Aix*Marseille
université
Socialement engagée

Math
Institut
Camille
Jordan

Representation of a prime by a quadratic form

Emmy CHABERT

L3 MPCI December 2025

Institut Camille Jordan, supervised by Jérôme Germoni

Contents

1 Introduction

The interest in decomposing an integer p prime as a sum of squares dates back to Antiquity. Easy at first glance, this theorem is based on algebraic structures which will bring us to study the ring $\mathbb{Z}[i]$ and its properties to explain the decomposition as a sum of two squares. This question will lead us to be convinced that the Euclidean division exists in certain rings just like the gcd. This problem illustrates that highly abstract algebraic concepts can be employed to solve and practically implement very concrete problems.

Two closely related problems are resolved in detail, namely the decomposition of the prime p into the form $a^2 + 2b^2$ and $a^2 - ab + b^2$ but we went further by studying equations of the form $a^2 + db^2$ in terms of the roots of the polynomial $X^2 - d$. In fact, the fundamental idea to represent a prime number by the quadratic forms considered consists of studying the possible factorization of this prime number in a quadratic extension $\mathbb{Z}$: $\mathbb{Z}[i]$ for the two squares, $\mathbb{Z}[\sqrt{-2}]$ for the equation $a^2 + 2b^2$. And finally, $\mathbb{Z}[\omega]$ where ω is a cubic root of the unit distinct from 1 for $a^2 - ab + b^2$. In each case, the quotient $A/(p)$ is identified to $\mathbb{F}_p[X]/(f)$ where f is a unit polynomial of degree 2 such as $(X^2 + 1, X^2 + 2, X^2 + X + 1)$. The number p can be factored in the extension if and only if f admits a root in $\mathbb{F}_p$. The key point that allows us to go to the end of the question is the hypothesis that A is Euclidean.

In each section an algorithm will be propose and detailed. For the implementation, we need two essential ingredients:
— an algorithm for calculating square roots modulo p; we chose the Cipolla algorithm. because it is explained very clearly from the structure of the fields of cardinal p^2 (and that it is effective with a prime number of several hundred digits);
— a GCD algorithm in a Euclidean ring. In fact, the Euclide algorithm is a succession of a Euclidean division algorithm. To be more precise, we find thanks to the algorithm of Cipolla an element w in A which is not in $\mathbb{Z}$ whose norm is a multiple of p. The gcd of p and w is then automatically one of the two irreducible factors of p in A ;
we thus see how the abstract algebraic structure of a Euclidean ring is exploited to prove the existence, then calculate a representation of a prime number as the norm of a element of said ring.
One can see a great success in the theory (if it is easy to find head that $13 = 3^2 + 2^2$, one cannot find through blind tests that

$$360027784083079948259017962255826129 = a^2 + b^2 \quad \text{where} \begin{cases} a = 42037360450663977 \\ b = 49298907507065764 0. \end{cases} \tag{1}$$

By contrast, most quadratic forms, even those of the form $a^2 + nb^2$, are not norms of a Euclidean ring, which indicate the limitations of the proposed methods. However, for non-Euclidean cases, the situation is really more complex, as evidenced by the 550 pages of David A. Cox's book : *Primes of the form $x^2 + ny^2$* : it appeals to class field theory and largely exceeds the framework of a four-week internship and even that of the third year of a bachelor's degree.

2 Acknowledgments

I would like to express my sincere gratitude to all those who contributed, directly or indirectly, to my internship. First and foremost, I would like to thank Jérôme Germoni my internship supervisor, associated professor at University of Lyon 1, for his guidance and valuable advice throughout this experience. I would like to quote too Jean-Baptiste Aubin, associate professor at INSA Lyon, thanks to whom I found accommodation for the duration of the internship. But also Philippe Caldero, Associate Professor at University of Lyon 1, with whom I was able to discuss my results. I would also like to thank my academics supervisors, Guillaume Maire and Frederic Palesi, Faculty member, for their support and for following my progress during the internship. Finally, I thank the referee for reading this report.

3 Presentation of department

The internship took place at the Institut Camille Jordan, a major research centre in France. It brings together researchers, professors, and PhD students divided into research teams working in many areas of mathematics :
– algebra, geometry, logic;
– combinatorics and Number Theory;
– partial differential equations and analysis (PDEA);
– history of Mathematics;
– mathematical modeling and scientific computing (MMSC);
– probability, statistics, and mathematical physics.
érôme Germoni belongs to the algebra team, that gathers about 75 persons. 1 The Camille Jordan Institute (ICJ) is attached to the Lyon 1 university, but also to the Jean Monnet university in Saint-Étienne, to the INSA de Lyon and to the École centrale de Lyon, as well as the Centre national de la recherche scientifique. Most of the 190 faculty members share their time between teaching duties and research, while 30 of them are CNRS researchers. There are more than 90 PhD students, and nearly 20 postdocs. Many members of ICJ are involved in activities aimed at promoting mathematics to the general public. Examples include the monthly mathematics evening, which offers college students a meeting with a researcher around a current research topic, the Lyon Mathematical Rally for middle and high school pupils, as well as the 'Girls, Math, and Computer Science' Days for high school girls interested in science

4 Fermat's two square theorem

The aim of the report is to study some quadratic forms and apply them to study algebraic structures around a few quadratic forms and apply them to find a way to represent a prime number p by these forms. What is fascinating about this subject is how highly abstract algebraic concepts can allow us to understand and implement very concrete problems. In this report, A is a commutative unitary ring, except in the last part (quaternions ring). In general, I and J will denote ideals of A. We denote the field of cardinal p, by $\mathbb{F}_p^*$ the group of invertible elements (a cyclic group of order $p-1$), and by $\mathbb{F}_p^{*2}$ the subgroup of invertible squares. We assume familiarity with the notions of principal, prime, irreducible, prime and irreducible ideals, as well as the usual basic properties of these structures.

Fermat stated the following result without proof, as he did with many of his theorems, which sparked the interest of several generations of mathematicians still today. It was finally Leonhard Euler who provided the first complete proof in the 18^{th} century, developing new methods in number theory. The theorem later played an important role in the study of Gaussian integers and contributed to the rise of algebraic number theory.

Theorem 4.0.1 (Fermat's theorem on sums of two squares). *Let p be an odd prime number. Then, there exist integers a and b be such that.*

$$p = a^2 + b^2 \iff p \equiv 1 \pmod 4.$$

Example 4.0.2. The first prime numbers of the form $1+4k$ are squares.

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2, \quad 29 = 2^2 + 5^2, \quad 37 = 1^2 + 6^2. \tag{2}$$

We also introduce the ring of Gaussian integers :

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \tag{3}$$

The aim is to understand the algebraic notions behind the equation and to prove the theorem 4.0.1, so that we can implement it later in SageMath software. Indeed, finding a solution for $p = 5$ is easy, but what about a 100-digits number? How long will it take?

4.1 Theory

Structures

Definition 4.1.1 (Euclidean domain). A Euclidean domain is a commutative ring equipped with a Euclidean function

$$\phi : A \setminus \{0\} \longrightarrow \mathbb{N}.$$

that satisfies the following Euclidean division property : for all $a, b \in A$ with $b \neq 0$, there exist $q, r \in A$ such that $a = bq + r$ and $[r = 0$ or $\phi(r) < \phi(b)]$. We call q the quotient and r the remainder.

Definition 4.1.2 (factorial ring). A factorial ring is an domain in which for every element $A \backslash \{0\}$, there exist an integer $n \geq 0$, irreducible elements $p_1, \cdots, p_n$, and $a \in A^\times$ such that $a = p_1 \dots p_n$ and such a decomposition is unique up to a permutation of factors and replacing an irreducible element by a product by some unit.

These notions are closely related: every Euclidean domain is principal, and every principal ideal domain is a unique factorization domain. For this reason, we treat them together.

Definition 4.1.3. A a ring and I be an ideal, there exist elements $p_1, \dots, p_n \in A$ such that every element of I can be written as $a_1p_1 + \cdots + a_np_n, \quad$ with $a_i \in A$.

Lemma 4.1.4. Any principal domain is Noetherian.

Proof. Let A be a principal ring, i.e., a commutative ring in which every ideal is generated by a single element. Let $I \subseteq A$ be an arbitrary ideal. By the definition of a principal ring, there exists an element $x \in A$ such that $I = (x) = \{ax \mid a \in A\}$. This shows that I is generated by one element, which is finite. Thus, every ideal of A is finitely generated. Therefore, by definition, A is Noetherian. □

Proposition 4.1.5. Any Euclidean domain is principal.

