CSE107: Intro to Modern Cryptography

https://cseweb.ucsd.edu/classes/sp22/cse107-a/

Emmanuel Thomé

April 28, 2022

Lecture 9a

Computational Number Theory

Intro

Groups

Computing in $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$

Plan

Intro

Groups

Computing in $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$

Secret key exchange

Problem: Obtain a joint secret key via interaction over a public channel:

Alice		**Bob**
$x \xleftarrow{\$} \ldots;\ X \leftarrow \ldots$		
	$\xrightarrow{X}$	
		$y \xleftarrow{\$} \ldots;\ Y \leftarrow \ldots$
	$\xleftarrow{Y}$	
$K_A \leftarrow F_A(x, Y)$		$K_B \leftarrow F_B(y, X)$

Desired properties of the protocol:

- $K_A = K_B$, meaning Alice and Bob agree on a key
- Adversary given X, Y can't compute K_A

Secret Key Exchange

Can you build a secret key exchange protocol?

Secret Key Exchange

Can you build a secret key exchange protocol?

Symmetric cryptography has existed for thousands of years.

But no secret key exchange protocol was found in that time.

Many people thought it was impossible.

Secret Key Exchange

Can you build a secret key exchange protocol?

Symmetric cryptography has existed for thousands of years.

But no secret key exchange protocol was found in that time.

Many people thought it was impossible.

In 1976, Diffie and Hellman proposed one.

This was the birth of public-key (asymmetric) cryptography.

DH Key Exchange Video

http://www.youtube.com/watch?v=3QnD2c4Xovk

DH Secret Key Exchange

The following are assumed to be public: A large prime p and a number g called a generator mod p. Let $\mathbb{Z}_{p-1} = \{0, 1, \ldots, p-2\}$.

Alice		**Bob**
$x \xleftarrow{\$} \mathbb{Z}_{p-1}$; $X \leftarrow g^x \bmod p$		
	$\xrightarrow{X}$	
		$y \xleftarrow{\$} \mathbb{Z}_{p-1}$; $Y \leftarrow g^y \bmod p$
	$\xleftarrow{Y}$	
$K_A \leftarrow Y^x \bmod p$		$K_B \leftarrow X^y \bmod p$

- $Y^x = (g^y)^x = g^{xy} = (g^x)^y = X^y$ modulo p, so $K_A = K_B$
- Adversary is faced with computing $g^{xy} \bmod p$ given $g^x \bmod p$ and $g^y \bmod p$, which nobody knows how to do efficiently for large p.

DH Secret Key Exchange: Questions

- How do we pick a large prime p, and how large is large enough?
- What does it mean for g to be a generator modulo p?
- How do we find a generator modulo p?
- How can Alice quickly compute $x \mapsto g^x \bmod p$?
- How can Bob quickly compute $y \mapsto g^y \bmod p$?
- Why is it hard to compute $(g^x \bmod p, g^y \bmod p) \mapsto g^{xy} \bmod p$?
- ...

To answer all that and more, we will forget about DH secret key exchange for a while and take a trip into computational number theory ...

Notation

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{N} = \{0, 1, 2, \ldots\}$

$\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$

For $a, N \in \mathbb{Z}$ let $\gcd(a, N)$ be the largest $d \in \mathbb{Z}_+$ such that d divides both a and N.

Example: $\gcd(30, 70) = 10$.

Integers mod N

For $N \in \mathbb{Z}_+$, let

- $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$
- $\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N \ : \ \gcd(a, N) = 1\}$
- $\varphi(N) = |\mathbb{Z}_N^*|$

Example: $N = 12$

- $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
- $\mathbb{Z}_{12}^* =$

Integers mod N

For $N \in \mathbb{Z}_+$, let

- $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$
- $\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N \ : \ \gcd(a, N) = 1\}$
- $\varphi(N) = |\mathbb{Z}_N^*|$

Example: $N = 12$

- $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
- $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$
- $\varphi(12) =$

Integers mod N

For $N \in \mathbb{Z}_+$, let

- $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$
- $\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N \ : \ \gcd(a, N) = 1\}$
- $\varphi(N) = |\mathbb{Z}_N^*|$

Example: $N = 12$

- $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
- $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$
- $\varphi(12) = 4$

Division and mod

INT-DIV(a, N) returns (q, r) such that
- $a = qN + r$
- $0 \leq r < N$

Refer to q as the quotient and r as the remainder. Then

Definition (The mod operation)

$$a \bmod N = r \in \mathbb{Z}_N$$

is the remainder when a is divided by N.
mod is a two argument (a.k.a. binary) operation, like $+$, $\times$, ...

Example: INT-DIV$(17, 3) = (5, 2)$ and $17 \bmod 3 = 2$.

Definition (Congruences mod something)

$a \equiv b \pmod{N}$ means $a \bmod N = b \bmod N$.

Example: $17 \equiv 14 \pmod{3}$

Plan

Plan

Groups

Let G be a non-empty set, and let $\cdot$ be a binary operation on G. This means that for every two points $a, b \in G$, a value $a \cdot b$ is defined.

Groups

Let G be a non-empty set, and let $+$ be a binary operation on G. This means that for every two points $a, b \in G$, a value $a + b$ is defined.

Groups

Let G be a non-empty set, and let $\perp$ be a binary operation on G. This means that for every two points $a, b \in G$, a value $a \perp b$ is defined.

