Lecture 4: Modular Exponentiation

Lecture 4

Objectives

By the end of this lecture you should be able to understand

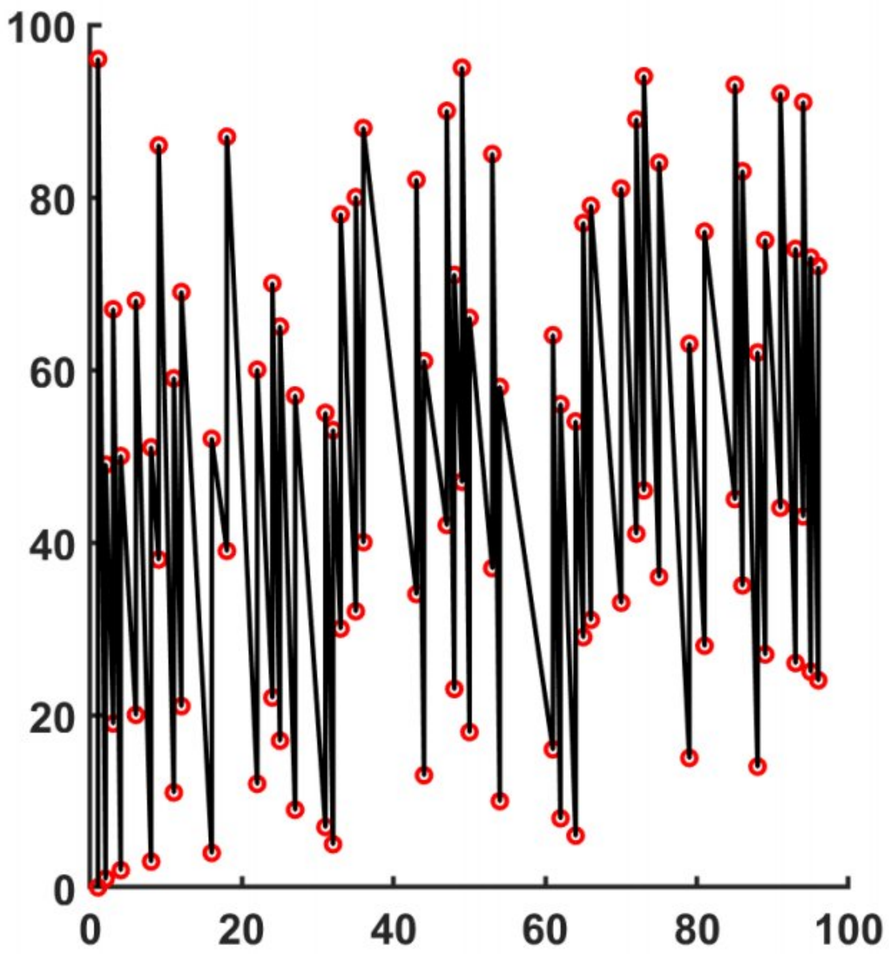
1. How to do fast modular exponentiation
2. Fermat's Little Theorem
3. Euler's Totient Function
4. Euler's Theorem

