

Get these
slides ➡



Zero-knowledge-proofs - part 1

ENGINEERING WORKSHOP - DEC 2025
(IRELAND)

typst

$$\nabla \cdot \mathbf{E} = \rho \quad (15)$$

Let \mathbf{E} be given by

$$\mathbf{E} = \frac{1}{\epsilon_0} \nabla \phi \quad (16)$$

The first part into the term chosen to be quadratic in the field tensor because we want to derive a linear field equation in which the interposition theorem holds. The action has to be a scalar, the simplest quadratic scalar of the field tensor is the product given in Eq. (20).

$$\begin{pmatrix} E_1 & E_2 & E_3 \\ E_2 & -E_1 & 0 \\ E_3 & E_1 & 0 \end{pmatrix}$$

The three spatial components of \mathbf{E} , (20)

yield the magnetic induction law

$$\nabla \times \mathbf{B} = \frac{1}{c} \frac{\partial \mathbf{E}}{\partial t} \quad (26)$$



Pawel Jakubas

Plan of the tutorial

Plan of the tutorial

Let's get a little deeper than usual and understand what main building blocks of ZKP looks like

This tutorial will focus on

Plan of the tutorial

Let's get a little deeper than usual and understand what main building blocks of ZKP looks like

This tutorial will focus on

1. sketching the landscape of what we want to understand during 3-4 parts
- 2.

Plan of the tutorial

Let's get a little deeper than usual and understand what main building blocks of ZKP looks like

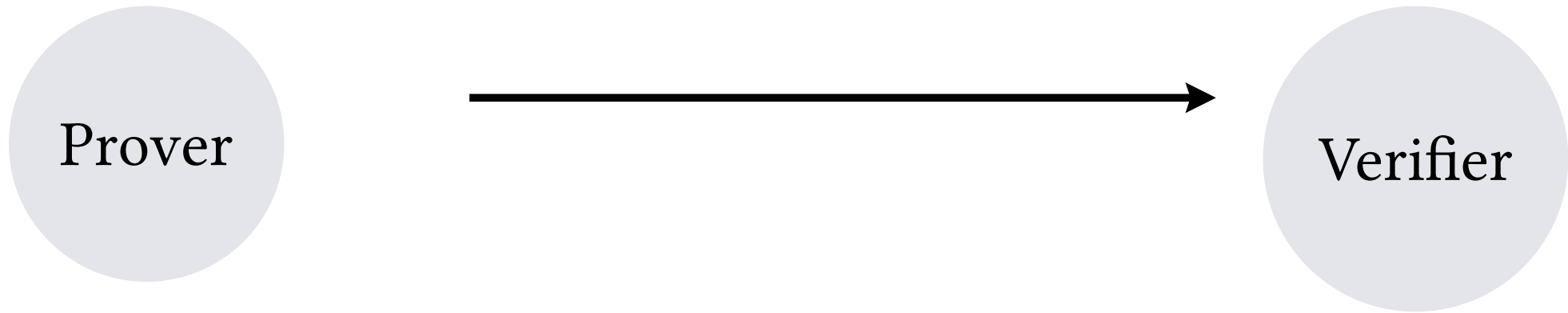
This tutorial will focus on

1. sketching the landscape of what we want to understand during 3-4 parts
2. cover the first part in some detail **elliptic curves**

Verifiable computing vs ZKP (1)

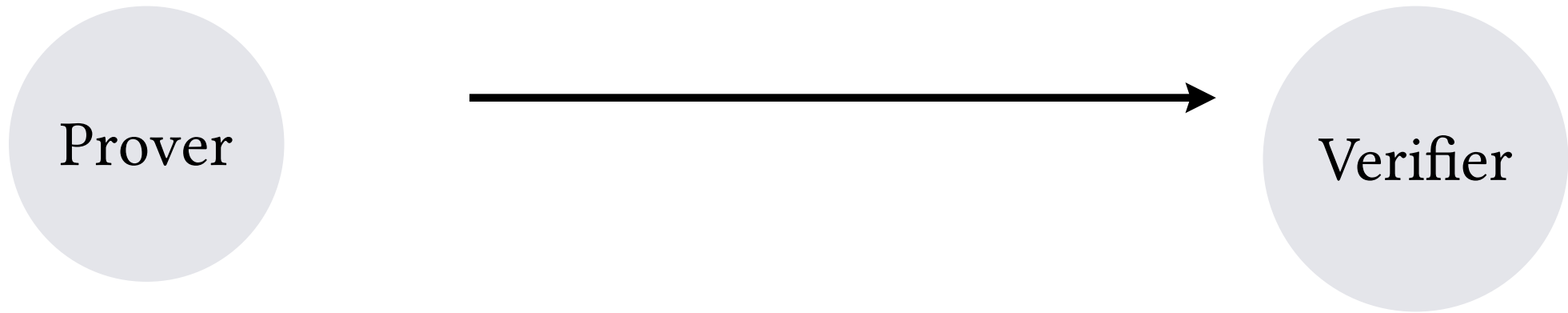
Verifiable computing vs ZKP (1)

There is **asymmetry** built into those systems. It is much easier to get public key from secret. But not the other way



Verifiable computing vs ZKP (1)

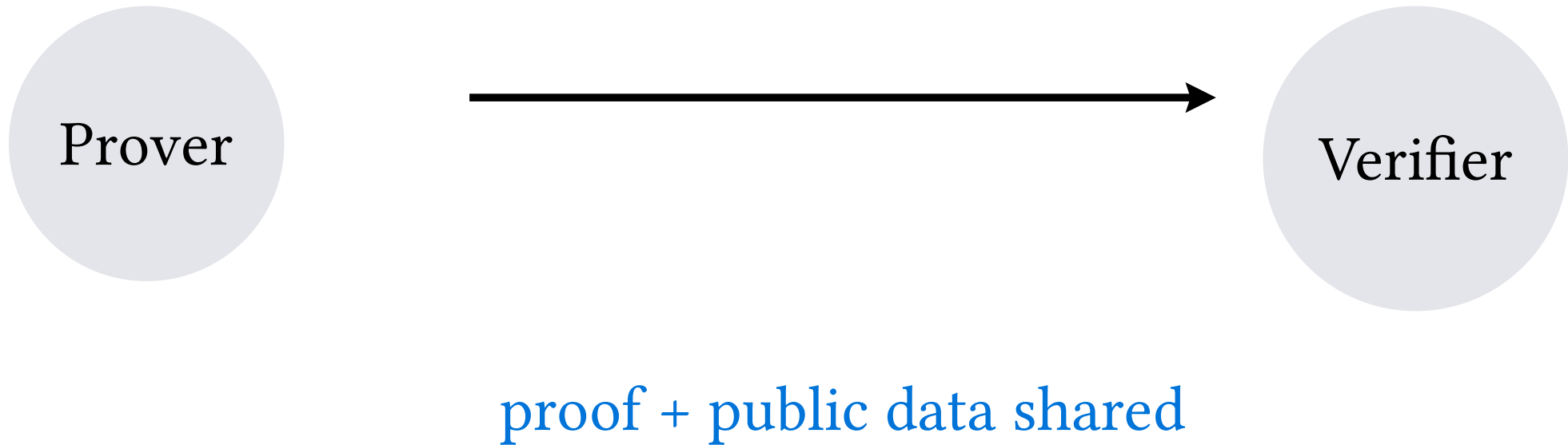
There is **asymmetry** built into those systems. It is much easy to get public key from secret. But not the other way



secret -> (easy) -> public

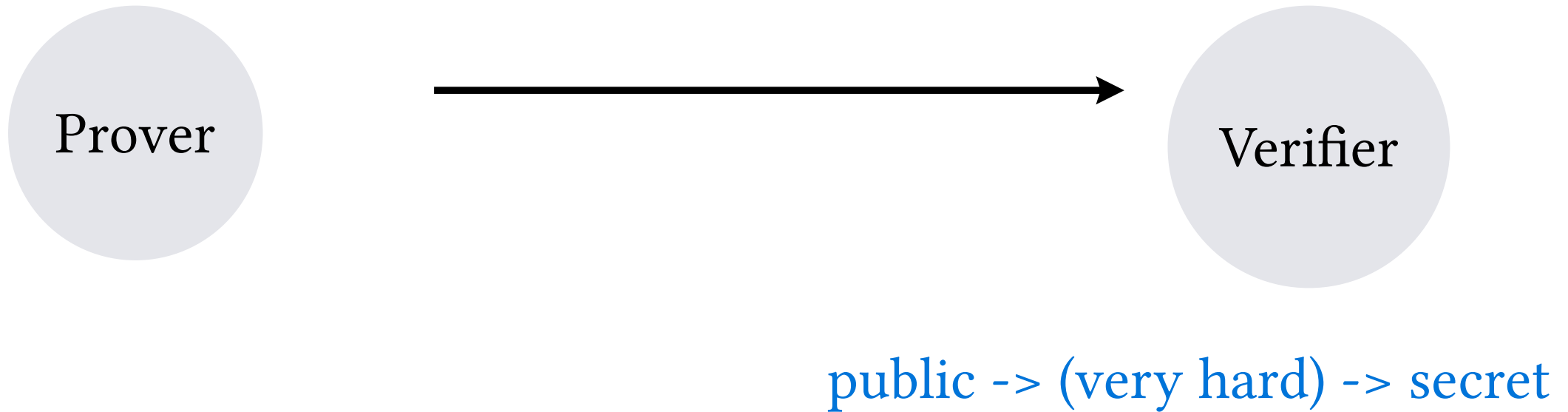
Verifiable computing vs ZKP (1)

