Some slides for 8th Lecture, Algebra

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

28-02-2013

- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ 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