Algebra MATH-310

All information on Moodle

Anna Lachowska

anna.lachowska@epfl.ch

September 9, 2024

Organization

Lectures: Mondays 15:15 - 17:00 CM 1 1, live streaming in CM 1 4
Exercises: Mondays 17:15 - 19:00, CM 1 1 and ~~CM 1 4~~.

+ Lectures live streamed and video recorded on Zoom, link on Moodle
+ Polls on Zoom during class
+ Ed Discussion: questions at any time
+ 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

Damien Bridel
Kasimir De Guilhem De Lataillade
Fabien Donnet-Monay
Mehdi Jelassi
Vladislav Shashkov (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 $n+1 \in S$.
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 $S = \mathbb{N}$.

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 the strongest? A: Induction, B: Strong induction, C: Well ordering, D: All are equivalent

correct answer.

Induction and Well ordering

IP → SIP

Proposition IP => SIP => WOP => IP (PS1)

Induction, Strong induction and Well ordering principles are equivalent.

IP => SIP

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

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

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

Then $P(0)$ is true ; if $P(n)$ true : $\{0, \dots n\} \in S \Rightarrow n+1 \in S$

$\Rightarrow \{0, \dots n, n+1\} \subset S \Rightarrow P(n+1)$ is true

$\Rightarrow$ By simple induction $P(n)$ is true $\forall n \in \mathbb{N}$

$\Rightarrow \{0, \dots n\} \subset S \ \forall n \Rightarrow S = \mathbb{N}$

Induction and Well ordering

Proposition WOP => IP

Induction, Strong induction and Well ordering principles are equivalent.

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

let $S' = \mathbb{N} \setminus S$ Suppose $S' \neq \emptyset$ => by WOP $\exists k \in S'$

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

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

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

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

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. elts in S has no prime divisor $\Rightarrow$ 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 $\Rightarrow$ both a and b have >1 >1 prime divisors; q prime $q \mid a$

$\Rightarrow$

$\Rightarrow q \mid k = a \cdot b$ ▨

Application: prime factorization

Theorem

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

(2) prime factorization is unique.

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

(n smallest)

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

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

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

$t = (q_1 - p_1) q_2 \dots q_m \Rightarrow p_1 \mid (q_1 - p_1) \Rightarrow q_1 - p_1 = s p_1$

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

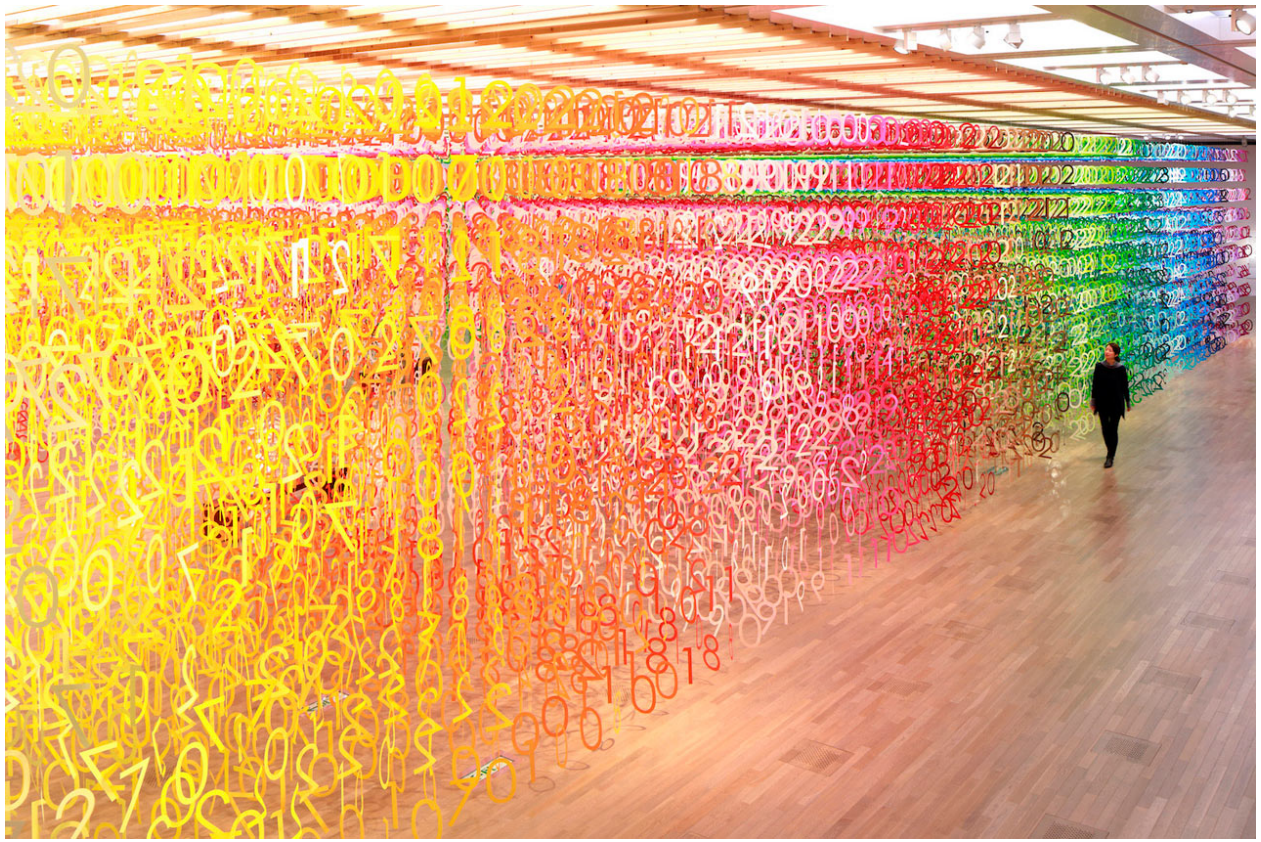
$\Rightarrow$ no such minimal n can exist

$\Rightarrow$ any $n > 1$ has a unique prime factoriz.