Groups

Let G be a non-empty set, and let $\otimes$ be a binary operation on G. This means that for every two points $a, b \in G$, a value $a \otimes b$ is defined.

Groups

Let G be a non-empty set, and let $\uparrow$ be a binary operation on G. This means that for every two points $a, b \in G$, a value $a \uparrow b$ is defined.

Groups

Let G be a non-empty set, and let $\$$ be a binary operation on G. This means that for every two points $a, b \in G$, a value $a\$b$ is defined.

Groups

Let G be a non-empty set, and let $\cdot$ be a binary operation on G. This means that for every two points $a, b \in G$, a value $a \cdot b$ is defined.

Example: $G = \mathbb{Z}_{12}^*$ and "$\cdot$" is multiplication modulo 12, meaning

$$a \cdot b = ab \bmod 12$$

Definition (Groups)

We say that G is a *group* if it has four properties called closure, associativity, identity and inverse that we present next.

Fact: If $N \in \mathbb{Z}_+$ then $G = \mathbb{Z}_N^*$ with $a \cdot b = ab \bmod N$ is a group.

Groups: Closure (property 1/4)

Definition (Closure)

Closure: For every $a, b \in G$ we have $a \cdot b$ is also in G.
We also say that G is closed under the operation $\cdot$.

Example: $G = \mathbb{Z}_{12}$ with $a \cdot b = ab$ does not have closure (is not closed under multiplication) because $7 \cdot 5 = 35 \notin \mathbb{Z}_{12}$.

Groups: Closure (property 1/4)

Definition (Closure)

Closure: For every $a, b \in G$ we have $a \cdot b$ is also in G.
We also say that G is closed under the operation $\cdot$.

Example: $G = \mathbb{Z}_{12}$ with $a \cdot b = ab$ does not have closure (is not closed under multiplication) because $7 \cdot 5 = 35 \notin \mathbb{Z}_{12}$.

Example: The set of real numbers in $[0, 1]$ is closed under the operation

$$x \cdot y = x + y - xy.$$

Groups: Closure (property 1/4)

Definition (Closure)

Closure: For every $a, b \in G$ we have $a \cdot b$ is also in G.
We also say that G is closed under the operation $\cdot$.

Example: $G = \mathbb{Z}_{12}$ with $a \cdot b = ab$ does not have closure (is not closed under multiplication) because $7 \cdot 5 = 35 \notin \mathbb{Z}_{12}$.

Fact: If $N \in \mathbb{Z}_+$ then $G = \mathbb{Z}_N^*$ with $a \cdot b = ab \bmod N$ satisfies closure, meaning

$$\gcd(a, N) = \gcd(b, N) = 1 \text{ implies } \gcd(ab \bmod N, N) = 1$$

Example: Let $G = \mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$. Then

$$5 \cdot 7 \bmod 12 = 35 \bmod 12 = 11 \in \mathbb{Z}_{12}^*$$

Exercise: Prove the above Fact.

Groups: Associativity (property 2/4)

Definition (Associativity)

Associativity: For every $a, b, c \in G$ we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Fact: If $N \in \mathbb{Z}_+$ then $G = \mathbb{Z}_N^*$ with $a \cdot b = ab \bmod N$ satisfies associativity, meaning

$$((ab \bmod N)c) \bmod N = (a(bc \bmod N)) \bmod N$$

Example:

$$\begin{aligned}(5 \cdot 7 \bmod 12) \cdot 11 \bmod 12 &= (35 \bmod 12) \cdot 11 \bmod 12 \\ &= 11 \cdot 11 \bmod 12 = 1 \\ 5 \cdot (7 \cdot 11 \bmod 12) \bmod 12 &= 5 \cdot (77 \bmod 12) \bmod 12 \\ &= 5 \cdot 5 \bmod 12 = 1\end{aligned}$$

Groups: Identity element (property 3/4)

Definition ((existence of) Identity element)

Identity element: There exists an element $\mathbf{id} \in G$ such that $a \cdot \mathbf{id} = \mathbf{id} \cdot a = a$ for all $a \in G$.

Fact: If $N \in \mathbb{Z}_+$ and $G = \mathbb{Z}_N^*$ with $a \cdot b = ab \bmod N$ then 1 is the identity element because $a \cdot 1 \bmod N = 1 \cdot a \bmod N = a$ for all a.

Groups: Inverses (property 4/4)

Definition (Inverse)

Inverses: For every $a \in G$ there exists a unique $b \in G$ such that $a \cdot b = b \cdot a = \mathbf{id}$.

Fact: If $N \in \mathbb{Z}_+$ and $G = \mathbb{Z}_N^*$ with $a \cdot b = ab \bmod N$ then $\forall a \in \mathbb{Z}_N^* \quad \exists b \in \mathbb{Z}_N^*$ such that $a \cdot b \bmod N = 1$.

Example: The inverse of 5 in $\mathbb{Z}_{12}^*$ is the $b \in \mathbb{Z}_{12}^*$ satisfying $5b \bmod 12 = 1$, so $b =$

Groups: Inverses (property 4/4)

Definition (Inverse)

Inverses: For every $a \in G$ there exists a unique $b \in G$ such that $a \cdot b = b \cdot a = \mathbf{id}$.

Fact: If $N \in \mathbb{Z}_+$ and $G = \mathbb{Z}_N^*$ with $a \cdot b = ab \bmod N$ then $\forall a \in \mathbb{Z}_N^* \quad \exists b \in \mathbb{Z}_N^*$ such that $a \cdot b \bmod N = 1$.

