Discrete Algebraic Structures

WiSe 2025/2026

Prof. Dr. Antoine Wiehe
Research Group for Theoretical Computer Science

Definition. Let $d \geq 2$. Define $a \equiv_d b$ by "b and b' have the same remainder in the division by d". We then say that a and b are congruent modulo d.

Equivalence relation with d equivalence classes Set of equivalence classes: $\mathbb{Z}/d\mathbb{Z}$

Definition. We define addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ as follows:

- $[a]_d + [b]_d$ is defined to be $[a+b]_d$
- $[a]_d \times [b]_d$ is defined to be $[a \times b]_d$

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

$\times$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

Definition. Let $a \in \mathbb{Z}$. An inverse of a modulo d is a number $b \in \mathbb{Z}$ such that $a \times b \equiv_d 1$.

Theorem. Let $a \in \mathbb{Z}$ and $d \geq 2$. Then a has an inverse modulo d if, and only if, a and d are coprime.

Definition. Let $n \geq 1$. Define $\varphi(n)$ to be the number of numbers in $\{0, \ldots, n-1\}$ that have an inverse modulo n.

$$\varphi(n) = |\{a \in \{0, \ldots, n-1\} \mid \gcd(a, n) = 1\}|$$

n	1	2	3	4	5	6	7	8	9
	$\{0\}$	$\{1\}$	$\{1,2\}$	$\{1,3\}$	$\{1,2,3,4\}$	$\{1,5\}$	$\{1,2,3,4,5,6\}$	$\{1,3,5,7\}$	$\{1,2,4,5,7,8\}$
$\varphi(n)$	1	1	2	2	4	2	6	4	6

Theorem. Let n have prime decomposition $p_1^{e_1} \times \cdots \times p_k^{e_k}$. Then $\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1}$.

Theorem (Fermat's little theorem)**.** If a and n are coprime, then $a^{\varphi(n)} = 1 \bmod n$.

Theorem. Let m, n be coprime. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x & = & a \bmod m \\ x & = & b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \ldots, mn - 1\}$.

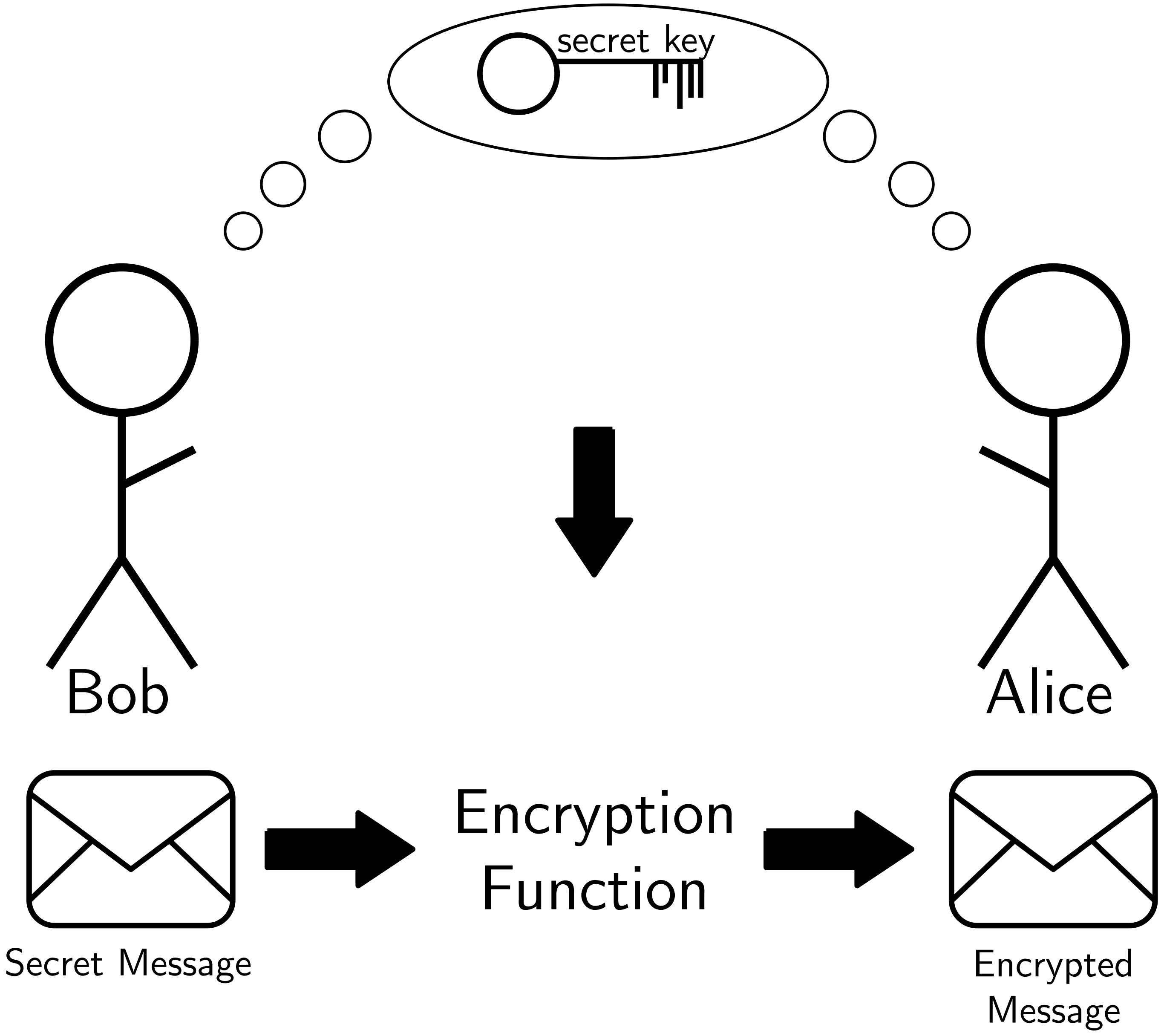
Proof of existence:

- Let u, v be the Bézout coefficients for m, n:
$$um + vn = 1$$
- Define $x = umb + vna$
- Divide x by mn with remainder to get a solution in $\{0, \ldots, mn - 1\}$

Proof of uniqueness:

