ZAHLENTHEORIE SS 2019

Daniele Agostini
daniele.agostini@math.hu-berlin.de
Raum 1.429

Book: DANIEL MARCUS, "Number fields"
(there are two editions, both ok)

Time:

Mo	9-11	1.013	RUD 25
Mo	15-17	3.006	RUD 25
Mi	11-13	0311	RUD 26

Can be changed to Monday.

Office hours: Mo 11-13.

Exercises: one would need to present twice a solution in class.

Algebraic Number Theory: essentially, it is the study of integer/rational solutions of algebraic equations.

Example: 1) FERMAT'S EQUATION:

$$x^n + y^n = z^n$$

2) Another example comes now

§ 1. EXTENDED EXAMPLE: PRIMES THAT ARE SUMS of TWO SQUARES

We want to solve: $p = x^2 + y^2$ $\quad x, y \in \mathbb{Z}$, p prime

p	SUM OF SQUARES?
2	$1^2 + 1^2$
3	NO
5	$1^2 + 2^2$
7	NO
11	NO
13	$2^2 + 3^2$
17	$1^2 + 4^2$
19	NO

See any pattern?

1640 1750 1770 1800 1870

Thm [FERMAT, EULER, LAGRANGE, GAUSS, DIRICHLET 1990 ZAGIER, ...]

An odd prime p is a sum of two squares iff

$$p \equiv 1 \pmod 4.$$

We want to prove this theorem: first the easy part.

Lemma 1: If an odd prime p is a sum of two squares, then $p \equiv 1 \pmod 4$

proof: modulo 4 we have:

n	0	1	2	3
n^2	0	1	0	1

If $p = x^2+y^2$
since p is odd it must be that one of x, y is even and the other is odd. Hence $p \equiv 0+1 \equiv 1 \pmod 4$.

What about the other implication? The first observation is that $p = x^2+y^2$ can be rewritten (in $\mathbb{C}$) as

$$p = (x+iy)(x-iy)$$

This takes place naturally in the ring $\mathbb{Z}[i]$ (other than in the whole of $\mathbb{C}$. Then we could hope for something like this: Let p be a prime s.t. $p \equiv 1 \pmod 4$, then it turns out that p is <u>not irreducible</u> in $\mathbb{Z}[i]$, hence it can be written as $p = (a+ib)(c+id)$ for certain $a, b, c, d \in \mathbb{Z}$. However, taking conjugates, we also have the factorization

$$p = (a-ib)(c-id)$$

If there is some kind of <u>unique factorization</u> in $\mathbb{Z}[i]$ then it could follow that $c+id = a-ib$

and we will be happy.

In this strategy, it is the factorization inside $\mathbb{Z}[i]$ that plays the key role. We study it now:
We have

$$\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\} \subseteq \mathbb{Q}(i)$$

$\mathbb{Q}(i)$ is a Galois extension of $\mathbb{Q}$, with Galois group generated by the involution

$$\sigma : \mathbb{Q}(i) \to \mathbb{Q}(i)$$
$$i \longmapsto -i$$
$$z \longmapsto \overline{z}$$

def: NORM of $\mathbb{Z}[i]$

The norm is the map

$$N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}$$
$$z = a+ib \longmapsto z\cdot\sigma(z) = z\cdot\overline{z}$$
$$= a^2+b^2 = |z|^2$$

Lemma 2: The norm is multiplicative

$$N(\alpha\beta) = N(\alpha)N(\beta) \quad \forall \alpha,\beta \in \mathbb{Z}[i]$$

proof: Since σ is a ring homomorphism we have

$$N(\alpha\beta) = \alpha\beta\,\sigma(\alpha\beta) = \alpha\beta\,\sigma(\alpha)\sigma(\beta)$$
$$= \alpha\sigma(\alpha)\cdot\beta\sigma(\beta) = N(\alpha)N(\beta)$$

Otherwise, using the complex norm:

$$N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta). \quad \square$$

Cor 3: The units in $\mathbb{Z}[i]$ coincide with the elements of norm 1. These are

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

proof: Suppose $\alpha \in \mathbb{Z}[i]^*$. Then there is $\beta \in \mathbb{Z}[i]^*$ s.t. $\alpha\beta = 1$, hence $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. Since $N(\alpha), N(\beta)$ are both nonnegative, it must be that $N(\alpha) = N(\beta) = 1$. Conversely, if $N(\alpha) = 1$ then $\alpha \cdot \sigma(\alpha) = N(\alpha) = 1$, hence α is invertible.
To conclude, it is easy to show that the elements in $\mathbb{Z}[i]$ of norm 1 are precisely $1, i, -1, -i$. $\square$

