RV College of Engineering®
Mysore Road, RV Vidyaniketan Post,
Bengaluru - 560059, Karnataka, India

hod.maths@rvce.edu.in
www.rvce.edu.in
Tel: 080-68188263

Department of Mathematics

UNIT-I

NUMBER THEORY

Topic Learning Objectives:

Upon completion of this unit, students will be able to:

- Find quotients and remainders from integer division.
- Apply Euclid's algorithm and backwards substitution.
- Understand the definitions of congruences, residue classes and least residues.
- Add and subtract integers, modulo n, multiply integers and calculate powers, modulo n.
- Determine multiplicative inverses, modulo n and use to solve linear congruences.
- Apply to Encryption and Decryption.

Introduction

Number theory is the study of natural or counting numbers, including prime numbers. Number theory is important because the simple sequence of counting numbers from one to infinity conceals many relationships beneath its surface.

Number theory is an immensely rich area and it is defined by the important problems that it tries to solve. Sometimes a problem was considered solved, but years later the solution was found to be flawed. One important challenge in number theory has been trying to find a formula that will describe all the prime numbers. To date, that problem has not been solved.

One of Gauss's most important contributions to number theory involved the invention of the idea of congruence in numbers and the use of what he called "modulo" or small measures or sets of numbers. In effect, his theory of congruence allows people to break up the infinite series of whole numbers into smaller, more manageable chunks of numbers and perform computations upon them. This arrangement makes the everyday arithmetic involved in such things as telling time much easier to program into computers.

Prime and composite numbers play an important role in modern cryptography or coding systems. Huge volumes of confidential and large amounts of money are transferred electronically around the world every day, all of which must kept secret. One of the important applications of number theory is keeping secrets.

This time gap between finding out if a number is prime and factoring the primes in a composite number is useful to cryptographers. To create a security system, they invent numerical codes for the letters and characters of a message.

Number theory: a huge, ancient, complex, and above all, beautiful branch of mathematics. Historically, number theory was known as the Queen of Mathematics and was very much a branch of pure mathematics, studied for its own sake instead of understanding real world applications. This has changed in recent years however, as applications of number theory have been unearthed. Probably the most well-known example of this is RSA cryptography, one of the methods used in encrypting data on the internet. It is number theory that makes this possible.

Divisibility

If a and b are integers such that $a \neq 0$, then we say "a divides b" if there exists an integer k such that $b = ka$.

If a divides b, we also say "a is a factor of b" or "b is a multiple of a" and we write $a|b$. If a doesn't divide b, we write $a \nmid b$. For example, $2|4$ and $7|63$, while $5 \nmid 26$.

Note that any even integer has the form $2k$ for some integer k, while any odd integer has the form $2k+1$ for some integer k. Thus $2|n$ if n is even, while $2 \nmid n$ if n is odd.

Elementary properties:

1. If a is any non-zero integer, then $a|a$ and $a|0$.

2. If $a|b$, then $a|-b$, $-a|b$ and $-a|-b$.

3. If a is any integer, then $1|a$ and $-1|a$.

4. Only divisors of 1 are 1 and -1.

5. Only divisors of -1 are 1 and -1.

Properties:

(1) If a and b are non-zero integers such that $a|b$ and $b|a$, then $a = \pm b$.

Proof: $a|b \Rightarrow b = ak_1$ (1) where $k_1 \in Z$

$b|a \Rightarrow a = bk_2$ (2) where $k_2 \in Z$

Multiplying (1) and (2), we get

$ba = (k_1k_2)ab$

$\Rightarrow k_1k_2 = 1$

As k_1 and k_2 are integers, $k_1k_2 = 1 \Rightarrow k_1 = k_2 = 1$ or $k_1 = k_2 = -1$

Thus $a = b$ or $a = -b$

$\therefore a = \pm b$

(2) If $a|b$ and $b|c$ then $a|c$ (transitive law)

Proof: $a|b \Rightarrow b = ak_1$ (1) where $k_1 \in Z$

$b|c \Rightarrow c = bk_2$ (2) where $k_2 \in Z$

(1) and (2) gives $c = k_1\, k_2a$

$\Rightarrow c = k_3a$ where $k_3 = k_1k_2 \in Z$

$\therefore a|c$.