Example: The inverse of 5 in $\mathbb{Z}_{12}^*$ is the $b \in \mathbb{Z}_{12}^*$ satisfying $5b \bmod 12 = 1$, so $b = 5$

Examples of groups

Fact: If $N \geq 1$ is an integer then $\mathbb{Z}_N$ is a group under the operation of addition modulo N, namely $a \cdot b = (a + b) \bmod N$.

- The law is written additively.
- The identity element is $\mathbf{id} = 0$, since $\mathbf{id} + a = a + \mathbf{id} = a$ for all $a \in \mathbb{Z}_N$.
- The inverse (of a) with respect to the group law $+$ is $(-a) \bmod N$.

This example is useless for cryptography.

Examples of groups

Fact: If $N \geq 2$ is an integer then $\mathbb{Z}_N^*$ is a group under the operation of multiplication modulo N, namely $a \cdot b = (ab) \bmod N$.

- The identity element is $\mathbf{id} = 1$, since $\mathbf{id} \cdot a = a \cdot \mathbf{id} = a$ for all $a \in \mathbb{Z}_N^*$.
- The inverse (of a) is computed with the EXT-GCD computation, which we will study later.

This example is very important for cryptography.

Examples of groups

Fact: The set of real numbers in $[0, 1)$ is a group under the operation $x \cdot y = x + y - xy$.

- the identity element is 0
- the inverse of x is $\frac{x}{x-1}$.

This example is useless for cryptography.

Examples of groups

Fact: The set of pairs (x, y) of rational numbers such that $x^2 + y^2 = 1$ is a group under the operation:

$$(c_1, s_1) \cdot (c_2, s_2) = (c_1 c_2 - s_1 s_2, c_1 s_2 + c_2 s_1)$$

- the identity element is $\mathbf{id} = (1, 0)$.
- the inverse of (c, s) is $(c, -s)$.

Examples of elements: $(3/5, 4/5)$, or $(5/13, 12/13)$ (Pythagorean triples).

This example (per se) is not useful for cryptography, but the way it is defined is interesting because it connects to elliptic curves.

Some non-examples

Fact: If $N \geq 2$ is an integer then $\mathbb{Z}_N$ is a NOT A GROUP under the operation of multiplication modulo N.

Because:

Some non-examples

Fact: If $N \geq 2$ is an integer then $\mathbb{Z}_N$ is a NOT A GROUP under the operation of multiplication modulo N.

Because:

- The only possible way to define the identity element is $\mathbf{id} = 1$.

Some non-examples

Fact: If $N \geq 2$ is an integer then $\mathbb{Z}_N$ is a NOT A GROUP under the operation of multiplication modulo N.

Because:

- The only possible way to define the identity element is $\mathbf{id} = 1$.
- But $0 \in \mathbb{Z}_N$ and there is no way we can find x such that $0x \equiv 1 \bmod N$.

(note that $\mathbb{Z}_N$ has two distinct operations: addition and multiplication modulo N, and has what we call a ring structure. Not our topic for the moment.)

Some non-examples

What if we take 0 out?

Fact: If $N \geq 4$ is a composite integer then $\mathbb{Z}_N$ is a NOT A GROUP under the operation of multiplication modulo N.

Because:

Some non-examples

What if we take 0 out?

Fact: If $N \geq 4$ is a composite integer then $\mathbb{Z}_N$ is a NOT A GROUP under the operation of multiplication modulo N.

Because:

- The only possible way to define the identity element is $\mathbf{id} = 1$.

Some non-examples

What if we take 0 out?

Fact: If $N \geq 4$ is a composite integer then $\mathbb{Z}_N$ is a NOT A GROUP under the operation of multiplication modulo N.

Because:

- The only possible way to define the identity element is $\mathbf{id} = 1$.
- But if $N = pq$ then $p \in \mathbb{Z}_N$ and there is no way we can find x such that $px \equiv 1 \bmod N$.

This is the reason why when we multiply modulo N, we want to restrict to numbers that are coprime to N.

Plan

Group law, many times

Let G be a group and $a \in G$. Given any integer $n \geq 1$, we have:

$$\underbrace{a \cdot a \cdots a}_{n \text{ times}} \in G$$

(and this element is defined with no ambiguity thanks to associativity).

We can say a few things that follow from the definitions.

- $(\underbrace{a \cdot a \cdots a}_{m \text{ times}}) \cdot (\underbrace{a \cdot a \cdots a}_{n \text{ times}}) = \underbrace{a \cdot a \cdots a}_{m+n \text{ times}}$.
- If b is the inverse of a in G, then $\underbrace{a \cdot a \cdots a}_{n \text{ times}} \cdot \underbrace{b \cdot b \cdots b}_{n \text{ times}} = \mathbf{id}$.
- If $m > n$, $\underbrace{a \cdot a \cdots a}_{m \text{ times}} \cdot \underbrace{b \cdot b \cdots b}_{n \text{ times}} = \underbrace{a \cdot a \cdots a}_{m-n \text{ times}}$.
- If $m < n$, $\underbrace{a \cdot a \cdots a}_{m \text{ times}} \cdot \underbrace{b \cdot b \cdots b}_{n \text{ times}} = \underbrace{b \cdot b \cdots b}_{n-m \text{ times}}$.

We want a notation for $\underbrace{a \cdot a \cdots a}_{n \text{ times}}$, because it's a burden.

