s \geq 3$. Since a is odd, let α be the inverse of a modulo 2^s. We have that $a\alpha \equiv 1 \pmod 8$ and hence $b\alpha \equiv 1 \pmod 8$. This means that $b\alpha = 8k + 1$ and congruence $ax^2 \equiv b \pmod{2^s}$ becomes $x^2 \equiv 8k+1 \pmod{2^s}$. The result follows because $8k + 1$ is a quadratic residue modulo 2^s if $s \geq 3$. □

Proposition 3. *The congruence*

$$5x^2 + 5y^2 \equiv 1 \pmod{2^s}$$

has a solution for every $s \geq 1$.

Proof. Given $s \geq 1$ let us denote by α_s the inverse of 5 modulo 2^s. The original congruence is equivalent to $x^2 + y^2 \equiv \alpha_s \pmod{2^s}$.

It can easily be seen that $\alpha_1 = \alpha_2 = 1$, $\alpha_3 = 5$ and that, for every $k \geq 1$:

$$\alpha_{4k} = \alpha_{4k+1} = \alpha_{4k+3} = \frac{2^{4k+2}+1}{5},$$
$$\alpha_{4k+3} = \alpha_{4k+2} + 2^{4k+2}.$$

Now, we claim that every prime divisor of $2^{4k+2} + 1$ is of the form $4h + 1$: let p be a prime divisor of $2^{4k+2} + 1$. Then $2^{4k+2} \equiv -1 \pmod p$ and the order of 2 in $\mathbb{Z}/p\mathbb{Z}$ must be $8k + 4$. This means that $8k + 4|p - 1$ and $p = (8k + 4)l + 1 = 4h + 1$ as claimed.

This implies that $\alpha_{4k}, \alpha_{4k+1}$ and α_{4k+2} are the sum of two squares so *a fortiori* the congruence $x^2 + y^2 \equiv \alpha_s \pmod{2^s}$ has a solution if $s = 4k, 4k + 1, 4k + 2$.

We know that there exist $A, B \in \mathbb{Z}$ such that $A^2 + B^2 = \alpha_{4k+2}$ and we can assume, without loss of generality, that A is odd. Let a be the inverse of A modulo 2^{4k+3}. Then:

$$\begin{aligned}(A + 2^{4k+1}a)^2 + B^2 &= A^2 + B^2 + 2^{8k+2}a^2 + 2^{4k+2}\\ &\equiv A^2 + B^2 + 2^{4k+2} = \alpha_{4k+2} + 2^{4k+2}\\ &= \alpha_{4k+3} \pmod{2^{4k+3}}.\end{aligned}$$

Consequently, the congruence $x^2 + y^2 \equiv \alpha_s \pmod{2^s}$ has a solution if $s = 4k+2$ and the result follows. □

3. Hamilton Quaternions Over $\mathbb{Z}_n$ and $\left(\frac{1,1}{\mathbb{Z}/n\mathbb{Z}}\right)$

It is well-known that the Hamiltonian quaternions over the real numbers form an $\mathbb{R}$-algebra isomorphic to a subalgebra of the matrix algebra $\mathbb{M}_2(\mathbb{C})$, where the isomorphism is given by:

$$\mathbb{H}(\mathbb{R}) := \left(\frac{-1,-1}{\mathbb{R}}\right) \cong \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} : z, \quad w \in \mathbb{C} \right\}.$$

In the same way, it is easy to observe that $\left(\frac{1,1}{\mathbb{R}}\right)$ is also isomorphic to a subalgebra of complex matrices. Namely:

$$\mathbb{L}(\mathbb{R}) := \left(\frac{1,1}{\mathbb{R}}\right) \cong \left\{ \begin{pmatrix} z & w \\ \overline{w} & \overline{z} \end{pmatrix} : z, \quad w \in \mathbb{C} \right\}.$$

These isomorphisms are also valid if we consider the quaternion rings over an arbitrary commutative, associative, unital ring. We just have to replace $\mathbb{C}$ by the quotient ring $R[i]/\langle i^2 + 1 \rangle$. In particular:

$$\mathbb{H}(R) := \left(\frac{-1,-1}{R}\right) \cong \left\{ \begin{pmatrix} \alpha - \beta i & -\gamma + \delta i \\ \gamma + \delta i & \alpha + \beta i \end{pmatrix} : \alpha, \beta, \gamma, \quad \delta \in R \right\},$$

$$\mathbb{L}(R) := \left(\frac{1,1}{R}\right) \cong \left\{ \begin{pmatrix} \alpha - \beta i & \gamma + \delta i \\ \gamma - \delta i & \alpha + \beta i \end{pmatrix} : \alpha, \beta, \gamma, \quad \delta \in R \right\}.$$