(3) If $a|b$ and $a|c$ then (i) $a|b + c$ (ii) $a|b - c$ (iii) $a|bc$

Proof: $a|b \Rightarrow b = ak_1$ (1) where $k_1 \in Z$

$a|c \Rightarrow c = ak_2$ (2) where $k_2 \in Z$

(i) Adding (1) and (2), $b + c = (k_1 + k_2)a$

$\therefore a|b + c$

(ii) Subtracting (1) and (2), $b - c = (k_1 - k_2)a$

$\therefore a|b-c$

(iii) Multiplying (1) and (2),

$bc = (k_1k_2)a^2 \Rightarrow bc = (k_1k_2a)a$

$\therefore a|bc$

(4) If $a|b$ and x is any integer, then $a|bx$.

Proof: $a|b \Rightarrow b = ka$ where $k \in Z$

Multiplying both sides by x, we get

$bx = kax = (kx)a$

$\therefore a|bx$

(5) If $a|b$ and $c|d$, then $ac|bd$.

Proof: $a|b \Rightarrow b = ak_1$ (1) where $k_1 \in Z$

$c|d \Rightarrow d = ck_2$ (2) where $k_2 \in Z$

Multiplying (1) and (2), we get

$bd = (k_1a)(k_2c) \Rightarrow bd = (k_1k_2)ac$

$bd = k_3ac$ where $k_3 = k_1k_2 \in Z$

$\therefore ac|bd.$

(6) If $ac|bc$, then $a|b$. $(c \neq 0)$

Proof: $ac|bc \Rightarrow bc = kac$ where $k \in Z$

On dividing by c,

$b = ka$ where $k \in Z$

$\therefore a|b.$

Division algorithm

The division algorithm, despite its name, it is not really an algorithm. It states that when you divide two numbers, there is a unique quotient and remainder. Specifically, it says the following:

Theorem: Let $a, b \in Z$ with $b > 0$. Then there exist unique $q, r \in Z$ such that $a = bq + r$ and $0 \leq r < b$.

The integers q and r are called the quotient and remainder respectively.

For example, if $a = 27$ and $b = 7$, then $q = 3$ and $r = 6$. That is, $27 \div 7$ is 3 with a remainder of 6, or in equation form: $27 = 7 \times 3 + 6$.

The Greatest Common Divisor

In this section we define the greatest common divisor (GCD) of two integers and discuss its properties. We also prove that the greatest common divisor of two integers is a linear combination of these integers.

Two integers a and b, not both 0, can have only finitely many divisors, and thus can have only finitely many common divisors. In this section, we are interested in the greatest common divisor of a and b. Note that the divisors of a and that of $|a|$ are the same.

Definition: The greatest common divisor of two integers a and b is the greatest integer that divides both a and b.

We denote the greatest common divisor of two integers a and b by $gcd(a, b)$ or (a, b).

Example: Note that the greatest common divisor of 24 and 18 is 6. In other words

$gcd(24, 18) = 6$.

There are integers (e.g. 3 and 4, etc.) whose greatest common divisor is 1 so we call such integers relatively prime integers.

Definition: Two integers a and b are relatively prime if $gcd(a, b) = 1$.

Example: The greatest common divisor of 9 and 16 is 1, thus they are relatively prime.

Note that every integer has positive and negative divisors. If a is a positive divisor of m, then $-a$ is also a divisor of m. Therefore, by our definition of the greatest common divisor, we can see that $gcd(a,b) = gcd(|a|,|b|)$.

We now present a theorem about the greatest common divisor of two integers. The theorem states that if we divide two integers by their greatest common divisor, then the outcome is a couple of integers that are relatively prime.

NOTE:

1. If $'a'$ is a non-zero integer, then $gcd(a,0) = a$.
2. If $gcd(a,b) = d$ then $gcd\left(\frac{a}{d},\frac{b}{d}\right) = 1$
3. If $gcd(a,b) = d$ and m is any positive integer, then $gcd(ma,mb) = md$.

The Euclidean Algorithm

In this section we describe a systematic method that determines the greatest common divisor of two integers. This method is called the Euclidean algorithm.

The two numbers a and b can be assumed as positive. Let $a < b$. b is divided by a and let r_1 be the remainder. Then $0 \le r_1 < a$. Now a is divided by r_1 and the remainder obtained is taken as r_2, then $0 \le r_2 < r_1$. Again r_1 is divided by r_2 and the remainder obtained is r_3.