There is **asymmetry** built into those systems. It is much easier to get public key from secret. But not the other way



Verifiable computing vs ZKP (1)

There is **asymmetry** built into those systems. It is much easy to get public key from secret. But not the other way



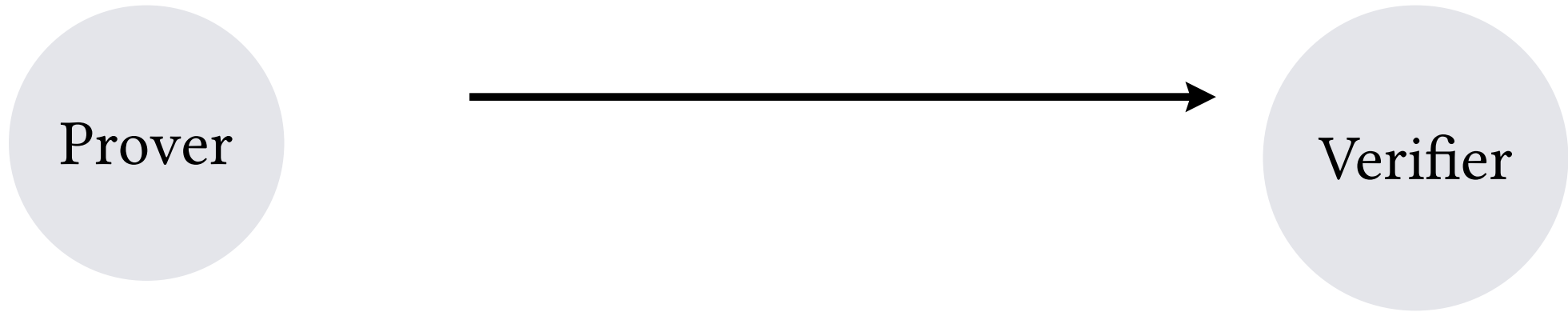
Verifiable computing vs ZKP (1)

There is **asymmetry** built into those systems. It is much easy to get public key from secret. But not the other way



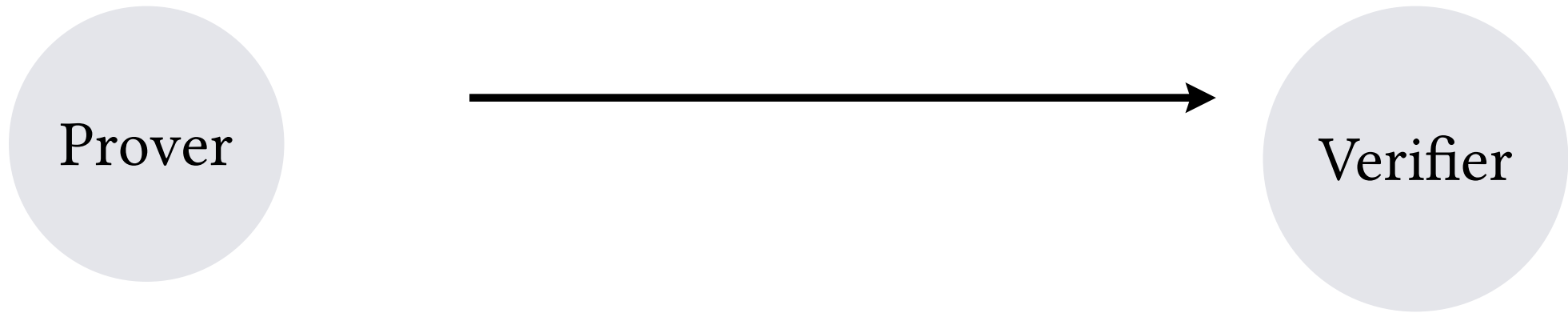
Verifiable computing vs ZKP (2)

There is **asymmetry** built into those systems. It is much quicker to verify than prove something.



Verifiable computing vs ZKP (2)

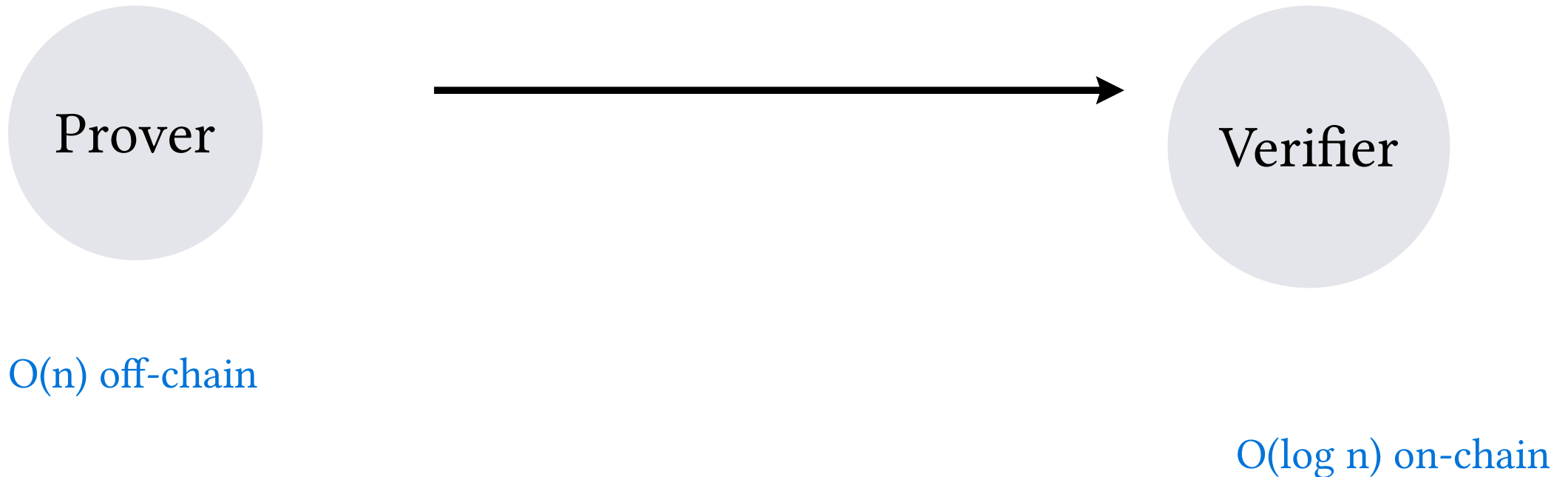
There is **asymmetry** built into those systems. It is much quicker to verify than prove something.



$O(n)$ off-chain

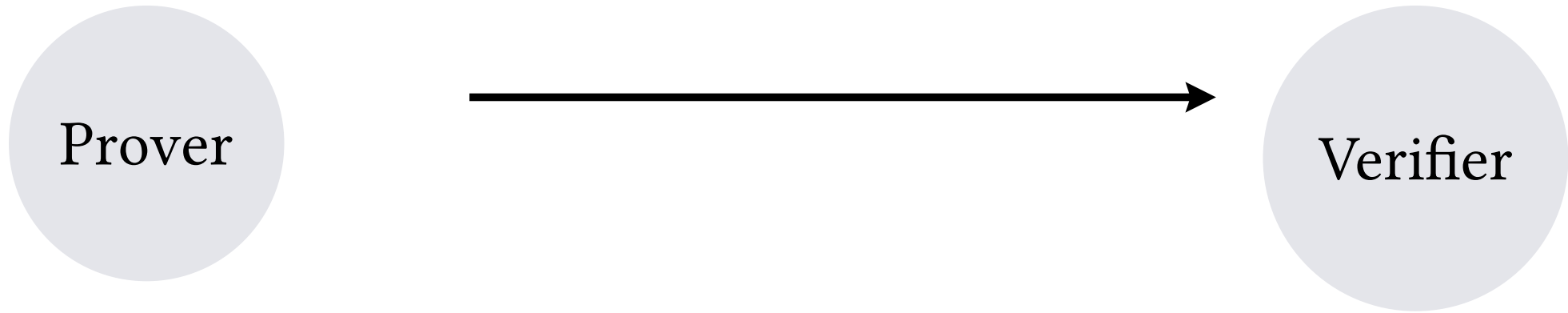
Verifiable computing vs ZKP (2)

There is **asymmetry** built into those systems. It is much quicker to verify than prove something.



