Algebraic number theory (ANT)

§1 Introduction & Basics

Q1: What is ANT?

A1: The study of $\underbrace{\text{algebraic number fields}}_{\text{field extensions } K/\mathbb{Q} \text{ of finite degree}}$

Example 1.1 i) $K = \mathbb{Q}(i) \ni a+bi \quad a,b \in \mathbb{Q}$

degree $\rightarrow [K:\mathbb{Q}] = \dim_{\mathbb{Q}} K = 2.$

$a,b \in \mathbb{Z}$

$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$, $a+bi \in \mathbb{Z}[i]$

$$\begin{array}{ccc} \mathbb{Q} & \subset & K \\ \cup & & \cup \\ \mathbb{Z} & \subset & \mathcal{O}_K \end{array}$$

$\alpha \in K \quad c_i \in \mathbb{Z}$

$\ni \alpha \iff \alpha^n + c_{n-1}\alpha^{n-1} + \dots + c_0 = 0$

$\mathcal{O}_K \leftarrow$ ring of integers of K

$\mathbb{Z} \subset \mathcal{O}_K$: integral closure

Units?

$6 = 2\cdot 3$ unique (UFD) factorization $\rightsquigarrow$ Not always $\rightsquigarrow$ ideals (Kummer/Dedekind)

p prime $\rightsquigarrow$?

ii) $K = \mathbb{Q}(\sqrt{5})$

$\mathcal{O}_K = \mathbb{Z}\left[\frac{\sqrt{5}+1}{2}\right]$

iii) $K = \mathbb{Q}(\sqrt{-5})$ not UFD

$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

irreducible

Q2: Why is ANT?

A2: Alg. number fields appear naturally when studying $\underbrace{\text{Diophantine equations}}$

polynomial equations where one is interested in integer/rational solutions

Examples 1.2 (See [IR] Chapter 17 for details)
(KKT) Chapter 1

i) Linear Diophantine equation: Given $a, b, c \in \mathbb{Z}$, find $x, y \in \mathbb{Z}$ with $ax + by = c$.

Check: Has a solution iff c is a multiple of $\gcd(a, b)$.

ii) Pell's equation: Given nonsquare integer n:

$$x^2 - ny^2 = 1$$

Lagrange (1768): For any nonsquare n this has infinitely many distinct sol's $x, y \in \mathbb{Z}$.

iii) Sum of four squares: For $n \in \mathbb{N}$ find $a, b, c, d \in \mathbb{Z}$ with

$$a^2 + b^2 + c^2 + d^2 = n \qquad (\star)$$

Lagrange (1770): (★) Has a solution for any n.

$$2021 = 0^2 + 1^2 + 16^2 + 42^2 = 1^2 + 18^2 + 20^2 + 36^2 = \dots$$

How many?

Jacobi (1834): If $r_4(n) = \#\{(a,b,c,d) \in \mathbb{Z}^4 \mid ★\}$

then $$r_4(n) = 8 \sum_{\substack{m \mid n \\ 4 \nmid m}} m$$

$m \mid n$ — m divides n but m is not divisible by 4

($\rightsquigarrow$ Easy to prove by using modular forms for $\Gamma_0(4)$.)

iv) Sum of two squares: $a^2 + b^2 = n$

Does not always have a solution (e.g. $n=3$)

$\rightsquigarrow$ Section 1.1

v) Fermat's last theorem (FLT):

For given $n \geq 1$ consider

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

$n=1$: trivial

$n=2$: Pythagoran triples

$3^2 + 4^2 = 5^2$

$5^2 + 12^2 = 13^2$

$\dots$ (HW1)

Fermats claim: For $n \geq 3$ there are no non-trivial solutions. (i.e. $x \cdot y \cdot z = 0$)

ANT- Timetable

Pythagoras 500 BC

250	1637	17XX	1847	Ernst Kummer	1863	1897	1994
Diophantus of Alexandria	Pierre de Fermat	Sophie Germain	Gabriel Lamé	"ideal numbers"	Richard Dedekind	David Hilbert	Andrew Wiles
	$x^n+y^n=z^n$	FLT	(wrong) proof		$\mathcal{O}_K$ & ideals	Zahlbericht	FLT for all n!
	no trivial sol: $n=3,4$	$p<100$		FLT for regular primes			

modern ANT

1.1 Primes as sum of two squares & some ring theory

$2=1^2+1^2$, $3=$ not possible $\times$, $5=1^2+2^2$, $7=\times$, $11=\times$, $13=2^2+3^2$
$17=1^2+4^2$, $19=\times$, $23=\times$, $29=2^2+5^2$

<u>Fact</u>: Any square is congruent to 0 or 1 modulo 4,

since $(2m)^2 = 4m^2 \equiv 0 \mod 4$

$(2m+1)^2 = 4m^2+4m+1 \equiv 1 \mod 4$

Theorem 1.3 (Fermat) "$\Rightarrow$"

If $p \geq 3$ is a prime then

$$p = a^2+b^2 \quad \Longleftrightarrow \quad p \equiv 1 \mod 4$$
$$\exists a,b \in \mathbb{Z}$$

To prove this we will leave the ring of integers and go into a larger ring.

