The University of Sydney
School of Computer Science
Dr Suranga Seneviratne
Senior Lecturer - Security

THE UNIVERSITY OF SYDNEY

Number Theory

Number theory and abstract algebra are vital in cryptography. In this handout we will cover key number theory concepts we will need to understand cryptography.

1 Divisibility

We say that a non-zero b divides a if $a = mb$ for some m, where a, b, and m all are integers.

In other words, b divides a if there is no remainder on the division.

The notation $b|a$ is commonly used to mean b divides a. If $b|a$ we say that b is a divisor of a.

Example 1 The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.

Example 2 $13|182$ - Meaning 13 divides 182 - i.e., we can write as $182 = 14 \times 13$.

Example 3 $17|289$ - Meaning 17 divides 289 - i.e. we can write as $289 = 17 \times 17$.

2 Properties of Divisibility

- If $a|1$, then $a = \pm 1$
- If $a|b$ and $b|a$, then $a = \pm b$
- Any $b \neq 0$ divides 0
- If $a|b$ and $b|c$, then $a|c$

  Example 1 Given that $3|9$ and $9|27$, it follows that $3|27$.

  This means that there exists integers m and n such that $9 = 3m$ and $27 = 9n$. By substituting the first equation into the second, we get $27 = 3mn$, which shows that 3 divides 27.

  Example 2 Given that $11|66$ and $66|198$, it follows that $11|198$.

  This means that there exists integers m and n such that $66 = 11m$ and $198 = 66n$. By substituting the first equation into the second, we get $198 = 11mn$, which shows that 11 divides 198.

- If $b|g$ and $b|h$, then $b|(m.g + n.h)$ for arbitrary integers m and n.

  Example Consider the divisibility relations $11|66$ and $11|77$. According to the property of divisibility, for any arbitrary integers m and n, 11 will also divide the linear combination $m \cdot 66 + n \cdot 77$, which can be denoted as $11|(m \cdot 66 + n \cdot 77)$.

  To elaborate:

  – Since $11|66$, we can write $66 = 11k$ for some integer k.

  – Since $11|77$, we can also write $77 = 11l$ for some integer l.

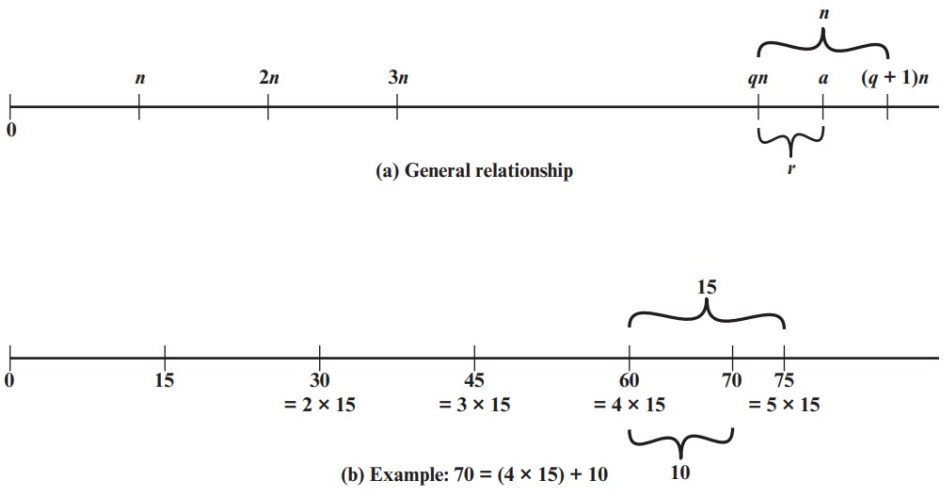
  Now, consider the expression $m \cdot 66 + n \cdot 77$. Substituting the values from above, we get $m \cdot 11k + n \cdot 11l = 11(mk + nl)$. Therefore, this expression is a multiple of 11, which proves that 11 divides $m \cdot 66 + n \cdot 77$.

3 Division Algorithm

Given any positive integer n and any non-negative integer a, if we divide a by n we get an integer quotient q and an integer remainder r that obey the following relationship:

$$a = qn + r \qquad 0 \leq r < n \; ; \; q = \left\lfloor \frac{a}{n} \right\rfloor$$

The notation $q = \left\lfloor \frac{a}{n} \right\rfloor$ refers to the floor function or greatest integer function. In the context of division, it means q is the greatest integer that is less than or equal to the fraction $\frac{a}{n}$.



