Algebraic number theory

1. Introduction

Basic problem: given $F \in \mathbb{Z}[X_1, \dots, X_n]$, find $x_1, \dots, x_n \in \mathbb{Z}$ s.t. $F(x_1, \dots, x_n) = 0$.

Equations of this form $F(X_1 \dots X_n) = 0$ are called Diophantine equations

Examples 1) Fermat's problem: for $n \geq 3$ ~~$\exists$~~ non-trivial integral solutions to

$$X^n + Y^n = Z^n,$$

i.e. if $(x, y, z) \in \mathbb{Z}^3$ is a solution, then $xyz = 0$.

Solved by Andrew Wiles (1995)

2) Sums of squares (Euler?). Let p be an odd prime. Can we find $x, y \in \mathbb{Z}$ s.t. $p = x^2 + y^2$?

In this example $F = X^2 + Y^2 - p$

Answer: it is possible iff $p \equiv 1 \pmod 4$

Also possible for $p = 2$.

3) Pell's equation: let $d>1$ be a square-free integer (i.e. not divisible by p^2 $\forall$ prime p). Consider

$$X^2 - dY^2 = 1$$

This equation has ∞ solutions.

2. Sums of squares

Fix odd prime p. Consider

$$X^2 + Y^2 = p \qquad (*)$$

Rewrite: $(X+iY)(X-iY) = p \qquad i^2 = -1$

$x+iy = z$, then $x^2+y^2 = p \Leftrightarrow z \cdot \bar{z} = p$

Def The ring of Gaussian integers

$$\mathbb{Z}[i] = \{x+iy \in \mathbb{C} \mid x, y \in \mathbb{Z}\}$$

Remark "Ring" will always mean a commutative ring with identity.

Solving $(*) \Leftrightarrow$ finding $z \in \mathbb{Z}[i]$, s.t. $z \cdot \bar{z} = p$

Def A ring R is

1) an integral domain, if $\forall a, b \in R$

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$

2) a Euclidean domain, if it is integral s.t. $\exists$ a map $N: R \longrightarrow \mathbb{Z}_{\geq 0}$ with

a) $N(0) = 0$

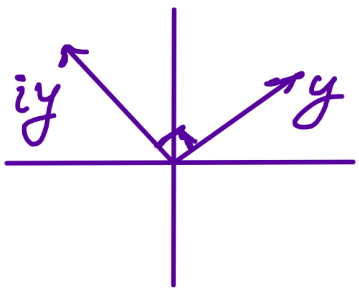
b) $\forall x, y \in R, y \neq 0 \quad \exists a, b \in R$ s.t.
$x = ay + b$ and $N(b) < N(y)$
or $b = 0$

This means: we can divide x by y with "remainder" b.

Example $R = K[x]$ K = a field
R is Euclidean dom. with $N(f) = \deg(f)$ for $f \in K[x]$

Proposition 2.1 $\mathbb{Z}[i]$ is a Euclidean domain.

Proof $\mathbb{Z}[i]$ integral, because it is a subring of $\mathbb{C}$. Define $N(z) = z \cdot \bar{z} = |z|^2$
Let $x, y \in \mathbb{Z}[i]$, $y \neq 0$
Need: $x = ay + b$, $N(b) < N(y)$
y and iy are linear indep./$\mathbb{R}$ vectors in $\mathbb{R}^2 \cong \mathbb{C}$



Elements of the form ay, with $a \in \mathbb{Z}[i]$ form a lattice

$$\mathbb{Z}\cdot y \oplus i\mathbb{Z}y$$

$x = \alpha y + \beta i y, \quad \alpha, \beta \in \mathbb{R}$

Let $\alpha = \alpha_0 + \alpha_1, \quad \alpha_0 \in \mathbb{Z}, -\frac{1}{2} \le \alpha_1 < \frac{1}{2}$

$\beta = \beta_0 + \beta_1, \quad \beta_0 \in \mathbb{Z}, -\frac{1}{2} \le \beta_1 < \frac{1}{2}$

$$x = \underbrace{(\alpha_0 + i\beta_0)}_{a}\cdot y + \underbrace{(\alpha_1 + i\beta_1)y}_{b}$$

$b = x - a\cdot y \in \mathbb{Z}[i]$

$N(b) = |\alpha_1 + i\beta_1|^2 \cdot N(y) =$

$= (\alpha_1^2 + \beta_1^2)\cdot N(y) \le \left(\frac{1}{4} + \frac{1}{4}\right)\cdot N(y)$

$= \frac{1}{2} N(y) < N(y)$. □

Recall: 1) an int. domain R is called principal ideal domain (PID) if any ideal in R is generated by one element.

2) Prop. 2.2 R Euclidean domain $\Rightarrow$ R PID

Idea of proof: $I \subset R$ ideal.

Pick $0 \neq x \in I$ s.t.

$\forall 0 \neq y \in I \quad N(x) \leq N(y)$

Then check that $I = (x)$ $\square$

3) an element $x \in R$ is a unit, if $\exists y \in R$ s.t. $xy = 1$. Set of all units denoted by $R^\times$

4) Let $x \in R$ s.t. $x \neq 0$, $x \notin R^\times$

x is called irreducible if $x = ab$, $a, b \in R$

$\Rightarrow$ either $a \in R^\times$ or $b \in R^\times$

otherwise x is called reducible

5) An int. domain R is called unique factorization domain, if $\forall 0 \neq x \in R$ s.t. $x \notin R^\times$ $\exists$ a decomposition

$x = p_1 \cdot \ldots \cdot p_n$ with p_i are irred.

and if $x = q_1 \cdot \ldots \cdot q_m$ another decomposition with q_j irred, then $n = m$ and after permuting q_j we have $p_i = a_i q_i$ for some $a_i \in R^\times$

6) <u>Prop 2.3</u> R is PID $\Rightarrow$ R is UFD

Corollary: $\mathbb{Z}[i]$ is UFD and PID

7) Prop 2.4 Assume that R is UFD

Then $0 \neq x \in R$ is irreducible

$\Leftrightarrow$ (x) is prime, i.e. $R/(x)$ is integral.

