Lecture 7

Discrete logarithm problems, handbook RSA

Stefan Dziembowski

www.crypto.edu.pl/Dziembowski

University of Warsaw

23.11.16 **version 1.0**

Plan

1. Discrete logarithm problem
    1. over $\boldsymbol{Z}_p^*$ and its subgroups
    2. over elliptic curves
2. RSA
    1. RSA as an operation over $\boldsymbol{Z}_N^*$
    2. algebraic properties of RSA
    3. algorithmic question about quadratic residues over $\boldsymbol{Z}_N^*$
    4. group $\boldsymbol{Z}_N$ vs $\boldsymbol{Z}_N^*$

From the last exercises:

$f : \{0, \ldots, p-1\} \rightarrow Z_p^*$ defined as $f(x) = g^x$ is believed to be a **one-way function** (informally speaking),

This is an **informal statement** since the function f depends on p.

To make it formal we would need to define a notion of a **one-way function family parametrized by a parameter p** (chosen according to some distribution).

We will do it later.

A problem

$\boldsymbol{f} : \{\mathbf{0}, \dots, \boldsymbol{p} - \mathbf{1}\} \rightarrow \boldsymbol{Z}_{\boldsymbol{p}}^{*}$ defined as $\boldsymbol{f}(\boldsymbol{x}) = \boldsymbol{g}^{\boldsymbol{x}}$ is believed to be a **one-way function** (informally speaking),

but

from $\boldsymbol{f}(\boldsymbol{x})$ one can compute the **parity of** $\boldsymbol{x}$.

We now show how to do it.

Quadratic Residues

Definition

a is a **quadratic residue modulo** p if there exists b such that

$$a = b^2 \bmod p$$

$\mathbf{QR}_p$ – a set of quadratic residues modulo p

$\mathbf{QR}_p$ is a subgroup of Z_p^*

Why?

because:

- $1 \in \mathbf{QR}$
- if $a, a' \in \mathbf{QR}$ then $a \cdot a' \in \mathbf{QR}$

$$\mathbf{QNR}_p := Z_p^* \setminus \mathbf{QR}_p$$

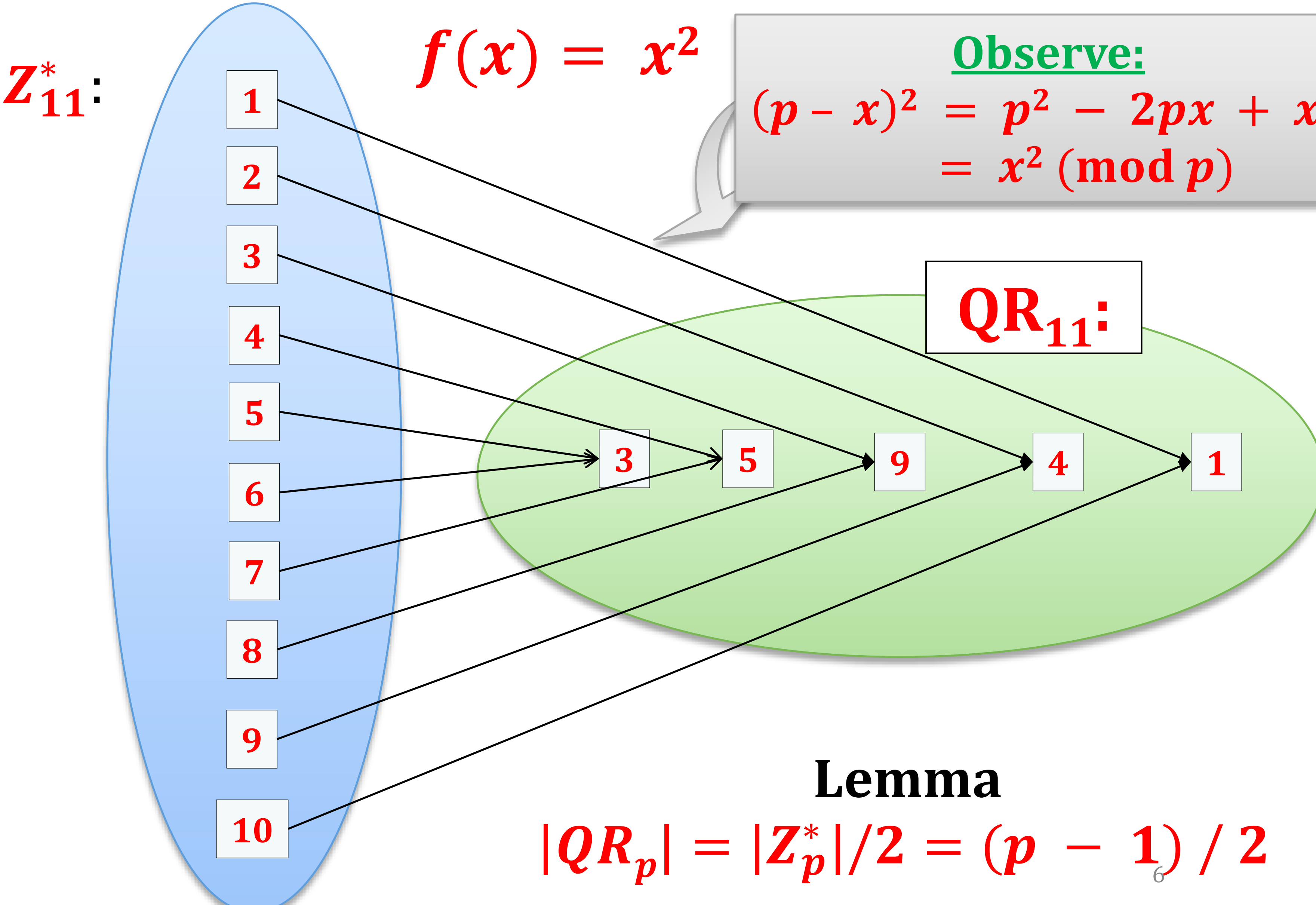
What is the size of $\mathbf{QR}_p$?

Example: $\mathbf{QR_{11}}$

$f(x) = x^2$

Observe:

$$(p - x)^2 = p^2 - 2px + x^2 = x^2 \pmod{p}$$



Lemma

$$|QR_p| = |Z_p^*|/2 = (p - 1) / 2$$

A proof that $|\mathbf{QR}_p| = (p-1)/2$

Observation

Let g be a generator of Z_p^*.

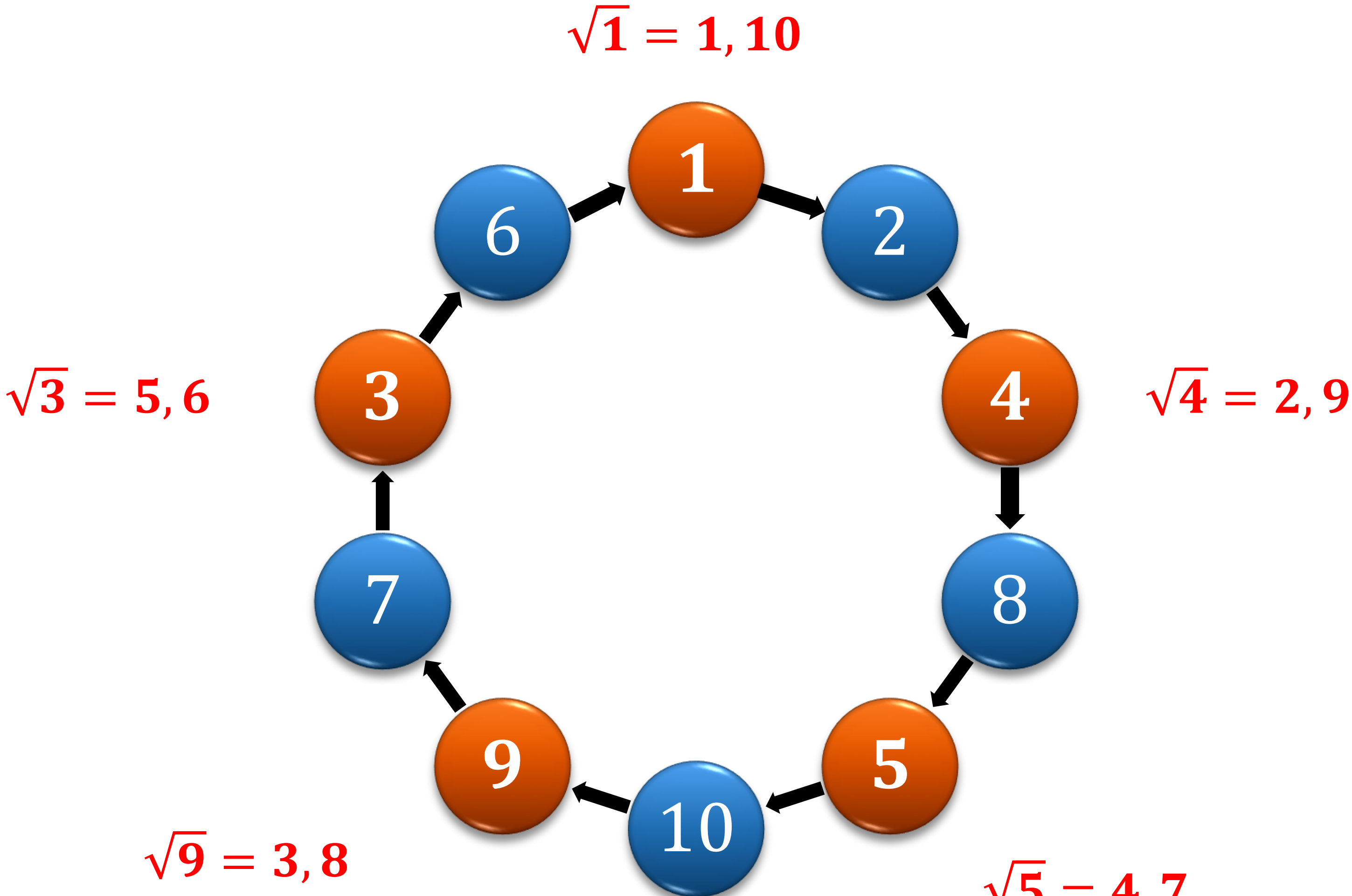
Then $\mathbf{QR}_p = \{g^2, g^4, \dots, g^{p-1}\}$.

Proof

Every element $x \in Z_p^*$ is equal to g^i for some i.

Hence $x^2 = g^{2i \bmod (p-1)} = g^j$, where j is even.