Proof. Let I be an ideal of A an Euclidean domain, if $I = \{\emptyset\}$, $I = (0)$. Otherwise, let $a \in I$ as $\phi(a)$ be minimal. Let $b \in I$, we apply the Euclidean division of a by b. It exists $q, r \in A$ such that $a = bq + r$ with $\phi(r) < \phi(a)$. It follows that $r \in I$ because $a, b \in I$. However, if $\phi(r) \neq 0$, $\phi(a)$ bearer is not minimal, then $r = 0$ and $b = aq$. Hence, $b \in (a)$ and so $I = (a)$, A are principal. □

Proposition 4.1.6. Any principal ring is factorial.

Proof. Set A as a principal ideal ring and I be an ideal of A such that $I = (a)$. If a is irreducible, then it is over. If not, it exists $b, c \in A$ such that $a = bc$. Thus, determined if b, c are not irreducible, we continue the development until we arrive at an irreducible element product because the ring is Noetherian. □

Quadratic residues

Quadratic residues reveal interesting patterns in the behaviour of numbers when they are squared modulo a prime. Surprisingly, they help to understand the criteria under which numbers can be expressed as a sum of squares. The Legendre symbol provides a useful way to track these patterns and uncover deeper relationships between numbers.

Definition 4.1.7. Let p be a prime and a be an integer. We say that a is a quadratic residue mod p if there exist $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod{p}$. We define the Legendre symbol;

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a non-zero quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is not a quadratic residue modulo } p. \end{cases}$$

Many properties follow from this definition and will be very useful for our proof and for implementation.

Proposition 4.1.8. Let a, b be integers, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof. First of all, notice that if $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$, then $ab \equiv 0 \pmod{p}$. In this case, the Legendre symbol immediately satisfies: $\left(\frac{ab}{p}\right) = 0 = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. We can therefore restrict ourselves to the case where a, b are invertible modulo p, that is, $a, b \in \mathbb{F}_p^*$.
The set of squares is the image of the morphism $c : \mathbb{F}_p^* \to \mathbb{F}_p^*, \quad x \mapsto x^2$, the kernel of

which is $\{-1,1\}$ (the polynomial equation $x^2 = 1$ has two solutions in the field $\mathbb{F}_p$). Thus, we have $[\mathbb{F}_p^* : \mathbb{F}_p^{*2}] = 2$. It follows that $\mathbb{F}_p^*/\mathbb{F}_p^{*2} \simeq \{-1,1\}$. For $a, x \in \mathbb{F}_p^*$, notice that a is a square if and only if ax^2 is a square. Hence, one can identify $\left(\frac{a}{p}\right)$ with the coset of a modulo $\mathbb{F}_p^{*2}$. The multiplicativity of the Legendre symbol follows from that of the canonical projection $\mathbb{F}_p^* \to \mathbb{F}_p^*/\mathbb{F}_p^{*2}$. □

Lemma 4.1.9 (Euler's criterion)**.** An element x in $\mathbb{F}_p^\times$ is a square if and only if $x^{\frac{p-1}{2}} = 1$. In other terms, the kernel of the morphism ;

$$\chi : \mathbb{F}_p^* \to \{-1,1\}, \quad a \mapsto a^{\frac{p-1}{2}}.$$

is the set of squares in $\mathbb{F}_p^*$.

Proof. First, we check that χ is well-defined. Indeed, for $a \in \mathbb{F}_p^\times$, we have $\chi(a)^2 = a^{p-1} = 1$ according to Fermat's little theorem. Then $\chi(a) \in \{-1,1\}$. It is clear that χ is a morphism. Its kernel has an order at most $(p-1)/2$ since its elements are the roots of the polynomial $a^{(p-1)/2} - 1$. In particular, its image is not reduced to $\{1\}$, so it is $\{-1,1\}$, and the order of $\ker\chi$ is $|\mathbb{F}_p^\times|/|\operatorname{Im}(\chi)\| = \frac{p-1}{2}$.
We know from 4.1.8 that there are $\frac{p-1}{2}$ squares in $\mathbb{F}_p^*$, so that the kernel of χ is exactly the subgroup of squares, which proves the lemma. □

We will end with an essential proof for our demonstration. The second part of the proposition is trivial; instead we will focus on the first.

Proposition 4.1.10. An immediate consequence of Euler's criterion is the following ;
-1 is a square of $\mathbb{F}_p$ if and only if $(-1)^{\frac{p-1}{2}} = 1$ if and only if $p \equiv 1 \pmod 4$.

Proof. There are several ways to demonstrate it, we choose to use a exact sequence. Let us introduce (4) and we prove that $\operatorname{Im}(f) = \ker(\chi)$.

$$1 \longrightarrow \mathbb{F}_p^{*2} \xrightarrow{f} \mathbb{F}_p^* \xrightarrow{\chi} \{\pm 1\} \longrightarrow 1. \tag{4}$$

$\boxed{\subset}$ Let us show that $\operatorname{Im}(f) \subset \ker(\chi)$. Let $x \in \operatorname{Im}(f)$. There exist y such that $x = y^2$. It follows that $\chi(x) = (x^{\frac{p-1}{2}})^2 = y^{p-1} = 1$ by Fermat's theorem.
$\boxed{\supset}$ We have to show that $\ker(\chi) \subset \operatorname{Im}(f)$ by reasoning on cardinalities. By Lagrange's theorem we have $|(\mathbb{F}_p^{*2})| = |(\mathbb{F}_p^*)/\{\pm 1\}| = \frac{p-1}{2}$. It follows that $\mid \operatorname{Im}(f) \mid = \frac{p-1}{2}$. Moreover, the order of the kernel of χ is at most the number of roots of $x^{\frac{p-1}{2}}$ i.e. $\frac{p-1}{2}$. Moreover, we had prove that $\operatorname{Im}(f) \subset \ker(\chi)$, we can deduce the equalities. □

The isomorphisms are a mean of connecting two elements that have nothing to do with each other. In particular all properties are preserved by the isomorphism. In fact, if A is an integral domain, that implies B is isomorph to A is also an integral domain thanks to the isomorphism.

Lemma 4.1.11 (third isomorphism theorem)**.** Let A be a ring, let I, J be two ideal. There is a canonical isomorphism

$$A/I \Big/ (I+J)/I \simeq A/(I+J).$$

Proof. The application

$$\begin{aligned}\phi:\ \ & A/I \longrightarrow A/(I+J)\\ & a+I \longrightarrow a+(I+J).\end{aligned}$$

. We have to check that the function is well-defined, let $a, a' \in A$. As $a+I = a'+I$, then, $a - a' \in I \subset I + J$. To prove that φ is surjective, let $\alpha \in A/(I+J)$. Choose $a \in A$ such that $\alpha = a + (I+J)$; then $\alpha = \varphi(a+I)$. As for the kernel of φ, an element $a+I$ lies in the kernel if and only if $a+(I+J) = 0+(I+J)$, if and only if $a \in I+J$, if and only if $a+I \in (I+J)/I$. By the isomorphism theorems we have a canonical quotient by its kernel. Therefore, $A/I \Big/ (I+J)/I \simeq A/(I+J)$. □

We apply it to our problem. Let us set $A = \mathbb{Z}[X]$. Let $I = (p)$ and $J = (X^2+1)$ where we denote by (a) the ideal of $\mathbb{Z}[X]$. One has $I + J = (p, X^2+1)$. Let $A = \mathbb{Z}[X]$. Consider the polynomial X^2+1. Given $P \in \mathbb{Z}[X]$, we can perform the Euclidean division of P by X^2+1 in $\mathbb{R}[X]$: this gives $Q, R \in \mathbb{R}[X]$ such that $P = (X^2+1)Q + R$, with $\deg(R) < 2$, i.e. $R(X) = bX + a$ for $a, b \in \mathbb{R}$. Since X^2+1 has integer coefficients and its leading coefficient is 1, the coefficients of Q and R are actually integers: $a, b \in \mathbb{Z}$.

