Next lecture and exercise will be on 21-6.
Lecture Hall of the exam: Audimax

Def 7.4 Let a be a PE mod n, $y \in \mathbb{Z}_n^*$. There exists a unique $x \in \{0, \dots, \varphi(n)-1\}$ with $y = a^x \bmod n$.
x is called the <u>discrete logarithm</u> of y. Notation $x = \log_a(y)$

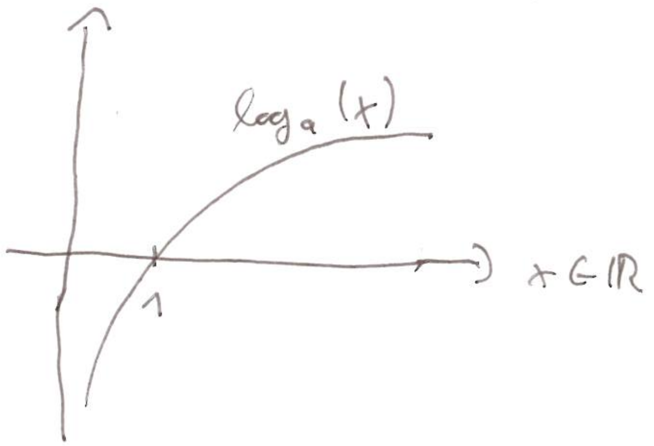
Particularly, if $n = p$ prime, a PE mod p:

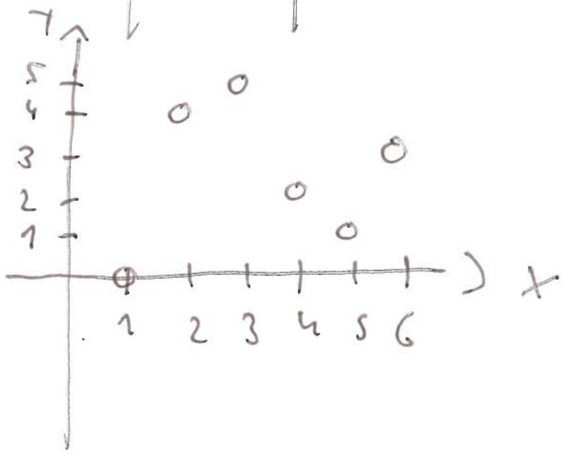
$$\forall y \in \mathbb{Z} \setminus \{0\} \; \exists! \; x \in \{0, \dots, p-2\} : y = a^x \bmod p$$

$y = a^x \bmod n$ is a <u>one-way function</u>.

<u>Example</u> on (discrete) logarithm:
Let $n = 7$, $a = 5$ $\qquad a^y \equiv x \pmod n$

x	1	2	3	4	5	6
$y = \log_a(x)$	0	4	5	2	1	3





1. $a^x \bmod n$ (modular exponentiation) can be efficiently computed by the square-and-multiply-alg.

<u>Example</u>. $y = a^{26}$ $\qquad 26 = (11010)_2$ binary representation

$$26 = 2 \cdot 13 + \boxed{0}$$
$$13 = 2 \cdot 6 + \boxed{1}$$
$$6 = 2 \cdot 3 + \boxed{0}$$
$$3 = 2 \cdot 1 + \boxed{1}$$
$$1 = 2 \cdot 0 + \boxed{1}$$

$$\Big(\underbrace{\big(\underbrace{(\underbrace{a^2 \cdot a}_{a^3})^2}_{a^6}\big)^2 \cdot a}_{a^{13}}\Big)^2 = a^{26}$$

Alg : Let $x = (b_k, \dots, b_1, b_0)_2 = \sum_{i=0} b_i 2^i$, $b_k = 1$

Square-And-Multiply

$Y \leftarrow a \bmod n$; // $b_k = 1$

for i from $k-1$ downto 0 do

$Y \leftarrow Y^2 \bmod n$

if $(b_i = 1)$ then

$Y \leftarrow Y \cdot a \bmod n$

end if

end for

Number of multiplications : $\underbrace{\lfloor \log_2(x) \rfloor}_{k \text{ squarings}} + \underbrace{\sum_{i=0}^{k-1} b_i}_{\# \text{ of multiplications by } a}$

2. For appropriate a and n, computing $\log_a(x)$ is considered infeasible

Overview of existing alg.

