number theory viewed as (1) study of primes

(2) study of Diophantine problems

(involving Diophantine equations: polynomial eqns with integer coefficients)

Example (Fermat): Which primes can be written as sum of two squares? $p : p = x^2 + y^2,\ x, y \in \mathbb{Z}$

Any immediate obstructions? congruence conditions? $x^2 \equiv 0, 1 \ (4)$ for any x

so $x^2 + y^2 \equiv 0, 1, 2 \ (4)$

So no primes $p \equiv 3 \ (4)$ are sums of squares.

Now left to answer: which primes $p \equiv 1 \ (4)$? (noting $1 + 1 = 2$)

are sum of squares

Strategy: Work in larger ring than $\mathbb{Z}$ where arithmetic of problem is easier, but can still draw conclusions about original Q. over integers.

$x^2 + y^2 = (x + iy)(x - iy)$ so consider algebraic number field

$\mathbb{Q}(i)/\mathbb{Q}$ - two dim'l (Galois) extn. - $\{ a + bi \mid a, b \in \mathbb{Q} \}$

with subring $\mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \}$ "Gaussian integers"

Claim: If we understand this ring $\mathbb{Z}[i]$ well enough, we can solve this Diophantine problem.

More precisely, we wish to describe how rational primes decompose into "primes" in $\mathbb{Z}[i]$. For example, in $\mathbb{Z}[i]$,

$5 = (2 + i)(2 - i)$ but 7 remains prime.

so not prime in $\mathbb{Z}[i]$.

(check small values of $a + bi$ in potential factorization.

So "algebraic number theory" for us will be an investigation of algebraic number fields (and their subrings), ultimately trying to answer ~~where~~ how a prime decomposes in a finite extension.

This is a two semester course: Semester 1: Answer for abelian (Galois) extensions of $\mathbb{Q}$.

(Class Field Theory)

Many open questions remain, but broader questions resolved in first 1/2 of 20th century.

Semester 2: Answer for non-abelian extensions.

(L-functions, Langlands program)

Only very limited set of partial results. Formulated in late 60's

Also: algebraic number fields are modern language for most all questions in number theory and modern setting

Rough principle: treat number fields just like rationals, when we use right terminology / constructions.

At Minnesota: few people working on finer structure questions about algebraic number theory. More focused on questions related to "Semester 2" topics. - Adrian Dracone, Kai-Wen Lan, Paul Garrett, Dihua Jiang, Me.

This semester's plan: (1) Classic introduction to number theory
algebraic exploration of rings of integers and their invariants

(2) Introduce topology and analysis to study # fields. (p-adic fields)

(3) Explain why (2) is better than (1) and connect to geometry.

(4) Statements of "local CFT" and "global CFT"

Returning to our question about primes of form x^2+y^2, there are 3 steps:

(1) Show $\mathbb{Z}[i]$ is a unique factorization domain – we'll have general setup to this later

(2) Prove $p \equiv 1 \ (4) \Rightarrow$ p not prime in $\mathbb{Z}[i]$ * = main step

(3) Prove p not prime in $\mathbb{Z}[i] \Rightarrow p = a^2+b^2$ for some $a, b \in \mathbb{Z}$

Proof of Step 3: Define norm map $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ by

$N(\alpha) = \alpha \cdot \bar{\alpha}$ ← cx. conjugation.

This is multiplicative $N(\alpha\beta) = N(\alpha)N(\beta)$,

and if $\alpha = a+bi$, $N(\alpha) = a^2+b^2$. And $\alpha \in \mathbb{Z}[i]$ is a unit iff $N(\alpha)=1$.

(i.e. invertible elt.)

If p not prime in $\mathbb{Z}[i]$, then $p = \alpha \cdot \beta$

with α, β non-units (via step 1)

Taking norms of both sides $p^2 = N(\alpha) \cdot N(\beta)$.

$\Rightarrow$ $p = N(\alpha) = N(\beta)$ so $p = a^2+b^2$ with $\alpha = a+bi$.

Proof of Step 2: If $p \equiv 1 \ (4)$, then $\mathbb{F}_p^\times$ is cyclic subgp. with

$p-1 = 4k$, some k, elts

so has elt. of order 4,

call it m, with $m^2 \equiv -1 \pmod p$, since -1 is uniq. elt. of order 2.

So $p \mid m^2+1 = (m+i)(m-i)$. If p prime, then either

$p \mid m+i$ or $m-i$ (and hence the other by taking cx. conjugates)

$\Rightarrow p \mid (m+i)-(m-i) = 2i$ ↯.

* Neukirch says take $m = (2k)!$ and use Wilson's thm $-1 \equiv (p-1)! \ (p)$

Finally to prove step 1, show $\mathbb{Z}[i]$ is Euclidean domain, which

implies $\mathbb{Z}[i]$ is a unique factorization domain ("factorial" in Neukirch)

Recall that a Euclidean domain is a domain with Euclidean algorithm.

That is, $\exists$ norm function N on domain $\Theta \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$

s.t.

(i) $N(b) \leq N(ab) \quad \forall\ a, b \in \Theta \setminus \{0\}$

(ii) $a = qb + r$ for some $q, r \in \Theta$, with $N(r) < N(b)$ or $r = 0$.

For any $a, b \in \Theta \setminus \{0\}$,

Using $N(\alpha) := \alpha \cdot \bar{\alpha}$ on $\mathbb{Z}[i]$, then (i) is clear from multiplicativity and fact that $N(\alpha) = 0 \Rightarrow \alpha = 0$.

(ii) follows b/c $\mathbb{Z}[i]$ is square lattice in $\mathbb{C}$.

We must show $\exists\ q \in \mathbb{Z}[i]$ s.t. $\left| \frac{a}{b} - q \right| < 1$ (since $N(\alpha) = |\alpha|^2$)

But $\frac{a}{b} \in \mathbb{C}$ is always at most $\frac{\sqrt{2}}{2}$ from lattice point (i.e. < 1)

Finally recall that Euclidean domains are UFDs. (converse is false)

This is immediate from the existence of norm function.

[Given ideal $\mathfrak{a}$, pick elt. $a \in \mathfrak{a}$ of minimal norm. This must be generator. Else $\exists$ b with $b = q \cdot a + r$ with $0 < N(r) < N(\mathfrak{a})$ contradicting the minimality of a. so Θ is a P.I.D.

But P.I.Ds are U.F.D.s:

show that P.I.D.s satisfy (A) divisor chain condition (no infinite sequence of proper divisibility of elts)

$\Rightarrow$ factorization exists

(B) every irreducible (no proper factors) is prime ($p \mid ab \Rightarrow p \mid a$ or $p \mid b$)

$\Rightarrow$ factorization unique

(A) follows b/c given $(a_1) \subsetneq (a_2) \subsetneq \cdots$ then $\bigcup_i (a_i)$ is ideal (d) so $d \in (a_n)$ for some n

so $(a_m) \supset (a_n) \supset d \supset (a_m) \quad \forall\ m \geq n$. chain stabilizes!