These isomorphisms turn out to be a very useful tool from the computational point of view when we deal with quaternions over $\mathbb{Z}/n\mathbb{Z}$. Now, we will have a close look at the rings $\mathbb{H}(\mathbb{Z}/n\mathbb{Z})$ and $\mathbb{L}(\mathbb{Z}/n\mathbb{Z})$. Recall that the natural isomorphism (2) allows us to focus on the prime-power case.

3.1. The Odd Prime Power Case

Hamilton quaternions over the field $\mathbb{Z}/p\mathbb{Z}$ have been studied in [5]. Indeed, in [5] an isomorphism between the Hamilton quaternions $\mathbb{H}(\mathbb{Z}/p\mathbb{Z})$ and the matrix ring $\mathbb{M}_2(\mathbb{Z}/p\mathbb{Z})$ for a given odd prime p is constructed. Here we generalize this result to Hamilton quaternions over $\mathbb{Z}/p^s\mathbb{Z}$ with p an odd prime and $s \geq 1$.

Proposition 4. *Let p be a odd prime number. Then,*

$$\mathbb{H}(\mathbb{Z}/p^s\mathbb{Z}) \cong \mathbb{L}(\mathbb{Z}/p^s\mathbb{Z}) \cong \mathbb{M}_2(\mathbb{Z}/p^s\mathbb{Z})$$

for every $s \geq 1$.

Proof. Due to Proposition 1 the congruence $x^2 + y^2 \equiv -1 \pmod{p^s}$ has a solution for every $s \geq 1$. Let $a, b \in \mathbb{Z}/p^s\mathbb{Z}$ such that $a^2 + b^2 = -1$ and define an algebra homomorphism $\phi\colon \mathbb{H}(\mathbb{Z}/p^s\mathbb{Z}) \longrightarrow \mathbb{M}_2(\mathbb{Z}/p^s\mathbb{Z})$ by:

$$\phi(i) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \phi(j) = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}.$$

The system of linear equations associated to

$$\phi(x_0 + x_1 i + x_2 j + x_3 k) = \begin{pmatrix} X & Y \\ Z & T \end{pmatrix}$$

always has a solution, namely:

$$\begin{aligned} x_0 &= (X + T)/2, \\ x_1 &= (Y - Z)/2, \\ x_2 &= (aT - aX - bY - bZ)/2, \\ x_3 &= (bT - bX + aY + aZ)/2. \end{aligned}$$

Hence, ϕ is an isomorphism.

The case $\mathbb{L}(\mathbb{Z}/p^s\mathbb{Z})$ is completely analogous considering $a, b \in \mathbb{Z}/p^s\mathbb{Z}$ such that $a^2 + b^2 = 1$. In this case the isomorphism is given by:

$$\phi(i) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \phi(j) = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}.$$

□

Corollary 1. *Let n be a odd integer. Then,*

$$\mathbb{H}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{L}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{M}_2(\mathbb{Z}/n\mathbb{Z}).$$

3.2. The Power of Two Case

It is clear that $\mathbb{H}(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{L}(\mathbb{Z}/2\mathbb{Z})$. Now we will see that if $s > 1$, then $\mathbb{H}(\mathbb{Z}/2^s\mathbb{Z}) \ncong \mathbb{L}(\mathbb{Z}/2^s\mathbb{Z})$. To do so we first focus on the case $s = 2$.

Lemma 3. $\mathbb{H}(\mathbb{Z}/4\mathbb{Z}) \ncong \mathbb{L}(\mathbb{Z}/4\mathbb{Z})$.