- Menezes et al, p. 104 - 113 (Baby-Step Giant Step → AMC)
- Stinson (02) p 228 ff
- Cohen et al (06), chapter 19

7.1 Diffie-Hellman Key Distribution and Key Agreement ('76)

Technique providing (unauthenticated) key agreement, allowing two parties to establish a shared (secret) key over an unsecure channel

- Initial setup: A prime p and a PE mod p, $a \in \{2, \dots, p-2\}$ are selected and published.
- Protocol actions:

  A chooses a random secret $x \in \{2, \dots, p-2\}$, sends to B: $u = a^x \bmod p$
  B chooses a random secret $y \in \{2, \dots, p-2\}$, sends to A: $v = a^y \bmod p$
  B receives, computes the shared key $K = u^y = (a^x)^y \bmod p$
  A receives, computes the shared key $K = v^x = (a^y)^x \bmod p$

- Generation of a, p, a PE mod p:

Prop 7.5) $p \geq 3$, prime, $p - 1 = \prod_{i=1}^{k} p_i^{x_i}$

$$a \text{ PE mod } p \iff a^{(p-1)/p_i} \not\equiv 1 \pmod p \quad \forall i = 1, \dots, k$$

Proof: Exe.

Application

1. Choose a large random number prime q until $p = 2q+1$ is prime as well (MRPT)
2. Choose randomly $a \in \{2, \dots, p-2\}$ until $a^2 \not\equiv 1 \pmod p$ and $a^q \not\equiv 1 \pmod p$

For $p = 2q+1$ there are $\varphi(\varphi(p)) = \varphi(p-1) = \varphi(2) \cdot \varphi(q) = q-1$

There exists $q-1$ PE mod p. Hence,

$$P(\text{selecting a PE in step 2}) = \frac{q-1}{p-1} = \frac{q-1}{2q} \approx \frac{1}{2}$$

Remark

Primes p such that $2p+1$ is also prime are called Sophie Germain primes (SG primes).

It is conjectured that

$$|\{p \mid p \text{ SG prime}, p \leq N\}| \sim \frac{2C_2 N}{(\log(N))^2}$$

with $C_2 \approx 0.66016\ldots$

Hence, there are sufficiently many SG primes

See http://primes.utm.edu/top20/page.php?id=2

For example: $N = 2^{64}$ $\Rightarrow$

Probability of finding SG primes $\approx 0.68‰ \mathrel{\hat{\approx}}$ Finding two primes $\frac{1}{1491}$

" " " primes $\approx 2.25\%$ $\frac{1}{45}$

Recall Prop 6.7 $|\{p \mid p \text{ prime}, p \leq N\}| \sim \frac{N}{\log(N)}$

- The opponent O knows $u = a^x \bmod p$, $v = a^y \bmod$, a, p

If O is able to calculate discrete log's, the system is broken, i.e., breaking the DH-procedure is no harder than calculating discrete log's.

Diffie-Hellman-Problem (DHP)

Given p, a a PE mod p, $a^x \bmod p$, $a^y \bmod p$

Calculate $a^{xy} \bmod p$

An efficient alg. to break the DHP would break the DH scheme.

Open question: Does an efficient alg for solving the DHP lead to an efficient alg. for calculating discrete log's?

- **Intruder in the middle attack on DH-system**

Let $p = 2q+1$, p prime, q prime, a PE mod p. Then

$a^q = a^{(p-1)/2}$ has order 2, since $\left(a^{(p-1)/2}\right)^2 \equiv a^{p-1} \underset{\uparrow}{\equiv} 1 \pmod p$

by Fermat's little Theorem

$$
\begin{array}{ccccc}
A & & \text{Opponent changes} & & B \\
a^x & \longrightarrow & a^{xq} & \longrightarrow & a^{xq} \\
a^{yq} & \longleftarrow & a^{yq} & \longleftarrow & a^y
\end{array}
$$

Joint key for A and B: $K = a^{x \cdot y \cdot q}$ (without knowing of O's action)

$k = (a^q)^{xy} \bmod p$ has only two possible values -1 or 1

Oscar can try both as a key

Important: Authenticity of exponentials a^x and a^y

$\rightsquigarrow$ digital signatures