# Gaussian integers + sums of squares

Jacob Richey and Carl de Marcken

University of Washington 2nd year Math Circle

3/26/2020

# Imaginary numbers

Regular integers are boring! Let's spice things up, with a new number: $i$. It's defined by the equation

$$i^2 = -1.$$

Using $i$, we can form lots of new numbers by adding or multiplying. Some examples of imaginary numbers:

$$i + 1, i^3, \frac{6i - 4}{i - 1}$$

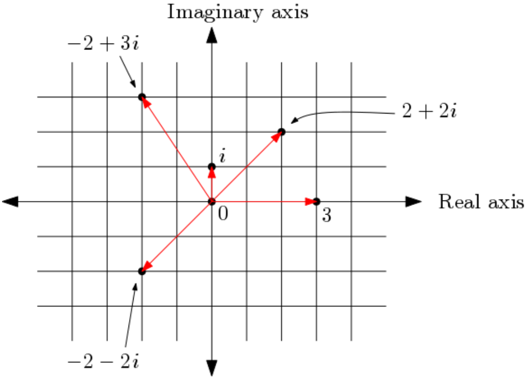
It turns out that all of these can be written in the form $a + bi$ for some real numbers $a, b$. For example, $i^3 = i^2 \cdot i = -1 \cdot i$, and

$$\frac{6i - 4}{i - 1} = \frac{6i - 4}{i - 1} \cdot \frac{i + 1}{i + 1} = \frac{6i^2 + 6i - 4i - 4}{i^2 - 1} = \frac{-10 + 2i}{-2} = 5 + i.$$

# Imaginary numbers

For today, we'll focus on imaginary numbers $a + bi$, where $a$ and $b$ are integers. $a$ is called the 'real part' and $b$ is called the 'imaginary part.'

The set $\{a + bi : a, b \text{ are integers}\}$ are known as the 'Gaussian integers.' Gaussian integers can be visualized as points in the plane:



# Imaginary numbers

Algebraically, multiplying Gaussian integers looks like this:

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i.$$

The 'norm' of a Gaussian integer is the square of it's length (as a vector):

$$N(a + bi) = a^2 + b^2.$$

When you multiply Gaussian integers, the norms also multiply:

$$N((a + bi)(c + di)) = N(a + bi) \cdot N(c + di)$$

# Imaginary numbers

**Question:** What properties of the integers do the Gaussian integers have?
Some properties of the 'normal' integers:

- No zero divisors (if $ab = 0$ then $a = 0$ or $b = 0$)
- Prime numbers exist (if $p|ab$ then $p|a$ or $p|b$)
- Unique factorization into primes ($n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$)
- Euclidean algorithm ($a = qb + r$ for some $q$ and $0 \leq r < b$)
- GCD algorithm ($\gcd(x, y) = ax + by$ for some integers $a, b$)

# Imaginary numbers

**Question:** What properties of the integers do the Gaussian integers have?
Some properties of the ‘normal’ integers:

- No zero divisors (if $ab = 0$ then $a = 0$ or $b = 0$)
- Prime numbers exist (if $p|ab$ then $p|a$ or $p|b$)
- Unique factorization into primes ($n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$)
- Euclidean algorithm ($a = qb + r$ for some $q$ and $0 \leq r < b$)
- GCD algorithm ($\gcd(x, y) = ax + by$ for some integers $a, b$)

It turns out that...

# Imaginary numbers

**Question:** What properties of the integers do the Gaussian integers have?
Some properties of the 'normal' integers:

- No zero divisors (if $ab = 0$ then $a = 0$ or $b = 0$)
- Prime numbers exist (if $p|ab$ then $p|a$ or $p|b$)
- Unique factorization into primes ($n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$)
- Euclidean algorithm ($a = qb + r$ for some $q$ and $0 \leq r < b$)
- GCD algorithm ($\gcd(x, y) = ax + by$ for some integers $a, b$)

It turns out that...

All of these things also work for the Gaussian integers!!!

# Gaussian primes

The property we will focus on today is unique factorization into primes. A Gaussian integer $z$ is called a G-prime (Gaussian prime) if

$$z = uw \implies N(u) = 1 \text{ or } N(w) = 1.$$

The integer prime 2 is *not* a G-prime, because $2 = (1-i)(1+i)$, and $N(1-i) = N(1+i) = 2$. (Note $N(2) = 4$.)