Exponentiation

Reminder: the group law $\cdot$ can be $\cdot, +, \perp, \otimes, \uparrow, \$, \ldots$

Exponentiation

Reminder: the group law $\cdot$ can be $\cdot, +, \perp, \otimes, \uparrow, \$, \ldots$

We need a notation for $\underbrace{a \cdot a \cdots a}_{n \text{ times}}$. This is a matter of taste.

- If the group law is $\cdot$, let's write $\underbrace{a \cdot a \cdots a}_{n \text{ times}} = a^n$.
- If the group law is $+$, let's write $\underbrace{a + \cdots + a}_{n \text{ times}} = na$ or $[n]a$.
- If the group law is \$, we don't really know, we're free to choose ($a \mathfrak{S} n$? who cares...).

Exponentiation (or multiplication)

Given the notation that we choose, the pieces fit nicely together.

If the notation is $\cdot$ (multiplication-ish), then we talk about exponentiation.

- We let $a^0 = \textbf{id}$ (and **id** is often denoted 1).
- We let a^{-1} be the inverse of a in G.
- We let $a^{-n} = (a^{-1})^n$.

This ensures that for all $i, j \in \mathbb{Z}$,
- $a^{i+j} = a^i \cdot a^j$
- $a^{ij} = (a^i)^j = (a^j)^i$

Meaning we can manipulate exponents "as usual".

Groups using multiplicative notation

Notations are most often multiplicative: $x \cdot y$ and x^n.
This is also the preferred notation when we speak of an "abstract" group.

Exponentiation (or multiplication)

Given the notation that we choose, the pieces fit nicely together.

If the notation is $+$ (addition-ish), then we talk about multiplication.

- We let $[0]a = \mathbf{id}$ (and $\mathbf{id}$ is often denoted 0).
- We let $[-1]a = -a$ be the inverse of a in G (wrt the group law $+$).
- We let $[-n]a = [n]([-1]a)$.

This ensures that for all $i, j \in \mathbb{Z}$,

- $[i+j]a = [i]a + [j]a$.
- $[ij]a = [i]([j]a)$.

Meaning we can manipulate the multipliers "as usual".

Groups using additive notation

Additive notations are rare, but exist in cryptography (elliptic curves): $P + Q$ and $[n]P$.

Plan

Computational Shortcuts

Fact: Let $a, b, c \in \mathbb{Z}$ and $N \in \mathbb{Z}_+$. Then

$$abc \bmod N = ((ab \bmod N)\, c) \bmod N$$

Example: What is $5 \cdot 8 \cdot 10 \cdot 16 \bmod 21$?

Slow way:

- $5 \cdot 8 \cdot 10 \cdot 16 = 40 \cdot 10 \cdot 16 = 400 \cdot 16 = 6400$
- $6400 \bmod 21 = 16$

Faster way, using above Fact:

- $5 \cdot 8 \bmod 21 = 40 \bmod 21 = 19$
- $19 \cdot 10 \bmod 21 = 190 \bmod 21 = 1$
- $1 \cdot 16 \bmod 21 = 16$

Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo N we have

$$5^3 =$$

Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo N we have

$$5^3 = 5 \cdot 5 \cdot 5$$

Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo N we have

$$5^3 = 5 \cdot 5 \cdot 5 \equiv 25 \cdot 5 \equiv 11 \cdot 5 \equiv 55 \equiv 13$$

and

$$5^{-3} =$$

Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo N we have

$$5^3 = 5 \cdot 5 \cdot 5 \equiv 25 \cdot 5 \equiv 11 \cdot 5 \equiv 55 \equiv 13$$

and

$$5^{-3} = 5^{-1} \cdot 5^{-1} \cdot 5^{-1}$$

Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo N we have

$$5^3 = 5 \cdot 5 \cdot 5 \equiv 25 \cdot 5 \equiv 11 \cdot 5 \equiv 55 \equiv 13$$

and

$$5^{-3} = 5^{-1} \cdot 5^{-1} \cdot 5^{-1} \equiv 3 \cdot 3 \cdot 3$$

Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo N we have

$$5^3 = 5 \cdot 5 \cdot 5 \equiv 25 \cdot 5 \equiv 11 \cdot 5 \equiv 55 \equiv 13$$

and

$$5^{-3} = 5^{-1} \cdot 5^{-1} \cdot 5^{-1} \equiv 3 \cdot 3 \cdot 3 \equiv 27 \equiv 13$$

Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo N we have

$$5^8 = \underbrace{5 \cdot 5 \cdots 5}_{8 \text{ times}}$$

Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo N we have

$$\begin{aligned} 5^8 &= \underbrace{5 \cdot 5 \cdots 5}_{8 \text{ times}} \\ &\equiv \underbrace{(5 \cdot 5) \cdot (5 \cdot 5) \cdots (5 \cdot 5)}_{4 \text{ times}} = (5 \cdot 5)^4 \equiv 11^4 \end{aligned}$$

Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo N we have

$$\begin{aligned}
5^8 &= \underbrace{5 \cdot 5 \cdots 5}_{8 \text{ times}} \\
&\equiv \underbrace{(5 \cdot 5) \cdot (5 \cdot 5) \cdots (5 \cdot 5)}_{4 \text{ times}} = (5 \cdot 5)^4 \equiv 11^4 \\
&\equiv (11 \cdot 11) \cdot (11 \cdot 11) = (11 \cdot 11)^2 \equiv ((-3) \cdot (-3))^2
\end{aligned}$$

Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo N we have

$$
\begin{aligned}
5^8 &= \underbrace{5 \cdot 5 \cdots 5}_{8 \text{ times}} \\
&\equiv \underbrace{(5 \cdot 5) \cdot (5 \cdot 5) \cdots (5 \cdot 5)}_{4 \text{ times}} = (5 \cdot 5)^4 \equiv 11^4 \\
&\equiv (11 \cdot 11) \cdot (11 \cdot 11) = (11 \cdot 11)^2 \equiv ((-3) \cdot (-3))^2 \\
&\equiv 9^2 \equiv (-5)^2 \equiv 25 \equiv 11.
\end{aligned}
$$

So $5^8 \equiv 11 \pmod{14}$. Note that we also have $5^2 \equiv 11 \pmod{14}$.

Group Orders

The order of a group G is its size $|G|$, meaning the number of elements in it.

Example: The order of $\mathbb{Z}_{14}^*$ is

Group Orders

The order of a group G is its size $|G|$, meaning the number of elements in it.

Example: The order of $\mathbb{Z}_{14}^*$ is 6 because

$$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$$

Fact: Let G be a group of order m and $a \in G$. Then, $a^m = \mathbf{id}$.

Example: Modulo 14 we have

- $5^6 \equiv (5^2)^3 \equiv (-3)^3 \equiv -27 \equiv 1$ (all of this $\pmod{14}$)
- $9^6 \equiv (9^3)^2 \equiv 729^2 \equiv (1)^2 \equiv 1$ (all of this $\pmod{14}$)

Simplifying exponentiation

Fact: Let G be a group of order m and $a \in G$. Then, $a^m = \mathbf{id}$.

Corollary: Let G be a group of order m and $a \in G$. Then for any $i \in \mathbb{Z}$,

$$a^i = a^{i \bmod m}.$$

Proof: Let $(q, r) \leftarrow \text{INT-DIV}(i, m)$, so that $i = mq + r$ and $r = i \bmod m$. Then

$$a^i = a^{mq+r} = (a^m)^q \cdot a^r$$

But $a^m = \mathbf{id}$ by Fact.

Simplifying exponentiation

Corollary: Let G be a group of order m and $a \in G$. Then for any $i \in \mathbb{Z}$,

$$a^i = a^{i \bmod m}.$$

Example: What is $5^8 \bmod 14$?

Simplifying exponentiation

Corollary: Let G be a group of order m and $a \in G$. Then for any $i \in \mathbb{Z}$,

$$a^i = a^{i \bmod m}.$$

Example: What is $5^8 \bmod 14$?

Solution: Let $G = \mathbb{Z}_{14}^*$ and $a = 5$. Then, $m = |\mathbb{Z}_{14}^*| = 6$, so

$$\begin{aligned} 5^8 \bmod 14 &= 5^{8 \bmod 6} \bmod 14 \\ &= 5^2 \bmod 14 \\ &= 11. \end{aligned}$$

Simplifying exponentiation

Corollary: Let G be a group of order m and $a \in G$. Then for any $i \in \mathbb{Z}$,

$$a^i = a^{i \bmod m}.$$

Example: What is $5^{74} \bmod 21$?

Simplifying exponentiation

Corollary: Let G be a group of order m and $a \in G$. Then for any $i \in \mathbb{Z}$,

$$a^i = a^{i \bmod m}.$$

Example: What is $5^{74} \bmod 21$?

Solution: Let $G = \mathbb{Z}_{21}^*$ and $a = 5$. We have

$$\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 10\}$$

Thereferore, $m = |\mathbb{Z}_{21}^*| = 12$, so

$$\begin{aligned} 5^{74} \bmod 21 &= 5^{74 \bmod 12} \bmod 21 \\ &= 5^2 \bmod 21 \\ &= 4. \end{aligned}$$

Do not simplify too hastily!

Say you are working modulo $N = 762$. Pro tip: $|\mathbb{Z}^*_{762}| = 252$

What is $17^{20220428} \mod 762$?

- You certainly don't want to compute the integer $17^{20220428}$ (which has about 80 million bits).
- You want to reduce the exponent.

The correct way

- $|\mathbb{Z}^*_{762}| = 252$
- Reduce the exponent $\bmod 252$.
- $20220428 \mod 252 = 200$.

$$\begin{aligned} 17^{20220428} &\equiv 17^{200} \\ &\equiv (((((17)^2)^2)^2)^5)^5. \end{aligned}$$

The wrong way

- You don't understand the distinction between N and $|\mathbb{Z}^*_N|$.
- Reducing $\bmod 762$ is fine when doing $+$ or $\cdot$,
- but WRONG for exponents!

