INTEGERS: VIDEO VIII MOTIVATION AND FIRST DEFINITIONS

Motivation for the integers

Important material:
EQUIVALENCE RELATIONS, EQUIVALENCE CLASSES, DIVISORS

Motivation for the integers

Important material:
EQUIVALENCE RELATIONS, EQUIVALENCE CLASSES, DIVISORS

- Until now we only have addition and multiplication...

Motivation for the integers

Important material:
EQUIVALENCE RELATIONS, EQUIVALENCE CLASSES, DIVISORS

- Until now we only have addition and multiplication...
- **So how do we solve for x equations like**

$$x + 4 = 2?$$

We want to have "$x = 2 - 4$"!

Motivation for the integers

Important material:
EQUIVALENCE RELATIONS, EQUIVALENCE CLASSES, DIVISORS

- Until now we only have addition and multiplication...
- **So how do we solve for x equations like**

$$x + 4 = 2?$$

We want to have "$x = 2 - 4$"!

Idea: define "$2 - 4$" as the ordered pair $(2, 4) \in \mathbb{N} \times \mathbb{N}$ satisfying certain rules?

Important material:
EQUIVALENCE RELATIONS, EQUIVALENCE CLASSES, DIVISORS

- Until now we only have addition and multiplication...
- **So how do we solve for x equations like**

$$x + 4 = 2?$$

We want to have "$x = 2 - 4$"!

Idea: define "$2 - 4$" as the ordered pair $(2, 4) \in \mathbb{N} \times \mathbb{N}$ satisfying certain rules?
Problem: $2 - 4 = 3 - 5 = 17 - 19 = \ldots\ldots \Rightarrow (2, 4) = (3, 5) = (17, 19)$ so it is not unique.

Motivation for the integers

Important material:
EQUIVALENCE RELATIONS, EQUIVALENCE CLASSES, DIVISORS

- Until now we only have addition and multiplication...
- **So how do we solve for x equations like**

$$x + 4 = 2?$$

We want to have "$x = 2 - 4$"!

Idea: define "$2 - 4$" as the ordered pair $(2, 4) \in \mathbb{N} \times \mathbb{N}$ satisfying certain rules?
Problem: $2 - 4 = 3 - 5 = 17 - 19 = \ldots\ldots \Rightarrow (2, 4) = (3, 5) = (17, 19)$ so it is not unique.

$$\bigstar \text{ Note: } a - b = c - d \Leftrightarrow a + d = b + c \bigstar$$

What would be your next idea....?

Definition of the integers

New Idea:

Define the equivalence relation on $\mathbb{N} \times \mathbb{N}$

$$(a, b) \sim (c, d) \text{ if and only if } a + d = b + c.$$

Definition of the integers

New Idea:

Define the equivalence relation on $\mathbb{N} \times \mathbb{N}$

$$(a, b) \sim (c, d) \text{ if and only if } a + d = b + c.$$

$$a - b := cl((a, b)) = \{(x, y) \in \mathbb{N} \times \mathbb{N} | (x, y) \sim (a, b)\}$$

Definition of the integers

New Idea:

Define the equivalence relation on $\mathbb{N} \times \mathbb{N}$

$$(a, b) \sim (c, d) \text{ if and only if } a + d = b + c.$$

$$a - b := cl((a, b)) = \{(x, y) \in \mathbb{N} \times \mathbb{N} | (x, y) \sim (a, b)\}$$

$\mathbb{Z}$ **is the set of all equivalence classes** $a - b$**.**

Definition of the integers

New Idea:

Define the equivalence relation on $\mathbb{N} \times \mathbb{N}$

$$(a, b) \sim (c, d) \text{ if and only if } a + d = b + c.$$

$$a - b := cl((a, b)) = \{(x, y) \in \mathbb{N} \times \mathbb{N} | (x, y) \sim (a, b)\}$$

$\mathbb{Z}$ **is the set of all equivalence classes** $a - b$**.**

Equivalence classes $a - 0$ will be written a, $0 - b$ will be written -b

Definition of the integers

New Idea:

Define the equivalence relation on $\mathbb{N} \times \mathbb{N}$

$$(a, b) \sim (c, d) \text{ if and only if } a + d = b + c.$$

$$a - b := cl((a, b)) = \{(x, y) \in \mathbb{N} \times \mathbb{N} | (x, y) \sim (a, b)\}$$

$\mathbb{Z}$ is the set of all equivalence classes $a - b$.