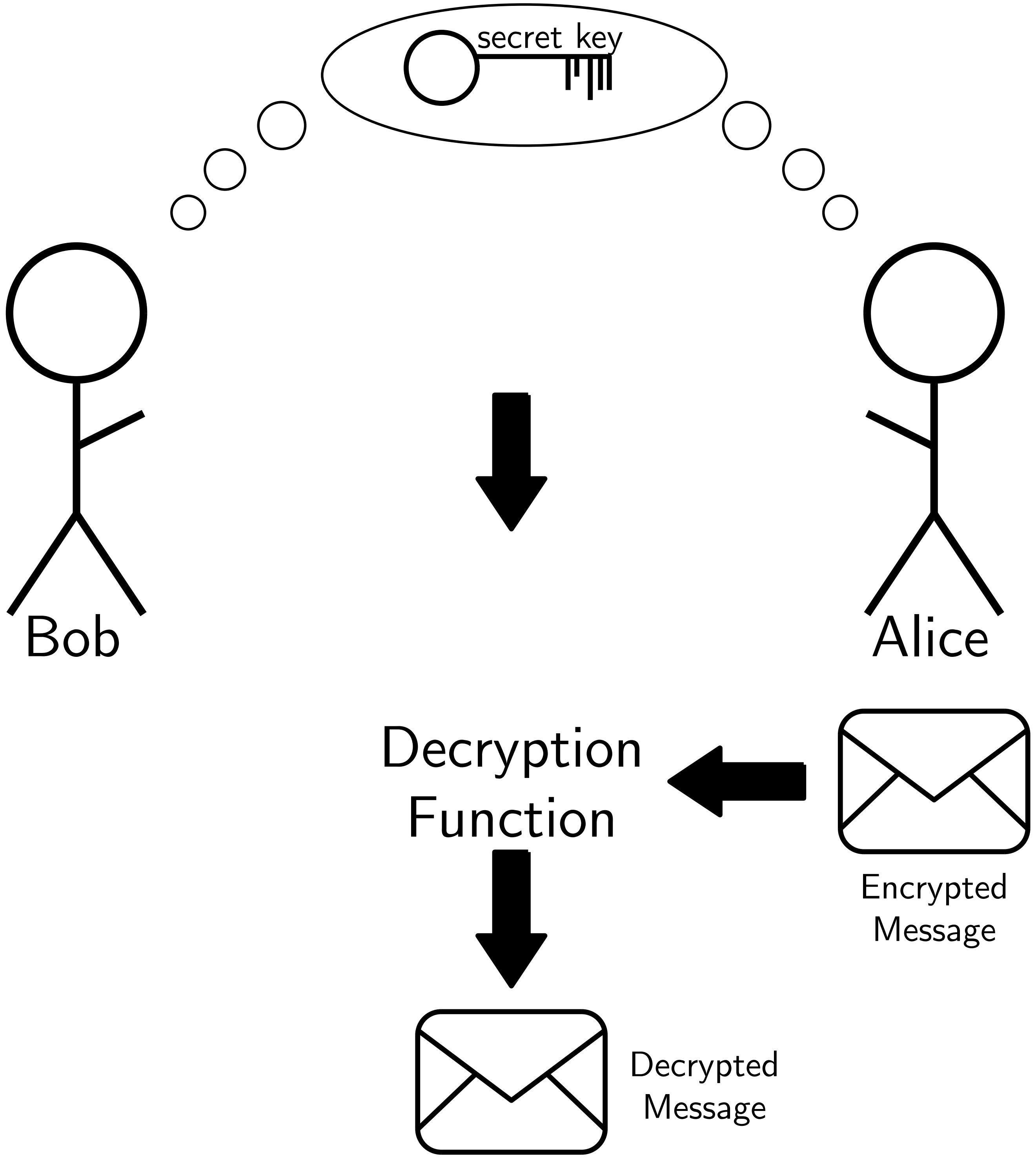
- Define $f\colon \{0, \ldots, mn - 1\} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $f(x) = ([x]_m, [x]_n)$
- We proved that f is... surjective
- Since the domain and codomain have same size, f must be injective!
- This means
  if $[x]_m = [y]_m$ and $[x]_n = [y]_n$, then $x = y$.

