Math 538, Lecture 1, 10/1/2024

Introduction

Rough course plan:

(1) Intro/ Motivation
(2) Number fields, rings of integers,
unique factorization, primes ~
(3) Valuations & completions, local number fields
(4) Ramification, different, discriminant
(5) Geometry of numbers
(6) ? L-functions

Today: (1) Alg. NT?
(2) Review $\mathbb{Z}$
(3) Example: $x^2+y^2=p$ & $\mathbb{Z}[i]$
next time (4) $x^3+y^3=z^3$, ...

Def: Number theory studies integer solutions to polynomial equations

- Analytic NT counts solutions
- Algebraic NT studies individual ones

Compare equations: $p+q=x$ ← analysis
$x^2+y^2=p$ ← algebra
(more generally $x^2+y^2=n$)

Observations $(x^2+y^2)(z^2+w^2)=(xz-yw)^2+(xw+yz)^2$
(in $\mathbb{Z}[x,y,z,w]$) so study prime n first.

Prop: (Fermat) $p=x^2+y^2$ is solvable iff $p=2$
or $p\equiv 1\ (4)$

Cor: If $n=\prod_p p^{e_p}$ is a positive integer, and e_p is even when $p\equiv 3\ (4)$ then $x^2+y^2=n$ is solvable.

Thm: (Fermat) Converse holds

Observation: If x,y both even, both odd, $2 \mid x^2+y^2$
if x even, y odd, $x^2\equiv 0\ (4)$, $y^2\equiv 1\ (4)$
so $x^2+y^2\equiv 1\ (4)$.

Review of $\mathbb{Z}$

(1) $\mathbb{Z}$ is a ring.
(2) it's an integral domain
(3) it's a UFD ("fund thm of arithmetic")
(4) it's a Euclidean domain:

$$\text{If } a,b \in \mathbb{Z},\ b>0,\ \exists!\, q,r \in \mathbb{Z},\ 0 \le r < b \text{ s.t. } a = bq+r.$$

(5) $\mathbb{Z}^\times = \{\pm 1\}$

$\Rightarrow$ In $\mathbb{Z}$ $p \in \mathbb{Z}$ is irreducible ($p = xy \Rightarrow x$ or y in $\mathbb{Z}^\times$)
iff p is prime ($p \mid xy \Rightarrow p \mid x$ or $p \mid y$)

Back to $x^2+y^2=p$

let $\mathcal{O} = \mathbb{Z}[i]$, satisfies (1) $\to$ (4), $\mathcal{O}^\times = \{\pm 1, \pm i\}$
let $z \mapsto \bar{z}$ be the Galois automorphism of $\mathbb{Q}(i)$
Then

$$N z \overset{\text{def}}{:=} z\bar{z} \quad \text{is a multiplicative map } \mathcal{O} \to \mathcal{O}.$$

(identity from before: if $z = x+iy$, $Nz = x^2+y^2$)
See: $N: \mathcal{O} \to \mathbb{Z}$

(fact: if $a, b \in \mathcal{O}$, $b \neq 0$, $\exists q, r$ s.t. $a = bq + r$,
$Nr < Nb$.)

(if $z \in \mathcal{O}^\times$, say $zw = 1$, then $Nz\, Nw = N(zw) = 1$
so $Nz \in \mathbb{Z}^\times$, so $Nz = 1$)

Let p be a rational prime, $\pi \in \mathcal{O}$ a prime divisor of p. Then $N\pi \mid Np = p^2$

so $N\pi \in \{1, p, p^2\}$ (unique factorization in $\mathbb{Z}$)

$N\pi \neq 1$, since if $\pi\bar{\pi} = 1$, π is a unit.

If $N\pi = p^2$, $N(\frac{p}{\pi}) = \frac{Np}{N\pi} = \frac{p^2}{p^2} = 1$ so $\frac{p}{\pi} \in \mathcal{O}^\times$
so π is associate to p, p is prime in $\mathcal{O}$

If $N\pi = p$ then $\pi\bar{\pi} = p$ must be the prime factorization of p in $\mathcal{O}$. Then also
$p = x^2 + y^2$, where $\pi = x + iy$.