Now, evaluation at i (a square root of -1) is a morphism $A \to \mathbb{C}$, $P \mapsto P(i)$. If $P = (X^2+1)Q+R$ as above, then $P(i) = R(i) = a + bi$, so P is in the kernel if and only if $a = b = 0$ (since i is irrational), i.e. if P is a multiple of X^2+1, and the image of the evaluation map is the set of all $a+bi$ where a, b run over $\mathbb{Z}$, i.e. the subring $\mathbb{Z}[i]$ generated by i in $\mathbb{C}$. In other terms,

$$A/J = \mathbb{Z}[X]/(X^2+1) \simeq \mathbb{Z}[i].$$

On the other hand, the reduction map $\mathbb{Z}[X] \to \mathbb{F}_p[X]$, $\sum_{k=0}^{r} a_k X^k \mapsto \sum_{k=0}^{r} \pi(a_k) X^k$, where $\pi : \mathbb{Z} \to \mathbb{F}_p$ is the canonical projection, is a morphism of rings and its kernel is $I = (p)$. Hence,

$$A/I = \mathbb{Z}[X]/(p) \simeq \mathbb{F}_p[X].$$

$$\begin{tikzcd}
& \mathbb{Z}[X] \arrow[ld] \arrow[rd] & \\
\mathbb{F}_p[X] \arrow[rd] & & \mathbb{Z}[X]/(X^2+1) \simeq \mathbb{Z}[i] \arrow[ld] \\
& \mathbb{Z}[X]/(p, X^2+1) \simeq \mathbb{F}_p[X]/(X^2+1) \simeq \mathbb{Z}[i]/p\mathbb{Z}[i] &
\end{tikzcd}$$

Figure 1: Illustration of 4.1.11 in this context.

Proof of Fermat's Theorem

Thanks to all the propositions, we will now prove the theorem 4.0.1.

Proof. Let p be a prime number as p $\equiv 1 \pmod 4$, thanks to 4.1.10, we have any difficulty in rolling out the demonstration.

$$\begin{aligned}
p \equiv 1 \pmod 4 &\iff (-1)^{\frac{p-1}{2}} = 1 \\
&\iff \left(\frac{-1}{p}\right) = 1 \\
&\iff \exists z \in \mathbb{F}_p,\ z^2 = -1 \\
&\iff X^2+1 \text{ has a root in } \mathbb{F}_p \\
&\iff \text{the ideal } (X^2+1) \text{ is not prime in } \mathbb{F}_p[X] \\
&\iff \mathbb{F}_p[X]/(X^2+1) \text{ is not integral} \\
&\iff \mathbb{Z}[i]/(p) \text{ is not integral (since } \mathbb{F}_p[X]/(X^2+1) \simeq \mathbb{Z}[i]/(p)) \\
&\iff (p) \text{ is not irreducible in } \mathbb{Z}[i] \\
&\iff \exists a,b \in \mathbb{Z},\ p = (a+bi)(a-bi) \\
&\iff \exists a,b \in \mathbb{Z},\ p = a^2+b^2.
\end{aligned}$$

□

Thus, one can see that this practical problem is governed by laws of abstract number theory. This theoretical approach will be essential to implement an efficient algorithm for quite large numbers.

4.2 Implementation.

We chose to use SageMath because it is a free software for symbolic and numerical computation, designed to explore and manipulate a wide range of mathematical structures. Unlike Python, SageMath allows the construction and manipulation of abstract mathematical objects, such as rings, fields, vector spaces, or groups, in a natural and algorithmic way. This makes it a powerful tool for experimenting or illustrating practical concepts with theoretical notions. We want to implement an algorithm which finds values of a, b such that $p = a^2 + b^2$ within a reasonable computational time. The key idea is that the norm of a Gaussian integer gives exactly a and b in the desired form;

$$N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}, \quad z = a+bi \longmapsto N(z) = z\overline{z} = (a+bi)(a-bi) = a^2+b^2.$$

The implementation of Euclidean division in $\mathbb{Z}[i]$

First of all, we want to prove that $\mathbb{Z}[i]$ is Euclidean, and to use the Euclidean division to compute gcd's. For a real number u, we set $\{u\} = \lfloor u + \frac{1}{2} \rfloor$, so that $u - \{u\} \leq \frac{1}{2}$; it is the closest integer to u (or, if $u \in \frac{1}{2} + \mathbb{Z}$, one of the two closest integers).

Proposition 4.2.1. The ring $\mathbb{Z}[i]$ is Euclidean. More precisely, let $a, b \in \mathbb{Z}[i]$ with $b \neq 0$. Write $a/b = u+vi$, with $u, v \in \mathbb{R}$. Let $q = \{u\}+\{v\}i$ and $r = a-bq$. Then $a = bq+r$ and $N(r) < N(b)$, where N is the norm $N(x + yi) = x^2 + y^2$.

Proof. The equality $a = bq + r$ follows directly from the definition of r. We have $N(r/b) = N(a/b - q) = N((u - \{u\}) + (v - \{v\})i) = (u - \{u\})^2 + (v - \{v\})^2 \leq 1/2^2 + 1/2^2 = 1/2 < 1$, and, since N is multiplicative, it follows that $N(r) < N(b)$. □

First, we have to define the field Number K containing a root of x^2+1. Here, $K = \mathbb{Q}(i)$ and $i^2 = 1$. This allows us to work in SageMath with Gaussian numbers. The quotient of a by b is a rational number that we must round down (or up) to the nearest integer to find suitable q, r integers. We have 4 possibilities because a, b can be approximate by two integers each as we can see on figure (2). Thanks to that we have the smaller value of q and the reminder r can be deduce easily.

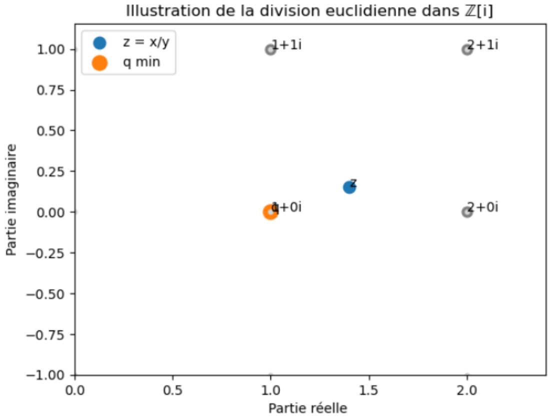

Figure 2: Illustration of the Euclidean division in $\mathbb{Z}[i]$.

Now, we can implement gcd. We want to implement an algorithm in order to handle numbers that are impossible to manipulate by hand. Thus, the algorithmic complexity must be appropriate, meaning that it does not grow too quickly with the size of the number. Answering this question requires some algorithmic notions, to be detailed in the book of Michel Demazure : *Cours D'algebre* especially with Lamé's theorem which provides an explanation. One can easily see that the worst case occurs when $q = 1$ at each iteration. Moreover, the course of the Euclid algorithm follows a Fibonacci sequence $F_{n+2} = F_{n+1} + F_n$ with $F_0 = 0, F_1 = 1$ by definition. Lame's theorem states that the longer the algorithm, the larger the initial numbers.

Proposition 4.2.2 (Lamé's theorem)**.** Let $a > b > 0$ be two positive integers and $d = pgcd(a, b)$. If Euclid's algorithm requires n steps to compute, then: $a, b \leq F_{n+1}$ where F_{n+1} is the $(n+1)^{th}$ Fibonacci number.

Proof. Without loss of generality, one assumes oneself $a > b$. We reason by recurrence on n. If $n = 1$, b is a multiple of a. We have $\gcd(a, b) = b$. Then, we have $b = d = dF_2$ and $x > 2d = dF_3$ because $F_2 = F_0 + F_1 = 1$ et $F_3 = F_2 + F_1 = 1 + 1 = 2$. If $n > 1$, we suppose $z \geq dF_n, y \geq dF_{n+1}$. In the n^{th} iteration, (x, y) became (y, z) with relation $z = x - qy \leq x - y$. But by hypothesis of recurrence. $x \geq y + z \geq dF_n + dF_{n+1} = dF_{n+2}$. We have the result. □

Corollary 4.2.3. Let $a > b > 0$ be two positive integers. If Euclid's algorithm requires at most $\frac{2}{3}\log(a, b) + O(1)$ steps.

Proof. Wee associate this sequence with the characteristic polynomial $r^{j+1} = r^j + r^{j-1}$ which is equivalent to $r^2 = r + 1$. The root is the golden ratio $\phi = \frac{\pm 1+\sqrt{5}}{2}$ and $\bar{\phi} = \frac{1-\sqrt{5}}{2}$. By the formula of Binet (admitted), we have the expression of $F_k = \frac{\phi^k}{\sqrt{5}}$ and $b \geq F_{k+1}$. By the logarithm properties, it follows that $k \approx O(\log_\phi(b))$ □

This concludes the first step of our goal.