Proof. From Definition 2 (ii) we have that he norm in $\mathbb{H}(\mathbb{Z}/4\mathbb{Z})$ is given by $n_1(x_0 + x_1 i + x_2 j + x_3 k) = x_0^2 + x_1^2 + x_2^2 + x_3^2$, while the norm in $\mathbb{L}(\mathbb{Z}/4\mathbb{Z})$ is given by $n_2(x_0 + x_1 i + x_2 j + x_3 k) = x_0^2 + 3x_1^2 + 3x_2^2 + x_3^2$. Since the quadratic forms n_1 and n_2 have a different number of isotropic vectors, namely 32 for n_1 and 96 for n_2, the result follows. □

Proposition 5. *If $s > 1$ then $\mathbb{L}(\mathbb{Z}/2^s\mathbb{Z}) \ncong \mathbb{H}(\mathbb{Z}/2^s\mathbb{Z})$.*

Proof. Assume, on the contrary, that $\mathbb{H}(\mathbb{Z}/2^s\mathbb{Z}) \cong \mathbb{L}(\mathbb{Z}/2^s\mathbb{Z})$ with $s > 1$. This isomorphism naturally induces an isomorphism

$$\mathbb{H}(\mathbb{Z}/2^s\mathbb{Z})/4\mathbb{H}(\mathbb{Z}/2^s\mathbb{Z}) \cong \mathbb{L}(\mathbb{Z}/2^s\mathbb{Z})/4\mathbb{L}(\mathbb{Z}/2^s\mathbb{Z}).$$

Now, $4\mathbb{H}(\mathbb{Z}/2^s\mathbb{Z})$ and $4\mathbb{L}(\mathbb{Z}/2^s\mathbb{Z})$ are, respectively, the kernels of the surjective homomorphisms

$$\mathbb{H}(\mathbb{Z}/2^s\mathbb{Z}) \xrightarrow{\text{mod } 4} \mathbb{H}(\mathbb{Z}/4\mathbb{Z}),$$

$$\mathbb{L}(\mathbb{Z}/2^s\mathbb{Z}) \xrightarrow{\text{mod } 4} \mathbb{L}(\mathbb{Z}/4\mathbb{Z}).$$

Hence, it follows that $\mathbb{H}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{L}(\mathbb{Z}/4\mathbb{Z})$ contradicting Lemma 3. □

To end this section we will see that both $\mathbb{H}(\mathbb{Z}/2^s\mathbb{Z})$ and $\mathbb{L}(\mathbb{Z}/2^s\mathbb{Z})$ are local rings, so that they cannot be isomorphic to $\mathbb{M}_2(\mathbb{Z}/2^s\mathbb{Z})$. Recall that a unital ring R is local if and only if $1 \neq 0$ and for every $r \in R$ either r or $1-r$ is a unit.

Proposition 6. *If $s \geq 1$ then $\mathbb{H}(\mathbb{Z}/2^s\mathbb{Z})$ and $\mathbb{L}(\mathbb{Z}/2^s\mathbb{Z})$ are local rings.*

Proof. We will only focus on $\mathbb{H}(\mathbb{Z}/2^s\mathbb{Z})$, the other case being completely analogous. Obviously $1 \neq 0$, now assume that $z \in \mathbb{H}(\mathbb{Z}/2^s\mathbb{Z})$ is not a unit. This means that $\mathrm{n}(z)$ is not a unit in $\mathbb{Z}/2^s\mathbb{Z}$; i.e., that $\mathrm{n}(z)$ is even. Now, $\mathrm{n}(1-z) = (1-z)\overline{(1-z)} = (1-z)(1-\bar{z}) = 1 + \mathrm{n}(z) - \mathrm{tr}(z)$. Since $\mathrm{tr}(z)$ is even (recall Definition 2) it follows that $\mathrm{n}(1-z)$ is odd; i.e., it is a unit in $\mathbb{Z}/2^s\mathbb{Z}$ and, consequently $1-z$ is a unit. □

3.3. The General Case

We can summarize the previous work in the following theorem.

