ZERO KNOWLEDGE PROOFS

by Marija Mikić

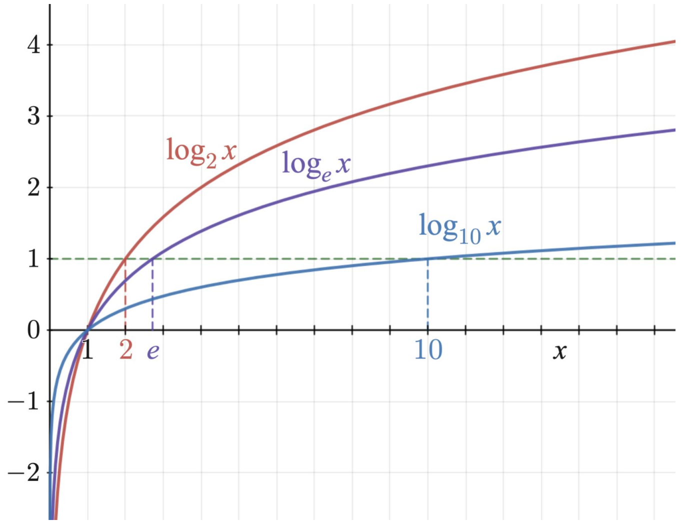
ZKP Course

Class 2: Discrete log

МАТЕМАТИЧКА АКАДЕМИЈА

Logarithm

Given a positive real number *g* such that $g \neq 1$, the logarithm of a positive real number b with respect to base *g* is the exponent by which *g* must be raised to yield b. In other words, the logarithm of b to base *g* is the unique real number x such that **g^x = b**. The logarithm is denoted "$\mathbf{\log_g b = x}$".

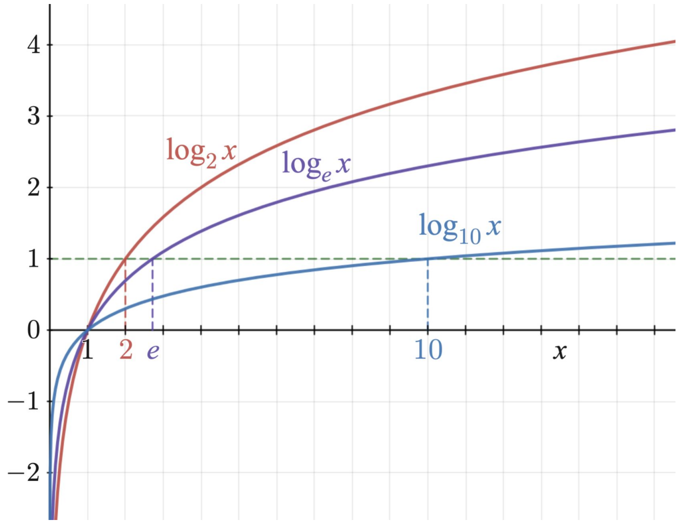


Example 1. $\log_2 8$?

There's More 👉

Logarithm

Given a positive real number *g* such that *g* ≠ 1, the logarithm of a positive real number b with respect to base *g* is the exponent by which *g* must be raised to yield b. In other words, the logarithm of b to base *g* is the unique real number x such that ***g*^x=b**. The logarithm is denoted "$\mathbf{log_g b=x}$".



Example 1. $\log_2 8$?

$2^x = 8$

$x = 3$

$\log_2 8 = 3$

There's More 👉

Cyclic group ($\mathbb{Z}p^*$,·)

$\mathbb{Z}p^*$ = {1, ..., p-1} where p is prime number. Operation · define:

$$a \cdot b = a * b \bmod p$$

МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

Cyclic group $(\mathbb{Z}p^*, \cdot)$

$\mathbb{Z}p^*$ = {1, ..., p-1} where p is prime number. Operation · define:

$$a \cdot b = a * b \bmod p$$

Properties of $(\mathbb{Z}p^*, \cdot)$:

1) If a, b $\in \mathbb{Z}p^*$, then $a \cdot b \in \mathbb{Z}p^*$;
2) If a, b, c $\in \mathbb{Z}p^*$, then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
3) If a $\in \mathbb{Z}p^*$, then $a \cdot 1 = a$;
4) If a $\in \mathbb{Z}p^*$, then there is b $\in \mathbb{Z}p^*$ such that $a \cdot b = 1$.

