Discrete Logarithms and Diffie Hellman Key Exchange

Dept. of Computer Science & Engg.
IIT Kharagpur, India

Dipanwita Roy Chowdhury

Powers of an Integer, Modulo n

- Euler's Theorem

  For every a and n that are relatively prime,

  $a^{\Phi(n)} \equiv 1 \bmod n$, $\Phi(n)$ is Euler's Totient function.

- Consider more general expression:

  $a^m \equiv 1 \bmod n$, where a and n are relatively prime

The least positive exponent m for which equation holds is referred as

- the order of a (mod n)
- the exponent to which a belongs (mod n)
- the length of the period generated by a

Period

Example: Consider the powers of 7 modulo 19

- $7^1 =$ 7 mod 19
- $7^2 = 49 = 2 \times 19 + 11 =$ 11 mod 19
- $7^3 = 343 = 18 \times 19 + 1 =$ 1 mod 19
- $7^4 = 2401 = 126 \times 19 + 7 =$ 7 mod 19
- $7^5 = 16807 = 884 \times 19 + 11 =$ 11 mod 19

The sequence is periodic and the length of the period is the smallest positive exponent m such that $7^m \equiv 1 \bmod 19$

Here, $7^3 \equiv 1 \bmod 19$, So the period is 3

Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1

Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Primitive Root

- The length of the sequence:
  - All sequences end in 1
  - The length of a sequence divides $\Phi(19) = 18$
  - Some of the sequences are of length 18. Base integer a generates the set of nonzero integers modulo 19.

Definition: The highest possible exponent to which a number can belong (mod n) is $\Phi(n)$. If a number is of order $\Phi(n)$, it is referred to as a primitive root of n.

For the prime number 19, primitive roots are

2, 3, 10, 13, 14, 15

- Not all integers have primitive root. Integers with primitive roots are of the form **2, 4, p^{α} and $2p^{\alpha}$** , where p is odd prime ans α is a positive integer.

Indices

- With ordinary positive real number, the logarithm function is the inverse of exponentiation.

For base x and a value y,

$$y = x^{\log_x(y)}$$

$$\log_x(1) = 0$$

$$\log_x(x) = 1$$

$$\log_x(yz) = \log_x(y) + \log_x(z)$$

$$\log_x(y^r) = r \times \log_x(y)$$

Indices for Modular Arithmetic

- For a primitive root **a** with some prime number **p**, the powers of a from 1 through (p-1) produce each integer from 1 through (p-1) [true for non-prime also]
- Any integer b can be expressed as

$$b \equiv r \bmod p, \text{ where } 0 \le r \le (p-1)$$

So, $b \equiv a^i \bmod p$, where $0 \le i \le (p-1)$

Here, i is referred to as the index of the number b for the base a (mod p)

$$\mathbf{i = ind_{a,p}(b)}$$

- $\mathbf{ind_{a,p}(1) = 0}$, **because** $a^0 \bmod p = 1 \bmod p = 1$
- $\mathbf{ind_{a,p}(a) = 1}$, **because** $a^1 \bmod p = a$

Indices for Modular Arithmetic

Example: Consider, non-prime modulus n = 9

Here, $\Phi(9) = 6$ and a = 2 is a primitive root

- $2^0 =$ 1
- $2^1 =$ 2
- $2^2 =$ 4
- $2^3 =$ 8
- $2^4 =$ 7
- $2^5 =$ 5 (mod 9)
- $2^6 =$ 1