$17^{20220428} \bmod 762$

Reduce the **exponent** modulo $|\mathbb{Z}^*_{762}| = 252$

$$17^{20220428} \equiv 17^{200}$$
$$\equiv ((((17^2)^2)^2)^5)^5$$

$17^{20220428} \bmod 762$

Reduce the **exponent** modulo $|\mathbb{Z}^*_{762}| = 252$

$$17^{20220428} \equiv 17^{200}$$
$$\equiv ((((17^2)^2)^2)^5)^5$$
$$\equiv (((289^2)^2)^5)^5$$

Here we can reduce modulo 762

$17^{20220428} \bmod 762$

Reduce the **exponent** modulo $|\mathbb{Z}^*_{762}| = 252$

$$
\begin{aligned}
17^{20220428} &\equiv 17^{200} \\
&\equiv ((((17^2)^2)^2)^5)^5 \\
&\equiv (((289^2)^2)^5)^5 \\
&\equiv ((463^2)^5)^5
\end{aligned}
$$

Because
$289 \times 289 \equiv 463 \pmod{762}$

$17^{20220428} \bmod 762$

Reduce the **exponent** modulo $|\mathbb{Z}^*_{762}| = 252$

$$
\begin{aligned}
17^{20220428} &\equiv 17^{200} \\
&\equiv ((((17^2)^2)^2)^5)^5 \\
&\equiv (((289^2)^2)^5)^5 \\
&\equiv ((463^2)^5)^5 \\
&\equiv \ldots \\
&\equiv 661 \pmod{762}.
\end{aligned}
$$

CSE107: Intro to Modern Cryptography

https://cseweb.ucsd.edu/classes/sp22/cse107-a/

Emmanuel Thomé

May 3, 2022

Lecture 9b

Computational Number Theory (end of previous lecture)

Algorithms on numbers

Plan

Algorithms on numbers

Measuring Running Time of Algorithms on Numbers

In an algorithms course, the cost of arithmetic is often assumed to be $\mathcal{O}(1)$, because numbers are small. In cryptography numbers are

very, very BIG!

Typical numbers are 2^{512}, 2^{1024}, 2^{2048}: hundreds or thousands of bits.

Numbers are provided to algorithms in binary. The length of a, denoted $|a|$, is the number of bits in the binary encoding of a.

Example: $|7| = 3$ because 7 is 111 in binary.

Running time is measured as a function of the lengths of the inputs.

Algorithms on numbers

The straightforward algorithms have the following complexities:

Algorithm	Input	Output	Time
ADD	$a,\ b$	$a + b$	$\mathcal{O}(\lvert a\rvert + \lvert b\rvert)$
MULT	$a,\ b$	ab	$\mathcal{O}(\lvert a\rvert \cdot \lvert b\rvert)$
INT-DIV	$a,\ N$	q,r	$\mathcal{O}(\lvert a\rvert \cdot \lvert N\rvert)$
MOD	$a,\ N$	$a \bmod N$	$\mathcal{O}(\lvert a\rvert \cdot \lvert N\rvert)$
EXT-GCD	$a,\ N$	(d, a', N')	$\mathcal{O}(\lvert a\rvert \cdot \lvert N\rvert)$
MOD-INV	$a \in \mathbb{Z}_N^*,\ N$	$a^{-1} \bmod N$	$\mathcal{O}(\lvert N\rvert^2)$
MOD-EXP	$a \in \mathbb{Z}_N,\ n,\ N$	$a^n \bmod N$	$\mathcal{O}(\lvert n\rvert \cdot \lvert N\rvert^2)$
EXP_G	$a \in G,\ n$	$a^n \in G$	$\mathcal{O}(\lvert n\rvert)$ G-ops

Plan

Algorithms on numbers

- (Extended) gcd
- Exponentiation

Extended gcd

Definition (EXT-GCD)

EXT-GCD(a, N) returns (r, u, v) such that

$$r = \gcd(a, N) = a \cdot u + N \cdot v \ .$$

Example: EXT-GCD$(12, 20) =$

Extended gcd

Definition (EXT-GCD)

EXT-GCD(a, N) returns (r, u, v) such that

$$r = \text{gcd}(a, N) = a \cdot u + N \cdot v \ .$$

Example: EXT-GCD$(12, 20) = (4, 2, -1)$ because

$$4 = \text{gcd}(12, 20) = 12 \cdot 2 + 20 \cdot (-1) \ .$$

The (extended) Euclidean algorithm

Algorithm for gcd

To compute the (extended) gcd, we use the (extended) Euclidean algorithm.

Extended gcd Algorithm: rough idea

Definition (EXT-GCD)

EXT-GCD(a, N) returns (r, u, v) such that

$$r = \gcd(a, N) = a \cdot u + N \cdot v \ .$$

Lemma

Let $(q, r) = \text{INT-DIV}(a, N)$*. Then,* $\gcd(a, N) = \gcd(N, r)$

We use this lemma repeatedly.

Extended gcd Algorithm: code

Alg EXT-GCD(a, N) // $(a, N) \neq (0, 0)$
$(r_0, u_0, v_0) \leftarrow (N, 0, 1)$ // $u_0 a + v_0 N = r_0$
$(r_1, u_1, v_1) \leftarrow (a, 1, 0)$ // $u_1 a + v_1 N = r_1$
while $r_1 \neq 0$
  $(q, r_2) \leftarrow$ INT-DIV(r_0, r_1); // $r_0 - q r_1 = r_2$
  $u_2 = u_0 - q u_1$
  $v_2 = v_0 - q v_1$ // now $u_2 a + v_2 N = r_2$
  $(r_0, u_0, v_0) \leftarrow (r_1, u_1, v_1)$
  $(r_1, u_1, v_1) \leftarrow (r_2, u_2, v_2)$
return (r_0, u_0, v_0) // $u_0 a + v_0 N = r_0 = \gcd(a, N)$

Running time is $\mathcal{O}(|a| \cdot |N|)$, so the extended gcd can be computed in quadratic time. If $0 < a < N$ then $\mathrm{abs}(u) \leq N$ and $\mathrm{abs}(v) \leq a$ where $\mathrm{abs}(\cdot)$ denotes the absolute value.