Equivalence classes $a - 0$ will be written a, $0 - b$ will be written -b

★ Wanted:

$$\begin{aligned} (a-b)+(c-d) &= (a+c)-(b+d), \\ (a-b)\dot{}(c-d) &= (ac+bd)-(ad+bc). \end{aligned}$$

We define on $\mathbb{Z}$:

Addition: $(a, b) + (c, d) := (a + c, b + d)$

Multiplication: $(a, b) \cdot (c, d) := (ac + bd, ad + bc)$.

To go further

Beyond the scope of this lecture (but in the notes) we can show

- Addition and multiplication are well-defined on $\mathbb{Z}$ (i.e. do not depend on the representant of the class).
- Any element in $\mathbb{Z}$ is either an $n \in \mathbb{N}$ or $-n$, with $n \in \mathbb{N}$. Therefore

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

FROM NOW ON WE CAN USE WHATEVER RULES WE KNOW FOR ADDITION, SUBSTRACTION, MULTIPLICATION ON THE INTEGERS! (Yippie)

INTEGERS: VIDEO IX GCD (hcf) /LCM AND QUOTIENT-REMAINDER THEOREM

GCD(HCF)/LCM

Reminder (but for integers!):

Definition

Let $n, m \in \mathbb{Z}$. We say that m divides n if and only if there exists a number $k \in \mathbb{Z}$, such that $n = k \cdot m$. Notation: $m|n$.

GCD(HCF)/LCM

Reminder (but for integers!):

Definition

Let $n, m \in \mathbb{Z}$. We say that m divides n if and only if there exists a number $k \in \mathbb{Z}$, such that $n = k \cdot m$. Notation: $m|n$.

Definition

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

- A **common divisor** of a and b is an integer $n \in \mathbb{Z}$ such that $n|a$ and $n|b$.

GCD(HCF)/LCM

Reminder (but for integers!):

Definition

Let $n, m \in \mathbb{Z}$. We say that m divides n if and only if there exists a number $k \in \mathbb{Z}$, such that $n = k \cdot m$. Notation: $m|n$.

Definition

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

- A **common divisor** of a and b is an integer $n \in \mathbb{Z}$ such that $n|a$ and $n|b$.
  The **greatest common divisor (gcd)** of a and b is the largest such integer. Notation: gcd(a,b).

GCD(HCF)/LCM

Reminder (but for integers!):

Definition

Let $n, m \in \mathbb{Z}$. We say that m divides n if and only if there exists a number $k \in \mathbb{Z}$, such that $n = k \cdot m$. Notation: $m|n$.

Definition

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

- A **common divisor** of a and b is an integer $n \in \mathbb{Z}$ such that $n|a$ and $n|b$.
  The **greatest common divisor (gcd)** of a and b is the largest such integer. Notation: gcd(a,b).
- A **common multiple** of a and b is an integer $n \in \mathbb{Z}$ such that $n = ka$ and $n = lb$ for some $k, l \in \mathbb{Z}$.

GCD(HCF)/LCM

Reminder (but for integers!):

Definition

Let $n, m \in \mathbb{Z}$. We say that m divides n if and only if there exists a number $k \in \mathbb{Z}$, such that $n = k \cdot m$. Notation: $m|n$.