The relationship $a = qn + r \; ; 0 \leq r < n$

Figure 1: Explaining the division algorithm using the number line

*__Source:__ Cryptography and Network Security – 7th Edition by William Stallings

4 Euclidean Algorithm

Euclidean Algorithm is a procedure for determining the Greatest Common Divisor (GCD) of two positive integers.

Definition - GCD : The greatest common divisor of a and b is the largest integer that divides both a and b.

- We can use the notation $gcd(a, b)$ to mean the greatest common divisor of a and b.
- We also define $gcd(0, 0) = 0$
- Positive integer c is said to be the gcd of a and b if:
  - c is a divisor of a and b
  - Any divisor of a and b is a divisor of c
- An equivalent definition is:

$$gcd(a, b) = \max[k, \text{ such that } k|a \text{ and } k|b]$$

- Because we require that the greatest common divisor be positive, $gcd(a, b) = gcd(a, -b) = gcd(-a, b) = gcd(-a, -b)$
- In general, $gcd(a, b) = gcd(|a|, |b|)$

  Example: $\gcd(60, 24) = \gcd(60, -24) = 12$

- Also, because all nonzero integers divide 0, we have $gcd(a, 0) = |a|$
- We stated that two integers a and b are relatively prime if their only common positive integer factor is 1; this is equivalent to saying that a and b are relatively prime if $gcd(a, b) = 1$.

Definition - Relative Primes: Two integers are relatively prime if their only common positive integer factor is 1.

Example: 8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

4.1 Finding the Greatest Common Divisor (GCD)

We can find the greatest common divisor of two integers by repetitive application of the division algorithm. This scheme is known as the Euclidean Algorithm.

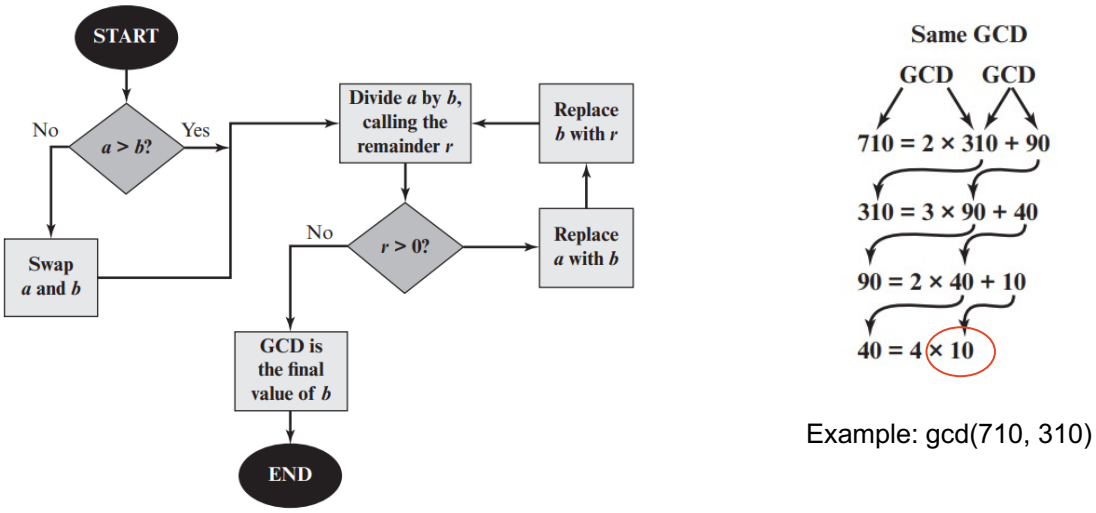


Figure 2: Euclidean Algorithm for finding the GCD

*Source: Cryptography and Network Security – 7th Edition by William Stallings

5 Modular Arithmetic

5.1 The Modulus

If a is an integer and n is a positive integer, we define $a \mod n$ to be the remainder when a is divided by n; the integer n is called the modulus.

Definition - $a \mod n$: is the remainder when a is divided by n.