Outline

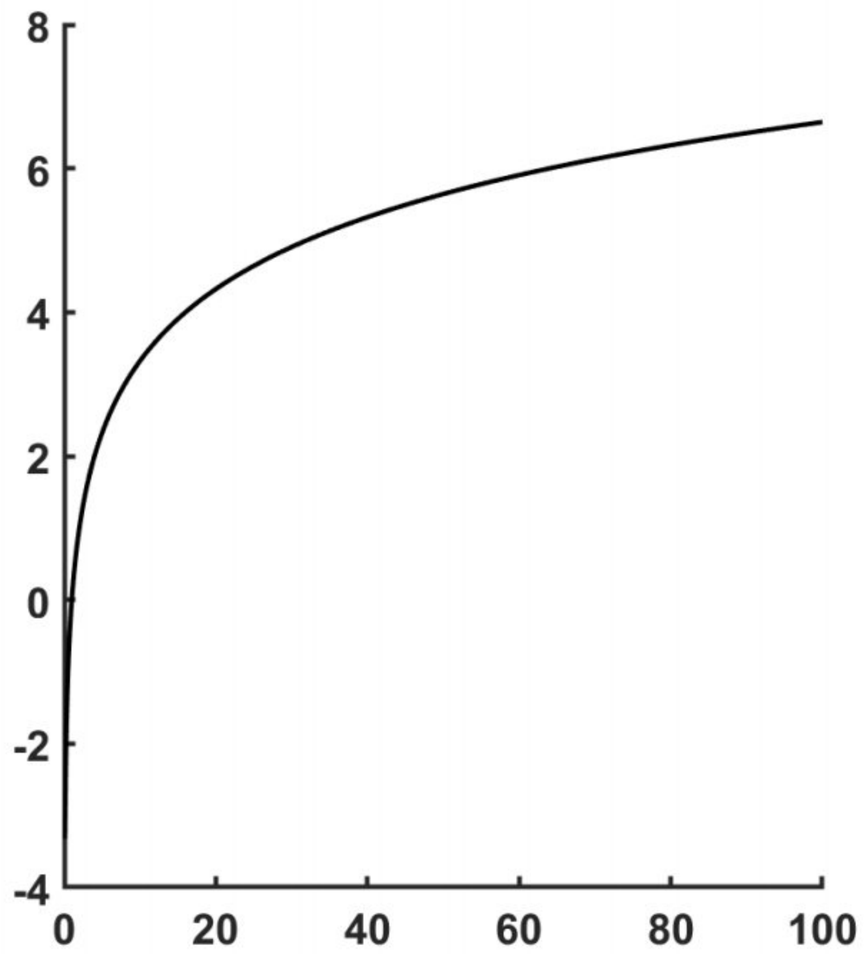
Modular Exponentiation

- We want to calculate $b^e \pmod{m}$,
- b is the base and e the exponent.
- Can be computed with efficient algorithms
- The reverse process (modular or discrete logarithm) is very hard for large b, e and m unless some information is given.
- Used as a key block in public key RSA cryptography

Discrete Logarithm is Hard to predict!



Left: Inversion of $y \equiv 2^x \pmod{97}$,



Right: Inversion of $y = 2^x$

Recursive Computation

- No need to compute the giant number b^e then divide by m
- Since $ab \pmod m \equiv (a \bmod m)\,(b \bmod m) \pmod m$
- We can start with 1, then multiply by b, immediately take the result modulo m to avoid large numbers, and repeat e times

```
def fastExp(b, e, m):
    c = 1
    for i in range(e):
        c = (c * b) % m
    return c
```

- We compute $7^4 \pmod{11}$ with the following steps $c = 1$, $c \equiv 7 \pmod{11}$, $c \equiv 49 \equiv 5 \pmod{11}$, $c \equiv 35 \equiv 2 \pmod{11}$, $c \equiv 14 \equiv 3 \pmod{11}$.
- e multiplications. Can we do faster?

Recursive Computations for $e = 2^k$

- We can reduce number of multiplications by using powers of 2

Example

For $b = 7, e = 128, m = 11$, we can compute $7^{128} \pmod{11}$ as:

- $7^2 \equiv 49 \equiv 5 \pmod{11}$
- $7^4 \equiv 25 \equiv 3 \pmod{11}$
- $7^8 \equiv 9 \equiv 9 \pmod{11}$
- $7^{16} \equiv 81 \equiv 4 \pmod{11}$
- $7^{32} \equiv 16 \equiv 5 \pmod{11}$
- $7^{64} \equiv 25 \equiv 3 \pmod{11}$
- $7^{128} \equiv 9 \equiv 9 \pmod{11}$

- $\log_2(e) = 7$ multiplications are required instead of 128

Recursive Computations for General e

- What if $e \neq 2^k$? Split it into powers of 2 using binary form

Example

For $b = 7, e = 13, m = 11$, we can compute $7^{13} \pmod{11}$ as:

- $e = 13 = 1101_2 = 8 + 4 + 1 \Longrightarrow 7^{13} = 7^8 \times 7^4 \times 7^1$
- $7^1 \equiv 7 \equiv 7 \pmod{11}$
- $7^2 \equiv 49 \equiv 5 \pmod{11}$
- $7^4 \equiv 25 \equiv 3 \pmod{11}$
- $7^8 \equiv 9 \equiv 9 \pmod{11}$
- $7^{13} = 7^8 \times 7^4 \times 7^1 = 9 \times 3 \times 7 \equiv 21 \times 9 \equiv 10 \times 9 \equiv 2 \pmod{11}$

- At most $2\log_2(e)$ multiplications are required

Fermat's Little Theorem

Theorem

Let p is a prime, and suppose $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$

This theorem can be stated in a more general way in which the requirement that $p \nmid a$ is dropped.