Definition

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

- A **common divisor** of a and b is an integer $n \in \mathbb{Z}$ such that $n|a$ and $n|b$.
  The **greatest common divisor (gcd)** of a and b is the largest such integer. Notation: gcd(a,b).
- A **common multiple** of a and b is an integer $n \in \mathbb{Z}$ such that $n = ka$ and $n = lb$ for some $k, l \in \mathbb{Z}$.
  The **least common multiple (lcm)** is the smallest positive such integer. Notation: lcm(a,b).

GCD(HCF)/LCM

Reminder (but for integers!):

Definition

Let $n, m \in \mathbb{Z}$. We say that m divides n if and only if there exists a number $k \in \mathbb{Z}$, such that $n = k \cdot m$. Notation: $m|n$.

Definition

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

- A **common divisor** of a and b is an integer $n \in \mathbb{Z}$ such that $n|a$ and $n|b$.
  The **greatest common divisor (gcd)** of a and b is the largest such integer. Notation: gcd(a,b).
- A **common multiple** of a and b is an integer $n \in \mathbb{Z}$ such that $n = ka$ and $n = lb$ for some $k, l \in \mathbb{Z}$.
  The **least common multiple (lcm)** is the smallest positive such integer. Notation: lcm(a,b).
- a and b are called **relatively prime** if $gcd(a, b) = 1$.

By convention $gcd(0, 0) = 0$

Compute $\gcd(8, 12)$:

Proposition

Suppose $a, b \in \mathbb{Z} - \{0\}$. *Then*

a) $gcd(a, b) = gcd(b, a)$.
b) *if* $a > 0$ *and* $a|b$ *then* $gcd(a, b) = a$
c) *if* $a = bq + r$, *for some* $q, r \in \mathbb{Z}$ *then* $gcd(a, b) = gcd(r, b)$.

Proof of c):

Quotient-Remainder theorem (Q-R T)

Theorem

Let $a, b \in \mathbb{Z}$, $b > 0$. Then there exist unique integers q and r such that

$$a = qb + r, \quad 0 \leq r < b$$

Examples: if $a = 11$, $b = 4$, $11 = 2 \cdot 4 + 3$, hence $q = 2$, $r = 3$
if $a = -8$, $b = 3$, $-8 = -3 \cdot 3 + 1$, hence $q = -3$, $r = 1$.

★ : This result comes directly from long division of a by b, where q is the quotient and r the remainder.

Quotient-Remainder theorem (Q-R T)–Proof of existence

Theorem

Let $a, b \in \mathbb{Z}$, $b > 0$. Then there ***exists*** *unique* ***integers*** *q* ***and*** *r such that*

$$a = qb + r, \quad 0 \leq r < b$$

Proof: To show: $\exists r$, such that $r = a - qb$ and $0 \leq r < b$, for fixed a and $b > 0$ and some q

Quotient-Remainder theorem (Q-R T)–Proof of existence

Theorem

Let $a, b \in \mathbb{Z}$, $b > 0$. Then there ***exists*** *unique* ***integers*** *q* ***and*** *r such that*

$$a = qb + r, \quad 0 \leq r < b$$

Proof: To show: $\exists r$, **such that** $r = a - qb$ **and** $0 \leq r < b$, **for fixed** a **and** $b > 0$ **and some** q **Idea: Use the Well-Ordering principle (WOP)!**

- Define the appropriate set $S \subseteq \mathbb{N}$:

- Show S is not empty:

- By WOP S has **a least element** r, such that $r = a - qb$ and $r \geq 0$
- It remains to show that $r < b$

...........**and uniqueness of** r **(read your notes!)**

INTEGERS: VIDEO X
EUCLIDEAN ALGORITHM

Euclidean algorithm to compute $gcd(a, b)$

Reminder:

Theorem (Q-R Theorem)

Let $a, b \in \mathbb{Z}$, $b > 0$. Then there ***exists*** *unique* ***integers*** *q* ***and*** *r such that*
$a = qb + r, \quad 0 \leq r < b$

Euclidean algorithm to compute $gcd(a, b)$

Reminder:

Theorem (Q-R Theorem)

*Let $a, b \in \mathbb{Z}$, $b > 0$. Then there **exists** unique **integers** q **and** r such that*
$a = qb + r, \quad 0 \le r < b$

Proposition

Suppose $a, b \in \mathbb{Z}$, $b \neq 0$. If $a = bq + r$, for some $q, r \in \mathbb{Z}$ then
$gcd(a, b) = gcd(r, b)$.

