$\Pr[\text{FAIL after } t \text{ steps}] \leq \left(1 - \frac{1}{3\lambda}\right)^t$

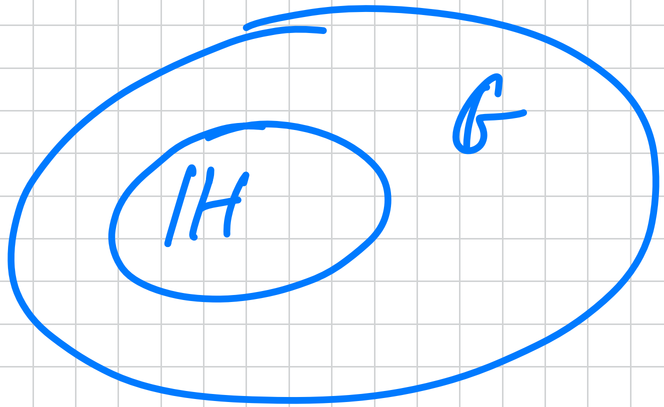
CONJECTURE The FACTORING problem is a OWF:

$$f(p, q) = p \cdot q = n$$

p, q primes s.t. $|p| \approx |q| \approx \lambda$

A few more facts about modular arithmetic.

THM If $\mathbb{H}$ is a subgroup of $\mathbb{G}$, then $|\mathbb{H}| \mid |\mathbb{G}|$.



Cor For all $a \in \mathbb{Z}_n^*$, Then:

- $a^{\varphi(n)} \equiv 1 \mod n$ (<u>EULER'S THM</u>)
- $a^b \equiv a^{b \mod \varphi(n)}$
- If $n = p$ (prime), $a^{p-1} \equiv 1 \mod p$. (FERMAT'S LITTLE THM)

Order of a group: For $a \in \mathbb{Z}_n$ the order of a is the minimum i s.t. $a^i \equiv 1 \mod n$.

$(\mathbb{Z}_n, \cdot)$

Proof. If $n = p$ (prime), then $\varphi(n) = p - 1$.
For every b, $a^b \equiv a^{q \cdot \varphi(n) + b \mod \varphi(n)}$

$$\equiv \underbrace{\left(a^{\varphi(m)}\right)^q}_{\equiv 1} \cdot a^{b \bmod \varphi(m)}$$

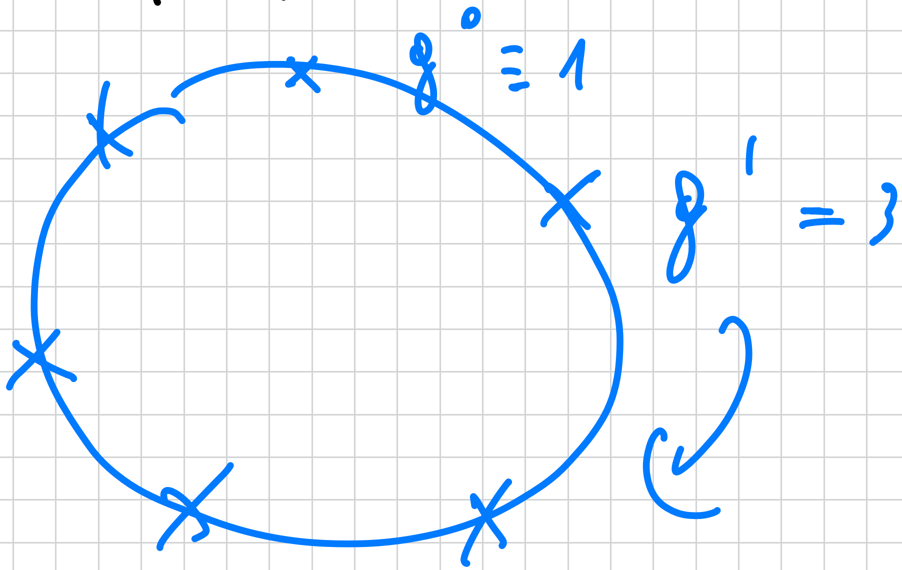
The first thing follows by Lagrange. $(\mathbb{Z}_m^*, \cdot)$ is a group with $\varphi(m)$ elements. Take the subgroup $\{a^0 \equiv 1, a, a^2, \dots, a^{d-1}\}$ has multiplicative order d s.t. $\varphi(m) = d \cdot k$ $\blacksquare$

