Quaternion Orders and Diophantine Equations

Adriana Cardoso `adriana.cardoso@fc.up.pt`

Joint Work with António Leite, António Machiavelo, Rafael Moreira and Luís Roçadas

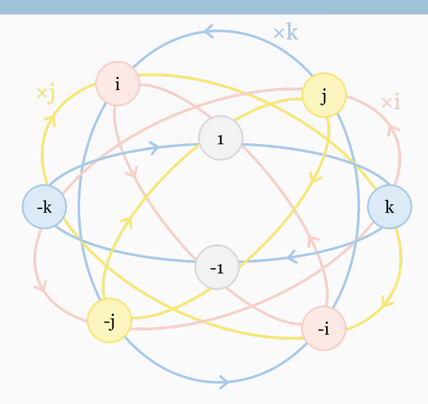
Centro de Matemática da Universidade do Porto, Departamento de Matemática,
Faculdade de Ciências da Universidade do Porto, rua do Campo Alegre s/n, 4169–007 Porto, Portugal

Introduction

One important problem in Number Theory is the study of **Diophantine equations**: algebraic equations with integer coefficients in two or more unknowns, whose integers solutions are of interest. In this work, our focus lies on equations of the form $t^2 - ax^2 - by^2 + abz^2$, since those can be viewed as the norm of an arbitrary integral quaternion, which allows us to use **quaternion orders** to study them. The most famous example of this is Hurwitz's [3] proof of the Four Squares Theorem using a quaternion order inside the 4-dimensional associative division algebra over the rational numbers,

$$\mathbb{H}(\mathbb{Q}) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k, \text{ where } i^2 = -1 = j^2 \text{ and } ij = k = -ji.$$

Other examples of the use of quaternions in the study of Diophantine Equations include the work of Deutsch [1] and Fitzgerald [2].



Quaternion Algebras

Let $\mathbb{F}$ be a field whose characteristic is not 2 and a and b be non-zero elements in $\mathbb{F}$. We say that $\mathbb{A} := \left(\frac{a,b}{\mathbb{F}}\right)$ is a **quaternion algebra over** $\mathbb{F}$ if it is a central simple 4-dimensional algebra over $\mathbb{F}$ with basis $1, i, j, k$ such that

$$i^2 = a, \quad j^2 = b, \quad ij = k = -ji.$$

The **conjugate** of $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathbb{A}$ is

$$\overline{x} := x_0 - x_1 i - x_2 j - x_3 k.$$

The map $\mathrm{N}\colon \mathbb{A} \to \mathbb{F}$ denotes the **norm** map given by

$$\mathrm{N}(x) = x\overline{x} = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2,$$

and the map $\mathrm{Tr}\colon \mathbb{A} \to \mathbb{F}$ denotes the **trace** map given by

$$\mathrm{Tr}(x) = x + \overline{x} = 2x_0.$$

$\times$	1	i	j	k
1	1	i	j	k
i	i	a	k	aj
j	j	$-k$	b	$-bi$
k	k	$-aj$	bi	$-ab$

Quaternion Orders

Definition. *Let $\mathbb{A}$ be a quaternion algebra over $\mathbb{Q}$. A **(quaternion) order** H of $\mathbb{A}$ is a finitely generated $\mathbb{Z}$-module contained in the algebra, such that H is also a subring of $\mathbb{A}$ and $\mathbb{Q} \otimes H \cong \mathbb{A}$.*

Proposition. *For any order H, we have that $\mathbb{Q} \cap H = \mathbb{Z}$. Moreover the norm and the trace of any element of H is in $\mathbb{Z}$.*