(1) If $p \equiv 3$ (4) then p is a prime of $\mathcal{O}$.
Pf (a) p is not a sum of two squares
Pf (2) map $\mathbb{F}_p[x] \to \mathcal{O}/p\mathcal{O}$ by $x \mapsto i + p\mathcal{O}$

factors through $\mathbb{F}_p[x]/(x^2+1)$ which is a field ($\mathbb{F}_{p^2}$)

since x^2+1 is irred in $\mathbb{F}_p[x]$, $\mathbb{F}_p^\times = C_{p-1}$

$p-1 \equiv 2\ (4)$

a root of x^2+1 has order 4, so no roots in $\mathbb{F}_p^\times$

As a $\mathbb{Z}$-module $\mathcal{O}/p\mathcal{O} \cong \mathbb{Z}^2/p\mathbb{Z}^2 \cong (\mathbb{Z}/p\mathbb{Z})^2$

so $\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_{p^2}$ and is a field, so p is prime

(2) If $p \equiv 1\ (4)$ then p is not prime in $\mathcal{O}$

Pf (a) The cyclic group $\mathbb{F}_p^\times = C_{p-1}$ has $4 \mid p-1$, so has solution to $a^2 \equiv -1\ (p)$. So $p \mid a^2+1 = (a+i)(a-i)$ but p divides neither so p isn't prime

Pf (2) images of $\pm a$, $\pm i$ in $\mathcal{O}/p\mathcal{O}$ all solve $z^2+1=0$

so $\mathcal{O}/p\mathcal{O}$ isn't a field, so p isn't prime

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

(if $p \equiv 1(4)$ $p = N(x+iy)$ then $x-iy$ not associate,

If $x+iy = i^a(x-iy)$ then either $x=0$
$y=0$
or $|x|=|y|$)

<u>Summary:</u> Fermat's thm on $x^2+y^2=p$
$\Leftrightarrow$
(1) Every prime p of $\mathbb{Z}$ is either
inert (still prime)
split ($p=\pi\bar{\pi}$ $\pi \not\sim \bar{\pi}$)
ramified ($p \sim \pi^2$)
in $\mathcal{O}=\mathbb{Z}[i]$

(2) Only finitely many ramified primes
(fact: $\frac{1}{2}$ primes split, $\frac{1}{2}$ inert)

(3) Covers all primes of $\mathbb{Z}[i]$: if π is prime, $\pi | N\pi$, so π divides some (rational) prime factor of $N\pi$.

Use unique factorization in $\mathcal{O}$ to solve $x^2+y^2=n$

<u>HW:</u> do the same for $n=x^2+xy+y^2$
using $\mathbb{Z}[\omega]$, $\omega=\frac{-1+\sqrt{3}i}{2}$.

Similarly study $x^2+y^2=z^2$ as

$$(x+iy)(x-iy)=z^2$$

Can assume x,y,z pairwise prime.
Then can't have $x \equiv 1\ (2)$ then $x^2+y^2 \equiv 2\ (4)$
So x,y of opposite parity $\Rightarrow z$ odd

Then $(x+iy,\ x-iy) = (x+iy,\ 2x)$
$(1+i) \nmid z^2 \Rightarrow 1+i \nmid x+iy$ so 2 prime to $x+iy$
so $(x+iy,\ x-iy,\ 2x) = (x+iy,\ \cancel{x}) = (y,x)=1$

So $x+iy$, $x-iy$ are squares in $\mathbb{Z}[i]$
(mod units)

$$\Rightarrow \exists\, m,n \text{ s.t. } x+iy = i^a(m+in)^2$$

$\Rightarrow$ up to signs, switching x,y,

$$x=m^2-n^2,\quad y=2mn,\quad z=m^2+n^2$$

Next, let's study $x^p-y^p=z^p$ $\quad p\geq 3$ prime

Again take x,y,z to be a primitive solution
Write: $\quad x^p-y^p=\prod_{j=0}^{p-1}(x-\zeta_p^j y) \quad \zeta_p$ root of $\zeta_p^p=1$