Example: $\mathbf{QR_{11} = \{1, 4, 5, 9, 3\}}$



Is it easy to test if $a \in \mathrm{QR}_p$ **Yes!**

Observation

$a \in \mathrm{QR}_p$ **iff** $a^{(p-1)/2} = 1 \pmod p$

Proof

($\Longrightarrow$)

If $a \in \mathrm{QR}_p$ then $a = g^{2i}$ (for $i \in \mathbb{N}$).

Hence:

$$\begin{aligned} a^{(p-1)/2} &= \left(g^{2i}\right)^{(p-1)/2} \\ &= g^{i \cdot (p-1)} \\ &= 1. \end{aligned}$$

$a \in \mathrm{QR}_p$ **iff** $a^{(p-1)/2} = 1 \pmod p$

($\Longleftarrow$)

Suppose a is **not a quadratic residue**.

Then $a = g^{2i+1}$ (for $i \in \mathbf{N}$). Hence

$$a^{(p-1)/2} = \left(g^{2i+1}\right)^{(p-1)/2}$$

$$= \underbrace{g^{i\cdot(p-1)}}_{=1} \cdot g^{(p-1)/2}$$

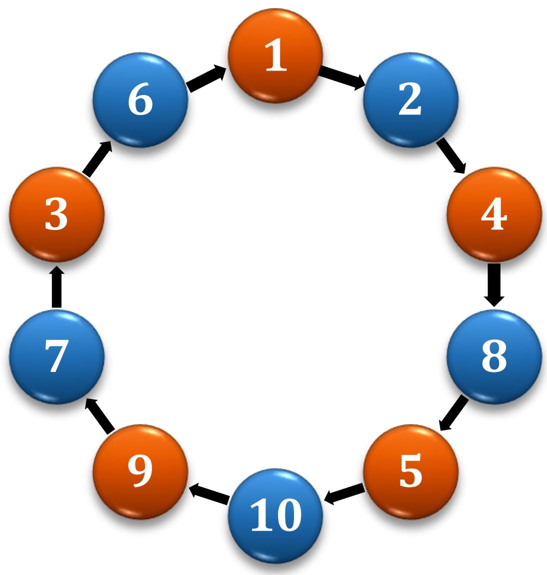
$$= g^{(p-1)/2}$$

which cannot be equal to 1 since g is a generator.

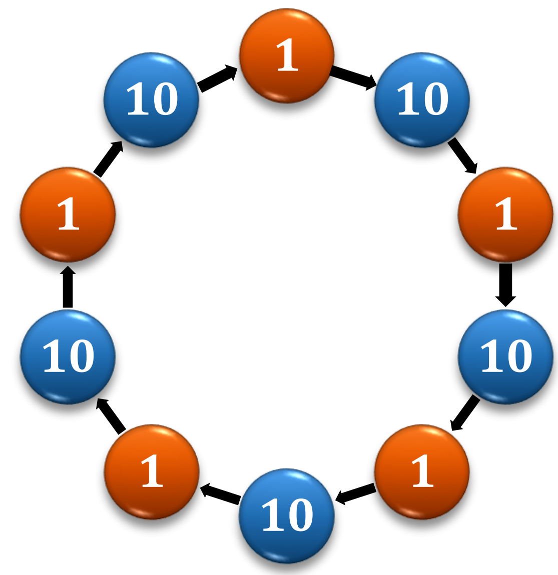
QED

Example $\boldsymbol{Z}_{11}^{*}$

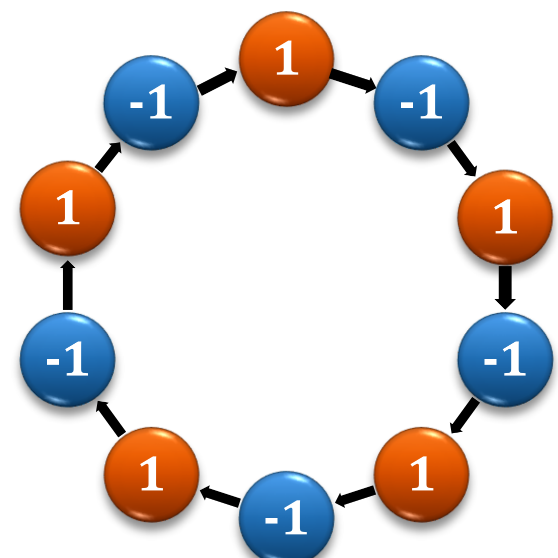
$$\frac{11-1}{2} = 5$$



$$f(x) = x^5$$



another way to look at it:



Not a coincidence:

$$x^{(p-1)/2} \in \{-1, 1\}$$

Consequence

$\boldsymbol{g}$ – a generator of $\boldsymbol{Z_p^*}$

$\boldsymbol{f}: \{\mathbf{0}, \dots, \boldsymbol{p}-\mathbf{1}\} \rightarrow \boldsymbol{Z_p^*}$ defined as $\boldsymbol{f(x) = g^x}$ is a one-way function, **but**

from $\boldsymbol{f(x)}$ **one can compute the parity of** $\boldsymbol{x}$

(by checking if $\boldsymbol{f(x)} \in$ **QR**)...

For some applications this is **not good**.

(but sometimes people don't care)

How to compute square roots modulo a prime $\boldsymbol{p}$?

Yes!

We show it only for $\boldsymbol{p = 3 \pmod 4}$ (for $\boldsymbol{p = 1 \pmod 4}$ this fact also holds, but the algorithm and the proof are more complicated).

How to compute a square root of $\boldsymbol{x}$?

Method over reals: compute $\boldsymbol{x^{\frac{1}{2}}}$

Problem: $\boldsymbol{\frac{1}{2}}$ doesn't make sense in $\boldsymbol{Z_n^*}$...

Write: $p = 4m + 3$ (where $m \in \mathbf{N}$).

Hence: $|\mathrm{QR}_p|$ is equal to:

$$\frac{p-1}{2} = \frac{4m+2}{2} = 2m+1$$

Fact: $\sqrt{x} = x^{m+1}, -x^{m+1}$

Proof:

$$\begin{aligned}\left(x^{m+1}\right)^2 &= x^{2\cdot(m+1)} \\ &= x^{2m+2} \\ &= x^{2m+1} \cdot x \\ &= x\end{aligned}$$

Of course also: $\left(-x^{m+1}\right)^2 = \left(x^{m+1}\right)^2 = x$

$x^{2m+1} = 1$
because of this

What to do?

Instead of working in $\boldsymbol{Z_p^*}$ work in its **subgroup**: $\mathbf{QR}_{\boldsymbol{p}}$

How to find a generator of $\mathbf{QR}_{\boldsymbol{p}}$?

A practical method: Choose $\boldsymbol{p}$ that is a **strong prime**, which means that:

$$\boldsymbol{p} = \mathbf{2} \cdot \boldsymbol{q} + \mathbf{1}, \text{ with } \boldsymbol{q} \text{ prime.}$$

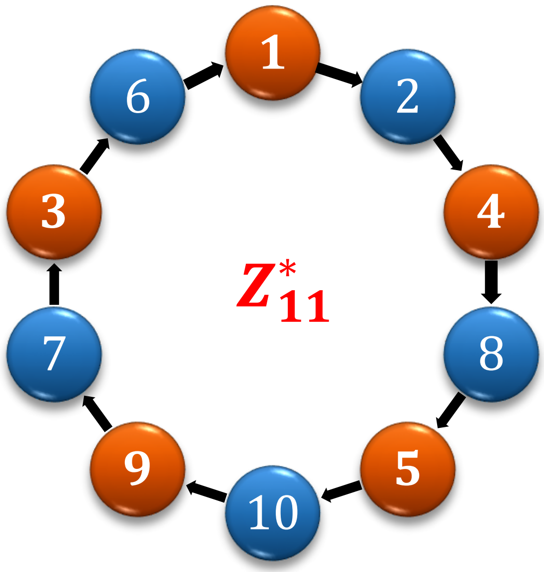
Hence: $\mathbf{QR}_{\boldsymbol{p}}$ has a **prime order** ($\boldsymbol{q}$).

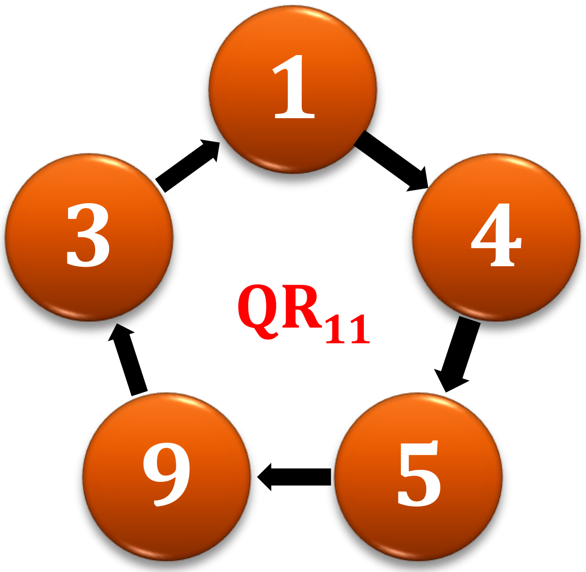
Every element (except of **1**) of a group of a prime order is its **generator**!

Therefore: every element of $\mathbf{QR}_{\boldsymbol{p}}$ is a generator.