Symmetric Cryptography



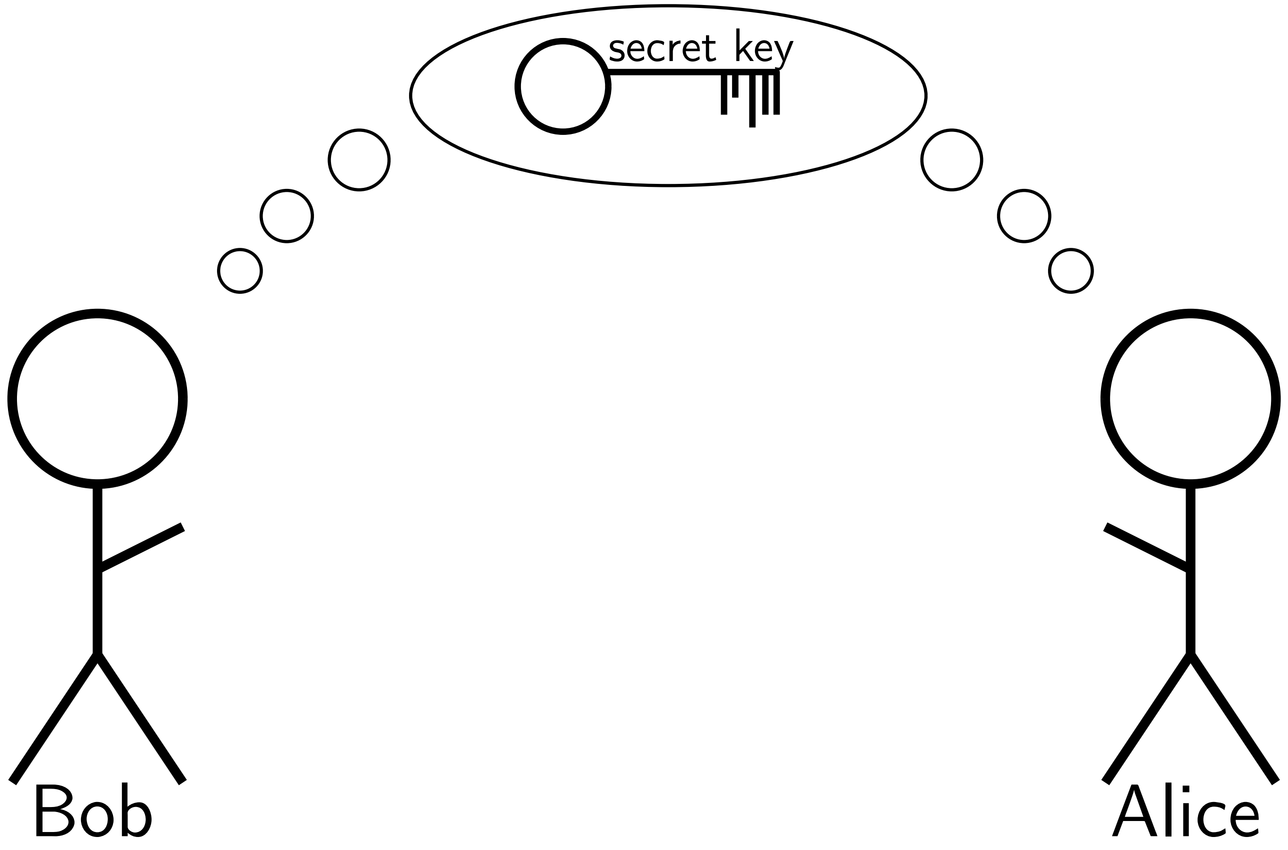
Asymmetric Cryptography

Symmetric Cryptography

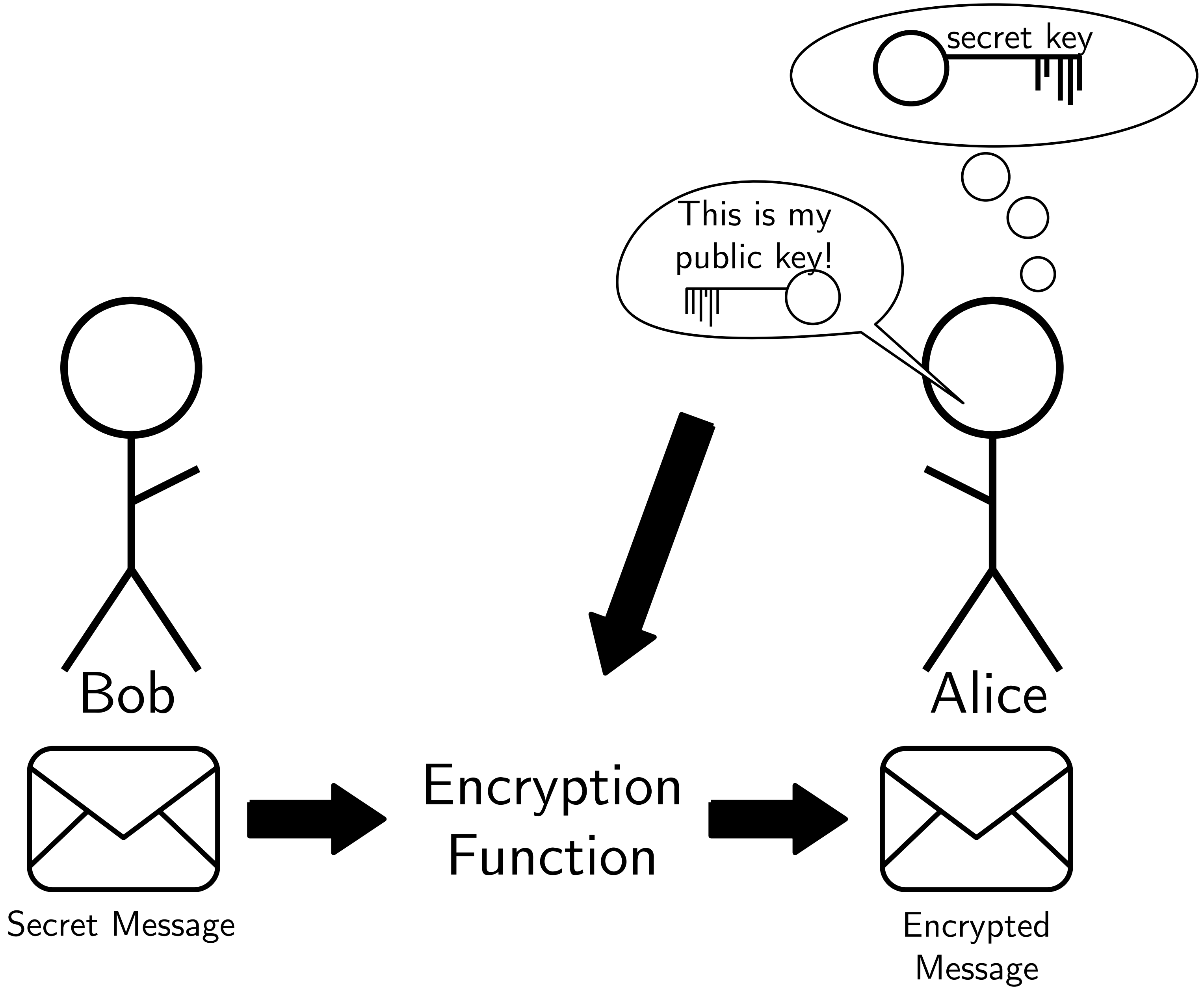


Asymmetric Cryptography

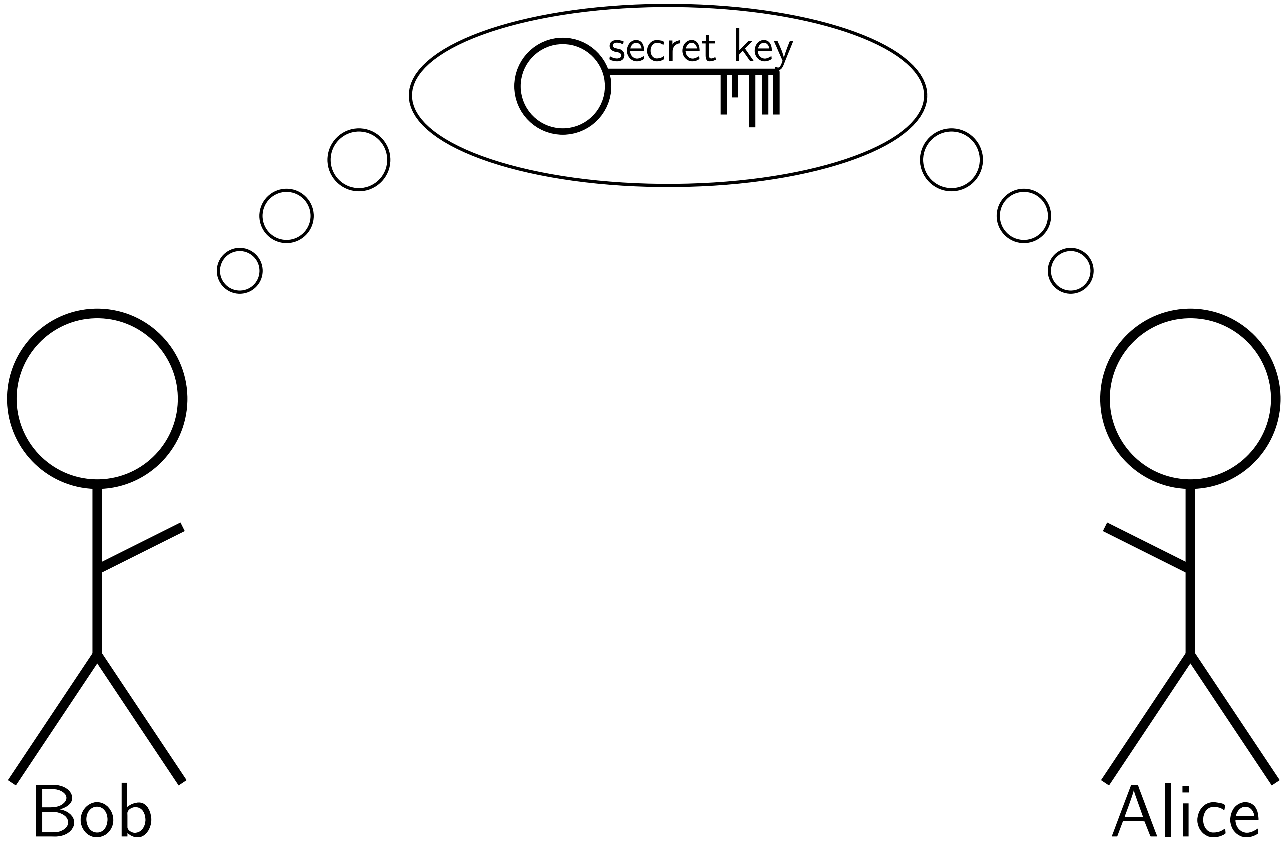
Symmetric Cryptography



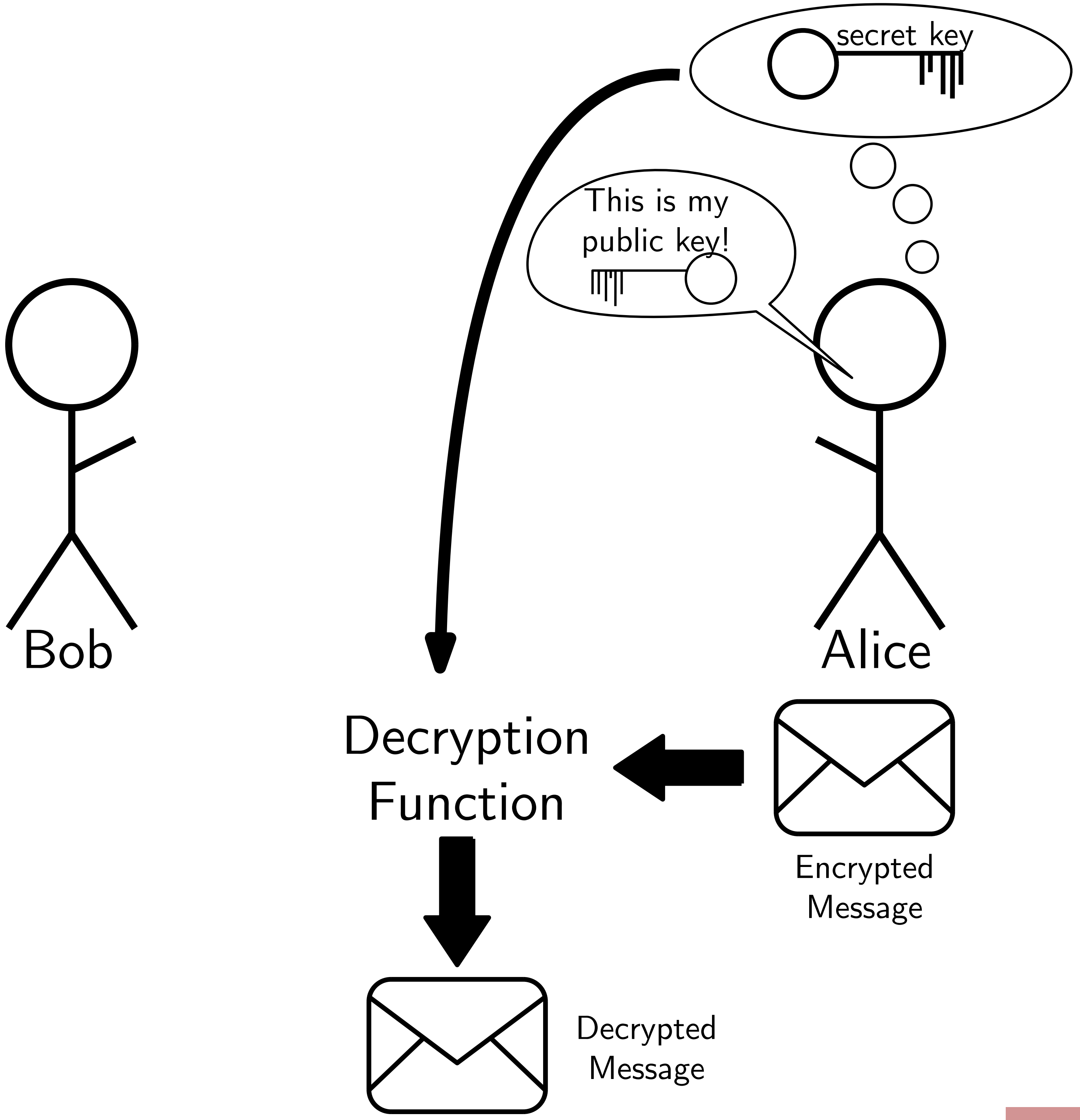
Asymmetric Cryptography



Symmetric Cryptography



Asymmetric Cryptography



Advantages compared to symmetric crypto:

- If n people want to write Alice, no need for Alice to create n different keys
- Can also be used to sign messages

- Keys and messages are (tuples of) numbers
- Messages can be seen as elements of $\mathbb{Z}/n\mathbb{Z}$
