Algebra MATH-310

All information on Moodle

Anna Lachowska (she, her)

anna.lachowska@epfl.ch

September 8, 2025

Organization

Lectures: Mondays 15:15 - 17:00 SG 1, + live streaming
Exercises: Mondays 17:15 - 19:00, SG 1

+ Lectures live streamed and video recorded, link on Moodle
+ Polls on Zoom during class
+ Ed Discussion: questions at any time
  new: Tutor Bot in Ed see information on Moodle (Also possible: NoBotLand)
+ Old video recordings online, link on Moodle
+ Polycopie written by Joachim Favre, available on Moodle
+ My typed course notes on Moodle
+ Problem sets and solutions on Moodle

One graded written assignment in November: 15% of the final grade
Written exam in January: 85% of the final grade

Assistants

Mohamed Abbes

Damien Bridel

Maryam Harakat

Charbel Raffoul

Amal Seddas (DA)

Plan of the course

1. Integers: 1 lecture
2. Groups: 6 lectures
3. Rings and fields: 5 lectures
4. Review: 1 lecture

Today: Integers

(a) Induction principle and well-ordering principle

(b) Prime factorization. Uniqueness.

(c) Euclidean division. Bézout's theorem

(d) Euler's totient function

Integers

Question

What is the most basic property of natural numbers?

$$\mathbb{N} = \{0, 1, 2, \ldots\}$$

Induction

Question

What is the most basic property of natural numbers?

$$\mathbb{N} = \{0, 1, 2, \ldots\}$$

Induction principle

Let $S \subset \mathbb{N}$ such that
(1) $0 \in S$;
(2) If $n \in S$, then $n + 1 \in S$.
Then $S = \mathbb{N}$.

Induction vs. Strong Induction

Induction principle

Let $S \subset \mathbb{N}$ such that
(1) $0 \in S$;
(2) If $n \in S$, then $n+1 \in S$. stronger condition on S
Then $S = \mathbb{N}$.

Strong Induction principle

Let $S \subset \mathbb{N}$ such that
(1) $0 \in S$;
(2) If $\{0, 1, \ldots n\} \subset S$, then $n+1 \in S$. weaker condition on S
Then $S = \mathbb{N}$.

Induction principle

Let $S \subset \mathbb{N}$ such that
(1) $0 \in S$;
(2) If $n \in S$, then $n+1 \in S$.
Then $S = \mathbb{N}$.

Strong Induction principle

Let $S \subset \mathbb{N}$ such that
(1) $0 \in S$;
(2) If $\{0, 1, \ldots n\} \subset S$, then $n+1 \in S$.
Then $S = \mathbb{N}$.

Well ordering principle

Every nonempty subset of $\mathbb{N}$ has a least element.

Poll: Which statement is stronger? A: Induction is stronger than Well ordering, B: Strong induction is stronger than Well ordering, C: Well ordering is stronger than Induction, D: All are equivalent ← correct answer

Induction and Well ordering

Proposition $IP \Rightarrow SIP \overset{[PS1]}{\Rightarrow} WOP \Rightarrow IP$

Induction, Strong induction and Well ordering principles are equivalent.

$IP \Rightarrow SIP$

Let $S \subset \mathbb{N}$: $0 \in S$ and if $\{0, 1 \ldots n\} \subset S \Rightarrow n+1 \in S$

Want to show: $S = \mathbb{N}$ using only IP.

Let $P(n)$ be the statement: $\{0, 1 \ldots n\} \subset S$

Then: $P(0)$ is true: $0 \in S$.

If $P(n)$ is true: $\{0, 1, \ldots n\} \subset S \Rightarrow n+1 \in S \overset{\text{means}}{\Rightarrow} \{0, 1 \ldots n+1\} \subset S \Rightarrow$ $P(n+1)$ is true.

$\Rightarrow$ by IP, $P(n)$ is true $\forall n \in \mathbb{N}$

$\Rightarrow \{0, 1, \ldots n\} \subset S \ \forall n \in \mathbb{N} \Rightarrow S = \mathbb{N}$

Induction and Well ordering

Proposition WOP => IP

Induction, Strong induction and Well ordering principles are equivalent.

