

## Discrete logarithms.

$$\overline{a^x} \equiv b \pmod{n}, \quad x = L_a(b) \pmod{n}$$

(Fast) modular exponentiation: Given  $a, x, n$ , compute  $b$ .

discrete log : Given  $a, b, n$ , compute  $x$ .

It's called discrete log :  $a^x = b \Leftrightarrow x = \log_a b$

Example:  $2^6 \equiv 9 \pmod{11}$

$$L_2(q) = 6, 16, 26, \dots$$

$$2^{10} \equiv 1 \pmod{11}$$

$$L_2(9) \equiv 6 \pmod{10}$$

$$2^{16} \equiv 9 \pmod{11}$$

We often use the smallest non-negative value.

Usually we consider discrete logs mod a prime  $p$ .

a is taken to be a primitive root mod p.

Example : No solution  $x > 0$  in  $2^x \equiv 3 \pmod{4}$ .

Example :  $2^x \pmod{7}$   $\equiv$  1, 2, or 4. (2 is not a primitive root of 7)

$$x = 1, 2, 3, 4, 5, 6, \dots$$

$$2^x \bmod 7 = 2, 4, 1, 2, 4, 1, \dots$$

$3^x \pmod{7}$  (3 is a primitive root of 7)

$$x = 1, 2, 3, 4, 5, 6, 7, \dots$$

$$3^x \bmod 7 = 3, 2, 6, 4, 5, 1, 3 \dots$$

Index Calculus : If  $a$  is a primitive root of  $p$ .

$$La(b_1 \cdot b_2) \equiv La(b_1) + La(b_2) \pmod{p-1}.$$

Proof : Let  $k_1 = La(b_1) \Leftrightarrow a^{k_1} \equiv b_1 \pmod{p}$   
 $k_2 = La(b_2) \Leftrightarrow a^{k_2} \equiv b_2 \pmod{p}$

$$La(b_1 \cdot b_2) = k_1 + k_2 \pmod{p-1} \Leftrightarrow a^{k_1+k_2} \equiv b_1 \cdot b_2 \pmod{p}$$