- Example of RSA key: `~/.ssh/id_rsa.pub`


```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQD6LhW7+bdi195HW/D3SHMUX7F8KZrgtfyns+o1hRBRJPmrbvy8ZQu/
LkZE8iNGP4Ti7gYXom4XyC3DkSmtafm+nofy73lnvFlG5QvQxtfaBHT15IHHNXxiFHo6wt+MCVIMFu/JFtxOmQJSn8NB
F46zfYMgKVWEiTNPK2f4HERVkKNh41gB2JNzaxDg8TEnhlft4t2HpL8eLhzpxvUjusBw+2hz7bfzGVSgrIVYcw9MBcTR
aRFRcZMnXaUe7BiySHTKLCS1Ysc1UXrdLg8qGSMHH2vT1gUY/VQ3EF5nmHku+4Cv894wpQbyGJ02fK1e/Vd/pbI43lDX
tiEa7o4uE9oKGpp6tbq6AH1HzVHjFAnYk5sBoEFg4fd+VEaxn5BIH3Al9mpsbfaO0064DqyHsX4D8nkvh1wo7cpvW3ex
HBq/3bxFW6HKPn72Qe0xLevDfDe2tekiBtwVesiKs92S1xh2Z484FbriBPtdsFF1pyk/y9ya1vjqt4fxI8aNqrcqfyM=
```

