International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-2, Issue-5)
Research Article
May 2013

Review of Number Theory for RSA Algorithm

Ravi Shankar Prasad
Research Scholar,
T. M. Bhagalpur University,
Bhagalpur, India

A. K. Sah*
Marwari College,
T. M. Bhagalpur University,
Bhagalpur, India

Abstract—

In this paper, we will discuss basis of number theory which are essential to understand the workings of cryptography and hash function. This paper also discusses the extended Euclidean algorithm, Chinese remainder theorem, and Euler's theorem.

Keywords— Euclidean Algorithm, binary expansion, cryptography, hash function, Modular Arithmetic.

I. INTRODUCTION

Number theory is well known as The Queen of Mathematics. Since the beginning of recorded history, numbers have enchanted the human mind. It was evident when we found the famous Rhind papyrus among the treasures of Egyptian antiquity. It tells us about the mathematics practiced in Egypt almost 2000 years B.C. On the other hand, cuneiform tablets show us that arithmetic was already quite sophisticated at the end of the third millennium B.C in Mesopotamia.Number theory is the branch of pure mathematics concerned with the properties of, and the relationships between, the particular types of numbers. Nevertheless, the most important of the sets of numbers studies in number theory is the set of positive integers, especially prime numbers. Recently, number theory has come to be concerned with wider classes of problems that have arisen from the studies of integers ([1-7]). We use decimal notation to represent integers as usual. In fact, integers can be represented by using base b expansion. When b is a positive integer, every positive integer has a unique base b expansion. For instance, base 10 expansions is decimal notation, base 2 expansions are called binary expansion, and base 16 are called hexadecimal expansion

II. THEOREMS ON THE NUMBER THEORY WITH THEIR APPLICATION

Theorem 1: Let b > 1, then every positive integer n can be written uniquely in the form.

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0 \ ,$$

where k is a nonnegative integer, a_j is an integer with $0 \le a_j \le b-1$ for $j = 0,1,....,k,$ and the initial coefficient $a_k \neq 0$.

In order to differentiate the representation of integers with different bases, we use $(a_k a_{k-1} ..... a_1 a_0)_b$ to represent the number $a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$.

Binary Code

Binary code is base 2 expansions. It uses 0 and 1 to represent the number. Computer use binary expansions to represent integers internally where digit 1 represents "on" and digit 0 represents "off". The correspondence between binary and decimal notation are shown as Table I.

Table I
Binary code

Decimal	Binary		Decimal	Binary
1	1		8	1000
2	10		9	1001
3	11		10	1010
4	100		16	10000
5	101		32	100000
6	110		64	1000000
7	111		256	100000000

Definition

The greatest integer in a real number *x*, denoted by [*x*], is the largest integer ≤ *x*.
That is [*x*] satisfying

$[x] \le x\ [x]\ +1$.

Algorithm: Binary Representations

Input : A positive integer n
Output : The binary representation $(a_k a_{k-1}.....a_1 a_0)_2$ of n
Set $i = 0$
While $n > 0$ Do
$Set\ a_i = n - \lfloor n/2 \rfloor 2$
$Set\ n = \lfloor n/2 \rfloor$
$Set\ i = i + 1$
End While
Set $k = i - 1$
Return $k, a_0, a_1, ..., a_k$

Hexadecimal Code

In hexadecimal notation, there have 16 digits which denoted by 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *A, B, C, D, E, F*. The letter *A, B, C, D, E, and F* represent 10, 11, 12, 13, 14 and 15 respectively in decimal notion. The hexadecimal notations are listed in the table – II.

Table – II
Hexadecimal code

Decimal	Hexadecimal	Binary		Decimal	Hexadecimal	Binary
0	0	0000		8	8	1000
1	1	0001		9	9	1001
2	2	0010		10	*A*	1010
3	3	0011		11	*B*	1011
4	4	0100		12	*C*	1100
5	5	0101		13	*D*	1101
6	6	0110		14	*E*	1110
7	7	0111		15	*F*	1111

Greatest Common Divisor

An integer b is said to be divisible by an integer $a \neq 0,$ in symbols $a/b,$ if there exists some integer *c* such that $b = ac$. We write $a \neq b$ to indicate that *b* is not divisible by *a*.

Definition: If *a* and *b* are integers, at least one of which is nonzero, then the greatest common divisor d of a and b is the largest of the common divisors of *a* and *b*. We write the greatest common divisor of a and b as d = gcd(*a*, *b*).

Example: The common divisor of 6 and 18 are ±1, ±2, ±3, ±6. Therefore, gcd (6,18) = 6.