Suppose $S \subset \mathbb{N}$: $0 \in S$ and if $n \in S \Rightarrow n+1 \in S$. Want to show: $S = \mathbb{N}$ using WOP.

Let $S' = \mathbb{N} \setminus S$. Suppose $S \neq \emptyset \Rightarrow$ by WOP $\exists\, k \in S'$ least elt.

$k \neq 0$ because $0 \in S \Rightarrow 0 \notin S'$

$k \in S'$ is minimal

$\Rightarrow k = m+1 \in \mathbb{N}$ for some $m \in \mathbb{N}$, $m \notin S' \Rightarrow m \in S$

$\Rightarrow$ by condition $m \in S \Rightarrow m+1 \in S$

$k = m+1 \in S'$ and $k = m+1 \in S$

contradiction: $S \cap S' = \emptyset$

$\Rightarrow S' = \emptyset \Rightarrow S = \mathbb{N}$ ▨

proof by „minimal criminal"

..

Application: prime factorization

Definition

Let $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$. If $a, b \in \mathbb{Z}$ and $a \neq 0$, we say that a divides b if there exists $c \in \mathbb{Z}$ such that $b = ac$.

Definition

A number $p \in \mathbb{Z}_+ = \{1, 2, \ldots\}$ is prime if $p > 1$ and the only divisors of p are 1 and p. Other integer numbers are composite.

Theorem

Any number $n > 1$ has a prime divisor.

Application: prime factorization

Theorem

Any number $n > 1$ has a prime divisor.

Suppose $S \subset \mathbb{N}_{>1}$ s.t. elements of S have no prime divisor

Suppose $S \neq \emptyset$ $\Rightarrow$ by WOP $\exists$ a minimal $k \in S$

minimal criminal

If $k = p$ is a prime $\Rightarrow$ then $p \mid k$

If $k = a \cdot b$ composite. Both a and b have prime divisors

$a > 1$, $b > 1$

since $a < k$, $b < k$

for example $q \mid a$, q a prime

$\Rightarrow$ $q \mid k$

.

Application: prime factorization

Theorem

(1) Any number $n > 1$ is a product of primes; ← exercise

(2) prime factorization is unique. minimal criminal!

Let $n = p_1 \cdots p_k = q_1 \cdots q_m$ the smallest with 2 different prime factorizations
$\Rightarrow p_i \neq q_j$

smallest

WLOG assume $q_1 > p_1$, let $t = (q_1 - p_1) q_2 \cdots q_m > 0$, $t < n$

$t = \underbrace{q_1 \cdots q_m}_{h = p_1 \cdots p_k} - p_1 q_2 \cdots q_m = p_1 p_2 \cdots p_k - p_1 q_2 \cdots q_m = p_1 (p_2 \cdots p_k - q_2 \cdots q_m)$

t has a unique prime factorization $\Rightarrow p_1 \mid t$

$t = (q_1 - p_1) q_2 \cdots q_m \Rightarrow p_1 \mid (q_1 - p_1) \Rightarrow q_1 - p_1 = s p_1$, $s \in \mathbb{N}$, $s \geq 1$

