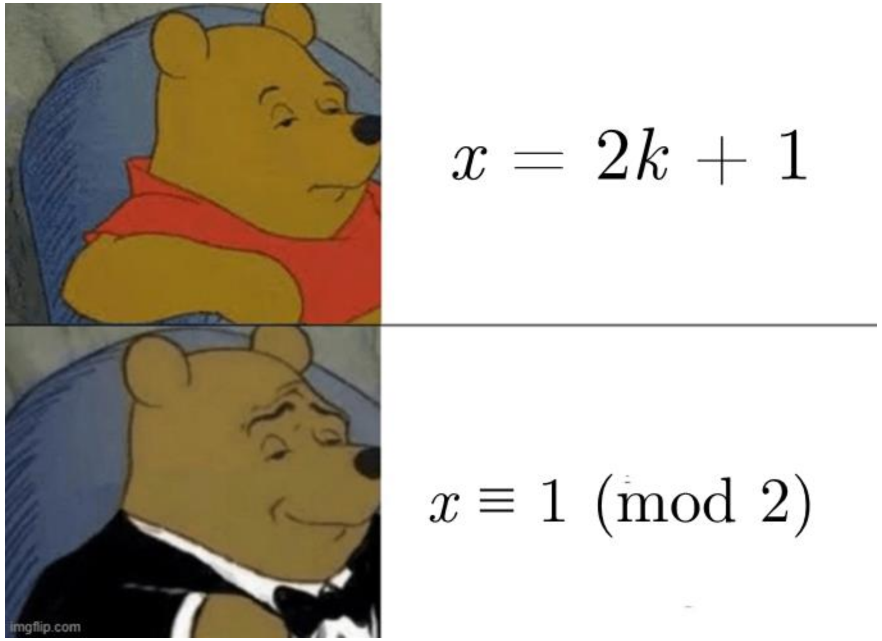
D11: Fingerprinting & Modular Arithmetic Review



Sec 101: MW 3:00-4:00pm DOW 1018
IA: Eric Khiu

Fingerprinting

Setup

- Suppose Alice wants to communicate some large n-bits number x to Bob
- She wants to send as few bits as possible, so instead she uploads this number to a server for him to download
- The server is untrusted, so once Bob downloads the number y, he and Alice will need to confirm that x and y are the same

Randomized Fingerprinting

- Alice randomly chooses a prime p from the first $10n$ primes and sends Bob the message $(p, x \bmod p)$
- Bob computes $y \bmod p$
  - If $x \bmod p = y \bmod \mathrm{p}$, Bob concludes that $x = y$
  - Otherwise, Bob concludes that $x \neq y$
- When $x = y$, this protocol is correct for all choices of p
- When $x \neq y$, this protocol is correct for at least 90% of the choices of p
  - Example: $p = 3$; $x = 1, y \in \{7,10,13, \ldots\}$ breaks the protocol

Randomized Fingerprinting Exercise

- Alice randomly chooses a prime p from the first $10n$ primes and sends Bob the message $(p, x \bmod p)$
- Bob computes $y \bmod p$
  - If $x \bmod p = y \bmod p$, Bob concludes that $x = y$
  - Otherwise, Bob concludes that $x \neq y$
- State whether the algorithm is correct for all choices of p, or give all examples of p that cause the protocol to result in the incorrect decision
  - $x = 70, y = 64$
  - $x = 342, y = 342$

  Hint: If $x \bmod p = y \bmod p$, what is $(x - y) \bmod p$?

Randomized Fingerprinting Exercise

- Recall that a and b are congruent modulo n, written as $a \equiv b (\mathrm{mod}\ n)$ if
  - $a \bmod n = b \bmod \mathrm{n}$, or equivalently,
  - $\exists k \in \mathbb{Z}$ such that $a = b + kn$, or equivalently
  - $a - b$ is a multiple of n
- So if $x \bmod p = y \bmod p$, then $(x - y) \bmod p = 0$
- This means we just need to find the prime divisors of $x - y$
- State whether the algorithm is correct for all choices of p, or give all examples of p that cause the protocol to result in the incorrect decision
  - $x = 70, y = 64$
  - $x = 342, y = 342$

Modular Arithmetic Review

Notes

Modular Arithmetic Review

- Let a, b, n be integers
- **Definition:** $a \bmod n$ is the remainder of a when divided by n
  - $a \bmod n$ is a unique value in $\mathbb{Z}_n = \{0, \ldots, n-1\}$
- **Definition:** a and b are congruent modulo n, written as $a \equiv b (\text{mod } n)$ if
  - $a \bmod n = b \bmod \mathrm{n}$, or equivalently,
  - $\exists k \in \mathbb{Z}$ such that $a = b + kn$, or equivalently
  - $a - b$ is a multiple of n
- **Modular Arithmetic:** Suppose $a \equiv b (\text{mod } n)$, $c \in \mathbb{Z}$
  - Addition: $a + c \equiv b + c \pmod n$
  - Multiplication: $ac \equiv bc \pmod n$