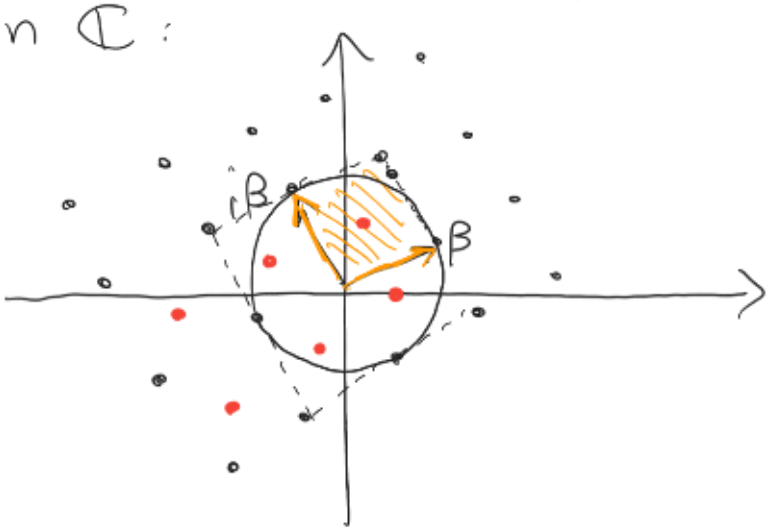
Using the norm, we can show that $\mathbb{Z}[i]$ is an EUCLIDEAN DOMAIN (like $\mathbb{Z}$ and $\mathbb{C}[X]$) and in particular it is a UFD.

Prop 4: Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Then There are $q, r \in \mathbb{Z}[i]$ s.t.

$$\alpha = q\cdot\beta + r \quad \text{with} \quad N(r) < N(\beta).$$

proof: Let's look at the multiples $q\beta$ of β: these

form the set $\{(a+ib)\beta \mid a,b\in\mathbb{Z}\}$.
$=\{a\beta+b\cdot(i\beta) \mid a,b\in\mathbb{Z}\}$. This is a lattice in $\mathbb{C}$:



It is clear that every point in $\mathbb{C}$ can be translated with the lattice to an element in the "fundamental square"

$$\{x\beta+y\,i\beta \mid x,y\in[0,1)\}$$

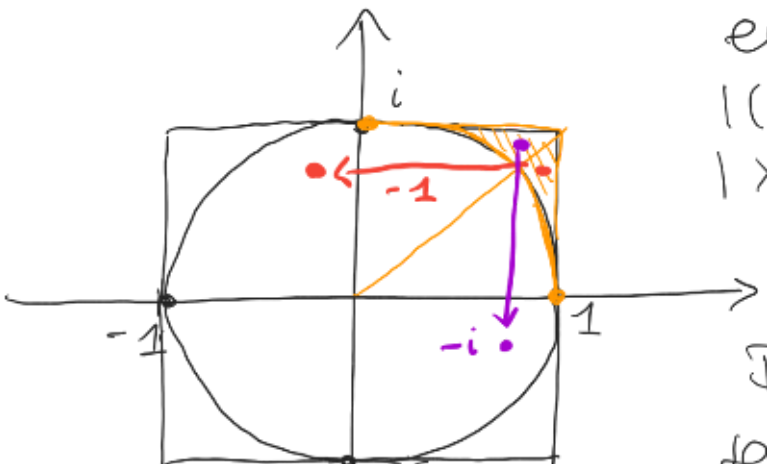
Hence we can write

$$\alpha=(a+ib)\beta+r \quad \text{with } r=x\beta+y\,i\beta$$

as above. Now we observe that

$$N(r)=|r|^2=|\beta|^2|x+iy|^2=N(\beta)|x+iy|^2$$

hence, if $|x+iy|^2<1$, then $N(r)<N(\beta)$ and we are happy. If instead $|x+iy|^2\geq 1$, then



either
$|(x-1)+iy|^2<1$
$|x+i(y-1)^2|<1$
holds.

Indeed, we see that

- $y \leq x$: $|(x-1)+iy|^2 =$
$= x^2 - 2x + 1 + y^2 \leq 2x(x-1) + 1 < 1$
$\Leftrightarrow 2x(x-1) < 0$ true!

