Plan for today

- Recap: rings, groups, Lagrange's Theorem, Euler φ-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 $a, b, c \in R$

√ (R1) $a + b = b + a \in R$

√ (R2) $(a + b) + c = a + (b + c)$

√ (R3) There exists an element $0 \in R$ with $a + 0 = a$

√ (R4) There exists an element $-a \in R$ with $a + (-a) = 0$

√ (R5) $a(bc) = (ab)c$

√ (R6) There exists an element $1 \in R$ with $1 \cdot a = a \cdot 1 = a$

√ (R7) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

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.

→ HERE MULTIPLICATION DOES NOT COMMUTE

Example of an easy ring-theorem

Theorem

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

$$0 \cdot r = 0 = r \cdot 0.$$

<u>PF.</u>

$0 = 0 + 0 \Rightarrow 0 \cdot r = (0+0) \cdot r = 0r + 0r$

$\Rightarrow 0 = 0 \cdot r - 0 \cdot r = 0r \cancel{+0r} \cancel{-0r} = 0r \quad \square$

Ring homomorphism

If R and R_1 are rings, a mapping $\partial : R \to R_1$ is called a *ring homomorphism* if for all $r, s \in R$:

(1) $\partial(r + s) = \partial(r) + \partial(s)$

(2) $\partial(rs) = \partial(r) \cdot \partial(s)$

(3) $\partial(1_R) = 1_{R_1}$

Examples:

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

$N = 8$

$x = 19$

$f(x) = 3$

Chinese remainder theorem

Theorem

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

$$\begin{array}{rccc} f: & \mathbb{Z}_{a \cdot b} & \to & \mathbb{Z}_a \times \mathbb{Z}_b \\ & [x]_{a \cdot b} & \mapsto & ([x]_a, [x]_b) \end{array}$$

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

EQUIVALENT STATEMENT:

$\forall\ x_1 \in \{0, \dots, a-1\},\ x_2 \in \{0, \dots, b-1\}\quad \exists!\ x \in \{0, \dots, ab-1\}$:

$$x \equiv x_1 \mod a$$
$$x \equiv x_2 \mod b$$

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 $N \in \mathbb{N}$, $\phi(N) = |\mathbb{Z}_N^*| = |\{x \in \{0, \dots, N\} : \gcd(x, N) = 1\}|$

Corollary

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

PF.

Let $x \in \mathbb{Z}_{ab}$. x HAS A MULTIPLICATIVE INVERSE $\Longleftrightarrow$ $f(x) = ([x]_a, [x]_b)$ HAS A MULTIPLICATIVE INVERSE

$\Longleftrightarrow$

$\Longleftarrow$ $[x]_a \in \mathbb{Z}_a^*$, $[x]_b \in \mathbb{Z}_b^*$

$$|\mathbb{Z}_{ab}^*| = |\mathbb{Z}_a^*| \times |\mathbb{Z}_b^*|$$

$$\phi(ab) = \phi(a) \cdot \phi(b)$$

$\square$

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*

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

PF.

$$\phi(N) = \phi\left(\prod_{i=1}^{k} p_i^{e_i}\right) = \prod_{i=1}^{k} \phi(p_i^{e_i}) \overset{(*)}{=} \prod_{i=1}^{k} (p_i - 1)\, p_i^{e_i - 1} \quad \square$$

WHAT IS LEFT TO SHOW? $\phi(p^e) = ?$

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

$\gcd(x, p^e) \neq 1$ IFF $x = 1 \cdot p, 2 \cdot p, 3p, \ldots, (p^{e-1})\, p$. HOW MANY? p^{e-1}

$$\phi(p^e) = p^e - (p^{e-1}) = p^{e-1}(p-1) \quad (*)$$

Recap: Groups

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

✓ (G0) $a \circ b \in G$

✓ (G1) $a \circ (b \circ c) = (a \circ b) \circ c$

✓ (G2) There exists an element $1 \in G$ with $1 \circ a = a \circ 1 = a$

✓ (G3) There exists an element $a^{-1} \in G$ with $a \circ a^{-1} = a^{-1} \circ a = 1$

↳ MULTIPLICATIVE INVERSE

EXAMPLES

- $\mathbb{Z}_N^*$ IS A FINITE GROUP $\forall N \in \mathbb{N}$ ["$\circ$" = MODULAR MULTIPLICATION]

↳ $\mathbb{Z}_N$ IS NOT A GROUP WRT MULTIPLICATION

- $\mathbb{Q} \setminus \{0\}$ IS AN INFINITE GROUP.

