Modular Arithmetic

Applications to Cryptography

Abhijit Das

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

October 5, 2020

Congruence Modulo n

- Take $n \in \mathbb{N}$ (preferable to have $n \geqslant 2$).
- Two integers $a, b \in \mathbb{Z}$ are said to be **congruent** modulo n if $n|(a-b)$.
- We denote this as $a \equiv b \pmod{n}$.
- Congruence modulo n is an equivalence relation on $\mathbb{Z}$.
- There are n equivalence classes: $[0], [1], [2], \ldots, [n-1]$.

Integers Modulo n

- Define $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$.
- You may view $\mathbb{Z}_n$ as the set of remainders of Euclidean division by n.
- You can also view the elements of $\mathbb{Z}_n$ as representatives of the equivalence classes under congruence modulo n.
- There is also an algebraic description (not covered). $\mathbb{Z}_n$ is quotient $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ with respect to the ideal $n\mathbb{Z}$ of $\mathbb{Z}$.
- For $a, b \in \mathbb{Z}_n$, define the following operations.
  - $a +_n b = \begin{cases} a+b & \text{if } a+b < n, \\ a+b-n & \text{if } a+b \geqslant n. \end{cases}$
  - $a \cdot_n b = (ab) \operatorname{rem} n$.
- $\mathbb{Z}_n$ is a *commutative ring with identity* under these two operations.

Units of $\mathbb{Z}_n$

Theorem: $a \in \mathbb{Z}_n$ is a unit if and only if $\gcd(a,n) = 1$.

Proof [If] There exist integers u, v such that $ua + vn = 1$. We can choose u such that $0 \leqslant u < n$. But then $ua \equiv 1 \pmod{n}$.
[Only if] If a is a unit of $\mathbb{Z}_n$, then $ua \equiv 1 \pmod{n}$ for some $u \in \mathbb{Z}_n$, that is, $ua = 1 + vn$ for some v. Since $\gcd(a,n)$ divides a (and so ua) and n (and so vn), it divides 1, that is, $\gcd(a,n) = 1$.

- $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$.
- $|\mathbb{Z}_n^*| = \phi(n)$ (Euler totient function).
- Since $\mathbb{Z}_n^*$ is a group, we have $a^{\phi(n)} \equiv 1 \pmod{n}$ for any $a \in \mathbb{Z}_n^*$ (**Euler's theorem**).
- For a prime p, we have $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$, and $\phi(p) = p - 1$.
- For $a \in \mathbb{Z}_p^*$, we have $a^{p-1} \equiv 1 \pmod{p}$ (**Fermat's little theorem**).

Modular Exponentiation

Given $a \in \mathbb{Z}_n$ and $e \in \mathbb{N}_0$, to compute $a^e \pmod{n}$.

The square-and-multiply algorithm

modexp (a, e, n)
{
    If $(e = 0)$, return 1.
    Write $e = 2f + r$ with $f = \lfloor e/2 \rfloor$ and $r \in \{0, 1\}$.
    Set $t = \text{modexp}(a, f, n)$.
    Set $t = t^2 \pmod{n}$.
    If $(r = 1)$, set $t = ta \pmod{n}$.
    Return t.
}

Modular Exponentiation: Iterative Version

Let $e = (e_{l-1}e_{l-2}\ldots e_2e_1e_0)_2$ be the binary expansion of e.

```
modexp (a, e, n)
{
    Initialize t = 1.
    For i = l-1, l-2, ..., 2, 1, 0, repeat:
        Set t = t^2 (mod n).
        If (e_i = 1), set t = ta (mod n).
    Return t.
}
```

For $e < n$, the running time is $O(\log^3 n)$.