Corollary

Let p is a prime, then $a^p \equiv a \pmod{p}$

Proof.

- If $p \mid a$, then $a^p \equiv 0 \equiv a$
- If $p \nmid a$, then we can multiply the congruence of Fermat's little theorem by a to get $a^p \equiv a \pmod{p}$

□

Proof of Fermat's Little Theorem

- Consider the first $p-1$ multiples of a: $\{a, 2a, \ldots, (p-1)a\}$
- In modulo p, these multiples are not pairwise congruent nor congruent to 0 since $p \nmid a$
- Therefore, the set $\{a, 2a, \ldots, (p-1)a\}$ must have the same values in the set of remainders $\{1, 2, \ldots, p-1\}$
- Multiplying all these congruences together, we have

$$a \times 2a \times \ldots \times (p-1)a \equiv 1 \times 2 \times \ldots (p-1) \pmod{p}$$

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

- Since $p \nmid (p-1)!$, we can cancel $(p-1)!$ from both sides to get

$$a^{p-1} \equiv 1 \pmod{p}$$

Fast Modular Exponentiation using Fermat's theorem

- To compute $a^n \pmod p$, we only need to compute powers up to $p-1$ even if n is much larger than p
- For exponent, we only care about remainder of n mod (p-1) because every $a^{p-1} \equiv 1 \pmod p$, i.e.,

$$a^n \equiv a^{n \bmod (p-1)} \pmod p$$

- Example: We can compute $7^{222} \pmod{11}$ by knowing that $7^{10} \equiv 1 \pmod{11}$, then $7^{10k} \equiv 1 \pmod{11}$, then we have

$$7^{222} = 7^{22\times 10+2} \equiv \left(7^{10}\right)^{22} \times 7^2 \equiv (1)^{22} \times 49 \equiv 5 \pmod{11}$$

Primality Test using Fermat's Theorem

- If it could be shown that the congruence

$$a^n \equiv a \pmod{n}$$

fails to hold for some choice of a, then n is necessarily composite.

- To simplify computations, use a small base $a = 2$
- Example: For $n = 117$

$$2^{117} \equiv 44 \not\equiv 2 \pmod{117}$$

Therefore, 117 is definitely not a prime, actually $117 = 13 \times 9$

Example on Fermat's Theorem

Assume all powers $a^e \pmod p$, where $p = 7$ is a prime number

a/e	1	2	3	4	5	6
$1^e \pmod 7$	1	1	1	1	1	1
$2^e \pmod 7$	2	4	1	2	4	1
$3^e \pmod 7$	3	2	6	4	5	1
$4^e \pmod 7$	4	2	1	4	2	1
$5^e \pmod 7$	5	4	6	2	3	1
$6^e \pmod 7$	6	1	6	1	6	1

- We note that all exponentiations with $e = p - 1 = 6$ gives 1

$$a^{p-1} \equiv 1 \; \forall \; a : p \nmid a$$

- Note that: some values of a gives 1 at exponents less than $p - 1$.
- We will revisit this in Lecture 6.

The Sum and Number of Divisors

Any function whose domain of definition is the set of positive integers is said to be a number-theoretic (or arithmetic) function

Definition

Given a positive integer n, let $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of these divisors.

Example

- For $n = 12$, positive divisors are 1, 2, 3, 4, 6, 12.
- Then $\tau(12) = 6$, $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$

$\tau(n) = 2$ and $\sigma(n) = n + 1$ iff n is a prime number.

Notation

Definition

The symbol

$$\sum_{d \mid n} f(d)$$

means: "Sum the values $f(d)$ as d runs over all the positive divisors of the positive integer n"

Using this notation, we can write τ and σ as

$$\tau(n) = \sum_{d \mid n} 1, \quad \text{and} \quad \sigma(n) = \sum_{d \mid n} d$$

Positive Divisors of n

Theorem

If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ *is the prime factorization of* $n > 1$, *then the positive divisors are precisely those integers* d *of the form*

$$d = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r},$$

where $0 \leq a_i \leq k_i \forall i = 1, 2, \dots, r$

Multiplicative Functions

Definition

A number-theoretic function f is said to be *multiplicative* if

$$f(mn) = f(m)f(n) \quad \text{whenever} \quad \gcd(m,n) = 1$$

Theorem

The functions τ and σ are both multiplicative functions

Proof.