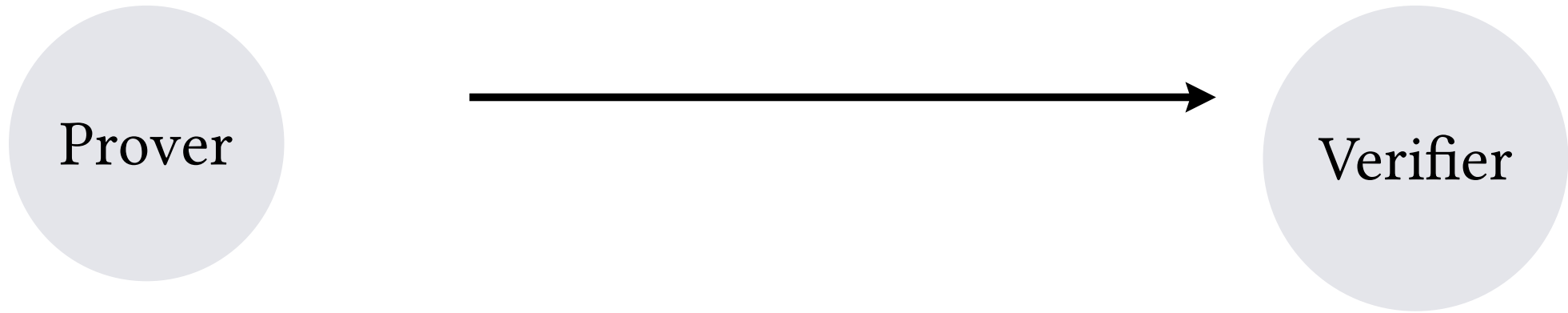
ZKP (3)

Data sent to verifier is compressed, and can be hidden



ZKP (3)

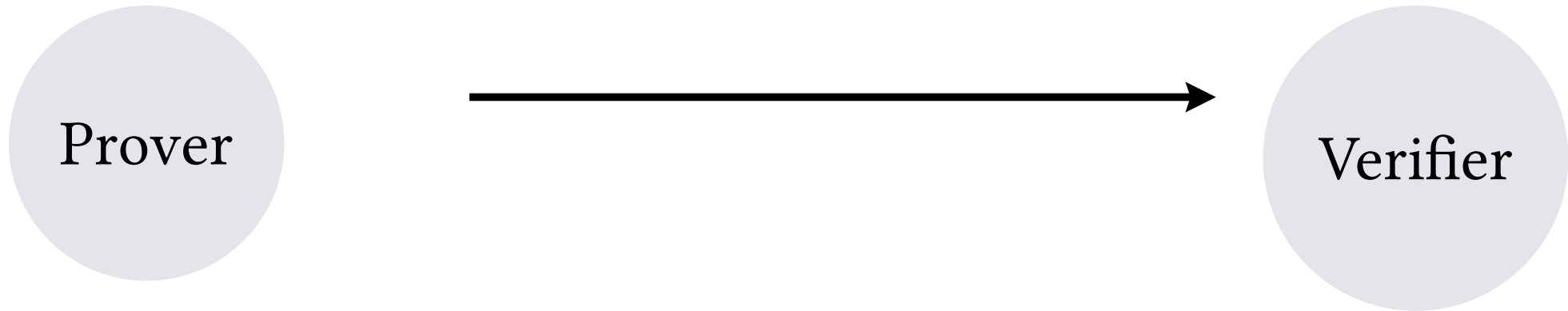
Data sent to verifier is compressed, and can be hidden



size: n

ZKP (3)

Data sent to verifier is compressed, and can be hidden

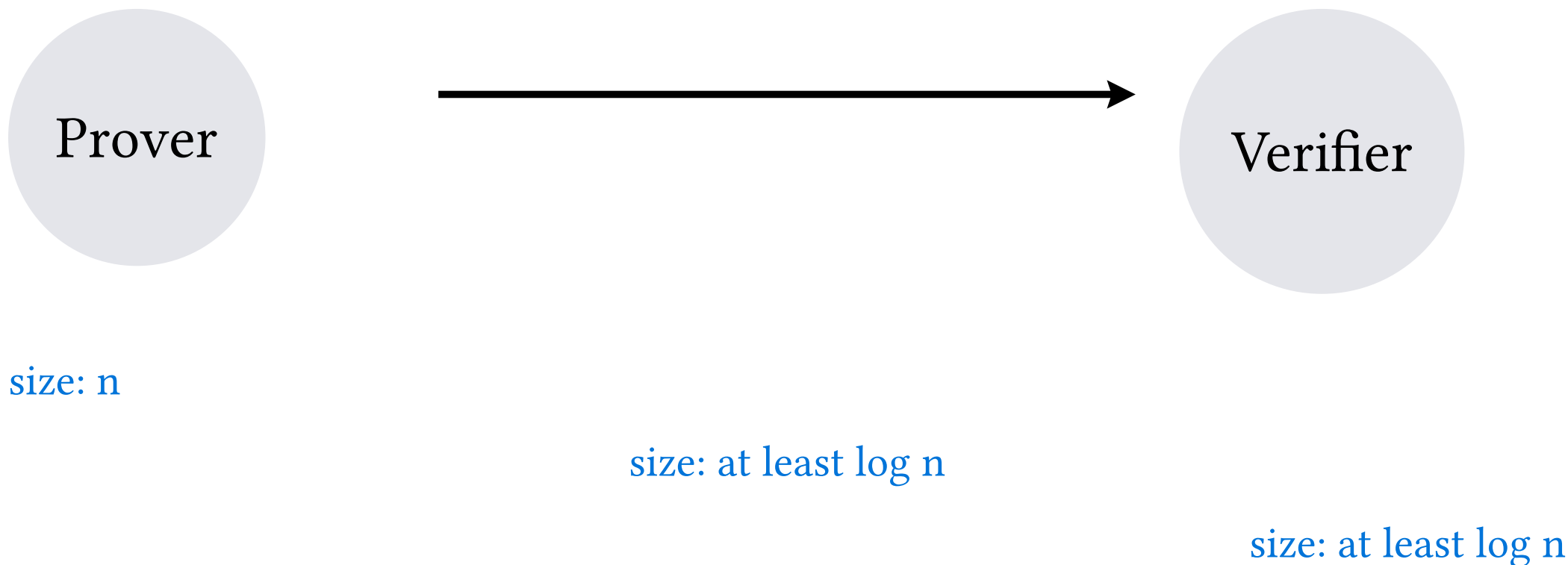


size: n

size: at least $\log n$

ZKP (3)

Data sent to verifier is compressed, and can be hidden



Modular arithmetics (1)

It is about integers.

Modular arithmetics (1)

It is about integers.

Let's assume we arithmetics **mod 8**. It means the possible values are 0,1,2,3,4,5,6,7. if we move below or above we need to wrap up.

Modular arithmetics (1)

$$3 + 3 \bmod 8 = 6 \bmod 8$$

$$10 \bmod 8 = 2 \bmod 8$$

$$5 + 5 \bmod 8 = 2 \bmod 8$$

$$5 \cdot 5 \bmod 8 = 25 \bmod 8 = (3 \cdot 8 + 1) \bmod 8 = 1 \bmod 8$$

Modular arithmetics (1)

$$3 + 3 \bmod 8 = 6 \bmod 8$$

$$10 \bmod 8 = 2 \bmod 8$$

$$5 + 5 \bmod 8 = 2 \bmod 8$$

$$5 \cdot 5 \bmod 8 = 25 \bmod 8 = (3 \cdot 8 + 1) \bmod 8 = 1 \bmod 8$$

congruent groups

Modular arithmetics (2)

addition mod 8	multiplication mod 8
0 1 2 3 4 5 6 7	1 2 3 4 5 6 7
1 2 3 4 5 6 7 0	2 4 6 0 2 4 6
2 3 4 5 6 7 0 1	3 6 1 4 7 2 5
3 4 5 6 7 0 1 2	4 0 4 0 4 0 4
4 5 6 7 0 1 2 3	5 2 7 4 1 6 3
5 6 7 0 1 2 3 4	6 4 2 0 6 4 2
6 7 0 1 2 3 4 5	7 6 5 4 3 2 1
7 0 1 2 3 4 5 6	

