Arithmetics of b-bit numbers ... $O(b^{const})$

Euclid's algorithm for computing $gcd(x,y)$

- in the modulo version: $O(b)$ iteration, 1 iteration takes $O(b^2)$ time } $O(b^3)$
- more careful analysis: $O(b^2)$ time
- alt: binary alg.: $O(b^2)$ time

$x, y$ coprime $\equiv gcd(x,y)=1 \equiv x \perp y$

everything E.a. computes is $\alpha x + \beta y$

$\Rightarrow \exists \alpha, \beta \in \mathbb{Z}: gcd(x,y) = \alpha x + \beta y$

$\alpha, \beta$: Bézout coefficients; extended Euclid's alg.

---

Computation modulo $N$ → the ring $(\mathbb{Z}_N, +, -, \cdot, 0, 1)$, $\in \{0 \dots N-1\}$

When is $a \in \mathbb{Z}_N$ invertible? $\exists x: ax \equiv 1 \pmod N$

$x$: multiplicative inverse of $a$, $a^{-1}$

$\exists x \exists y: ax + Ny = 1$

if $gcd(a,N)=1$ → $x, y$ are Bézout's coeffs

if $gcd(a,N)>1$ → no sol. exists

Thm: $a$ is invertible $\Leftrightarrow a \perp N$.

Df: $\mathbb{Z}_N^* := \{a \in \mathbb{Z}_N \mid a \perp N\}$ set of invertible elements

$1 \in \mathbb{Z}_N^*$ $\forall a,b \in \mathbb{Z}_N^*: ab \in \mathbb{Z}_N^*$

Df: $(\mathbb{Z}_N^*, \cdot, 1)$ multiplicative group mod $N$

If $N=p$ is a prime: $\mathbb{Z}_p^* = \{1 \dots N-1\}$

$\mathbb{Z}_p$ is a field

Df: $\varphi(N) := |\mathbb{Z}_N^*|$ Euler function; $\varphi(p) = p-1$

all operations in the field computed in $O(b^3)$ time

---

Thm (Little Fermat's): For $p$ prime, $x \perp p$: $x^{p-1} \bmod p = 1$.

$x^{p-2} \equiv x^{-1} \pmod p$

$x^{p-2} \cdot x = x^{p-1} \equiv 1$

↓ generalization

Thm (Euler): For $N>1$, $x \perp N$: $x^{\varphi(N)} \equiv 1 \pmod N$.

Proof: Consider $1 = x^0, x^1, x^2, x^3, \dots, x^k = 1$ (all distinct)

$H$

$H$ is a subgroup of $\mathbb{Z}_N^*$

by Lagrange: $|H| \setminus |\mathbb{Z}_N^*|$

$k$ | $\varphi(N)$

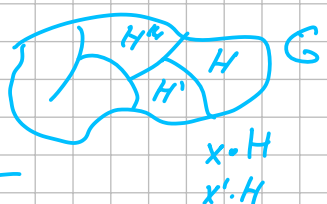
so $\varphi(N) = k \cdot \ell$ for some $\ell$

$x^{\varphi(N)} \equiv x^{k \cdot \ell} \equiv (x^k)^\ell \equiv 1^\ell \equiv 1.$ QED

if $x^i = x^j$ for $i<j$ then $x^{j-i} = 1$

$x^i \cdot x^j = x^{(i+j) \bmod k}$

Thm (Lagrange): If $G$ is a finite group, $H \leq G$, then $|H| \setminus |G|$.



**Thm** (Chinese Remainder Theorem, CRT): For $N_1, \dots, N_k$ pairwise coprime, $N := \prod_i N_i$:

$$\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \dots \times \mathbb{Z}_{N_k} \cong \mathbb{Z}_N$$

2 proofs for the case $k=2$ (continue by induction...)

$x \in \mathbb{Z}_N \to (x \bmod N_1, x \bmod N_2, \dots, x \bmod N_k)$

① Consider $f: \mathbb{Z}_N \to \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$

$f: x \mapsto (x \bmod N_1, x \bmod N_2)$

- $f$ is injective: if $f(x) = f(y)$ then $f(x-y) = (0,0)$
  $x-y$ is divisible by both $N_1, N_2$
  $x-y$ is divisible by $N_1 \cdot N_2 = N$
  so $x = y$.
- $f$ is bijective: both sets have the same cardinality $N$.

② Constructive: given $(a,b)$ find $x$ : $f(x) = (a,b)$

find $u, v$: $f(u) = (1,0)$ $f(v) = (0,1)$

then $f(\underbrace{au + bv}_{\text{the inverse of } (a,b)}) = a \cdot f(u) + b \cdot f(v) = (a,0) + (0,b) = (a,b)$

$f(N_1) = (0, c_1)$, $c_1 \perp N_2$

If $c_1 = 1$: $v := N_1$

else: $c_1^{-1}$ := mult. inverse of $c_1$ mod $N_2$

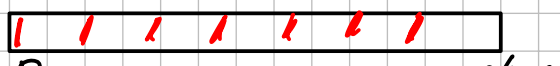
$f(c_1^{-1} \cdot N_1) = c_1^{-1} \cdot (0, c_1) = (0,1)$ (mod $N$; mod $N_2$)

Similarly from $f(N_2)$ obtain $u$.