$(\mathbb{Z}p^*, \cdot)$ is a **group**. **Cyclic?**

There's More 👉

Cyclic group ($\mathbb{Z}p^*$,·)

$\mathbb{Z}p^*$ = {1, …, p-1} where p is prime number. Operation ·define:

a·b = a*b mod p

Properties of ($\mathbb{Z}p^*$, ·):

1) If a, b ∈ $\mathbb{Z}p^*$, then a·b∈ $\mathbb{Z}p^*$;
2) If a, b, c ∈ $\mathbb{Z}p^*$, then a·(b·c) = (a·b)·c;
3) If a ∈ $\mathbb{Z}p^*$, then a·1 = a;
4) If a ∈ $\mathbb{Z}p^*$, then there is b ∈ $\mathbb{Z}p^*$ such that a·b = 1.

($\mathbb{Z}p^*$, ·) is a **group**.

Example 2. ($\mathbb{Z}_{11}^*$, ·)

$\mathbb{Z}_{11}^*$={1, 2, …,10}. Let g = 2.

$g = 2 \bmod 11 = 2$
$g^2 = 2^2 \bmod 11 = 4$
$g^3 = 2^3 \bmod 11 = 8$
$g^4 = 2^4 \bmod 11 = 5$
$g^5 = 2^5 \bmod 11 = 10$
$g^6 = 2^6 \bmod 11 = 9$
$g^7 = 2^7 \bmod 11 = 7$
$g^8 = 2^8 \bmod 11 = 3$
$g^9 = 2^9 \bmod 11 = 6$
$g^{10} = 2^{10} \bmod 11 = 1$

МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

Cyclic group ($\mathbb{Z}p^*$,·)

$\mathbb{Z}p^*$ = {1, ..., p-1} where p is prime number. Operation · define:

a·b = a*b mod p

Properties of ($\mathbb{Z}p^*$, ·):

1) If a, b $\in \mathbb{Z}p^*$, then a·b $\in \mathbb{Z}p^*$;
2) If a, b, c $\in \mathbb{Z}p^*$, then a·(b·c) = (a·b)·c;
3) If a $\in \mathbb{Z}p^*$, then a·1 = a;
4) If a $\in \mathbb{Z}p^*$, then there is b $\in \mathbb{Z}p^*$ such that a·b = 1.

($\mathbb{Z}p^*$, ·) is a **group**.

Example 2. ($\mathbb{Z}_{11}^*$, ·)

$\mathbb{Z}_{11}^*$ = {1, 2, ...,10}. Let g = 2.

g = 2 mod 11 = **2**
$g^2 = 2^2$ mod 11 = **4**
$g^3 = 2^3$ mod 11 = 8
$g^4 = 2^4$ mod 11 = 5
$g^5 = 2^5$ mod 11 = 10
$g^6 = 2^6$ mod 11 = 9
$g^7 = 2^7$ mod 11 = 7
$g^8 = 2^8$ mod 11 = 3
$g^9 = 2^9$ mod 11 = 6
$g^{10} = 2^{10}$ mod 11 = 1

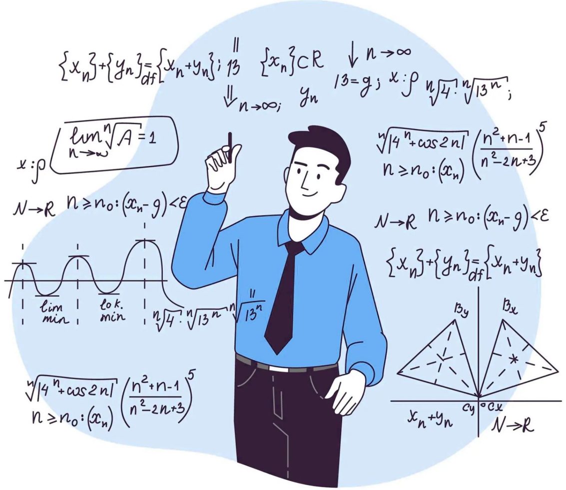
$g^{11} = 2^{11}$ mod 11 = **2**
$g^{12} = 2^{12}$ mod 11 = **4** **=> g=2 is generator of $\mathbb{Z}_{11}^*$**

Cyclic group ($\mathbb{Z}p^*, \cdot$)

We say that $g \in \mathbb{Z}p^*$ is a **generator** of $\mathbb{Z}p^*$ if $\{g, g^2, \ldots, g^{p-1}\} = \mathbb{Z}p^*$.

