Basics + Euklid's Alg.   [all proofs on blackboard]

$\mathbb{Z} = \{ \ldots -2, -1, 0, 1, 2 \ldots \}$
$\mathbb{N} = \{ 0, 1, 2 \ldots \}$

$d \mid a$ if $a = k \cdot d$, $k \in \mathbb{Z}$

d <u>divisor</u> of a if $d \mid a$ & $d \geq 0$
<u>trivial divisor</u> of a is a & 1
non-trivial divisors are called <u>factors</u>

$a > 1$ & a has only trivial divisors: a <u>prime</u>

<u>Thm 1.1</u>: $\forall a, b \in \mathbb{Z}, a > 0$: $\exists!\, q, r \in \mathbb{Z}$: $0 \leq r < a$ & $b = qa + r$

<u>Lemma 1.1</u>: $d \mid a, d \mid b \Rightarrow d \mid (ax + by)$ $\forall x, y \in \mathbb{Z}$

greatest common divisor (gcd) of a, b (not both 0)
is largest of the common divisors of a & b,
$\gcd(0, 0) := 0$

<u>Thm 1.2 [Lemma Bezout]</u>:
Let $a, b \in \mathbb{Z}$ (not both 0)
Then, $\gcd(a,b)$ is smallest positive Element
of the set $\{ax + by : x, y \in \mathbb{Z}\}$

<u>Kor</u>: $\forall a, b \in \mathbb{Z}$: 1) $d \mid a$ & $d \mid b \Rightarrow d \mid \gcd(ab)$
$\forall n \in \mathbb{N}$ 2) $\gcd(an, bn) = n \gcd(ab)$

3) a, b, n positive $\Rightarrow n \mid b$
with
$n \mid ab$
$\gcd(a, n) = 1$

a, b relative prime, if $\gcd(a,b) = 1$

Thm 1.3: a, p rel. prime & b, p rel. prime $\Rightarrow$ ab, p relative prime

Thm 1.4: $\forall$ primes p $\forall a, b \in \mathbb{Z}$ with $p \mid ab$
$\Rightarrow p \mid a$ or $p \mid b$

Thm 1.5: exist unique factorization of any $a \in \mathbb{N} \setminus \{0\}$ into primes.

$a \bmod n := a - n \left\lfloor \frac{a}{n} \right\rfloor$

Thm 1.6: $\forall a, b \in \mathbb{N}, b > 0$: $\gcd(a, b) = \gcd(b, a \bmod b)$

```
EUKLID(a,b)
    IF (b=0) RETURN (a)
    ELSE RETURN (b, a mod b)
```

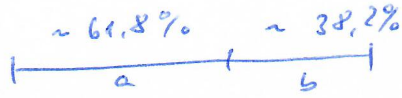
Correctness: clear, Thm 1.6.
Runtime? $\longrightarrow$ Fibonacci numbers & golden ratio.

Fibonacci Numbers:

$$F_0 := 0$$
$$F_1 := 1$$
$$F_i = F_{i-1} + F_{i-2}, \quad i \geq 2$$

$$0, 1, 1, 2, 3, 5, 8, 13, \ldots$$

GOLDEN RATIO: $\phi = \dfrac{a+b}{a} = \dfrac{a}{b}$



$$\phi = \frac{a+b}{a} = \frac{a}{b} \iff \frac{a}{b} - 1 - \frac{b}{a} = 0$$
$$\iff \phi - 1 - \frac{1}{\phi} = 0$$
$$\iff \phi^2 - \phi - 1 = 0$$
$$\iff \phi = \frac{1+\sqrt{5}}{2}$$
$$\hat{\phi} = \frac{1-\sqrt{5}}{2}$$

Lemma 1.2: $F_i = \dfrac{\phi^i - \hat{\phi}^i}{\sqrt{5}}$

$$F_i \sim \frac{\phi^i}{\sqrt{5}} \quad \text{(expon. growth)}$$

Runtime Euclid:

Lemma 1.3: $a > b \geq 0$ integers

Assume the call EUCLID (a,b) performs $k \geq 1$ recursive calls, then

$$a \geq F_{k+2}$$
$$b \geq F_{k+1}$$

Thm 1.7 (Lamé's Thm)

$\forall\, k \geq 1$: IF $a > b \geq 1$ & $b < F_{k+1}$
THEN EUCLID (a,b) makes fewer than k recursive calls.

NOTE: $F_k \sim \dfrac{\phi^k}{\sqrt{5}} \Rightarrow$ # calls $k \approx \log_\phi\left(\dfrac{\phi^k}{\sqrt{5}}\right) \approx \log_\phi(F_k)$
$\leq \log_\phi(b) \leq \log_2(b)$

$\Rightarrow$ fast!

