Some slides for 1st Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

5-09-2011

The natural numbers and the integers

This is our starting point:

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

We may order $\mathbb{Z}$:

- $X \leq Y$ if $Y - X \in \mathbb{N}$
- $X < Y$ if $X \neq Y$ and $X \leq Y$

We say that:

$$s \in S \subset \mathbb{Z} \text{ is a first element in } S \text{ if } s \leq x \text{ for all } x \in S$$

- Does any subset of $\mathbb{Z}$ have a first element?
- Can a subset of $\mathbb{Z}$ have two different first elements? (Exercise 1).

Axiom for $\mathbb{N}$: The previous ordering is a well ordering. That is:

- Every non-empty subset of $\mathbb{N}$ has a first element
- And that is equivalent to mathematical induction

Division with remainder

Theorem 1.2.1

Let $d \in \mathbb{Z}$, where $d > 0$. For every $x \in \mathbb{Z}$ there is a unique remainder $r \in \mathbb{N}$ such that

$$x = qd + r,$$

where $q \in \mathbb{Z}$ and $0 \leq r < d$

Notation:

Let $a = bc$, with $a, b, c \in \mathbb{Z}$. Then c is a divisor of a,

$$c \mid a$$

$[x]_d$ is the unique remainder r in Theorem 1.2.1, for $x, d \in \mathbb{Z}$.

Congruences

Let $a, b, c \in \mathbb{Z}$. Then a an b are **congruent modulo c** if $c \mid (b - a)$.

$$a \equiv b \pmod{c}$$

Proposition 1.3.2

Let $a, b, c \in \mathbb{Z}$, where $c > 0$. Then

- $a \equiv [a]_c \pmod{c}$
- $a \equiv b \pmod{c}$ if and only if $[a]_c = [b]_c$

Proposition 1.3.4

If $x_1 \equiv x_2 \pmod{d}$, $y_1 \equiv y_2 \pmod{d}$. Then

- $x_1 + y_1 \equiv x_2 + y_2 \pmod{d}$
- $x_1 y_1 \equiv x_2 y_2 \pmod{d}$

Repeated squared Algorithm

How to compute the remainder of 12^{11} divided by 21?

- Exercise 1.3: $[xy] = [[x][y]]$
- $a^b a^c = a^{b+c}$
- $(a^b)^c = a^{bc}$

Allow us to have the repeated squared algorithm:

$$\left[a^{2^n}\right] = \left[(a^{2^{n-1}})^2\right] = \left[\left[a^{2^{n-1}}\right]\left[a^{2^{n-1}}\right]\right]$$

Greatest common divisor

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

Lemma 1.4.2 (Euclid)

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

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

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 $\mathbb{Z}$.