Modular arithmetics (2)

addition mod 8

0 1 2 3 4 5 6 7
1 2 3 4 5 6 7 0
2 3 4 5 6 7 0 1
3 4 5 6 7 0 1 2
4 5 6 7 0 1 2 3
5 6 7 0 1 2 3 4
6 7 0 1 2 3 4 5
7 0 1 2 3 4 5 6

multiplication mod 8

1 2 3 4 5 6 7
2 4 6 0 2 4 6
3 6 1 4 7 2 5
4 0 4 0 4 0 4
5 2 7 4 1 6 3
6 4 2 0 6 4 2
7 6 5 4 3 2 1

Let's solve the eq in mod 8:

$$9(2x + 7) - 6 \equiv 2x + 6$$

Modular arithmetics (2)

addition mod 8

0 1 2 3 4 5 6 7
1 2 3 4 5 6 7 0
2 3 4 5 6 7 0 1
3 4 5 6 7 0 1 2
4 5 6 7 0 1 2 3
5 6 7 0 1 2 3 4
6 7 0 1 2 3 4 5
7 0 1 2 3 4 5 6

multiplication mod 8

1 2 3 4 5 6 7
2 4 6 0 2 4 6
3 6 1 4 7 2 5
4 0 4 0 4 0 4
5 2 7 4 1 6 3
6 4 2 0 6 4 2
7 6 5 4 3 2 1

Let's solve the eq in mod 8:

$$9(2x + 7) - 6 \equiv 2x + 6$$

$$19 \cdot 2x + 19 \cdot 7 - 6 \equiv 2x + 6$$

Modular arithmetics (2)

addition mod 8

0 1 2 3 4 5 6 7

1 2 3 4 5 6 7 0

2 3 4 5 6 7 0 1

3 4 5 6 7 0 1 2

4 5 6 7 0 1 2 3

5 6 7 0 1 2 3 4

6 7 0 1 2 3 4 5

7 0 1 2 3 4 5 6

multiplication mod 8

1 2 3 4 5 6 7

2 4 6 0 2 4 6

3 6 1 4 7 2 5

4 0 4 0 4 0 4

5 2 7 4 1 6 3

6 4 2 0 6 4 2

7 6 5 4 3 2 1

Let's solve the eq in mod 8:

$$9(2x + 7) - 6 \equiv 2x + 6$$

$$19 \cdot 2x + 19 \cdot 7 - 6 \equiv 2x + 6$$

$$38x + 133 - 6 \equiv 2x + 6 \quad \# \quad 133 \bmod 8 = 5$$

Modular arithmetics (2)

addition mod 8

0 1 2 3 4 5 6 7
1 2 3 4 5 6 7 0
2 3 4 5 6 7 0 1
3 4 5 6 7 0 1 2
4 5 6 7 0 1 2 3
5 6 7 0 1 2 3 4
6 7 0 1 2 3 4 5
7 0 1 2 3 4 5 6

multiplication mod 8

1 2 3 4 5 6 7
2 4 6 0 2 4 6
3 6 1 4 7 2 5
4 0 4 0 4 0 4
5 2 7 4 1 6 3
6 4 2 0 6 4 2
7 6 5 4 3 2 1

Let's solve the eq in mod 8:

$$9(2x + 7) - 6 \equiv 2x + 6$$

$$19 \cdot 2x + 19 \cdot 7 - 6 \equiv 2x + 6$$

$$38x + 133 - 6 \equiv 2x + 6 \quad \# \quad 133 \bmod 8 = 5$$

$$6x + 5 - 6 \equiv 2x + 6$$

Modular arithmetics (2)

addition mod 8

0 1 2 3 4 5 6 7
1 2 3 4 5 6 7 0
2 3 4 5 6 7 0 1
3 4 5 6 7 0 1 2
4 5 6 7 0 1 2 3
5 6 7 0 1 2 3 4
6 7 0 1 2 3 4 5
7 0 1 2 3 4 5 6

multiplication mod 8

1 2 3 4 5 6 7
2 4 6 0 2 4 6
3 6 1 4 7 2 5
4 0 4 0 4 0 4
5 2 7 4 1 6 3
6 4 2 0 6 4 2
7 6 5 4 3 2 1

Let's solve the eq in mod 8:

$$9(2x + 7) - 6 \equiv 2x + 6$$

$$19 \cdot 2x + 19 \cdot 7 - 6 \equiv 2x + 6$$

$$38x + 133 - 6 \equiv 2x + 6 \quad \# \quad 133 \bmod 8 = 5$$

$$6x + 5 - 6 \equiv 2x + 6$$

$$6x + 5 - 6 + 6 \equiv 2x + 6 + 6$$

Modular arithmetics (2)

addition mod 8

0 1 2 3 4 5 6 7
1 2 3 4 5 6 7 0
2 3 4 5 6 7 0 1
3 4 5 6 7 0 1 2
4 5 6 7 0 1 2 3
5 6 7 0 1 2 3 4
6 7 0 1 2 3 4 5
7 0 1 2 3 4 5 6

multiplication mod 8

1 2 3 4 5 6 7
2 4 6 0 2 4 6
3 6 1 4 7 2 5
4 0 4 0 4 0 4
5 2 7 4 1 6 3
6 4 2 0 6 4 2
7 6 5 4 3 2 1

Let's solve the eq in mod 8:

$$9(2x + 7) - 6 \equiv 2x + 6$$

$$19 \cdot 2x + 19 \cdot 7 - 6 \equiv 2x + 6$$

$$38x + 133 - 6 \equiv 2x + 6 \quad \# \quad 133 \bmod 8 = 5$$

$$6x + 5 - 6 \equiv 2x + 6$$

$$6x + 5 - 6 + 6 \equiv 2x + 6 + 6$$

$$6x + 5 \equiv 2x + 4 \quad \# \quad 12 \bmod 8 = 4$$

$$6x - 2x + 5 - 5 \equiv 2x - 2x + 4 - 5$$

Modular arithmetics (2)

addition mod 8	multiplication mod 8	Let's solve the eq in mod 8:
0 1 2 3 4 5 6 7	1 2 3 4 5 6 7	$9(2x + 7) - 6 \equiv 2x + 6$
1 2 3 4 5 6 7 0	2 4 6 0 2 4 6	$19 \cdot 2x + 19 \cdot 7 - 6 \equiv 2x + 6$
2 3 4 5 6 7 0 1	3 6 1 4 7 2 5	$38x + 133 - 6 \equiv 2x + 6 \quad \# \quad 133 \bmod 8 = 5$
3 4 5 6 7 0 1 2	4 0 4 0 4 0 4	$6x + 5 - 6 \equiv 2x + 6$
4 5 6 7 0 1 2 3	5 2 7 4 1 6 3	$6x + 5 - 6 + 6 \equiv 2x + 6 + 6$
5 6 7 0 1 2 3 4	6 4 2 0 6 4 2	$6x + 5 \equiv 2x + 4 \quad \# \quad 12 \bmod 8 = 4$
6 7 0 1 2 3 4 5	7 6 5 4 3 2 1	$6x - 2x + 5 - 5 \equiv 2x - 2x + 4 - 5$
7 0 1 2 3 4 5 6		$4x \equiv 7 \quad \# \quad -1 \bmod 8 = 7$

Now we do **NOT have multiplication inverse** for 4, ie. we cannot divide by 4 in modulo 8, ie. solve this equation We have only multiplication inverse for 1 which is 1; 3 which is 3; 5 which is 5, and 7 which is 7.

Modular arithmetics (3)

addition mod 11

0	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	0
2	3	4	5	6	7	8	9	10	0	1
3	4	5	6	7	8	9	10	0	1	2
4	5	6	7	8	9	10	0	1	2	3
5	6	7	8	9	10	0	1	2	3	4
6	7	8	9	10	0	1	2	3	4	5
7	8	9	10	0	1	2	3	4	5	6
8	9	10	0	1	2	3	4	5	6	7
9	10	0	1	2	3	4	5	6	7	8
10	0	1	2	3	4	5	6	7	8	9

multiplication mod 11

1	2	3	4	5	6	7	8	9	10
2	4	6	8	10	1	3	5	7	9
3	6	9	1	4	7	10	2	5	8
4	8	1	5	9	2	6	10	3	7
5	10	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	10	5
7	3	10	6	2	9	5	1	8	4
8	5	2	10	7	4	1	9	6	3
9	7	5	3	1	10	8	6	4	2
10	9	8	7	6	5	4	3	2	1