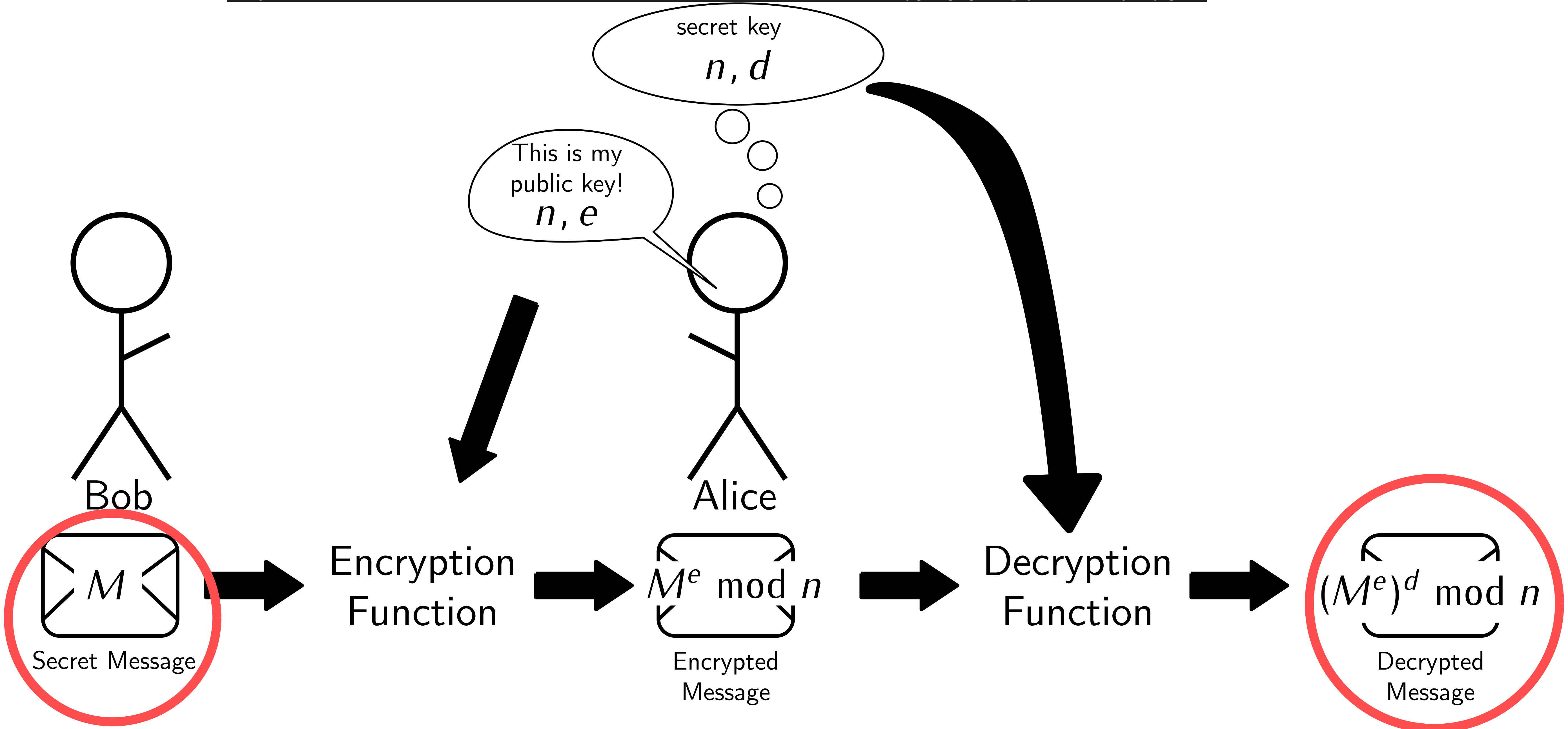

Number in base 64

n = 567752866840011746463544500936886250111400065730849894156245297798167124819633453907235687927854028945433075256023603482475622628050511765625505980788742387062054421146689095340381118003785492882129905187238916640972959096441189338863022151351830828159787234959335180112414456289494975636503222293625831101234087918496698624489627407986048217152067805164292793251529563302630003531744019209469508394783908243723805010445110723595773462881437866356094601552828897330844071537942554658283748195897751011494536163615797581537457128657029463801514647301329649523994176665505421933227765799135681549359968831573569986337714436450544812478862975125067800964594296674382038955759213491052482927648527076026788125273283304395462832426134277909014890731330177488217345012351709590633503895934397591422774726484312206203793262015314021839217793300991829666712747175627185177612969282716497065323469353415915994982154493436821268558621 and e = 17

- Keys and messages are (tuples of) numbers
- Messages can be seen as elements of $\mathbb{Z}/n\mathbb{Z}$
- Example of RSA key: `~/.ssh/id_rsa.pub`

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQD6LhW7+bdi195HW/D3SHMUX7F8KZrgtfyns+o1hRBRJPmrbvy8ZQu/
LkZE8iNGP4Ti7gYXom4XyC3DkSmtafm+nofy73lnvFlG5QvQxtfaBHT15IHHNXxiFHo6wt+MCVIMFu/JFtxOmQJSn8NB
F46zfYMgKVWEiTNPK2f4HERVkKNh41gB2JNzaxDg8TEnhlft4t2HpL8eLhzpxvUjusBw+2hz7bfzGVSgrIVYcw9MBcTR
aRFRcZMnXaUe7BiySHTKLCS1Ysc1UXrdLg8qGSMHH2vT1gUY/VQ3EF5nmHku+4Cv894wpQbyGJ02fK1e/Vd/pbI43lDX
tiEa7o4uE9oKGpp6tbq6AH1HzVHjFAnYk5sBoEFg4fd+VEaxn5BIH3Al9mpsbfaO0064DqyHsX4D8nkvh1wo7cpvW3ex
HBq/3bxFW6HKPn72Qe0xLevDfDe2tekiBtwVesiKs92S1xh2Z484FbriBPtdsFF1pyk/y9ya1vjqt4fxI8aNqrcqfyM=

Number in base 64



Want: n, e, d such that $(M^e)^d = M \bmod n$ for all $M \in \mathbb{Z}/n\mathbb{Z}$

Key generation:

- Choose distinct prime numbers p and q
- $n := pq$
- $e \in \{2, \ldots, \varphi(n) - 1\}$ coprime with $\varphi(n)$
- d inverse of e modulo $\varphi(n)$

Theorem. RSA works: for all $M \in \mathbb{Z}/n\mathbb{Z}$, we have $(M^e)^d = M \bmod n$.

Part 5: Algebra

- Cryptography
- Error correction
- Quantum Computing

Part 3: Combinatorics and counting

- Runtime analysis of algorithms
- Basics of probabilities

Part 4: basic number theory

Part 2: Graphs and relations

- Representing data and relationships between things
- Important basis for the rest of your studies (in particular "Algorithms and Data Structures")

Part 1: introduction to mathematics

- Sets
- Basics in logic and proofs

Algebra: study of **operations** and **equations** on *stuff*

Number theory

Boolean algebra

Numbers: $+, \times, 1/x, 1, 0$

Matrices: $+, \times, M^{-1}, I, 0$

Sets: $\cap, \cup, \times, \Delta, \emptyset, \dots$

Functions: $\circ, f^{-1}, \mathrm{Id}_A$

Booleans: $\wedge, \vee, \Rightarrow, \neg, \top, \bot$

Relations: $\circ, R^T, \mathrm{Id}, \cup, \cap, \times, \dots$

Linear algebra

Relational algebra

Modular arithmetic: $+,\ \times,\ [a]_d^{-1}, [1]_d, [0]_d$

Introduction to Abstract Algebra

Abstract means **not concrete**

Abstract	**Concrete**
Structures with multiplication, neutral elements	Relations: $\circ$, Id
Structures with multiplication, inverses, neutral elements	Real Numbers: $\times$, $1/x$, 1 Matrices: $\times$, M^{-1}, I Bijective Functions: $\circ$, f^{-1}, Id_A Modular arithmetic: $\times$, $[a]_d^{-1}$, $[1]_d$
Structures with meet and join (and maximal/minimal elements)	Booleans: $\wedge, \vee, \top, \bot$ Numbers: $\wedge, \vee, 0, 1$

Definition of abstract object that
; we know

Concrete examples we want to study

for example, Fermat's little theorem

Tip: have many examples in mind to not be overwhelmed

Identify some properties that are important in the concrete case

General theorems about all our examples

Definition. An internal composition law or binary operation on A is a function $\circ \colon A^2 \to A$.

We write $a \circ b$ instead of $\circ(a, b)$.

- If A is finite, a binary operation can be drawn by a Cayley table:

Example.

	a	b	c
a	a	b	c
b	b	c	a
c	c	b	b

- If A is infinite, we usually give some kind of formula:

Example. Law on $\mathbb{N}$: $n \circ m := nm + n + m + 1$

$5 \circ 3 = 24 \qquad 1 \circ 3 = 8$

Only property to check: for every $a, b \in A$, $a \circ b$ is an element of A

For the following operations, decide if they are internal composition laws:

- Addition/Multiplication on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$
- Addition of vectors in $\mathbb{R}^n$
- Addition and multiplication of $n \times n$ matrices
- Composition of functions $A \to A$
- Subtraction of natural numbers
- Division of real numbers
- Scalar product in $\mathbb{R}^n$: $v \circ w = v_1 w_1 + v_2 w_2$

Definition. An internal composition law or binary operation on A is a function $\circ \colon A^2 \to A$.

We write $a \circ b$ instead of $\circ(a, b)$.

- If A is finite, a binary operation can be drawn by a Cayley table:

Example.

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	b	b

- If A is infinite, we usually give some kind of formula:

Example. Law on $\mathbb{N}$: $n \circ m := nm + n + m + 1$

$5 \circ 3 = 24 \qquad 1 \circ 3 = 8$

Only property to check: for every $a, b \in A$, $a \circ b$ is an element of A

For $v, w \in \mathbb{R}^3$, define $v \wedge w := \begin{pmatrix} v_2 w_3 - v_3 w_2 \\ v_3 w_1 - v_1 w_3 \\ v_1 w_2 - v_2 w_1 \end{pmatrix}$.