Example

11 is a strong prime (because **5** is a prime)





Plan

1. Discrete logarithm problem
   1. over $\boldsymbol{Z_p^*}$ and its subgroups
   2. over elliptic curves
2. RSA
   1. RSA as an operation over $\boldsymbol{Z_N^*}$
   2. algebraic properties of RSA
   3. algorithmic question about quadratic residues over $\boldsymbol{Z_N^*}$
   4. group $\boldsymbol{Z_N}$ vs $\boldsymbol{Z_N^*}$

Elliptic curves over the reals

Let $\boldsymbol{a, b \in R}$ be two numbers such that

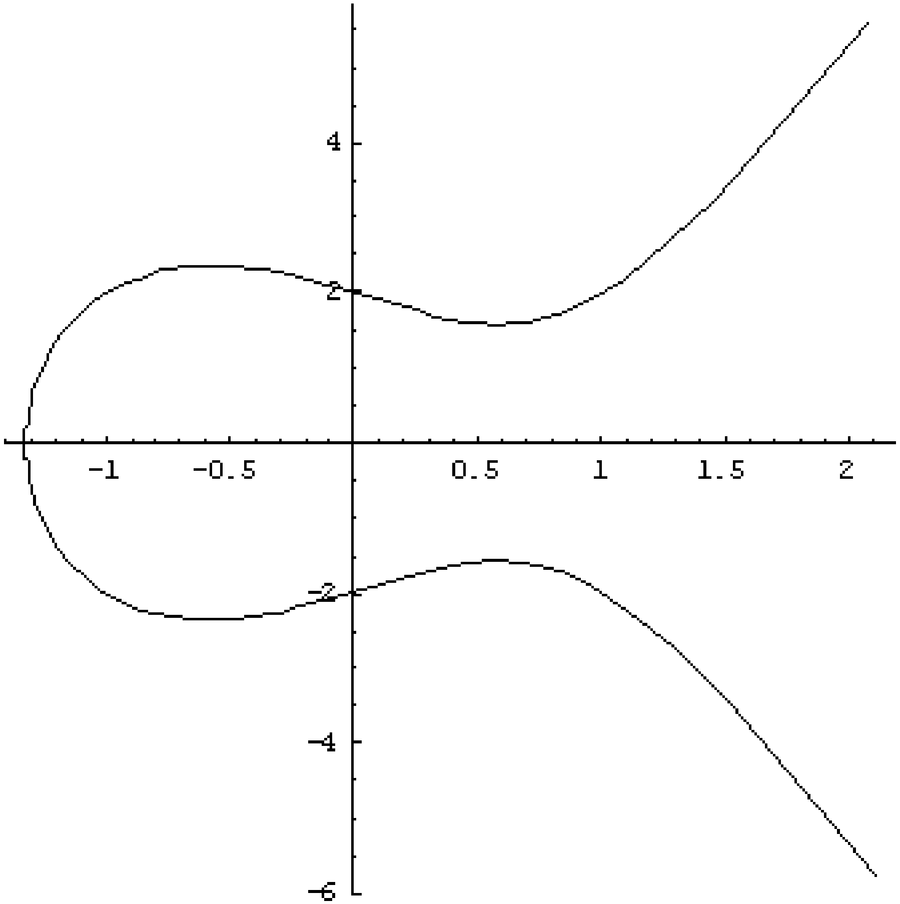
$$\boldsymbol{4a^3 + 27b^2 \neq 0}$$

A **non-singular elliptic curve** is a set $\boldsymbol{E}$ of solutions $(\boldsymbol{x, y}) \in \mathbf{R}^2$ to the equation

$$\boldsymbol{y^2 = x^3 + ax + b}$$

together with a special point $\mathcal{O}$ called the **point in infinity**.

Example $y^2 = 4x^3 - 4x + 4$



Abelian group over an elliptic curve

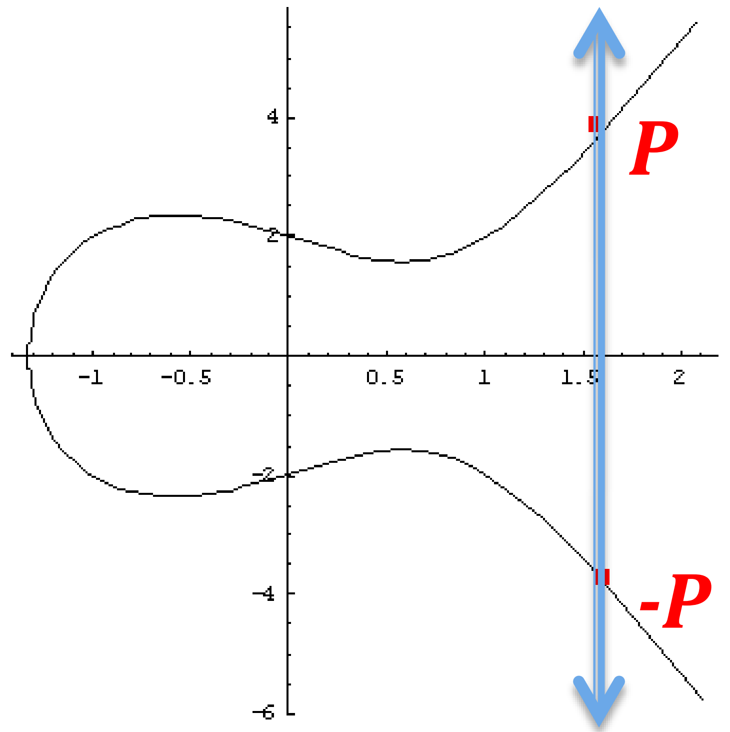
$\boldsymbol{E}$ – elliptic curve

$(\boldsymbol{E}, +)$ – a group

neutral element: $\mathcal{O}$

inverse of $\boldsymbol{P} = (\boldsymbol{x}, \boldsymbol{y})$:

$$-\boldsymbol{P} = (\boldsymbol{x}, -\boldsymbol{y})$$



“Addition”

Suppose that $\boldsymbol{P}, \boldsymbol{Q} \in \boldsymbol{E} \setminus \{\mathcal{O}\}$ where

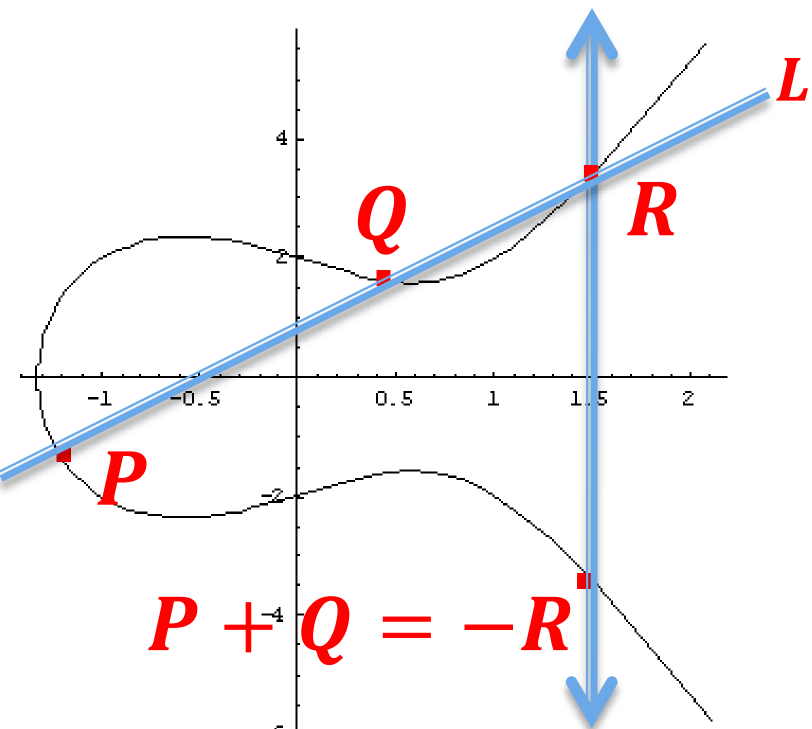
$$\boldsymbol{P} = (\boldsymbol{x_1}, \boldsymbol{y_1}) \text{ and } \boldsymbol{Q} = (\boldsymbol{x_2}, \boldsymbol{y_2}).$$

Consider the following cases:

1. $\boldsymbol{x_1 \neq x_2}$
2. $\boldsymbol{x_1 = x_2}$ and $\boldsymbol{y_1 = -y_2}$
3. $\boldsymbol{x_1 = x_2}$ and $\boldsymbol{y_1 = y_2}$.

Case 1: $x_1 \neq x_2$

$P = (x_1, y_1)$ and
$Q = (x_2, y_2)$



L – line through P and Q

Fact

L intersects E in exactly one point
$R = (x_3, y_3)$.
Where:

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

and

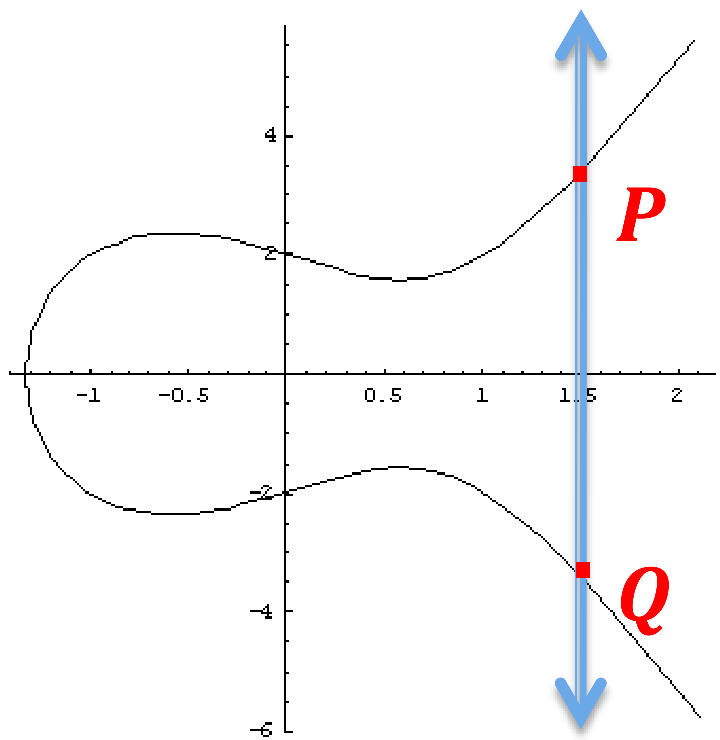
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

Case 2:

$x_1 = x_2$ and $y_1 = -y_2$

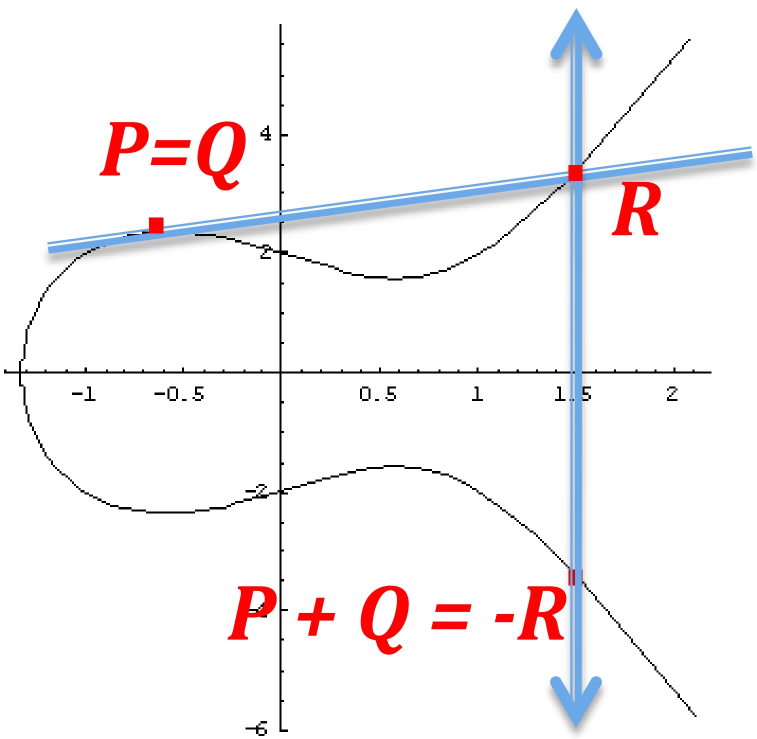
$P = (x_1, y_1)$ and
$Q = (x_2, y_2)$

$P + Q = \mathcal{O}$



Case 3:
$x_1 = x_2$ and $y_1 = y_2$

$P = (x_1, y_1)$ and
$Q = (x_2, y_2)$



L – line tangent to E at point R

Fact

L intersects E in exactly one point
$R = (x_3, y_3)$.
Where:

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

and

$$\lambda = \frac{3x_1^2 \cdot y_2 + a}{2y_1}$$

How to prove that this is a group?

