Plan for today

- Recap: rings, groups, Lagrange’s Theorem, Euler $\phi$-function, Chinese remainder theorem
- Euler’s and Fermat’s little theorem
- RSA cryptography
- Primality tests
Recap: Rings

A set $R$ is a ring if it has two binary operations, written as addition and multiplication, such that for all $a, b, c \in R$

1. $a + b = b + a \in R$ \hspace{1cm} (R1)
2. $(a + b) + c = a + (b + c)$ \hspace{1cm} (R2)
3. There exists an element $0 \in R$ with $a + 0 = a$ \hspace{1cm} (R3)
4. There exists an element $-a \in R$ with $a + (-a) = 0$ \hspace{1cm} (R4)
5. $a(bc) = (ab)c$ \hspace{1cm} (R5)
6. There exists an element $1 \in R$ with $1 \cdot a = a \cdot 1 = a$ \hspace{1cm} (R6)
7. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ \hspace{1cm} (R7)

WHAT IS NOT REQUIRED:

- Multiplication may not commute
- Some elements may not have a multiplicative inverse
Recap: Rings

Examples:

- \( \mathbb{Z} \)
- \( \mathbb{Z}_n \) \{ numbers here may not have a multiplicative inverse \}
- \( R_1 \times \cdots \times R_k \), where \( R_1, \ldots, R_k \) are rings.
- The set of \( n \times n \) matrices over \( \mathbb{Z} \) with the standard matrix addition and multiplication.
Theorem

Let $R$ be a ring, then for each $r \in R$ one has

$$0 \cdot r = 0 = r \cdot 0.$$
If $R$ and $R_1$ are rings, a mapping $\vartheta : R \rightarrow R_1$ is called a ring homomorphism if for all $r, s \in R$:

1. $\vartheta(r + s) = \vartheta(r) + \vartheta(s)$
2. $\vartheta(rs) = \vartheta(r) \cdot \vartheta(s)$
3. $\vartheta(1_R) = 1_{R_1}$

Examples:

- $f : \mathbb{Z} \rightarrow \mathbb{Z}_N, f(x) = [x]_N$
- $g : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}_N, f(x) = (x, [x]_N)$.

$N = 8$

$x = 15$

$f(x) = 3$
Chinese remainder theorem

**Theorem**

Suppose $a$ and $b$ are relatively prime integers. Then the map

$$f : \mathbb{Z}_{a \cdot b} \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b$$

$[x]_{a \cdot b} \mapsto ([x]_a, [x]_b)$

is a **ring isomorphism**, that is, a ring homomorphism that is also a bijection.

**Equivalent Statement**:

$\forall x_1 \in \{0, \ldots, a-1\}, x_2 \in \{0, \ldots, b-1\}$ \exists ! x \in \{0, \ldots, (a \cdot b) - 1\}

such that

$$x \equiv x_1 \mod a,$$

$$x \equiv x_2 \mod b.$$  

**Proof (Sketch)**

1) $f$ is homomorphism

2) $|\mathbb{Z}_{a \cdot b}| = |\mathbb{Z}_a \times \mathbb{Z}_b| = |\mathbb{Z}_a| \cdot |\mathbb{Z}_b|$  

3) $f$ is surjective
\( \phi(\cdot) \) is multiplicative

For \( N \in \mathbb{N} \), \( \phi(N) = \left\lfloor \frac{N}{\prod p^e} \right\rfloor \)

Corollary

If \( a, b \in \mathbb{N} \) and \( \gcd(a, b) = 1 \), then \( \phi(a \cdot b) = \phi(a) \cdot \phi(b) \).

\[ \phi \left( \left\lfloor \frac{x}{ab} \right\rfloor \right) = \phi(x) \]

\( x \) was a multiplicative inverse

\[ \left\lfloor \frac{x}{ab} \right\rfloor \in \mathbb{N} \]

\( \phi(a) \in \mathbb{N} \)

\( \phi(b) \in \mathbb{N} \)

\[ \phi(ab) = \phi(a) \cdot \phi(b) \]
**Corollary**

Let \( N = p_1^{e_1} \cdots p_k^{e_k} \) be the factorization of \( N \) into distinct prime numbers \( p_1, \ldots, p_k \), then

\[
\phi(N) = \prod_{i=1}^{k} (p_i - 1) \cdot p_i^{e_i - 1}
\]

\[
\phi(p^e) = \phi(\prod_{i=1}^{k} p_i^{e_i}) = \prod_{i=1}^{k} \phi(p_i^{e_i}) = \prod_{i=1}^{k} (p_i^{e_i} - 1) p_i^{e_i - 1}
\]