Division in $\mathbb{Z}_n$

- **Definition:** Let $a \in \mathbb{Z}$. $a^{-1} \in \mathbb{Z}$ is a multiplicative inverse of a in modulo n such that
$$a^{-1} \cdot a \equiv 1 \pmod{n}$$
  - Note: We typically standardize a^{-1} to be in $\mathbb{Z}_n$
- In modular arithmetic, dividing by a is the same as multiplying by a^{-1}
- WARNING: Division is not always possible, as a does not always have an inverse
  - For example: 2 has no inverse in $\mathbb{Z}_4 = \{0,1,2,3\}$
$$0 \cdot 2 \equiv 2 \cdot 2 \equiv 0 \pmod{4}, 1 \cdot 2 \equiv 3 \cdot 2 \equiv 2 \pmod{4}$$
- **Theorem:** An integer a has a multiplication inverse in mod n iff $\gcd(a, n) = 1$
  - **Corollary:** For all $a \neq 0 \in \mathbb{Z}_p$, where p is prime, there is a multiplicative inverse of a in modulo p. -This is key in cryptography!

Finding Multiplicative Inverse: Intuition

- Suppose we want to find multiplicative inverse of 4 in mod 7
  - By inspection, $\gcd(4,7) = 1$, so 4 has multiplicative inverse in mod 7
- By definition, we want some $b \in \mathbb{Z}$ such that
$$4b \equiv 1 \pmod 7$$
- By definition of modular congruence, $\exists k \in \mathbb{Z}$ such that
$$4b = 1 + 7k$$
- Rearranging,
$$4b - 7k = 1 = \gcd(4,7)$$
- **Obs:** b and k are coefficients of 4 and 7 in the linear combination of their gcd
- We have seen this in **Extended Euclid Algorithm**!

Extended Euclid Algorithm

- Example: Find the multiplicative inverse of 4 in mod 7

```
function EXTENDEDEUCLID(x, y)
    if y = 0 then
        return (x, 1, 0)
    else
        Write x = qy + r for an integer q, where 0 ≤ r < y
        (g, a', b') ← EXTENDEDEUCLID(y, r)
        a ← b'
        b ← a' − b'q
        return (g, a, b)
```

x	y	q	r	g	$a \leftarrow b'$	$b \leftarrow a' - b'q$
7	4	1	3			

Extended Euclid Algorithm

function ExtendedEuclid(x, y)
  if $y = 0$ **then**
    return $(x, 1, 0)$
  else
    Write $x = qy + r$ for an integer q, where $0 \leq r < y$
    $(g, a', b') \leftarrow$ ExtendedEuclid(y, r)
    $a \leftarrow b'$
    $b \leftarrow a' - b'q$
    return (g, a, b)

- Example: Find the multiplicative inverse of 4 in mod 7

x	y	q	r	g	$a \leftarrow b'$	$b \leftarrow a' - b'q$
7	4	1	3			
4	3	1	1			
3	1	3	0			
1	0	-	-			

Extended Euclid Algorithm

function EXTENDEDEUCLID(x, y)
  if $y = 0$ **then**
    return $(x, 1, 0)$
  else
    Write $x = qy + r$ for an integer q, where $0 \le r < y$
    $(g, a', b') \leftarrow$ EXTENDEDEUCLID(y, r)
    $a \leftarrow b'$
    $b \leftarrow a' - b'q$
    return (g, a, b)

- Example: Find the multiplicative inverse of 4 in mod 7

x	y	q	r	g	$a \leftarrow b'$	$b \leftarrow a' - b'q$
7	4	1	3	1	-1	1-(-1)(1)=2
4	3	1	1	1	1	0-1(1)=-1
3	1	3	0	1	0	1-0(3)=1
1	0	-	-	1	1	0

- Observe that $4(2) - 7(-1) = 15 \equiv 1 (\text{mod } 7)$
- In fact, $4^{-1} \bmod 7 = 2$
  - Check $2 \cdot 4 = 8 \equiv 1 \ (\text{mod } 7)$

Exercise

- Find $13^{-1} \bmod 21$

```
function ExtendedEuclid(x, y)
    if y = 0 then
        return (x, 1, 0)
    else
        Write x = qy + r for an integer q, where 0 ≤ r < y
        (g, a', b') ← ExtendedEuclid(y, r)
        a ← b'
        b ← a' − b'q
        return (g, a, b)
```

x	y	$q \leftarrow \lfloor x/y \rfloor$	$r \leftarrow x/y - q$	g	$a \leftarrow b'$	$b \leftarrow a' - b'q$
21	13					