Cipolla's algorithm

As we saw in 4.1, find z such that $z^2 \equiv -1 \mod p$ is crucial to find a, b. Thus, we have to construct an algorithm that allows us to find this z in a reasonable amount of time : we can implement Cipolla's algorithm which is based on field extension.

Theorem 4.2.4. *$\forall$ p prime and $\forall d \in \mathbb{N}^*$, $\exists!$ field L of the cardinal of p^d.*

The proof is too complex and not really important for our case. However, we can focus on the case $d = 2$. Indeed, we are looking for a field extension whose cardinal is p^2.

Lemma 4.2.5. Let p be a prime number, and let n be a square in $\mathbb{F}_p^*$. There exists $a \in \mathbb{F}_p$ such that $a^2 - n$ is not a square. More precisely, the number of such a is $\frac{p-1}{2}$.

Proof. For $a \in \mathbb{F}_p$, $a^2 - n$ is a square if and only if there exists $b \in \mathbb{F}_p$ such that $a^2 - n = b^2$, i.e. $(a+b)(a-b) = n$. Equivalently, there exists $t \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$ such that

$$a + b = t, \quad a - b = \frac{n}{t}.$$

In other terms, $a^2 - n$ is a square if and only if there exist t and b such that

$$a = \frac{1}{2}\left(t + \frac{n}{t}\right), \quad b = \frac{1}{2}\left(t - \frac{n}{t}\right).$$

Set $f : \mathbb{F}_p^* \to \mathbb{F}_p$, $t \mapsto \frac{(t^2+n)}{(2t)}$. Then $f(t) = f(\frac{n}{t})$. It means that if $a^2 - n$ is a square, then a has two preimages under f, unless $a = f(t)$ with $t = \frac{n}{t}$, i.e., t is one of the square roots of n. Hence, there are $\frac{p-3}{2} + 2 = \frac{p+1}{2}$ values of a for which $a^2 - n$ is a square, and $\frac{p-1}{2}$ values for which $a^2 - n$ is not a square.

This means that when we look for an a such that $a^2 - n$ is not a square, trying a random value for a gives a probability of success of about $\frac{1}{2}$, and we should find a solution in approximately 2 trials on average.

Once such an a is found, we know that the polynomial $X^2 - (a^2 - n)$ is irreducible in $\mathbb{F}_p[X]$. We build the quadratic field extension $L = \mathbb{F}_p[X]/(X^2 - a^2 + n)$, in which the projection ω of X is a square root of $a^2 - n$. As a vector space over $\mathbb{F}_p$, the dimension of L is 2 and $(1, \omega)$ is a basis of L. In particular, L has cardinality p^2.

The field L comes with an interesting map:

$$F : L \to L, \quad x \mapsto x^p.$$

For any $k \in \{1, \dots, p-1\}$, the binomial coefficient $\binom{p}{k}$ is a multiple of p, so $F(x+y) = F(x) + F(y)$ for any $x, y \in L$. Obviously, $F(xy) = F(x)F(y)$ and $F(1) = 1$. Therefore, F is a field morphism. As such, F is injective, and since L is finite, it is surjective too. The map F is called the Frobenius automorphism.

It is an involution. First of all, the polynomial equation $F(x) = x$ has at most p solutions, and Fermat's little theorem says that elements of $\mathbb{F}_p$ are indeed solutions. Next, from $\omega^2 = a^2 - n$ we deduce that $F(\omega)^2 = a^2 - n$ and $F(\omega) \neq \omega$ since $\omega \notin \mathbb{F}_p$ (because $a^2 - n$ is not a square). Hence, $F(\omega)$ is the other square root of $a^2 - n$, namely $-\omega$. For $u, v \in \mathbb{F}_p$, it follows that $F(u + v\omega) = u - v\omega$. In particular, $F^2 = \mathrm{id}_L$. □

Proposition 4.2.6. Let p be a prime number, let n be a square in $\mathbb{F}_p$, and let a be such that $a^2 - n$ is not a square. Let ω be a square root of $a^2 - n$ in an extension of $\mathbb{F}_p$. Then $(a + \omega)^{\frac{p+1}{2}}$ is a square root of n in $\mathbb{F}_p$.

Proof. Let $x = (a+\omega)^{\frac{p+1}{2}}$. Then

$$x^2 = (a+\omega)^{p+1} = (a+\omega)F(a+\omega) = (a+\omega)(a-\omega) = a^2 - (a^2 - n) = n.$$

Since n is a square, we know that $x \in \mathbb{F}_p$. □

Final implementation

Now, we have all the tools to implement a resolution of theorem 4.0.1 : finding a, b for all p be prime such that $p \equiv 1 \pmod 4$.

Lemma 4.2.7. Let p be a prime number such that $p \equiv 1 \pmod 4$. Let r be an integer such that $r^2 \equiv -1 \pmod p$, and let $d = \gcd(p, r+i)$ in $\mathbb{Z}[i]$. Then $N(d) = p$, where N is the norm $N(a+bi) = a^2 + b^2$.

Proof. Let $x \in \mathbb{F}_p$ such that $x^2 + 1 \equiv 0$ $[p]$. Consequently, we have $p|(x+i)(x-i)$. Let us pose $d = \gcd(p, x+i)$. We must check that the gcd is not a unit (that is, $\pm 1, \pm i$). On the one hand $p \mid (x^2+1) = (x-i)(x+i)$. Thus, $\gcd(p, (x+i)) \neq 1$. On the other hand, we can assume that $\gcd(p, x+i) = a+bi$. $p \mid (x-i)(x+i)$ and $(a+bi) \mid p$ (definition of gcd), we can deduce that $a+bi \mid (x-i)(x+i)$. Thus, $a+bi \mid x-i$ or $a+bi \mid x+i$. It follows that $\gcd(p, x+i) = a+ib$. Using the norm, we can deduce $N(a+bi) = a^2+b^2 \mid N(p) = p$ or p^2. Impossible for p^2 because otherwise $d = p$ or $d = pi$. Thus, $N(d) = p = a^2 + b^2$.

□

You will find the algorithm in the appendix. This is really impressive because our algorithm takes only 0.03 seconds to find a solution for a 50-digit number, 3,45 seconds for a 200-digit number.

5 Resolution of $p = a^2 + db^2$

After solving the theorem, we realize that it is only a particular case of a much larger question. We want to find a, b be integers that satisfy (5).

Let p be an odd number and a, b, p be integers ;

$$p = a^2 + db^2. \tag{5}$$

For this, we consider the ring $\mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Z}\}$. Can we reason in a similar way? The proof is possible because the ring is Euclidean, so for which values of d is the ring Euclidean? Although difficult, the question is solved. On the one hand, we chose to consider small cases such that $d = 2$, $d = 3$. But we will soon see that the reasoning is almost identical. On the other hand, we want to generalize to all d.

5.1 Case $d = 2$

We want to solve equation $p = a^2 + 2b^2 = (a + b\sqrt{-2})(a - b\sqrt{-2})$ that is clearly related to the ring $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$. In fact, p can be expressed in this form under certain conditions.

Theorem 5.1.1. *Let p be an odd integer. There exist a and b such that ;*

$$p = a^2 + 2b^2 \quad \Longleftrightarrow \quad p \equiv \pm 1 \pmod{8}. \tag{6}$$

As one might expect, the proof of the theorem is essentially the same as 4.1. This time, the quotient$A/(p)$ is identified at $\mathbb{F}_p[X]/(f)$ where $f = X^2 + 2$ thanks to theorem 4.1.11. Moreover, we have an essential condition $x^2 = -2[p]$. We can conclude that p can be factored in $\mathbb{Z}[\sqrt{-2}]$ by the same way. Moreover, we still need to use the quadratic residue thank to the second quadratic reciprocity. Indeed, if $\left(\frac{-2}{p}\right) = 1$, it exists z such as $z^2 \equiv -2 \pmod{p}$.

Proposition 5.1.2. Let p be odd prime.

