CHAPTER 6

Number Theory

6.1 INTRODUCTION

Since ancient times, the study of number systems especially prime numbers has fascinated mathematicians. On the other hand due to increase of internet for communication there is a need for security in the transmission of information. In the last twenty five years, there are number of discoveries of new mathematical methods. This helps to increase the computation speed. Number system is the base of cryptographic algorithms. It is difficult to find out the largest prime number as there is no simple and efficient algorithms are available to find out such prime number. The strength of any encryption algorithm depends on the selection of various parameters, i.e., numbers. The most secure methods for transmission of information depends on properties of prime number. This chapter provides the basic of number theory which is useful for different cryptographic algorithms. In this chapter, we are going to discuss about prime numbers, modular arithmetic, Fermat's theorem, Euler's theorem, Euclidean algorithm, different methods for primality test, Chinese remainder theorem, discrete logarithms.

6.2 PRIME NUMBERS

We learn about various classical and symmetric encryption techniques. Every one of us knows about prime number. To design a strong encryption algorithm, prime number plays a very important role. So in cryptography, prime number has its own important role. A positive integer number which is greater than 1 and has no factors other than 1 and that number itself is called a *prime number*. In other word, the number which is divisible only by itself and 1 called prime number. Prime numbers are always positive integers. For example, 2, 3, 5, 7, 11, 13. These numbers have the factors as 1 and itself only. If we consider the number 14, the factors are 1, 2, 7 and 14. So, 14 is not a prime number. Positive integer numbers greater than 2, which are not prime

numbers, are called *composite numbers*. The smallest prime numbers less than 50 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 and 47. The integer number 1 is neither prime nor composite. There are infinite numbers of prime numbers.

6.2.1 Relative Prime Numbers

Two numbers are called relatively prime if the greatest common divisor (GCD) of those numbers is 1. The numbers 8 and 15 are relatively prime number, in respect to each other. The factors of 8 are 1, 2, 4, 8 and the factors of 15 are 1, 3, 5 15. Examples of relatively prime numbers are: (10, 21), (14, 15), (45, 91), ...

The greatest common divisor (GCD) of two numbers can be determined by comparing their prime factors and selecting the least powers of the factor. For example, the two numbers are 81 and 99.

The factors of these numbers are:

$$81 = 1 * 9 * 9 = 1 * 3 * 3 * 3 * 3 = 1 * 3^4$$

$$99 = 1 * 3 * 33 = 1 * 3 * 3 * 11 = 1 * 3^2 * 11$$

The GCD is the least power of a number in the factors,

So, $$GCD(81, 99) = 1 * 3^2 * 11^0 = 9$$

(If the GCD of two numbers is 1, then those numbers are relatively prime.)

Therefore, 81 and 99 are not relatively prime numbers.

For example, two relative prime numbers are 45 and 91.

The factors of these numbers are:

$$45 = 1 * 3 * 3 * 5 = 1 * 3^2 * 5$$

And $$91 = 1 * 7 * 13$$

So, $$GCD(45, 91) = 1$$

Therefore, 45 and 91 are relatively prime numbers. It is not necessary that both the numbers should be prime number. A prime number is also relatively prime number to any other number other than itself and 1. Large prime number provides more security in cryptography.

6.3 MODULAR ARITHMETIC

We are familiar to find out the mod of any number with some base. Suppose we have to find out the mod of a number m with base n as:

$$m \bmod n$$

The mod with respect to n is $(0, 1, 2, \ldots n - 1)$.

Suppose $m = 23$ and $n = 9$, then

$$23 \bmod 9 = 5$$

For any value of m, the value of $m \bmod 9$ is from $(0, 1, 2, \ldots 8)$.

If m is negative, suppose $m = -15$, then

$$-15 \bmod 9 = -6 \bmod 9$$
$$= (9 - 6) \bmod 9$$
$$= 3 \bmod 9$$

Table 6.1 shows the value of m mod 9 for different values of m.

Table 6.1 Values of m mod 9

18	19	20	21	22	23	24	25	26
9	10	11	12	13	14	15	16	17
0	1	2	3	4	5	6	7	8
9	–8	–7	–6	–5	–4	–3	–2	–1
–18	–17	–16	–15	–14	–13	–12	–11	–10
–27	–26	–25	–24	–23	–22	–21	–20	–19

6.3.1 Properties

1. *Addition of modular number*
The addition of two numbers p and q with same modular base n is:

$$(p \bmod n + q \bmod n) \bmod n = (p + q) \bmod n$$

For example:

$$15 \bmod 9 + 17 \bmod 9 = (15 \bmod 9 + 17 \bmod 9) \bmod 9$$
$$= (6 + 8) \bmod 9$$
$$= 14 \bmod 9 = 5$$

OR

$$15 \bmod 9 + 17 \bmod 9 = (15 + 17) \bmod 9$$
$$= (32) \bmod 9 = 5$$

2. *Subtraction of modular number*
The subtraction of two numbers p and q with same modular base n is:

$$(p \bmod n - q \bmod n) \bmod n = (p - q) \bmod n$$

For example:

$$17 \bmod 9 - 15 \bmod 9 = (17 \bmod 9 - 15 \bmod 9) \bmod 9$$
$$= (8 - 6) \bmod 9$$
$$= 2 \bmod 9 = 12$$

OR

$$17 \bmod 9 - 15 \bmod 9 = (17 - 15) \bmod 9$$
$$= 2 \bmod 9 = 2$$

3. *Multiplication of modular number*
The multiplication of two numbers p and q with same modular base n is:

$$(p \bmod n * q \bmod n) \bmod n = (p * q) \bmod n$$

For example:

$$17 \bmod 9 * 15 \bmod 9 = (17 \bmod 9 * 15 \bmod 9) \bmod 9$$
$$= (8 * 6) \bmod 9$$
$$= 48 \bmod 9 = 3$$

OR

$$17 \bmod 9 * 15 \bmod 9 = (17 * 15) \bmod 9$$
$$= (255) \bmod 9 = 3$$

Note: $m^a \bmod n = m^{pq} \bmod n$ where $a = p * q$
$= (m^p \bmod n)^q \bmod n$

EXAMPLE 6.1 Find the value of $7^7 \bmod 9$.

Solution $7^7 \bmod 9 = (7^2)^3 * 7 \bmod 9$
$= (7^2 \bmod 9)^3 \bmod 9 * 7 \bmod 9$
$7^2 \bmod 9 = 49 \bmod 9 = 4$
$7^6 \bmod 9 = (7^2)^3 \bmod 9 = 4^3 \bmod 9 = 64 \bmod 9 = 1$
$7^7 = 7^6 * 7 \bmod 9 = 1 * 7 \bmod 9 = 7$

EXAMPLE 6.2 Find $3^{110} \bmod 13$

Solution $3^1 \bmod 13 = 3$
$3^2 \bmod 13 = 9 \bmod 13 = 9$
$3^3 \bmod 13 = 27 \bmod 13 = 1$

Now, 3^{110} may be split into: $3^{108} * 3^2$ (since 108 is divisible by 3)
$3^{108} \bmod 13 = (3^3)^{36} \bmod 13 = 1^{36} \bmod 13 = 1$ (since $3^3 \bmod 13 = 1$)

Therefore, $3^{110} = 3^{108} * 3^2 \bmod 13$
$= 1 * 9 \bmod 13$
$= 9 \bmod 13 = 9$

EXAMPLE 6.3 Find the value of unit place digit of 51^{51}.

Solution We know that unit place digit can be found by taking mod 10 of the given number.

Here, $51 \bmod 10 = 1$

Therefore, $51^{51} \bmod 10 = 1^{51} \bmod 10 = 1$

Therefore, the unit place digit of 51^{51} is 1.

EXAMPLE 6.4 Find the value of final digit (LSB) of $(((((((7^7)^7)^7)^7)^7)^7)^7)^7$?

Solution To find out the LSB we have to take mod 10 for the given value.