Modular arithmetics (3)

addition mod 11

0	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	0
2	3	4	5	6	7	8	9	10	0	1
3	4	5	6	7	8	9	10	0	1	2
4	5	6	7	8	9	10	0	1	2	3
5	6	7	8	9	10	0	1	2	3	4
6	7	8	9	10	0	1	2	3	4	5
7	8	9	10	0	1	2	3	4	5	6
8	9	10	0	1	2	3	4	5	6	7
9	10	0	1	2	3	4	5	6	7	8
10	0	1	2	3	4	5	6	7	8	9

multiplication mod 11

1	2	3	4	5	6	7	8	9	10
2	4	6	8	10	1	3	5	7	9
3	6	9	1	4	7	10	2	5	8
4	8	1	5	9	2	6	10	3	7
5	10	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	10	5
7	3	10	6	2	9	5	1	8	4
8	5	2	10	7	4	1	9	6	3
9	7	5	3	1	10	8	6	4	2
10	9	8	7	6	5	4	3	2	1

Let's solve in mod 11:

$$19(2x + 7) - 6 \equiv 2x + 6$$

Modular arithmetics (3)

addition mod 11

0	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	0
2	3	4	5	6	7	8	9	10	0	1
3	4	5	6	7	8	9	10	0	1	2
4	5	6	7	8	9	10	0	1	2	3
5	6	7	8	9	10	0	1	2	3	4
6	7	8	9	10	0	1	2	3	4	5
7	8	9	10	0	1	2	3	4	5	6
8	9	10	0	1	2	3	4	5	6	7
9	10	0	1	2	3	4	5	6	7	8
10	0	1	2	3	4	5	6	7	8	9

multiplication mod 11

1	2	3	4	5	6	7	8	9	10
2	4	6	8	10	1	3	5	7	9
3	6	9	1	4	7	10	2	5	8
4	8	1	5	9	2	6	10	3	7
5	10	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	10	5
7	3	10	6	2	9	5	1	8	4
8	5	2	10	7	4	1	9	6	3
9	7	5	3	1	10	8	6	4	2
10	9	8	7	6	5	4	3	2	1

Let's solve in mod 11:

$$19(2x + 7) - 6 \equiv 2x + 6$$

$$19 \cdot 2x + 19 \cdot 7 - 6 \equiv 2x + 6$$

Modular arithmetics (3)

addition mod 11

0	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	0
2	3	4	5	6	7	8	9	10	0	1
3	4	5	6	7	8	9	10	0	1	2
4	5	6	7	8	9	10	0	1	2	3
5	6	7	8	9	10	0	1	2	3	4
6	7	8	9	10	0	1	2	3	4	5
7	8	9	10	0	1	2	3	4	5	6
8	9	10	0	1	2	3	4	5	6	7
9	10	0	1	2	3	4	5	6	7	8
10	0	1	2	3	4	5	6	7	8	9

multiplication mod 11

1	2	3	4	5	6	7	8	9	10
2	4	6	8	10	1	3	5	7	9
3	6	9	1	4	7	10	2	5	8
4	8	1	5	9	2	6	10	3	7
5	10	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	10	5
7	3	10	6	2	9	5	1	8	4
8	5	2	10	7	4	1	9	6	3
9	7	5	3	1	10	8	6	4	2
10	9	8	7	6	5	4	3	2	1

Let's solve in mod 11:

$$19(2x + 7) - 6 \equiv 2x + 6$$

$$19 \cdot 2x + 19 \cdot 7 - 6 \equiv 2x + 6$$

$$5x + 1 - 6 \equiv 2x + 6$$

Modular arithmetics (3)

addition mod 11

0	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	0
2	3	4	5	6	7	8	9	10	0	1
3	4	5	6	7	8	9	10	0	1	2
4	5	6	7	8	9	10	0	1	2	3
5	6	7	8	9	10	0	1	2	3	4
6	7	8	9	10	0	1	2	3	4	5
7	8	9	10	0	1	2	3	4	5	6
8	9	10	0	1	2	3	4	5	6	7
9	10	0	1	2	3	4	5	6	7	8
10	0	1	2	3	4	5	6	7	8	9

multiplication mod 11

1	2	3	4	5	6	7	8	9	10
2	4	6	8	10	1	3	5	7	9
3	6	9	1	4	7	10	2	5	8
4	8	1	5	9	2	6	10	3	7
5	10	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	10	5
7	3	10	6	2	9	5	1	8	4
8	5	2	10	7	4	1	9	6	3
9	7	5	3	1	10	8	6	4	2
10	9	8	7	6	5	4	3	2	1

Let's solve in mod 11:

$$19(2x + 7) - 6 \equiv 2x + 6$$

$$19 \cdot 2x + 19 \cdot 7 - 6 \equiv 2x + 6$$

$$5x + 1 - 6 \equiv 2x + 6$$

$$5x + 1 - 6 + 6 \equiv 2x + 6 + 6$$

Modular arithmetics (3)

addition mod 11

0	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	0
2	3	4	5	6	7	8	9	10	0	1
3	4	5	6	7	8	9	10	0	1	2
4	5	6	7	8	9	10	0	1	2	3
5	6	7	8	9	10	0	1	2	3	4
6	7	8	9	10	0	1	2	3	4	5
7	8	9	10	0	1	2	3	4	5	6
8	9	10	0	1	2	3	4	5	6	7
9	10	0	1	2	3	4	5	6	7	8
10	0	1	2	3	4	5	6	7	8	9

multiplication mod 11

1	2	3	4	5	6	7	8	9	10
2	4	6	8	10	1	3	5	7	9
3	6	9	1	4	7	10	2	5	8
4	8	1	5	9	2	6	10	3	7
5	10	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	10	5
7	3	10	6	2	9	5	1	8	4
8	5	2	10	7	4	1	9	6	3
9	7	5	3	1	10	8	6	4	2
10	9	8	7	6	5	4	3	2	1

Let's solve in mod 11:

$$19(2x + 7) - 6 \equiv 2x + 6$$

$$19 \cdot 2x + 19 \cdot 7 - 6 \equiv 2x + 6$$

$$5x + 1 - 6 \equiv 2x + 6$$

$$5x + 1 - 6 + 6 \equiv 2x + 6 + 6$$

$$5x + 1 \equiv 2x + 1$$

Modular arithmetics (3)

addition mod 11

0	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	0
2	3	4	5	6	7	8	9	10	0	1
3	4	5	6	7	8	9	10	0	1	2
4	5	6	7	8	9	10	0	1	2	3
5	6	7	8	9	10	0	1	2	3	4
6	7	8	9	10	0	1	2	3	4	5
7	8	9	10	0	1	2	3	4	5	6
8	9	10	0	1	2	3	4	5	6	7
9	10	0	1	2	3	4	5	6	7	8
10	0	1	2	3	4	5	6	7	8	9

multiplication mod 11

1	2	3	4	5	6	7	8	9	10
2	4	6	8	10	1	3	5	7	9
3	6	9	1	4	7	10	2	5	8
4	8	1	5	9	2	6	10	3	7
5	10	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	10	5
7	3	10	6	2	9	5	1	8	4
8	5	2	10	7	4	1	9	6	3
9	7	5	3	1	10	8	6	4	2
10	9	8	7	6	5	4	3	2	1

Let's solve in mod 11:

$$\begin{aligned}19(2x + 7) - 6 &\equiv 2x + 6 \\19 \cdot 2x + 19 \cdot 7 - 6 &\equiv 2x + 6 \\5x + 1 - 6 &\equiv 2x + 6 \\5x + 1 - 6 + 6 &\equiv 2x + 6 + 6 \\5x + 1 &\equiv 2x + 1 \\x &\equiv 0\end{aligned}$$

We have solution: $\{.., -22, -11, 0, 11, 22, ...\}$ As in each row of mult table there is 1 we have inverse for each congruence group!

Modular arithmetics (4)

addition mod 13

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

multiplication mod 13

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

As in each row of mult table there is 1 we have inverse for each congruence group! => we want to work with mod **PRIME** as we want inverses!