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } \pm 1 \text{ mod}(8). \\ -1 & \text{if } \pm 3 \ \text{ mod}(8). \end{cases}$$

Proof. Let α be a root of $X^4 + 1 = 0$. It is an eighth root of unity in an algebraic extension of $\mathbb{F}_p$. Hence, $\alpha^8 = 1$ but $\alpha^4 = (\alpha^2)^2 = -1$ is a square of -1. So we have the relation : $\alpha^2 = -\alpha^{-2}$. Let $\beta = \alpha + \alpha^{-1}$. $\beta^2 = (\alpha + \alpha^{-1})^2 = 2$. Thus, 2 is a square in $\mathbb{F}_p$ if and only if $\beta^p - \beta = 0$ with $\beta^p = \alpha^p - \alpha^{-p}$. On the one hand, if $p \equiv \pm 1$ [8], if and only if $\beta \in \mathbb{F}_p$, $\beta^p = \beta$ it is over. On the other hand, if $p \equiv \pm 3$ [8] $\beta^3 = \alpha^3 - \alpha^{-3} = -\beta$ there is no square in $\mathbb{F}_p$. □

The implementation will be essentially the same expect a slight nuance. Indeed, the notion of real or imaginary part does not exist; instead, a function is used to extract the coefficients. Before implementing the Euclidean division in $\mathbb{Z}[\sqrt{-2}]$, we must prove that the ring is Euclidean.

Proposition 5.1.3. The ring $\mathbb{Z}[\sqrt{-2}]$ is Euclidean.

Proof. Let $a, b \in \mathbb{Z}[\sqrt{-2}]$ with $b \neq 0$.
One has $\frac{r}{b} = \frac{a}{b} - q = (u - \{u\}) + (v - \{v\})\sqrt{-2}$. Then, we apply the norm :
$N\left(\frac{r}{b}\right) = (u - \{u\})^2 + 2(v - \{v\})^2 \leq \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{3}{4} < 1$. Thus, $N(r) = N(b) \cdot N\left(\frac{r}{b}\right) < N(b)$. □

The gcd and Cipolla's algorithm are identical, so it only remains to find the correct coefficients of gcd to use to obtain the desired form.

Lemma 5.1.4. Let p be a prime number such that $p \equiv 1 \pmod 4$. Let r be an integer such that $r^2 \equiv -2 \bmod p$, and let $d = \gcd(p, r+i)$. Then $N(d) = p$, where N is the norm $N(a + \sqrt{-2}b) = a^2 + 2b^2$.

Proof. Let $d = \gcd(p, z + \sqrt{-2}) = a + \sqrt{-2}b$ by same argument. Thus, $(a + \sqrt{-2}) \mid p$ by passing through the norm $N(a + \sqrt{-2}) \mid N(p)$ so $a^2 + 2b^2 \mid p^2$. It follows that $a^2 + 2b^2 = p$. □

We have an efficient algorithm which find a solution as quickly as the previous one.

Example 5.1.5.

$$(-214835139219429)^2 + 2 \times 1700595085590310^2 = 5830201427311259029681742878241. \quad (7)$$

5.2 Resolution of $a^2 - ab + b^2$, Eisenstein integers

We want to prove this theorem.

Theorem 5.2.1. *Let p an odd prime number, a and b be integers ;*

$$p = a^2 - ab + b^2 \iff p \equiv 1 \pmod{3}.$$

The resolution of this new equation allow us to studies the ring of Eisenstein integers ;

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\},$$

with $\omega = e^{2i\pi/3} = \frac{-1+i\sqrt{3}}{2}$. We can deduce the relations $j^2 = \bar{w} = \frac{-1-\sqrt{3}}{2}$ and the polynomial $w^2 + w + 1 = 0$ because $0 = w^3 - 1 = (w-1)(w^2 + w + 1)$. We can deduce that $\mathbb{Z}[w] \simeq \mathbb{Z}[X]/(w^2 + w + 1 = 0)$. Moreover, one can see that $N(a + wb) = a^2 - ab + b^2$ that exactly the good form.

As one can expect, quadratic reciprocity will allow us to prove theorem 5.2.1.

Proposition 5.2.2. Let p be prime.

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3, \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Proof. Let p be an odd prime. If $p = 3$, $\left(\frac{-3}{3}\right) = 0$, we suppose $p \neq 3$.
$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$. However, by the quadratic reciprocity ; $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{2(p-1)}{4}}$. Moreover $\left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \mod 3$ (It enough to compute the squares modulo 3). Finally, we can deduce that $\left(\frac{-3}{p}\right) = (-1)^{p-1}\left(\frac{p}{3}\right)$. Moreover, $(-1)^{p-1} = 1$ because p is an odd prime and the squares modulo 3 are 0 and 1, which concludes the proof.

□

Regarding the Euclidean division, the reasoning is the same but involves a subtlety. Indeed as you can see in 3, the lattice of Eisenstein integers is triangular. Then to find the nearest integer of the quotient $\frac{a}{b} \in \mathbb{R}$, one must project the real quotient onto this lattice through a change of basis. We have to prove that the ring is Euclidean. We have the same inequalities for the closest integers. Then, by using the norm, we obtain

$$N\left(\frac{r}{b}\right) = N\left(\frac{a}{b} - q\right) = (u - \{u\})^2 - (u - \{u\})(v - \{v\}) + (v - \{v\})^2 \leq \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} = \frac{5}{8} < 1.$$

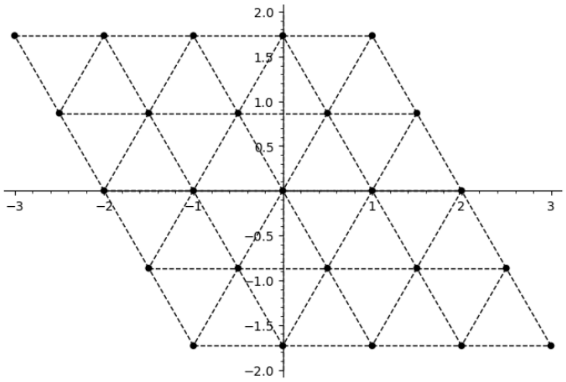

Figure 3: Illustration of Eisenstein integers.

The gcd algorithm and Cipolla's algorithm coincide in this setting, so it only remains to determine the appropriate coefficients of the greatest common divisor in order to obtain the desired quadratic form. Indeed, $\mathbb{Z}[\omega]$, one has $\gcd(p,\, z + \omega) = a + b\omega$ by the same argument as in the classical case. Hence $a + b\omega$ divides p in $\mathbb{Z}[\omega]$. Passing to the norm, we obtain $a^2 - ab + b^2 \mid p^2$. And finally, $a^2 - ab + b^2 = p$. To exact a, b, we use an automorphism σ which is the analogue of the complex conjugation for Gaussian integers. Let $z = a + b\omega$, one has $\sigma(z) = a + b(\omega - 1)$. Moreover, we solve the system ;

$$\begin{cases} z + \sigma(z) = 2a - b, \\ z - \sigma(z) = (1 + 2\omega)b. \end{cases}$$

and we find $b = \frac{z - \sigma(z)}{1+2\omega}$, $a = \frac{1}{2}(z - \sigma(z) + \frac{z-\sigma(z)}{1+2\omega})$. However, σ is solution of $\sigma(\omega)^2 + \sigma(\omega) = 0$, it follows that $\omega + \sigma(\omega) = -1$ and $\omega\sigma(\omega) = 1$. We will store these values in a variable C with $(\frac{1}{2}(1 + \frac{1}{1+2\omega}), \frac{1}{2}(1 - \frac{1}{1+2\omega}),\ \frac{1}{1+2\omega})$. We introduce a function **Re_im** which return the coefficients a, b of $z = a + b\omega$:

$$\begin{cases} a = \alpha z + \beta\sigma(z); \\ b = \gamma z - \gamma\sigma(z). \end{cases}$$

Example 5.2.3. $107011^2 - 107011 \times 69420 + 69420^2 = 8841786901$.

5.3 General d

We want to resolve with the same method the equation (5). Quite intuitively, we will use the field $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ square-free. We have many proprieties.

Proprieties of the ring.