We first find out

$$7^2 \bmod 10 = 49 \bmod 10$$
$$= 9 \bmod 10$$
$$= (-1) \bmod 10 \quad \text{(since } 9 \bmod 10 = -1 \bmod 10\text{)}$$

We know that

$$7^7 = (7^2)^3 * 7$$
$$7^7 \bmod 10 = (7^2)^3 * 7 \bmod 10$$
$$= (-1)^3 * 7 \bmod 10 \quad \text{(since } 7^2 \bmod 10 = -1\text{)}$$
$$= -7 \bmod 10$$

Now,

$$(7^7)^7 \bmod 10 = (-7)^7 \bmod 10$$
$$= (-1)^7(7)^7 \bmod 10$$
$$= -1 * (-7) \bmod 10 \quad \text{(since } 7^7 \bmod 10 = -7\text{)}$$
$$= 7 \bmod 10$$

Now, $((7^7)^7)^7 \bmod 10 = (7)^7 \bmod 10$ (since $(7^7)^7 \bmod 10 = 7$)
$= -7 \bmod 10$ (since $7^7 \bmod 10 = -7$)

Now, $(((7^7)^7)^7)^7 \bmod 10 = (-7)^7 \bmod 10$ (since $((7^7)^7)^7 \bmod 10 = -7$)
$= (-1)^7\ (7)^7 \bmod 10$
$= -\ (-7) \bmod 10$ (since $7^7 \bmod 10 = -7$)
$= 7 \bmod 10$

As 7 to the power 7 for odd number of times answer is $-7 \bmod 10$ and even number of times answer is $7 \bmod 10$

Therefore, $(((((((7^7)^7)^7)^7)^7)^7)^7)^7 = -7 \bmod 10$
$= 3 \bmod 10$
$= 3$

6.4 FERMAT'S THEOREM

Fermat's theorem is one of the most important theorems in cryptography. It is also known as Fermat's Little theorem. It is useful in public key encryption techniques and primality testing.

Fermat's theorem states that if p is a prime number and n is a positive integer number which is not divisible by p, then

Therefore,

$$n^p = n \bmod p$$
$$n^{p-1} = 1 \bmod p$$
$$n^{p-1} \bmod p = 1$$

where p is prime and GCD $(n, p) = 1$ (6.1)

Fermat's theorem $n^{P-1} = 1 \bmod p$

EXAMPLE 6.5 Suppose, the prime number $p = 7$ and a positive integer number $n = 3$ then prove Fermat's Little theorem.

Solution Using Fermat's Little theorem (Equation 6.1), we have:

$$3^{7-1} \bmod 7 = 3^6 \bmod 7$$
$$= 729 \bmod 7$$
$$= 1$$

Therefore, $3^{7-1} \bmod 7 = 1$
Hence, the theorem is proved.

EXAMPLE 6.6 Suppose $n = 7$ and $p = 19$ then prove Fermat's Little theorem.

Solution Using Equation (6.1), we have:

$$7^{19} \bmod 19 = 1$$
$$7^2 = 49 \bmod 19 = 11 \pmod{19}$$
$$7^4 = (7^2)^2 = (11)^2 = 121 = 7 \pmod{19}$$
$$7^8 = (7^4)^2 = (7)^2 = 49 \bmod 19 = 11 \pmod{19}$$
$$7^{16} = (7^8)^2 = (11)^2 = 121 \bmod 19 = 7 \pmod{19}$$
$$n^{p-1} = 7^{18} = 7^{16} \times 7^2 = 7 \times 11 = 77$$
$$n^{p-1} \pmod{p} = 77 \pmod{19} = 1$$

Hence proved.

EXAMPLE 6.7 Find the smallest positive residue y in the following congruence.

$$7^{69} = y \bmod 23$$

Solution Here $n = 7$ and $p = 23$ as p is prime number and we can apply Fermat's Little theorem to solve this problem.

Fermat's Little theorem is

$$n^{p-1} = 1 \bmod p$$

By substituting the values of n and p and rewrite the equation:

$$7^{(23-1)} = 1 \bmod 23$$
$$7^{(22)} = 1 \bmod 23$$

We can write 7^{69} as $(7^{22})^3 * 7^3$
Therefore,

$$7^{69} = y \bmod 23$$

And can be written as:

$$7^{69} = 7^{66} * 7^3$$
$$7^{69} = (7^{22})^3 * 7^3 \bmod 23$$
$$7^{69} = (1)^3 * 7^3 \bmod 23$$
$$7^{69} = 343 \bmod 23$$

Therefore, the smallest positive residue $y = 343$.

EXAMPLE 6.8 Find the smallest positive residue y in the following congruence.

$$3^{101} = y \bmod 13$$

Solution Here $n = 3$ and $p = 13$ as p is prime number and we can apply Fermat's Little theorem to solve this problem.

Fermat's Little theorem is

$$n^{p-1} = 1 \bmod p$$

By substituting the values of n and p and rewrite the equation:

$$3^{(13-1)} = 1 \bmod 13$$

$$3^{(12)} = 1 \bmod 13$$

We can write 3^{101} as $(3^{12})^8 * 3^5$

Therefore, $3^{101} = y \bmod 13$

And can be written as:

$$3^{101} = 3^{96} * 3^5$$

$$3^{101} = (3^{12})^8 * 3^5 \bmod 13$$

$$3^{101} = (1)^8 * 3^5 \bmod 13$$

$$3^{101} = 243 \bmod 13$$

$$3^{101} = 9 \bmod 13$$

Therefore, the smallest positive residue $y = 9$.

6.4.1 An Application of Fermat's Little Theorem and Congruence

Suppose a positive integer be p and two integers x and y are congruent mod p. This is shown as:

$$x \equiv y \bmod p \qquad \text{if } p \mid (x - y)$$

For example:

(i) $5 \equiv 2 \bmod 3$

(ii) $12 \equiv \bmod 19$

(iii) $23 \equiv -1 \bmod 12$

(iv) $-8 \equiv 0 \bmod 4$

Properties

Suppose p is a positive integer number and w, x, y, z are the integers then it follows following properties:

1. $x \equiv x \bmod p$.
2. If $x \equiv y \bmod p$, then $y \equiv x \bmod p$.
3. If $x \equiv y \bmod p$ and $y \equiv z \bmod p$, then $x \equiv z \bmod p$.

4. (a) If $x \equiv Ap + B \bmod p$, then $x \equiv B \bmod p$.
   (b) Every integer x is congruent with mod p to exactly one of 0, 1, 2, ..., $p - 1$.
5. If $x \equiv y \bmod p$ and $z \equiv w \bmod p$, then $x \pm z \equiv y \pm w \bmod p$ and $xz \equiv yw \bmod p$.
6. If $(z, p) = 1$ and $xz \equiv yz \bmod p$, then $x \equiv y \bmod p$.

To find all the solutions of the congruence $zx \equiv y \bmod p$, following steps should be followed.

Step 1 Calculate the GCD of z and p. If the GCD is not equal to 1, then there is no solutions for the said congruence.

Step 2 If GCD is 1, find the multiplicative inverse of $z \bmod p$.

Step 3 Write the equation as $x = y * w \bmod p$, where w is the multiplicative inverse of $z \bmod p$.

After solving Step 3, we get the solution of the congruence in terms of $x = \bmod p$.

EXAMPLE 6.9 Find all solutions of the following congruence.

$$4x = 8 \bmod 11$$

Solution

1. Calculate the GCD of 4 and 11.

$$\text{GCD}(4, 11) = 1$$

2. As GCD is 1, find the multiplicative inverse.
   The multiplicative inverse of $1 = 4 \bmod 11$ is 3. (As $4 * 3 = 12 \bmod 11 = 1$)
3. $x = 8 * 3 \bmod 11$
   $x = 2 \bmod 11$

All the solutions of the given congruence is $x = 2 \bmod 11$.

EXAMPLE 6.10 Find all solutions of the following congruence.

$$2x = 7 \bmod 10$$

Solution

1. Calculate the GCD of 2 and 10.

$$\text{GCD}(2, 10) = 2$$

2. As GCD is 2, the theorem cannot be apply directly.
   $2x = 7 \bmod 10$ is equivalent to $2x - 10y = 7$. This is not possible as LHS is divisible by 2 whereas RHS is not divisible by 2.

So, there is no solution for the given congruence $2x = 7 \bmod 10$.

EXAMPLE 6.11 Find the last digit (unit place digit) of $(7654321)^{23456789}$.

Solution: We know that the unit place digit can be calculated by taking mod 10 of the given number.

