Computing in $\mathbb{Z}_N$

- $N \in \mathbb{N}$, $a \in \mathbb{Z}$: $[a] = \{x \in \mathbb{Z} : N \mid (a - x)\}$
- $\boxed{\mathbb{Z}_N = (\{[a] : a \in \mathbb{Z}\}, \oplus, \odot) \text{ is a ring}}$
- $\mathbb{Z}_N^*$ is (multiplicative) group of invertible elements.

[a] set of integers that have same remainder as a when we perform division by N.

$(\mathbb{Z}_N, \oplus)$ abelian group. $(\mathbb{Z}_N, \odot)$ is not a group

$(\mathbb{Z}_N^*, \odot)$ is an abelian group.

Theorem

$[a] \in \mathbb{Z}_N$ *is invertible if and only if* $\gcd(a, N) = 1$.

proof: if $\gcd(a,N)=1$, then there exist $x, y \in \mathbb{Z}$ with

$x \cdot a + y \cdot N = 1 \Rightarrow N \mid x \cdot a - 1$ i.e. $[x]$ is inverse of $[a]$.

$([x] = [a]^{-1})$

if $\exists [x]$ with $[x] \cdot [a] = [1]$,

then $N \mid x \cdot a - 1 \Rightarrow \gcd(a, N) = 1$ ∎

Computing the inverse

- Given: $a \in \mathbb{Z}, N \in \mathbb{N}$
- Compute $x, y \in \mathbb{Z}$ with $\gcd(a, N) = x \cdot a + y \cdot N$ with extended Euclidean algorithm
- If $\gcd(a, N) \neq 1$, then $a \notin \mathbb{Z}_N^*$
- Else: $a^{-1} = x$

[ ] [ ]

Fast exponentiation

- Given: $\underline{a, e, N} \in \mathbb{N}$ input in binary representation.
- Task: Compute $a^e \pmod N$
- Suppose: e has n bits, i.e.,

$$e = \underline{\langle b_{n-1}, \ldots, b_0 \rangle} = \sum_{j=0}^{n-1} b_i 2^i.$$

last bit

$e = \langle 1, 1, 0, 1 \rangle$

$a^e = a^{2^3 + 2^2 + 2^0}$

$= a^{2^3} \cdot a^{2^2} \cdot a^{2^0}$

$S = 1$

For $i := 1$ to e

$S := S \cdot a$

Return S.

count multiplications:

e many.

$\Rightarrow$ exponential time alg.

$(a^{2^i})^2 = a^{2 \cdot 2^i} = \quad h = a^{2^{i+1}}$

$h = a^{2^i}$

$S = 1$

$h = a$

For $i = 0$ to 3

if $b_i = 1$

$S := S \cdot h$

$h = h^2$

Return S

Fast exponentiation algorithm

```
function exp(a, e, N)

Input: a, e, N ∈ ℕ
Output: h ∈ ℕ with h ≡ a^e (mod N)

h = 1, s = a

for j = 0 to n − 1
    if b_j = 1
        h = h · s (mod N)
    s = s^2 (mod N)

return h
```

← # of bits of h is $O(\lg N) = O(\text{Size}(N))$

Theorem: a^e can be computed with $O(\log(e))$ arithmetic operations.

$$\text{Size}(a^e) = \Theta(\log a^e)$$

$$= \Theta(\underbrace{e}_{2^{\text{size}(e)}} \cdot \underbrace{\log a}_{\approx \text{size}(a)})$$

# of bits of a^e is exponential in # bits of e.

Theorem

Given $a, e, N \in \mathbb{N}$ with $0 \leq a \leq N$, one can compute $s \in \mathbb{N}$ with $s \equiv a^e \pmod{N}$ in time $O(M(\mathrm{size}(N)) \cdot \mathrm{size}(e))$, where $M(n)$ denotes the time required for n-bit multiplication.

Remark: $M(n)$ is also time required for division with remainder. input two n-bit numbers.

Definition

Let G together with $\odot$ be a group. A subset $H \subseteq G$ is called a subgroup of G, if H together with $\odot$ is itself a group. We write $H \trianglelefteq G$.