Prop 2.5 $z \in \mathbb{Z}[i]^\times \Leftrightarrow N(z)=1$

$\Leftrightarrow z \in \{\pm 1, \pm i\}$

Proof: $z \in \mathbb{Z}[i]^\times \Rightarrow \exists\, w$ s.t. $zw=1$

$\Rightarrow N(z)\cdot N(w)=1 \Rightarrow N(z)\cdot N(w)=1$

$\Rightarrow z \in \{\pm 1, \pm i\}$ □

Back to the equation

$$X^2+Y^2=p \qquad (*)$$

p = odd prime

Prop. 2.6 $(*)$ has an integral solution iff p is reducible as an element of $\mathbb{Z}[i]$.

Proof: 1) $(*)$ solvable $\Rightarrow \exists\, z \in \mathbb{Z}[i]$ s.t. $z\cdot\bar{z}=p$. But $N(z)=N(\bar{z})=p>1$, so neither z nor $\bar{z}$ is a unit

$\Rightarrow p$ is reducible.

2) Assume p is reducible

$\Rightarrow \exists\, z, w \in \mathbb{Z}[i]$, $N(z) > 1$, $N(w) > 1$

$p = z \cdot w$

$N(p) = p^2 = N(z) \cdot N(w)$

$\Rightarrow N(z) = N(w) = p$

$\Rightarrow p = z \cdot \bar{z}$ $\Rightarrow$ (*) is soluable $\square$

<u>Thm 2.7</u> An odd prime p can be represented as the sum of two squares iff $p \equiv 1 \pmod 4$

<u>Proof:</u> (*) is soluable $\overset{\text{Prop. 2.6}}{\Longleftrightarrow}$ p is reducible in $\mathbb{Z}[i]$

$\overset{\text{Prop 2.4}}{\Longleftrightarrow}$ (p) is not a prime ideal in $\mathbb{Z}[i]$.

$\Longleftrightarrow \mathbb{Z}[i]/(p)$ has zero-divisors.

Note: $\mathbb{Z}[i] = \dfrac{\mathbb{Z}[x]}{(x^2+1)}$

$$\frac{\mathbb{Z}[i]}{(p)} \simeq \frac{\mathbb{Z}[x]}{(x^2+1,\, p)} \simeq \frac{\mathbb{Z}/(p)[x]}{(x^2+1)} = \frac{\mathbb{F}_p[x]}{(x^2+1)}$$

$\mathbb{F}_p$ = the field with p elements

$\dfrac{\mathbb{F}_p[x]}{(x^2+1)}$ has zero-div. $\overset{\text{Prop 2.4}}{\Longleftrightarrow}$ x^2+1 is reducible

$\Leftrightarrow$ X^2+1 has a root in $\mathbb{F}_p$,

i.e. $\exists\, u \in \mathbb{F}_p$, s.t. $u^2 = -1$

Lemma $-1 \in \mathbb{F}_p$ is a square $\Leftrightarrow p \equiv 1 \pmod 4$

Proof: $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ is a cyclic group (exercise)

Let $\omega \in \mathbb{F}_p^\times$ is a generator

then $\mathbb{Z}/(p-1) \xrightarrow{\sim} \mathbb{F}_p^\times$

$a \longmapsto \omega^a$

$\frac{p-1}{2} \longmapsto \omega^{\frac{p-1}{2}} = -1$

-1 is a square $\Leftrightarrow$ $\exists\, a \in \mathbb{Z}$, s.t.

$(\omega^a)^2 = \omega^{\frac{p-1}{2}} \Leftrightarrow 2a \equiv \frac{p-1}{2} \pmod{p-1}$

$\Leftrightarrow \exists\, a, b \in \mathbb{Z}$: $2a = \frac{p-1}{2} + b\cdot(p-1)$

if $p = 1+4n$ take $a = n$, $b = 0$

if $p = 3+4n$ then $\frac{p-1}{2} = 1+2n$

odd, but $2a - b(p-1)$ is even $\Rightarrow$ not solvable

This proves the lemma and the thm $\square$

Ideas arising from this proof

- need to study extensions of $\mathbb{Z}$ such as $\mathbb{Z}[i]$; $\mathbb{Z}[i]$ is the ring of integers in the field $\mathbb{Q}(i)$
  Need to study finite extensions of $\mathbb{Q}$ (number fields)
- important to understand factorization into irred. factors in rings like $\mathbb{Z}[i]$
  Unfortunately, not all rings of integers in number fields are UFD.

Example $R = \mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{-5}\,b \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$

$N(a + \sqrt{-5}\,b) = a^2 + 5b^2$

R is not UFD. Consider $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

2 and 3 are irred, e.g. let $2 = z \cdot w$

$N(z) \cdot N(w) = 4 \Rightarrow N(z) = 2$ — contr.

$\Rightarrow 2$ is irred, but $1 \pm \sqrt{-5}$ is not divisible by 2 in R $\Rightarrow$ contradicts uniqueness of factor. into irred. factors.

- Solution to this problem: consider prime ideals instead of irred. elements.