Therefore, $7654321 = 1 \bmod 10$

Therefore, $(7654321)^{23456789} = (1)^{23456789} = 1 \bmod 10$

Therefore, the last digit (unit place digit) of $(7654321)^{23456789}$ is 1.

EXAMPLE 6.12 Compute the value of $12345^{23456789} \bmod 101$.

Solution By Fermat's Little theorem $n^{p-1} = 1 \bmod p$ where $n = 12345$ and $p = 101$.

$$12345^{(101-1)} \bmod 101 = 1$$

$$12345^{100} \bmod 101 = 1$$

Therefore, $12345^{23456789} \bmod 101 = (12345^{100})^{234567} * 12345^{89} \bmod 101$

$$= 1 * 12345^{89} \bmod 101$$

$$= 12345^{89} \bmod 101$$

But $12345 \bmod 101 = 23$

Therefore, $23^{89} \bmod 101$

$$23 \bmod 101 = 23$$

$$23^2 \bmod 101 = 24$$

$$23^3 \bmod 101 = 47$$

$$23^4 \bmod 101 = 71$$

$$23^5 \bmod 101 = 17$$

$$23^7 \bmod 101 = 4$$

$$23^{89} \bmod 101 = (23^7)^{12}\ 23^5 \bmod 101$$

$$= 4^{12} * 17 \bmod 101$$

$$= 5 * 17 \bmod 101$$

$$= 85$$

Therefore, the value of $12345^{23456789} \bmod 101 = 85$.

6.5 EULER'S THEOREM

Before discussing Euler's theorem, we first take a look on Euler totient function. In cryptography, Euler's totient function plays an important role. The totient of a positive integer n is the total number of the positive integer numbers which are less than n and are relatively prime to n. It is shown as $\Phi(n)$, where $\Phi(n)$ is the number of positive integers less than n and relative prime to n.

If $n = 8$, the positive integers less than 8 are 1, 2, 3, 4, 5, 6, 7. Out of these numbers, only 1, 3, 5 and 7 are relatively prime to 8. These numbers do not have any factors common with 8. There are total four such numbers which are relatively prime to 8, therefore $\Phi(8) = 4$.

Take another number $n = 7$, where 7 is the prime number. The positive integers less than 7 are 1, 2, 3, 4, 5, 6, 7. As 7 is a prime number, all the positive integers from 1 to 7 are relatively prime to 7. Thus, $\Phi(7) = 6$. For any prime number n, $\phi(n) = n - 1$.

We can see the totient function for some more numbers as:

$\Phi(3) = 2$ (numbers relatively prime to 3 are 1, 2)

$\Phi(4) = 2$ (numbers relatively prime to 4 are 1, 3)

$\Phi(5) = 4$ (numbers relatively prime to 5 are 1, 2, 3, 4)

$\Phi(6) = 2$ (numbers relatively prime to 6 are 1, 5)

$\Phi(9) = 4$ (numbers relatively prime to 9 are 1, 2, 4, 5)

$\Phi(10) = 4$ (numbers relatively prime to 10 are 1, 3, 7, 9)

$\Phi(11) = 10$ (numbers relatively prime to 11 are 1, 2, 3, 4, 5, 6, 7, 8, 9, 10)

$\Phi(n)$ = Total numbers between 1 and n–1 which are relatively prime to n.

As you can see from the above examples that if n is a prime number $\Phi(n) = n - 1$. This helps to calculate the totient function when the factors of n are two different prime numbers. For example, suppose n has two factors A and B, where A and B are primes, then

$$\begin{aligned}\Phi(n) &= \Phi(A * B)\\ &= \Phi(A) * \Phi(B)\\ &= (A - 1)*(B - 1)\end{aligned}$$

EXAMPLE 6.13 To find the totient function of $n = 91$.

Solution
$$\begin{aligned}\Phi(91) &= \Phi(13 * 7)\\ &= \Phi(13) * \Phi(7)\\ &= (13 - 1)*(7 - 1)\\ &= 12 * 6\\ &= 72\end{aligned}$$

Thus, using above properties it is easy to find out the totient function of a large number whose factors are two prime numbers.

$$\Phi(n) = \Phi(A * B) = \Phi(A) * \Phi(B) = (A - 1) * (B - 1)$$

If A and B are prime numbers

6.5.1 The General Formula to Compute $\Phi(n)$

For a prime number A, the totient function is $\Phi(A) = A - 1$ (because all the numbers less than A are relatively prime to A).

If $B = A^p$, then the numbers which have a common factor with B are the multiples of A. These factors are: A, AA, AAA, ... $(A^{p-1})A$. There is total A^{p-1} multiples of A. Therefore, total number of factors relatively prime to A^p is

$$\begin{aligned}\Phi(A^p) &= A^p - A^{p-1} \\ &= A^{p-1}(A-1) \\ &= A * A^{p-1}\left(1-\frac{1}{A}\right) \\ &= A^p\left(1-\frac{1}{A}\right)\end{aligned}$$

Consider a general form, B is divisible by A. Let $\Phi_A(B)$ be the positive integer number $\leq B$ but not divisible by A and have common factors as: A, $2A$, ... $(B/A)B$.

$$\begin{aligned}\Phi_A(B) &= B - \frac{B}{A} \\ &= B\left(1-\frac{1}{A}\right)\end{aligned}$$

Now, C is the prime number which is dividing B. The integer numbers which are divisible by C are C, $2C$, ... $(B/C)C$. But this duplicate AC, $2AC$, ... $(B/(AC))AC$. So, the total number of terms that must be subtracted from Φ_A to obtain Φ_{AC} is

$$\begin{aligned}\Delta\Phi_C(B) &= \frac{B}{C} - \frac{B}{AC} \\ &= \frac{B}{C}\left(1-\frac{1}{A}\right) \text{ and} \\ \Phi_{AC}(B) &= \Phi_A(B) - \Delta\Phi_C(B) \\ &= B\left(1-\frac{1}{A}\right) - \frac{B}{C}\left(1-\frac{1}{A}\right) \\ &= B\left(1-\frac{1}{A}\right)\left(1-\frac{1}{C}\right)\end{aligned}$$

By induction, the general case is then

$$\Phi(n) = n\prod_{A|n}\left(1-\frac{1}{A}\right)$$

The generalise formula to calculate $\Phi(n)$ of a number n is:

$$\Phi(n) = A_1^{m_1} * A_2^{m_2} * A_3^{m_n} * \ldots * A_n^{m_n}$$

$$\phi(n) = n * \left(1-\frac{1}{A_1}\right) * \left(1-\frac{1}{A_2}\right) * \left(1-\frac{1}{A_3}\right) * \ldots \left(1-\frac{1}{A_n}\right)$$

$\Phi(n^m) = n^{m-1}\Phi(n)$ [identity relating to $\Phi(n^m)$ to $\Phi(n)$]

For example, $\Phi(43) = 43 - 1 = 42$

$$\Phi(21) = \Phi(3 \times 7) = \Phi(3) \times \Phi(7) = (3 - 1) \times (7 - 1) = 2 \times 6 = 12$$

$$4 = 2^2,\ \Phi(4) = 4 * \left(1 - \frac{1}{2}\right) = 2$$

$$15 = 3 * 5,\ \Phi(15) = 15 * \left(1 - \frac{1}{3}\right) * \left(1 - \frac{1}{5}\right) = 15 * \left(\frac{2}{3}\right) * \left(\frac{4}{5}\right) = 8$$

EXAMPLE 6.14 If $n = 9$, find $\Phi(n)$.

Solution $9 = 3^2$, here $A = 3$

$$\Phi(9) = 9 * \left(1 - \frac{1}{3}\right)$$

$$= 9 * \left(\frac{2}{3}\right)$$

$$= 6$$

EXAMPLE 6.15 If $n = 75$, find $\Phi(n)$.

Solution $75 = 5 * 15$

$$= 5 * 5 * 3$$

$$= 5^2 * 3;\ \text{here } A_1 = 5 \text{ and } A_2 = 3$$

$$\Phi(75) = 75 * (1 - 1/5) * \left(1 - \frac{1}{3}\right)$$

$$= 75 * \left(\frac{4}{5}\right) * \left(\frac{2}{3}\right)$$

$$= 40$$

Therefore, $\Phi(75) = 40$.

EXAMPLE 6.16 If $n = 5488$, find $\Phi(n)$.