Exercise

- Find $13^{-1} \bmod 21$

```
function ExtendedEuclid(x, y)
    if y = 0 then
        return (x, 1, 0)
    else
        Write x = qy + r for an integer q, where 0 ≤ r < y
        (g, a', b') ← ExtendedEuclid(y, r)
        a ← b'
        b ← a' − b'q
        return (g, a, b)
```

$-8 \bmod 21 = 13$

x	y	$q \leftarrow \lfloor x/y \rfloor$	$r \leftarrow x/y - q$	g	$a \leftarrow b'$	$b \leftarrow a' - b'q$
21	13	1	8	1	5	-3-5(1)=-8
13	8	1	5	1	-3	2-(-3)(1)=5
8	5	1	3	1	2	-1-(2)(1)=-3
5	3	1	2	1	-1	1-(-1)(1)=2
3	2	1	1	1	1	0-1(1)=-1
2	1	2	0	1	0	1-0(2)=1
1	0	-	-	1	1	0

Fast Modular Exponentiation

Notes

Exponentiation in Modular Arithmetic

- Recall that if $a \equiv b (\mathrm{mod}\ n)$, then for any $k \in \mathbb{Z}$,
  - $a + k \equiv b + k \pmod{n}$
  - $ak \equiv bk \pmod{n}$
- **Property 215:** Suppose $a = a' (\mathrm{mod}\ n)$ and $b = b' (\mathrm{mod}\ n)$, then
$$ab \equiv a'b' \pmod{n}$$
  - Proof idea: Let $a - a' = kn$ and $b - b' = mn$ for some integers k and m, then
$$ab = (kn + a') \cdot (mn + b') = \cdots = (kmn + a'm + b'k)n + a'b'$$
  - Therefore, $ab - a'b' = (kmn + a'm + b'k)n$, so $ab \equiv a'b' \pmod{n}$
- **Corollary:** If $a \equiv b (\mathrm{mod}\ n)$, then $a^k \equiv b^k \pmod{n}$
  - Proof idea: $a^k = \underbrace{a \cdot a \cdot \ldots \cdot a}_{k \text{ times}}$, use property 215 and induction

Property 215: Suppose $a = a'(\bmod n)$ and $b = b'(\bmod n)$, then

$$ab \equiv a'b' \pmod n$$

Fast Modular Exponentiation

- Suppose we want to compute $a^b \bmod n$
- Consider the binary representation of b

$$b = b_r \cdot 2^r + b_{r-1} \cdot 2^{r-1} + \cdots + b_0 \cdot 2^0$$

  - Here, b_i is either 0 or 1
  - $r = \lfloor \log_2 b \rfloor$
- Then, we can represent a^b as

$$\begin{aligned} a^b &= a^{b_r \cdot 2^r + b_{r-1} \cdot 2^{r-1} + \cdots + b_0 \cdot 2^0} \\ &= a^{b_r \cdot 2^r} \times a^{b_{r-1} \cdot 2^{r-1}} \times \cdots \times a^{b_0 \cdot 2^{r-1}} \end{aligned}$$

- Thus, we can compute $a^{2^i} \bmod n$ for each $a \leq i \leq r$ and include those whose $b_i = 1$ in the product

Fast Modular Exponentiation

Property 215: Suppose $a = a' (\mathrm{mod}\ n)$ and $b = b' (\mathrm{mod}\ n)$, then

$$ab \equiv a'b' \ (\mathrm{mod}\ n)$$

14 × 1	=	14
14 × 2	=	28
14 × 3	=	42
14 × 4	=	56
14 × 5	=	70
14 × 6	=	84
14 × 7	=	98
14 × 8	=	112
14 × 9	=	126
14 × 10	=	140

- Example: $3^5 \bmod 14$
- Step 1: Express $b = 5$ in binary

$$5 = 101$$

- Step 2: Compute $3^{2^i} \bmod 14$ for $i = 0 \leq i \leq \lfloor \log_2 5 \rfloor = 2$

$$3^{2^0} = 3^1 = 3 \equiv 3 \ (\mathrm{mod}\ 14)$$
$$3^{2^1} = 3^2 = 9 \equiv 9 \ (\mathrm{mod}\ 14)$$
$$3^{2^2} = 9^2 = 81 \equiv 11 \ (\mathrm{mod}\ 14)$$