- Thus, for any integer a:

$$a = qn + r \quad \text{where } 0 \leq r < n;\ q = \left\lfloor \frac{a}{n} \right\rfloor$$

$$a = \left\lfloor \frac{a}{n} \right\rfloor \times n + (a \mod n)$$

Example: $11 \mod 7 = 4$

Example: $-11 \mod 7 = 3$ (Note here that the mod value is positive.)

5.2 Congruent modulo n

Definition - Congruent modulo n: Two integers a and b are said to be congruent modulo n if $(a \mod n) = (b \mod n)$.

- In short, this is written as $a \equiv b \pmod{n}$. Verbally it is expressed as "a is congruent to b modulo n."

- Note that if $a \equiv 0 \pmod{n}$, then $n|a$.

Example 1: $73 \equiv 4 \pmod{23}$ - 73 is congruent to 4 modulo 23.

Example 2: $21 \equiv 31 \pmod{10}$ - 21 is congruent to 31 modulo 10.

5.3 Modular Operations

Modular arithmetic exhibits the following properties:

1. $[(a \mod n) + (b \mod n)] \mod n = (a + b) \mod n$
2. $[(a \mod n) - (b \mod n)] \mod n = (a - b) \mod n$
3. $[(a \mod n) \cdot (b \mod n)] \mod n = (a \cdot b) \mod n$

Let's verify these using some examples. Let $a = 11$, $b = 9$, and $n = 8$. Also note that $11 \mod 8 = 3; 9 \mod 8 = 1$. Below LHS means "left hand side" and RHS means "right hand side"

Example 1:
LHS $[(11 \mod 8) + (9 \mod 8)] \mod 8 = [3 + 1] \mod 8 = 4$
RHS $(11+9) \mod 8 = 4$
$\implies$ LHS = RHS.

Example 2:
LHS $[(11 \mod 8) - (9 \mod 8)] \mod 8 = [3 - 1] \mod 8 = 2$
RHS $(11\text{-}9) \mod 8 = 2$
$\implies$ LHS = RHS.

Example 3:
LHS $[(11 \mod 8) * (9 \mod 8)] \mod 8 = [3 * 1] \mod 8 = 3$
RHS $(11*9) \mod 8 = 2$
$\implies$ LHS = RHS.

We can also do exponentiation using repeated multiplication. This is one of the important results we will use later (i.e., Diffie-Hellman key exchange in Asymmetric Cryptography).

Example : Say you want to find $11^7 \mod 13$.
$11^2 = 121 \equiv 4 \pmod{13}$
$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13} \pmod{13}$
$11^7 = 11 \times 11^2 \times 11^4$
$11^7 = 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$

Thus, the rules for ordinary arithmetic involving addition, subtraction, and multiplication carry over into modular arithmetic.

5.4 Properties of Modular Arithmetic for integers in $\mathbb{Z}_n$

Define the set $\mathbb{Z}_n$ as the set of non-negative integers less than n.

Definition - Set of residues $\mathbb{Z}_n$: $\mathbb{Z}_n = \{0, 1, ..., (n-1)\}$

Here the elements of $\mathbb{Z}_n$ have a more precise meaning. Each integer in $\mathbb{Z}_n$ represents a residual class. We label the residue classes (mod n) as $[0], [1], [2], ..., [n-1]$ where, $[r] = \{a; a \text{ is an integer}, a \equiv r \mod n\}$. Of all the integers in a residue class, the smallest non-negative integer is the one used to represent the residue class. Now, we can perform modular arithmetic as shown in Figure 3.

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse ($-w$)	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

Figure 3: Properties of Modular Arithmetic for integers in Z_n

*__Source:__ Cryptography and Network Security – 7th Edition by William Stallings

6 Extended Euclidean Algorithm

With this background, we look at an extension to the Euclidean algorithm that will be important for later computations in the area of finite fields and in encryption algorithms, such as RSA. For given integers a and b, the extended Euclidean algorithm calculates not only the greatest common divisor d but also two additional integers x and y that satisfy the following equation.

$$ax + by = d = gcd(a, b)$$

Example: Applying the Extended Euclidean Algorithm for $a = 240$ and $b = 46$:

$$\begin{aligned} 240 &= 46 \times 5 + 10 && (1)\\ 46 &= 10 \times 4 + 6 && (2)\\ 10 &= 6 \times 1 + 4 && (3)\\ 6 &= 4 \times 1 + 2 && (4)\\ 4 &= 2 \times 2 + 0 && (5) \end{aligned}$$