Solution $5488 = 16 * 343$

$$= 2^4 * 7^3;\ \text{here } A_1 = 2 \text{ and } A_2 = 7$$

$$= 5488 * \left(1 - \frac{1}{2}\right) * \left(1 - \frac{1}{7}\right)$$

$$= 5488 * \left(\frac{1}{2}\right) * \left(\frac{6}{7}\right)$$

$$= 2352$$

$$\Phi(n) = A_1^{m_1} * A_2^{m_2} * A_3^{m_n} * \ldots * A_n^{m_n}$$

$$= n * \left(1 - \frac{1}{A_1}\right) * \left(1 - \frac{1}{A_2}\right) * 1 - \frac{1}{A_3} * \ldots \left(1 - \frac{1}{A_n}\right)$$

Thus, when we calculate arithmetic modulo n, we get a complete set of residues as (0, 1, 2, ..., $n - 1$). From this set of residues, the numbers which are relatively prime to n forms a set called the *reduced set of residues*.

For example, if $n = 15$, the complete set of residues is $r_1 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$ and the reduced set of residues is $r_2 = \{1, 2, 4, 7, 8, 11, 13, 14\}$. All the numbers from set r_2 are relatively prime to 15. The total count of number in r_2 is called the *Euler totient function* $\Phi(n)$.

Based on the above explanations, the Euler's theorem state that for every a and n that are relatively prime:

$$a^{\Phi(n)} = 1 \bmod(n)$$

$$a = 3;\ n = 8$$

$$\Phi(8) = 4$$

$$3^4 = 81 = 1 \bmod 8$$

where $\Phi(n)$ equals Euler's totient function.

Euler's totient theorem generalises Fermat's theorem. This theorem is an important key to the RSA algorithm. If GCD(a, n) = 1, and $a < n$, then $a^{\Phi(n)} = 1(\text{mod } n)$. In other words, if a and n are relatively prime, with a being the smaller integer, and when we multiply a with itself $\Phi(n)$ times and divide the result by n, the remainder will be 1.

For any number n, let the reduced set of residues be $\{r_1, r_2, r_3, \ldots, r_p\}$ then totient function = $\Phi(n) = p$. Multiply each remainder by a and divide by n.

$$r_p a = q_p n + r_p \Phi(n)$$

where r_p is a positive integer less than n.

Then r'_i is relatively prime to n because any common factor of $q_i n$ and r'_i would be a factor of *ria*.

$$ria = r'_i \bmod (n)$$

Two different remainders r_i and r_j cannot have the same congruence. Therefore, r_i and r'_i run through the same set of remainders.

EXAMPLE 6.17 Let $n = 9$, $a = 5$. Show that $a^{\Phi(n)} \bmod(n) = 1$.

Solution The totient value of 9 is $\Phi(9) = 6$. Therefore, the residues of 9 which are relatively prime to 9 are: 1, 2, 4, 5, 7, 8. Multiply all remainders by $a = 5$ and congruence mod($n = 9$).

$$1a = 5 \bmod 9 = 5$$

$$2a = 10 \bmod 9 = 1$$

$$4a = 20 \bmod 9 = 2$$

$$5a = 25 \bmod 9 = 7$$

$$7a = 35 \bmod 9 = 8$$

$$8a = 40 \bmod 9 = 4$$

Multiplying all congruence together:

$$5^6(1)(2)(4)(5)(7)(8) \bmod(9) = (5)(1)(2)(7)(8)\ (4)\bmod(9)$$

$5^6 \bmod(9) = 1 \bmod(10)$

$5^{\Phi(9)} \bmod(9) = 1 \bmod(10)$ (since $6 = \Phi(9)$)

This prove the Fermat's little theorem.

EXAMPLE 6.18 Let $n = 15$, $a = 8$. Show that $a^{\Phi(n)} \bmod(n) = 1$.

Solution The totient value of $\Phi(15) = 8$. Therefore, the residues of 15 which are relatively prime to 15 are 1, 2, 4, 7, 8, 11, 13, 14. Multiply all remainders by $a = 8$ and congruence mod($n = 15$).

$$1a = 8 \bmod 15 = 8$$
$$2a = 16 \bmod 15 = 1$$
$$4a = 32 \bmod 15 = 2$$
$$7a = 56 \bmod 15 = 11$$
$$8a = 64 \bmod 15 = 4$$
$$11a = 88 \bmod 15 = 13$$
$$13a = 104 \bmod 15 = 14$$
$$14a = 112 \bmod 15 = 7$$

Multiplying all congruence together:

$$8^8(1)(2)(4)(7)(8)(11)(13)(14) \bmod(15) = (1)(2)(4)(7)(8)(11)(13)(14) \bmod(15)$$
$$8^8 \bmod(15) = 1 \bmod(15)$$
$$8\Phi^{(15)} \bmod(15) = 1 \bmod(15) \text{ (since } 8 = \Phi(15))$$

This prove the Fermat's little theorem.

6.6 EUCLIDEAN ALGORITHM

GCD is a common problem in number theory. Suppose p and q are two numbers. GCD (p, q) is the largest number that divides evenly both p and q. Euclidean algorithm is used to compute the greatest common divisor (GCD) of two integer numbers. This algorithm is also known called as *Euclid's algorithm*. It is named after the Greek mathematician Euclid. This algorithm has many theoretical and practical applications. In modern number theory, this theorem uses as a basic tool for proving theorems.

Euclid theorem: GCD(p, q) = GCD(q, p mod q)

Euclid's algorithm to compute GCD(p, q):

```
n = p, m = q
while m > 0
r = n mod m
n = m, m = r
return n
```

Program to find the GCD of two given numbers.

```
void main()
{
   clrscr();
    int p, q,n,m,r;
    cout<<"Please enter two numbers";
    cin>>p>>q;
    if(p>q)
    {
    n=p;
    m=q;
    }
    else
    {
    n=q;
    m=p;
    }
Loop: r=n%m;
   if(r==0) goto exit;
   else
      n=m;
      m=r;
      goto Loop;
   exit: cout<<"GCD of two numbers is"<<m;
   getch();
}
```

Let p and q be integers, and both are not zero. We know that GCD (p, q) is the greatest common divisor of p and q. Above algorithm gives us the GCD of p and q. We illustrate this theorem using some examples below:

EXAMPLE 6.19 Compute GCD(831, 366) using Euclid's algorithm

Solution

$$831 = 2 * 366 + 265$$
$$366 = 1 * 265 + 101$$
$$265 = 2 * 101 + 63$$
$$101 = 1 * 63 + 38$$
$$63 = 1 * 38 + 25$$
$$38 = 1 * 25 + 13$$
$$25 = 1 * 13 + 12$$
$$13 = 1 * 12 + 1$$
$$12 = 12 * 1 + 0$$

GCD (831, 366) = 1

EXAMPLE 6.20 Compute GCD(2071, 206) using Euclid's algorithm.

Solution

$$2071 = 10 * 206 + 11$$
$$206 = 18 * 11 + 8$$
$$11 = 1 * 8 + 3$$
$$8 = 2 * 3 + 2$$
$$3 = 1 * 2 + (1)$$
$$2 = 2 * 1 + 0$$

The GCD(2071, 206) = 1

EXAMPLE 6.21 Compute GCD(2222, 1234) using Euclid's algorithm.

Solution

$$2222 = 1 * 1234 + 988$$
$$1234 = 1 * 988 + 246$$
$$988 = 4 * 246 + 4$$
$$246 = 61 * 4 + (2)$$
$$4 = 2 * 2 + 0$$

GCD(2222, 1234) = 2

Example 6.22 Compute GCD(12345, 2345678) using Euclid's algorithm.

Solution

$$2345678 = 190 * 12345 + 128$$
$$12345 = 96 * 128 + 57$$
$$128 = 2 * 57 + 14$$
$$57 = 4 * 14 + (1)$$
$$14 = 14 * 1 + 0$$

GCD(12345, 2345678) = 1

6.6.1 Extended Euclidean Algorithm

Suppose p and q are two integer numbers. There exist two integers x and y such that $xp + yq = \text{GCD}(p, q)$. p and b are expressed as trivial combinations: $x = 1x + 0y$ and $y = 0x + 1y$. Now, use extended Euclidean algorithm to find the value of x and y.