Euclidean algorithm to compute $gcd(a, b)$

Reminder:

Theorem (Q-R Theorem)

*Let $a, b \in \mathbb{Z}$, $b > 0$. Then there **exists** unique **integers** q **and** r such that*
$a = qb + r, \quad 0 \leq r < b$

Proposition

Suppose $a, b \in \mathbb{Z}$, $b \neq 0$. If $a = bq + r$, for some $q, r \in \mathbb{Z}$ then
$gcd(a, b) = gcd(r, b)$.

Euclidean Algorithm: How to compute $\gcd(a, b)$**,** $a, b \in \mathbb{Z}$**,** $b > 0$**?**

- Start with $gcd(a, b)$. (We can assume Wlog that $a > b$)

Euclidean algorithm to compute $gcd(a, b)$

Reminder:

Theorem (Q-R Theorem)

*Let $a, b \in \mathbb{Z}$, $b > 0$. Then there **exists** unique **integers** q **and** r such that*
$a = qb + r, \quad 0 \le r < b$

Proposition

Suppose $a, b \in \mathbb{Z}$, $b \neq 0$. If $a = bq + r$, for some $q, r \in \mathbb{Z}$ then
$gcd(a, b) = gcd(r, b)$.

Euclidean Algorithm: How to compute $\gcd(a, b)$, $a, b \in \mathbb{Z}$, $b > 0$**?**

- Start with $gcd(a, b)$. (We can assume Wlog that $a > b$)
- By Q-R theorem $a = bq_1 + r_1$ for some $q_1 \in \mathbb{Z}$, $0 \le r_1 < b$.

Euclidean algorithm to compute $gcd(a, b)$

Reminder:

Theorem (Q-R Theorem)

*Let $a, b \in \mathbb{Z}$, $b > 0$. Then there **exists** unique **integers** q **and** r such that*
$a = qb + r, \quad 0 \leq r < b$

Proposition

Suppose $a, b \in \mathbb{Z}$, $b \neq 0$. If $a = bq + r$, for some $q, r \in \mathbb{Z}$ then
$gcd(a, b) = gcd(r, b)$.

Euclidean Algorithm: How to compute $\gcd(a, b)$, $a, b \in \mathbb{Z}$, $b > 0$**?**

- Start with $gcd(a, b)$. (We can assume Wlog that $a > b$)
- By Q-R theorem $a = bq_1 + r_1$ for some $q_1 \in \mathbb{Z}$, $0 \leq r_1 < b$.
- By Proposition above $gcd(a, b) = gcd(b, r_1)$.

Euclidean algorithm to compute $gcd(a, b)$

Reminder:

Theorem (Q-R Theorem)

*Let $a, b \in \mathbb{Z}$, $b > 0$. Then there **exists** unique **integers** q **and** r such that* $a = qb + r, \quad 0 \le r < b$

Proposition

Suppose $a, b \in \mathbb{Z}$, $b \neq 0$. If $a = bq + r$, for some $q, r \in \mathbb{Z}$ then $gcd(a, b) = gcd(r, b)$.

Euclidean Algorithm: How to compute $\gcd(a, b)$**,** $a, b \in \mathbb{Z}$**,** $b > 0$**?**

- Start with $gcd(a, b)$. (We can assume Wlog that $a > b$)
- By Q-R theorem $a = bq_1 + r_1$ for some $q_1 \in \mathbb{Z}$, $0 \le r_1 < b$.
- By Proposition above $gcd(a, b) = gcd(b, r_1)$.
- Again by By Q-R theorem $b = r_1 q_2 + r_2$ for some $q_2 \in \mathbb{Z}$, $0 \le r_2 < r_1$.

