Lecture 1, 28.10.

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

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

Lecture notes

Credits: 9 for oral exam.

Prerequisites: 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 number are a sum of two squares?

Such prime numbers are called Pythagorean, e.g.

$p = 2 + 1, 5 = 1 + 4, 13 = 4 + 9,...$
Not every prime is pythagorean, e.g. $p = 3$.

**Lemma 1.3** If $p > 2$ is pythagorean, then $p \equiv 1 \pmod{4}$.

**Proof**: $x \in \mathbb{Z}/4\mathbb{Z} \Rightarrow x^2 \in \{0, 1, 2, 3\}$. Hence, if $p = a^2 + b^2$, then $p \in \{0, 1, 2\}$ in $\mathbb{Z}/4\mathbb{Z}$.

Last case cannot happen: $p = 4k + 2$ for $k \in \mathbb{Z} \Rightarrow p$ divides by $2$.

What is a sufficient condition? Answer lies in the Gaussian integers

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

Namely: if $p = a^2 + b^2$, then $p = (a + bi)(a - bi)$ no factorization question in $\mathbb{Z}[i]$.

**Prop 1.4** $\mathbb{Z}[i]$ is euclidean.

**Proof**: Let $N: \mathbb{Z}[i] \rightarrow \mathbb{N}$, $x = a + bi \rightarrow a^2 + b^2 = x^2$ be the norm function.

We claim that for $x, y \in \mathbb{Z}[i], \quad y \neq 0$, then is $q, r \in \mathbb{Z}[i]$ with $x = qy + r$

and either $r = 0$ or $N(r) < N(1)$.

**Note**:

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

Hence:

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

$x$ lies somewhere in the complex plane.

\[
\begin{array}{c}
\text{at (b+bi)} \\
\text{1 + (a+bi)} \\
\text{C} \\
\end{array}
\]

\[
\begin{array}{c}
\cdot \frac{x}{y} \\
\text{at (a+bi)} \\
\end{array}
\]

\[q = a + bi \\
(qx + bi)
\]

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 elements, 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 if $N(X) = 1$. Hence

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

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

$$1 = xy \iff 1 = N(1) = N(x)N(y) = (a^2 + b^2)(c^2 + d^2) \iff a^2 + b^2 = 1$$

Can now answer the question:

Prop 1.6. The following are equivalent:

a) $p$ is pythagorean
b) $p$ is not a prime anymore; $\mathbb{Z}[i]$
c) $p = 2$ or $p \equiv 1 \mod 4$.

Proof:

a $\Rightarrow$ c: Lemma 1.3.

b $\Rightarrow$ c: 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 $x \in \mathbb{Z}/p\mathbb{Z}$ 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 $x = -1 \neq p - 1$ in $\mathbb{F}_p$. Hence, $i\in\mathbb{F}_p$.

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

We can pair each factor $= 1$, $p - 1$ with its unique and distinct inverse. What remains is $(p-1)! = 1 \cdot (p-1) = -1$ in $\mathbb{F}_p$. □
Back to $p \equiv 1 \mod 4$, i.e. $p = 4n + 1$. Mod $p$ we have

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

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

$$\equiv (2n)! \cdot (-1)^{2n} (2n)! \equiv ((2n)!)^2 \mod p.$$ 

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

**b)** Suppose $p$ is not a prime element in $\mathbb{Z}[i]$.

$\mathbb{Z}[i]$ is Euclidean $\Rightarrow p$ not irreducible $\Rightarrow p = xy$ with non-zero non-units $x, y \in \mathbb{Z}[i]$ $\Rightarrow p^2 = N(p) = N(x)N(y)$.

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

\[\square\]

**Remark 1.7** $p \equiv 2$ pythagorean $\Leftrightarrow p \equiv 1 \mod 4$ claimed by Girard (1635) and Euler (1749). First proof by Euler 1749 (complicated).

Dedekind (1894) used $\mathbb{Z}[i]$.

**Corollary 1.8** Up to multiplication by units, prime elements $\pi$ of $\mathbb{Z}[i]$ are:

1. $\pi = 1 + i$
2. $\pi = a + bi$ for $a^2 + b^2 = p$ prime $> 2$, $a > |b| > 0$ ($p \equiv 1 \mod 4$)
3. $\pi = p$ for $p \equiv 3 \mod 4$
Proof: $\pi$ in $a$ and $b$ is prime since $N(\pi)$ is prime (and Z[i] factorial).

Let $\pi \in \mathbb{Z}[i]$ be an arbitrary prime. Let $N(\pi) = p, \ldots, p_r$ with prime number $p$.

$N(\pi) = \pi \cdot \frac{1}{\pi} \Rightarrow \pi \text{ divides } p_i := p$ for some $i$.

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

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

(ii) $N(\pi) = p^2 = M(\pi) \Rightarrow N(M(\pi)) = 1 = \frac{M(\pi)}{p}$. $\pi$ is a unit by Lemma 1.6 $\Rightarrow \pi$ is care.

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

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

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

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

c) If $p = 3 \mod 4$, 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, unit).

Other number theory problems $\Rightarrow$ similar rings, e.g. $\mathbb{Z}[\sqrt{-5}]$ called rings of integers. Definition?
Algebraic number theory: study of such rings
In general not factorial (e.g. $\mathbb{Z}[\sqrt{-3}]$) is much more difficult, but also much more interesting!

* By 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.

Specific case of Dirichlet's theorem on arithmetic progressions proved using $L$-functions (generalized $\zeta$-functions) = analytic number theory