Analysis showing all this is non-trivial (worst case is Fibonacci numbers).

Modular Inverse

For a, N such that $\gcd(a, N) = 1$, we want to compute $a^{-1} \bmod N$, meaning the unique $a' \in \mathbb{Z}_N^*$ satisfying $aa' \equiv 1 \pmod{N}$.

But if we let $(d, a', N') \leftarrow \text{EXT-GCD}(a, N)$ then

$$d = 1 = \gcd(a, N) = a \cdot a' + N \cdot N'$$

But $N \cdot N' \equiv 0 \pmod{N}$ so $aa' \equiv 1 \pmod{N}$

Alg MOD-INV(a, N)
$(d, a', N') \leftarrow \text{EXT-GCD}(a, N)$
$\text{return } a' \bmod N$

Modular inverse can be computed in quadratic time.

Plan

Algorithms on numbers

- (Extended) gcd
- Exponentiation

Modular Exponentiation

Let G be a group and $a \in G$. For $n \in \mathbb{N}$, we want to compute $a^n \in G$.

We know that

$$a^n = \underbrace{a \cdot a \cdots a}_{n}$$

Consider:

$y \leftarrow 1$
for $i = 1, \ldots, n$ do $y \leftarrow y \cdot a$
return y

Question: Is this a good algorithm?

Modular Exponentiation

Let G be a group and $a \in G$. For $n \in \mathbb{N}$, we want to compute $a^n \in G$.

We know that

$$a^n = \underbrace{a \cdot a \cdots a}_{n}$$

Consider:

$y \leftarrow 1$
for $i = 1, \ldots, n$ do $y \leftarrow y \cdot a$
return y

Question: Is this a good algorithm?

Answer: It is correct but VERY SLOW. The number of group operations is $\mathcal{O}(n) = \mathcal{O}(2^{|n|})$ so it is exponential time. For $n \approx 2^{512}$ it is prohibitively expensive.

Fast exponentiation idea

We can compute

$$a \longrightarrow a^2 \longrightarrow a^4 \longrightarrow a^8 \longrightarrow a^{16} \longrightarrow a^{32}$$

in just 5 steps by repeated squaring. So we can compute a^n in i steps when $n = 2^i$.

But what if n is not a power of 2?

Square-and-Multiply Exponentiation Example

Suppose the binary length of n is 5, meaning the binary representation of n has the form $b_4 b_3 b_2 b_1 b_0$. (We sometimes write $n = (b_4 b_3 b_2 b_1 b_0)_2$.)

Then

$$\begin{aligned} n &= 2^4 b_4 + 2^3 b_3 + 2^2 b_2 + 2^1 b_1 + 2^0 b_0 \\ &= 16 b_4 + 8 b_3 + 4 b_2 + 2 b_1 + b_0 \ . \end{aligned}$$

We want to compute a^n. Our exponentiation algorithm will proceed to compute the values $y_5, y_4, y_3, y_2, y_1, y_0$ in turn, as follows:

$$\begin{aligned} y_5 &= \mathbf{id} \\ y_4 &= y_5^2 \cdot a^{b_4} &&= a^{b_4} \\ y_3 &= y_4^2 \cdot a^{b_3} &&= a^{2b_4+b_3} \\ y_2 &= y_3^2 \cdot a^{b_2} &&= a^{4b_4+2b_3+b_2} \\ y_1 &= y_2^2 \cdot a^{b_1} &&= a^{8b_4+4b_3+2b_2+b_1} \\ y_0 &= y_1^2 \cdot a^{b_0} &&= a^{16b_4+8b_3+4b_2+2b_1+b_0} \ . \end{aligned}$$

Square-and-Multiply Exponentiation Example

Let $N = 131$, $G = \mathbb{Z}_N^*$, and $a = 2 \in \mathbb{Z}_N^*$.
We want to compute $a^{107} \bmod N$.

We start with $107 = 64 + 32 + 0 + 8 + 0 + 2 + 1 = (1101011)_2$.

$(1101011)_2 \qquad y \leftarrow a = 2,$

Square-and-Multiply Exponentiation Example

Let $N = 131$, $G = \mathbb{Z}_N^*$, and $a = 2 \in \mathbb{Z}_N^*$.
We want to compute $a^{107} \bmod N$.

We start with $107 = 64 + 32 + 0 + 8 + 0 + 2 + 1 = (1101011)_2$.

$$(1101011)_2 \qquad y \leftarrow a = 2,$$
$$(1101011)_2 \qquad y \leftarrow y^2 a = a^3 = 8,$$

Square-and-Multiply Exponentiation Example

Let $N = 131$, $G = \mathbb{Z}_N^*$, and $a = 2 \in \mathbb{Z}_N^*$.
We want to compute $a^{107} \bmod N$.

We start with $107 = 64 + 32 + 0 + 8 + 0 + 2 + 1 = (1101011)_2$.

$$
\begin{aligned}
&(1101011)_2 & y &\leftarrow a = 2, \\
&(1101011)_2 & y &\leftarrow y^2 a = a^3 = 8, \\
&(1101011)_2 & y &\leftarrow y^2 = a^6 = 64,
\end{aligned}
$$

Square-and-Multiply Exponentiation Example

Let $N = 131$, $G = \mathbb{Z}_N^*$, and $a = 2 \in \mathbb{Z}_N^*$.
We want to compute $a^{107} \bmod N$.