Modular arithmetics (4)

addition mod 13

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

multiplication mod 13

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

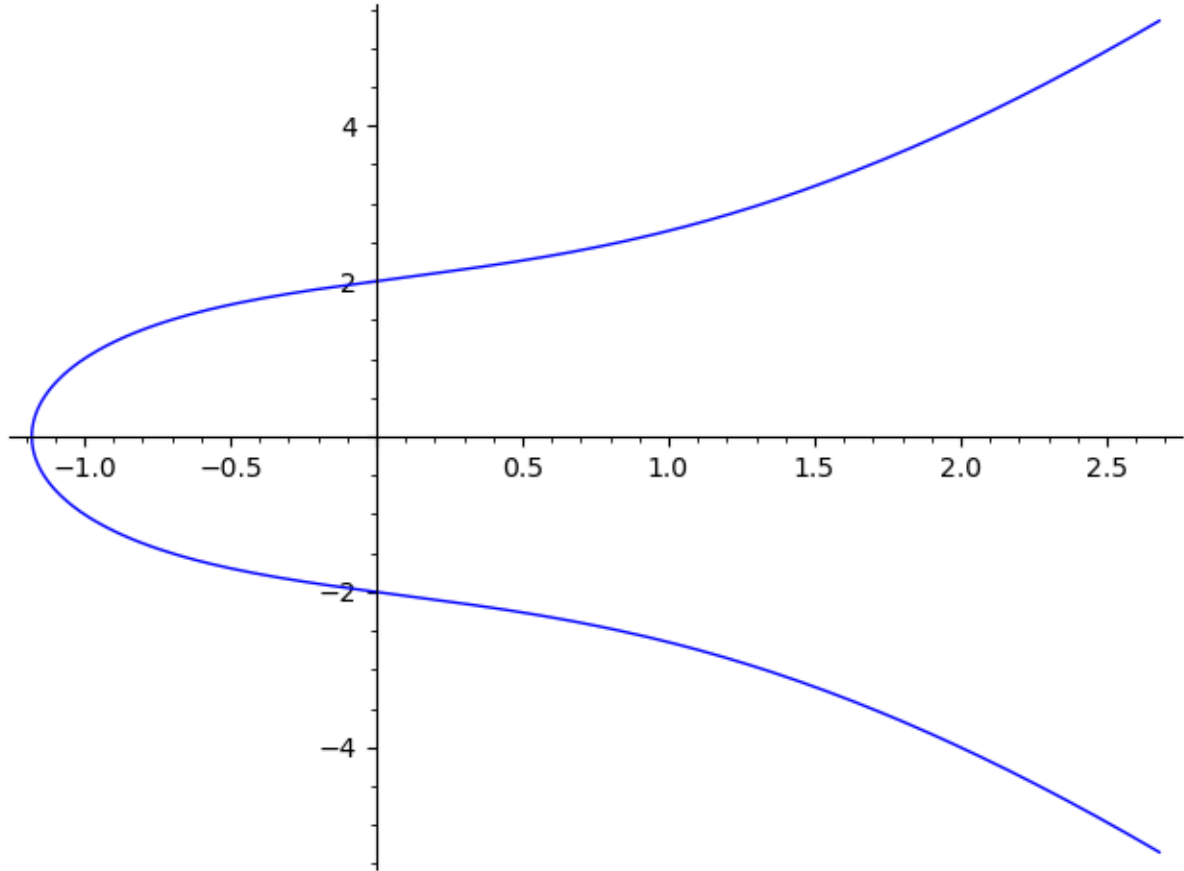
diagonal: 1 2 3 4 5 6 7 8 9 10 11 12
val: 1 4 9 3 12 10 10 12 3 9 4 1

- not always square is possible within modulus
- 1, 3, 4, 9, 10, 12

are quadratic residues

Elliptic curves (1)

```
sage: # Let's plot the following  
elliptic curve in R  
sage: #  $y^2 = x^3 + 2x + 4$  in R  
  
sage: E = EllipticCurve([2,4]);  
sage: P = E.plot()  
sage: P.save("ellipticR.png")
```



Elliptic curves (2)

$$y^2 \equiv x^3 + 2x + 4 \pmod{13}$$

$x=0, y^2 \equiv 4 \Rightarrow (0,2) \text{ and } (0,11) \rightarrow$ two points

$x=1, y^2 \equiv 1 + 2 + 4 = 7 \rightarrow$ no point

$x=2, y^2 \equiv 8 + 4 + 4 = 16 \pmod{13} = 3 \rightarrow (2,4) \text{ and } (2,9)$

$x=3, y^2 \equiv 1 + 6 + 4 = 11 \rightarrow$ no point

$x=4, y^2 \equiv 12 + 8 + 4 = 24 \pmod{13} = 11 \rightarrow$ no point

$x=5, y^2 \equiv 8 + 10 + 4 = 9 \rightarrow (5,3) \text{ and } (5,10)$

$x=6, y^2 \equiv 8 + 12 + 4 = 24 \pmod{13} = 11 \rightarrow$ no point

$x=7, y^2 \equiv 5 + 14 + 4 = 23 \pmod{13} = 10 \rightarrow (7,6) \text{ and } (7,7)$

$x=8, y^2 \equiv 5 + 16 + 4 = 25 \pmod{13} = 12 \rightarrow (8,5) \text{ and } (8,8)$

$x=9, y^2 \equiv 1 + 18 + 4 = 23 \pmod{13} = 10 \rightarrow (9,6) \text{ and } (9,7)$

$x=10, y^2 \equiv 12 + 20 + 4 = 36 \pmod{13} = 10 \rightarrow (10,6) \text{ and } (10,7)$

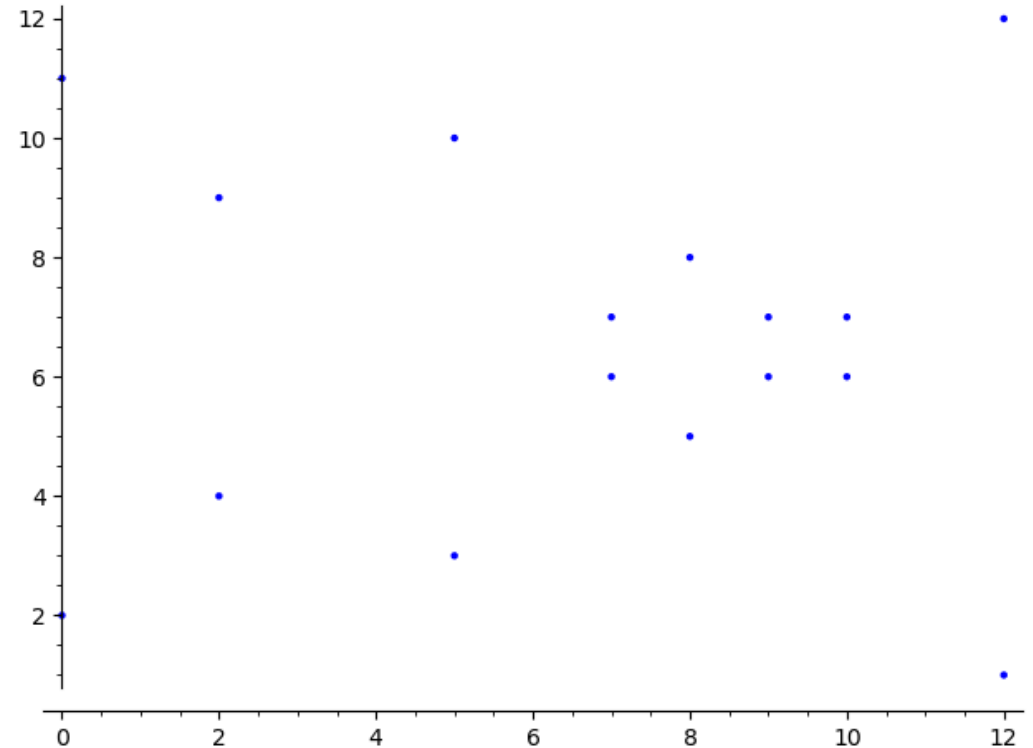
$x=11, y^2 \equiv 5 + 22 + 4 = 31 \pmod{13} = 5 \rightarrow$ no point

$x=12, y^2 \equiv 12 + 24 + 4 = 40 \pmod{13} = 1 \rightarrow (12,1) \text{ and } (12,12)$

For some x there are no solutions when we have mod 13, for the rest we have two!

Elliptic curves (3)

```
sage: F13=GF(13)
sage: a = F13(2)
sage: b = F13(4)
sage: # discriminant obeys condition
sage: F13(6)*(F13(4)*a^3+F13(27)*b^2) != F13(0)
True
sage: E = EllipticCurve(F13,[a,b]) #  $y^2 = x^3 + 2x + 4$ 
sage: P = E(0,2) #  $2^2 = 0^3 + 2*0 + 4 \pmod{13}$ 
sage: P.xy()
(0, 2)
sage: INF=E(0)
sage: try:
....:     INF.xy()
....: except ZeroDivisionError:
....:     pass
....:
sage: P = E.plot()
sage: P.save("elliptic13.png")
```



Modular arithmetics (5)

addition mod 13

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

Addition forms a **group** as

- 0 is identity element
- addition is associative op
- addition is closed op
- each element has the inverse

Modular arithmetics (5)

multiplication mod 13

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

Mult forms a **group** as

- 1 is identity element
- mult is associative op
- mult is closed op
- each element has the inverse (thanks to p being prime)