From the Euclidean Algorithm, the GCD of 240 and 46 is 2. We now express 2 as a combination of 240 and 46:

$$\begin{aligned} 2 &= 6 - 4 \times 1 && \text{using } (4)\\ 2 &= 6 - (10 - 6 \times 1) \times 1 && \text{using } (3)\\ 2 &= 6 \times 2 - 10 && \text{simplify}\\ 2 &= (46 - 10 \times 4) \times 2 - 10 && \text{using } (2)\\ 2 &= 46 \times 2 - 10 \times 9 && \text{simplify}\\ 2 &= 46 \times 2 - (240 - 46 \times 5) \times 9 && \text{using } (1)\\ 2 &= 46 \times 47 - 240 \times 9 && \text{simplify} \end{aligned}$$

Thus, the coefficients are $x = -9$ and $y = 47$, meaning $240 \times (-9) + 46 \times 47 = \gcd(240, 46) = 2$.

Extended Euclidean Algorithm can be used to efficiently find the modular inverse of a number when it is of co-prime number with the modulus.

Example: To find the modular inverse of $a = 3$ modulo $n = 11$ (Note here that 3 and 11 are co-primes), we solve for x in the congruence:

$$3x \equiv 1 \pmod{11}$$

We use the Extended Euclidean Algorithm to express the GCD of 3 and 11 as a linear combination of 3 and 11:

$$11 = 3 \times 3 + 2 \quad (1)$$
$$3 = 1 \times 2 + 1 \quad (2)$$

Work backwards from these equations: From (2), we have $1 = 3 - 1 \times 2$.
Substitute 2 from (1):

$$2 = 11 - 3 \times 3$$

Thus, we have:

$$1 = 3 - 1 \times (11 - 3 \times 3)$$
$$1 = 3 - 11 + 3 \times 3$$
$$1 = 3 \times 4 - 11$$

Here, the coefficient of 3 in this expression, which is 4, is the modular inverse of 3 modulo 11. It satisfies:

$$3 \times 4 \equiv 1 \pmod{11}$$

This confirms that 4 is the modular inverse of 3 modulo 11.

Important: Note here that the modular inverse of a under modulus n exists only when a and n are co-primes.

For example, consider $a = 2$ and $n = 10$. So we have to find an element x of $\mathbb{Z}_{10}$ such that $2 \times x \equiv 1 \pmod{10}$.

Since the greatest common divisor (GCD) of 2 and 10 is not 1 (in fact, $\gcd(2, 10) = 2$), they are not co-prime.

This means that there is no integer x that satisfies the equation $2x \equiv 1 \pmod{10}$, indicating that 2 does not have a modular inverse under modulus 10.

To formally prove this, we can examine the set of all possible products of 2 with elements in $\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$. Multiplying 2 by any of these elements yields products that are even numbers, and taking these products modulo 10 will result in even remainders. Since 1 is not an even number, there is no element in $\mathbb{Z}_{10}$ that will satisfy the equation, confirming that the modular inverse does not exist in this case.

The modular inverse plays a crucial role in the RSA encryption and decryption process, particularly in the generation of the private key, which is fundamental to the RSA algorithm's functionality and security.

7 Prime Numbers

Definition - Prime Numbers: Prime numbers only have divisors of 1 and itself. i.e., They cannot be written as a product of other numbers.

- Prime numbers are central to number theory.
- The **fundamental theorem of arithmetic**
  Any integer $a > 1$ can be factored in a unique way as:

$$a = p_1^{a_1} * p_2^{a_2} * ... * p_t^{a_i}$$

  where $p_1 < p_2 < ... < p_t$ are prime numbers and where each a_i is a positive integer

Example: $36 = 2^2 \times 3^3$ or $360 = 2^3 \times 3^2 \times 5$

8 Fermat's Little Theorem

Fermat's Little Theorem: Fermat's Little Theorem states that for any integer a not divisible by a prime p, the following congruence holds: $a^{p-1} \equiv 1 \pmod{p}$

Example: Given Fermat's Little Theorem, for any integer a not divisible by a prime p, it holds that $a^{p-1} \equiv 1 \pmod{p}$.