Definition: If gcd (*a*,*b*) = 1, then we say that a and b are relatively prime and write a ⊥ b.

Example: Since gcd (19, 27) = 1, hence, 19 and 27 are relatively prime.

Theorem 2: For integers a and b (not both zero), we have $\gcd(a,b) = \gcd(|a|,|b|)$.

Example: $\gcd(9,15) = \gcd(-9,-15) = 3$. Hence, we restrict our concentration on the pair of positive integers.

Theorem 3: If $\gcd(a,b) = d,\ then\ \gcd(a|d, b|d) = 1$.

Example: $\gcd(30,81) = 3,\ then\ \gcd(30|3, 81|3) = \gcd(10,27) = 1$.

Theorem 4: If $a > 0$, then gcd(*a*,*a*) = *a* and gcd(*a*,0) = *a*

Theorem 5: For integers *a* and *b* (not both zero), we have gcd (*a*,*b*) = gcd (*b*,*a*).

Theorem 6: For integers a and b (not both zero), we have gcd (a,b) = gcd $(a+kb, b)$ for any integer k.

Example: Let $a = 5$, $b = 10$ and $k = 2$.
Since gcd(5,10) = 5. So, gcd(5+20,10) = gcd (25,10) = 5.

Theorem 7: If $a \mid bc$ and $a \perp bc$, then $a \mid c$.

Function: Let n > 0. For any integer a, a mod n = a – $\lfloor n \rfloor$n. Thus a mod n is the remainder upon dividing a by n.
Example: Let a = 99, n = 8.
99mod8 = 99 – $\lfloor 99/8 \rfloor$8 = 99 – 12.8 = 3.

The addition and multiplication modular function which defines on finite sets of integers of the form 0,1,2,3,…..,n–1 can be represented by cayley table.
Example: Let n = 4 and define $\oplus$ and $\otimes$ on {0,1,2,3} by
$a \oplus b = (a+b) \bmod 4$
$a \otimes b = ab \bmod 4$

Cayley table of addition and multiplication modulo 4 can be shown as below:

$\oplus$	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Euclidean Algorithm

Euclidean Algorithm was discovered over 2000 years ago by Euclid and this algorithm is one of the most efficient ways to find the greatest common divisor (gcd) of two large integers. It is an algorithm which can find the gcd without factorization of the numbers.

Theorem 8: Given a and b integers with $b>0$, we have gcd (a,b) = gcd$(b, a \bmod b)$.

Example: Compute gcd (78, 163)
Solution: gcd (163,78) = gcd (78,163 mod 78)= gcd (78,7)
= gcd (7,78, mod 7)= gcd (7,1)
= gcd (1,7 mod 1)= gcd (1,0)= 1

Extended Euclidean Algorithm

Theorem 9: Let a and b be two integers, not both of which are zero, and let d = gcd (a,b). Then there exist integers x, y such that $ax+by = d$.

The value of d, x, y can be computed by using the extended Euclidean algorithm.

Algorithm: Extended Euclidean Algorithm

Input : Integer a and b, not both zero
Output : integers x,y, and d, where d = ged(a,b) = $ax + by$

$$Set\ d_0 = a$$
$$Set\ x_0 = 1$$
$$Set\ y_0 = 0$$
$$Set\ d_1 = b$$
$$Set\ x_1 = 0$$
$$Set\ y_1 = 1$$
$$While\ d_1 \neq 0\ Do$$
$$Set\ q = \left[d_0/d_1\right]$$
$$Set\ d_2 = d_1$$
$$Set\ x_2 = x_1$$
$$Set\ y_2 = y_1$$
$$Set\ d_1 = d_0 - qd_1$$
$$Set\ x_1 = x_0 - qx_1$$
$$Set\ y_1 = y_0 - qy_1$$
$$Set\ d_0 = d_2$$
$$Set\ x_0 = x_2$$
$$Set\ y_0 = y_2$$
$$End\ \ while$$
$$Return\ \left[d, x, y\right] = \left[d_0, x_0, y_0\right]$$

Example: Let a = 4 and b = 6. The extended Euclidean algorithm produces the numbers in the table below:

d_0	x_0	y_0	d_1	x_1	y_1	q
4	1	0	6	0	1	0
6	0	1	4	1	0	1
4	1	0	2	-1	1	2
2	-1	1	0	3	-2	

Thus, 2 = gcd (4,6) = (–1)4+(1)6 where x = –1 and y = 1

Modular Arithmetic

Given two integers a and b and a positive integer n, we say that a is congruent to b modulo n and write

$a \equiv b(\text{mod } n)$

if a mod n = b mod n.