Write the two linear combinations vertically as shown below and apply Euclid's algorithm to get $g = \text{GCD}(p, q)$ and the values of x and the y to satisfy the equation $xp + yq = g$.

$$x = 1 \cdot x + 0 \cdot y$$
$$y = 0 \cdot x + 1 \cdot y$$
$$r = 1 \cdot x + (-z) \cdot y$$

Extended Euclidean Algorithm

1. Enter two positive integer numbers p and q such that $p \geq q$.
2. If $q = 0$ then $r = p$, $x_1 = 1$, $y_1 = 0$, and return(r, x_1, y_1).
3. If $q > 0$, do
   (a) $z = p/q$, $r = p \bmod q$, $x_1 = x_3 - zx_2$, $y_1 = y_3 - zy_2$.
   (b) $p = q$, $q = r$, $x_3 = x_2$, $x_2 = x_1$, $y_3 = y_2$, $y_2 = y_1$.
4. $g = p$, $x_1 = x_3$, $y_1 = y_3$, and return (g, x_1, y_1).
5. Print g, x_1 and y_1

EXAMPLE 6.23 Find integers p and q such that $2322p + 654q = 6$ and also find the GCD(2322, 654).

Solution The identity states for 2 numbers x and y with greatest common divisor g, an equation exists that says $g = xp + yq$.

i	x math*	x_i	y math	y_i	r math	r	z math	z
1	Set to 1	1	Set to 0	0		2322		
2	Set to 0	0	Set to 1	1		654	Quotient of 2322/654	3
3	$1-(3*0)$ $x_1 - z_2 * x_2$	1	$0-(3*1)$ $y_1 - z * y_2$	−3	Remainder of 2322/654	360	Quotient of 654/360	1
4	$0-(1*1)$ $x_2 - z_3 * x_3$	−1	$1-(1*-3)$ $y_2 - z * y_3$	4	Remainder of 654/360	294	Quotient of 360/294	1
5	$1-(1*-1)$ $x_3 - z_4 * x_4$	2	$-3-(1*4)$ $y_3 - z * y_4$	−7	Remainder of 360/294	66	Quotient of 294/66	4
6	$-1-(4*2)$ $x_4 - z_5 * x_5$	−9	$4-(4*-7)$ $y_4 - z * y_5$	32	Remainder of 294/66	30	Quotient of 66/30	2
7	$2-(2*-9)$ $x_5 - z_6 * x_6$	20	$-7-(2*32)$ $y_5 - z * y_6$	−71	Remainder of 66/30	6	Quotient of 30/6	5
					Remainder of 30/6	0		

*Math indicates the mathematical computations for the values of x, y, z and r.

By taking the last non-zero row, we get: $x = 20$ and $y = -71$ and GCD $= 6$.

Therefore, $20 * 2322 - 71 * 654 = 6$.

Here, 20 and 71 are relatively prime numbers. This is true for $xm + yn = \text{GCD}(x, y)$.

Note: For the above example, this is not the unique solution. But this method gives the simplest solution.

Alternative Method

$2322p + 654q = 6$

$2322 = 654(3) + 360$	$360 = 2322 - 654(3)$
$654 = 360(1) + 294$	$294 = 654 - 360(1)$
$360 = 294(1) + 66$	$66 = 360 - 294(1)$
$294 = 66(4) + 30$	$30 = 294 - 66(4)$
$66 = 30(2) + 6(\text{GCD})$	$6 = 66 - 30(2)$
$30 = 6(5) + 0$	

$6 = 66 - 30(2)$
$6 = 66 - [294 - 66(4)](2)$
$6 = 66(9) - 294(2)$
$6 = [360 - 294(1)](9) - 294(2)$
$6 = 360(9) - 294(11)$
$6 = 360(9) - [654 - 360(1)](11)$
$6 = 360(20) - 654(11)$
$6 = [2322 - 654(3)](20) - 654(11)$
$6 = 2322(20) - 654(71)$

Therefore, the values of $p = 20$ and $q = -71$ and GCD = 6.

EXAMPLE 6.24 Find integers p and q such that $51p + 36q = 3$. Also find the GCD (51, 36).

Solution The identity states for 2 numbers x and y with greatest common divisor g, an equation exists that says $g = xp + yq$.

i	x math	x_i	y math	y_i	r math	r	z math	z
1	Set to 1	1	Set to 0	0		51		
2	Set to 0	0	Set to 1	1		36	Quotient of 51/36	1
3	$1 - (1*0)$ $x_1 - z_2 * x_2$	1	$0 - (1*1)$ $y_1 - z*y_2$	−1	Remainder of 51/36	15	Quotient of 36/15	2
4	$0 - (2*1)$ $x_2 - z_3 * x_3$	−2	$1 - (2*-1)$ $y_2 - z*y_3$	3	Remainder of 36/15	6	Quotient of 15/6	2
5	$1 - (2*-2)$ $x_3 - z_4 * x_4$	5	$-1 - (2*3)$ $y_3 - z*y_4$	−7	Remainder of 15/6	3	Quotient of 6/3	2
					Remainder of 6/3	0		

By taking the last non-zero row, we get: $x = 5$ and $y = -7$ and GCD(51, 36) = 3.

Therefore, $5 * 52 - 7 * 36 = 3$.

Here, 5 and 7 are relatively prime numbers. This is true for $xm + yn = \text{GCD}(x, y)$.

Alternative Method

$51p + 36q = 3$

$51 = 36(1) + 15$ $36 = 15(2) + 6$ $15 = 6(2) + 3(\text{GCD})$ $6 = 3(2) + 0$	$15 = 51 - 36(1)$ $6 = 36 - 15(2)$ $3 = 15 - 6(2)$

$3 = 15 - 6(2)$
$3 = 15 - [36 - 15(2)](2)$
$3 = 15(5) - 36(2)$

$3 = [51 - 36(1)](5) - 36(2)$
$3 = 51(5) - 36(5) - 36(2)$
$3 = 51(5) - 36(7)$
$3 = 51(5) + 36(-7)$

Therefore, the values of $p = 5$ and $q = -7$ and GCD = 3.

EXAMPLE 6.25 Find integers p and q such that $56p + 72q = 40$ and also find the GCD(56, 72).

Solution The identity states for 2 numbers x and y with greatest common divisor g, an equation exists that says $g = xp + yq$.

i	x math	x_i	y math	y_i	r math	r	z math	z
						56		
1	Set to 1	1	Set to 0	0		72	Quotient of 56/72	0
2	Set to 0	0	Set to 1	1		56	Quotient of 72/56	1
3	$1 - (0 * 0)$ $x_1 - z_2 * x_2$	1	$0 - (0 * 1)$ $y_1 - z * y_2$	0	Remainder of 56/72	16	Quotient of 56/16	3
4	$0 - (1 * 1)$ $x_2 - z_3 * x_3$	−1	$1 - (1 * 0)$ $y_2 - z * y_3$	1	Remainder of 72/56	8	Quotient of 16/8	2
5	$1 - (3 * -1)$ $x_3 - z_4 * x_4$	4	$0 - (3 * 1)$ $y_3 - z * y_4$	−3	Remainder of 56/16	0		
					Remainder of 16/8			

By taking the last non-zero row, we get: x = 4 and y = −3 and GCD = 8.

Therefore, $56 * 4 + 72 * (-3) = 8$.

Here, 4 and 3 are relatively prime numbers. This is true for $xm + yn = \text{GCD}(x, y)$.

Note: For the above example, this is not the unique solution. But this method gives the simplest solution.

Alternative Method

$56p + 72q = 40$

$72 = 56(1) + 16$ $56 = 16(3) + 8(\text{GCD})$ $16 = 8(2) + 0$	$16 = 72 - 56(1)$ $8 = 56 - 16(3)$

$8 = 56 - 16(3)$
$8 = 56 - [72 - 56(1)](3)$
$8 = 56 - 72(3) + 56(3)$
$8 = 56(4) - 72(3)$
$8 = 56(4) + 72(-3)$

We get: $x = 4$ and $y = -3$ and GCD = 8

EXAMPLE 6.26 Use the extended Euclidean algorithm to find the multiplicative inverse of 77 mod 5.

Solution Apply Euclidean algorithm to compute GCD as shown in the left column. It will verify that GCD(77, 5) = 1. Then we will solve for the remainders in the right column.

