Some slides for 6th Lecture, Algebra

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

21-02-2013

Computing the GCD from prime factorizations

Let R be a unique factorization domain and there are prime elements $p_1, \ldots, p_n$ that are pair-wise non-associated such that

$$a = u p_1^{r_1} \cdots p_n^{r_n}$$

$$b = v p_1^{s_1} \cdots p_n^{s_n}$$

where $r_i, s_i \geq 0$, u, v are units and $p_1, \ldots, p_n$ are pairwise non-associated.

Then

$$\gcd(a, b) = p_1^{t_1} \cdots p_n^{t_n},$$

where $t_i = \min(r_i, s_i)$

What about the Euclidean algorithm?

Euclidean domains

A domain R is called Euclidean if there exists a Euclidean function $N : R \setminus \{0\} \to \mathbb{N}$.

A Euclidean function satisfies that for every $x \in R, d \in R \setminus \{0\}$, there exists $q, r \in R$ s.t.

$$x = qd + r$$

where either $r = 0$ or $N(r) < N(d)$

Proposition 3.5.9

A Euclidean domain is a principal ideal domain.

$$\langle a, b\rangle = \langle \gcd(a, b)\rangle$$

How do we compute $\gcd(a, b)$? In the same way as for integers!

Remark 3.5.10

There are principal ideal domains that are not Euclidean domains, for instance $\mathbb{Z}[\xi] = \{a + b\xi : a, b \in \mathbb{Z}\}$, where $\xi = (1 + \sqrt{-19})/2$.

Gaussian integers

Recall:

- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
- $N(\pi) = |\pi|^2 = \pi\overline{\pi} = (a + bi)(a - bi) = a^2 + b^2$

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

- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
- $N(\pi) = |\pi|^2 = \pi\overline{\pi} = (a + bi)(a - bi) = a^2 + b^2$
- $5 = (1 + 2i)(1 - 2i)$, 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.