Easy to see:

- set $\boldsymbol{E}$ is **closed under addition**
- addition is **commutative**
- $\mathcal{O}$ is an **identity**
- every point has an **inverse**

What remains is **associativity** **(exercise).**

How to use these groups in cryptography?

Instead of the reals use some **finite field**.

For example: Z_p where p is prime.

All the formulas remain the same!

Example

x	$x^3 + x + 6 \bmod 11$	quadratic residue?	y
0	6	no	
1	8	no	
2	5	yes	4,7
3	3	yes	5,6
4	8	no	
5	4	yes	2,9
6	8	no	
7	4	yes	2,9
8	9	yes	3,8
9	7	no	
10	4	yes	2,9

Hasse's Theorem

Let $\boldsymbol{E}$ be an elliptic curve defined over $\boldsymbol{Z_p}$ where $\boldsymbol{p > 3}$ is prime.

Then:

$$\boldsymbol{p + 1 - 2 \cdot \sqrt{p} \le |E| \le p + 1 + 2 \cdot \sqrt{p}}$$

How to use the elliptic curves in cryptography?

$(\boldsymbol{E},+)$ - elliptic curve

Sometimes $(\boldsymbol{E},+)$ is **cyclic** or it **contains a large cyclic** group $(\boldsymbol{E'},+)$.

There exist examples of such $(\boldsymbol{E},+)$ or $(\boldsymbol{E'},+)$ where the **discrete-log problem** is believed to be **computationally hard**!

Plan

1. Discrete logarithm problem
    1. over $\boldsymbol{Z}_{\boldsymbol{p}}^{*}$ and its subgroups
    2. over elliptic curves
2. RSA
    1. RSA as an operation over $\boldsymbol{Z}_{\boldsymbol{N}}^{*}$
    2. algebraic properties of RSA
    3. algorithmic question about quadratic residues over $\boldsymbol{Z}_{\boldsymbol{N}}^{*}$
    4. group $\boldsymbol{Z}_{\boldsymbol{N}}$ vs $\boldsymbol{Z}_{\boldsymbol{N}}^{*}$

A “problem” with the discrete log

In order to perform operations in a group $\boldsymbol{G}$ (where $\boldsymbol{G} = \boldsymbol{Z_p}$, or $\mathbf{QR}_{\boldsymbol{p}}$, or is an **elliptic curve**):

one needs to **know the full description of this group** (e.g.: $\boldsymbol{p}$)

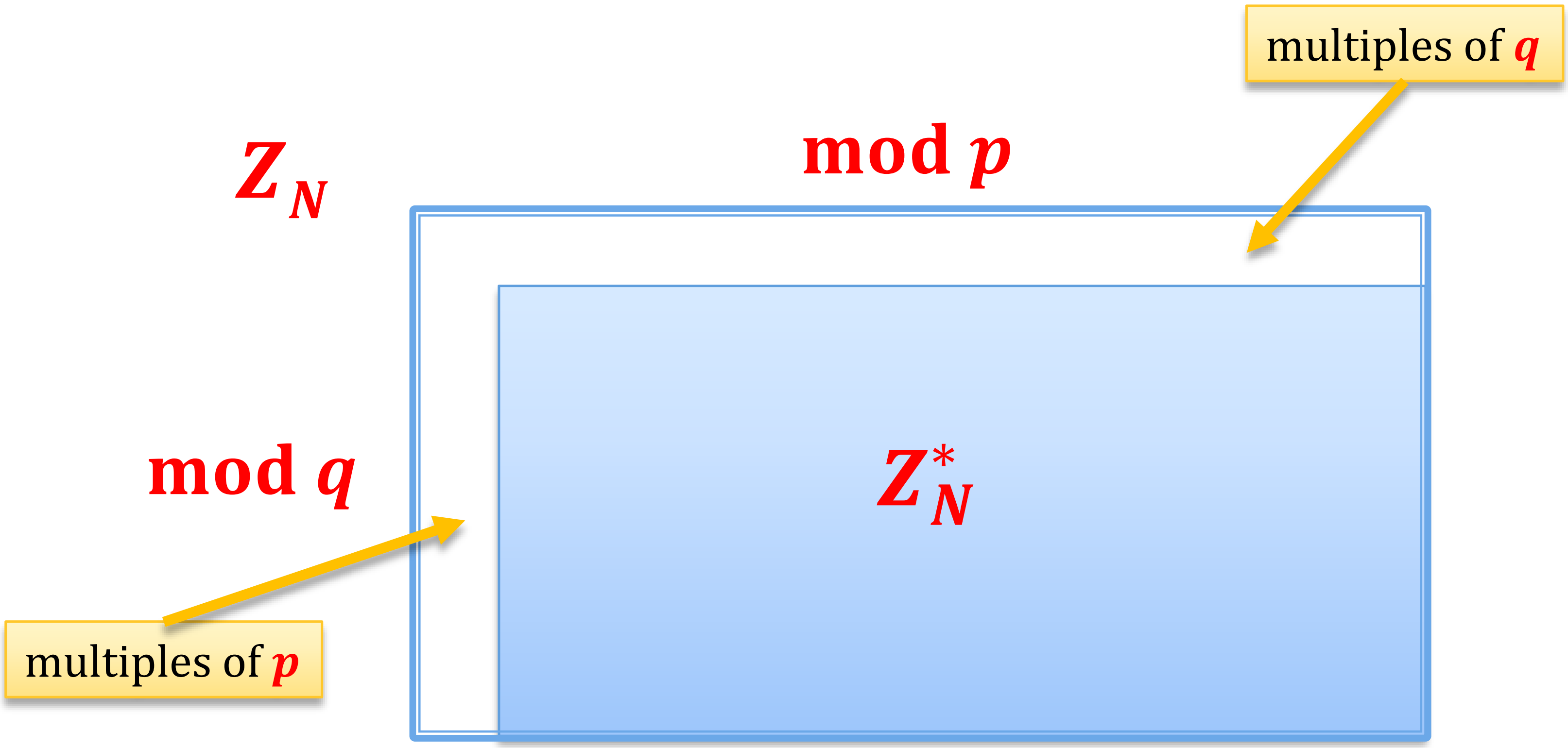
So “**everybody can perform the same operations**”.

<u>Main idea of the **RSA**</u>: work in a group where

- everybody **can multiply**
- but the **order of a group is hidden**, and **some operations are hard without knowing it**.

RSA group: Z_N^*, where $N = p \cdot q$ and p, q are distinct odd primes

On the last exercises we presented the following picture



Example: $p = 5, q = 7$

$x \bmod 7$

$x \bmod 5$

	0	1	2	3	4	5	6
0	0	15	30	10	25	5	20
1	21	1	16	31	11	26	6
2	7	22	2	17	32	12	27
3	28	8	23	3	18	33	13
4	14	29	9	24	4	19	34

Z_{35} Z_{35}^*

Which problems are easy and which are hard in Z_N^* $(N = pq)$?

- **multiplying elements?**

  easy!

- **finding inverse?**

  easy! (Euclidean algorithm)

- **computing** $\varphi(N)$?

  hard! - as hard as factoring N

- **raising an element to power** e (for a large e)?

  easy!

- **computing** e**th root** (for a large e)?

Computing eth roots modulo N

We want to invert a function:

$$f : Z_N^* \rightarrow Z_N^*$$

defined as

$$f(x) = x^e \bmod N.$$

This is possible only if f is a permutation.

Lemma

f is a permutation if and only if $e \perp \varphi(N)$.

In other words: $e \in Z_{\varphi(N)}^*$ (note: a "new" group!)

"$f(x) = x^e \bmod N$ is a permutation if and only if $e \perp \varphi(N)$."

1.

$\boxed{e \perp \varphi(N)}$ $\Rightarrow$ $\boxed{f(x) = x^e \bmod N \text{ is a permutation}}$

Let d be an inverse of e in $Z^*_{\varphi(N)}$. That is:

$$d \text{ is such that } d \cdot e = 1 \bmod \varphi(N).$$

Then: $$\left(f(x)\right)^d = (x^e)^d = x^{ed} = x^{ed \bmod \varphi(N)} = x^1$$

2.

$\boxed{e \perp \varphi(N)}$ $\Leftarrow$ $\boxed{f(x) = x^e \bmod N \text{ is a permutation}}$

[exercise]

Computing eth root – easy, or hard?

Suppose $e \perp \varphi(N)$.

We have shown that the function

$$f(x) = x^e \text{ (defined over } Z_N^*\text{)}$$

has an inverse

$$f^{-1}(x) = x^d, \text{ where } d \text{ is an inverse of } e \text{ in } Z_{\varphi(N)}^*$$

<u>Moral</u>:

If we know $\varphi(N)$ we can compute the roots efficiently.

What if we don't know $\varphi(N)$?

Can we compute the eth root if we do not know $\varphi(N)$?

It is conjectured to be hard.

This conjecture is called an **RSA assumption**:

security parameter 1^k

poly-time adversary

(x, e, N)

choose:

- $N = pq$ where p and q are random primes such that $|p| = |q| = k$
- x – a random element of Z_N^*,
- e – a random element of $Z_{\varphi(N)}^*$

<u>cannot</u> compute y such that $y^e = x$

More formally

<u>RSA assumption</u>

For any randomized polynomial time algorithm $\boldsymbol{A}$ we have:

$$\boldsymbol{P\left(y^e = x \bmod N:\ \ y := \ A(x, N, e)\right)}$$

is negligible in $|N|$

where $\boldsymbol{N = pq}$ where $\boldsymbol{p}$ and $\boldsymbol{q}$ are random primes such that
$|\boldsymbol{p}| = |\boldsymbol{q}|$, and $\boldsymbol{x}$ is a random element of $\boldsymbol{Z_N^*}$,
and $\boldsymbol{e}$ is a random element of $\boldsymbol{Z_{\varphi(N)}^*}$.