$77 = 5(15) + 2$ $5 = 2(2) + 1$ $1 = 5 - 2(2)$ $2 = 2(1) + 0$	$2 = 77 - 5(15)$ $1 = 5 - 2(2)$

Use the equations on the right side and perform reverse operation as:

$$1 = 5 - 2(2)$$
$$1 = 5 - [77 - 5(15)]\ (2)$$
$$1 = 5(31) + 77(-2)$$

Therefore, $1 \equiv 77(-2) \bmod 5$, or if we prefer a residue value for the multiplicative inverse,

$$1 \equiv 77(3) \bmod 101.$$

Therefore, 3 is the multiplicative inverse of 77.

The order of the numbers is important so be careful about the same.

EXAMPLE 6.27 Find the multiplicative inverse of 35 mod 11, using the extended Euclidean algorithm.

Solution Apply Euclidean algorithm first as shown in the left column. It will verify that GCD(35, 11) = 1. Then we will solve for the remainders in the right column, before back solving.

$35 = 11(3) + 2$	$2 = 35 - 11(3)$
$11 = 2(5) + 1$	$1 = 11 - 2(5)$
$2 = 1(2) + 0$	

Use the equations on the right and perform reverse operation as:

$$1 = 11 - 2(5)$$
$$1 = 11 - [35 - 11(3)]\ (5)$$
$$1 = 11(16) - 35(5)$$
$$1 = 11(16) + 35(-5)$$

Therefore, $1 \equiv 35(-5) \bmod 11$, and $-5 \bmod 11 = 6$ (since $11 - 5 = 6$)

Therefore, –5 or 6 is the multiplicative inverse of 11.

EXAMPLE 6.28 Find the multiplicative inverse of 40 mod 197, using the extended Euclidean algorithm.

Solution Apply Euclidean algorithm first as shown in the left column. It will verify that GCD(40, 197) = 1. Then we will solve for the remainders in the right column, before back solving.

$197 = 40(4) + 37$	$37 = 197 - 40(4)$
$40 = 37(1) + 3$	$3 = 40 - 37(1)$
$37 = 3(12) + 1$	$1 = 37 - 3(12)$
$3 = 1(3) + 0$	

Use the equations on the right and perform reverse operation as:

$$1 = 37 - 3(12)$$
$$1 = 37 - [40 - 37(1)](12)$$
$$1 = [197 - 40(4)] - [40(12) - (197 - 40(4))(12)]$$
$$1 = 197 - 40(4) - 40(12) + 197(12) - 40(48)$$
$$1 = 197(13) - 40(64)$$
$$1 = 197(13) + 40(-64)$$

Therefore, $1 \equiv 40(-64) \bmod 197$, and $-64 \bmod 197 = 133$ (since $197 - 64 = 133$)

Therefore, -64 or 133 is the multiplicative inverse of 40.

EXAMPLE 6.29 Find the multiplicative inverse of -74 mod 501, using the extended Euclidean algorithm.

Solution $-74 \bmod 501 = (501 - 74) \bmod 501 = 427 \bmod 501$. Apply Euclidean algorithm first as shown in the left column. It will verify that GCD(427, 501) = 1. Then we will solve for the remainders in the right column, before back solving.

$501 = 74(6) + 57$	$57 = 501 - 74(6)$
$74 = 57(1) + 17$	$17 = 74 - 57(1)$
$57 = 17(3) + 6$	$6 = 57 - 17(3)$
$17 = 6(2) + 5$	$5 = 17 - 6(2)$
$6 = 5(1) + 1$	$1 = 6 - 5(1)$
$5 = 1(5) + 0$	

Use the equations on the right and perform reverse operation as:

$$1 = 6 - 5(1)$$
$$1 = 6 - [17 - 6(2)](1)$$
$$1 = 6(3) - 17(1)$$
$$1 = [57 - 17(3)](3) - 17(1)$$
$$1 = 57(3) - 17(10)$$
$$1 = [57(3) - (74 - 57(1))(10)]$$
$$1 = 57(3) - 74(10) + 57(10)$$
$$1 = [501 - 74(6)](13) - 74(10)$$
$$1 = 501(13) - 74(88)$$

Therefore, $1 \equiv -74(88) \bmod 501$.

Therefore, 88 is the multiplicative inverse of -74 mod 501.

6.7 PRIMALITY TEST

There is no simple and efficient mechanism to find out the prime number. To know whether a given number is prime or not, a test is conducted. That test is called as *primality test*. It is an algorithm which checks whether a given number is prime or not. Primality testing and integer factorisation is different. Factorisation is a computationally hard as compared to primality testing. We know that the frequency of prime number for different equal intervals is not same. There are around 4 * 1097 prime numbers in an integer number of 200 digits. Primality tests are of two types: deterministic test and probabilistic test. The first test, deterministic test always correctly determines the prime number. Its accuracy is 100%. But it is slower as compared to probabilistic test. The second test, probabilistic test is less accurate. Its accuracy is not 100% as sometime it may falsely determine a composite number as a prime. But it is faster than deterministic test.

6.7.1 Naïve Methods

The simplest primality test follows the following steps.

Step 1 Enter the positive integer number n.

Step 2 Set the value of $m = 2$.

Step 3 Divide n by m. Find the remainder, if the remainder is zero, then n is divisible by m and go to step 7.

Step 4 Increase the value of m by 1.

Step 5 Repeat steps 3 and 4 until $m < n/2$.

Step 6 Number n is a prime number and exit.

Step 7 Number n is a composite number and exit.

Program to print prime numbers

```
void main()
{
  clrscr();
  cout<<"\n\n Program to Print Prime number upto given number\n\n ";
  int i,n,r,a,k;
  cout<<" Please enter the number.\n\n ";
  cin>>k;
  cout<<"The Prime Numbers are:\n\n ";
  for(n=3; n<=k; n++)
  {
  for(i=2; i<n; i++)
    {
    r=n%i;
    if(r==0)
    {
```

4. If $n \leq r$, then the number is prime.
5. For $a = 1$ to $\lfloor \text{sqrt}\ (\Phi(r))\ \log(n) \rfloor$ do
   if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$, then the number is composite.
6. The number is prime.

6.8 CHINESE REMAINDER THEOREM

According to D. Wells, the problem posed by Sun Tsu (4th century AD) there are certain things whose numbers are not known. Suppose there is some number p which is divided by 2, the remainder is 1, if p is divided by 3, the remainder is 1 and if p is divided by 4, 5 and 6, the remainder is 1. But if it is divided by 7, the remainder is zero. Then what is the smallest value of p. Chinese remainder theorem is used to get the solution of such problem. Using this theorem we get the value of p.

Chinese remainder theorem: There are two relatively prime numbers m and n, which are modulo m and n, the congruence

$$p \equiv a \bmod m$$
$$p \equiv b \bmod n$$

have a unique solution: $p \bmod mn$

Theorem Suppose $n_1, n_2, \ldots, n_r$ are the relatively prime integer numbers and $b_1, b_2, \ldots, b_r$ are the remainders for $n_1, n_2, \ldots, n_r$ respectively. Then the system of congruence, $p \equiv b_i \pmod{n_i}$ for $1 \leq i \leq r$, has a unique solution.

$$N = n_1 * n_2 * \cdots * n_r,$$

which is given by:

$$p \equiv b_1N_1y_1 + b_2N_2y_2 + \cdots + b_rN_ry_r \pmod{N},$$

where $N_i = N/n_i$ and

$$y_i \equiv (N_i)^{-1} \pmod{n_i} \text{ for } 1 \leq i \leq r,$$

where y_i is the multiplicative inverse of $(N_i) \pmod{n_i}$. (Use extended Euclidean algorithm to calculate multiplicative inverse)

Observe that $\text{GCD}(N_i, n_i) = 1$ for $1 \leq i \leq r$. Therefore, all y_i exist. Now, notice that since $N_iy_i \equiv 1 \pmod{n_i}$,

we have $b_iN_iy_i \equiv b_i \pmod{n_i}$ for $1 \leq i \leq r$.

On the other hand, $b_iN_iy_i \equiv 0 \pmod{n_j}$ if $j \neq i$ (since $n_j \mid N_i$ in this case).

