Some slides for 2nd Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

11-09-2012

Greatest common divisor

$$\operatorname{div}(n) = \{d \in \mathbb{N} : d \mid n\}$$

Lemma 1.4.2 (Euclid)

Let $m, n \in \mathbb{Z}$. There exists a unique natural number $d \in \mathbb{N}$ such that

$$\operatorname{div}(m) \cap \operatorname{div}(n) = \operatorname{div}(d)$$

d is called the greatest common divisor of m and n and denoted by

$$\gcd(m, n)$$

Exercise 9: greatest common divisor is really the greatest among these with respect to the usual ordering of $\mathbb{Z}$.

Computing the $\gcd$: The Euclidean algorithm

Proposition 1.5.1

Let $m, n, \in \mathbb{Z}$. Then,

- $\gcd(m, 0) = m$ if $m \in \mathbb{N}$
- $\gcd(m, n) = gcd(m - qn, n)$, for every $q \in \mathbb{Z}$.

Let $m \geq n \geq 0$

- $r_{-1} = m$ and $r_0 = n$
- If $r_0 = 0$ then $\gcd(r_{-1}, r_0) = r_1$. Otherwise define remainder r_1:

$$r_{-1} = q_1 r_0 + r_1$$

- We have $\gcd(r_{-1}, r_0) = \gcd(r_0, r_1)$ and $r_{-1} > r_0 > r_1$

We iterate this process

Computing the gcd: The Euclidean algorithm

Let $m \geq n \geq 0$

- $r_{-1} = m$ and $r_0 = n$
- If $r_0 = 0$ then $\gcd(r_{-1}, r_0) = r_1$. Otherwise define remainder r_1:

$$r_{-1} = q_1 r_0 + r_1$$

- We have $\gcd(r_{-1}, r_0) = \gcd(r_0, r_1)$ and $r_{-1} > r_0 > r_1$

We iterate this process if ($r_1 \neq 0$):

- Define remainder r_2:

$$r_0 = q_1 r_1 + r_2$$

- We have $\gcd(r_0, r_1) = \gcd(r_1, r_2)$ and $r_{-1} > r_0 > r_1 > r_2$

We will get $r_N = 0$ for some step N. Why???

Extended Euclidean algorithm

$$\lambda m + \mu n = \gcd(m, n)$$

$$a_i m + b_i n = r_i$$

Start:

- $a_{-1} = 1, b_{-1} = 0$
- $a_0 = 0, b_0 = 1$

First step:

- $r_1 = r_{-1} - q_1 r_0$
- $a_1 = a_{-1} - q_1 a_0,\ b_1 = b_{-1} - q_1 b_0$

i-th step:

- $r_i = r_{i-2} - q_i r_{i-1}$
- $a_i = a_{i-2} - q_i a_{i-1},\ b_i = b_{i-2} - q_i b_{i-1}$

Assuming that

- $a_{i-1}m + b_{i-1}n = r_{i-1}$
- $a_{i-2}m + b_{i-2}n = r_{i-2}$

We have

$$\begin{aligned} a_i m + b_i n &= (a_{i-2} - q_i a_{i-1})m + (b_{i-2} - q_i b_{i-1})n \\ &= a_{i-2}m + b_{i-2}n - q_i(a_{i-1}m + b_{i-1}n) \\ &= r_{i-2} - q_i r_{i_1} = r_i \end{aligned}$$

Lemma 1.5.7

Let $m, n \in \mathbb{Z}$. Then there are integers $\lambda, \mu \in \mathbb{Z}$ such that

$$\lambda m + \mu n = \gcd(m, n)$$

Two integers $a, b \in \mathbb{Z}$ are called relatively prime if

$$\gcd(a, b) = 1$$

Exercise 14: If there are $\lambda, \mu \in \mathbb{Z}$ such that $\lambda m + \mu n = 1$ then a and b are relatively prime.

Corollary 1.5.10

Suppose that $a \mid bc$, where $a, b, c \in \mathbb{Z}$ and a and b are relatively prime. Then $a \mid c$.

Lemma 1.5.7

Let $m, n \in \mathbb{Z}$. Then there are integers $\lambda, \mu \in \mathbb{Z}$ such that

$$\lambda m + \mu n = \gcd(m, n)$$

Corollary 1.5.11

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

- If a and b are relatively prime, $a \mid c$, $b \mid c$ then $ab \mid c$.
- If a and b are relatively prime and a and c are relatively prime then a and bc are relatively prime.