What can be shown?

Does the **RSA assumption** follow from the assumption that factoring is hard?

We don't know...

What **can** be shown is that

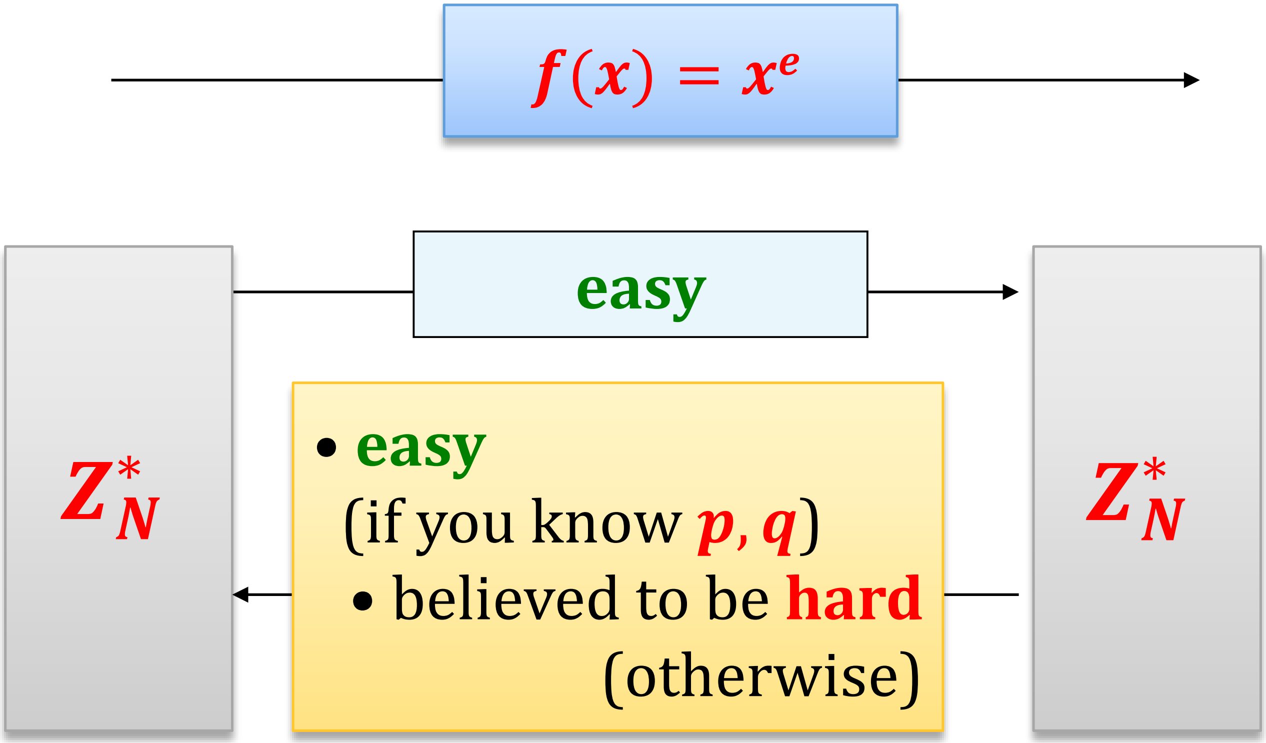
computing d from e is not easier than factoring N.

How is it proven?

One needs to show that from d and e one can compute the factors of N.

Note: $de = 1 \bmod \varphi(N)$.

One can show that the knowledge of a multiple of $\varphi(N)$ suffices to factor N.



Functions like this are called **trap-door one-way permutations**.
f is called an **RSA function** and is extremely important.
We will denote it $\mathbf{RSA}_{e,N}$.

Outlook

$\boldsymbol{N}$ – a product of two large primes

factoring $\boldsymbol{N}$ is hard

computing $\boldsymbol{e}$th roots in $\boldsymbol{Z}_N^*$ is hard

computing $\boldsymbol{\varphi(N)}$ hard

$\boldsymbol{P \neq NP}$

computing $\boldsymbol{d}$ from $\boldsymbol{e}$ is hard

Plan

1. Discrete logarithm problem
    1. over $\boldsymbol{Z}_p^*$ and its subgroups
    2. over elliptic curves
2. RSA
    1. RSA as an operation over $\boldsymbol{Z}_N^*$
    2. algebraic properties of RSA
    3. algorithmic question about quadratic residues over $\boldsymbol{Z}_N^*$
    4. group $\boldsymbol{Z}_N$ vs $\boldsymbol{Z}_N^*$

Handbook RSA – an algebraic view

Take $\boldsymbol{Z}_N^*$ (where $\boldsymbol{N = pq}$ and $\boldsymbol{p, q}$ are **two distinct odd primes**), defined as follows:

- $\boldsymbol{e \leftarrow Z_{\varphi(N)}^*}$
- $\boldsymbol{d = e^{-1} \bmod \varphi(N)}$

$\mathbf{RSA}_{e,N}$ is a **permutation of** $\boldsymbol{Z}_N^*$ defined as follows:

- $\mathbf{RSA}_{e,N}(\boldsymbol{m}) = \boldsymbol{m^e}$
- $\mathbf{RSA}_{e,N}^{-1}(\boldsymbol{c}) = \boldsymbol{c^d}$

equal to $\mathbf{RSA}_{d,N}(\boldsymbol{m})$

We have:

$$\mathbf{RSA}_{e,N}^{-1}\left(\mathbf{RSA}_{e,N}(\boldsymbol{m})\right) = (\boldsymbol{m}^e)^d = \boldsymbol{m}^{ed} = \boldsymbol{m}^1 = \boldsymbol{m}$$

Algebraic properties of RSA

1. **RSA** is homomorphic:

$$\mathbf{RSA}_{e,N}(m_0 \cdot m_1) = (m_0 \cdot m_1)^e$$
$$= m_0^e \cdot m_1^e$$
$$= \mathbf{RSA}_{e,N}(m_1) \cdot \mathbf{RSA}_{e,N}(m_2)$$

   why is it bad?

   By checking if $c = c_0 \cdot c_1$ the adversary can check if the messages m, m_0, m_1 corresponding to c, c_0, c_1 satisfy:

$$m = m_0 \cdot m_1$$

2. The **Jacobi symbol** leaks.

to explain it we will first talk about **QRs** in Z_N^*

Square roots modulo $N = pq$

So, far we discussed a problem of computing the eth root modulo N.

What about the case when $e = 2$?

Clearly $\mathbf{gcd}(2, \varphi(N)) \neq 1$, so $f(x) = x^2$ is **not** a bijection.

Question

Which elements have a square root modulo N?

Quadratic Residues modulo pq

Z_{15}^*

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
a^2		1	4		1			4	4			1		4	1

$\mathbf{QR_{15}}$: | 1 | 4 |

Observation: every quadratic residue modulo **15** has **exactly 4** square roots, and hence $|\mathbf{QR_{15}}| = \frac{|Z_{15}^*|}{4}$.

A lemma about QRs modulo pq

Fact: For $N = pq$ we have $|\mathbf{QR}_N| = |Z_N^*| / 4$.

Proof:

$$x \in \mathbf{QR}_N$$

iff

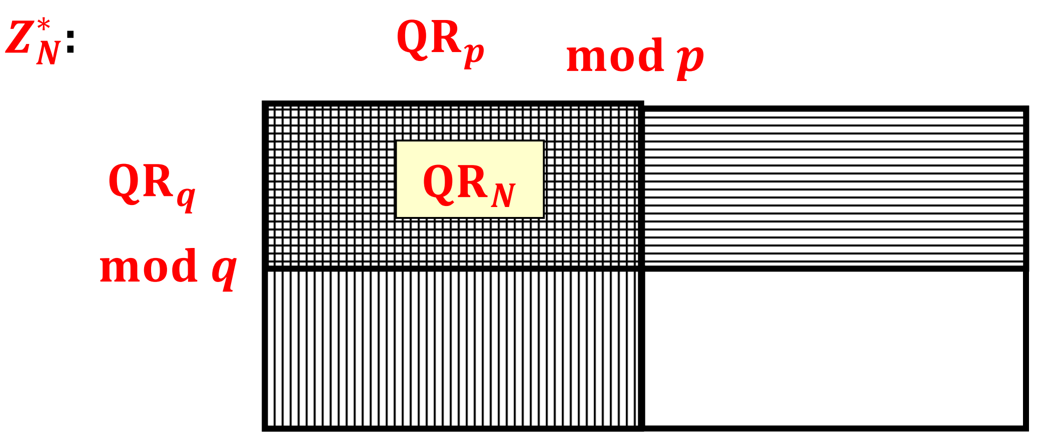
$$x = a^2 \bmod N, \text{ for some } a$$

iff (by **CRT**)

$$x = a^2 \bmod p \text{ and } x = a^2 \bmod q$$

iff

$$x \bmod p \in \mathbf{QR}_p \text{ and } x \bmod q \in \mathbf{QR}_q$$



$\mathbf{QR}_{pq}$ – an example

Z_{15}:

	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

$1^2 \bmod 5$
$4^2 \bmod 5$

QR_5

$2^2 \bmod 5$
$3^2 \bmod 5$

QR_3

$1^2 \bmod 3$
$2^2 \bmod 3$

QR_{15}

Z_{15}^*

Every $x \in \mathbf{QR}_N$ has exactly **4** square roots

More precisely, every $z = x^2$ has square roots x_+^+, x_-^+, x_+^-, and x_-^- such that:

- $x_+^+ = x \pmod{p}$ **and** $x_+^+ = x \pmod{q}$
- $x_-^+ = x \pmod{p}$ **and** $x_-^+ = -x \pmod{q}$
- $x_+^- = -x \pmod{p}$ **and** $x_+^- = x \pmod{q}$
- $x_-^- = -x \pmod{p}$ **and** $x_-^- = -x \pmod{q}$

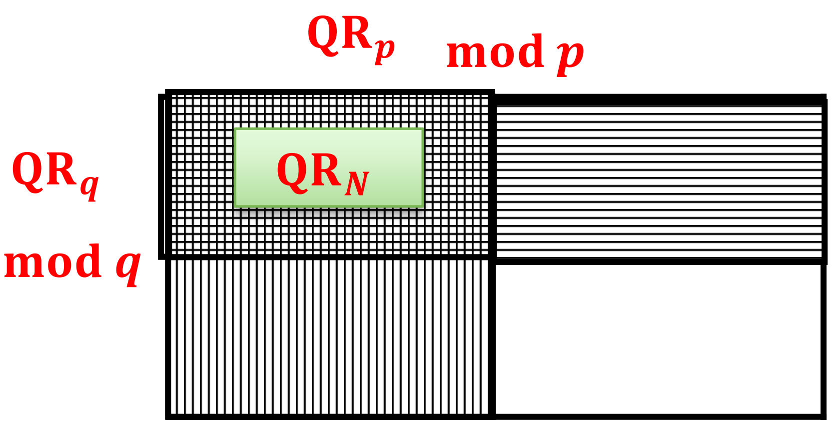
equals to x

equals to $-x$

Jacobi Symbol

for any prime $\boldsymbol{p}$ define $J_p(x) := \begin{cases} +1 & \text{if } x \in \mathbf{QR}_p \\ -1 & \text{otherwise} \end{cases}$

for $N = pq$ define $J_N(x) := J_p(x) \cdot J_q(x)$



$J_N(x) :=$

+1	**-1**
-1	**+1**

It is a subgroup of Z_N^*

$$Z_N^+ := \{x \in Z_N^* : J_N(x) = +1\}$$

Jacobi symbol can be computed efficiently!

