Some slides for 7th Lecture, Algebra

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

26-02-2014

- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a Euclidean domain.
- $N(\pi) = |\pi|^2 = \pi\overline{\pi} = (a + bi)(a - bi) = a^2 + b^2$
- $5 = (1 + 2i)(1 - 2i)$, 5 is not prime.

Proposition 3.5.11

Let $\pi = a + bi \in \mathbb{Z}[i]$ be a Gaussian integer with $N(\pi) = p$, where p is a prime integer. Then π is a prime element in $\mathbb{Z}[i]$.

Proof:

- We have already seen that $\mathbb{Z}[i]$ is a principal ideal domain (Theorem 3.1.11).
- In a unique factorization domain every irreducible element is prime (Prop. 3.5.3).
- We may check that π is irreducible.
- If $\pi = ab$ then $p = N(\pi) = N(a)N(b)$.
- Therefore, $N(a) = p$ (wlog) and $N(b) = 1$. Hence b is a unit and π irreducible.

Lemma 3.5.12 (Lagrange)

Let p be a prime number. If $p \equiv 1 \pmod 4$ then the congruence

$$x^2 \equiv -1 \pmod p$$

can be solved by $x = (2n)!$ where $p = 4n + 1$.

Exercise 1.29

Let p a prime number, prove that

$$(p-1)! \equiv -1 \pmod p$$

Corollary 3.5.14

A prime number $p \equiv 1 \pmod 4$ is not a prime element in $\mathbb{Z}[i]$.

Theorem 3.5.15 (Fermat)

A prime number $p \equiv 1 \pmod 4$ is a sum of two uniquely determined squares.

$$5 = 1^2 + 2^2$$

$$13 = 3^2 + 2^2$$

How do we find the two squares?

The Euclidean algorithm strikes again

Quadratic residues

Let p be a prime number. If p $\nmid a$ then a is called a quadratic residue modulo (kvadratisk rest modulo) p if it is congruent to a square modulo p, i.e. there exists$x \in \mathbb{Z}$ such that

$$a \equiv x^2 \pmod{p}.$$

Otherwise a is called a quadratic non-residue modulo (kvadratisk ikke-rest modulo) p.

If $p \mid a$, then a is considered neither a quadratic residue nor a quadratic non-residue.

Legendre Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

$$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right), \text{ with } k \in \mathbb{Z}$$

Proposition 1.11.3

Let p denote and odd prime. Half of the numbers $1, 2, \ldots, p-1$ are quadratic residues; the other half are quadratic non-residues modulo p.

Theorem 1.11.4 (Euler)

Let p be an odd prime and let a be an integer not divisible by p. Then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Prime numbers congruent to 1 modulo 4

Lemma 3.5.18

A prime number $p \equiv 3 \pmod 4$ is a prime element in $\mathbb{Z}[i]$.

Corollary 3.5.19

If p is an odd prime number dividing $x^2 + 1$ for some $x \in \mathbb{Z}$ then $p \equiv 1 \pmod 4$.

Theorem 3.5.20

There are infinitely many primes congruent to 1 modulo 4.

Fermat’s last theorem