We will also focus on $m = p$ (prime). Now $(\mathbb{Z}_p^*, +, \cdot)$ is a FIELD. This is special as $(\mathbb{Z}_p^*, \cdot)$ is a CYCLIC GROUP: $\exists g \in \mathbb{Z}_p^*$ s.t. $\mathbb{Z}_p^* = \{g^0, g^1, g^2, \dots, g^{p-2}\}$

For example: $\mathbb{Z}_7^*$ then $g = 3$ is a generator.

$$\mathbb{Z}_7^* = \{ 3^0, 3^1, 3^2, 3^3, \dots, 3^5 \}$$

$$= \{ 1, 3, 2, 6, 4, 5 \}$$



But 2 is not a generator:

$$2^3 \equiv 1 \mod 7$$

Good news: We can sample random p along with generator g of $\mathbb{Z}_p^*$. How? Basically we pick random $g \in \mathbb{Z}_p^*$ and test if g is a generator.

What's the hard problem in $\mathbb{Z}_p^*$? The DISCRETE Log problem: $f_g(x) = g^x \bmod p$ is a OWF. (CONJECTURE).

y; $x =$ "$\log_g y$"

Back to 1976: Diffie-Hellman introduced public-key crypto.

Alice $\boxed{(\mathbb{Z}_p^*, g, p)}$ Bob

$x \leftarrow \mathbb{Z}_{p-1}$ $\qquad$ $y \leftarrow \mathbb{Z}_{p-1}$

$\xrightarrow{g^x \bmod p}$

$\xleftarrow{g^y \bmod p}$

Useful Tooling

NM TCS 1 & 3.

$K = (g^y)^x \bmod p$
$= g^{xy} \bmod p$

$K = (g^x)^y \bmod p$
$= g^{xy} \bmod p$

Q: What security? If Eve can break DL

Then she can compute K !

Def (CDH) The computational DH assumption holds in $\mathbb{Z}_p^*$ if:

$$\mathcal{A} \qquad \xleftarrow{\ (\mathbb{Z}_p^*,\ g,\ p)\ } \qquad \mathcal{C}$$

$$\xleftarrow{\quad g^x,\ g^y \quad} \qquad x, y \leftarrow \mathbb{Z}_{p-1}$$

$$\xrightarrow{\quad Z \quad}$$

win iff $Z = g^{xy}$

CDH $\Rightarrow$ DL, but DL $\overset{???}{\Rightarrow}$ CDH.

Much better security: Eve (passive) can't distinguish key from uniform.

DEF (DDH - TAKE 1) The DECISIONAL DH assumption holds in $(\mathbb{Z}_p^*, g, p-1)$ if:

$$(g^x, g^y, g^{xy}) \approx_c (g^x, g^y, g^z)$$

for $x, y, z \leftarrow \mathbb{Z}_{p-1}$.

Bad news: DDH false in $\mathbb{Z}_p^*$:(

The reason are the so-called QUADRATIC RESIDUES mod p:

$$QR_p = \{ y : y = x^2 \bmod p \}$$
$$= \{ y : y = g^z \text{ for even } z \}$$

Test: Check if $y \in QR_p$ by checking
$$y^{(p-1)/2} \equiv 1 \bmod p$$

Why? If $y = g^{2z'}$ then
$$y^{(p-1)/2} \equiv g^{z'(p-1)} \equiv 1 \bmod p$$

If $y = g^{2z'+1}$ then

$$g^{(p-1)/2} \equiv \underbrace{g^{z'(p-1)}}_{\equiv 1} \cdot \underbrace{g^{(p-1)/2}}_{\not\equiv 1} \not\equiv 1 \bmod p$$

The distinguisher: given (X, Y, Z) check if Z is a square and output $b' = 1$ iff it is a square. Now:

- If $Z = g^z$ (UNIFORM), it is a square w.p. $1/2$.
- If $Z = g^{xy}$, then Z is a square

if either of g^x or g^y is a square.
So it's a square w.p. 3/4.