**Theorem**

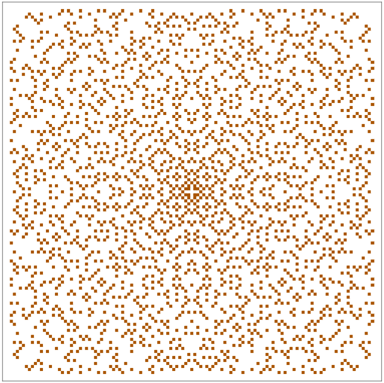
*Every Gaussian integer $z$ can be factored uniquely into a product of G-primes, up to reordering and multiplication by $-1, i$ and $-i$.*

For example, the Gaussian integer $1 + 7i$ has prime factorization

$$1 + 7i = i(1+i)(2-i)^2.$$

# Gaussian primes

A picture of all the G-primes $a + bi$ for $-60 \leq a, b \leq 60$:



# Sums of squares

**Theorem (Fermat's two square theorem)**

*If $p$ is a prime integer and $p \equiv 1 \bmod 4$, then $p = a^2 + b^2$ for some integers $a, b$.*

For example, $5 = 1^2 + 2^2, 13 = 2^2 + 3^2, 17 = 1^2 + 4^2, 29 = 2^2 + 5^2$. There is an easy converse:

**Fact (Converse)**

*If $p = a^2 + b^2$ for integers $a$ and $b$ and $p$ is odd, then $p \equiv 1 \bmod 4$.*

*Proof:* Since $0^2 \equiv 2^2 \equiv 0 \bmod 4$ and $1^2 \equiv 3^2 \equiv 1 \bmod 4$, the only possible sums of two squares mod 4 are $0, 1$ and $2$. The only odd sum is $1$. $\square$

# Sums of squares

To prove the two square theorem, we'll use the Gaussian integers and a couple of other ingredients:

**Theorem (Wilson's theorem)**

*If $p$ is prime, then $(p-1)! \equiv -1 \bmod p$.*

For example, $4! = 24 \equiv 4 \equiv -1 \bmod 5$.

We only need Wilson's theorem to prove:

**Lemma (Lagrange)**

*If $p$ is prime and $p \equiv 1 \bmod 4$, then there exists an integer $m$ such that $p | m^2 + 1$.*

For example, $13 | 5^2 + 1$.

# Sums of squares

**Theorem (Fermat's two square theorem)**

*If $p$ is a prime integer and $p \equiv 1 \mod 4$, then $p = a^2 + b^2$ for some integers $a, b$.*

*Proof:* Let $p \equiv 1 \mod 4$ be prime, and choose $m$ such that $p | m^2 + 1$ (by Lagrange's lemma). Note that

$$m^2 + 1 = (m + i)(m - i).$$

$p$ cannot divide either $m + i$ or $m - i$, because $\frac{m}{p} \pm \frac{1}{p} i$ isn't a Gaussian integer.

We found Gaussian integers $x$ and $y$ such that $p$ divides $xy$ but $p$ divides neither $x$ nor $y$. So $p$ isn't a Gaussian prime!

# Sums of squares

So, $p$ factors as a Gaussian integer, i.e. we can write

$$p = (a + bi)(c + di)$$

for some integers $a, b, c, d$, with neither factor equal to $p$. Now take the norm of both sides:

$$p^2 = N(p) = N(a + bi)N(c + di) = (a^2 + b^2)(c^2 + d^2).$$

Now all these numbers are integers again! As an integer, the unique factorization of $p^2$ is $p \cdot p$. Thus $a^2 + b^2 = p = c^2 + d^2$. $\square$

# Lagrange's four square theorem

Another interesting theorem involving sums of four squares:

**Theorem (Lagrange's four square theorem)**

*Every positive integer can be written as a sum of at most four squares.*

For example, $7 = 2^2 + 1^2 + 1^2, 15 = 3^2 + 2^2 + 1^2 + 1^2$, and $1729 = 40^2 + 11^2 + 2^2 + 2^2$.

The proof is similar to the one we just saw, but it uses the integer quaternions $a + bi + cj + dk$, or 'Hurwitz integers,' instead of the Gaussian integers.