Proposition 5.3.1. Let d be a square-free integer. Then the ring $\mathcal{O}_d$ of algebraic integers in $\mathbb{Q}(\sqrt{d})$ is

$$\mathcal{O}_d = \begin{cases} a+b\sqrt{d}, & a,b \in \mathbb{Z}, \text{ if } d \equiv 2,3 \pmod 4, \\ \frac{a+b\sqrt{d}}{2}, & a,b \in \mathbb{Z}, \text{ if } d \equiv 1 \pmod 4. \end{cases}$$

Proof. Let $\sqrt{d}$ be the root of the polynomial $X^2 - d$. A general element of K is expressed as $a + b\sqrt{d}, a - b\sqrt{d}$. $x \in K$, we can deduce $\sigma(x) = -x \in A$. By pose $x = a + b\sqrt{d}$, with $a, b \in \mathbb{Q}$ we have : $x + \sigma(x) = 2a \in \mathbb{Q}$, $x\sigma(x) = a^2 + db^2 \in \mathbb{Q}$ (1). Thus, $\mathbb{Z}$ is principal and, above all, integrally closed. Conditions (1) are essential if $a + b\sqrt{d}$ is an integer in $\mathbb{Z}$. Hence,x is a root of $X^2 - 2aX + a^2 - db^2 = 0$.
By (1), $(2a)^2 - d(2b^2) \in \mathbb{Z}$.Since $2a \in \mathbb{Z}$, it follows that $d(2b)^2 \in \mathbb{Z}$. However, d is square-free. If $2b$ is not an integer, he has a prime factor at the denominator express as p^2 thus d cannot make it an integer. So, $2b \in \mathbb{Z}$. We can pose $a = \frac{u}{2}, b = \frac{v}{2}$, then we have.

$$\left(\frac{u^2}{4}\right) - \left(\frac{dv^2}{4}\right) \in \mathbb{Z} \longleftrightarrow u^2 - dv^2 \in 4\mathbb{Z} \qquad (2).$$

- If v is even, u also, it follows that $a, b \in \mathbb{Z}$.
- If v is odd, $v^2 \equiv 1[4]$, so $u^2 \equiv 0, 1 \pmod 4$ (only possibilities). d is square-free, thus not a multiple of 4 $u^2 \equiv 1 \pmod 4$ and $d \equiv 1 \pmod 4$. □

Classification of $\mathbb{Z}[X]/(X^2 - d)$

To resolve the equation (5) for each value of d, we have to study the structure of the quotient $\mathbb{Z}[X]/(X^2 - d)$ in the quadratic integer ring $\mathbb{Z}[\sqrt{d}]$.

Let A a field of integer, $d \in \mathbb{Z}$ square-free, and $L = \mathbb{Q}[\sqrt{d}]$. We can suppose $p \neq 2$. $A = \mathbb{Z}+\mathbb{Z}[\sqrt{d}]$ where $B \subset \mathbb{Z} + (\frac{1}{2} + \frac{\sqrt{d}}{2})\mathbb{Z}$ we work modulo p $B \subset a + (b + p)(\frac{1+\sqrt{d}}{2})$. We can deduce that $A/Ap \simeq \mathbb{Z} + \sqrt{d}/(p)$ because p, d are odds. Moreover, $\mathbb{Z} + \sqrt{d} \simeq \mathbb{Z}[X]$ by a natural isomorphism. Let determinism his kernel : $ker(\phi) = \{P(x) \in \mathbb{Z}[X] \mid P(\sqrt{d}) = 0\} = (X^2 - d)$. By theorem of isomorphism.

$$\mathbb{Z}[X]/(X^2 - d) \simeq \mathbb{Z} + \mathbb{Z}\sqrt{d}.$$

we can distinguish several cases based on the roots of the polynomial :
- The polynomial $(X^2 - d)$ has two roots. It follows that the quotient A/p is decomposed into two fields by the Chinese remainder theorem. The polynomial can be expressed as $X^2 - d = (X - a)(X - b) = X^2 - X(a + b) + ab$. However, there is no term in X, then $a + b = 0$ and $ab = -a^2 = -d$. Then, d is a quadratic residue mod p and p is decomposed.
- The polynomial $(X^2 - d)$ has no root,. It is irreducible, therefore maximal. It follows that A/Ap is a field and d is not a quadratic residue mod p and p is inert.
- The polynomial (X^2-d) has a unique root, the quotient $\mathbb{Z}[X]/(X^2-d)$ had nilpotent elements. p is ramified.

Let us focus on the case $p = 2$. On the one hand, if $d \equiv 2, 3 \pmod 4$, $B = \mathbb{Z} + \mathbb{Z}[\sqrt{d}]$, so $A/2A \simeq \mathbb{F}_2/X^2 - d$ with $X^2 + 1 = (X^2 + 1)^2$, it follows that it is a square; we say that it decomposed.
On an other hand, if $d \equiv 1 \pmod 4$, $\frac{1+\sqrt{d}}{2}$ admits as its minimal polynomial$X^2 - X - \frac{d-1}{4}$. In

fact, we have $A/Ap \simeq \mathbb{F}_2/X^2 - X - \delta$. We can deduce different cases. If $d \equiv 1 \pmod 8$, $\delta = 0$ it follows that $X^2 - X = X(X-1)$. If not, $d \equiv 5 \pmod 8$, $\delta = 1$, $X^2 - X - 1 = X^2 + X + 1$ because $X^2 = 1$ which is irreducible.

Euclidean ring

This classification highlights the importance of the polynomial for the classification of an Ideal p prime. Our problem corresponds to the first case. This allows showing that the problem is actually much deeper and that it can be solved for any value of d. We have implemented the Euclidean division and an algorithm allows the decomposition of a prime number p into a sum of squares for $d = 1, 2, 3$ but in reality the Euclidean rings are much more numerous, although not infinite. It comes from this theorem that we will not prove because it is obvious difficulty.

Proposition 5.3.2. The ring of integers $\mathcal{O}_d$ of a quadratic number field $\mathbb{Q}(\sqrt{d})$ is norm-Euclidean if and only if $d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$.

With this general study of rings, we seek to standardize our algorithms into a single by entering d, p and returning the decompositions when possible. On the one hand, we realize that object-oriented programming would be more appropriate. The algorithm works very well for $d < 0$ but often crashes for $d > 0$ because the number of Neighbors needed to have a minimum standard changes from one value to another. Nevertheless, a satisfactory result is achieved.

6 Lagrange's Four-Square Theorem

Theorem 6.0.1. *Let p be odd integer prime, it exists $a, b, c, d \in \mathbb{N}$ such that $p = a^2+b^2+c^2+d^2$.*

Remark 6.0.2. If $p \equiv 1 \pmod 4$, then Lagrange's theorem follows from Fermat's two-square theorem by writing $p = a^2 + b^2$, and then setting $c = d = 0$.

6.1 Theory of the quaternion ring

The ring of quaternions was born from a desire to find an extension of the ring of complex numbers. It is impossible to find consistent relations for three dimensions, whereas for four components, one can define the following algebraic properties. It is moreover what makes the 3 squares theorem difficult to study. The quaternions ring is a classic example of non commutative Euclidean ring that complicate all our reasoning.

Definition 6.1.1. The algebra of quaternions is the real vector space with a basis denoted by $(1, i, j, k)$, endowed with the unique bilinear product such that $i^2 = j^2 = k^2 = ijk = -1$ and the multiplication rules

$$ij = k, \quad ji = -k, \quad jk = i, \quad kj = -i, \quad ki = j, \quad ik = -j.$$

It is tedious but straightforward to check directly that this algebra is associative. Alternatively, one can realize it as the algebra with basis

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

If R is a subring of $\mathbb{R}$, we denote $\mathbb{H}(R) = \{a + bi + cj + dk \mid a, b, c, d \in R\}$. Then $\mathbb{H}(R)$ is a subring of $\mathbb{H}(\mathbb{R})$.

We pose $\mathbb{H}_H$, we introduce Hurwitz's quaternions which have interesting properties. Indeed, coefficients a, b, c, d are all integers or all half-integers. In this last case, all of them are odd; otherwise, one can reduce to the first case.

$$\mathbb{H}_H = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\} \cup \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z} + \frac{1}{2}\} \subset \mathbb{H}(\mathbb{Z}) \qquad (8)$$

The Following is a list of properties of this subring. The first three properties are not very difficult. It is especially the fourth one that is important and makes the theorem work.

Proposition 6.1.2. 1) The set of Hurwitz quaternions is a non-commutative subring of $\mathbb{H}(\mathbb{Q})$ contains $\mathbb{H}(\mathbb{Z})$.
2) Let $z \in \mathbb{H}$ $z + \bar{z} \in \mathbb{Z}, N(z) = z\bar{z} \in \mathbb{Z}$.
3) Let z be invertible if $N(z) = 1$.
4) Every left (respectively, right) ideal is principal.