What is left to show? \( \phi(p^e) = ? \)

\[
\phi(p^e) = \left| \mathbb{Z}_{p^e}^* \right| = \left| \{ x \in \{1, \ldots, p^e \} : \gcd(x, p^e) = 1 \} \right|
\]

\[
\gcd(x, p^e) \neq 1 \iff x = 1, \phi, 2 \cdot \phi, 3 \cdot \phi, \ldots, (p^{e-1}) \phi.
\]

How many? \(\phi(p^e) = p^e - (p^{e-1}) \cdot \phi \cdot p^{e-1} (p - 1) \cdot \phi \)
Recap: Groups

A set $G$ is called a **group** if it has a binary operation $\circ$ such that for all $a, b, c \in G$

1. **(G0)** $a \circ b \in G$
2. **(G1)** $a \circ (b \circ c) = (a \circ b) \circ c$
3. **(G2)** There exists an element $1 \in G$ with $1 \circ a = a \circ 1 = a$
4. **(G3)** There exists an element $a^{-1} \in G$ with $a \circ a^{-1} = a^{-1} \circ a = 1$

**Examples**

- The set $\mathbb{Z}_*^\times \subseteq \mathbb{Z}$, where $\mathbb{Z}$ is the set of integers and $\mathbb{Z}_*^\times$ denotes the set of positive integers, is a group for all $N \in \mathbb{N}$.

- $\mathbb{Q} \setminus \{0\}$ is an infinite group.

- $\mathbb{Z}_N$ is not a group w.r.t. multiplication.
Subgroups

Let $G$ be a group and $H \subseteq G$. $H$ is a **subgroup** of $G$ if $H$ is a group itself. We write $H \triangleleft G$.

**Theorem**

Let $G$ be a group and $H \subseteq G$. Then $H \triangleleft G$ if and only if for each $a, b \in H$ one has

$$a \cdot b^{-1} \in H.$$

----------------------------------

**Proof**

$$\forall a, b \in H \quad a \cdot b^{-1} \in H \implies H \triangleleft G \quad (G_1) \checkmark$$

*Take $b = a$* \quad $a \cdot a^{-1} = 1 \in H \implies (G_2) \checkmark$

*To show: $\forall c \in H, c^{-1} \in H$. $a = 1$ $b = c \implies 1 \cdot c^{-1} = c^{-1} \in H \quad (G_3)$*

*To show: $\forall c, d \in H$, $c \cdot d \in H$. $a = c$ $b = d^{-1}$ $\implies c \cdot (d^{-1})^{-1} = c \cdot d \in H \quad (G_0)$*

**Converse:** *(Very Easy) Exercise*
Theorem

Let $G$ be a finite group and $H$ be a subgroup of $G$, then

$$|H| \text{ divides } |G|.$$
Theorem

Let $G$ be a finite group and $H$ be a subgroup of $G$, then

$$|H| \text{ divides } |G|.$$
The order of a group-element

Let $G$ be a group and $g \in G$. The *order* of $g$ is the smallest number $i \in \mathbb{N}_0 \cup \{\infty\}$ such that

$$g^i = 1$$

holds.

Theorem. Let $G$ be a finite group. Then $\forall g \in G$, $|G| = 1$

Fix $g \in G$. $H = \{ g^i : i \in \mathbb{N}_0 \}$ is the set of all powers of $g$.

Corollary. $H \subseteq G$ is a (rather) easy exercise, just use the "2.3.4-criterion.

$|H| = \text{ord}(g)$. In fact, $1 + g^t = 1 \iff g^t = 1 \implies g^{t+l} = g^t \cdot g^l = g^l$

From Lagrange's theorem, $|H| \cdot t = |G|$, $t \leq |H|$\text{ }\Rightarrow \text{ }1 = g^{|G|} = (g^t)^{\frac{|G|}{t}} = 1$
Fermat’s little theorem

Corollary

Let \( N \in \mathbb{N} \) and \( a \in \mathbb{Z}_N^* \), then
\[
a^{\phi(N)} = 1.
\]

Corollary (Fermat’s little theorem)

Let \( N \) be a prime number. For each \( a \in \{1, \ldots, N-1\} \) one has
\[
a^{N-1} \equiv 1 \pmod{N}.
\]

\[\text{PF.}\]