Theorem 1. *Let n be an integer. Then*:

(i) $\mathbb{H}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{L}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{M}_2(\mathbb{Z}/n\mathbb{Z})$, *if n is odd.*
(ii) $\mathbb{H}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{L}(\mathbb{Z}/n\mathbb{Z})$, *if $n \equiv 2 \pmod 4$.*
(iii) $\mathbb{H}(\mathbb{Z}/n\mathbb{Z}) \ncong \mathbb{L}(\mathbb{Z}/n\mathbb{Z})$, *if $n \equiv 0 \pmod 4$.*

Hence, $\mathbb{H}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $\mathbb{L}(\mathbb{Z}/n\mathbb{Z})$ if and only if $n \nmid 4$ and, in addition, they are isomorphic to $\mathbb{M}_2(\mathbb{Z}/n\mathbb{Z})$ only if n is odd. Note that (iii) does not imply the existence of three non-isomorphic quaternion rings over $\mathbb{Z}/n\mathbb{Z}$ if $4|n$, because if n is even $\mathbb{M}_2(\mathbb{Z}/n\mathbb{Z})$ cannot be seen as a quaternion ring. Theorem 5 below will establish the number of non-isomorphic quaterion rings over $\mathbb{Z}/n\mathbb{Z}$ for every n.

4. Quaternions Rings Over $\mathbb{Z}/n\mathbb{Z}$ with n Odd

It is well-known that every quaternion algebra over a finite field $\mathbb{F}_q$ of characteristic not two splits; i.e., it is isomorphic to the matrix ring of $\mathbb{M}_2(\mathbb{F}_q)$. This is a consequence of two classical theorems by Wedderburn: the structure theorem on finite dimensional simple algebras over a field and Wedderburn's little theorem. The following theorem generalizes this result to quaternion algebras over the ring of integers modulo an odd integer n. Again, the natural isomorphism (2) allows us to consider only the prime-power case.

Theorem 2. *Let p be an odd prime number and let $s \geq 1$. Then, all quaternion algebras defined over the ring of residual classes $\mathbb{Z}/p^s\mathbb{Z}$ are isomorphic. Moreover, all quaternion algebras defined over $\mathbb{Z}/p^s\mathbb{Z}$ split; i.e., they are isomorphic to the matrix ring $\mathbb{M}_2(\mathbb{Z}/p^s\mathbb{Z})$.*

Proof. Let a, b be units in $\mathbb{Z}/p^s\mathbb{Z}$. Due to Proposition 1 we can find $u, v \in \mathbb{Z}/p^s\mathbb{Z}$ such that $b \equiv u^2 - av^2 \pmod{p^s}$.

Now, let us consider the matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} u & -av \\ v & -u \end{pmatrix}.$$

Clearly we have that $A^2 = aI$, $B^2 = bI$ and $AB = -BA$.

Moreover, if $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/p^s\mathbb{Z}$ and we solve the linear system of equation associated to

$$x_0 I + x_1 A + x_2 B + x_3 AB = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

we get that the unique solution is given by:

$$\begin{aligned} x_0 &= \frac{\alpha + \delta}{2}, \\ x_1 &= \frac{\beta + a\gamma}{2a}, \\ x_2 &= \frac{\alpha\ u - \delta u + \beta v - a\gamma v}{2b}, \\ x_3 &= \frac{-\beta u + a\gamma u - a\alpha v + a\delta v}{-2ab}. \end{aligned}$$

Consequently, the set $\{I, A, B, AB\}$ is a basis of $\mathbb{M}_2(\mathbb{Z}/p^s\mathbb{Z})$ and the result follows. □

5. Quaternions Rings Over $\mathbb{Z}/n\mathbb{Z}$ with n a Power of Two

The first result of this section shows that, in order to study the structure of $\left(\frac{a,b}{\mathbb{Z}/2^s\mathbb{Z}}\right)$, we can restrict ourselves to the cases when $\{a, b\} \subset \{-1, 1, 3, 5\}$.

Lemma 4. *Let a, b, a', b' be odd integers such that $a \equiv a' \pmod 8$ and $b \equiv b' \pmod 8$. Then,*

$$\left(\frac{a,b}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \left(\frac{a',b'}{\mathbb{Z}/2^s\mathbb{Z}}\right)$$

Proof. Let α be a solution to the congruence $a'x^2 \equiv a \pmod{2^s}$ and let β be a solution to the congruence $b'y^2 \equiv b \pmod{2^s}$ (they exist due to Proposition 2). Denote by α^{-1} and β^{-1} their inverses modulo 2^s. Now, considering $i' = \alpha^{-1}i$ and $j' = \beta^{-1}j$ we have that $i'^2 = a'$, $j'^2 = b'$ and $i'j' = -j'i'$. Since the set $\{1, i', j', i'j'\}$ is obviously a basis of $\left(\frac{a',b'}{\mathbb{Z}/2^s\mathbb{Z}}\right)$, the result follows. □

Proposition 7. *Let a, b be odd integers. Then:*

(i) $\left(\frac{a,b}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \left(\frac{-1,b}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \left(\frac{-1,a}{\mathbb{Z}/2^s\mathbb{Z}}\right)$, *if* $ab \equiv 1 \pmod 8$.