(even in $\boldsymbol{p}$ and $\boldsymbol{q}$ are unknown)

Fact: the **RSA** function "preserves" the **Jacobi symbol**

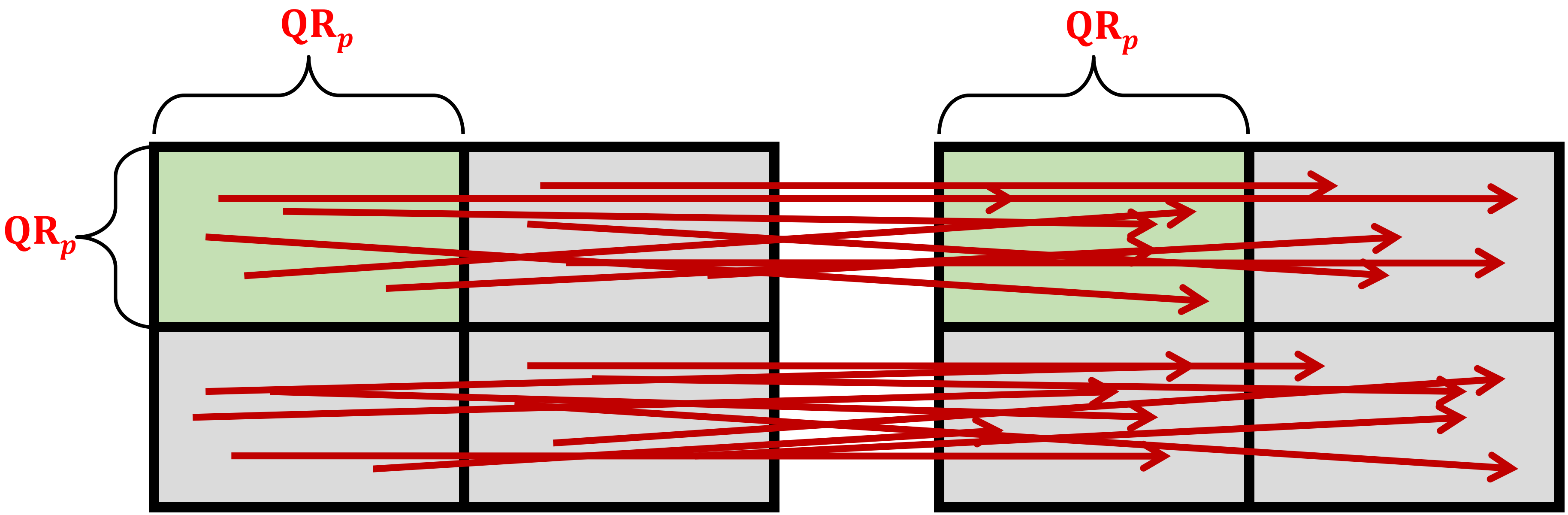
$N = pq$ - **RSA** modulus

e is such that $e \perp \varphi(N)$

$$J_N(x) = J_N(x^e \bmod N)$$

Actually, something even stronger holds:

$\mathbf{RSA}_{N,e}$ is a permutation on each "quarter" of $\mathbb{Z}_N^*$



In other words:

- m **mod** $p \in \mathbf{QR}_p$ **iff** m^e **mod** p $\mathbf{QR}_p$
- m **mod** $q \in \mathbf{QR}_q$ **iff** m^e **mod** $q \in \mathbf{QR}_q$

Example Z_{35}^{*}

We calculate $\mathbf{RSA}_{23,35}(m) = m^{23} \bmod 35$

QR_7 / mod 7 (columns); QR_5 / mod 5 (rows)

	1	**2**	**4**	**3**	**5**	**6**
1	1	16	11	31	26	6
4	29	9	4	24	19	34
2	22	2	32	17	12	27
3	8	23	18	3	33	13

	1	**4**	**2**	**5**	**3**	**6**
1	1	11	16	26	31	6
4	29	4	9	19	24	34
3	8	18	23	33	3	13
2	22	32	2	12	17	27

How to prove it?

By the **CRT** and by the fact that $\boldsymbol{p}$ and $\boldsymbol{q}$ are symmetric it is enough to show that

$$\boldsymbol{m} \text{ is a } \mathbf{QR}_{p}$$

iff

$$\boldsymbol{m}^{\boldsymbol{e}} \text{ is a } \mathbf{QR}_{p}$$

Fact

For an odd e:

$$m^e \bmod p \text{ is a } QR_p$$
$$\text{iff}$$
$$m \bmod p \text{ is a } QR_p$$

Proof:

Let g be the generator of Z_p^*. Let y be such that $m = g^y$.

Recall that x is a QR_p iff x is an even power of g

Observe that

$$(g^y)^e \bmod p \text{ is an **even** power of } g$$
$$\text{iff}$$
$$g^y \bmod p \text{ is an **even** power of } g.$$

Because $g^{ye} = g^{ye \bmod (p-1)}$
(remember that p and e are **odd**)

QED

Conclusion

The Jacobi symbol "leaks", i.e.:

from c

one can compute $J_N(\mathbf{Dec}_{N,d}(c))$

(without knowing the factorization of N)

Is it a big problem?

Depends on the application...

Note: The fact that the Jacobi symbol leaks **does not contradict** the **RSA assumption**.

security parameter 1^k

choose:

- $N = pq$ where p and q are random primes such that $|p| = |q| = k$
- x – a random element of Z_N^*,
- e – a random element of $Z_{\varphi(N)}^*$

(x, e, N)

adversary

cannot compute

$$\mathrm{RSA}_{e,N}^{-1}(x)$$

but **can** compute

$$J_N\left(\mathrm{RSA}_{e,N}^{-1}(x)\right)$$

Plan

1. Discrete logarithm problem
    1. over $\mathbf{Z}_p^*$ and its subgroups
    2. over elliptic curves
2. RSA
    1. RSA as an operation over $\mathbf{Z}_N^*$
    2. algebraic properties of RSA
    3. algorithmic question about quadratic residues over $\mathbf{Z}_N^*$
    4. group $\mathbf{Z}_N$ vs $\mathbf{Z}_N^*$

Algorithmic questions about QRs

Suppose $N = pq$.

Question: Is it easy to test membership in QR_N?

Answer: if one knows p and q – then **yes**!

Because:

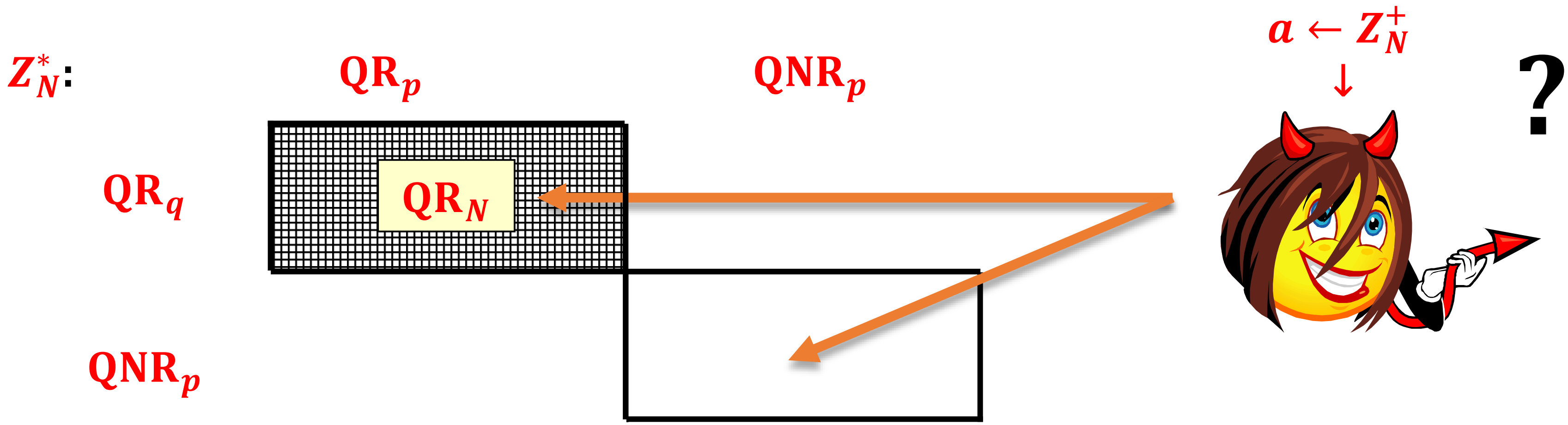
1. testing membership modulo a prime is easy
2. the "**CRT function**"

$$f(x) := (x \bmod p, x \bmod q)$$

can be efficiently computed in both directions

What if one does **not** know p and q?

Quadratic Residuosity Assumption



Quadratic Residuosity Assumption (QRA):
For a random $a \leftarrow Z_N^+$ it is computationally hard to determine if $a \in \mathrm{QR}_N$.
Formally: for every **polynomial-time** probabilistic algorithm D the value:

$$\left| P\big(D(N,a) = Q_N(a)\big) - \frac{1}{2} \right|$$

(where $a \leftarrow Z_N^+$) is **negligible**.

Where a predicate $Q_N : Z_N^+ \to \{0,1\}$ is defined as follows:
$Q_N(a) = 1$ if $a \in \mathrm{QR}_N$
$Q_N(a) = 0$ otherwise

How to compute a square root of $x \in \mathbf{QR}_N$?