Subgroups

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

Theorem

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

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

PF.

$\forall a, b \in H \quad a \cdot b^{-1} \in H \implies H \trianglelefteq G$

(G1) ✓

- TAKE $b = a \quad a \cdot a^{-1} = 1 \in H \implies$ (G2) ✓
- TO SHOW: $\forall c \in H,\ c^{-1} \in H.\quad a = 1 \quad b = c \implies 1 \cdot c^{-1} = c^{-1} \in H$ (G3) ✓
- TO SHOW: $\forall c, d \in H,\ c \cdot d \in H.\quad a = c \quad b = d^{-1} \implies c\,(d^{-1})^{-1} = c \cdot d \in H$ (G0) ✓

CONVERSE: (VERY EASY) EXERCISE □

Lagrange's theorem

Theorem

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

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

Pf.

$\forall a \in G: \quad aH = \{ab,\ b \in H\}$

CL 1: $|aH| = |H|$ CHECK THIS!

CL 2: $\bigcup_{a \in G} aH = G$ CHECK THIS!

CL 3: $\forall a, b$, EITHER $aH = bH$ OR $aH \cap bH$

Pf. SUPPOSE $aH \cap bH \neq \emptyset \Rightarrow \exists\, h_1, h_2 \in H: \ a h_1 = b h_2 \cdot h_1^{-1}$

h_1^{-1}

$\Rightarrow a = b \cdot \underbrace{h_2 \cdot h_1^{-1}}_{h_3} = b \cdot h_3$

$h' \in H$

Then $\forall h \in H \quad a \cdot h = b \cdot h_3 \cdot h = b h' \in bH$

Lagrange's theorem

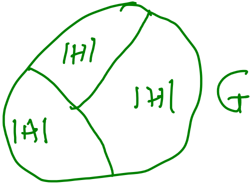
Theorem

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

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

...CONTINUES

$aH \subseteq bH$. But $|aH| = |H| = |bH| \Rightarrow aH = bH$ $\blacksquare$



$\exists\, t \in \mathbb{N}: \; t \cdot |H| = |G|$

$\Leftrightarrow |H| \mid |G|$ $\square$

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.

THM. Let G be a finite group. Then $\forall g \in G$, $g^{|G|} = 1$.

PF. Fix $g \in G$. $H = \{ g^i : i \in \mathbb{N}_0 \} = \{ 1 = g^0, g = g^1, g^2, g^3, \dots \}$

CL. $H \leq G$ PF. (RATHER) EASY EXERCISE, JUST USE THE "$a \cdot b^{-1}$-CRITERION"

$|H| = \mathrm{ord}(g)$. IN FACT, IF $g^t = 1$, $g^{t+\ell} = \underbrace{g^t}_{=1} \cdot g^\ell = g^\ell$

FROM LAGRANGE $|H| \cdot t = |G|$, $t \in \mathbb{N}$

$g^{|G|} = g^{t \cdot |H|} = (g^{|H|})^t \longrightarrow 1 \Rightarrow g^{|G|} = (1)^t = 1$ $\square$

Fermat's little theorem

Corollary

Let $N \in \mathbb{N}$ and $a \in \mathbb{Z}_N^*$, then

$$a^{\phi(N)} = 1.$$

PF.

GROUP WITH $|\mathbb{Z}_N^*| = \phi(N)$

Corollary (Fermat's little theorem)

Let N be a prime number. For each $a \in \{1, \ldots, N-1\}$ one has

$$a^{N-1} \equiv 1 \pmod{N}.$$

PF.