Thus, we see that $p \equiv b_i \pmod{n_i}$ for $1 \leq i \leq r$.

If p_0 and p_1 are the solutions, then we would have

$p_0 - p_1 \equiv 0 \pmod{n_i}$ for all i, so $p_0 - p_1 \equiv 0 \pmod{N}$, i.e., they are the same modulo N.

Chinese Remainder Theorem

1. Firstly expressed the problem as a system of congruence,
$$p \equiv b_i (\text{mod } n_i)$$
where, n_i are relatively prime numbers: n_1, n_2, n_3 and so on
b_i is the respective remainder for modulo n_i such that b_1 for n_1, b_2 for n_2 and so on.
p is the value of solution.
2. Calculate the value of N
$$N = n_1 * n_2 * \dots * n_i$$
3. Calculate the value of $N_i = N/n_i$ such that $N_1 = N/n_1$, $N_2 = N/n_2$ and so on.
4. Calculate the multiplicative inverse for $y_i \equiv (N_i)^{-1} \pmod{n_i}$
where y_i is the multiplicative inverse of N_i mod n_i.
5. The value of p is calculated as:
$$p \equiv (b_1 N_1 y_1 + b_2 N_2 y_2 + \dots + b_r N_r y_r) \bmod N$$
where, p is the solution of the problem.

EXAMPLE 6.30 Find the smallest multiple of 10 which has remainder 1 when divided by 3, remainder 6 when divided by 7 and remainder 6 when divided by 11.

Solution The factors of 10 are: 2 and 5.
Problem is now expressed as a system of congruence as:
$$p \equiv b_i (\text{mod } n_i)$$
where $n = 2, 3, 5, 7$ and 11 which are relatively prime and $b = 0, 1, 0, 6$ and 6 are the remainders for respective value of n.

$$p = 0 \bmod 2$$
$$p = 1 \bmod 3$$
$$p = 0 \bmod 5$$
$$p = 6 \bmod 7$$
$$p = 6 \bmod 11$$

To solve for p we first calculate the value of N as:
$$N = n_1 * n_2 * \dots * n_r$$
$$N = 2 * 3 * 5 * 7 * 11 = 2310$$
and find the value of $N_i = N/n_i$ as:
$$N_2 = 2310/2 = 1155$$
$$N_3 = 2310/3 = 770$$
$$N_5 = 2310/5 = 462$$
$$N_7 = 2310/7 = 330$$
$$N_{11} = 2310/11 = 210$$

Now, find out the multiplicative inverse as:

$$y_i \equiv (N_i)^{-1} (\text{mod } n_i)$$
$$y_2 = (1155)^{-1} (\text{mod } 2) = 1$$
$$y_3 = (770)^{-1} (\text{mod } 3) = 2$$
$$y_5 = (462)^{-1} (\text{mod } 5) = 3$$
$$y_7 = (330)^{-1} (\text{mod } 7) = 1$$
$$y_{11} = (210)^{-1} (\text{mod } 11) = 1$$

The solution for the above problem is:

$$p \equiv b_1 N_1 y_1 + b_2 N_2 y_2 + \cdots + b_r N_r y_r \ (\text{mod } N),$$
$$p = 0(N_2 * y_2) + 2(N_3 * y_3) + 0(N_5 * y_5) + 6(N_7 * y_7) + 6(N_{11} * y_{11})$$
$$p = 0(1155)(1) + 1(770)(2) + 0(462)(3) + 6(330)(1) + 6(210)(1)$$
$$p = 0 + 1540 + 0 + 1980 + 1260$$
$$p = 4780 \text{ mod } 2310 = 160.$$

EXAMPLE 6.31 An old woman purchases a basket of some eggs from the market. While walking on the road she stops for a while and keep her basket of eggs down on the road. A horse running on the road accidentally steps on the basket and crushing all the eggs in the basket. The rider offers to pay the old woman for the damaged eggs. So, he asks her about the total number of eggs she had brought. The old woman does not remember the exact number of eggs in the basket. So she told the rider that when she had taken out two eggs at a time from the basket, there was one egg left. When she had taken out three eggs at a time from the basket, there were two eggs left. When she had taken out five eggs at a time from the basket, there were four eggs left. Find out, the smallest number of eggs an old woman could have had in her basket?

(Above puzzle is mentioned by Oystein Ore taken from Brahma-Sphuta-Siddhanta by Brahmagupta (born 598 AD)):

Solution Problem is now expressed as a system of congruence as:

$$p \equiv b_i \ (\text{mod } n_i)$$

where $n = 2, 3, 5$ and $b = 1, 2, 4$.

$$p = 1 \text{ mod } 2$$
$$p = 2 \text{ mod } 3$$
$$p = 4 \text{ mod } 5$$

Use CRT Find →

To solve for p we first calculate the value of N as

$$N = n_1 * n_2 * \cdots * n_r$$
$$N = 2 * 3 * 5 = 30$$

and find the value of $N_i = N/n_i$ as:

$$N_2 = 30/2 = 15$$
$$N_3 = 30/3 = 10$$
$$N_5 = 30/5 = 6$$

Now, find out the multiplicative inverse as:

$$y_i \equiv (N_i)^{-1} (\text{mod } n_i)$$
$$y_2 = (15)^{-1} (\text{mod } 2) = 1$$
$$y_3 = (10)^{-1} (\text{mod } 3) = 2$$
$$y_5 = (6)^{-1} (\text{mod } 5) = 3$$

The solution for the above problem is:

$$p \equiv b_1 N_1 y_1 + b_2 N_2 y_2 + \ldots + b_r N_r y_r (\text{mod } N)$$
$$p = b_2(N_2 * y_2) + b_3(N_3 * y_3) + b_5(N_5 * y_5)$$
$$p = 1(15)(1) + 2(10)(1) + 4(6)(1)$$
$$p = 15 + 20 + 24$$
$$p = 59 \text{ mod } 30 = 29.$$

There are total 29 eggs in the basket.

EXAMPLE 6.32 Monica breeds some pets. She does not know the exact number of pets she has. So she told that when she takes rounds, she observed some things. In the morning there are five pets in each group except one group which has only two pets. In the afternoon there are seven pets in each group except one group which has six pets. In the evening, there are eleven pets in each group. Monica is sure that there are fewer than 150 pets. Find out, the smallest number of pets does she have.

Solution Problem is now expressed as a system of congruence as:

$$p \equiv b_i (\text{mod } n_i)$$

where $n = 5, 7, 11$ and $b = 2, 6, 0$

$$p = 2 \text{ mod } 5$$
$$p = 6 \text{ mod } 7$$
$$p = 0 \text{ mod } 11$$

To solve for p we first calculate the value of N as:

$$N = n_1 * n_2 * \ldots * n_r$$
$$N = 5 * 7 * 11 = 385$$

and find the value of $N_i = N/n_i$ as:

$$N_5 = 385/5 = 77$$
$$N_7 = 385/7 = 55$$
$$N_{11} = 385/11 = 35$$

Now, find out the multiplicative inverse as:

$$y_i \equiv (N_i)^{-1} (\text{mod } n_i)$$
$$y_5 = (77)^{-1} (\text{mod } 5) = 3$$
$$y_7 = (55)^{-1} (\text{mod } 7) = 6$$
$$y_{11} = (35)^{-1} (\text{mod } 11) = 6$$

The solution for the above problem is:

$$p \equiv b_1N_1y_1 + b_2N_2y_2 + \ldots + b_rN_ry_r(\text{mod } N),$$
$$p = b_2(N_2 * y_2) + b_3(N_3 * y_3) + b_5(N_5 * y_5)$$
$$p = 2(77)(3) + 6(55)(6) + 0(35)(6)$$
$$p = 462 + 1980 + 0$$
$$p = 2442 \text{ mod } 385$$
$$p = 132$$

There are total 132 pets.

6.9 DISCRETE LOGARITHMS

Discrete logarithms have an important role in Diffie–Hellman and the digital signature algorithms.

From Euler's theorem, for every p and n which are relatively prime we have,

$$p^{\Phi(n)} = 1 \text{ mod}(n)$$

where $\Phi(n)$ is the number of positive integers less than n and relative prime to n.

So in general it is:

$$p^n = 1 \text{ mod } n$$

If p and n are relatively prime, then there is at least one integer n that satisfies above equation.