(ii) $\left(\frac{a,b}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \left(\frac{1,b}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \left(\frac{1,a}{\mathbb{Z}/2^s\mathbb{Z}}\right)$, *if* $ab \equiv -1 \pmod 8$.

Proof. It is enough to apply the previous lemma together with the well-known fact that

$$\left(\frac{-ab,a}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \left(\frac{a,b}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \left(\frac{-ab,b}{\mathbb{Z}/2^s\mathbb{Z}}\right),$$

where the first isomorphism is induced by the permutation (i, k, j) and the second by the permutation (i, k). □

This result leads to the following isomorphisms.

Corollary 2.

$$\left(\frac{5,5}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \left(\frac{-1,5}{\mathbb{Z}/2^s\mathbb{Z}}\right),$$
$$\left(\frac{3,3}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \left(\frac{-1,3}{\mathbb{Z}/2^s\mathbb{Z}}\right),$$
$$\left(\frac{3,5}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \left(\frac{1,3}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \left(\frac{1,5}{\mathbb{Z}/2^s\mathbb{Z}}\right).$$

The following series of propositions describe more isomorphisms.

Proposition 8. *Let $b \in \{-1,1,3,5\}$. Then,*

$$\left(\frac{1,b}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \mathbb{L}(\mathbb{Z}/2^s\mathbb{Z}).$$

Proof. Given $b \in \{-1,1,3,5\}$, there exist integers η, θ such that $-\eta^2+\theta^2 = b$. Let us consider matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad B = \begin{pmatrix} \eta i & \theta \\ \theta & -\eta i \end{pmatrix}.$$

Clearly we have that $A^2 = I$, $B^2 = bI$ and $AB = -BA$.

Moreover, the linear system of equations associated to

$$\begin{pmatrix} \alpha - \beta i & \gamma + \delta i \\ \gamma - \delta i & \alpha + \beta i \end{pmatrix} = xI + yA + zB + tAB$$

has the following unique solution:

$$\begin{aligned} x &= \alpha, \\ y &= \delta, \\ z &= \frac{-\beta\,\eta - \gamma\,\theta}{\eta^2 - \theta^2}, \\ t &= \frac{\gamma\,\eta + \beta\,\theta}{\eta^2 - \theta^2}. \end{aligned}$$

Hence, the set $\{I, A, B, AB\}$ is a basis of $\mathbb{L}(\mathbb{Z}/2^s\mathbb{Z})$ and the result follows. □

Proposition 9.

$$\left(\frac{-1,5}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \mathbb{L}(\mathbb{Z}/2^s\mathbb{Z}).$$

Proof. Let $\{1,i,j,k\}$ and $\{1',i',j',k'\}$ be the canonical basis of $\left(\frac{-1,1}{\mathbb{Z}/2^s\mathbb{Z}}\right)$ and $\left(\frac{-1,5}{\mathbb{Z}/2^s\mathbb{Z}}\right)$, respectively. Given (η,θ) a solution to $5x^2+5y^2 \equiv 1 \pmod{2^s}$ (it exists due to Proposition 3), we can define a linear transformation $\phi\colon \left(\frac{-1,5}{\mathbb{Z}/2^s\mathbb{Z}}\right) \longrightarrow \left(\frac{-1,1}{\mathbb{Z}/2^s\mathbb{Z}}\right)$ by:

$$\phi(1') = 1, \quad \phi(i') = i, \quad \phi(j') = \eta j + \theta k, \quad \phi(k') = \eta k - \theta j.$$

It is easily seen that ϕ is in fact a well-defined algebra homomorphism, and since the set $\{1, i, \eta j + \theta k, \eta k - \theta j\}$ is linearly independent, the proof is complete. □

Proposition 10.

$$\left(\frac{-1,3}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \mathbb{H}(\mathbb{Z}/2^s\mathbb{Z}).$$

Proof. Note that, due to Lemma 4 $\left(\frac{-1,3}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \left(\frac{-1,-5}{\mathbb{Z}/2^s\mathbb{Z}}\right)$. Hence we can proceed in a similar way as in the previous proposition. □

All the previous results can be summarized in the following theorem.