Theorem $H \neq \emptyset$

$H \trianglelefteq G$ if and only if for each $a, b \in H$ one has $a \odot b^{-1} \in H$.

proof: if $H \trianglelefteq G$, then for $a, b \in H$, one has 1.) $b^{-1} \in H$

2.) $a \odot b^{-1} \in H$

Suppose now that $a \odot b^{-1} \in H$ for ~~all~~ all $a, b \in H$.

i) e (Neutral element) is in H, $a \cdot a^{-1} = e \in H$

ii) $a \in H$ to show $a^{-1} \in H$: $e, a \in H \Rightarrow e \cdot a^{-1} \in H \rightarrow a^{-1} \in H$

iii) associativity clear: iv) $a \odot b \in H$? whenever $a, b \in H$?

since $b^{-1} \in H$ we have $a \odot (b^{-1})^{-1} \in H$

$= a \odot b$

Example

- $H \leq \mathbb{Z}, +$
- $H \leq \mathbb{Z}_5$

$\exists\, d \in \mathbb{N}_0$ s.th. $H = \{ d \cdot z : z \in \mathbb{Z} \}$

Case 1: $H = \{0\} \Rightarrow d = 0$

Case 2: $H \neq \{0\}$. $(H \cap \mathbb{N}_{\geq 1}) \neq 0$

$d = \min \{ H \cap \mathbb{N}_{\geq 1} \}$.

$H = d \cdot \mathbb{Z}$.

$\mathbb{Z}_5 = \{ [0], [1], [2], [3], [4] \}$

$+$

$H = \{0\}$

$H = \mathbb{Z}_5$ are only subgroups. Why?

$|H| \; \Big| \; |\mathbb{Z}_5| = 5$

$\Rightarrow$ $\mathbb{Z}_5$ has only two subgroups.

Theorem

on G

Let $H \trianglelefteq G$. The relation $a \sim b$ if $a \odot b^{-1} \in H$ is an equivalence relation with equivalence class $[a] = a \odot H = \{a \odot h \colon h \in H\}$.

proof: Reflexivity. $\forall g \in G$: $g \sim g$ because $g \odot g^{-1} = e \in H$

Symmetry. $\forall a, b \in G$ if $a \sim b$ $(a \odot b^{-1} \in H)$ one has

$b \sim a$ since $(a \odot b^{-1})^{-1} = b \cdot a^{-1} \in H$

Transitivity: Suppose $a \sim b$, $b \sim c$

$a \odot b^{-1} \in H$, $b \odot c^{-1} \in H$

$\Rightarrow$ $\odot$ closed $\Rightarrow$ $a \odot b^{-1} \odot b \odot c^{-1} = a \odot e \odot c^{-1}$

$= a \odot c^{-1} \in H$.

"$\subseteq$" $c \in [a]$, then $a \sim c \Rightarrow a \cdot c^{-1} = h$ for some $h \in H \Rightarrow a = c \cdot h$ $\Rightarrow a \in c \cdot H$

"$\supseteq$" equally simple.

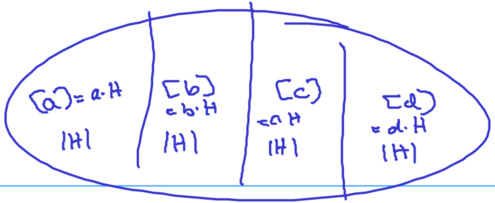
$G = \mathbb{Z}_{25}$

$H \trianglelefteq G$

$H = \{0\}$

$H = \mathbb{Z}_{25}$

are only possibilities.



$|G| \leq \infty$

$H \trianglelefteq G$

$|a \cdot H| = |H|$

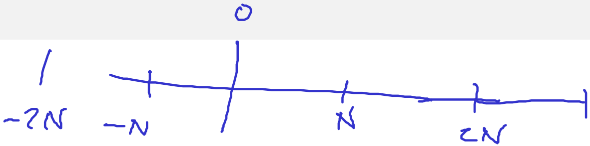
$a^{-1} \, a \cdot h_1 = a^{-1} a \cdot h_2 \quad = h_1 = h_2$

$\Rightarrow \quad |H| \;\big|\; |G|$

$\Rightarrow$ Theorem of Lagrange.

Example

- $G = \mathbb{Z}, \odot = +, H = N \cdot \mathbb{Z}$



$a \sim b$ $\quad$ $a - b \in N \cdot \mathbb{Z}$

$[a] = [a]$

from before.

Cosets

$H \trianglelefteq G, \quad H \neq \emptyset$

Lemma

If H is finite, then $|a \odot H| = |b \odot H|$ for each $a, b \in G$.

Corollary (Theorem of Lagrange)

If G is a finite group and $H \trianglelefteq G$, then $|H| \mid |G|$.

divides.

Fermat's little theorem

Good for later: Alg that tests whether N is prime. Alg should run in poly time in size(N). Basis for that is Fermat's little theorem.