Assume the canonical factorizations $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ and $n = q_1^{j_1} q_2^{j_2} \dots q_r^{j_r}$, then because $\gcd(m,n) = 1$, no p_i can occur among q_j, then $mn = p_1^{k_1} \dots p_r^{k_r} q_1^{j_1} \dots q_r^{j_r}$. Using the theorem in previous slide, we can get $\tau(mn) = \tau(m)\tau(n)$ and $\sigma(mn) = \sigma(m)\sigma(n)$. □

τ and σ in terms of prime factorization

Theorem

If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ *is the prime factorization of* $n > 1$, *then*

$$\tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_r + 1),$$

and

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \dots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

τ and σ in terms of prime factorization: Proof

- Assume a prime number p with divisors 1 and p
- Raising to power n, divisors become $1, p, p^2, \ldots, p^n$
- Then $\tau(p^n) = n + 1$ and $\sigma(p^n) = \sum_{i=0}^{n} p^i = \frac{p^{n+1}-1}{p-1}$
- Using the multiplicative property of σ and τ:

$$\begin{aligned}
\tau(n) &= \tau(p_1^{k_1})\tau(p_2^{k_2})\ldots\tau(p_r^{k_r}) \\
&= (k_1+1)(k_2+1)\ldots(k_r+1) \\
\sigma(n) &= \sigma(p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}) \\
&= \sigma(p_1^{k_1})\sigma(p_2^{k_2})\ldots\sigma(p_r^{k_r}) \\
&= \frac{p_1^{k_1+1}-1}{p_1-1}\frac{p_2^{k_2+1}-1}{p_2-1}\cdots\frac{p_r^{k_r+1}-1}{p_r-1}
\end{aligned}$$

Euler's Totient Function

- Key for the RSA encryption
- Easy to compute if factorization of n is known
- No fast algorithms are known to compute if factorization of n is unknown
- No fast algorithms are known for factorization of integers
- Easy to compute with some private information, but no known way to compute without it – this is the key property for cryptography

Definition

Definition

For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.

- Example: $\phi(30) = 8$ because we have 8 numbers that are less than 30 and co-primes with it: $\{1, 7, 11, 13, 17, 19, 23, 29\}$
- $\phi(1) = 1$ because $\gcd(1, 1) = 1$
- $\phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(5) = 4, \phi(6) = 2, \phi(7) = 6, ...$
- $\phi(n) = n - 1$ iff n is a prime

Euler's Theorem

- Generalization of Fermat's Little Theorem to composites
- Used for encryption and decryption in RSA algorithm

Theorem

If $n \geq 1$ *and* $\gcd(a, n) = 1$, *then*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

- Before we prove Euler's theorem, let's define a useful tool in number theory proofs: *The Reduced Residue Systems*.

Reduced Residue Systems

Definition

A *Reduced Residue System Modulo n*: $\{a_1, a_2, \ldots, a_k\}$ is a subset of the complete residue system $\{0, 1, \ldots, n-1\}$ that satisfies:

1. $\gcd(a_i, n) = 1 \ \forall \ i \in \{1, \ldots, k\}$
2. $a_i \not\equiv a_j \pmod{n} \ \forall \ i \neq j$ and $i, j \in \{1, \ldots, k\}$

- Condition 1: All elements are co-primes with n
- Condition 2: All elements are pair-wise incongruent
- Then, any number m that is co-prime to n must be represented by one of the elements in the reduced residue system, i.e.,

$$\text{For any } m \in \mathbb{Z} \text{ and } \gcd(m, n) = 1, \exists\, j : m \equiv a_j \pmod{n}$$

- For $n = 12$, the set $\{1, 5, 7, 11\}$ is a reduced residue system.