Continuing this process of dividing each divisor by the next remainder, at some stage 0 remainder is obtained. The last non zero remainder is the GCD of a and b. This is known as Euclid's algorithm method.

Now to express the GCD as $ax + by$, the successive divisors are as follows

$a)\ b\ (q$
$\quad qa$
$\_\_\_\_\_$
$b - qa = r_1$

$$r_1 = b - qa \qquad (1)$$

$r_1)\ a(q_1$
$\quad q_1 r_1$
$\_\_\_\_\_$
$a - q_1 r_1 = r_2$

$$r_2 = a - q_1 r_1 \qquad (2)$$

$r_2)\ r_1(q_2$
$\quad q_2 r_2$
$\_\_\_\_\_$
$r_1 - q_2 r_2 = r_3$

$$r_3 = r_1 - q_2 r_2 \qquad (3)$$

The process is continued till the remainder is 0. Similarly, the following equations are obtained.

$$r_4 = r_2 - q_3 r_3 \qquad (3)$$

$\vdots$

$\vdots$

$$r_{n-2} = r_{n-4} - q_{n-3} r_{n-3}$$

$$r_{n-1} = r_{n-3} - q_{n-2} r_{n-2}$$

$$r_n = r_{n-2} - q_{n-1} r_{n-1}$$

Next remainder r_{n+1} becomes 0.

$\therefore$ GCD of a and b is r_n.

Example: Find the greatest common divisor of 4147 and 10672:

Solution:

$10672 = 4147 \times 2 + 2378$

$4147 = 2378 \times 1 + 1769$

$2378 = 1769 \times 1 + 609$

$1769 = 609 \times 2 + 551$

$609 = 551 \times 1 + 58$

$551 = 58 \times 9 + 29$

$58 = 29 \times 2$

Hence $(4147,10672) = 29$

We now use the steps in the Euclidean algorithm to write the greatest common divisor of two integers as a linear combination of the two integers. The following example will determine the variables m and n. The following algorithm can be described by a general form but for the sake of simplicity of expressions we will present an example that shows the steps for obtaining the greatest common divisor of two integers as a linear combination of the two integers.

Example: Express 29 as a linear combination of 4147 and 10672:

Solution: $29 = 551 - 9 \times 58$

$29 = 551 - 9(609 - 551 \times 1)$

$= (10 \times 551) - (9 \times 609)$

$= 10 \times (1769 - 609 \times 2) - 9 \times 609$

$= 10 \times 1769 - (29 \times 609)$

$= 10 \times 1769 - 29(2378 - 1769)$

$= 39 \times 1769 - (29 \times 2378)$

$= 39 \times (4147 - 2378 \times 1) - 29$

$= 39 \times 4147 - (68 \times 2378)$

$= 39 \times 4147 - 68(10672 - 4147)$

$29 = 175 \times 4147 - (68 \times 10672)$

As a result, we see that $29 = 175 \times 4147 - 68 \times 10672$.

Exercises:

1. By using the Euclidean algorithm, find the greatest common divisor d of 1769 and 2378 and then find integers x and y to satisfy $1769x + 2378y = d$. Also show that x and y are not unique.

2. By using the Euclidean algorithm, find the greatest common divisor d of 2689 and 4001 and then find integers x and y to satisfy $2689x + 4001y = d$. Also show that x and y are not unique.

3. Find the greatest common divisor d of the numbers 1819 and 3587 using Euclid's algorithm and then find integers x and y to satisfy $1819x + 3587y = d$.

Answers:

1. $GCD(1769,2378) = 29$ and $29 = 1769x + 2378y$ where $x = 39$ and $y = -29$

2. $GCD(2689,4001) = 1$ and $1 = 2689x + 4001y$ where $x = 1662$ and $y = -1117$

3. $GCD(1819,3587) = 17$ and $17 = 1819x + 3587y$ where $x = 71$ and $y = -36$

Prime Numbers

Prime numbers, the building blocks of integers, have been studied extensively over the centuries. Being able to present an integer uniquely as product of primes is the main reason behind the whole theory of numbers and behind the interesting results in this theory. Many interesting theorems, applications and conjectures have been formulated based on the properties of prime numbers.

Definition: A prime is an integer greater than 1 that is only divisible by 1 and itself.

