Lecture 1, 28.10.

Lectures: Mon + Wed, 1:45 – 3:15 in 48 – 438

Course website: https://ulthiel.com/math/teaching-org/ant-19

↳ Lecture notes

Credits: 9 for oral exam.

Prerequesites: Algebra (groups, rings, ideals, factorial rings, field extensions, ...)

Exercise sessions: Tue, 8:15 – 9:45 in 48 – 438

↳ Exercise sheets on course website every Monday (starting today).

↳ Exercises are part of the course (and thus of the exam)

In general: Please ask questions!

1. What this is all about

Number theory: study of numbers like 1, 2, 3, ...

Is there anything to study?

Conjecture 1.1 (Goldbach, 1742)

„Every even integer greater than 2 is the sum of two primes."

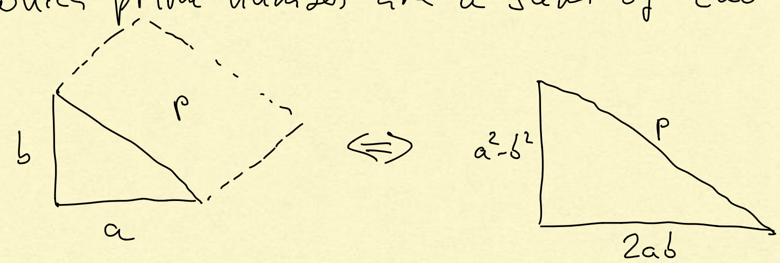
→ still unsolved!

→ there is a lot to study!

1.1. The sum of two squares problem

Question 1.2 (Diophantus, 200 BCE?)

Which prime numbers are a sum of two squares?



Such prime numbers are called pythagorean, e.g.

$$2 = 1+1, \quad 5 = 1+4, \quad 13 = 4+9, \ldots$$

Not every prime is pythagorean, e.g. $p=3$.

<u>Lemma 1.3</u> If $p>2$ is pythagorean, then $p \equiv 1 \mod 4$.

<u>Proof</u>: $x \in \mathbb{Z}/4\mathbb{Z} \Rightarrow x^2 \in \{0,1\}$. Hence, if $p = a^2+b^2$, then $p \in \{0,1,2\}$ in $\mathbb{Z}/4\mathbb{Z}$.
Last case cannot hapen: $p = 4k+2$ for $k \in \mathbb{Z} \Rightarrow p$ divisible by 2. $\square$

What is a sufficient condition? Answer lies in the <u>Gaussian integers</u>

$$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}, \quad i = \sqrt{-1}$$

Namely: if $p = a^2+b^2$, then $p = (a+bi)(a-bi) \rightsquigarrow$ factorization question in $\mathbb{Z}[i]$.

<u>Prop 1.4</u> $\mathbb{Z}[i]$ is euclidean.

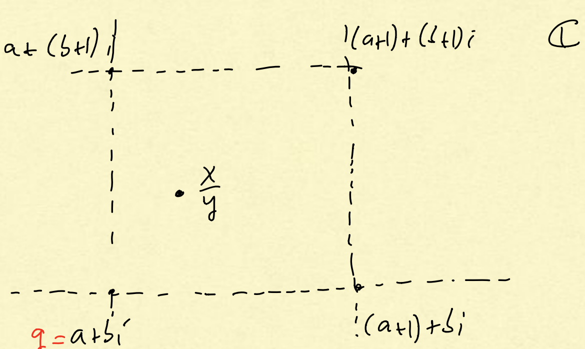
<u>Proof</u>: Let $N: \mathbb{Z}[i] \longrightarrow \mathbb{N}$, $x = a+bi \mapsto a^2+b^2 = |x|^2$, be the <u>norm</u> function.
We claim that for $x,y \in \mathbb{Z}[i]$, $y \neq 0$, there is $q,r \in \mathbb{Z}[i]$ with $x = qy+r$ and either $r=0$ or $N(r) < N(y)$.