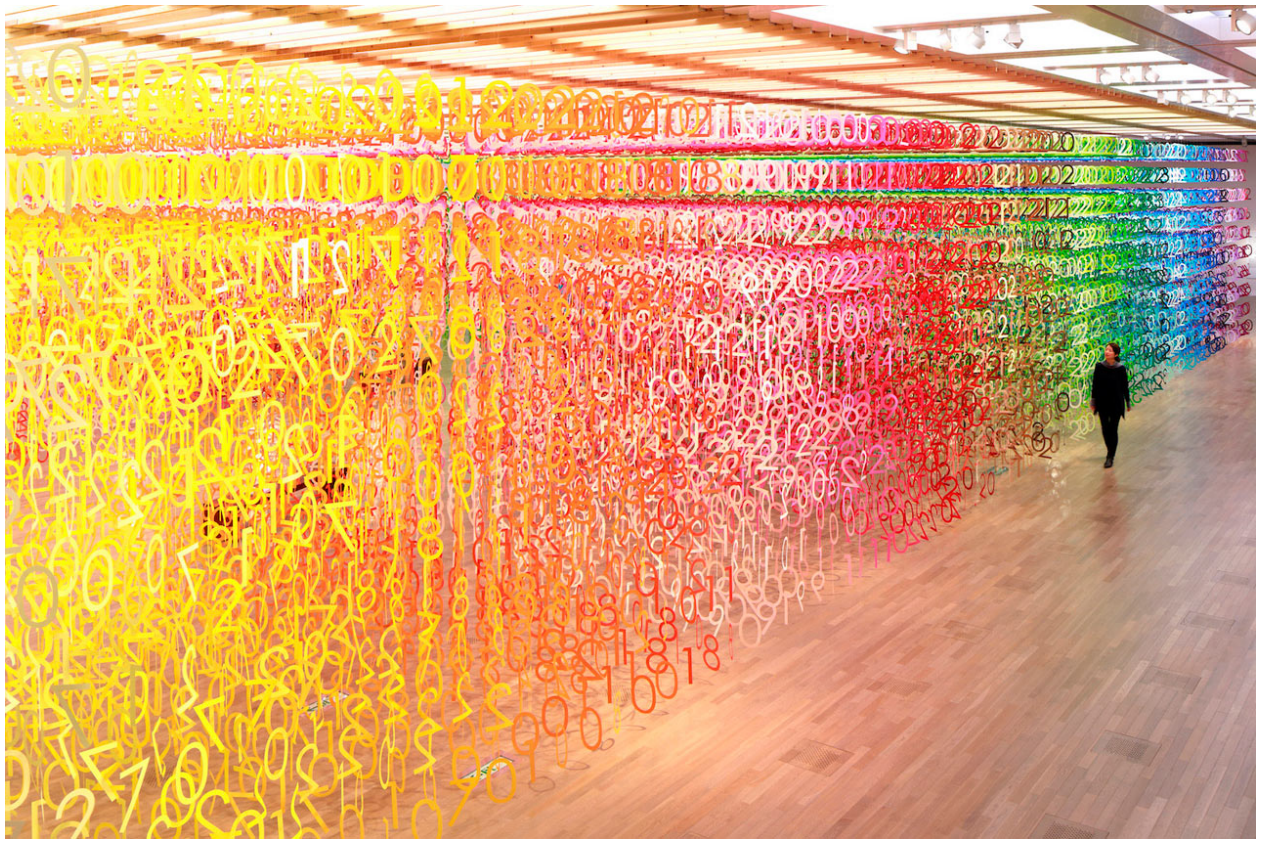
$\Rightarrow q_1 = \underbrace{(s+1)}_{>1} p_1 \Rightarrow q_1$ is not prime! contradiction

$\Rightarrow$ no such minimal n can exist

$\Rightarrow$ any $n > 1$ has a unique prime factorization ☑

Conclusion: basic properties of $\mathbb{N}$:

(1) Natural numbers are constructible by induction starting from 0;
(2) Natural numbers > 1 admit a unique prime factorization.

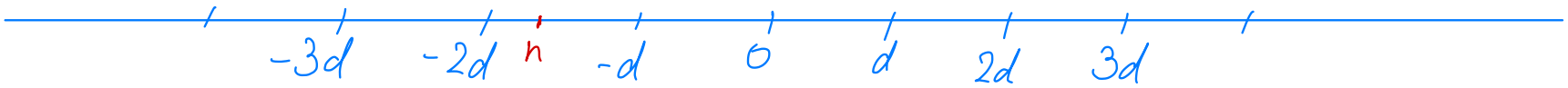


Euclidean division

Theorem

Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}_+$. Then there exist two integers $q, r \in \mathbb{Z}$ such that $n = qd + r$ and $0 \leq r < d$. These q, r are unique.

Existence: WOP. Let $S = \{n - kd\}_{k \in \mathbb{Z}} \cap \mathbb{N}$.