Theorem 3.

$$\left(\frac{a,b}{\mathbb{Z}/2^s\mathbb{Z}}\right) \cong \begin{cases} \mathbb{H}(\mathbb{Z}/2^s\mathbb{Z}), & \textit{if } a \equiv b \equiv -1 \pmod 4; \\ \mathbb{L}(\mathbb{Z}/2^s\mathbb{Z}), & \textit{otherwise.} \end{cases}$$

6. Conclusions

In this short final section we present the main result of the paper, which collects all our previous work. It describes the structure of quaternion rings over $\mathbb{Z}/n\mathbb{Z}$.

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*

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

We can restate the result in the following terms.

Theorem 5.

$$\left(\frac{a,b}{\mathbb{Z}/n\mathbb{Z}}\right) \cong \begin{cases} \mathbb{H}(\mathbb{Z}/n\mathbb{Z}), & \textit{if } a \equiv b \equiv -1 \pmod 4; \\ \mathbb{L}(\mathbb{Z}/n\mathbb{Z}), & \textit{otherwise.} \end{cases}$$

In conclusion, quaternion rings over $\mathbb{Z}/n\mathbb{Z}$ split; i.e., are isomorphic to the matrix ring $\mathbb{M}_2(\mathbb{Z}/n\mathbb{Z})$ if and only if n is odd. If $n \equiv 2 \pmod 4$ there is only one quaternion ring over $\mathbb{Z}/n\mathbb{Z}$ up to isomorphism (which is not isomorphic to $\mathbb{M}_2(\mathbb{Z}/n\mathbb{Z})$) and, if $4|n$ there are exactly two classes of non-isomorphic quaternion rings over $\mathbb{Z}/n\mathbb{Z}$ [none of them isomorphic to $\mathbb{M}_2(\mathbb{Z}/n\mathbb{Z})$].

References

[1] Gross, B.H., Lucianovic, M.W.: On cubic rings and quaternion rings. J. Number Theory **129**(6), 1468–1478 (2009)

[2] Hahn, A.J.: Quadratic algebras, Clifford algebras, and arithmetic Witt groups. Universitext. Springer, New York, (1994)

[3] Kanzaki, T.: On non-commutative quadratic extensions of a commutative ring. Osaka J. Math **10**, 597–605 (1973)

[4] Knus, M.A.: Quadratic and Hermitian forms over rings, volume 294 of Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences). Springer, Berlin (With a foreword by I. Bertuccioni) (1991)

[5] Miguel, C.J., Serôdio, R.: On the structure of quaternion rings over $\mathbb{Z}_p$. Int. J. Algebra **5**(25-28), 1313–1325 (2011)

[6] O'Meara, T.O.: Introduction to quadratic forms. Classics in Mathematics. Springer, Berlin (Reprint of the 1973 edition) (2000)

[7] Özdemir, M.: The roots of a split quaternion. Appl. Math. Lett. **22**(2), 258–263 (2009)

[8] Özen, M., Güzeltepe, M.: Cyclic codes over some finite quaternion integer rings. J. Franklin Inst. **348**(7), 1312–1317 (2011)

[9] Pierce, R.S.: Associative algebras, volume 88 of Graduate Texts in Mathematics. Studies in the History of Modern Science, vol. 9. Springer, New York (1982)

[10] Rosen, K.H.: Elementary number theory and its applications, 4th edn. Addison-Wesley, Reading (2000)

[11] Shah, T., Rasool, S.S.: On codes over quaternion integers. Appl. Algebra Eng. Commin. Comput. **24**(6), 477–496 (2013)

[12] Tuganbaev, A.A.: Quaternion algebras over commutative rings. (Russian). Mat. Zametki. **53**(2), 126–131 (1993). Translation in Math. Notes **53**(1–2), 204–207 (1993)

[13] Voight, J.: Characterizing quaternion rings over an arbitrary base. J. Reine Angew. Math. **657**, 113–134 (2011)

[14] 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, volume 31 of Developments in Mathematics, 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
Department of Mathematics
Instituto de Telecomunicações
Beira Interior University
Covilhã
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: September 23, 2014.
Accepted: March 21, 2015.