For example, let $p = 7$ and $a = 3$. According to the theorem, we should find that $3^{7-1} \equiv 1 \pmod{7}$. Calculating 3^6:

$$3^6 = 729$$

And indeed, when divided by 7:

$$729 \mod 7 = 1$$

Thus, $3^6 \equiv 1 \pmod{7}$, as predicted by Fermat's Little Theorem.

Also, note here that we discussed a way of calculating $3^6 \mod 7$ easily by using repeated multiplication. That is we find that $3 \mod 7 = 3$ and $3^2 \mod 7 = 2$. Now we write $3^6 = 3^2 \times 3^2 \times 3^2 \mod 7 = 2 \times 2 \times 2 \mod 7 = 1$.

You can extend this idea to compute modular exponentiations for much larger numbers using a method called Exponentiation by Squaring.

9 How can we calculate $A^B \mod C$ quickly for any B?

Say we want to compute $5^{117} \mod 19$

Step 1: Divide B into powers of 2 by writing it in binary

$117 = 1110101$ in binary

Start at the rightmost digit, let $k = 0$ and for each digit:

- If the digit is 1, we need a part for 2^k, otherwise we do not.
- Add 1 to k, and move left to the next digit.

$$117 = (2^0 + 2^2 + 2^4 + 2^5 + 2^6)$$

$$117 = 1 + 4 + 16 + 32 + 64$$

$$5^{117} \mod 19 = 5^{(1+4+16+32+64)} \mod 19$$

$$5^{117} \mod 19 = (5^1 \times 5^4 \times 5^{16} \times 5^{32} \times 5^{64}) \mod 19$$

Step 2: Calculate $\mod C$ of the powers of two $\leq B$

$$
\begin{aligned}
5^1 &\mod 19 = 5 \\
5^2 &\mod 19 = (5^1 \times 5^1) \mod 19 = (5^1 \mod 19 \times 5^1 \mod 19) \mod 19 \\
5^2 &\mod 19 = (5 \times 5) \mod 19 = 25 \mod 19 \\
5^2 &\mod 19 = 6 \\
5^4 &\mod 19 = (5^2 \times 5^2) \mod 19 = (5^2 \mod 19 \times 5^2 \mod 19) \mod 19 \\
5^4 &\mod 19 = (6 \times 6) \mod 19 = 36 \mod 19 \\
5^4 &\mod 19 = 17 \\
5^8 &\mod 19 = (5^4 \times 5^4) \mod 19 = (5^4 \mod 19 \times 5^4 \mod 19) \mod 19 \\
5^8 &\mod 19 = (17 \times 17) \mod 19 = 289 \mod 19 \\
5^8 &\mod 19 = 4 \\
5^{16} &\mod 19 = (5^8 \times 5^8) \mod 19 = (5^8 \mod 19 \times 5^8 \mod 19) \mod 19 \\
5^{16} &\mod 19 = (4 \times 4) \mod 19 = 16 \mod 19 \\
5^{16} &\mod 19 = 16 \\
5^{32} &\mod 19 = (5^{16} \times 5^{16}) \mod 19 = (5^{16} \mod 19 \times 5^{16} \mod 19) \mod 19 \\
5^{32} &\mod 19 = (16 \times 16) \mod 19 = 256 \mod 19 \\
5^{32} &\mod 19 = 9 \\
5^{64} &\mod 19 = (5^{32} \times 5^{32}) \mod 19 = (5^{32} \mod 19 \times 5^{32} \mod 19) \mod 19 \\
5^{64} &\mod 19 = (9 \times 9) \mod 19 = 81 \mod 19 \\
5^{64} &\mod 19 = 5
\end{aligned}
$$

Step 3: Use modular multiplication properties to combine the calculated $\mod C$ values

$$
\begin{aligned}
5^{117} &\mod 19 = (5^1 \times 5^4 \times 5^{16} \times 5^{32} \times 5^{64}) \mod 19 \\
5^{117} &\mod 19 = (5^1 \mod 19 \times 5^4 \mod 19 \times 5^{16} \mod 19 \times 5^{32} \mod 19 \times 5^{64} \mod 19) \mod 19 \\
5^{117} &\mod 19 = (5 \times 17 \times 16 \times 9 \times 5) \mod 19 \\
5^{117} &\mod 19 = 61200 \mod 19 = 1 \\
5^{117} &\mod 19 = 1
\end{aligned}
$$

We will need this idea later when we learn the Diffie-Hellman key exchange.