$\Rightarrow S \neq \emptyset$, $S \subset \mathbb{N} \Rightarrow$ WOP $\Rightarrow \exists r$ the least elt in S.

$\Rightarrow r = n - kd \Rightarrow n = kd + r$, $r \geq 0$ because $S \subset \mathbb{N}$

If $r \geq d \Rightarrow r' = r - d \in \mathbb{N}$ and $r' = n - kd - d = n - (k+1)d \in S$

$r' < r$

$\Rightarrow r$ is not minimal in S, contradiction

$\Rightarrow r < d$, and finally $0 \leq r < d$. ∎

Euclidean division

Theorem

Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}_+$. Then there exist two integers $q, r \in \mathbb{Z}$ such that $n = qd + r$ and $0 \leq r < d$. These q, r are unique.

Uniqueness: Suppose $r_1 + q_1 d = r_2 + q_2 d$, WLOG $q_1 > q_2$.

$(q_1 - q_2)\, d + r_1 = r_2$

≥ 1 $\quad \geq 0$ $\quad \geq d$

$\geq d$

contradiction because $r_2 < d$.

Definition

If $a, b \in \mathbb{Z}$, then $\gcd(a, b)$ is a positive integer c such that $c|a$ and $c|b$, and if there is another positive integer d with this property, then $d|c$.

Euclidean division

$n = qd + r$

Proposition

If $n, q \in \mathbb{Z}$ and $d \in \mathbb{Z}_+$ such that $n = qd + r$, $0 \leq r < d$, then $\gcd(n, d) = \gcd(d, r)$.

c common divisor of n, d $\Rightarrow$ $n = qd + r$ $\Rightarrow$ c divides r

c common divisor of r, d $\Rightarrow$ $n = qd + r$ $\Rightarrow$ c divides n

$\Rightarrow$ The set of common divisors of (n, d) equals to the set of common divisors of (r, d)

$\Rightarrow \gcd(n, d) = \gcd(r, d)$.

proof by staring

Use Euclidean division to find gcd of two numbers

$$
\begin{aligned}
d_1 &= q_1 d_2 + d_3 && d_3 < d_2 \\
d_2 &= q_2 d_3 + d_4 && d_4 < d_3 \qquad \gcd(d_1, d_2) = \gcd(d_2, d_3) \\
&\dots \\
d_{k-1} &= q_{k-1} d_k + d_{k+1} \\
d_k &= q_k d_{k+1} + 0 && \Longrightarrow \qquad d_{k+1} = \gcd(d_1, d_2).
\end{aligned}
$$

Example $\gcd(432, 315)$

$432 \mid 315$, $315 \mid 117$, $117 \mid 81$, $81 \mid 36$, $36 \mid 9$

$432 = 315 \cdot 1 + 117$

$315 = 234 \cdot 1 + 81$

$117 = 81 \cdot 1 + 36$

$81 = 72 \cdot 2 + 9$

$36 = 0 \cdot 4$

$\Rightarrow \gcd(432, 315) = 9.$

Applications of Euclidean division

Corollary 1

If $a, b \in \mathbb{Z}_+$, then there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$.

Run the Euclidean algorithm backwards!

Example: $\boxed{9} = 81 - 2 \cdot 36 = 81 - 2 \cdot (117 - 81) = 3 \cdot 81 - 2 \cdot 117 =$

$= 3(315 - 2 \cdot 117) - 2 \cdot 117 = 3 \cdot 315 - 8 \cdot 117 =$

$= 3 \cdot 315 - 8 \cdot (432 - 315) = 11 \cdot \boxed{315} - 8 \cdot \boxed{432}.$

$\gcd(315, 432)$

Corollary 2

If $a, b \in \mathbb{Z}_+$ and $d = \gcd(a, b)$, then the equation $ax + by = c \in \mathbb{Z}$ has a solution $x, y \in \mathbb{Z}$ if and only if c is a multiple of d.

If $c = kd \Rightarrow d = ax_0 + by_0$ by Corollary 1 $\Rightarrow kd = c = kx_0 a + ky_0 b$.

c is always of this form: if $d \mid a$ and $d \mid b \Rightarrow d \mid (ax + by) \Rightarrow d \mid c$.