We start with $107 = 64 + 32 + 0 + 8 + 0 + 2 + 1 = (1101011)_2$.

$$
\begin{aligned}
(1101011)_2 & \quad y \leftarrow a = 2, \\
(1101011)_2 & \quad y \leftarrow y^2 a = a^3 = 8, \\
(1101011)_2 & \quad y \leftarrow y^2 = a^6 = 64, \\
(1101011)_2 & \quad y \leftarrow y^2 a = a^{13} = 8192 \equiv 70,
\end{aligned}
$$

Square-and-Multiply Exponentiation Example

Let $N = 131$, $G = \mathbb{Z}_N^*$, and $a = 2 \in \mathbb{Z}_N^*$.
We want to compute $a^{107} \bmod N$.

We start with $107 = 64 + 32 + 0 + 8 + 0 + 2 + 1 = (1101011)_2$.

$$
\begin{array}{ll}
(1101011)_2 & y \leftarrow a = 2, \\
(1101011)_2 & y \leftarrow y^2 a = a^3 = 8, \\
(1101011)_2 & y \leftarrow y^2 = a^6 = 64, \\
(1101011)_2 & y \leftarrow y^2 a = a^{13} = 8192 \equiv 70, \\
(1101011)_2 & y \leftarrow y^2 = a^{26} \equiv 53,
\end{array}
$$

Square-and-Multiply Exponentiation Example

Let $N = 131$, $G = \mathbb{Z}_N^*$, and $a = 2 \in \mathbb{Z}_N^*$.
We want to compute $a^{107} \bmod N$.

We start with $107 = 64 + 32 + 0 + 8 + 0 + 2 + 1 = (1101011)_2$.

$$
\begin{array}{lc}
(1101011)_2 & y \leftarrow a = 2, \\
(1101011)_2 & y \leftarrow y^2 a = a^3 = 8, \\
(1101011)_2 & y \leftarrow y^2 = a^6 = 64, \\
(1101011)_2 & y \leftarrow y^2 a = a^{13} = 8192 \equiv 70, \\
(1101011)_2 & y \leftarrow y^2 = a^{26} \equiv 53, \\
(1101011)_2 & y \leftarrow y^2 a = a^{53} \equiv 116,
\end{array}
$$

Square-and-Multiply Exponentiation Example

Let $N = 131$, $G = \mathbb{Z}_N^*$, and $a = 2 \in \mathbb{Z}_N^*$.
We want to compute $a^{107} \bmod N$.

We start with $107 = 64 + 32 + 0 + 8 + 0 + 2 + 1 = (1101011)_2$.

$$
\begin{array}{lc}
(1101011)_2 & y \leftarrow a = 2, \\
(1101011)_2 & y \leftarrow y^2 a = a^3 = 8, \\
(1101011)_2 & y \leftarrow y^2 = a^6 = 64, \\
(1101011)_2 & y \leftarrow y^2 a = a^{13} = 8192 \equiv 70, \\
(1101011)_2 & y \leftarrow y^2 = a^{26} \equiv 53, \\
(1101011)_2 & y \leftarrow y^2 a = a^{53} \equiv 116, \\
(1101011)_2 & y \leftarrow y^2 a = a^{107} \equiv 57,
\end{array}
$$

So $2^{107} \equiv 57 \pmod{131}$.

Square-and-Multiply Exponentiation Algorithm

Let $\text{bin}(n) = b_{k-1} \ldots b_0$ be the binary representation of n, meaning

$$n = \sum_{i=0}^{k-1} b_i 2^i$$

Alg $\text{EXP}_G(a, n)$ $\quad$ // $a \in G$, $n \geq 1$
$b_{k-1} \ldots b_0 \leftarrow \text{bin}(n)$
$y \leftarrow 1$
for $i = k - 1$ downto 0 do $y \leftarrow y^2 \cdot a^{b_i}$
return y

The running time is $\mathcal{O}(|n|)$ group operations.

$\text{MOD-EXP}(a, n, N)$ returns $a^n \bmod N$ in time $\mathcal{O}(|n| \cdot |N|^2)$, meaning is cubic time.

Variants of Square-and-Multiply

There are many variants of the Square-and-Multiply algorithm.

- Left-to-Right (a.k.a. most significant bit first), as we presented.
- Right-to-Left.
- Fixed-window.
- Sliding-window.
- And more.

Algorithms on numbers

Algorithm	Input	Output	Time
ADD	$a,\ b$	$a+b$	$\mathcal{O}(\|a\|+\|b\|)$
MULT	$a,\ b$	ab	$\mathcal{O}(\|a\|\cdot\|b\|)$
INT-DIV	$a,\ N$	q, r	$\mathcal{O}(\|a\|\cdot\|N\|)$
MOD	$a,\ N$	$a \bmod N$	$\mathcal{O}(\|a\|\cdot\|N\|)$
EXT-GCD	$a,\ N$	(d, a', N')	$\mathcal{O}(\|a\|\cdot\|N\|)$
MOD-INV	$a \in \mathbb{Z}_N^*,\ N$	$a^{-1} \bmod N$	$\mathcal{O}(\|N\|^2)$
MOD-EXP	$a \in \mathbb{Z}_N,\ n,\ N$	$a^n \bmod N$	$\mathcal{O}(\|n\|\cdot\|N\|^2)$
EXP_G	$a \in G,\ n$	$a^n \in G$	$\mathcal{O}(\|n\|)$ G-ops