Numbers with given indices (mod 9) for the root a = 2

Index	**0**	**1**	**2**	**3**	**4**	**5**
Number	1	2	4	8	7	5

Indices for Modular Arithmetic

Example: Consider, non-prime modulus n = 9

Here, $\Phi(9) = 6$ and a = 2 is a primitive root

Rearrange the table to make the remainders relatively prime to 9

Number	1	2	4	5	7	8
Index	0	1	2	5	4	3

Rules of Indices for Modular Arithmetic

- Rules of modular multiplication

$$xy \bmod p = (x \bmod p)(y \bmod p)$$

$$a^{\text{ind }a,p(xy)} \bmod p = (a^{\text{ind }a,p(x)} \bmod p)(a^{\text{ind }a,p(y)} \bmod p)$$

$$= (a^{\text{ind }a,p(x) + \text{ind }a,p(y)}) \bmod p$$

Rules of Indices for Modular Arithmetic

- Euler's Theorem: $a^{\Phi(n)} \equiv 1 \bmod n$

  Any positive integer z can be expressed in the form

  $z = q + k\Phi(n)$

  $a^z \equiv a^q \bmod n$, if $z = q \bmod \Phi(n)$

Applying this equality to modular indices,

$$\mathrm{ind}_{a,p}(xy) = (\mathrm{ind}_{a,p}(x) + \mathrm{ind}_{a,p}(y)) \bmod \Phi(p)$$

Generalizing,

$$\mathrm{ind}_{a,p}(y^r) = (r \times \mathrm{ind}_{a,p}(y)) \bmod \Phi(p)$$

Discrete Logarithm Problem

- Consider the equation

$$y = g^{x} \mod p$$

- Given g, x, and p, it is a straightforward matter to calculate y
- However, given y, g, and p it is in general very difficult to calculate x take the discrete logarithm)
- The difficulty seems to be on the same order of magnitude as that of factoring primes required for RSA.

Diffie-Hellman Key Exchange

- first public-key type scheme proposed
- by Diffie & Hellman in 1976 along with the exposition of public key concepts
  - note: now know that Williamson (UK CESG) secretly proposed the concept in 1970
- is a practical method for public exchange of a secret key
- used in a number of commercial products

Diffie-Hellman Key Exchange

- a public-key distribution scheme
  - cannot be used to exchange an arbitrary message
  - rather it can establish a common key
  - known only to the two participants
- value of key depends on the participants (and their private and public key information)
- based on exponentiation in a finite (Galois) field (modulo a prime or a polynomial) - easy
- security relies on the difficulty of computing discrete logarithms (similar to factoring) – hard

Diffie-Hellman Setup

- all users agree on global parameters:
  - large prime integer or polynomial q
  - a being a primitive root mod q
- each user (eg. A) generates their key
  - chooses a secret key (number): $x_A < q$
  - compute their **public key**: $y_A = a^{x_A} \bmod q$
- each user makes public that key y_A

Diffie-Hellman Key Exchange

- shared session key for users A & B is K_{AB}:

$$K_{AB} = a^{x_A . x_B} \bmod q$$
$$= y_A^{x_B} \bmod q \quad \text{(which } \mathbf{B} \text{ can compute)}$$
$$= y_B^{x_A} \bmod q \quad \text{(which } \mathbf{A} \text{ can compute)}$$

- K_{AB} is used as session key in private-key encryption scheme between Alice and Bob
- if Alice and Bob subsequently communicate, they will have the **same** key as before, unless they choose new public-keys
- attacker needs an x, must solve discrete log

Diffie-Hellman Example

- users Alice & Bob who wish to swap keys:
- agree on prime $q=353$ and $a=3$
- select random secret keys:
  - A chooses $x_A=97$, B chooses $x_B=233$
- compute respective public keys:
  - $y_A=3^{97} \bmod 353 = 40$ (Alice)
  - $y_B=3^{233} \bmod 353 = 248$ (Bob)
- compute shared session key as:
  - $K_{AB}= y_B^{x_A} \bmod 353 = 248^{97} = 160$ (Alice)
  - $K_{AB}= y_A^{x_B} \bmod 353 = 40^{233} = 160$ (Bob)

Key Exchange Protocols

- users could create random private/public D-H keys each time they communicate
- users could create a known private/public D-H key and publish in a directory, then consulted and used to securely communicate with them
- both of these are vulnerable to a meet-in-the-Middle Attack
- authentication of the keys is needed