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

ALL $x \in \{0, .., N-1\}$; $\gcd(x, N) = 1$

RSA

WANTS TO RECEIVE THE MESSAGE

Bob:

- Generates large (512 bits) primes p and q ⟹ ? WE'LL SEE LATER.
- Computes $N = p \cdot q$. $(p-1)(q-1) = \phi(p) \cdot \phi(q)$
- Selects *encryption exponent* e such that $\gcd(e, \phi(N)) = 1$
- $\boxed{\text{Public key:}}$ (N, e)

EXTENDED EUCLIDEAN ALGORITHM

Alice: ⟵ SENDS THE MESSAGE

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

Bob:

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

FAST MODULAR EXPONENTIATION

EVE! KNOWS (N, e). IF SHE COULD FACTORIZE $N \Rightarrow$ KNOW p, q
$\Rightarrow \phi(N) \Rightarrow y \Rightarrow m$
BUT WE DON'T KNOW FAST ALGORITHMS FOR FACTORIZING N ¡

PROOF

To show $s^y = m \mod N$

$s^y = m^{e \cdot y}$. Since $y \cdot e \equiv 1 \mod \phi(N)$

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)

$s^y = m^{1 + K\phi(N)} = m^{1+K(p-1)(q-1)}$

K integer

Alice:

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

CASE 1: $p \nmid m \Rightarrow m^{p-1} \equiv 1 \mod p$

Bob:

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

Let's prove this!

$\Rightarrow \boxed{m^{1+K(q-1)(p-1)}} = m \cdot \underbrace{m^{K(q-1)(p-1)}}_{\equiv 1 \mod p}$

$\equiv \boxed{m \mod p}$

PROOF (CONTINUES)

<u>CASE 2:</u> $p \mid m \Rightarrow m = tp,\ t \in \mathbb{N} \Rightarrow \boxed{m^{1+x(p-1)(q-1)} = (tp)^{(\dots)}}$ $\underbrace{(tp)}_{\equiv\, 0 \bmod p}$

$\Rightarrow (0)^{(\dots)} \equiv 0 \bmod p$ $\equiv$

$\boxed{\equiv m \bmod p}$

SO WE GET

$s^y = m^{1+x(p-1)(q-1)} \equiv m \bmod p \Rightarrow s^y - m = m^{1+x(p-1)(q-1)} - m \equiv 0 \bmod p$

SIMILARLY $s^y \equiv m \bmod q$ $\equiv 0 \bmod q$

$p, q \mid s^y - m \Rightarrow N = p \cdot q \mid s^y - m$

$\Rightarrow s^y \equiv m \bmod N$ $\square$

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 THEOREM 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

FERMAT'S LITTLE THM.

N PRIME. THEN $\boxed{a^{N-1} \equiv 1} \bmod N \quad \forall a \in \mathbb{Z}_N \setminus \{0\}$

- 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*

IF N IS PRIME: $a^{N-1} \equiv 1 \bmod N \quad \forall a \in \mathbb{Z}_N \setminus \{0\}$

$\Rightarrow$ ALGORITHM ALWAYS ANSWERS "PRIME"

$\Rightarrow$ " " CORRECT

IF N NOT PRIME? ?

Carmichael numbers

An odd composite number $N \in \mathbb{N}$ is called *Carmichael number* if

$$\forall a \in \mathbb{Z}_N^*: a^{N-1} = 1.$$

CARMICHAEL NUMBERS FOOL FERMAT TEST!

CARMICHAEL NUMBERS EXIST!

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 $1/2$.*

$\Rightarrow$ (FOR N NOT CARMICHAEL, THE TEST IS WRONG WITH PR. $\leq \frac{1}{2}$)

If the weak Fermat test is repeated i times, then the probability that it asserts probably prime *in all i rounds is at most $1/2^i$.* $\longrightarrow$ GOES TO 0 VERY FAST

PF. Let N ODD, NON-CARM., COMPOSITE.

$$\boxed{H = \{ a \in \mathbb{Z}_N^* : a^{N-1} \equiv 1 \bmod N \}}$$

CL. $H \leq \mathbb{Z}_N^*$ PF. EXERCISE

$H \subsetneq \mathbb{Z}_N^*$ (N NOT CARM $\Rightarrow \exists a \in \mathbb{Z}_N^* : a^{N-1} \not\equiv 1 \bmod N$) $\Rightarrow$

$t|H| = |\mathbb{Z}_N^*|$ $\quad t \in \mathbb{N}_{\geq 2}$ $\Rightarrow$ $|H| \leq \frac{1}{2} |\mathbb{Z}_N^*|$ $\Rightarrow$ PR(AN $a \in H$ IS TAKEN) $\leq \frac{1}{2}$ $\square$

How do Carmichael numbers look like

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 $i = 1, \ldots, k$.