- $x \leq y$: $|x + i(y-1)|^2 =$
$= x^2 + y^2 - 2y + 1 \leq 2y(y-1) + 1 < 1$
$\Leftarrow 2y(y-1) < 0$ true! □

This proves that $\mathbb{Z}[i]$ is an euclidean domain, and in particular a PID and an UFD. So with regard to factorization properties, it is as nice as possible!

Now let $p \equiv 1 \pmod 4$ be a prime.

Lemma 5: -1 is a square in $\mathbb{F}_p$. In other words, there is an $m \in \mathbb{Z}$ s.t. $-1 \equiv m^2 \pmod p$.

proof: the multiplicative group $\mathbb{F}_p^*$ is cyclic of order $p-1$, hence $-1 \equiv a^n \pmod p$ for a certain a. Since -1 has order two, we see

$2 = o(-1) = o(a^n) = \dfrac{o(a)}{\quad} = \dfrac{p-1}{\quad}$

$GCD(o(a), n)$ $GCD(p-1, n)$

Hence $2 \cdot GCD(p-1, n) = p-1$, and since $4 \mid p-1$, it must be that $2 \mid GCD(p-1, n)$, and in particular $n = 2k$ is even. Hence

$$-1 \equiv a^{2k} \equiv (a^k)^2 \pmod{p}$$ □

Rmk: The same proof shows that

(-1) is a square in $\mathbb{F}_p \iff p \equiv 1 \pmod 4$

We conclude with the proof of the theorem:

proof: since $p \equiv 1 \pmod 4$, there exists a $m \in \mathbb{Z}$ s.t. $m^2+1 \equiv 0 \pmod p$, hence

$$kp = m^2+1 \quad \text{for a certain } k \in \mathbb{Z}$$

Inside $\mathbb{Z}[i]$, we can rewrite this as

$$kp = (m+i)(m-i)$$

However $p \nmid (m+i)$ and $p \nmid m-i$, because if $(m+i) = p(a+ib)$, then $pb = 1$, which is absurd, and the same holds for $m-i$.

Hence p is not prime, and since $\mathbb{Z}[i]$ is an UFD it follows that it is not irreducible, so that we can write

$$p = \alpha \cdot \beta \quad \text{for } \alpha, \beta \in \mathbb{Z}[i] \text{ not invertible}$$

Now we take the norm on both sides and we get

get:

$$p^2 = N(\alpha)N(\beta)$$

Since α, β are not invertible, it must be $N(\alpha), N(\beta) \neq 1$ so that it must be $N(\alpha) = p$. But then, if $\alpha = a+ib$, this means that

$$p = (a+ib)(a-ib) = a^2+b^2. \qquad \square$$

This proves the theorem, but we can also say more about the number of decompositions:

Prop: A prime $p \equiv 1 \pmod 4$ can be written as a sum of squares in a unique way (up to reordering)

proof suppose $p = \alpha \cdot \bar{\alpha}$ for some $\alpha \in \mathbb{Z}[i]$ then we saw before that $N(\alpha) = p$. Then we claim that α is irreducible: indeed, if

$$\alpha = \beta \cdot \gamma$$

then $p = N(\alpha) = N(\beta)N(\gamma)$ so that $N(\beta)$ or $N(\gamma) = 1$ and this means that β or γ is invertible. Of course, then $\bar{\alpha} = \sigma(\alpha)$ is also irreducible.
Now suppose that we can write p as a sum of squares in two different ways: this means that

$$p = \alpha \cdot \bar{\alpha} = \beta \cdot \bar{\beta}$$

Then we know that $\alpha, \bar{\alpha}, \beta, \bar{\beta}$ are all irreducible, and since $\mathbb{Z}[i]$ is a UFD it must

be that α, β differ by a unit or $\alpha, \bar{\beta}$ differ by a unit. In any case, if we write $\alpha = a+ib$, $\beta = c+id$, it follows that

$$a^2 = c^2 \quad \text{or} \quad a^2 = d^2$$
$$b^2 = d^2 \qquad\quad b^2 = c^2.$$

□

Many ideas that appear in this example will be central trough out the whole course: we saw that to solve a problem over $\mathbb{Z}$ it is helpful to consider an extension $\mathbb{Z}[i]$ and for this extension it is helpful to study the factorization properties To study this, we have useful tools such as the norm and later the trace, and we can also employ geometric techniques, ...

These are the themes that we will explore in our course.