Good news: DDH believed to hold in other groups G. In general, we'll write

"$(G, g, q) \leftarrow \mathrm{GroupGen}(\lambda)$

↳ q is the order.

(DDH $\Rightarrow$ CDH $\Rightarrow$ DL

DL, CDH $\Rightarrow$ DDH ???)

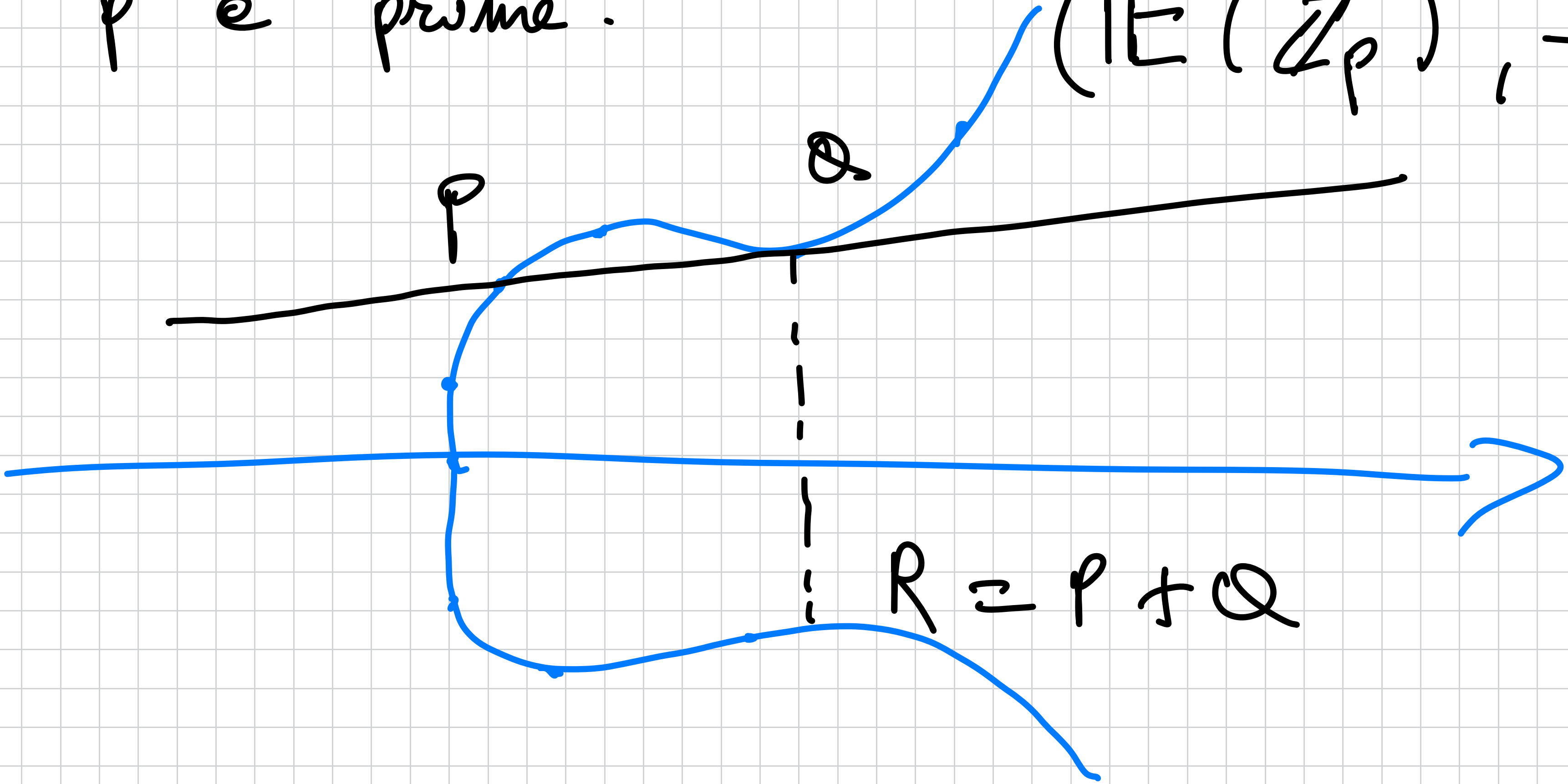
Examples:

- $G = QR_p$ but with $q = \frac{p-1}{2}$ a prime. It is also cyclic of order q.

$$QR_p = \{ g^0, g^1, \dots, g^{q-1} \}$$

- Elliptic curves. Basically this is some curve $y^2 = ax^3 + bx^2 + cx + d \mod p$ where p a prime.

$(\mathbb{E}(\mathbb{Z}_p), +)$



$\exists \quad P$ s.t. $E(\mathbb{Z}_p) = \{ \phi, P, P+P, P+P+P, \ldots, (q-1)\cdot P \}$

q = The order

Discrete log: Pick random $x \in \mathbb{Z}_q$ and output $Q = x \cdot P$. Compute x?

Bottom line: DH Key exchange is PASSIVELY SECURE assuming DDH is hard.

What about ACTIVE security?

Alice		Eve		Bob
x	$\xrightarrow{g^{x}}$	x', y'	$\xrightarrow{g^{x'}}$	y
	$\xleftarrow{g^{y'}}$		$\xleftarrow{g^{y}}$	
$g^{xy'}$		$g^{x'y}, g^{xy'}$		$g^{x'y}$

How to fix it?. We need authenticated channels. Alice and Bob should be able to use MACs or DIGITAL SIGNATURES.

Plan for next lectures: Build PKE and DS from FACTORING, DL, CDH, DDH, ...
First, note that these assumptions easily imply all the crypto we had so far.
Examples:

*) PRGs from FACTORING: $n = p \cdot q$

$$s_{i+1} = s_i^2 \bmod n \quad \left(\begin{array}{c}\text{start from} \\ s_0 = s\end{array}\right)$$

output LSB each time.
In other words this is HARD-CORE BIT.

*) PRG from DDH. (G, g, q)

$$G_{g,q}(x,y) = (g^x, g^y, g^{xy}) \approx (g^x, g^y, g^z)$$

$$\mathbb{Z}_q^2 \to G^3 \quad \leadsto \text{ stretches!}$$

$$(\mathbb{Z}_q \times \mathbb{Z}_q \to G \times G \times G)$$

I can improve the stretch:

$$G_{g,q}(x, y_1, \dots, y_\ell) = (g^x, g^{y_1}, g^{xy_1}, g^{y_2}, g^{xy_2}, \dots, g^{y_\ell}, g^{xy_\ell})$$

$$\mathbb{Z}_q^{\ell+1} \longrightarrow \mathbb{G}^{2\ell+1}$$

Exercise: Prove this is secure from DDH.

*) PRFs. There is a simple construction of PRFs from DDH.

$$\mathcal{F}_{NR} = \{ F_{q,g,\vec{a}} : \{0,1\}^n \to \mathbb{G} \}_{\vec{a} \in \mathbb{Z}_q^{n+1}}$$

$$\vec{a} = (a_0, a_1, \dots, a_n)$$

$$F_{q,g,\vec{a}}(x_1, \dots, x_n) = \left(g^{a_0}\right)^{\prod_{i=1}^{n} a_i^{x_i}}$$