RSA

Aim: Find $P_A(\,)$, $S_A(\,)$ s.t. $\forall M \in D$ (D = set of feasible messages) holds that
$$M = S(P(M))$$
$$\& \; M = P(S(M)).$$

Euler phi-Fct:

$$\varphi(n) = |\{a \in \mathbb{N} : 1 \le a < n \;\&\; \gcd(a,n) = 1\}|$$

m, n relat. prime $\Rightarrow \varphi(mn) = \varphi(n)\varphi(m)$

p prime $\Rightarrow \varphi(p) = p - 1$

p prime: $\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right)$

$$\varphi(n) = n \cdot \prod_{\substack{p:\\ p \text{ prime}\\ p \mid n}} \left(1 - \frac{1}{p}\right)$$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \gcd(a,n) = 1$$

$$\Rightarrow |\mathbb{Z}_n^*| = \varphi(n)$$

Thm (Euler): $\forall n \in \mathbb{N}, n > 1, a \in \mathbb{Z}_n^*$:
$$a^{\varphi(n)} \equiv 1 \pmod n$$

Thm (Fermat): p prime $\Rightarrow a^{p-1} \equiv 1 \pmod p \quad \forall a \in \mathbb{Z}_p^*$

Thm (modified EULER):
let $n = p \cdot q$, p, q distinct primes

Then, $a^{k\varphi(n)+1} \equiv a \pmod n \quad \forall \begin{array}{l} a \in \mathbb{N} \\ k \in \mathbb{N}. \end{array}$

RSA - Alg:

1) select p, q prime
2) $n \leftarrow p \cdot q$
3) choose odd integer $e > 1$
   with $\gcd(e, \varphi(n)) = 1$
4) compute d as multiplicative inverse of e, modulo $\varphi(n)$.
5) publish public pair $P = (e, n)$
6) keep secret key $S = (d, n)$

Here $D = \mathbb{Z}_n$
Let $M \in D$ be a message:

$$P(M) = M^e \bmod n$$
$$S(C) = C^d \bmod n$$

Why does this work?

a)
$$\begin{aligned} S(P(M)) &= S(M^e \bmod n) \\ &= (M^e \bmod n)^d \bmod n \\ &= M^{ed} \bmod n \\ &= (M^d \bmod n)^e \bmod n = P(S(M)) \end{aligned}$$

$\Rightarrow$ P & S are inverse of each other

b) how to get back M?

e, d multipl. inverse.
$\Rightarrow e \cdot d \equiv 1 \mod \varphi(n)$
$\Rightarrow ed = 1 +$ "some multiple of $\varphi(n)$"
$\quad = 1 + k\varphi(n)$

$$\Rightarrow M^{ed} = M^{1+k\varphi(n)} \underset{\substack{\text{modified} \\ \text{Thm} \\ \text{Euler}}}{=} M \pmod n \equiv M \quad \forall M \in D = \mathbb{Z}_n$$

Runtime (short)

RSA: Step 1 : Find primes (random from some database)
or choose poly-time Alg (AKS Test)
to test if random nr k is prime
(prob. that k is prime is $\sim \frac{1}{\ln(n)}$) —

Step 2 $n = p \cdot q$ ✓

Step 3 Find e with $\gcd(e, \varphi(n))$
→ Apply EUKLID-Alg on
$e \in [3, \min(p-1, q-1)]$

Step 4 Find d: with $ed \equiv 1 \mod \varphi(n)$.

How? : $\gcd(e, \varphi(n)) = 1 \underset{\text{Thm 1.2}}{\Rightarrow} 1 = ex + \varphi(n)y$

$\Rightarrow 1 \equiv ex + \varphi(n)y \pmod{\varphi(n)}$
$= ex \pmod{\varphi(n)}$

$\overset{\text{multiply with}}{\underset{e^{-1}}{\Rightarrow}} \Rightarrow ee^{-1}x \pmod{\varphi(n)} \equiv 1 \cdot e^{-1} = e^{-1} = d$

$\Rightarrow d = x \mod \varphi(n)$

Step 5/6 ✓

How to get $M^e \mod n$?
$C^d \mod n$?

NOTE, M, n, e, d are usually very large number (~512 / 1024 bit)

Consider M^e, e 50 bits long

$\Rightarrow \log_2(e) \approx 50 \Rightarrow e \approx 2^{50} \approx 10^{15}$
$\Rightarrow M^e \approx M^{10^{15}} \Rightarrow$ more than 1 quadrillion multiplications needed $\Rightarrow$ Bad!

$\Rightarrow$ HORNER schema!
Exampl $e = 13 \rightarrow$ binary: 1011
$M^{13} = \left(\left((M^1)^2 \cdot M^1\right)^2 \cdot (M^0)^2\right) M^1$
$\Rightarrow$ only $O(k)$ operations for $k \sim$ bit nr $\sim \log_2(e)$ operations
$\Rightarrow$ GOOD!