Proof of Euler Theorem

- Let $\{r_1, r_2, \ldots, r_k\}$ is a reduced residue system modulo n
- Since $\gcd(a, n) = 1$, then $\{ar_1, ar_2, \ldots, ar_k\}$ is also a reduced residue system equivalent to $\{r_1, r_2, \ldots, r_k\}$ in some order, i.e.,

$$ar_j \equiv r_{j_i} \pmod{n} \;\; \forall\, j, j_i \in \{1, \ldots, k\}$$

- The products of all elements in the two sets are the same

$$ar_1 ar_2 \ldots ar_k \equiv r_1 r_2 \ldots r_k \pmod{n}$$
$$a^k (r_1 r_2 \ldots r_k) \equiv (r_1 r_2 \ldots r_k) \pmod{n}$$
$$a^k \equiv 1 \pmod{n}$$

- We cancelled $r_1 r_2 \ldots r_k$ because $\gcd(r_1 r_2 \ldots r_k, n) = 1$
- From the definition of $\Phi(n)$, we know that $k = \Phi(n)$
- Therefore, $a^{\Phi(n)} \equiv 1 \pmod{n}$

Proof of Euler Theorem – Example

- For $n = 12$, the set $\{1, 5, 7, 11\}$ is a reduced residue system.
- Choose $a = 5$ which is co-prime with 12, i.e., $\gcd(5, 12) = 1$
- Multiply all elements in the reduced residue system by 5
- $\{r_1 = 1, r_2 = 5, r_3 = 7, r_4 = 11\} \Longrightarrow \{5r_1, 5r_2, 5r_3, 5r_4\}$
- $5r_1 \equiv 5 \equiv r_2 \pmod{12}$
- $5r_2 \equiv 25 \equiv r_1 \pmod{12}$
- $5r_3 \equiv 35 \equiv r_4 \pmod{12}$
- $5r_4 \equiv 55 \equiv r_3 \pmod{12}$
- We return back to the same set, but in different order.
- But anyway order is not important in sets, and in multiplication.

How to Calculate $\Phi(n)$ for $n = p^e$?

- For a set $\mathcal{S}$, the cardinality $|\mathcal{S}|$ is the number of elements in $\mathcal{S}$
- Then, $\Phi(p) = |\{x : 1 \leq x \leq p, \gcd(x,p) = 1\}| = p - 1$
- $\Phi(p^e) = |\{x : 1 \leq x \leq p^e, \gcd(x,p^e) = 1\}|$
- $\Phi(p^e) = |\{x : 1 \leq x \leq p^e, p \nmid x\}|$
- $\Phi(p^e) = p^e - |\{x : 1 \leq x \leq p^e, p \mid x\}|$
- $p \mid x \implies p \leq x = kp \leq p^e \implies 1 \leq k \leq p^{e-1}$, then
- $\Phi(p^e) = p^e - p^{e-1}$
- $\Phi(p^e) = p^e \left(1 - \frac{1}{p}\right)$

How to Calculate $\Phi(n)$ for general n?

- Knowing the factorization of n: $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$
- We will use the multiplicative property of Euler's totient function $\Phi(n)$: for co-prime m and n: $\Phi(mn) = \Phi(m)\Phi(n)$

$$\begin{aligned}\Phi(n) &= \Phi(p_1^{e_1})\Phi(p_2^{e_2}) \dots \Phi(p_k^{e_k}) \\ &= p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) \\ &= n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)\end{aligned}$$

Example

- $\Phi(35) = 35(1 - 1/5)(1 - 1/7) = 24$
- $\Phi(100) = 100(1 - 1/2)(1 - 1/5) = 40$

Euler Theorem and Fast Modular Exponentiation

Example

Calculate the least positive residue of $3^{100,000} \pmod{35}$

- Using Euler's theorem: $3^{\Phi(35)} \equiv 3^{24} \equiv 1 \pmod{35}$
- Then, $3^{100,000} \equiv 3^{100,000 \bmod 24} \equiv 3^{16} \pmod{35}$ – Still large!
- Split the modulo $35 = 7 \times 7$ into two sub modules 5 and 7
- $3^{\Phi(5)} \equiv 3^4 \equiv 1 \pmod{5}$ and $3^{\Phi(7)} \equiv 3^6 \equiv 1 \pmod{7}$
- $\text{lcm}(4,6) = 12 \Longrightarrow 3^{12} \equiv 1 \pmod{5}$ and $3^{12} \equiv 1 \pmod{7}$
- Then, we have $3^{12} \equiv 1 \pmod{35}$
- Then $3^{16} \equiv \cancel{3^{12}}\, 3^4 \equiv 3^4 \equiv 11 \pmod{35}$