Bezout's theorem

Definition

Two integers a, b are relatively prime if $\gcd(a, b) = 1$.

Theorem

Two numbers $a, b \in \mathbb{Z}_+$ are relatively prime if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

This is a particular case of Corollary 2.

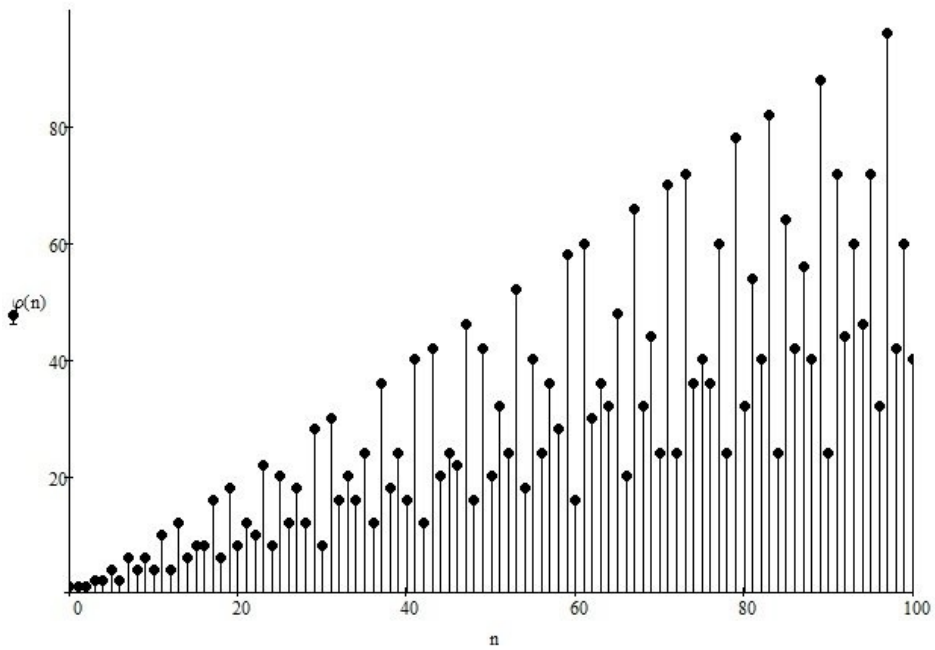
Conclusion: basic properties of $\mathbb{Z}$:

(1) Euclidean algorithm can be used to find the $\gcd$ of two integers
(2) For two integers a, b we can find two integers x, y such that $xa + yb = c$ if and only if c is a multiple of $\gcd(a, b)$.

Euler's totient function $\varphi(n)$

Definition

For any $n \in \mathbb{Z}_+$ the Euler's totient function $\varphi(n)$ is equal to the number of positive integers k such that $1 \leq k \leq n$ and $\gcd(n, k) = 1$.



$\varphi(2) = 1$

$\varphi(3) = 2$

$\varphi(19) = 18$

$\varphi(p) = p-1$ for any prime p.

$\varphi(15) = 8$

$\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$

$\varphi(p \cdot q) = pq - q - p + 1 = (p-1)(q-1)$ ▨

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 $\varphi(15)$

Euler's totient function $\varphi(n)$

Let p be a prime.

$\varphi(p^2) =$

A: $p^2 - 2p - 1$

B: $(\varphi(p))^2$

C: $p^2 - p$

D: $p^2 - 1$.

$1, 2, \ldots, p, \ldots, 2p, \ldots, 3p, \ldots, p(p-1), \ldots, p^2$

$1 \quad 2 \quad 3 \quad p$

$\Rightarrow \varphi(p^2) = p^2 - p \Rightarrow$ (C)

$\neq (\varphi(p))^2 = (p-1)^2 = p^2 - 2p + 1$

$\varphi(pq) = \varphi(p)\varphi(q)$ if p and q are distinct primes.

but $\varphi(p^2) \neq (\varphi(p))^2$

Later: $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \iff \gcd(m, n) = 1$

(application of ring theory ☺)