Modular arithmetics (5)

multiplication mod 13

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

- $3 \cdot 3 = 9$
- $3 \cdot 3 \cdot 3 = 1$
- $3 \cdot 3 \cdot 3 \cdot 3 = 3$

we can NOT generate EACH element -> 3 is not generator

Modular arithmetics (5)

multiplication mod 13

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

- $8 \cdot 8 = 12$
- $8 \cdot 8 \cdot 8 = 5$
- $8 \cdot 8 \cdot 8 \cdot 8 = 1$

we can NOT generate EACH element -> 8 is not generator

Modular arithmetics (5)

multiplication mod 13

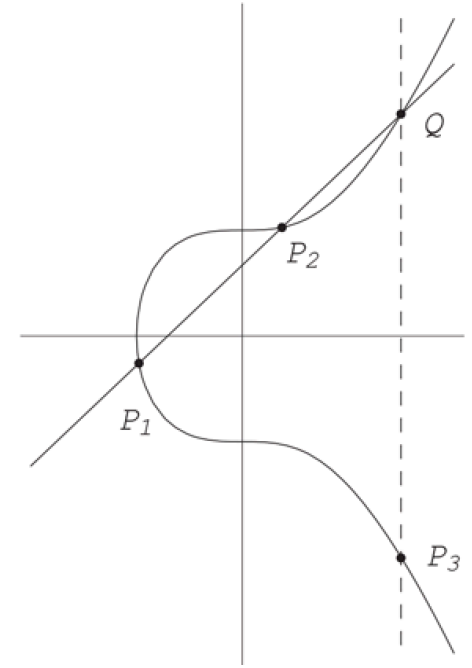
1	2	3	4	5	6	7	8	9	10	11	12
2	4	6	8	10	12	1	3	5	7	9	11
3	6	9	12	2	5	8	11	1	4	7	10
4	8	12	3	7	11	2	6	10	1	5	9
5	10	2	7	12	4	9	1	6	11	3	8
6	12	5	11	4	10	3	9	2	8	1	7
7	1	8	2	9	3	10	4	11	5	12	6
8	3	11	6	1	9	4	12	7	2	10	5
9	5	1	10	6	2	11	7	3	12	8	4
10	7	4	1	11	8	5	2	12	9	6	3
11	9	7	5	3	1	12	10	8	6	4	2
12	11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

- $2 \cdot 2 = 4$
- $2 \cdot 2 \cdot 2 = 8$
- $2 \cdot 2 \cdot 2 \cdot 2 = 3$
- $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 6$
- $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 12$
- $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 11$
- $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 9$
- $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 5$
- $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 10$
- $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 7$
- $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 1$

we can generate EVERY element -> 2 is **generator**, group is **cyclic**

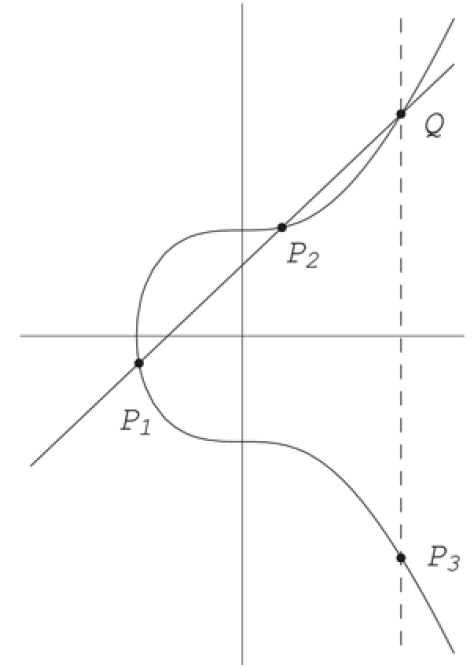
Elliptic curves (4)

Visually addition looks like here for elliptic curves with one remark: it is modulo PRIME



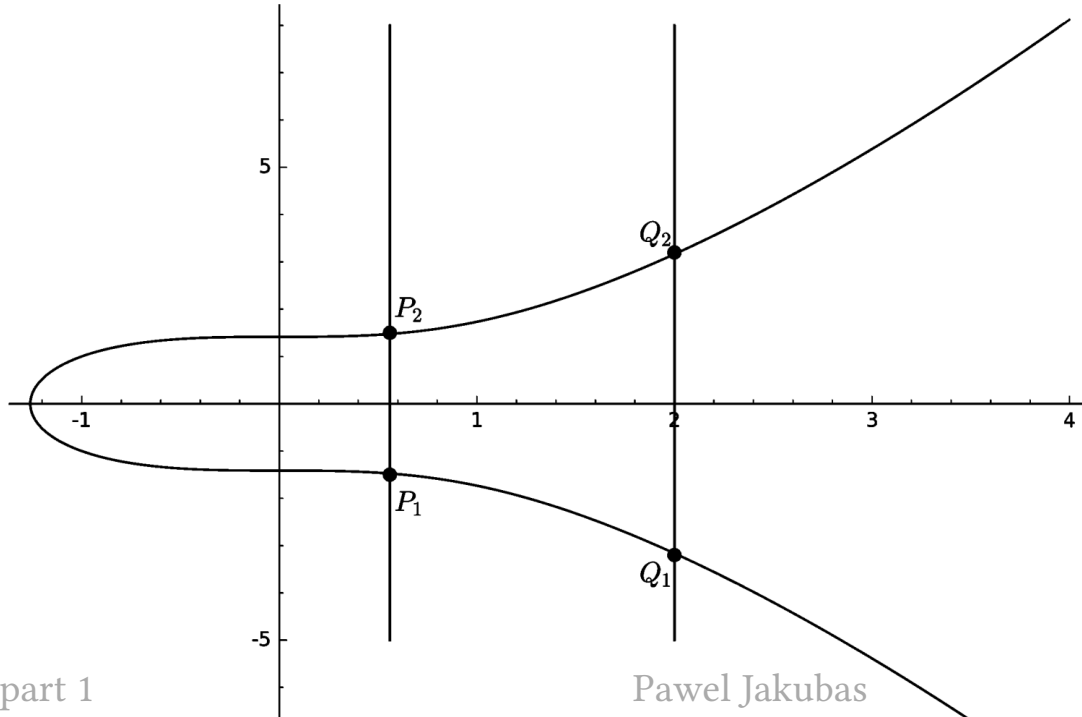
Elliptic curves (4)

It is called **Chord-and-tangent rule**
visually $P_1 + P_2 = P_3$



Elliptic curves (4)

$y=\text{INF}$ is identity element, and because of that $P_1^{-1} = P_2$
 $Q_1^{-1} = Q_2$



Elliptic curves (4)

Chord-and-tangent rule algebraically

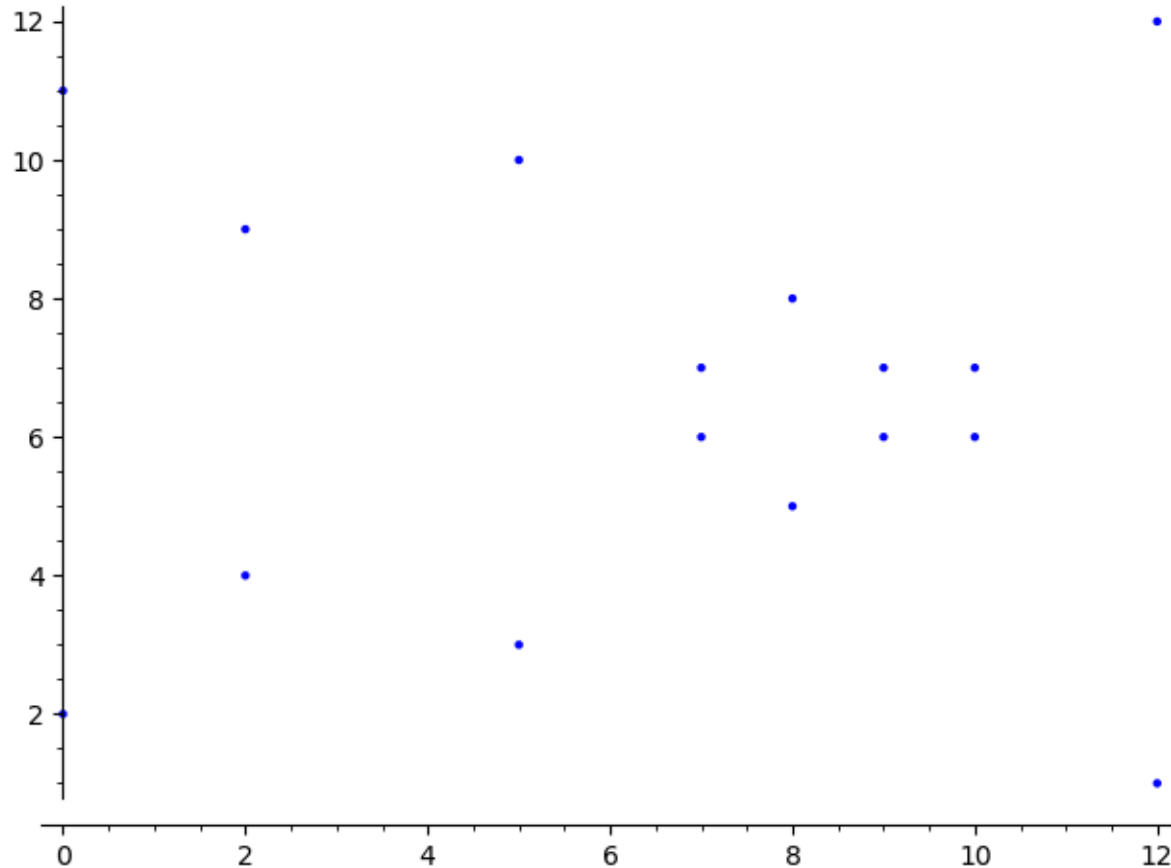
(Tangent Rule) If $P = (x, y)$ with $y \neq 0$, the group law $P \oplus P = (x', y')$ is defined as follows:

$$x' = \left(\frac{3x^2 + a}{2y} \right)^2 - 2x \quad , \quad y' = \left(\frac{3x^2 + a}{2y} \right) (x - x') - y$$