Theorem

If N is a prime number, then

$\forall a \in 1, \dots, N-1$: $a^{N-1} = 1 \pmod N$

proof: $|\mathbb{Z}_N^*| = N-1$

$H = \langle a \rangle \trianglelefteq \mathbb{Z}_N^*$ $\qquad \langle a \rangle = \{a^0, a^1, a^2, \dots, a^{\mathrm{ord}(a)-1}\}$.

$\langle a \rangle$ is a subgroup of $\mathbb{Z}_N^*$.

Lagrange theorem: $\mathrm{order}(a) \mid N-1$. $\qquad (N-1) = \mathrm{order}(a) \cdot x$ with some $x \in \mathbb{Z}$.

$\Rightarrow \quad a^{N-1} = \left(a^{\mathrm{order}(a)}\right)^x = 1^x = 1 \mod (N)$.

We swept two things under the rug.

1.) $\operatorname{order}(a) = \min\{x : x \geq 1,\ a^x = 1 \bmod N\}$ exists.

2.) $\langle a \rangle = \langle a^0, a^1, \dots, a^{\operatorname{order}(a)-1} \rangle \trianglelefteq \mathbb{Z}_N^*$.

Assuming 1) lets show 2.). $\forall\, c, d \in \langle a \rangle \quad c \cdot d^{-1} \in \langle a \rangle$.

$$c = a^i, \quad d = a^j$$

$$c \cdot d^{-1} = a^i \cdot a^{\operatorname{order}(a)-j}$$

$$= a^{i + \operatorname{order}(a) - j} = a^r \quad r = \text{remainder of div. of } i + \operatorname{order}(a) - j \text{ by } \operatorname{order}(a)$$

$\in \langle a \rangle$.

1.) $\underbrace{a^1, a^2, a^3, \dots, a^S}_{\text{No repetition.}}, \; a^{S+1} = a^2$ multiply by a^{-1}.

$\underbrace{1, a, \dots, a^{S-1}}, \; a \qquad a^S = a$ repetition before!

Definition

For $N \in \mathbb{N}$ we define $\phi(N) = |\mathbb{Z}_N^*|$.

Example

then.

$a \in \{1, 2, \dots, N-1\}$ $\gcd(a, N) = 1$

- $\phi(N) = N - 1$ if N is prime.
- $\phi(15) =$. $|\{1, 2, 4, 7, 8, 11, 13, 14\}| = 8$

$= \phi(5) \cdot \phi(3) = 4 \cdot 2$

I.F $N = N_1 \cdot N_2 \cdots \cdot N_k$ with $\gcd(N_i, N_j) = 1$ $\forall i \neq j$

then $\phi(N) = \phi(N_1) \cdot \phi(N_2) \cdots \phi(N_k)$

ϕ is multiplicative.

Recap: Rings

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

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 $a + (-a) = 0$

$(R, +)$ is an abelian group.

(R5) $a(bc) = (ab)c$ • Associative.

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

(R7) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$. ← Distributive laws.

• was commutative, then R is called commutative ring. if $a \cdot b \neq 0$ whenever $a, b \neq 0$ R is integral domain

Example: $N \in \mathbb{N}_+$, $(\mathbb{Z}_N, \oplus, \odot)$ is a ring

$N = 15$.

$3 \cdot 5 = 0$

Recap: Rings

Examples:

- $\mathbb{Z}$ ← commutative, integral domain
- $\mathbb{Z}_N$ ← commutative.
- $R_1 \times \cdots \times R_k$, 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.

$(R_i, \oplus_i, \odot_i)$ are rings.

not i.d. not commutative.

$$R_1 \times R_2 \times \cdots \times R_n = \{ (r_1, r_2, \ldots, r_n) : r_i \in R_i \}.$$

$$\oplus : (r_1, \ldots, r_n) \oplus (y_1, \ldots, y_n) = (r_1 \oplus_1 y_1, \ldots, r_n \oplus_n y_n)$$

$$\odot : (r_1, \ldots, r_n) \odot (y_1, \ldots, y_n) = (r_1 \odot_1 y_1, \ldots, r_n \odot_n y_n)$$

→ Ring

Example of an easy ring-theorem

Theorem

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

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

Proof:

$$0 \cdot r = (0+0) \cdot r = 0 \cdot r + 0 \cdot r \quad \Big| - 0 \cdot r$$

$$0 = 0 \cdot r.$$

$\square$

Ring homomorphism

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

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

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

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

Examples:

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

Chinese Remainder Thm.

$\Phi(N)$ multiplicative.

$\downarrow$

RSA.

↳ Efficient primality tests

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.

$\phi(\cdot)$ is multiplicative

Corollary

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

$\phi(\cdot)$ and factoring

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*

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