Example: The integers $2, 3, 5, 7, 11$ are prime integers.

Note1: Any integer greater than 1 that is not prime is said to be a composite number.

Note2: 0 and 1 are neither prime nor composite.

Note3: Every composite number can be expressed as the product of prime factors.

Example: 45 can be expressed as

$45 = 3 \times 3 \times 5 = 3^2 \times 5$

$408 = 2 \times 2 \times 2 \times 3 \times 17 = 2^3 \times 3 \times 17$

Number of positive divisors and sum of positive divisors of a positive integer:

Let a be an integer. Suppose prime factorization of a is:

$$a = p_1^{a_1} p_2^{a_2}\, p_3^{a_3} \cdots p_n^{a_n}.$$

The number of all positive divisors of a, denoted by $\tau(a)$, is given by,

$\tau(a) = (1 + a_1)(1 + a_2) \cdots (1 + a_n)$.

The sum of all positive divisors of a, denoted by $\sigma(a)$, is given by,

$\sigma(a) = \left(\frac{p_1^{a_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{a_2+1}-1}{p_2-1}\right) \cdots \left(\frac{p_n^{a_n+1}-1}{p_n-1}\right)$.

Example: Find the number and sum of all positive divisors of 960.

Solution: $960 = 2^6 \times 3 \times 5$

$\therefore p_1 = 2, p_2 = 3, p_3 = 5, a_1 = 6, a_2 = 1, a_3 = 1$

$\tau(960) = (1 + a_1)(1 + a_2)(1 + a_3)$

$\tau(960) = (1 + 6)(1 + 1)(1 + 1)$=28.

$$\sigma(960) = \left(\frac{p_1^{a_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{a_2+1} - 1}{p_2 - 1}\right)\left(\frac{p_n^{a_3+1} - 1}{p_3 - 1}\right)$$

$$\sigma(960) = \left(\frac{2^{6+1} - 1}{2 - 1}\right)\left(\frac{3^{6+1} - 1}{3 - 1}\right)\left(\frac{5^{6+1} - 1}{5 - 1}\right)$$

$\sigma(960) = (127)(4)(6) = 3048$

Properties of prime numbers

(1) The smallest positive divisor (> 1) of any integer $a > 1$ is always a prime number.

(2) There are infinitely many primes OR The number of prime numbers is infinite.

(3) If c and a are relatively prime and $c|ab$ then $c|b$.

(4) If p is a prime number and $p|ab$ where a and b are any integers, then either p$|a$ or $p|b$.

(5) If there exist integers x and y such that $ax + by = 1$, then $(a, b) = 1$.

(6) If $(a, b) = 1$ and $(a, c) = 1$, then $(a, bc) = 1$.

(7) If p is prime and a is any integer then either $(p, a) = 1$ *or* $p|a$.

(8) The smallest positive divisor (>1) of a composite number a does not exceed $\sqrt{a}$.

Exercises

1. Find the number of positive divisors and sum of all positive divisors of 1363.

2. Find the number of positive divisors and sum of all positive divisors of 8128.

3. Check whether 853 is a prime number or not?

4. Prove that there are infinitely many primes.

5. If p is a prime number and $p|ab$ where a and b are any integers, then prove that either p|a or $p|b$.

Answers:

1. Number of divisors = 4

   Sum of divisors = 1440

2. Number of divisors = 14

   Sum of divisors = 16256

3. 853 is a prime number.

The Fundamental Theorem of Arithmetic

Theorem: The Fundamental Theorem of Arithmetic states that every positive integer different from 1 can be written uniquely as a product of primes.

Example: $99 = 3 \times 3 \times 11 = 3^2 \times 11,$

$32 = 2 \times 2 \times 2 \times 2 \times 2 = 2^5.$

Congruences

Congruence is nothing more than a statement about divisibility. The theory of congruences was introduced by Carl Friedrich Gauss. Gauss contributed to the basic ideas of congruences and proved several theorems related to this theory. We start by introducing congruences and their properties.

Definition: Let m be a positive integer. We say that a is congruent to b modulo m if $m \mid (a - b)$ where a and b are integers, i.e. if $a = b + km$ where $k \in Z$.

If a is congruent to b modulo m, we write $a \equiv b(mod\ m)$.

Example 1: $19 \equiv 5(mod\ 7)$.