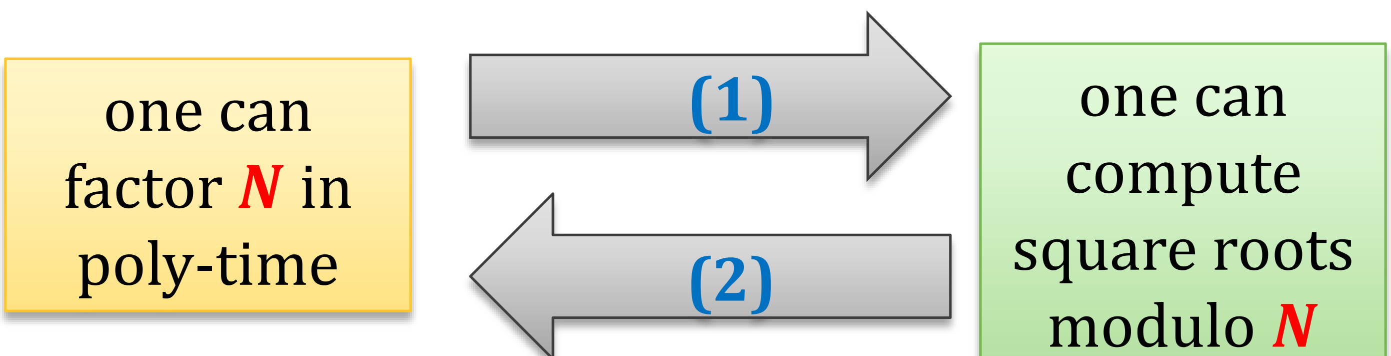
Fact

Let N be a random **RSA** modulus.

The problem of computing square roots (modulo N) of random elements in QR_N is poly-time equivalent to the problem of factoring N.

Proof

We need to show that:



one can factor N in poly-time $\xrightarrow{(1)}$ one can compute square roots modulo N

This follows from the fact that computing square roots modulo a prime p is easy.

$$f(x) = (x \bmod p, x \bmod q)$$ – the "CRT function"

$x \rightarrow$

1. Let
$(a, b) := f(x)$

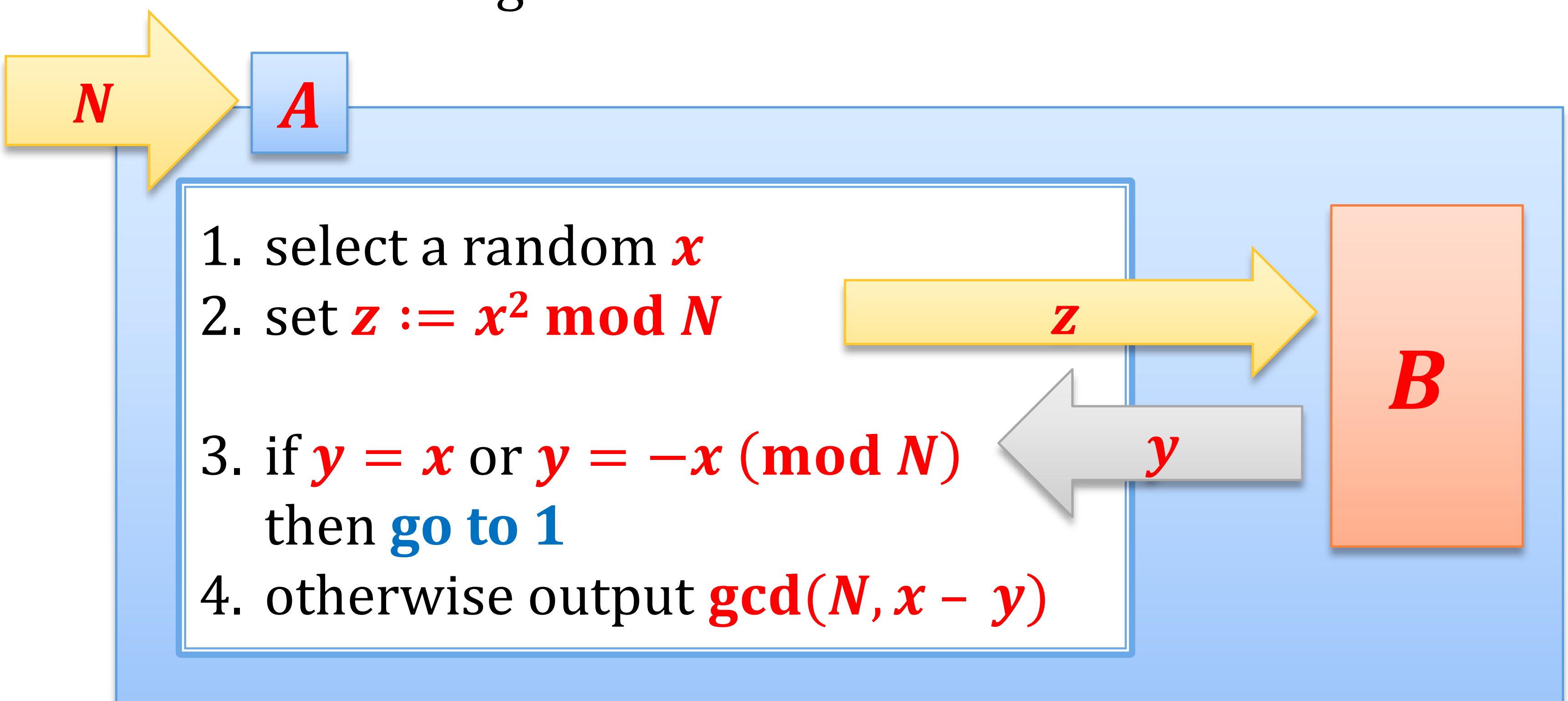
$\rightarrow$

2. Compute α and β such that
   - $\alpha^2 = a$
   - $\beta^2 = a$

$\rightarrow$

3. Output
$f^{-1}(\alpha, \beta)$,
$f^{-1}(-\alpha, \beta)$,
$f^{-1}(\alpha, -\beta)$,
$f^{-1}(-\alpha, -\beta)$

Suppose we have an algorithm $\boldsymbol{B}$ that computes the square roots.
We construct an algorithm $\boldsymbol{A}$ that factors $\boldsymbol{N}$.



To complete the proof we show that:

1. the probability that $y = x$ or $y = -x$ is equal to $\frac{1}{2}$

   (so the probability that it happens k times is 2^{-k})

and

2. If $y \neq x$ and $y \neq -x$ then

$$\gcd(N, x - y) \in \{p, q\}.$$

“the probability $\boldsymbol{\pi}$ that $\boldsymbol{y = x}$ or $\boldsymbol{y = -x}$ is equal to $\mathbf{1/2}$”

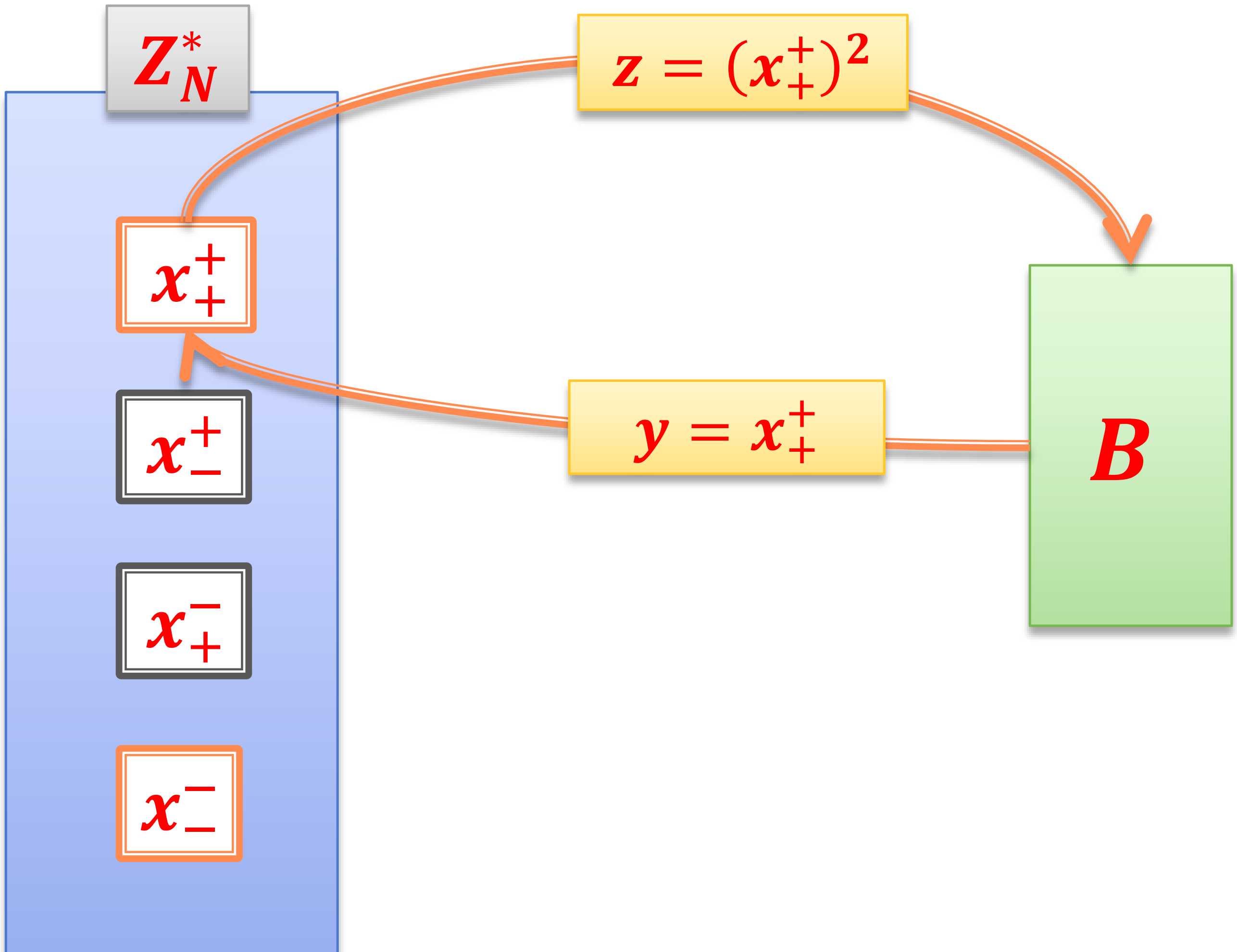
Recall that every $\boldsymbol{z = x^2}$ has square roots $\boldsymbol{x_+^+, x_-^+, x_+^-}$, and $\boldsymbol{x_-^-}$ such that:

- $\boldsymbol{x_+^+ = x \pmod{p}}$ **and** $\boldsymbol{x_+^+ = x \pmod{q}}$
- $\boldsymbol{x_-^+ = x \pmod{p}}$ **and** $\boldsymbol{x_-^+ = -x \pmod{q}}$
- $\boldsymbol{x_+^- = -x \pmod{p}}$ **and** $\boldsymbol{x_+^- = x \pmod{q}}$
- $\boldsymbol{x_-^- = -x \pmod{p}}$ **and** $\boldsymbol{x_-^- = -x \pmod{q}}$

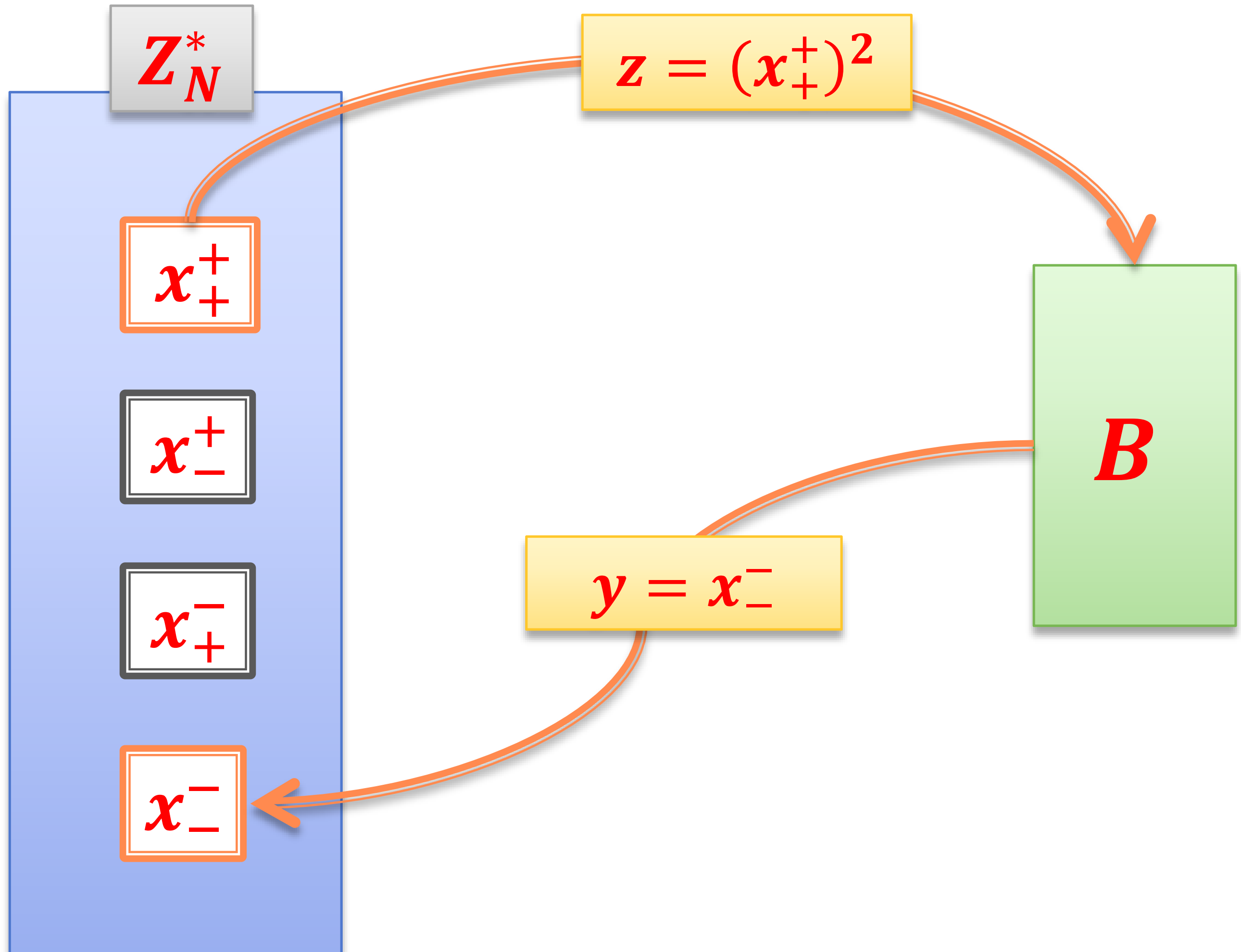
equals to $\boldsymbol{x}$

equals to $\boldsymbol{-x}$

If we are unlucky it happens that:



Or:



Observation

Since x is **chosen randomly**, thus each x_+^+, x_-^+, x_+^-, and x_-^- is chosen with the same probability.

Therefore the choice of the "strategy of B" doesn't matter!

Z_N^*

x_+^+

x_-^+

x_+^-

x_-^-

$z = (x_+^+)^2$

B

Therefore the probability π is equal to $\mathbf{1/2}$.

“If $y \neq x$ and $y \neq -x$ then $\mathbf{gcd}(N, x - y) \in \{p, q\}$.”

Suppose y is such that

$$y = x \ (\mathbf{mod}\ p) \text{ and } y = -x \ (\mathbf{mod}\ q)$$

(the other case is symmetric).

We have: $y - x = 0 \ \mathbf{mod}\ p$

Therefore: $p | \mathbf{gcd}(y - x, N)$.

But $0 < |y - x| < N$ because

- $x, y \in Z_N^*$
- and $x \neq y$

So it has to be the case that $\mathbf{gcd}(y - x, N) = p$

QED

Plan

1. Discrete logarithm problem
    1. over $\boldsymbol{Z}_p^*$ and its subgroups
    2. over elliptic curves
2. RSA
    1. RSA as an operation over $\boldsymbol{Z}_N^*$
    2. algebraic properties of RSA
    3. algorithmic question about quadratic residues over $\boldsymbol{Z}_N^*$
    4. group $\boldsymbol{Z}_N$ vs $\boldsymbol{Z}_N^*$

The $\boldsymbol{Z_N^*}$ group is a bit strange

Some elements of

$$\boldsymbol{Z_N = \{0, \ldots, n-1\}}$$

are not there but **you don't know which** if you don't know $\boldsymbol{p}$ and $\boldsymbol{q}$.

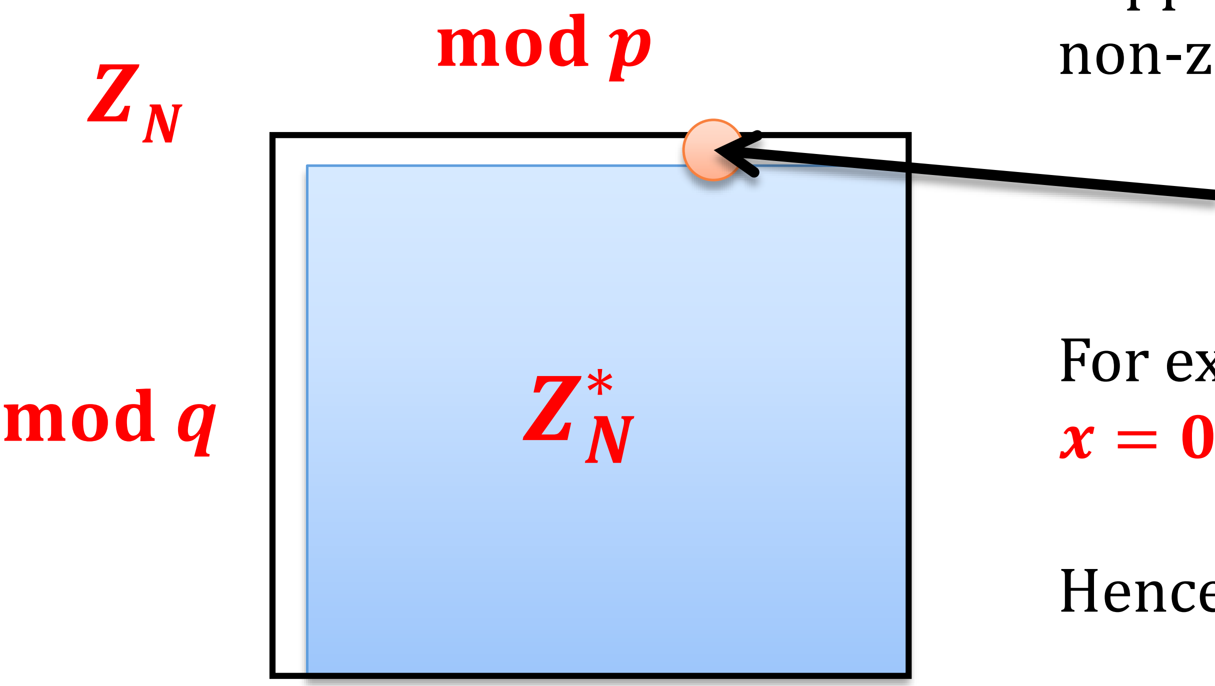
Is it a problem?

No, for **two** reasons:

- it is hard to find an element in $\boldsymbol{Z_N^* \setminus Z_N}$ (other than $\mathbf{0}$),
- **RSA** works also over $\boldsymbol{Z_N}$ ("by accident").

It is **hard to find** an element in $Z_N \setminus Z_N^*$ (other than $\mathbf{0}$)

Why?



Suppose we have found a non-zero element

$x \in Z_N \setminus Z_N^*$

For example:
$x = 0 \pmod{q}$ and $x \neq 0$

Hence $\gcd(x, N) = q$.

So we can factor N.

Example

gcd(15, 35) = 5

***x* mod 7**

***x* mod 5**	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	5	10	15	20	25	30
1	7	1	16	31	11	26	6
2	12	22	2	17	32	12	27
3	17	8	23	3	18	33	13
4	22	29	9	24	4	19	34

$\boldsymbol{Z_{35}}$ $\boldsymbol{Z_{35}^{*}}$

RSA works also over Z_N

Suppose x is such that

$$x \bmod q = 0 \text{ and } x \bmod p \neq 0$$

We show that

$$\mathrm{RSA}_{N,d}\left(\mathrm{RSA}_{N,e}(x)\right) = x \bmod N$$

$= x^{ed}$

By CRT it is enough to show that:

- $x^{ed} = x \bmod q$, and
- $x^{ed} = x \bmod p$.

this holds because both sides are divisible by q

Recall that: $(p-1)(q-1) \mid ed - 1$
Hence: $(p-1) \mid ed - 1$
Therefore: $x^{ed-1} = 1 \bmod p$
This implies that: $x^{ed} = x \bmod p$.