Diffie–Hellman Key Agreement

- First known public-key algorithm (1976).
- Alice and Bob want to share a secret.
- They use an insecure communication channel.
- They agree upon a suitable finite group G (say, multiplicative). Let $n = |G|$.
- Suppose that G is cyclic. They publicly decide a generator g of G.
- Alice generates $a \in_R \{0, 1, 2, \ldots, n-1\}$, and computes and sends g^a to Bob.
- Bob generates $b \in_R \{0, 1, 2, \ldots, n-1\}$, and computes and sends g^b to Alice.
- Alice computes $g^{ab} = (g^b)^a$.
- Bob computes $g^{ab} = (g^a)^b$.

Security of the Protocol

- How difficult is it for an eavesdropper to obtain g^{ab} from g, g^a, g^b?
- This is called the computational Diffie–Hellman problem (CDHP).
- a (resp. b) is called the discrete logarithm of g^a (resp. g^b) to the base g.
- Computing a or b enables an eavesdropper to get the shared secret.
- This is called the discrete-logarithm problem (DLP).
- If DLP is easy, then CDHP is easy.
- The converse is not known (but is believed to be true).
- A related problem: Given $g, g^a, g^b, h \in G$, decide whether $h = g^{ab}$.
- This is the decisional Diffie–Hellman problem (DDHP).
- For some groups, all these problems are assumed to be difficult.

A Candidate Group

- Take a large prime p.
- $G = \mathbb{Z}_p^*$ is cyclic.
- But computing a generator of $\mathbb{Z}_p^*$ requires complete factorization of $p-1$.
- So we generate a large prime p such that $p-1$ has a large prime factor q.
- Generate random $h \in G$, and compute $g \equiv h^{(p-1)/q} \pmod{p}$.
- If $g \not\equiv 1 \pmod{p}$, than g has order q.
- We can work in the subgroup of $\mathbb{Z}_p^*$, generated by g.
- The discrete-logarithm problem for $\mathbb{Z}_p^*$ is difficult for suitable choices of p.
- Only subexponential algorithms are known.

RSA Cryptosystem

- Invented by Rivest, Shamir, and Adleman (1978).
- The first public-key encryption algorithm.
- Alice wants to send a secret message to Bob.
- Bob chooses two large primes p, q, and computes $n = pq$ and $\phi(n) = (p-1)(q-1)$.
- Bob chooses an e such that $\gcd(e, \phi(n)) = 1$.
- Bob computes $d \equiv e^{-1} \pmod{\phi(n)}$.
- Bob publishes (n, e), and keeps d secret.
- Alice encodes her secret message to $m \in \mathbb{Z}_n$.
- Alice sends $c \equiv m^e \pmod{n}$ to Bob.
- Bob recovers $m \equiv c^d \pmod{n}$.

Correctness

- We have $ed = 1 + k\phi(n) = 1 + k(p-1)(q-1)$.
- If $p \not| m$, then by Fermat's little theorem, $m^{p-1} \equiv 1 \pmod{p}$.
- But then $m^{ed} \equiv m^{1+k(p-1)(q-1)} \equiv m \times (m^{p-1})^{k(q-1)} \equiv m \pmod{p}$.
- If $p|m$, we have $m^{ed} \equiv m \equiv 0 \pmod{p}$.
- In all cases, $m^{ed} \equiv m \pmod{p}$.
- Likewise, $m^{ed} \equiv m \pmod{q}$.
- By the Chinese remainder theorem, $m^{ed} \equiv m \pmod{n}$.

Security

- RSA key-inversion problem: Compute d from (n, e).
- This is as difficult as factoring n.
- RSA problem: Given (n, e, c), compute m.
- This is believed to be as difficult as factoring n.
- Factoring large n is very difficult.
- Only some subexponential algorithms are known.

But...

- Polynomial-time algorithms are known for quantum computers
- for both the factoring and the discrete-log problems.
- Peter Shor, 1994-1995.
- Diffie–Hellman and RSA are unsafe in the quantum world.
- But building quantum computers is very challenging.
- So far, quantum computers could factor 15 and 21.
- Time will tell who will win.