A **cyclic group** is a group with at least one generator.

$\mathbb{Z}p^* = \{1, \ldots, p-1\}$, where p is prime number, are always cyclic group.



МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

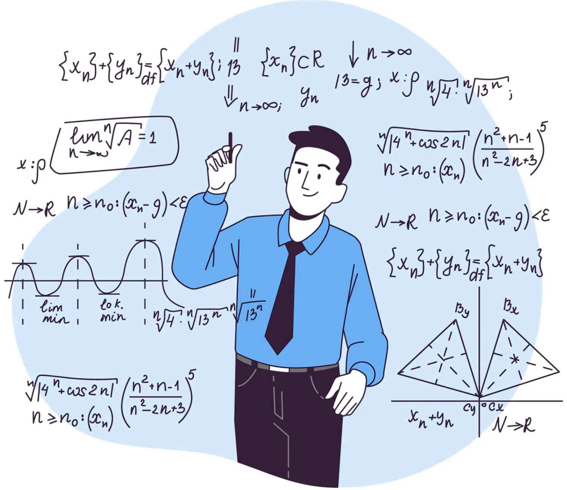
Cyclic group ($\mathbb{Z}p^*$,·)

We say that $g \in \mathbb{Z}p^*$ is a **generator** of $\mathbb{Z}p^*$ if $\{g, g^2, \ldots, g^{p-1}\} = \mathbb{Z}p^*$.

A **cyclic group** is a group with at least one generator.

$\mathbb{Z}p^* = \{1, \ldots, p-1\}$, where p is prime number, are always cyclic group.

Is there a faster way to check if an element of a cyclic group is a generator?



МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

Cyclic group (ℤp*,·)

Theorem. Let g∈ ℤp* . Element g is a generator of ℤp* if and only if **g^((p-1)/q) ≠ 1 mod p**, for all primes q such that q|(p-1).

Example 2. Find all generators of $\mathbb{Z}_{11}^*$.

p = 11 then p-1 = 10 = 2 * 5. So, 2 and 5 are primes that 2|10 and 5|10.

We know that g = 2 is generator, but now we will use the theorem.

МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

Cyclic group $(\mathbb{Z}p^*,\cdot)$

Theorem. Let $g \in \mathbb{Z}p^*$. Element g is a generator of $\mathbb{Z}p^*$ if and only if **$g^{((p-1)/q)} \neq 1 \bmod p$**, for all primes q such that $q|(p-1)$.

Example 2. Find all generators of $\mathbb{Z}_{11}^*$.

p=11 then p-1 = 10 = 2*5. So, 2 and 5 are primes that $2|10$ and $5|10$.

We know that g=2 is generator, but now we will use the theorem.

$2^{(10/2)} = 2^5 \bmod 11 = 10 \neq 1$ ✅

МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

Cyclic group (ℤp*,·)

Theorem. Let g∈ ℤp* . Element g is a generator of ℤp* if and only if **g^((p-1)/q) ≠ 1 mod p**, for all primes q such that q|(p-1).

Example 2. Find all generators of $\mathbb{Z}_{11}^*$.

p=11 then p-1=10=2*5. So, 2 and 5 are primes that 2|10 and 5|10.

We know that g=2 is generator, but now we will use the theorem.

2^(10/2) = 2^5 mod 11 = 10 ≠1 ✅
2^(10/5) = 2^2 mod 11 = 4 ≠ 1 ✅

МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

Cyclic group ($\mathbb{Z}p^*$,·)

Theorem. Let g∈ $\mathbb{Z}p^*$. Element g is a generator of $\mathbb{Z}p^*$ if and only if **g^((p-1)/q) ≠ 1 mod p**, for all primes q such that q|(p-1).

Example 2. Find all generators of $\mathbb{Z}_{11}^*$.

p=11 then p-1 = 10 = 2*5. So, 2 and 5 are primes that 2|10 and 5|10.