Is $\wedge$ an internal composition law on $\mathbb{R}^3$?

Definition. An internal composition law or binary operation on A is a function $\circ\colon A^2 \to A$.

We write $a \circ b$ instead of $\circ(a, b)$.

- If A is finite, a binary operation can be drawn by a Cayley table:

Example.

	a	b	c
a	a	b	c
b	b	c	a
c	c	b	b

- If A is infinite, we usually give some kind of formula:

Example. Law on $\mathbb{N}$: $n \circ m := nm + n + m + 1$

$5 \circ 3 = 24 \qquad 1 \circ 3 = 8$

Only property to check: for every $a, b \in A$, $a \circ b$ is an element of A

For $v \in \mathbb{R}^3$ and $\lambda \in \mathbb{R}^3$, define $\lambda \circ v := \begin{pmatrix} \lambda v_1 \\ \lambda v_2 \\ \lambda v_3 \end{pmatrix}$.

Is $\circ$ an internal composition law on $\mathbb{R}^3$?

Definition. Let $\circ$ be an internal composition law on A. We say that it:

- is associative if for all $a, b, c \in A$, we have $a \circ (b \circ c) = (a \circ b) \circ c$ (parentheses don't matter)
- is commutative if for all $a, b \in A$, we have $a \circ b = b \circ a$ (order doesn't matter)
- has a neutral element if there exists $e \in A$ such that for all $a \in A$, $e \circ a = a \circ e = a$

Notation (Multiplicative/Exponent notation)**.** For $n > 0$: a^n: $a \circ \cdots \circ a$.

If $\circ$ is commutative, we can use the additive notation instead:

Notation. Let $+$ be a commutative internal composition law on A.
We define $n \cdot a$ by $a + \cdots + a$.

Definition. Let $\circ$ be an internal composition law on A. We say that it:

- is associative if for all $a, b, c \in A$, we have $a \circ (b \circ c) = (a \circ b) \circ c$ (parentheses don't matter)
- is commutative if for all $a, b \in A$, we have $a \circ b = b \circ a$ (order doesn't matter)
- has a neutral element if there exists $e \in A$ such that for all $a \in A$, $e \circ a = a \circ e = a$

$(A, \circ)$ is a **monoid**: if $\circ$ is associative and has a neutral element

commutative monoid: if $\circ$ is associative, commutative, and has a neutral element

Examples. The following are monoids:

- $(\mathbb{N}_0, +)$
- $(\mathbb{Z}, +)$
- $(\mathbb{N}, \times)$
- $(\{0, 1\}^*, \text{concat})$
- $(A^A, \circ)$
- $\ldots$

Let M be the set of all $n \times n$ matrices.
Is $(M, \times)$ a monoid?

Theorem. Let $\circ$ be an internal composition law.
There can be at most one neutral element for $\circ$.

Definition. Let $(A, \circ)$ be a monoid and $a, b \in A$.
b is an inverse of a if $a \circ b = b \circ a = e$.

$(A, \circ)$ is a group if $\circ$ is associative, has a neutral element, and **every** element of A has an inverse.

Intuition: elements in A represent actions that can be reversed

Groups are extremely important in science:

- Quantum theory
- Quantum computing: allowed operations form a group
- Cryptography
- Discrete Fourier transform: Signal processing and other things
- Study of polynomial equations and their solutions

Definition. Let $(A, \circ)$ be a monoid and $a, b \in A$.
b is an inverse of a if $a \circ b = b \circ a = e$.

$(A, \circ)$ is a group if $\circ$ is associative, has a neutral element, and **every** element of A has an inverse.

Intuition: elements in A represent actions that can be reversed

Examples. The following are groups:

- $(\mathbb{R}, +)$
- $(\mathbb{Z}, +)$
- (bijective functions $A \to A, \circ$)
- $(\mathbb{Z}/3\mathbb{Z}, \times)$

Is $(\mathbb{R}, \times)$ a group?

Definition. Let $(A, \circ)$ be a monoid and $a, b \in A$.
b is an inverse of a if $a \circ b = b \circ a = e$.

$(A, \circ)$ is a group if $\circ$ is associative, has a neutral element, and **every** element of A has an inverse.

Intuition: elements in A represent actions that can be reversed

Examples. The following are groups:

- $(\mathbb{R}, +)$
- $(\mathbb{Z}, +)$
- (bijective functions $A \to A, \circ$)
- $(\mathbb{Z}/3\mathbb{Z}, \times)$

Theorem. Any $a \in A$ has at most one inverse.

- The inverse of a is written a^{-1}.
- Usual rules of exponentiation are true: $a^p = (a^{-p})^{-1}$ for $p < 0$

Theorem. Let $(A, \circ)$ be a group, and let a, b be such that $a \circ b = e$. Then $b \circ a = e$. (So b is the inverse of a.)

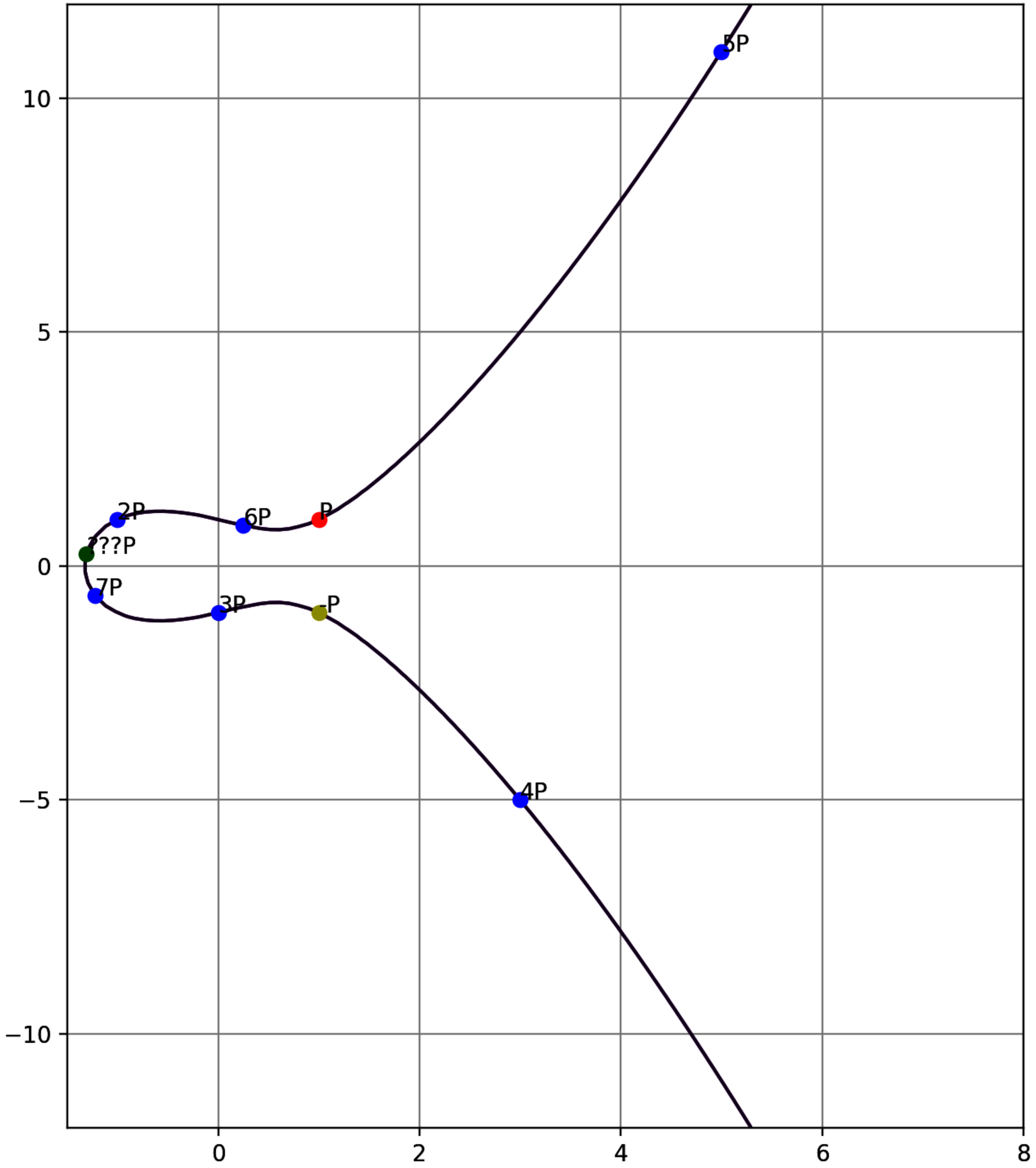
- Quaternion group Q_8
  - elements are $\{1, -1, i, -i, j, -j, k, -k\}$
  - operation given by the table