Definition 1.4

i) A <u>ring</u> $(R,+,\cdot)$ is a set R together with two binary operations $+$ (addition) and $\cdot$ (mult.), such that

- $(R,+)$ is an abelian group
  ($\exists\, 0 \in R$, $+$ associative, $\exists$ inverses $-a$, $a+b=b+a$)
- $(R,\cdot)$ is a semigroup
  ($\cdot$ associative)
- Distributive property
  $$a\cdot(b+c) = a\cdot b + a\cdot c$$
  $$(a+b)\cdot c = a\cdot c + b\cdot c$$

If "$\cdot$" is commutative we call R <u>commutative</u>.

Instead of $(R,+,\cdot)$ we just write R if "$+$" and "$\cdot$" are clear from context.

ii) A ring R is <u>unitary</u> if there exists a $1 \in R$ with $1\cdot a = a\cdot 1 = a$ $\forall a \in R$
(i.e. $(R,\cdot)$ is a monoid)

iii) A <u>ring homomorphism</u> is a map $\varphi: R \to S$ between two ring R, S, such that

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

If R, S are unitary one usually considers unitary ring homomorphism, which satisfy $\varphi(1) = 1$.

iv) A (non-zero) commutative ring R is called an <u>integral domain</u> if for all $a, b \in R$ $a \cdot b = 0$ implies $a = 0$ or $b = 0$. (often just "domain")

[The rings we consider in this course are commutative and unitary. (if not stated otherwise)]

<u>Examples 1.5</u>

i) $\mathbb{Z}$, $\mathbb{Z}[X]$, $\mathbb{R}$, $\mathbb{C}$, .. are integral domains

ii) $\mathbb{Z}/6\mathbb{Z}$ is not a domain, since $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$

iii) The ring of <u>Gaussian integers</u>
$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$
is a domain.

In $\mathbb{Z}[i]$ we can write $p = x^2 + y^2$ as $(x, y \in \mathbb{Z})$
$$p = (x + iy)(x - iy).$$

To prove Thm 1.1 we therefore want to understand when a prime p can be factored like this in $\mathbb{Z}[i]$.

In $\mathbb{Z}$ we can factor numbers (almost) uniquely into primes.

$$6 = 2 \cdot 3 = (-2)(-3)$$

up to units

Definition 1.6 i) An element $a \in R$ in an (unital) ring R is called a <u>unit</u> if there exists a $b \in R$ with $ab = 1$.

ii) The sets of units of a ring R is denoted $R^\times$.

Check: $(R^\times, \cdot)$ is a group.

iii) If $R^\times = R \setminus \{0\}$ and R is commutative then R is called a <u>field</u>.

(たい 体 german: Körper (body))

Examples 1.7

i) $\mathbb{Z}^\times = \{1, -1\}$.

ii) If R is a domain then $R[X]^\times = R^\times$.

iii) $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$ (HW1)

(if R is not a domain then there might be more units.

e.g $R = \mathbb{Z}/4\mathbb{Z}$ $\underset{\text{unit}}{(1+2X)^2} = 1$)

Definition 1.8

i) An element $a \in R$ with $a \notin R^\times$ is called <u>irreducible</u> if from $a = b \cdot c$ with $b, c \in R$ we obtain $b \in R^\times$ or $c \in R^\times$.

ii) An element $p \in R \setminus \{0\}$ with $p \notin R^\times$ is called <u>prime</u> and whenever $p \mid a \cdot b$ then $p \mid a$ or $p \mid b$.

$(\exists c : p \cdot c = a \cdot b)$

HW1: In an domain every prime element is irreducible.

The converse is not always true:

$R = \mathbb{Z}[\sqrt{-5}]$ is a domain.

2 is irreducible in R and

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

but $2 \nmid (1 + \sqrt{-5})$ and $2 \nmid (1 - \sqrt{-5})$.

does not divide

$\Rightarrow$ 2 is not prime.