We know that g=2 is generator, but now we will use the theorem.

2^(10/2) = 2^5 mod 11 = 10 ≠ 1 ✅
2^(10/5) = 2^2 mod 11 = 4 ≠ 1 ✅
So, **g=2 is generator of $\mathbb{Z}_{11}^*$.**

There's More 👉

Cyclic group ($\mathbb{Z}p^*$,·)

Theorem. Let $g \in \mathbb{Z}p^*$. Element g is a generator of $\mathbb{Z}p^*$ if and only if **$g^{((p-1)/q)} \neq 1 \bmod p$**, for all primes q such that $q|(p-1)$.

Example 2. Find all generators of $\mathbb{Z}_{11}^*$.

p=11 then p-1 = 10 = 2*5. So, 2 and 5 are primes that 2|10 and 5|10.

We know that g=2 is generator, but now we will use the theorem.

$2^{(10/2)} = 2^5 \bmod 11 = 10 \neq 1$ ✅

$2^{(10/5)} = 2^2 \bmod 11 = 4 \neq 1$ ✅

So, **g=2 is generator of $\mathbb{Z}_{11}^*$.**

$3^{(10/2)} = 3^5 \bmod 11 = 1$ ❌

МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

Cyclic group (ℤp*,·)

Theorem. Let g∈ ℤp* . Element g is a generator of ℤp* if and only if **g^((p-1)/q) ≠ 1 mod p**, for all primes q such that q|(p-1).

Example 2. Find all generators of $\mathbb{Z}_{11}^*$.

p=11 then p-1 = 10 = 2*5. So, 2 and 5 are primes that 2|10 and 5|10.

We know that g=2 is generator, but now we will use the theorem.

2^(10/2) = 2^5 mod 11 = 10 ≠ 1 ✅
2^(10/5) = 2^2 mod 11 = 4 ≠ 1 ✅
So, g=2 is generator of $\mathbb{Z}_{11}^*$.

3^(10/2) = 3^5 mod 11 = 1 ❌
So, g=3 is NOT generator of $\mathbb{Z}_{11}^*$.
⋮

МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

Cyclic group ($\mathbb{Z}p^*$,·)

Theorem. Let g∈ $\mathbb{Z}p^*$. Element g is a generator of $\mathbb{Z}p^*$ if and only if **g^((p-1)/q) ≠ 1 mod p**, for all primes q such that q|(p-1).

Example 2. Find all generators of $\mathbb{Z}_{11}^*$.

p=11 then p-1 = 10 = 2*5. So, 2 and 5 are primes that 2|10 and 5|10.

We know that g=2 is generator, but now we will use the theorem.

2^(10/2) = 2^5 mod 11 = 10 ≠ 1 ✅
2^(10/5) = 2^2 mod 11 = 4 ≠ 1 ✅
So, g=2 is generator of $\mathbb{Z}_{11}^*$.

3^(10/2) = 3^5 mod 11 = 1 ❌
So, g=3 is NOT generator of $\mathbb{Z}_{11}^*$.

⋮

We wil get that generators of $\mathbb{Z}_{11}^*$ are 2, 6, 7 and 8, so
$\mathbb{Z}_{11}^*=\{2,2^2, ..., 2^{10}\}$ i.e. $\mathbb{Z}_{11}^*=\{6,6^2, ..., 6^{10}\}$ i.e. $\mathbb{Z}_{11}^*=\{7,7^2, ..., 7^{10}\}$ i.e. $\mathbb{Z}_{11}^*=\{8,8^2, ..., 8^{10}\}$.

МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

Discrete logarithm

Let g be generator of $\mathbb{Z}p^*$. Then we know that $\{g, g^2,\ldots,g^{p-1}\}=\mathbb{Z}p^*$.

Little Fermat's theorem: $g^{p-1}=1$.