Proof. 1) By construction, we have $\mathbb{H}(\mathbb{Z}) \subset \mathbb{H}_H$. We show that a subring. Let $1 \in \mathbb{H}$, we have the stability by addition because the sum of two integers is an integer and The sum of two half-integers is an integer. We can also trivially prove the stability by multiplication thanks to the multiplicative rules on (6.1.1).

2) The proof is trivial if a, b, c, d are integers and the sum or multiplication of two half-integers are integers.
3)$\boxed{\Longrightarrow}$ If z is invertible, let z' be his inverse, we have : $= N(1) = N(zz') = N(z)N(z') = 1$. As $N(z), N(z')$ are positive integers, it follows that $N(z) = 1$.
$\boxed{\Longleftarrow}$, Let $z \in \mathbb{H}_H$ such that $N(z) = 1$: $z\bar{z} = \bar{z}z = N(z) = 1$, hence z is invertible.
4)Let $a \in \mathbb{H}$ be a left ideal of $\mathbb{H}$, we can suppose $(a) \neq 0$. Let the set $u \in (a)$ be of minimal reduced norm. u is invertible in $\mathbb{Q}$ invertible in $\bar{u}N(u)^{-1}$ because $u\bar{u}N(u)^{-1} = u\bar{u}(u\bar{u})^{-1} = 1$. Let $y \in A$ we focus on $yu^{-1} \in \mathbb{H}(\mathbb{Q})$ and $z \in \mathbb{H}$ which $N(yu^{-1} - z) < 1$. However, $N(y - zu) = N((yu^{-1} - z)u) = N(yu^{-1} - z)N(u) < N(u)$. Thus, $y - zu \in A$ and $N(u)$ are minimal. We can deduce from the inequality that $y - zu = 0$ and so $y = zu$, $y \in Hu$. That proves that a left ideal is principal. □

6.2 Demonstration of Lagrange's theorem

Proof. Let p be odd prime, commutes with all quaternions. Indeed, p is an integer and hence central. The left ideal is therefore two-sided, so $Hp = pH$. Hence, one may take the quotient by this ideal and study $H\big/Hp$ which is a ring. Let introduce $z = a + bi + cj + dk,\ a, b, c, d \in \mathbb{Z}$ or $\frac{1}{2} + \mathbb{Z}$. We want to show that it exists $z' \in \mathbb{Z}$ represents z mod p. If z is an integer it is over. If not, one set $u = 1 + i + j + k$ and $\frac{p}{2}u \in \mathbb{H}$. Let set $z' = z + \frac{p}{2}u$ which allows one to work modulo p $z \equiv z'$ and $z' \in \mathbb{Z}$. That works because p is odd. As desired $H/Hp \simeq \mathbb{H}(\mathbb{F}_p)$.
Firstly, the equation became $a^2 + b^2 + c^2 + d^2 = 0\ \ [p]$, hence exists a non-zero quaternion with zero norm which is not invertible (if not is norm will be 1). It follows that it engenders a left ideal non trivial.
Secondly, $Hz \subset H/Hp$ by the correspondence theorem $Hp \subset Hz \subset H$. Then, $p \in Hz, \exists z'$ such that $p = zz'$. By using the norm, we can conclude that $a^2+b^2+c^2+d^2 = N(z) = N(z') = p$. □

6.3 Implementation of division for the quaternion ring

Before implement the Euclidean division in $\mathbb{H}_H$, we need to prove that the subring is Euclidean. Let $\alpha \in A, \beta \in A\{0\}$. We perform the Euclidean division of a by b and we pose $\alpha\beta^{-1} = x + yI + zJ + tK \in \mathbb{H}$. As before, $\exists m \in \mathbb{Z}$ such as $|x - \frac{m}{2}|$. In fact, the elements quaternion of Hurwitz are either integers or half-integers. We pose $q = \frac{(m+nI+hJ+lK)}{2}$, however, m, n, h, l must have the same parity, the one which is already fixed by m. It follows the inequities $|y, z, t - n, h, l/2| < \frac{1}{2}$.

$$N(\alpha\beta^{-1} - q) < (x - \frac{m}{2})^2 + (y - \frac{n}{2})^2 + (z - \frac{l}{2})^2 + (t - \frac{k}{2})^2 < \frac{1}{16} + \frac{3}{4} < 1.$$

This proves the Euclidean division for the quaternion ring, which exploits the same principle as previous divisions. We begin with the definition of the ring. **H.** $< \mathbf{i}, \mathbf{j}, \mathbf{k} > =$ QuaternionAlgebra(QQ, -1, -1) which is a built-in SageMath function that defines the Hamilton quaternion algebra. The Euclidean division is more sensitive given the parity problems because all the coefficients must have the same parity (especially for half-integers). In fact, if the division in $\mathbb{Z}[i]$ gave us the choice between 4 neighbours, here it is 81 differents neighbours that we must analyse to choose one which respects the properties of the ring but also the minimality of the norm.

Finding a, b, c, d whose respects the equation is no more difficult. On the one hand, we will show that the equation $a^2 + b^2 + 1 \equiv 0\ [p]$ has a solution. Indeed, we saw that there are $\frac{p+1}{2}$ squares in $\mathbb{F}_p$, hence as many solutions for an equation $-1 - x^2 \in \mathbb{Z}/p\mathbb{Z}$. It follows that the intersection isn't empty. It exists y such that $y^2 = -1 - x^2$ in $\mathbb{F}_p$. Otherwise, said it exists $a, b \in p\mathbb{Z}$ such as $a^2 + b^2 + 1 = (1 + aI + bJ)(1 - aI - bJ) \in pA$. One considers the ideal $I = Ap + A(1 + aI + bJ)$. We have seen that all left ideal is principal hence it exists β such that

$P = A\beta$ and $Ap = pA \subset I \subset A$ because $p \in I$. It exists α such that $p = \alpha\beta$. We must show that these elements are not invertible if not, the ideal is all the ring and that is impossible. If α is invertible $\beta = \alpha^{-1}p$ and then $p \mid (1 + aI + bJ)$. That implies that $(1 + aI + bJ) = p[\frac{x+yI+zJ+tk}{2}]$ and particular that $px = 2$ impossible because $p > 2$ by hypothesis. If β is invertible $p = A$ and then $1 = q(1 + aI + bJ) + q'p$, by multiply by $(1 + aI + bJ)$ it follows that $(1 + aI + bJ) = q'p$ and that impossible. As required $N(p) = N(\alpha)N(\beta) = p^2$. As before, we can use the algorithm of Cipolla which find a solution effectively.
On the other hand, $p \mid a^2 + b^2 + 1 = (1 + ai + bj)(1 - ai - bj)$ and so $\gcd(a + bi + cj, p)$ is not trivial. We have $\gcd(1 + ai + bj, p) = a + bi + cj + dk$ passed by the norm we can conclude that $p = a^2 + b^2 + c^2 + d^2$.

Example 6.3.1.

$$261310810143^2 + 261310810143^2 + 3144269819^2 + 0^2 = 136576565427876657653659.$$

We will end up with an interesting result that allows one to count the number of quadruplets (a, b, c, d) such as $p = a^2 + b^2 + c^2 + d^2$. If the sum of two squares is unique to permutation and sign near, the sum of four squares offers more results. There is a theorem allows to show the number in a way that describes p as the sum of 4 squares.

Theorem 6.3.2 (Jacobi's Theorem)**.** *Let p is an integer. We pose $r_4(p)$ the number of ways to represent n as the sum of four squares.*

$$r_4(n) = 8 \sum_{\substack{m|n \\ 4|m}} m.$$

Example 6.3.3. Let $p = 12$, its divisors are $\{1, 2, 3, 4, 6, 12\}$, we remove those divisible by 4, $\{1, 2, 3, 6\}$. We have $8 \times 12 = 96$ possibilities : the quartets $(2, 2, 2, 0)$ and $(3, 1, 0, 2)$ up to a permutation and a sign.

Thus, when our algorithm finds a solution, it is only one among the others.

7 Conclusion

Writing a prime integer in a quadratic form is a vast research topic, and our work only addresses a tiny fraction of it. This illustrates how theoretical algebraic structures can help solve and implement a concrete problem. Indeed, we have seen that each quadratic form is closely associated with a ring from which essential algebraic properties can be derived: $\mathbb{Z}[i]$ for $p = a^2 + b^2$, more generally $\mathbb{Z}[\sqrt{-d}]$ for $a^2 + db^2$, and $\mathbb{H}$ for $p = a^2 + b^2 + c^2 + d^2$. This allowed us to examine certain properties for each ring and to generalize when studying more general equations. The key idea is that the ring must be Euclidean to find suitable pairs/quadruples integers, but there are many other ways to solve equations for example, using class field theory, which is entirely beyond the scope here. Implementing an efficient algorithm is only possible thanks to a deep understanding of the algebraic properties of each ring. Although there are some specificities, we have seen that the algorithms are not fundamentally different from each other and follow the same general protocol.