---

**Computation of $\varphi(N)$:**

- $\varphi(p) = p-1$
- $\varphi(p^k) = \frac{p-1}{p} \cdot p^k = (p-1)p^{k-1}$




every $p$-th element not coprime

- $\varphi(N_1 \cdot N_2) = \varphi(N_1) \cdot \varphi(N_2)$ for $N_1 \perp N_2$ (by CRT)

$\varphi(N)$ can be computed from the factorization of $N$

$f: x \mapsto (x \bmod N_1, x \bmod N_2)$ ← $\varphi(N_1) \cdot \varphi(N_2)$ pairs

$x \perp N \Leftrightarrow x \perp N_1$ & $x \perp N_2$

---

**Factorization** vs. **Primality testing**

$n^{\log n}$, $2^{\log n}$, $2^{\log n \cdot \text{const}}$

Factorization: given $x$, find all prime factors of $x$

considered hard

- straightforward algs are exponential
- complicated sub-exp. algs (getting better & better)
- poly-time quantum alg. [Shor 1994]

Primality testing: is $x$ a prime?

- fast randomized algorithms with one-sided error (composite can be claimed prime with $p_r < \varepsilon$)
- deterministic poly-time alg. [Agarwal et al. 2002]

# Primality Testing (a sketch)

Fermat test for $N \in \mathbb{Z}$

1. Generate $a \in_R \mathbb{Z}_N$, $a \neq 0$
2. If $a \perp N$ : NO (a is Euclid witness)
3. If $a^{N-1} \bmod N \neq 1$ : NO (a is Fermat witness)
4. YES

→ Rabin-Miller test
this also catches Carm. numbers ] used in practice

Analysis:
we want: if $N$ is not prime, $Pr_a[\text{YES}] < \varepsilon$
No...

- Carmichael numbers: (smallest: 561)
  $N$ is composite
  & $a \in \mathbb{Z}_N^*$ $a^{N-1} \bmod N = 1$

Thm: If $N$ is composite, but not Carmichael, then $Pr_a[\text{YES}] \leq 1/2$.

Pf: $H := \{ a \in \mathbb{Z}_N^* \mid a^{N-1} = 1 \}$
$H$ is a sub-group of $\mathbb{Z}_N^*$
so $|H| \mid |\mathbb{Z}_N^*|$
but $H \neq \mathbb{Z}_N^*$
so $|H| \leq 1/2 |\mathbb{Z}_N^*|$

How to generate a random 6-bit prime?
Generate a random 6-bit number with leading 1
Test primality, if NO, repeat.
Claim: density of primes around $N \sim \frac{1}{\ln N}$ → on average, $O(6)$ tries suffice

---

# Discrete Logs

$g^{p-1} = 1$ $\quad g^i \cdot g^j = g^{(i+j) \bmod (p-1)}$

Thm: The group $\mathbb{Z}_p^*$ is cyclic.

$$\exists g : \{g^0, g^1, g^2, \ldots, g^{p-2}\} = \mathbb{Z}_p^*$$

$g$: generator

$\exists$ isomorphism $f$: $\mathbb{Z}_p^* \simeq (\mathbb{Z}_{p-1}, +)$
$\leftarrow g^x$
$\rightarrow$ discrete log ] hardness similar to factorization

How to tell if $g$ generates $\mathbb{Z}_p^*$?

$H := \{g^0, g^1, g^2, g^3, \ldots, g^{k-1}\}$, $g^k = 1$
$H \subseteq \mathbb{Z}_p^*$ Lagrange → $|H| \mid |\mathbb{Z}_p^*|$
($|H| = k$, $|\mathbb{Z}_p^*| = p-1$)

if $k < p-1$ : $p-1 = k \cdot \ell$ ($g$ isn't gen., $\ell > 1$)

$g^k = 1$
$g^{\frac{p-1}{\ell}} = 1$
$\ell$ suffices to check
Try all $\ell$: prime factors of $p-1$ (prime $\ell$'s)
Check $g^{\frac{p-1}{\ell}} \bmod p$
if $\neq 1 \Rightarrow$ NO

$g^0, g^1, g^2, \ldots, g^{k-1}$ ($k$)

How to obtain a generator?
Try randomly... $Pr[\text{success}] = \frac{\varphi(p-1)}{p-1}$

if $g$ is a gen.
then $g^k$ is a gen $\Leftrightarrow k \perp p-1$

$\#\text{gens} = \varphi(p-1)$