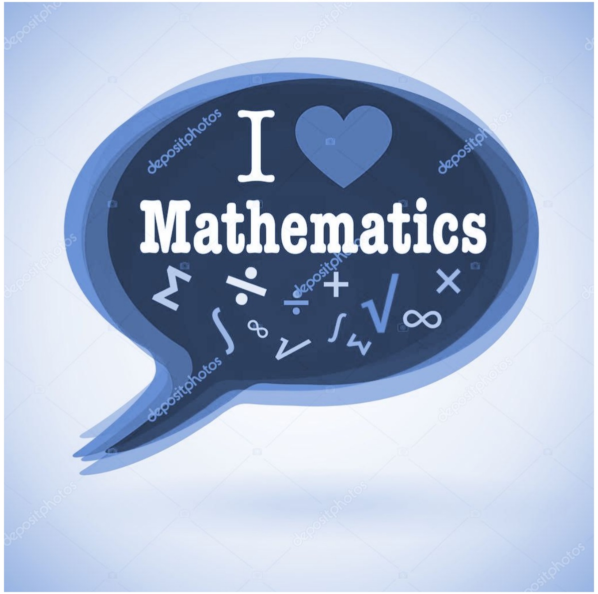
So, **$\mathbb{Z}p^*=\{1, g, g^2,\ldots, g^{p-2}\}$**.

If $b \in \mathbb{Z}p^*$ then b = g^x for some unique $0 \leq x \leq p-2$.

So, **x is discrete logarithm of b to base g** i.e.

log_g b = x ⇔ g^x = b in $\mathbb{Z}p^*$.

In $\mathbb{Z}p^*$: $0 \leq$ log_g b $\leq p-2$.



You can find more information on this link:

Link 1 >

Discrete logarithm problem

Example 3. Find $\log_7 8$ in $\mathbb{Z}_{17}^*$.

$\mathbb{Z}_{17}^* = \{1, 2, \ldots, 16\}$. Note that $g = 7$ is generator of $\mathbb{Z}_{17}^*$.

$g^2 = 7^2 \bmod 17 =$ **15**;

МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

Discrete logarithm problem

Example 3. Find $\log_7 8$ in $\mathbb{Z}_{17}^*$.

$\mathbb{Z}_{17}^*=\{1, 2, \ldots,16\}$. Note that $g=7$ is generator of $\mathbb{Z}_{17}^*$.

$g^2 = 7^2 \bmod 17 = 15$;

$g^3 = 7^3 \bmod 17 = \mathbf{3}$;

МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

Discrete logarithm problem

Example 3. Find $\log_7 8$ in $\mathbb{Z}_{17}^*$.

$\mathbb{Z}_{17}^*=\{1, 2, \ldots, 16\}$. Note that g=7 is generator of $\mathbb{Z}_{17}^*$.

$g^2 = 7^2 \bmod 17 = 15;$

$g^3 = 7^3 \bmod 17 = 3;$

$\vdots$

$g^{14} = 7^{14} \bmod 17 = \mathbf{8};$

So, $\mathbf{\log_7 8 = 14}$.

МАТЕМАТИЧКА АКАДЕМИЈА

There's More 👉

Discrete logarithm problem

Example 3. Find $\log_7 8$ in $\mathbb{Z}_{17}^*$.

$\mathbb{Z}_{17}^*=\{1, 2, ...,16\}$. Note that g=7 is generator of $\mathbb{Z}_{17}^*$.

$g^{14}= 7^{14} \bmod 17 = 8$;

So, **$\log_7 8 = 14$**.

DLP - Discrete Logarithm Problem

Given:

1) p a prime number;
2) g a generator of $\mathbb{Z}p^*$;
3) $b \in \mathbb{Z}p^*$,

find the x, such that x ∈ {0, 1, ...,p-2} and g^x = b mod p i.e. find log_g b.

There's More 👉

Discrete logarithm problem

Example 3. Find $\log_7 8$ in $\mathbb{Z}_{17}^*$.

$\mathbb{Z}_{17}^*=\{1, 2, ..., 16\}$. Note that g=7 is generator of $\mathbb{Z}_{17}^*$.

$g^{14}=7^{14} \bmod 17=8$

So, $\log_7 8= 14$.

If p is "large" and g is generator of ℤp* then finding log_g b is an "intractable" problem.

DLP - Discrete Logarithm Problem

Given:

1) p a prime number;
2) g a generator of ℤp*;
3) b ∈ ℤp*,

find the x, such that x ∈ {0, 1, ...,p-2} and g^x = b mod p i.e. find log_g b.

There's More 👉

Thank you!