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Find the neutral element and the inverse of $-j$

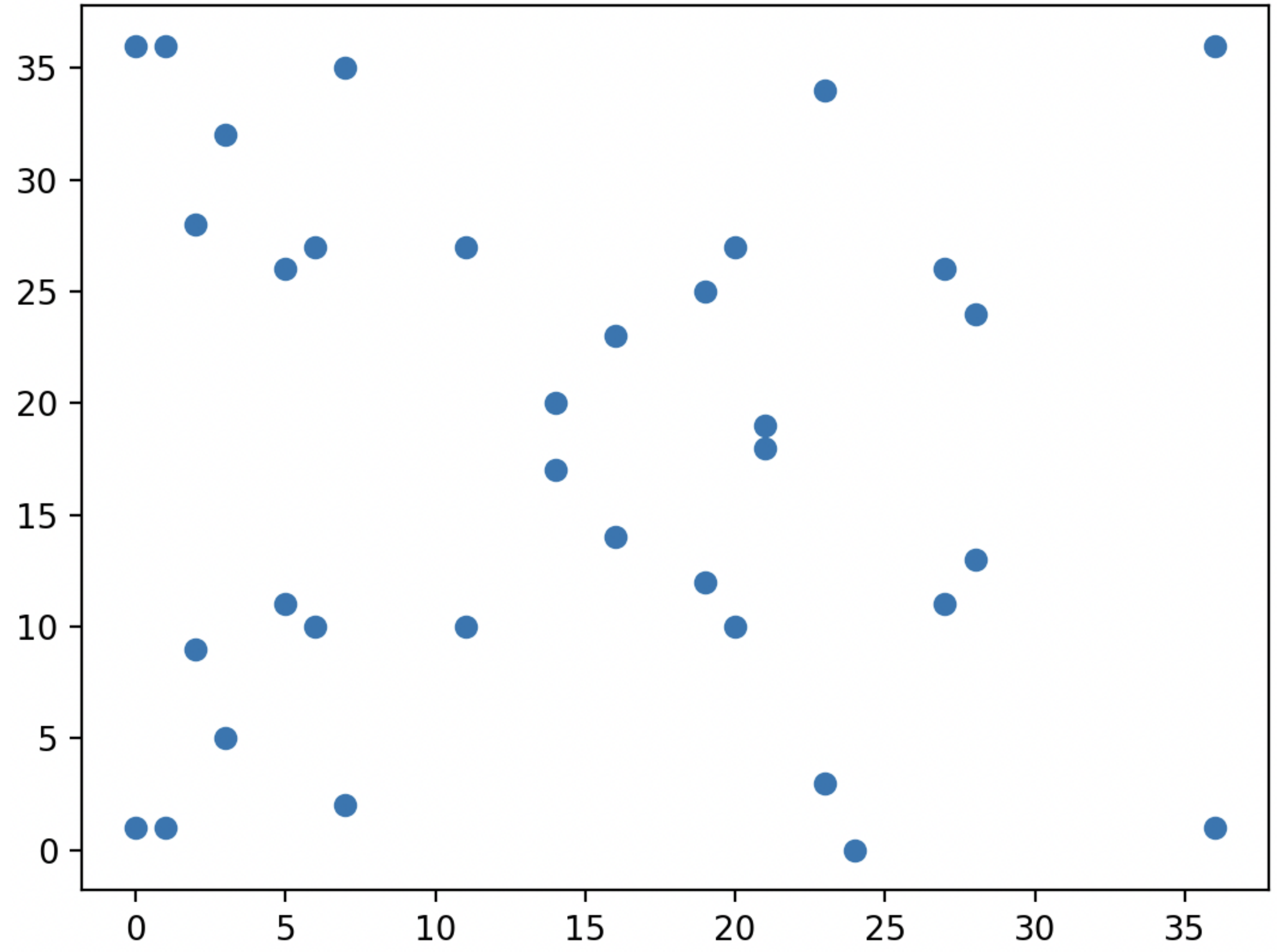
Applications: coordinates / movement in 3d.
- computer graphics
- motion planning for robots
- VR

- Elliptic curves
  - elements: set of pairs (x, y) such that $y^2 = x^3 + ax + b$ (for some fixed a, b)
  - there is a way to "multiply" points
  - this is a commutative group