Examples of Quaternion Orders

- In the quaternion algebra $\mathbb{H}(\mathbb{Q}) = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, we have:
  - the ring of **Lipschitz Integers**, denoted by $\mathcal{L}$ and defined as
    $$\mathcal{L} := \mathbb{Z}[1, i, j, k] = \{a + bi + cj + dk \in \mathbb{H}(\mathbb{Q})\colon a, b, c, d \in \mathbb{Z}\}.$$
    $\mathcal{L}$ is an order, but it neither Euclidean for the norm nor a Principal Ideal Domain (PID);
  - the ring of **Hurwitz Integers**, denoted by $\mathcal{H}$. It is characterized by
    $$\mathcal{H} = \mathcal{L} \cup (\mathcal{L} + \omega) = \mathbb{Z}[1, i, j, \omega],$$
    where $\omega = \frac{1+i+j+k}{2}$. It is a maximal order in the above algebra, Euclidean for the norm, and thus a PID.
- In the quaternion algebra $\left(\frac{-2,-5}{\mathbb{Q}}\right)$, we have the orders
  $$\mathcal{L}_{2,5} := \mathbb{Z}[1, i, j, k] \subset \mathcal{H}_{2,5} := \mathbb{Z}\left[1, \frac{2+i-k}{4}, \frac{2+3i+k}{4}, \frac{1+i+j}{2}\right],$$
  where $\mathcal{H}_{2,5}$ is a maximal order and Euclidean for the norm, thus a PID.
- In the quaternion algebra $\left(\frac{-1,-7}{\mathbb{Q}}\right)$, we have the orders
  $$\mathcal{L}_{1,7} := \mathbb{Z}[1, i, j, k] \subset \mathcal{H}_{1,7} := \mathbb{Z}\left[1, i, \frac{1}{2}(1+j), \frac{1}{2}(i+k)\right],$$
  where $\mathcal{H}_{1,7}$ is a maximal order. Although it is not Euclidean for the norm, it is a PID.

Four Squares Theorem

Theorem. *Four Squares Theorem (1770) Any $m \in \mathbb{N}$ can be written as the sum of four integer squares.*

This theorem is equivalent to showing that exits a Lipschitz Integer of norm m, for all $m \in \mathbb{N}$, that is,

$$\gamma = t + xi + yj + zk \in \mathcal{L} \text{ such that } \mathrm{N}(\gamma) = m.$$

The next lemma entails that it is enough to show that there exists an Hurwitz Integer of norm m instead.

Lemma. *If $\gamma \in \mathcal{H} \setminus \mathcal{L}$, then there exists a unit $u \in \mathcal{H}$ such that $u\gamma, \gamma u \in \mathcal{L}$.*

Finally, the existence of an element of norm m in $\mathcal{H}$ is guaranteed by the fact that $\mathcal{H}$ is a PID, since we have the following result.

Theorem 1. *(C., Leite, Machiavelo, Roçadas, Moreira) If H is a PID order in $\mathbb{A}$, then its norm form is universal.*

Metaconjugation

Consider the quadratic form $t^2 - ax^2 - by^2 + abz^2$ and let $\mathbb{A} := \left(\frac{a,b}{\mathbb{Q}}\right)$ be the rational quaternion algebra associated to it.

The problem of determining all the natural numbers n that are represented in $\mathbb{Z}$ by the above form is equivalent to finding all natural numbers n such that there exists an element α in the order of integral quaternions $\mathcal{L}_{a,b} := \mathbb{Z}[1, i, j, k]$ such that $\mathrm{N}(\alpha) = n$.

Our arguments are built upon a process that we call **metaconjugation**, which transforms elements from a PID order into elements of the same norm in $\mathcal{L}_{a,b}$. It works as follows: let $\mathcal{H}_{a,b}$ be a PID order that contains $\mathcal{L}_{a,b}$ and $\gamma \in \mathcal{H}_{a,b}$. If $\sigma, \tau \in \mathcal{H}_{a,b}$ are of equal norm, then $\sigma\gamma\tau^{-1}$ has norm equal to that of γ. Hence, in order to prove that $n \in \mathbb{N}$ is represented by the norm form of $\mathcal{L}_{a,b} = \mathbb{Z}[1, i, j, k]$, it is enough to find $\sigma, \tau \in \mathcal{H}_{a,b}$ such that

$$\sigma\gamma\tau^{-1} \in \mathcal{L}_{a,b},$$

for $\gamma \in \mathcal{H}_{a,b}$ of norm n.

Form $t^2 + 2x^2 + 5y^2 + 10z^2$

Consider the form $t^2 + 2x^2 + 5y^2 + 10z^2$ and its associated order $\mathcal{L}_{2,5} = \mathbb{Z}[1, i, j, k]$ in the quaternion algebra $\left(\frac{-2,-5}{\mathbb{Q}}\right)$, whose canonical basis satisfy $i^2 = -2, j^2 = -5$. Using PARI/GP [4], we proved the following proposition.

Proposition. *Let $\gamma \in \mathcal{H}_{2,5}$. Then there exist $\sigma, \tau \in \mathcal{H}_{2,5}$ of **norm 4**, such that*

$$\sigma\gamma\tau^{-1} \in \mathcal{L}_{2,5}.$$

The above Proposition and Theorem 1 yield the first Main Theorem of this work.

