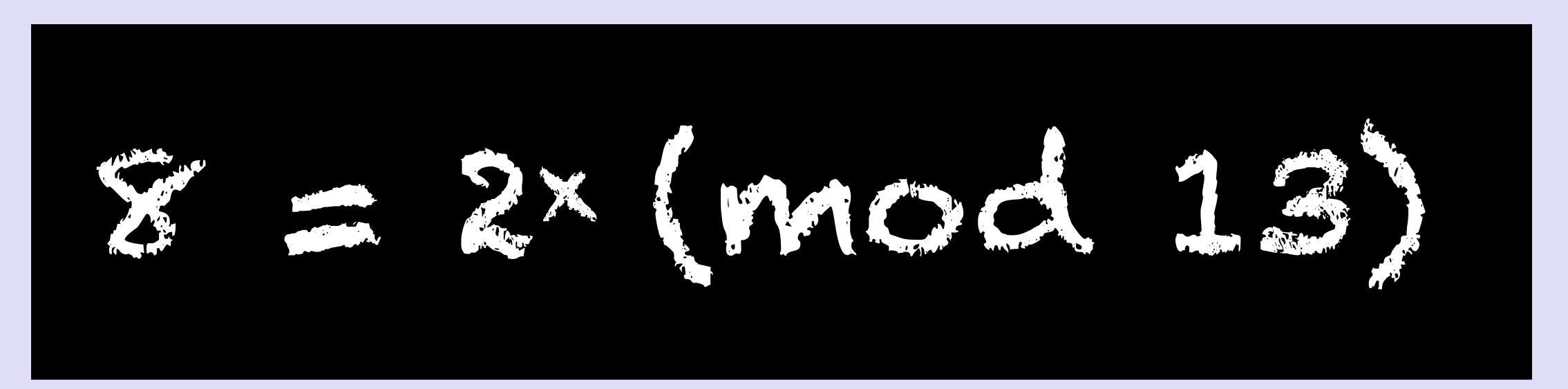
BLOCKCHAIN TUTORIAL 9



Discrete logarithm



BLOCKCHAIN TUTORIAL 9

Discrete logarithm

mobilefish.com



- The goal of exponentials is to calculate the product: $x = 2^{3}$
- The goal of logarithms is to calculate the exponent: $x = \log_2(8)$
- In discrete logarithm, you need to apply a modulo operation in the latter:
 - $x = \log_2 8 \pmod{13}$
 - Other way of notation: $x = dlog_{2,13}(8)$
 - where: x = exponent, 2 = base, 13 = modulus, 8 = remainder
 - If you find this confusing, you can also rewrite it this way: $8 = 2 \times (\text{mod } | 3)$

mobilefish.com

$(8 = 2^{\times})$



• Example:

- $2^{\times} \pmod{7} = 4$
- x = 2 or 5 $x = \{1,...,6\}$
- $4 \pmod{7} = 4$ and $32 \mod{7} = 4$
- There are two solutions. In the world of cryptography we are only interested in discrete logarithms where each exponent has a distinct remainder.

mobilefish.com

• If seems that if the modulus (p) is a prime number there are certain base values (b) which generate distinct remainders for different exponents (x = 1, ..., p-1). A prime number is a number that is divisible only by itself and 1. For example: 2, 3, 5, 7, 11, ...

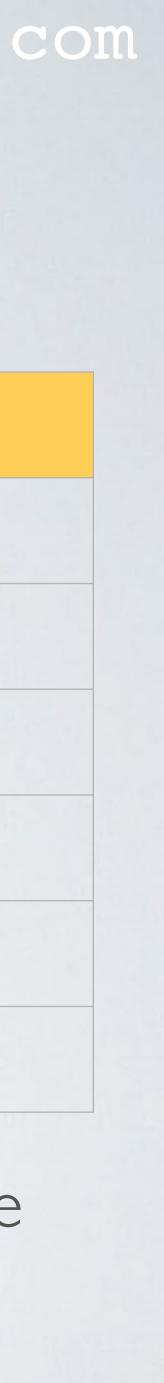


• Lets calculate $b^{\times} \pmod{7} = remainder \qquad x = \{1, \dots, 6\}$					modulus $p = 7$	
b	b ¹ mod7	b ² mod7	b ³ mod7	b4mod7	b ⁵ mod7	b ⁶ mod7
2	2	4		2	4	
3	3	2	6	4	5	
4	4	2		4	2	
5	5	4	6	2	3	
6	6		6		6	

value 3 or 5 and the remainders are in the range {1,...,6}

mobilefish.com

• The discrete logarithm for modulus 7 generates distinct remainders when using base



- discrete group {1, ... p -1} and not any real numbers (meaning fractions 2.58)
- digits long. REMEMBER: CALCULATING A DISCRETE LOGARITHM IS HARD. until the equation matches.

• The base values 3 and 5 are called the primitive roots of 7 or generators, often indicated by symbol α . It is called generator because applying the multiplication operation on one single element (α^{\times}), generates all elements in the discrete group {1, ... p -1}

• The word discrete in discrete logarithm refer to the aspect that we are working in a

• Calculating $3^{||}$ mod |7 = x is very easy, but doing the opposite, calculating the discrete logarithm $|1| = 3 \times \text{mod } |7|$ is very difficult. Especially if the modulus is at least 309 To solve $II = 3^{\times} \mod I7$ a computer needs to try each exponent x = 0, I, 2, 3...



- Example: α (generator) = 2 and p (modulus) = 1 discrete group {1, ..., p 1}
 - $2 \mod 1 = 2$ $2^6 \mod |1| = 9$ $2^7 \mod |1| = 7$ $2^2 \mod 1 = 4$ $2^8 \mod 11 = 3$ $2^3 \mod |1| = 8$ $2^4 \mod 1 = 5$ $2^9 \mod |1| = 6$ $2^5 \mod |1| = |0|$ $2^{10} \mod 11 = 1$
- and modulus operations, we have loop.
- If the remainder has value 1, the cycle starts all over again in the same order.

mobilefish.com

- $2^{16} \mod 11 = 9$ $2^{||} \mod || = 2$
- $2^{12} \mod 1 = 4$ $2^{17} \mod 1 = 7$ $2^{13} \mod 1 = 8$ $2^{18} \mod 11 = 3$
- $2^{19} \mod 1 = 6$ $2^{14} \mod 11 = 5$
- $2^{15} \mod 1 = 10$ $2^{20} \mod |1| = 1$

• This is called a cyclic group of generator α . After a certain number of exponentiations



- In the previous example (p=11) the cyclic group is referred to with notation: \mathbb{Z}_p^*
- For example: \mathbb{Z}^*
 - the * means no zero,
 - the discrete group is $\{1, ..., p I\} = \{1, ..., I0\}$
 - the number of elements in the discrete group is p 1 = 10
- Cyclic groups are the basis of discrete logarithm crypto systems.

mobilefish.com