- Step 3: Multiply and simplify

$$\begin{aligned} 3^5 &= 3^4 \cdot 3^1 \\ &\equiv 11 \cdot 3 \ (\mathrm{mod}\ 14) \\ &\equiv 33 \ (\mathrm{mod}\ 14) \\ &\equiv 5 \ (\mathrm{mod}\ 14) \end{aligned}$$

Your turn: Compute $3^{57} \bmod 14$

Ans: 13

Fast Modular Exponentiation Algorithm

- **(Take home) exercise:** Complete the following DP algorithm for fast modular exponentiation and analyze the runtime:

```
FastModExp(a, b, n):
    r ← ⌊log b⌋
    allocate an empty array DP[0, …, r]
    DP[0] ← a
    for i = 1, …, r do
        [                              ]
    ans ← 1
    for i = 0, …, r do
        if [        ] then
            [                          ]
    return ans
```

See Algorithm 220 on course notes for solution

Congruent Class and Generator

Notes

Congruent class

- **Congruent class:** For any $n \in \mathbb{N}$, we define $\mathbb{Z}_n = \{0,1,2,\dots,n-1\}$ as the set of congruence class modulo n.

- The group $\mathbb{Z}_n^* \subseteq \mathbb{Z}_n$ is the set of nonzero elements of $\mathbb{Z}_n$ that have an inverse in modulo n, i.e.,
$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : \gcd(x,n) = 1\}$$

  - A prime number is coprime to all natural numbers smaller than it

Discuss: What if n is prime?

Generator

- **Generator:** Let p be a prime. $g \in \mathbb{Z}_p^*$ is a *generator* if for every $x \in \mathbb{Z}_p^*$, there exists some $i \in \mathbb{N}$ such that $x = g^i \bmod p$

- Example: $g = 2$ is a generator of $\mathbb{Z}_5^*$:
  - $\mathbb{Z}_5^* = \{1,2,3,4\}$
  - $2^0 = 1 \equiv 1 \pmod 5$
  - $2^1 = 2 \equiv 2 \pmod 5$
  - $2^2 = 4 \equiv 4 \pmod 5$
  - $2^3 = 8 \equiv 3 \pmod 5$

- But $g = 2$ is a not generator of $\mathbb{Z}_7^*$:
  - $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$
  - $2^0 = 1 \equiv 1 \pmod 7$
  - $2^1 = 2 \equiv 2 \pmod 7$
  - $2^2 = 4 \equiv 4 \pmod 7$
  - $2^3 = 8 \equiv 1 \pmod 7$
  - $2^4 = 16 \equiv 2 \pmod 7$
  - …

Generator: Let p be a prime. $g \in \mathbb{Z}_p^*$ is a *generator* if for every $x \in \mathbb{Z}_p^*$, there exists some $i \in \mathbb{N}$ such that $x = g^i \bmod p$

Concept Check

- Is $g = 3$ a generator of $\mathbb{Z}_{11}^*$?
  - $\mathbb{Z}_{11}^* = \{1,2, \dots, 10\}$
  - $3^0 = 1 \equiv 1 \pmod{11}$
  - $3^1 = 3 \equiv 3 \pmod{11}$
  - $3^2 = 9 \equiv 9 \pmod{11}$
  - $3^3 = 27 \equiv 5 \pmod{11}$
  - $3^4 = 81 \equiv 4 \pmod{11}$
  - $3^5 = 3 \cdot 3^4 \equiv 3 \cdot 4 = 12 \equiv 1 \pmod{11}$
  - …

11	x	1	=	11
11	x	2	=	22
11	x	3	=	33
11	x	4	=	44
11	x	5	=	55
11	x	6	=	66
11	x	7	=	77
11	x	8	=	88
11	x	9	=	99
11	x	10	=	110

Another Definition of Generator

- We had the following definition for a generator:
  - Let p be a prime. $g \in \mathbb{Z}_p^*$ is a *generator* if for every $x \in \mathbb{Z}_p^*$, there exists some $i \in \mathbb{N}$ such that $x = g^i \bmod p$
- The following definition is equivalent:
  - Let p be a prime. $g \in \mathbb{Z}_p^*$ is a *generator* if for every $x \in \mathbb{Z}_p^*$, there exists some $y \in \{0, \dots, p-2\}$ such that $x = g^y \bmod p$
  - So instead of defining congruent class of a prime number as
$$\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p : \gcd(x, n) = 1\} = \{1, 2, \dots, p-1\}$$
  - The following definition is equivalent:
$$\mathbb{Z}_p^* = \{g^y \bmod p : y \in \{0, 1, \dots, p-2\}\}$$
- **Main takeaway:** g generates $\mathbb{Z}_p^*$ iff $g^0 \bmod p$ through $g^{p-2} \bmod p$ hit all elements of $\mathbb{Z}_p^*$ (exactly once)