Main Theorem 1. *(C., Leite, Machiavelo, Roçadas, Moreira) The form $t^2 + 2x^2 + 5y^2 + 10z^2$ is universal.*

Form $t^2 + x^2 + 7y^2 + 7z^2$

Consider the form $t^2 + x^2 + 7y^2 + 7z^2$ and its associated order $\mathcal{L}_{1,7} = \mathbb{Z}[1, i, j, k]$, which is an order in the quaternion algebra $\left(\frac{-1,-7}{\mathbb{Q}}\right)$, whose canonical basis satisfy $i^2 = -1, j^2 = -7$. It is easy to see that if $n = 2^\varepsilon \cdot 3 \cdot 7^k$, for some $\varepsilon \in \{0, 1\}$ and $k \in \mathbb{N}_0$, then the above form does not represent n. Using the multiplicative property of the norm, we get the following result.

Theorem 2. *If $t^2 + x^2 + 7y^2 + 7z^2$ **represents all primes different from 3** and **represents** $3p$, **for all odd prime** p **different from 7**, then it represents all n not of the form $n = 2^\varepsilon \cdot 3 \cdot 7^k$, for $\varepsilon \in \{0, 1\}$ and $k \in \mathbb{N}_0$.*

Using PARI/GP [4], we prove the first part of Theorem 2.

Proposition. *If $\gamma \in \mathcal{H}_{1,7} \setminus \mathcal{L}_{1,7}$ is s.t. $\mathrm{N}(\gamma) = p$ for a prime p greater than 3, then there exist $\sigma, \tau \in \mathcal{H}_{1,7}$ of **norm 6** such that*

$$\sigma\gamma\tau^{-1} \in \mathcal{L}_{1,7}.$$

*In particular, **if** p **is a prime different from 3, then** p **is represented** by $t^2 + x^2 + 7y^2 + 7z^2$.*

For the second part of Theorem 2, we show that the form represents $3p$ for an odd prime p if and only if there exists $\gamma \in \mathcal{H}_{1,7} \setminus \mathcal{L}_{1,7}$ such that $\mathrm{N}(\gamma) = p$. We prove this equivalent condition, using the usual conjugation.

Proposition. *For any $\gamma \in \mathcal{L}_{1,7}$ of prime norm p different from 2 and 7, there exists $k \in \mathbb{N}$ such that we have either*

$$\omega^k \gamma \omega^{-k} \text{ or } \bar{\omega}^k \gamma \bar{\omega}^{-k} \in \mathcal{H}_{1,7} \setminus \mathcal{L}_{1,7}.$$

*In other words, there exists $\gamma \in \mathcal{H}_{1,7} \setminus \mathcal{L}_{1,7}$ such that $\mathrm{N}(\gamma) = p$, for **all odd prime** p **different from** 7.*

Corollary. *If p is an odd prime different from 7, then $3p$ is represented by $t^2 + x^2 + 7y^2 + 7z^2$.*

From the above results and Theorem 2 follows the second Main Theorem of this work.

Main Theorem 2. *(C., Leite, Machiavelo, Roçadas, Moreira) The form $t^2 + x^2 + 7y^2 + 7z^2$ represents $n \in \mathbb{N}$ if and only if n is not of the form $n = 2^\varepsilon \cdot 3 \cdot 7^k$, for $\varepsilon \in \{0, 1\}$ and $k \in \mathbb{N}_0$.*

References

[1] J. I. Deutsch. "A quaternionic proof of the universality of some quadratic forms". In: *Integers* 8.2 (2008).

[2] R. W. Fitzgerald. "Norm Euclidean Quaternion Orders". In: *Integers* 11 (2011).

[3] A. Hurwitz. *Vorlesungen Über die Zahlentheorie der Quaternionen*. Springer Berlin Heidelberg, 1919.

[4] The PARI Group. *PARI/GP version* `2.17.0`. Available `http://pari.math.u-bordeaux.fr/`. Univ. Bordeaux, 2023.

PORTUGAL 2030 · UNIÃO EUROPEIA Fundo Social Europeu

The author was supported by the FCT doctoral scholarship with references 2022.13732.BD, DOI `https://doi.org/10.54499/2022.13732.BD`, and partially supported by CMUP, member of LASI, which is financed by national funds through FCT – Fundação para a Ciência e a Tecnologia, I.P., under the project with reference UID/00144/2025 and associated DOI given by `https://doi.org/10.54499/UID/00144/2025`.

fct Fundação para a Ciência e a Tecnologia