Theorem 10: The condition $a \equiv b$ (mod n) is equivalent to $n \mid (a–b)$.

Example

(i) $45 \equiv 29(\text{mod } 4)$ is equivalent to $4 \mid 16$.
(ii) $7 \equiv 7(\text{mod } 16)$ is equivalent to $16 \mid 0$.
(iii) $–19 \equiv 53(\text{mod } 8)$ is equivalent to $8 \mid –72$.

Theorem 11: If a and b are integers, then $a \equiv b(mod\ n)$ if and only if there is an integer k such that $a = b+kn$.

Example: Since $25 \equiv 40(\text{mod } 15)$ then 25 = 40+(–1).15. So, integer k = –1.

Definition

A complete residue system modulo n is a set C of integers such that

(i) If a is an integer, then $a \equiv c(mod\ n)$ is a set C of integers such that
(ii) If $c \equiv d(modn)$ for $c, d \in C$, then $c = d$.

The set $\{0,1,2,3,\ldots\ldots,n–1\}$ is one example of a complete residue system. This particular example is called the *least nonnegative residue system* modulo n.

Theorem 12: Let n > 0, d be positive integers and let a, b, c be any integers. The following hold:

(i) $a \equiv a \pmod n$.
(ii) If $a \equiv b \pmod n$, then $b \equiv a \pmod n$.
(iii) If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.
(iv) If $a \equiv b \pmod n$ then $a+c \equiv b+c \pmod n$, and $ac \equiv bc \pmod n$.
(v) If $a \equiv b \pmod n$ then $a^d \equiv b^d \pmod n$, for any positive d.
(vi) If $a \perp n$ and $ab \equiv ac \pmod n$, then $b \equiv c \pmod n$.
(vii) If $gcd(a,n) = d$ and $ab \equiv ac \pmod n$, then $b \equiv a \pmod n$.

Definition: If $ab = 1 \pmod n$, then b is called an inverse of a modulo n and $a^{-1} \bmod n$ is the smallest positive integer b such that $ab \equiv 1 \pmod n$.

Theorem 13: The integer a has an inverse modulo n if and only if $a \perp n$.

The algorithm below is to compute $a^{-1} \bmod n$.

Algorithm: $a^{-1} \bmod n$
Input : Integer a and n with n > 0 Output : Integer $a^{-1} \bmod n$ or message "inverse does not exist" $Set \begin{pmatrix} d_0 & x_0 \\ d_1 & x_1 \end{pmatrix} = \begin{pmatrix} a & 1 \\ n & 0 \end{pmatrix}$ $While\ d_1 \neq 0\ Do$ $Set \begin{pmatrix} d_0 & x_0 \\ d_1 & x_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ n & [d_0/d_1] \end{pmatrix} \begin{pmatrix} d_0 & x_0 \\ d_1 & x_1 \end{pmatrix}$ $End\ While$ $If\ d_0 = 1\ Then$ $Return\ a^{-1} = x_0 \bmod n$ $Else$ $Return\ 'Inverse\ does\ not\ exist'$ $End\ If$

Example: Find the inverse of 16 mod 31.
Solution:

$$\begin{pmatrix} 0 & 1 \\ 1 & -[16/31] \end{pmatrix} \begin{pmatrix} 16 & 1 \\ 31 & 0 \end{pmatrix} = \begin{pmatrix} 16 & 0 \\ 31 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -[31/16] \end{pmatrix} \begin{pmatrix} 31 & 0 \\ 16 & 1 \end{pmatrix} = \begin{pmatrix} 16 & 1 \\ 15 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -[16/15] \end{pmatrix} \begin{pmatrix} 16 & 1 \\ 15 & -1 \end{pmatrix} = \begin{pmatrix} 15 & -1 \\ 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -[15/1] \end{pmatrix} \begin{pmatrix} 15 & -1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & -3 \end{pmatrix}$$

$\therefore 16^{-1} \bmod 31 = 2$

Chinese Remainder Theorem
Theorem 14

If $m \perp n$, then the system

$x \equiv a \pmod m$

$x \equiv b \pmod{n}$

has a solution. In fact, if $t = m^{-1}(b - a) \bmod n$, then $x = a + mt$ is such a solution. Where m^{-1} represent the inverse of m modulo n. Any two solutions are congruent modulo mn.

Example: Solve the system

$x \equiv 5 \pmod{9}$

$x \equiv 4 \pmod{11}$

Solution:

$t = m^{-1}(b - a) \bmod n = 9^{-1}(4 - 5) \bmod 11 = -5 \bmod 11 = 6 \bmod 11 = 6$

$x = a + mt = 5 + 9(6) = 59$

Definition: A collection $m_1, m_2, \ldots, m_r$ of integers is pair wise relatively prime if $m_i \perp m_j$ whenever $i \neq j$.