8 Annexe

8.1 Algorithms

Representation of a prime number as $a^2 + b^2$

```
##Euclidean division for Gauss integers.
K.<i> = NumberField(x^2 + 1)
def division_euclidienne(x,y):
    z=x/y
    zr=z.real()
    zi=z.imag()

    voisins_proches = [
        K(a_ + b_*i)
        for a_ in [(floor(zr)), (ceil(zr))]
        for b_ in [(floor(zi)), (ceil(zi))]
    ]

    q = min(voisins_proches, key=lambda q: abs(x - y*q)**2)
    r=x-q*y
    return r,q,z, voisins_proches

r,q , z, v = division_euclidienne(K(12 + 7*i),K(9 + 4*i))

r,q , z, v = division_euclidienne(K(123+ 74*i),K(17-7*i))

q,r,z, v
```

```
#gcd (this algorithm is the same for all the rings).
def pgcd(a,b):
    while b !=0:
        r, q, z, v = division_euclidienne(a,b)
        a, b = b, r
    return a
```

```
#Cipolla's algorithm.
def cipolla(n, p):
    n = Integer(n) % p
    p = Integer(p)
    if p == 2:
        return n

    if pow(n, (p - 1)//2, p) != 1:
        return None

    a = Integer(0)
    while True:
        w2 = Integer((a*a - n) % p)
        if w2 != 0 and pow(w2, (p - 1)//2, p) == p - 1:
            break
        a += 1

    K = GF(p)
    PR = PolynomialRing(K, 'w')
    w = PR.gen()
    Q = PR.quotient(w**2 - PR(w2), 'w')
    ge = Q.gen()

    elem = Q(a) + ge
    res = elem**((p + 1)//2)

    c0 = Integer(res.lift()[0])
    root = Integer(c0 % p)
    return root
```

```
#find a,b
def sum_of_two_squares(p):
    p = Integer(p)
    if not is_prime(p):
        raise ValueError("p␣must␣congruent␣to␣1␣modulo␣4")
    if p % 4 != 1:
        raise ValueError("p␣congruent␣to␣1␣modulo␣4")


    x = cipolla(p- 1, p)
    if x is None:
        raise ValueError("Cipolla␣return␣None")

    ZI.<i> = GaussianIntegers()
    alpha = ZI(x) + i
    pi = gcd(ZI(p), alpha)


    a = Integer(pi.real())
    b = Integer(pi.imag())
    return (abs(a), abs(b))
```

Representation of a prime number as $a^2 + 2b^2$

```
#Euclidean division
K.<sqrt_m2> = QuadraticField(-2)

def division_euclidienne(x, y):
    z = x / y
    a, b = z.polynomial().coefficients(sparse=False)
    zr, zi = a, b
    voisins_proches = [
        K(a_ + b_*sqrt_m2)
        for a_ in [floor(zr), ceil(zr)]
        for b_ in [floor(zi), ceil(zi)]
    ]
    q = min(voisins_proches, key=lambda q_: abs(x - y*q_)**2)
    r = x - q*y

    return q,r , z, voisins_proches
```

The gcd and Cipolla's algorithm are the same

```
def find_ab(p):
    z = cipolla(-2,p)
    d=pgcd(p,z+sqrt_m2)
    a,b=tuple(d[j] for j in range(2))
    return a,b
```

```
p=5830201427311259029681742878148
while p%8!=1 :
    p=next_prime(p)
a,b=find_ab(p)
print(f"{a}^2 + 2*{b}^2 = {p}")
```

Representation of a prime number as $a^2 - ab + b^2$

```
K = CyclotomicField(3)
omega = K.gen()

def eisenstein_proche(z):
    zc = CC(z)
    u = float(zc.real())
    v = float(zc.imag())
    sqrt3 = 3**0.5
    y = 2.0 * v / sqrt3
    x = u + v / sqrt3
    m = int(round(x))
    n = int(round(y))
    return K(m) + K(n)*omega

def eisenstein_euclidean_division(alpha, beta):
    if beta == 0:
        raise ZeroDivisionError("division par z ro dans Zomega")

    z = alpha / beta
    q = eisenstein_proche(z)
    r = alpha - beta*q
    return q,r
```

```
K = CyclotomicField(3)
omega = K.gen()
sigma=K.automorphisms()[1]
C=((1+1/(1+2*omega))/2, (1-1/(1+2*omega))/2, 1/(1+2*omega))

def re_im(q):
    qb=sigma(q)
    return (C[0]*q+C[1]*qb, C[2]*(q-qb))

def trouver_ab(p):
    if p%3!=1 :
        print("Erreur")
        return
    z = cipolla(-3, p)
    Z = K(z) - 2*omega -1
    print(Z*sigma(Z))
    g = pgcd(p, Z)
    a,b=re_im(g)
    return a,b
```

Representation of a prime number as $a^2 + b^2 + c^2 + d^2$

```
    H.<i,j,k> = QuaternionAlgebra(QQ, -1, -1)

```

```
from itertools import product
def nearest_hurwitz(q):
    coeffs = list(vector(QQ, q))

    int_coeffs = [round(c) for c in coeffs]
    q_int = H(int_coeffs)
    half_coeffs = [round(c - QQ(1)/2) + QQ(1)/2 for c in coeffs]
    q_half = H(half_coeffs)

    def norm2(q1, q2):
        c1 = list(vector(QQ, q1))
        c2 = list(vector(QQ, q2))
        return sum((c1[i] - c2[i])^2 for i in range(4))

    if norm2(q, q_int) <= norm2(q, q_half):
        return q_int
    else:
        return q_half



def division_hurwitz(a, b):
    q = b.inverse() * a
    q=nearest_hurwitz(q)
    r = a - b*q
    min_norme = r.reduced_norm()

    deltas_val = [QQ(-1)/2, QQ(0), QQ(1)/2]
    for deltas in product(deltas_val, repeat=4):
        coeffs_c = [q[j] + deltas[j] for j in range(4)]
        tot = 0
        for c in coeffs_c:
            tot += floor(2 * c)
        parite = tot % 2
        for idx in range(4):
            if floor(2 * coeffs_c[idx]) % 2 != parite:
                if parite == 1:
                    coeffs_c[idx] += QQ(1) / 2
                else:
                    coeffs_c[idx] += -QQ(1) / 2
        q_c = H(coeffs_c)
        r_c = a - b*q_c
        nr = r_c.reduced_norm()
        if nr < min_norme:
            min_norme = nr
            q = q_c
            r = r_c

    return q, r, r.reduced_norm()
```

```
def trouver_abcd(p):
    x,y=trouver_xy(p)
    print(x,y)
    alpha = H([1, x, y, 0])
    beta  = H([p, 0, 0, 0])
    d = pgcd(alpha, beta)
    print(d)
    a, b, c, d = tuple(d[j] for j in range(4))
    return a, b, c, d
```

Bibliography

[1] David A. Cox, *Primes of the form $x^2 + ny^2$*, Mathematics lecture notes, 2020, pp. 1–57.

[2] Michel Demazure, *Cours d'algèbre*, Cassini, Paris, France, 2009.

[3] Marc Hindry, *Arithmetics*, Algebra and diophantine equations, 2011, pp. 75–100.

[4] Julien Lavauzelle, *Algorithmes arithmétiques — notes de cours*, 2022.

[5] Daniel Perrin, *Cours d'algèbre (agrégation)*, Éditions Ellipses, Paris, France, 1998.

[6] Pierre Samuel, *Théorème des deux carrés*, Théorie algébrique des nombres, 2003, pp. 75–100.

[7] Shruthi Sridhar, *Modular forms and jacobi's four square theorem*, 2017.

Résumé

This report explores ring theory through the representation of a prime number p in quadratic forms: the two-square theorem, its related problems, and the four-square problem. Each equation is associated with a ring whose properties allow both the theoretical resolution of the theorem and its practical implementation to quickly find solutions.

Keywords

Prime number, Ring theory, Implementation, quadratic extension, Euclidean