Example 2: $2k + 1 \equiv 1(mod\ 2)$ which means every odd number is congruent to 1 modulo 2.

There are many common properties between equations and congruences. Some properties are listed in the following theorem.

Theorem: Let a, b, c and d denotes integers. Let m be positive integers. Then:

1. If $a \equiv b(mod\ m)$, then $b \equiv a(mod\ m)$.
2. If $a \equiv b(mod\ m)$ and $b \equiv c(mod\ m)$, then $a \equiv c(mod\ m)$.
3. If $a \equiv b(mod\ m)$, then $a + c \equiv b + c(mod\ m)$.
4. If $a \equiv b(mod\ m)$, then $a - c \equiv b - c(mod\ m)$.
5. If $a \equiv b(mod\ m)$, then $ac \equiv bc(mod\ m)$.
6. If $a \equiv b(mod\ m)$, then $ac \equiv bc(mod\ mc)$, for $c > 0$.
7. If $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$ then $a + c \equiv (b + d)(mod\ m)$.
8. If $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$ then $a - c \equiv (b - d)(mod\ m)$.
9. If $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$ then $ac \equiv bd(mod\ m)$.

Example 1: Compute 6^{100} modulo 7

Solution: We have $6 \equiv -1\ (mod\ 7)$

So $6^{100} \equiv (-1)^{100}\ (mod\ 7)$

$6^{100} \equiv 1\ (mod\ 7)$.

Example 2: Compute 2^{100} modulo 7

Solution: $2^3 \equiv 1\ (mod\ 7)$

Further, we can write $100 = 3 \times 33 + 1$

Thus we have $2^{100} = 2 \times (2^3)^{33}$

$2^{100} \equiv 2 \times (2^3)^{33} \equiv 2 \times 1^{33} \equiv 2\ (mod\ 7)$.

Example 3: Find the remainder when 2^{23} is divided by 47

Solution: $2^8 = 256 \equiv 21(mod\ 47)$

$\therefore (2^8)^2 \equiv (21)^2(mod\ 47)$

$2^{16} \equiv 441(mod\ 47)$

$2^{16} \equiv 18\ (mod\ 47)$ ……..(1)

$2^7 = 128 \equiv 34(mod\ 47)$ ……..(2)

Multiplying (1) and (2). We get

$2^{16} \times 2^7 \equiv 18 \times 34(mod\ 47)$

$2^{23} \equiv 612(mod\ 47)$

$2^{23} \equiv 1(mod\ 47)$

$\therefore$ the remainder is 1.

Exercises

1. Determine the remainder when $53^{103} + 103^{53}$is divisible by 39.

2. Find the remainder obtained when $135 \times 74 \times 48$ is divided by 7

3. What is the remainder in the division of 2^{50} by 7

Answers

1. 0

2. 6

3. 4

Linear congruence:

A congruence of the form $ax \equiv b(mod\ m)$, where x is an unknown integer, is called a linear congruence in one variable.

(i) If $(a, m) = 1$, then the above congruence has a unique solution

(ii) If $(a, m) = d$ and $d|b$ then the above congruence has d incongruent solutions

(iii) If $(a, m) = d$ and $d \nmid b$ then the above congruence has no solution

Example 1: Solve $4x \equiv 5(mod\ 12)$

Solution: This congruence has no solution because

$4x \equiv 5(mod\ 12)$

$\Rightarrow 12|4x - 5$
$\Rightarrow 4x - 5 = 12k$

$$\Rightarrow x = \frac{12k + 5}{4}$$

$\Rightarrow x = 3k + \frac{5}{4}$, where $k \in Z$

This means x can never be an integer.

Example 2: Solve $12x \equiv 6(mod\ 3)$

Solution: This congruence has three incongruent solutions

$x \equiv 0(mod\ 3)$

$x \equiv 1(mod\ 3)$

$x \equiv 2(mod\ 3)$

They are incongruent because $0 \not\equiv 1 \not\equiv 2(mod\ 3)$.

Example 3: Solve $7x \equiv 9(mod\ 15)$

Solution: This congruence has unique solution because

$7x \equiv 9(mod\ 15)$

$\Rightarrow 15|7x - 9$
$\Rightarrow 7x - 9 = 15k$

$\Rightarrow x = \frac{15k+9}{7}$, where $k \in Z$

By inspection $k = 5$ gives $x = 12$.