Note:
- N extends in the same way to all of $\mathbb{C}$.
- N is multiplicative

Hence:

$$N(r) < N(y) \Leftrightarrow N\left(\frac{r}{y}\right) < 1 \Leftrightarrow N\left(\frac{x}{y} - q\right) < 1 \Leftrightarrow \left|\frac{x}{y} - q\right| < 1.$$

$\frac{x}{y}$ lies somewhere in the complex plane:



Diagonal of this square has length $\sqrt{2}$. Hence, can find $q \in \mathbb{Z}[i]$ with $\left|\frac{x}{y} - q\right| \leq \frac{\sqrt{2}}{2} < 1$. $\square$

So, $\mathbb{Z}[i]$ in particular a factorial ring, i.e. any element can be factored into prime element, factorization unique up to units.

Let's determine the units and the prime elements

Lemma 1.5 $x \in \mathbb{Z}[i]$ is a unit iff $N(x) = 1$. Hence

$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}.$$

Proof: Let $x = a+bi, y = c+di \in \mathbb{Z}[i]$. Then

$$1 = xy \iff 1 = N(1) = N(x)N(y) = \underbrace{(a^2+b^2)(c^2+d^2)}_{\text{product of natural numbers.}} \iff a^2+b^2 = \underline{1} \qquad \square$$

Can now answer the question:

Prop 1.6 The following are equivalent:

a) p is pythagorean.

b) p is not a prime anymore in $\mathbb{Z}[i]$

c) $p = 2$ or $p \equiv 1 \mod 4$.

Proof:

$a \Rightarrow c$: Lemma 1.3.

$c \Rightarrow b$: For $p = 2$ we have $2 = (1-i)(1+i)$, reducible $\Rightarrow$ not a prime.

For $p \equiv 1 \mod 4$ we'll use a general fact:

Wilson's theorem: $(p-1)! \equiv -1 \mod p$ for any prime p.

Proof: Any $x \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ has an inverse, and this is unique.

If $x = x^{-1}$, then $x^2 = 1$, so $0 = x^2 - 1 = (x+1)(x-1) \Rightarrow x = 1$ or $x = -1 = p-1$ in $\mathbb{F}_p$. Hence, in

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2)(p-1)$$

we can pair each factor $\neq 1, p-1$ with its unique and distinct inverse.

What remains is $(p-1)! = 1 \cdot (p-1) = -1$ in $\mathbb{F}_p$. $\square$

Back to $p \equiv 1 \bmod 4$, i.e. $p = 4n+1$. Mod p we have

$$-1 \equiv (p-1)! \equiv (4n)! \equiv 1 \cdot 2 \cdots (2n)(2n+1)(2n+2) \cdots (4n-1)(4n)$$

$$\equiv 1 \cdot 2 \cdots (2n)(p-2n)(p-2n+1) \cdots (p-2)(p-1)$$

$$\overset{\text{mod } p}{\equiv} (2n)! \cdot (-1)^{2n} (2n)! \equiv \left((2n)!\right)^2 \bmod p.$$

Hence, setting $c := (2n)! \Rightarrow p$ divides $c^2+1 = (c+i)(c-i)$ in $\mathbb{Z}[i]$.

But p does not divide any of the two factors: $p \cdot (a+bi) = c \pm i$

$\Rightarrow pa = c = (2n)!$ ↯ $\Rightarrow p$ is not a prime element in $\mathbb{Z}[i]$.

<u>$b \Rightarrow a$</u>: Suppose p is not a prime element in $\mathbb{Z}[i]$.

$\mathbb{Z}[i]$ is factorial $\Rightarrow p$ not irreducible $\Rightarrow p = xy$ with non-zero non-units $x, y \in \mathbb{Z}[i]$

$\Rightarrow \quad p^2 = N(p) = N(x)N(y)$

By Lemma 1.5 $\Rightarrow N(x), N(y) \neq 1 \Rightarrow p = N(x) = a^2+b^2$, $x = a+bi$

$\Rightarrow p$ is pythagorean

$\square$

<u>Remark 1.7</u> $p > 2$ pythagorean $\Leftrightarrow p \equiv 1 \bmod 4$ claimed by Girard (1625) and Euler (1640). First proof by Euler 1749 (complicated). Dedekind (1894) used $\mathbb{Z}[i]$.

