Gaussian primes	Season	3
	Episode	04
	Time frame	2 periods

Prerequisites : Notions about Gaussian integers.

Objectives :
- Review the concept of prime numbers in the context of Gaussian integers.
- Check the prime decomposition property on a few examples and find ways to decide if a Gaussian integer is prime.

Materials :
- *Lesson about Gaussian primes and unique factorization.*
- *Beamer about Gaussian primes with the two main questions and the first problem to be solved, an empty lattice and the properties about Gaussian primes and unique factorization.*

1 – Lecture about Gaussian primes — 15 mins

The concept of Gaussian prime and the notions of conjugate and norm are introduced. Two questions are asked : What Gaussian integers are prime and, in particular, are all prime integers Gaussian primes ? Is it still possible to decompose uniquely any Gaussian integer into a product of Gaussian primes ?

2 – Working together to get a bigger picture — 40 mins

The class, working in teams, has to study all the Gaussian numbers with a and b between 0 and 10. When a team knows for sure if one number is prime, someone goes to the board to color the adequate point in red if it's prime, in black if it's composite. When all points are done, the teacher explains that if p is prime, $-p$, ip and $-ip$ are also prime.
An exercise sheet helps them find out the answers.

3 – How to recognize Gaussian primes — 30 mins

Students are still working in teams. They have to find a rule for a Gaussian integer to be prime, working first on real integers (other Gaussian primes 11, 19 and 23 are given), then other Gaussian integers $a + bi$.

4 – End of the lecture about Gaussian primes — 15 mins

The rule of primality is given, and the theorem about unique factorization.

Gaussian primes	Season	3
	Episode	04
	Document	Lesson

In this lesson, we study the concepts of divisibility and primality in the set $\mathbf{Z}[i]$ of Gaussian integers. As always, we say that a Gaussian integer e divides another one g if there exists a Gaussian integer f such that $g = e \times f$.
Any Gaussian integer is obviously divisible by 1, -1, i and $-i$, as $(-1) \times (-1) = 1$ and $i \times (-i) = 1$. We call these four special numbers the *units* of $\mathbf{Z}[i]$. Moreover, any Gaussian integer g is divisible by 1, -1, i, $-i$, g, $-g$, $-ig$ and ig. A *Gaussian* prime is a Gaussian integer that is not divisible by an integer different from these ones. An equivalent definition is given below.

Definition 1 Gaussian prime

A Gaussian integer g is not *prime* if it can be written as a non-trivial product $g = e \times f$, where neither e nor f are units.

To study primality in $\mathbf{Z}[i]$, two other concepts are useful, the conjugate of a Gaussian integer and its norm.

Definition 2 Conjugate

The *conjugate* of a Gaussian integer $g = a + bi$ is the Gaussian integer $\overline{g} = a - bi$.

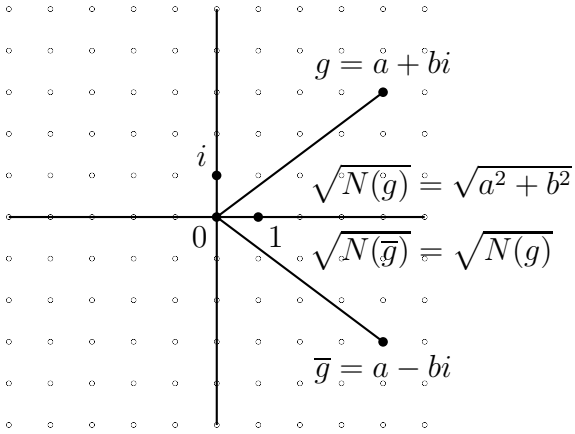
Definition 3 Norm

The product of a Gaussian integer $g = a + bi$ and its conjugate $\overline{g} = a - bi$ is a non-negative real number, as

$$g \times \overline{g} = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2.$$

This number is defined as the norm of g, noted $N(g)$.

Graphically, the conjugate is the symmetric of the point around the horizontal axis and the norm of a Gaussian integer g is the square of the distance between the points 0 and g. It's easy to see that this is also equal to the square of distance between 0 and $\overline{g}$, so $N(g) = N(\overline{g})$.