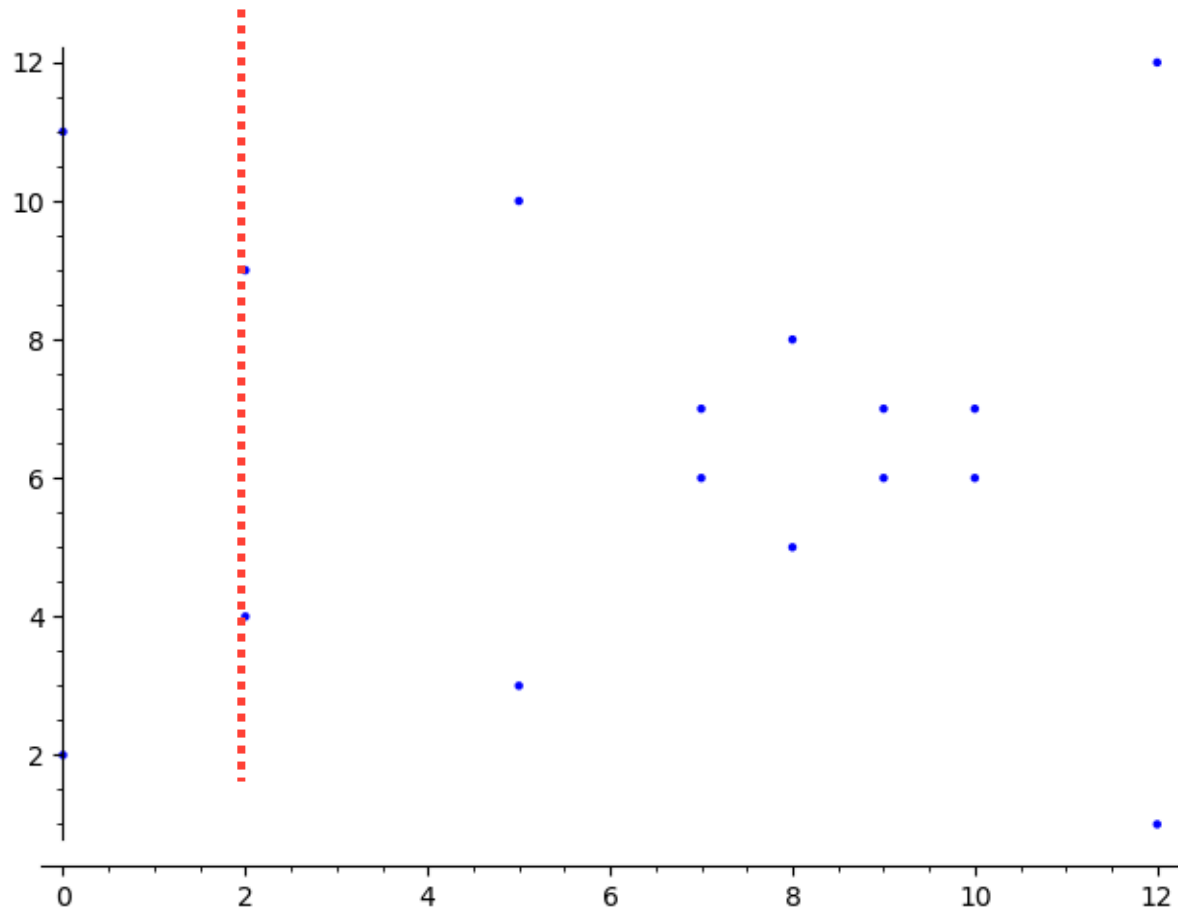
(Chord Rule) If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ such that $x_1 \neq x_2$, the group law $R = P \oplus Q$ with $R = (x_3, y_3)$ is defined as follows:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 \quad , \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3) - y_1$$

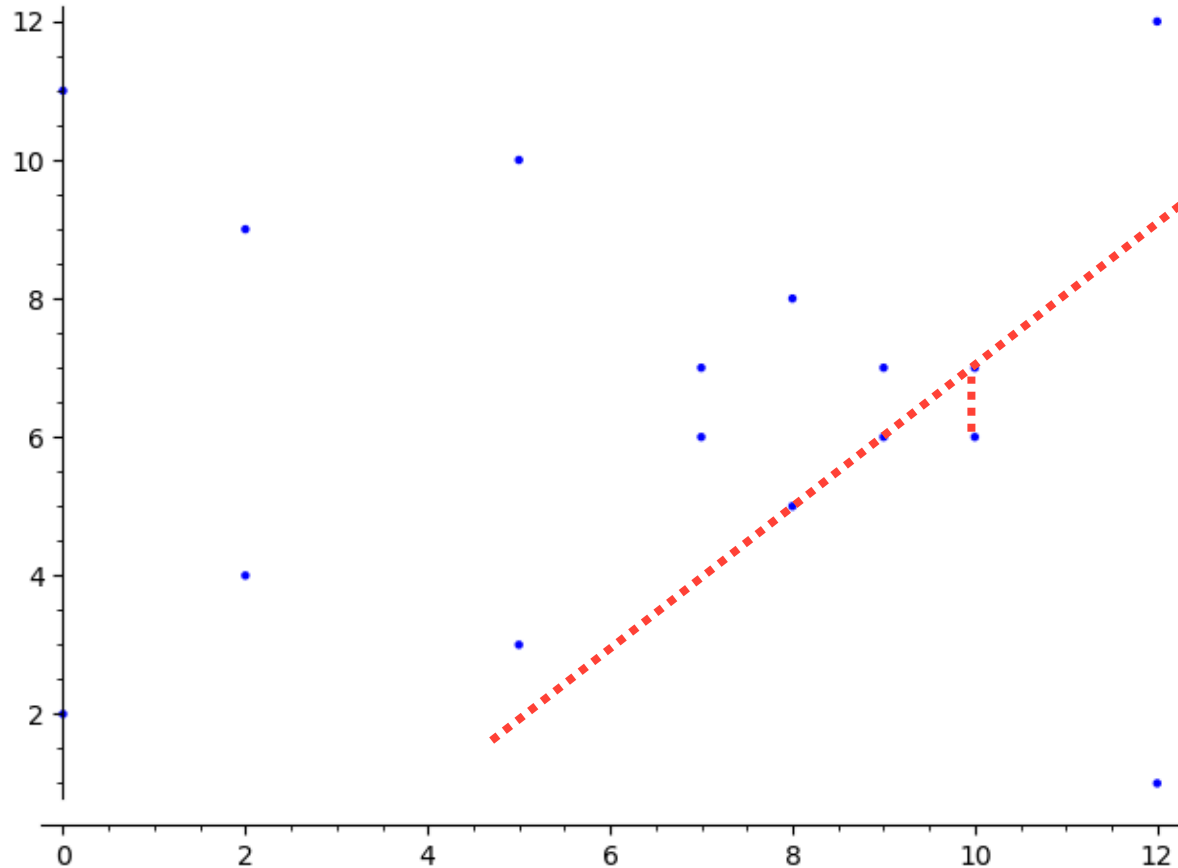
Elliptic curves (5) (mod 13)



Elliptic curves (5) (mod 13)



Elliptic curves (5) (mod 13)



Elliptic curves (6) (mod 13)

```
sage: F13 = GF(13)
sage: a = F13(2)
sage: b = F13(4)
sage: E = EllipticCurve(F13,[a,b]) #  $y^2 = x^3 + 2x + 4$ 
sage: INF=E(0)
sage: E(2,4) + E(2,9) == INF
True
sage: E(8,5) + E(9,6) == E(10,7)
False
sage: E(8,5) + E(9,6) == E(10,6)
True
```

That's it! More to come in the future



Get in touch 🖐️

📄 My notes on GitHub