Episode 04 – Gaussian primes
European section – Season 3
Definition (Units)

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 \(\mathbb{Z}[i]\).
### Definition (Units)

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 \(\mathbb{Z}[i]\).

### Definition (Gaussian prime)

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.

In other words, 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.
Definition (Conjugate)

The *conjugate* of a Gaussian integer $g = a + bi$ is $\bar{g} = a - bi$. 
Definition (Conjugate)

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

Example

The conjugate of $g = -3 + 4i$ is $\bar{g} = -3 - 4i$. 
**Conjugate and norm**

**Definition (Conjugate)**

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

**Example**

The conjugate of $g = -3 + 4i$ is $\bar{g} = -3 - 4i$.

**Definition**

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

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

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

Conjugate and norm

**Definition (Conjugate)**

The *conjugate* of a Gaussian integer \( g = a + bi \) is \( \bar{g} = a - bi \).

**Example**

The conjugate of \( g = -3 + 4i \) is \( \bar{g} = -3 - 4i \).

**Definition**

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

\[
g \times \bar{g} = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2.
\]

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

**Example**

The norm of \( g = -3 + 4i \) is \( N(g) = (-3)^2 + 4^2 = 25 \).
Conjugate and norm

\( g = a + bi \)
Conjugate and norm

\[ g = a + bi \]

\[ \bar{g} = a - bi \]
Conjugate and norm

\[ g = a + bi \]
\[ \bar{g} = a - bi \]
\[ \sqrt{N(g)} = \sqrt{a^2 + b^2} \]
Conjugate and norm

\[ g = a + bi \]

\[ \sqrt{N(g)} = \sqrt{a^2 + b^2} \]

\[ \sqrt{N(\bar{g})} = \sqrt{N(g)} \]

\[ \bar{g} = a - bi \]
Two important questions

Question 1
What Gaussian integers are prime and, in particular, are all prime integers Gaussian primes?
Two important questions

**Question 1**
What Gaussian integers are prime and, in particular, are all prime integers Gaussian primes?

**Question 2**
Is it still possible to decompose uniquely any Gaussian integer into a product of Gaussian primes?
Gaussian primes
Theorem

A Gaussian integer $g = a + bi$ is prime if and only if
Theorem

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 \(- (4n + 3)\);
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 the case when $b = 0$ and $a + bi = a \in \mathbb{Z}$. 
Proof.

We will just prove the first case, specifically the case when $b = 0$ and $a + bi = a \in \mathbb{Z}$. To do so, we will use two lemmas.
Proof.

We will just prove the first case, specifically the case when $b = 0$ and $a + bi = a \in \mathbb{Z}$. To do so, we will use two lemmas.

Lemma

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.”
Proof.

We will just prove the first case, specifically the case when $b = 0$ and $a + bi = a \in \mathbb{Z}$. To do so, we will use two lemmas.

**Lemma**

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**

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

We will just prove the first case, specifically the case when \( b = 0 \) and \( a + bi = a \in \mathbb{Z} \). To do so, we will use two lemmas.

Lemma

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

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.
Proof.
We will just prove the first case, specifically the case when \( b = 0 \) and \( a + bi = a \in \mathbb{Z} \). To do so, we will use two lemmas.

**Lemma**
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**
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.
Proof.
We will just prove the first case, specifically the case when $b = 0$ and $a + bi = a \in \mathbb{Z}$. To do so, we will use two lemmas.

Lemma

*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

*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 $4n + 3$. 

---

**Episode 04 – Gaussian primes**
Continued.

We must now prove the reciprocal: if \( a \) is a prime integer of the form \( 4n + 3 \), then it’s a Gaussian prime.
Continued.

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 $g = hk$. 
Continued.

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 $a^2 = N(g) = N(h)N(k)$. 
Continued.

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 $N(h) = N(k) = a$. 
Continued.

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 $u^2 + v^2$. 

Episode 04 – Gaussian primes
Continued.

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.
Continued.

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 of Gaussian primes

The following Gaussian integers are prime.

<table>
<thead>
<tr>
<th>1 + i</th>
<th>2 + i</th>
<th>3</th>
<th>3 + 2i</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 + i</td>
<td>5 + 2i</td>
<td>7 + i</td>
<td>5 + 4i</td>
</tr>
<tr>
<td>7</td>
<td>7 + 2i</td>
<td>6 + 5i</td>
<td>8 + 3i</td>
</tr>
<tr>
<td>6 + i</td>
<td>8 + 5i</td>
<td>9 + 4i</td>
<td></td>
</tr>
</tbody>
</table>
Gaussian primes on a lattice
The set $\mathbb{Z}[i]$ 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.