\( N \) prime \( \phi(N) = |\mathbb{Z}_N^*| = N-1 \)

\( \forall \ x \in \{1, \ldots, N-1\} \ : \ \gcd(x, N) = 1 \)
RSA

Bob:  
- Generates large (512 bits) primes $p$ and $q$
- Computes $N = p \cdot q$
- Selects encryption exponent $e$ such that $\gcd(e, \phi(N)) = 1$
- Public key: $(N, e)$

Alice:  
- Converts message to bit-string $m$
- Sends $s = m^e \pmod{N}$ to Bob

Bob:  
- Computes $y = e^{-1} \pmod{\phi(N)}$
- Computes $s^y \equiv m \pmod{N}$

EVE knows $(N, e)$. If she could factorize $N$, we know $p, q$.
Bob:
- Generates large (512 bits) primes $p$ and $q$
- Computes $N = p \cdot q$.
- Selects encryption exponent $e$ such that $\gcd(e, \phi(N)) = 1$
- Public key: $(N, e)$

Alice:
- Converts message to bit-string $m$
- Sends $s = m^e \pmod{N}$ to Bob

Bob:
- Computes $y = e^{-1} \pmod{\phi(N)}$
- Computes $s^y \equiv m \pmod{N}$.

---

**Proof**

To show $s^y = m \pmod{N}$:

$$s^y = m^{e \cdot y} \cdot s \in C \because y, e \equiv 1 \pmod{\phi(N)}$$

Let's prove this!
\textbf{Proof (Continues)}

\textbf{Case 2:} \( p \mid m \Rightarrow m = t \cdot p, \; t \in \mathbb{N} \Rightarrow m \cdot \left( 1 + x(p-1)(q-1) \right) \equiv (tp) \equiv 0 \mod p \Rightarrow (0) \equiv 0 \mod p \equiv 0 \mod p \equiv m \mod p \)

So we get

\[ y \equiv m \mod p \equiv y \mod p \]

Similarly

\[ y^y \equiv m \mod q \]

\[ p, q \mid y^y - m \Rightarrow N = p \cdot q \mid y^y - m \Rightarrow y^y \equiv m \mod N = \]
Implementing RSA: Two guiding questions

A) How to recognize prime numbers?  → PRIMALITY TEST

B) Are the prime numbers dense enough such that a random \( n \)-bit number is a prime with reasonable probability?  → PRIME NUMBER THEORY AND RELATED RESULTS
Primality tests

- Weak Fermat test
- Charmichael numbers
- The Miller-Rabin test

Randomized primality tests

[Their output may be incorrect, but this happens with bounded probability]

Deterministic primality tests exist!

First: (AKS Test, 2004)
The weak Fermat test

- Input: $N \in \mathbb{N}$ odd
- Assert: Composite or probably prime
- Choose $a \in \{1, \ldots, N - 1\}$ uniformly at random
- If $a^{N-1} \pmod{N} = 1$ assert probably prime
- else assert composite
An odd composite number $N \in \mathbb{N}$ is called *Carmichael number* if

$$\forall a \in \mathbb{Z}_N^* : a^{N-1} = 1.$$
If $N$ is not Carmichael

**Theorem**

Let $N$ be an odd composite number that is not Carmichael, then the weak Fermat test asserts *probably prime* with probability at most $1/2$.

If the weak Fermat test is repeated $i$ times, then the probability that it asserts *probably prime* in all $i$ rounds is at most $1/2^i$.

**Proof.** Let $N$ odd, non-Carmichael, composite.

\[ H = \{ a \in \mathbb{Z}_N^* : a^{N-1} \equiv 1 \mod N \} \]

\[ H \subseteq \mathbb{Z}_N^* \quad \text{Exhibit} \]

\[ \forall N \text{ not Carmichael} \Rightarrow \exists a \in \mathbb{Z}_N^* : a^{N-1} \not\equiv 1 \mod N \]

\[ |H| = 2^{\frac{N-1}{2}} \]

\[ |H| \leq \frac{1}{2} |\mathbb{Z}_N^*| \Rightarrow \Pr(\text{taken}) \leq \frac{1}{2} \]
Theorem

Every Carmichael number $N$ is of the form

$$N = p_1 \cdots p_k,$$

where the $p_i$ are distinct primes and $(p_i - 1) \mid (N - 1)$ for $i = 1, \ldots, k$. 