Theorem 1 Gaussian primes

A Gaussian integer $g = a + bi$ is prime if and only if
- one of a and b is zero and the other is a prime of the form $4n + 3$ or its negative $-(4n + 3)$;
- or both are nonzero and the norm of g, $N(g) = a^2 + b^2$ is prime.

Proof. We will just prove the first case, specifically when $b = 0$ and $a + bi = a \in \mathbf{Z}$. To do so, we will use two lemmas.
Lemma 1 If $a = 4n+1$, there exists two integers x and y such that $a = x^2+y^2 = (x+iy)(x-iy)$. This result is known as "Fermat's theorem on sums of two squares."

Lemma 2 No sum of integer squares can be written $4n + 3$.

It's obvious that a must be a prime integer, and that if $a = 4n$ or $4n + 2$ it is not prime, as it is divisible by 2. If $a = 4n + 1$, Fermat's theorem on sums of two squares assures us that there exists two integers x and y such that $a = x^2+y^2 = (x+iy)(x-iy)$, so a is composite. Therefore, if a is prime, it must be a prime integer of the form $4n + 3$.
We must now prove the reciprocal : if a is a prime integer of the form $4n+3$, then it's a Gaussian prime. Suppose that $g = a+0i$ for a prime integer $a = 4n+3$ and that it can be factored $g = hk$. Then $a^2 = N(g) = N(h)N(k)$. If the factorization is non-trivial, then $N(h) = N(k) = a$. But h is not an integer, so its norm is of the form $u^2 + v^2$. Then $u^2 + v^2 = a = 4n + 3$, which is in contradiction with lemma 2. So the factorization must have been trivial and g is a Gaussian prime.

Examples : The following Gaussian integers are prime : $1 + i$, $2 + i$, 3, $3 + 2i$, $4 + i$, $5 + 2i$, $7 + i$, $5 + 4i$, 7, $7 + 2i$, $6 + 5i$, $8 + 3i$, $8 + 5i$, $9 + 4i$.

Theorem 2 Unique factorization domain

The set $\mathbf{Z}[i]$ is a *unique factorization domain* : any Gaussian integer can be written as a product of Gaussian primes, and this decomposition is unique except for reordering or multiplication by units.

Gaussian primes	Season	3
	Episode	04
	Document	Exercises

4.1 Fill out the following multiplication table. In the upper right cells, you will put the products $g_1 g_2$, and in the lower left cells, the products $g_1 \overline{g_2}$. What can you say about the results in this table ?

g_2 \ g_1	$1+i$	$2+i$	$3+i$	$3+2i$	$4+i$
$1+i$					
$2+i$					
$3+i$					
$3+2i$					
$4+i$					

4.2 Let $a+bi$ and $c+di$ be two Gaussian integers and $x+yi$ their product.

1. Find a relation between x and a, b, c, d, and another between y and a, b, c, d.
2. Prove that there exist two Gaussian integers whose product is $x-yi$.
3. Prove that there exist two Gaussian integers whose product is $y+xi$.
4. Prove that there exist two Gaussian integers whose product is $y-xi$.
5. Deduce from that table in exercise 1 and the previous properties a list of other Gaussian integers that are not prime, by exhibiting in each case a non-trivial decomposition.

4.3 The aim of this exercise is to prove that 3 is a Gaussian prime. To do so, suppose that there exist two non-trivial Gaussian integers g_1 and g_2 such that $3 = g_1 g_2$. We will prove that one of these is a unit.

1. Let's start with a few general properties that will be useful later on.
   a. Prove that the only Gaussian integers $g = a+bi$ whose norm $N(g) = a^2+b^2$ is equal to 1 are the units.
   b. Prove that there are no Gaussian integer has a norm equal to 3.
   c. What can you say about $\overline{g}$ when g is an integer ?
   d. Prove that for any two Gaussian integers g and h, $\overline{gh} = \overline{g}\,\overline{h}$.
2. Prove that 3 is the product of two other Gaussian integers.
3. Deduce that $N(g_1)N(g_2) = 9$.
4. Knowing that $N(g_1)$ and $N(g_2)$ are positive integers, deduce the possible values for these two numbers.
5. Conclude.