$\therefore x \equiv 12(mod\ 15)$

Exercises

1. Examine if the linear congruence $7x \equiv 13(mod\ 24)$ has unique solution, and hence solve it.

2. If $2x \equiv 3(mod\ 7)$, find x such that $9 \leq x \leq 30$.

3. Examine if the linear congruence $3x \equiv 2(mod\ 10)$ has unique solution, and hence solve it.

Answers

1. $x \equiv 19(mod\ 24)$, the congruence has unique solution.

2. $x = 12,19,26$
3. $x \equiv 4(mod\ 10)$, the congruence has unique solution.

Multiplicative inverse modulo m

A multiplicative inverse of a modulo m is an integer v such that $av \equiv 1(mod\ m)$.

For example: 5 is a multiplicative inverse of 2 modulo 9 because $2 \times 5 \equiv 1\ (mod\ 9)$.

Euler phi function or Euler totient function

The number $\phi(m)$ is the number of positive integers less than or equal to m that are relatively prime to m.

ϕ is called Euler's – phi function or totient.

Properties

1. If p is a prime number then $\phi(p) = p - 1$

2. If p is a prime number and $k > 0$, then $\phi(p^k) = p^k - p^{k-1}$

3. If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_r^{k_r}$ then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$$

Example1: $\phi(5) = 4$.

1,2,3 and 4 are relatively prime to 5

Example 2: $\phi(9) = \phi(3^2) = 3^2 - 3 = 6$.

1,2,4,5,7,8 are relatively prime to 9.

Example 3: Calculate $\phi(360)$

$\phi(360) = \phi(2^3 3^2 5)$

$$\phi(360) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 96$$

Euler's Theorem

Euler's theorem states that if $(a, m) = 1$, then $a^{\phi(m)} \equiv 1\ (mod\ m)$.

Example1: Find the last digit of 55^5.

Solution: We note that $gcd(10, 55) = 5$, and hence this pair is not relatively prime, however, we know that 55 has a prime power decomposition of $55 = 5 \times 11$.

$gcd(11, 10) = 1$, hence it follows that

$11^{\phi(10)} \equiv 1\ (mod\ 10)$. We note that $\phi(10) = 4$. Hence $11^4 \equiv 1\ (mod\ 10)$, and more appropriately $55^5 = 5^5.11^5 = 5^5.11^4.11 \equiv 5^5.(1)^4.11 \equiv 34375 \equiv 5\ (mod\ 10)$

Hence the last digit of 55^5 is 5.

Example 2: Find the last two digits of 3333^{4444}.

Solution: We first note that finding the last two digits 3333^{4444} can be obtained by reducing $3333^{4444}(mod\ 100)$. Since $gcd(3333, 100) = 1$, we can apply Euler's theorem.

We first calculate that $\phi(100) = \phi(2^2 \times 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$.

Hence it follows from Euler's theorem that $3333^{40} \equiv 1\ (mod\ 100)$.

Let's apply the division algorithm on 4444 and 40 as follows:

$4444 = 40(111) + 4$

Hence it follows that:

$3333^{4444} \equiv (3333^{40})^{111}.3333^4 \equiv (1)^{111}.3333^4\ (mod\ 100)$

$3333^{4444} \equiv 33 \times 33 \times 33 \times 33\ (mod\ 100)$

$3333^{4444} \equiv 33^4 (mod\ 100) = 1185921 (mod\ 100)$

$3333^{4444} \equiv 21\ (mod\ 100)$

Hence the last two digits of 3333^{4444} are 2 and 1.

Cryptography

In the age of the internet, when we use the internet to conduct business transactions, check our bank account, use credit cards to buy things online, and take cash out of an ATM, security technologies such as armed guards and X-ray machines simply don't work. The danger with modern internet transactions is that you must send private data through a public network in order to reach its destination, such as your bank. The problem with this is that anyone can intercept read the message you have sent.

An internet-based economy therefore requires a new kind of security technology in order to protect information people send online. Actually, the field of information protection – known as "cryptography" or "hidden writing" – is not new. It dates back several thousand years.

Cryptography is the process of transferring information securely, in a way that no unwanted third party will be able to understand the message. It has been used for thousands of years. Number theory and Cryptography are inextricably linked, as we shall see in the following section.