10 Euler's Totient Function

Euler's Totient Function $\phi(n)$: The number of positive integers less than n and relatively prime to n.

Example: Determine $\phi(37)$ and $\phi(36)$.

1) Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus $\phi(37) = 36$.

2) To determine $\phi(35)$, we list all of the positive integers less than $35 = p - 1 = 34$ that are relatively prime to it:

1, 2, 3, 4, ~~5~~, 6, ~~7~~, 8, 9, ~~10~~, 11, 12, 13, ~~14~~, ~~15~~, 16, 17, 18, 19, ~~20~~, ~~21~~, 22, 23, 24, ~~25~~, 26, 27, ~~28~~, 29, ~~30~~, 31, 32, 33, 34

There are 24 numbers on the list. So $\phi(35) = 24$

Theorem: For two prime numbers p and q where $p \neq q$ and $n = pq$.

$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$$

Example: Find $\phi(21)$

Note that 21 is a product of two primes 7 and 3. So rather than listing all the numbers less than 21 and identifying numbers that are co-primes, we can directly use the above theorem.

$$\phi(n) = \phi(3) \times \phi(7) = (3-1) \times (7-1) = 2 \times 6 = 12$$

We can verify this with the previous method as well.

1, 2, ~~3~~, 4, 5, ~~6~~, ~~7~~, 8, ~~9~~, 10, 11, ~~12~~, 13, ~~14~~, ~~15~~, 16, 17, ~~18~~, 19, 20

There are 12 numbers in the list.

11 Euler's Theorem

Euler's Theorem is generalization of Fermat's Little Theorem.

Euler's Theorem: Euler's Theorem states that for every a and n that are relatively prime,

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

An alternative from is:

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

Example: Say $a = 3$ and $n = 5$

Note $\phi(5) = 4$

$$3^4 \pmod 5 = 1$$

$$1 \mod 5 = 1$$

$$\implies 3^{\phi(5)} \equiv 1 \pmod 5$$

12 Discrete Logarithm

Discrete Logarithms are fundamental to a number of public-key algorithms - e.g., Diffie-Hellman key exchange, Digital Signature Algorithm (DSA) etc.

12.1 Primitive root of a number

Consider this example. Here we have taken a prime number 19, and have considered all the integers less than 19. For each such integer a we compute $a^n \mod 19$, where n=1,2,...,18.

For example, consider row number 2 where $a = 2$.

$2^1 \mod 19 = 2$
$2^2 \mod 19 = 4$
$2^3 \mod 19 = 8$
$2^4 \mod 19 = 16$
$2^5 \mod 19 = 12$
$2^6 \mod 19 = 7$
...
$2^{17} \mod 19 = 10$
$2^{18} \mod 19 = 1$

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
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

2, 3, 10, 13, 14, 15 are primitive roots of modulus 19.

Figure 4: Power of an integer Modulo n

*__Source:__ Cryptography and Network Security – 7th Edition by William Stallings

The highest possible exponent to which a number can belong (mod n) is $\phi(n) = p - 1$.
If a number is of this order, we call it a primitive root of n.

Example: for the prime number 19, its primitive roots are 2, 3, 10, 13, 14, 15.

12.2 Discrete Logarithm Problem

The logarithm function is the inverse of exponentiation, and an analogous function exists for modular arithmetic. Consider

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

where p is a prime number and g is a primitive root of p.

Discrete Logarithm Problem (DLP: Given y, g, and p satisfying the equation

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

where p is a prime number and g is a primitive root of p, how do we find x?.

Example: Note that it given g, x, and p, it is easier and faster to calculate y. For example, consider $p = 19$, $g = 2$, and $x = 7$ (earlier we showed that 2 is a primitive root of 19).

$$y = 2^7 \mod 19$$

Computing this directly:

$$y = 128 \mod 19$$

Therefore, the result is:

$$y = 14$$

Also note that when p and x are very large we can use exponentiation by squaring to efficiently compute y.

Example: However, given g, y, and p, it is there is no efficient algorithm to calculate x. For example, consider $p = 19$, $g = 2$, and $y = 8$, there is no efficient way to calculate x.

Here, we want to find x such that

$$8 = 2^x \mod 19$$

As we saw in Figure 4 there is no specific pattern for x. Pretty much you have to try all x values and see which value of x gives you $y = 8$.