Euclidean algorithm to compute $gcd(a, b)$

Reminder:

Theorem (Q-R Theorem)

*Let $a, b \in \mathbb{Z}$, $b > 0$. Then there **exists** unique **integers** q **and** r such that*
$a = qb + r, \quad 0 \le r < b$

Proposition

Suppose $a, b \in \mathbb{Z}$, $b \neq 0$. If $a = bq + r$, for some $q, r \in \mathbb{Z}$ then
$gcd(a, b) = gcd(r, b)$.

Euclidean Algorithm: How to compute $\gcd(a, b)$**,** $a, b \in \mathbb{Z}$**,** $b > 0$**?**

- Start with $gcd(a, b)$. (We can assume Wlog that $a > b$)
- By Q-R theorem $a = bq_1 + r_1$ for some $q_1 \in \mathbb{Z}$, $0 \le r_1 < b$.
- By Proposition above $gcd(a, b) = gcd(b, r_1)$.
- Again by By Q-R theorem $b = r_1 q_2 + r_2$ for some $q_2 \in \mathbb{Z}$, $0 \le r_2 < r_1$.
- By the Proposition again $gcd(b, r_1) = gcd(r_1, r_2)$.

Euclidean algorithm to compute $gcd(a, b)$

Reminder:

Theorem (Q-R Theorem)

*Let $a, b \in \mathbb{Z}$, $b > 0$. Then there **exists** unique **integers** q **and** r such that*
$a = qb + r, \quad 0 \le r < b$

Proposition

Suppose $a, b \in \mathbb{Z}$, $b \neq 0$. If $a = bq + r$, for some $q, r \in \mathbb{Z}$ then
$gcd(a, b) = gcd(r, b)$.

Euclidean Algorithm: How to compute $\gcd(a, b)$, $a, b \in \mathbb{Z}$, $b > 0$**?**

- Start with $gcd(a, b)$. (We can assume Wlog that $a > b$)
- By Q-R theorem $a = bq_1 + r_1$ for some $q_1 \in \mathbb{Z}$, $0 \le r_1 < b$.
- By Proposition above $gcd(a, b) = gcd(b, r_1)$.
- Again by By Q-R theorem $b = r_1 q_2 + r_2$ for some $q_2 \in \mathbb{Z}$, $0 \le r_2 < r_1$.
- By the Proposition again $gcd(b, r_1) = gcd(r_1, r_2)$.
- Iterate!! Since $b > r_1 > r_2 > \cdots > 0$, eventually $r_k = 0$ for some k and

$$\gcd(a, b) = \gcd(r_{k-1}, r_k) = \gcd(r_{k-1}, 0) = r_{k-1}$$

Euclidean algorithm: Example

Compute $\gcd(42, 18)$

- Start with $gcd(42, 18)$.
- By Q-R theorem $a = bq_1 + r_1$ for some $q_1 \in \mathbb{Z}$, $0 \leq r_1 < b$.
- By our Proposition $gcd(a, b) = gcd(b, r_1)$.
- Again by By Q-R theorem $b = r_1 q_2 + r_2$ for some $q_2 \in \mathbb{Z}$, $0 \leq r_2 < r_1$.
- By our Proposition again $gcd(b, r_1) = gcd(r_1, r_2)$.

Euclidean algorithm: Example

Compute $\gcd(42, 18)$

- Start with $gcd(42, 18)$.
- By Q-R theorem $a = bq_1 + r_1$ for some $q_1 \in \mathbb{Z}$, $0 \leq r_1 < b$.
- By our Proposition $gcd(a, b) = gcd(b, r_1)$.
- Again by By Q-R theorem $b = r_1 q_2 + r_2$ for some $q_2 \in \mathbb{Z}$, $0 \leq r_2 < r_1$.
- By our Proposition again $gcd(b, r_1) = gcd(r_1, r_2)$.
- Iteration is finished!