RSA algorithm to encrypt and decrypt

RSA Algorithm is used to encrypt and decrypt data in modern computer systems and other electronic devices. RSA algorithm is an asymmetric cryptographic algorithm as it creates 2 different keys for the purpose of encryption and decryption. It is public key cryptography as one of the keys involved is made public. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman who first publicly described it in 1978. RSA makes use of prime numbers (arbitrary large numbers) to function. The public key is made available publicly (means to everyone) and only the person having the private key with them can decrypt the original message.

Working procedure of RSA Public key

RSA involves use of public key and private key for its operation. The keys are generated using following steps:

1. Two prime numbers are selected as p and q.

2.$n = pq$, which is the modulus of both the keys

3. Calculate the totient $= (p-1)(q-1)$

4. Choose e such that $e > 1$ and coprime to totient which means gcd $(e, totient)$ must be equal to 1, e is the public key

5. Choose d such that it satisfies the equation $de = 1 + k(totient)$, d is the private key not known to everyone

6. Cipher text is calculated using the equation $c = m^e (mod\ n)$, where m is the message.

7. With the help of c and d we decrypt message using the equation $m = c^d (mod\ n)$, where d is the private key.

A very simple example of RSA encryption

1. Select primes $p = 11, q = 3$.

2. $n = pq = 11 \times 3 = 33$

$\phi = (p-1)(q-1) = (11-1)(3-1) = 20$

3. Choose $e = 3$.

$gcd(e, p-1) = gcd(3, 10) = 1$

$gcd(e, q-1) = gcd(3, 2) = 1$

$\therefore gcd(e, \phi) = gcd(e, (p-1)(q-1)) = gcd(3, 20) = 1$

4. Compute d such that $ed \equiv 1\ (mod\ \phi)$

Compute $d = (1/e)\ (mod\ \phi) = (1/3)\ (mod\ 20)$

Find a value for d such that ϕ divides $(ed-1)$

Find d such that 20 divides $3d - 1$.

Simple testing $(d = 1, 2, \cdots)$ gives $d = 7$

$ed - 1 = 3 \times 7 - 1 = 20$, which is divisible by ϕ.

5. Public key $= (n, e) = (33, 3)$

Private key $= (n, d) = (33, 7)$

This is actually the smallest possible value for the modulus n for which the RSA algorithm works.

Now say we want to encrypt the message $m = 7$

$c = m^e (mod\ n) = 7^3 mod\ 33 = 343\ mod\ 33 = 13$

Hence the cipher text c $= 13$.

To check decryption, we compute

$m = c^d (mod\ n) = 13^7 mod\ 33 = 7$

If we wanted to use this system to keep secrets, we could let $A = 2, B = 3, \cdots, Z = 27$. Thus the plaintext message "**HELLO**" would be represented by the set of integers $m_1, m_2, \cdots$

(9,6,13,13,16)

For the encryption of the letter $H = 9$, we use
$c_1 = m^e (mod\ n) = 9^3 mod\ 33 = 729\ mod\ 33 = 3$

For the encryption of the letter $E = 6$, we use
$c_2 = m^e (mod\ n) = 6^3 mod\ 33 = 216\ mod\ 33 = 18$

For the encryption of the letter $L = 13$, we use
$c_3 = m^e (mod\ n) = 13^3 mod\ 33 = 2197\ mod\ 33 = 19$

For the encryption of the letter $O = 16$, we use
$c_4 = m^e (mod\ n) = 16^3 mod\ 33 = 4096\ mod\ 33 = 4$

We obtain cipher text integers $c_1, c_2, \cdots$

(3,18,19,19,4)

Therefore the cipher text is **BQRRC.**

Exercises

1. Given the public key $(e, n) = (7,55)$, encrypt plain text **PLAN,** where the alphabets $A, B, C, \ldots X, Y, Z$ are assigned the numbers $2,3, \cdots, 26,27$. Give the cipher text. Find the private key d.

2. Given the public key $(e, n) = (7,85)$, encrypt plain text **HI,** where the alphabets $A, B, C, \ldots X, Y, Z$ are assigned the numbers $2,3, \cdots, 26,27$. Give the cipher text. Find the private key d.

Answers:

1. Cipher text is **GFQD** $(8,7,18,5)$ and private key $d = 23$.

2. Cipher text is **RD** $(19, 5)$ and private key $d = 55$.