Suppose $p = 3$ and $n = 13$ are the numbers which are relatively prime. Let us see the power of 3, modulo 13:

$$3^1 = 3 = 3 \text{ mod } 13$$
$$3^2 = 9 = 9 \text{ mod } 13$$
$$3^3 = 27 = 13 * 2 + 1 = 1 \text{ mod } 13$$
$$3^4 = 81 = 13 * 6 + 3 = 3 \text{ mod } 13$$
$$3^5 = 243 = 13 * 18 + 9 = 9 \text{ mod } 13$$

This can prove that $3^3 = 1$ mod 13 and therefore $3^{3+i} = 3^3\ 3^i = 3^i$ mod 13 and hence any two powers of 3 whose exponents differ by 3 are congruent to each other (mod 13).

In general, let F be a finite cyclic group with n elements. We assume that the group is written multiplicatively. Let p be a generator of F; then every element f of F can be written in the form $f = p^k$ for some integer k. Furthermore, any two such integers representing f will be congruent modulo n. We can thus define a function

$$\log_b : F = Z_n$$

(where Z_n denotes the ring of integers modulo n) by assigning to f the congruence class of k modulo n. This function is a group isomorphism, called the *discrete logarithm* to base p.

The familiar base change formula for ordinary logarithms remains valid: If y is another generator of F, then we have

$$\log_y(f) = \log_y(p) \ . \ \log_p(f)$$

6.9.1 Index Calculus Algorithm

The index calculus algorithm is used for computing discrete logarithms. The discrete logarithms used to find p using $g^p = h \bmod n$, where g, h and n are given.

The discrete logarithms algorithm applies to the group where p is a prime using a factor base.

Factor base is a set of small primes. For example, factor base having n elements are $= \{p_1, p_2, p_3, \ldots p_n\}$. For $n = 5$, the factor base $= \{2, 3, 5, 7, 11\}$ i.e., five prime numbers. If the factor base is small, the efficiency of the algorithm increases. But if the group is large the factor base must be relatively large.

Smooth Integer

If the biggest prime factor of q is less than or equal number r then the number q is called *r-smooth*.

For example, if our $r = 11$, then the number $q = 100$ is r-smooth because it factorises to $2 * 2 * 5 * 5 = 2^2 * 5^2$ and the biggest prime factor is 5 which is less than 11 ($5 \leq 11$). If we take the number 248, it is NOT r-smooth because it factorises to $2 * 2 * 2 * 31 = 2^3 * 31$ and the biggest prime factor is 31 which is greater than 11 ($31 \leq 11$).

The algorithm is divided in two parts.

1. Gathering a number of linear relations between the factor base and powers of the generator g and solving the logarithms using linear algebra.
2. Computation of the discrete logarithm of a desired element.

Now, find out x using algebraic manipulation.

Given p, g, $x = g^a \pmod p$, determine a.

Choose bound B and factor base.

Suppose $p_0, p_1, \ldots, p_{n-1}$ are primes in factor base.

Pre-compute discrete logs:

$\log_g p_i$ for each i

Randomly select $k \in \{0,1,2,\ldots,p-2\}$ and

compute $y = x \cdot g^k \pmod p$ until find y that factors completely over factor base.

Then,

$y = x.\ g^k = {p_0}^{do} \cdot {p_1}^{d1} \ldots p_{n-1}^{dn-1} \pmod p$

Take $\log_g$ of y we get,

$a = \log_g x = (d_0 \log_g p_0 + d_0 \log_g p_0 + \ldots + d_0 \log_g p_0 - k) \pmod{(p-1)}$

This gives us a value of 'a'.

Note: $p - 1$ follows from Fermat's Little theorem.

SUMMARY

Prime number theory is very important in cryptography. There is no simple and efficient algorithms available to find out the largest prime number. Primality test is used to check whether the number is prime or not. Two numbers are relatively prime if their GCD is 1. Fermat's theorem is useful in public key encryption techniques and primality testing. The totient of a positive integer n is the total number of positive integer numbers which are less than n and are relatively prime to n. It is shown as $\Phi(n)$. Suppose there are two relatively prime numbers m and n, which are modulo m and n, Chinese remainder theorem provides the solution of the congruence. The index calculus algorithm is used for computing discrete logarithms. The discrete logarithms used to find p using $g^p = h \bmod n$, where g, h and n are given. Factor base is a set of small primes. If the biggest prime factor of q is less than or equal number r then the number q is called r-smooth. Euclid's algorithm is used to calculate the GCD of two numbers, whereas extended algorithm is used to find the multiplicative inverse of a number.

EXERCISES

6.1 Define prime number. What are the different tests to check whether a number is prime or not?

6.2 Explain Euler's totient function. Find the totient value for 25.

6.3 What is the primitive root of a number? How many primitive roots the number 15 has? Calculate all possible primitive roots for 15.

6.4 Explain index calculus algorithm.

6.5 Compare an index calculus algorithm with a discrete logarithm.

6.6 Explain fast deterministic test.

6.7 What is primality test?

6.8 Explain Fermat's theorem.

6.9 m and $m + 1$ are two consecutive integers. Prove why GCD $(m, m + 1) = 1$.

6.10 How many primitive roots the number 10 has? Find all primitive roots of 10.

6.11 Using Fermat's theorem, find $3^{110} \bmod 13$. [Ans: 9]

6.12 Find the value of $12346^{23456789} \bmod 11$?

6.13 Find the value of final digit (LSB) of $(((((((9^9)^9)^9)^9)^9)^9)^9)^9$?

6.14 Find the value of Φ (243). [Ans: 162]

6.15 Find the multiplicative inverse of 55 mod 101, using the Euclidean algorithm. [Ans: 90]

6.16 Compute GCD (1276, 244). [Ans: 4]

6.17 Find the GCD of 2740 and 1760 using Euclidean algorithm. [Ans: 20]

6.18 Compute GCD (12345, 120). [Ans: 15]

6.19 Find the multiplicative inverse of 121 mod 1245, using the Euclidean algorithm.

6.20 Find the multiplicative inverse of 1761 mod 2740, using the Euclidean algorithm. [Ans: 391]

6.21 Find the value of $\Phi(144)$. [Ans: 2281]

6.22 Find integers p and q for the equation $1124p + 84q$ and also find the GCD. [Ans: 48]

6.23 Find integers p and q such that $52p + 56q = 36$ and also find the GCD. [Ans: $p = 8$, $y = -107$]

6.24 Find integers p and q such that $7920p + 4536q = 72$. [Ans: There is no positive solution for the equation]

6.25 Find all solutions of the following congruence [Ans: $p = -4$, $q = 7$]

(a) $7x = 9 \bmod 15$ (b) $6x = 23 \bmod 31$

(c) $11x = 2 \bmod 45$ (d) $2x = 7 \bmod 11$

6.26 Use Chinese theorem and solve the following puzzle.

Five robbers and a monkey are stucked on an island. The robbers have collected a pile of bananas. They decided to divide the bananas equally among themselves in the next morning. The robbers are not having trust on one another. One robber wakes up during the night and divides the bananas into five equal parts with one left over, which he gives to the monkey. The robber then hides his portion of the pile. During the night, each of the other robbers does exactly the same thing by dividing the pile he finds into five equal parts leaving one banana for the monkey and hiding his portion. In the morning, the robbers gather and split the remaining pile of bananas into five equal parts and again one is left over for the monkey. What is the smallest number of bananas the robbers could have collected for their original pile?

MULTIPLE CHOICE QUESTIONS

6.1 The extended Euclidean algorithm is of interest to cryptographers because

(a) Large composites number can be factorised easily using this algorithm

(b) A multiplicative inverse can be calculated using this algorithm easily

(c) Primality of large primes can be checked using this algorithm

(d) None of of the above

6.2 If $n = 143 = 11 * 13$, calculate $15^{241} \bmod n$

(a) 18 (b) 9

(c) 1 (d) 15

6.3 If $n = 77$, then calculate $\Phi(n)$

(a) 5 (b) 14

(c) 30 (d) 60

6.4 Calculate $(36^{106} \bmod 107) \bmod 37$

(a) 1 (b) 3

(c) 107 (d) 7

Answers

6.1 (b) **6.2** (d) **6.3** (d) **6.4** (a)