.

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.

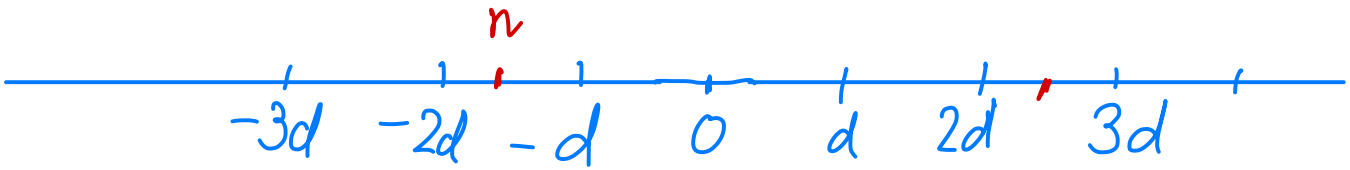


Euclidean division

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



WOP

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

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

If $r > d$ $\Rightarrow$ $r' = r - d$, $n = kd + d + r' = (k+1)d + r'$

$\Rightarrow r - d \in S \Rightarrow r$ is not minimal

$\Rightarrow 0 \leq r < d$.

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 ≥ 0 $\geq d$

$\geq d$

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

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 is common divisor of $n, d \Rightarrow c \mid r$

c is common divisor of $d, r \Rightarrow c \mid n$

$\Rightarrow$ the set of common divisors of (n, d) is equal to the set of common divisors of (r, d)

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

$\blacksquare$

proof by staring

Use Euclidean division to find gcd of two numbers

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

Example $\gcd(336, 180)$

$336 = 180 \cdot 1 + 156$

$180 = 156 \cdot 1 + 24$

$156 = 144 + 12 = 24 \cdot 6 + 12$

$24 = 12 \cdot 2 + 0$

$\Rightarrow \gcd(336, 180) = 12$

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!

$a = 336,\ b = 180$

Example: $12 = 156 - 6 \cdot 24 = 156 - 6 \cdot (180 - 156) =$

$= 7 \cdot 156 - 6 \cdot 180 = 7 \cdot (336 - 180) - 6 \cdot 180 =$

$= 7 \cdot 336 - 13 \cdot 180$

$\gcd(a, b)$

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.

(1) $d \mid a$ and $d \mid b \Rightarrow d \mid ax + by$ $\forall (x, y)$ integers $\Rightarrow ax + by = d\mathbb{Z}$

(2) Corollary 1 $\Rightarrow \exists\, x, y : ax + by = d \Rightarrow kax + kby = kd$ $\forall k \in \mathbb{Z}$

Bezout's theorem

Theorem

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

$\gcd(a,b) = 1$

This is a particular case of Corollary 2. .

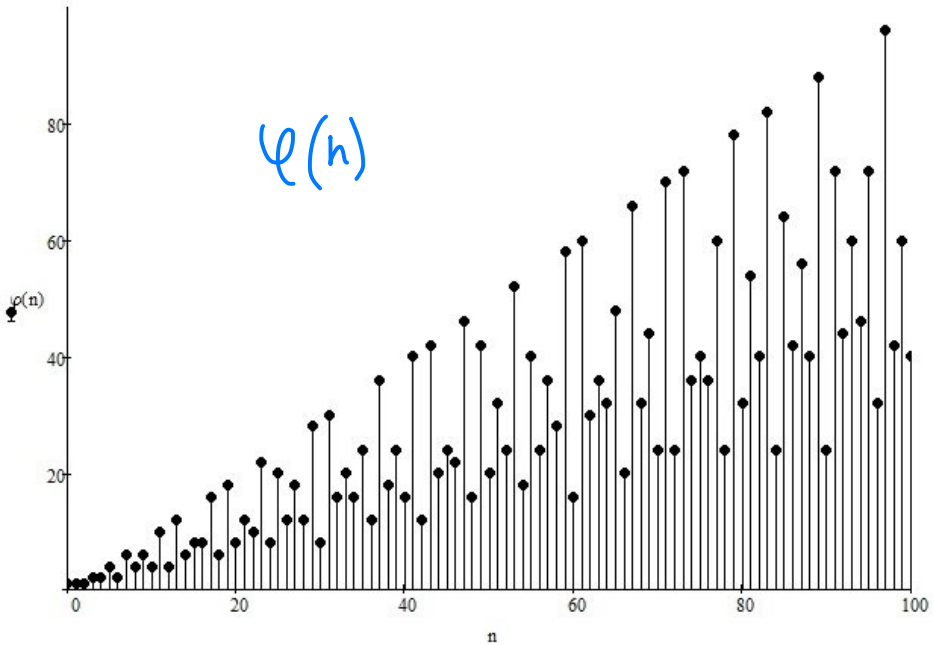
Conclusion: basic properties of $\mathbb{Z}$:

(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 $\gcd(n, k) = 1$.



$\varphi(n)$

$\varphi(2) = 1$

$\varphi(3) = 2$

$\varphi(19) = 18$

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

$\varphi(15) = 8$

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

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

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

Let p be a prime.

Poll: $\varphi(p^2) =$

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

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

C: $p^2 - p$

D: $p^2 - 1$.

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

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

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

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

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

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

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