<u>Corollary 1.8</u> Up to multiplication by units, prime elements π of $\mathbb{Z}[i]$ are:

a) $\pi = 1+i$

b) $\pi = a+bi$ for $a^2+b^2 = p$ prime > 2, $a > |b| > 0$ $(p \equiv 1 \bmod 4)$

c) $\pi = p$ for $p \equiv 3 \bmod 4$

Proof: π in a and b is prime since $N(\pi)$ is prime (and $\mathbb{Z}[i]$ factorial).
π in c is prime by Prop 1.6

Let $\pi \in \mathbb{Z}[i]$ be an arbitrary prime. Let $N(\pi) = p_1 \cdots p_r$ with prim numbers p_i.

$N(\pi) = \pi \cdot \overline{\pi}$ ← complex conjugate $\Rightarrow \pi$ divides $p_i =: p$ for some i.

$\Rightarrow N(\pi)$ divides $N(p) = p^2$. $\Rightarrow N(\pi) = p$ or $N(\pi) = p^2$.

If $N(\pi) = p \Rightarrow \pi = a + ib$ with $a^2 + b^2 = p \Rightarrow \pi$ is either case a or b.

If $N(\pi) = p^2 = N(p) \Rightarrow N\left(\frac{\pi}{p}\right) = 1 \Rightarrow \frac{\pi}{p}$ is a unit by Lemma 1.5 $\Rightarrow \pi$ is case c.

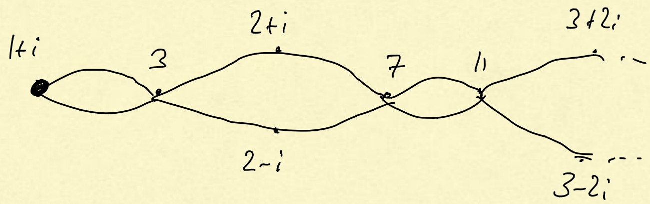
We must have $p \equiv 3 \bmod 4$ since otherwise not a prime by Prop 1.6.

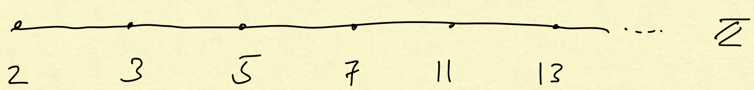
Corollary 1.9 A prime number $p \in \mathbb{Z}$ factorizes in $\mathbb{Z}[i]$ as follows:

a) If $p = 2$, then $p = -i(1+i)^2$

b) If $p \equiv 1 \bmod 4$, then $p = (a+ib)(a-ib)$

c) If $p \equiv 3 \bmod 4$, then p stays prime





1.2 Review

"Elementary" number theory problem $\Rightarrow$ splitting of primes in $\mathbb{Z}[i]$.
Had to establish properties of $\mathbb{Z}[i]$ (factorial, units).

Other number theory problems $\Rightarrow$ similar ring, e.g. $\mathbb{Z}[\sqrt{-5}]$, called rings of integers. Definition?

Algebraic number theory: Study of such rings

In general not factorial (e.g. $\mathbb{Z}[\sqrt{-5}]$) $\Rightarrow$ much more difficult, but also much more interesting!

↳ prime ideals instead of prime elements

↳ class group to analyze defect of being factorial

↳ units? (there can be infinitely many)

In addition to theory we will also discuss how to construct and compute these objects algorithmically (in principle)

↳ please do experiments with a computer! (PARI/GP, Sage, Magma, or just Python).

Remark 1.10 One can show there are infinitely many pythagorean primes. Special case of Dirichlets theorem on arithmetic progressions, proved using L-functions (generalized ζ-functions) $\Rightarrow$ analytic number theory