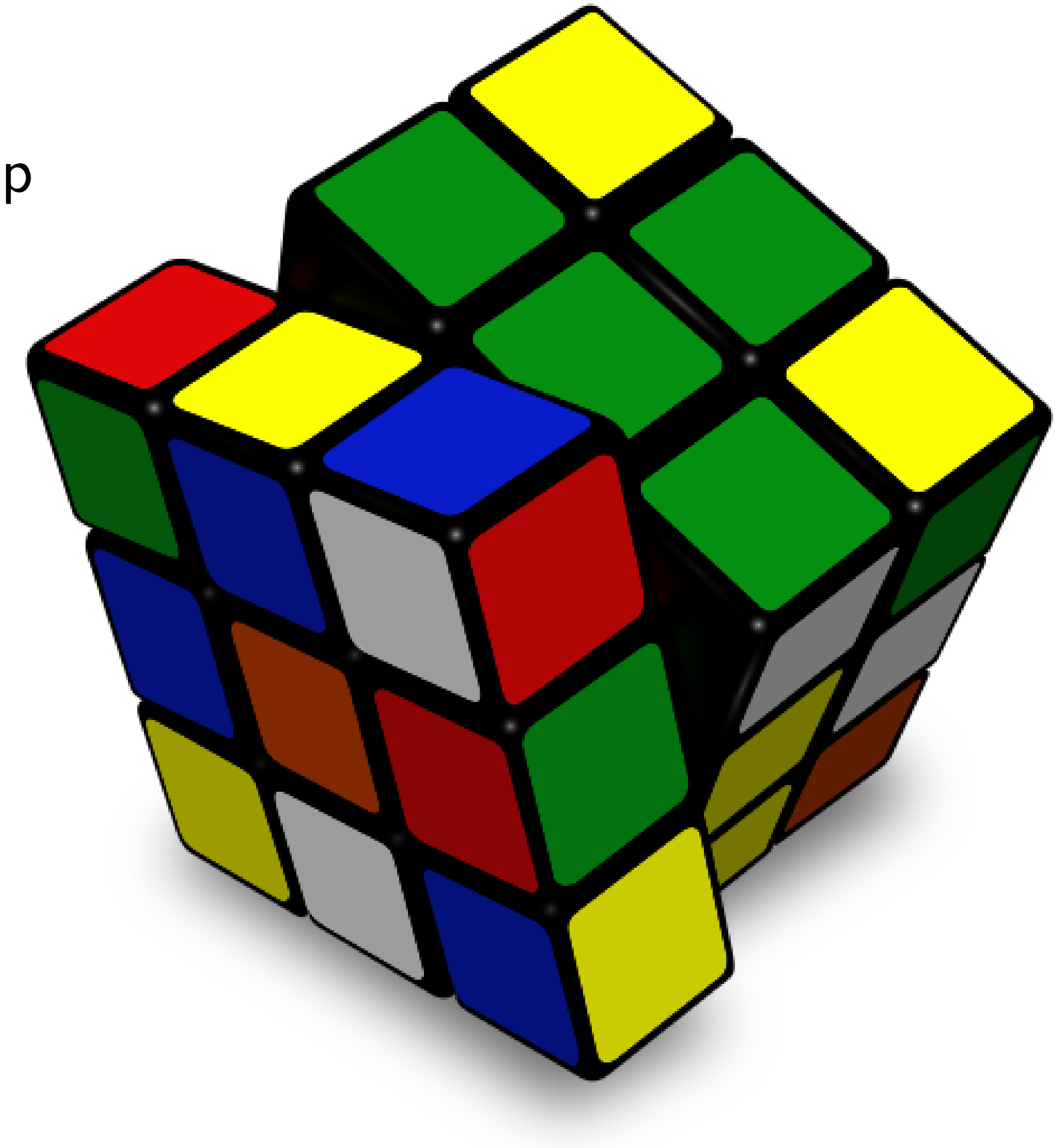
- Elliptic curves
  - elements: set of pairs (x, y) such that $y^2 = x^3 + ax + b$ (for some fixed a, b)
  - there is a way to "multiply" points
  - this is a commutative group

Application: elliptic curve cryptography
- Private key is an integer d
- Public key is the point $d \cdot P$



Points have coordinates in $\mathbb{Z}/37\mathbb{Z}$

- Rubik's cube
  - Elementary moves of the cube: F, B, U, D, L, R
  - Each position of the cube can be written as a sequence $FULR^{-1}\ldots$ of moves starting from a solved cube
  - Each move can be "undone" $\rightsquigarrow$ inverse elements $\rightsquigarrow$ group
  - $|G| > 43 \times 10^{18}$



Proof of Fermat's little theorem*

Antoine Wiehe

Theorem (Fermat's little theorem)**.** If a and n are coprime, then $a^{\varphi(n)} = 1 \bmod n$.

What does it have to do with groups?

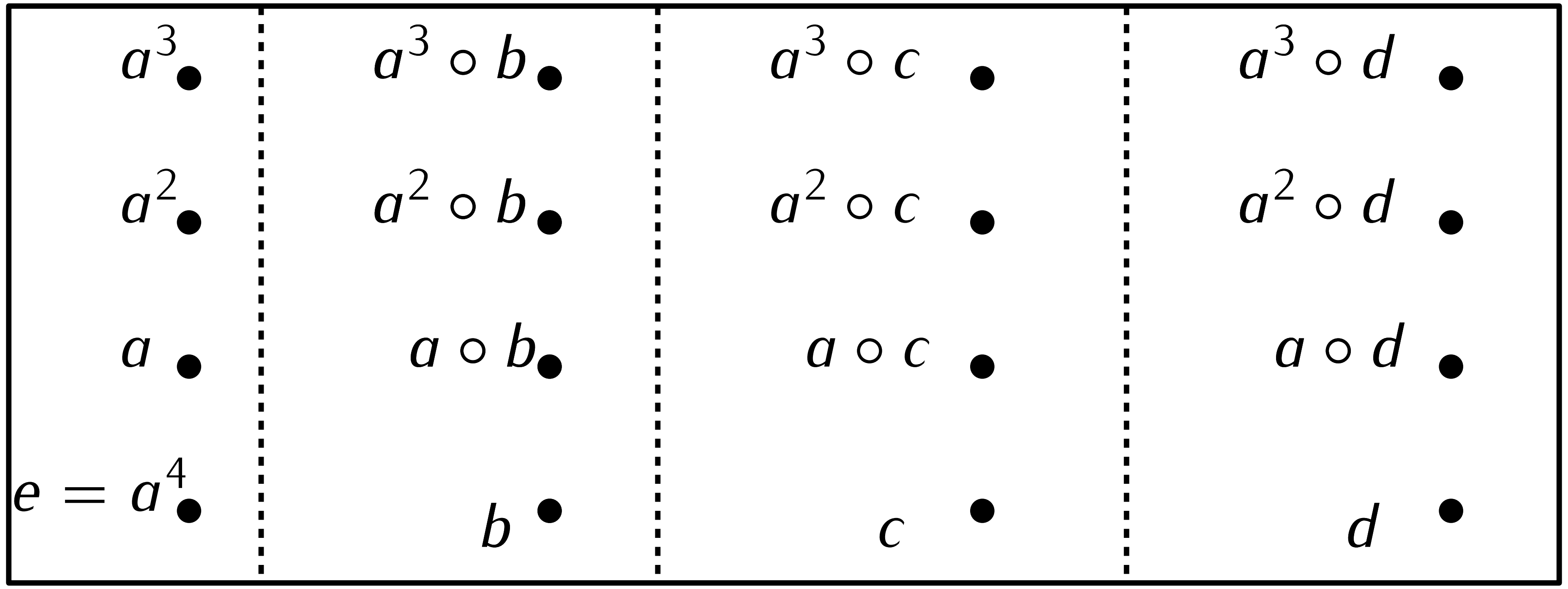
Theorem. Let U_n be the set of $[a] \in \mathbb{Z}/n\mathbb{Z}$ such that a coprime with n. Then $(U_n, \times)$ is a group.

Theorem. Let $(G, \circ)$ be a finite group and $a \in G$. Then $a^{|G|} = e$.

Step 1: For some $n > 0$, we have $a^n = e$

Step 2: define $b \sim c$ if $a^k \circ b = c$ for some $k \in \mathbb{Z}$

Step 3: all equivalence classes have the same size



Theorem **(Fermat's little theorem).** If a and n are coprime, then $a^{\varphi(n)} = 1 \bmod n$.

What does it have to do with groups?

Theorem. Let U_n be the set of $[a] \in \mathbb{Z}/n\mathbb{Z}$ such that a coprime with n. Then $(U_n, \times)$ is a group.

Theorem. Let $(G, \circ)$ be a finite group and $a \in G$. Then $a^{|G|} = e$.

The smallest $n > 0$ such that $a^n = e$ is called the order of a.

- definitions of associativity, commutativity, neutral element, inverses
- be able to check if some $(A, \circ)$ is a monoid/group
- definition of the order of an element
- be comfortable with the notation

	associative	neutral element	inverses
monoid	✓	✓	
group	✓	✓	✓