Theorem 15: Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_r$ be pair wise relatively prime positive integers. Then the system

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_r \pmod{m_r}$

has a unique solution modulo the product $m_1 m_2 \ldots m_r$.

Example: Solve the system

$x \equiv 3 \pmod{7}$

$x \equiv 2 \pmod{9}$

$x \equiv 1 \pmod{11}$

Solution

We start from the last pair $x \equiv 2 \pmod{9}$ & $x \equiv 1 \pmod{11}$

Since $9^{-1} \bmod 11 = 5$

$\therefore \quad t = 9^{-1}(1 - 2) \bmod 11$

$= 5(-1) \bmod 11 = 6 \bmod 11 = 6$

Hence, $x = a_2 + m_2 t$

$= 2 + 9(6) = 56 \equiv 56 \bmod 99$

Then, we solve $x \equiv 3 \pmod{7}$ and $x \equiv 56 \pmod{99}$

The calculation still same as above, we need to find $7^{-1} \bmod 99 = 85$, this implies that

$t = 7^{-1}(56 - 3) \bmod 99$

$= 85(53) \bmod 99 = 4505 \bmod 99 = 50$

And hence $x = 3 + 7(50) = 353$

Powers Modulo n

We will face a big problem when calculating very large powers modulo n. For example, $y = xe \bmod n$ with e and n are 100 or even 200 digits positive integers. It is impossible for us to calculate it with such large integer. However, it can be solved by the following algorithm.

Algorithm: Powers Modulo n

Input : Integers x,e,n
Output : Integer $y=x^e \bmod n$
Function: *Power (x,e,n)*
Set prod = 1
While e > 0 do
If $e \bmod 2 = 1$ then
Set prod = *prod. x mod n*
End if
Set $x = x^2 \bmod n$
Set $e = \lfloor e/2 \rfloor$
End while
Set *Power = prod*
Return

Example: Let $x = 17$, $e = 45$, and $n = 23$.

Solution

$x^2 \bmod 23 \rightarrow x$	$\lfloor e/2 \rfloor \rightarrow e$	$e \bmod 2$	$prod.x \bmod 23 \rightarrow prod$
17	45	1	$1.17 \bmod 23 = 17$
$17^2 \bmod 23 = 13$	$\lfloor 45/2 \rfloor = 22$	0	
$13^2 \bmod 23 = 8$	$\lfloor 22/2 \rfloor = 11$	1	$17.8 \bmod 23 = 21$
$8^2 \bmod 23 = 18$	$\lfloor 11/2 \rfloor = 05$	1	$21.18 \bmod 23 = 10$
$18^2 \bmod 23 = 02$	$\lfloor 5/2 \rfloor = 02$	0	

$2^2 \bmod 23 = 04$ $4^2 \bmod 23 = 16$	$\lfloor 2/2 \rfloor = 01$ $\lfloor 1/2 \rfloor = 00$	1 0	$10.4 \bmod 23 = 17$

$\therefore 17^{45} \bmod 23 = 17$.

Wilson's Theorem

Theorem 16

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Example: Let p = 11.

Solution:

$(11-1)! = 10! = 1.2.3.4.5.3.7.8.9.10$. We group the factors together in pairs of inverses modulo 11. We note that

$2.6 \equiv 1 \pmod{11}$

$3.4 \equiv 1 \pmod{11}$

$5.9 \equiv 1 \pmod{11}$

Hence, $10! \equiv 1.(2.6).(3.4).(5.9).(7.8).10 \equiv -1 \pmod{11}$.

Theorem 17

If n is a positive integer such that $(n-1)! = -1 \pmod{n}$, then n is prime.

Example: Let $n = 7$ and $n = 12$.

Solution:

$6! \bmod 7 = 6 \equiv -1 \pmod{7}$

$11! \bmod 12 = 0$

So, 7 is prime but 12 is composite.

Euler's Theorem

Definition: Let n be a positive integer. The Euler phi – function $\varphi(n)$ is defined to be the number of positive integers not exceeding n that are relatively prime to n.

Small value of $\varphi(n)$ are listed in the following table:

Table – III
Euler phi – function

$\phi(1) = 1$	$\phi(2) = 1$	$\phi(3) = 2$	$\phi(4) = 2$	$\phi(5) = 4$
$\phi(6) = 2$	$\phi(7) = 6$	$\phi(8) = 4$	$\phi(9) = 6$	$\phi(10) = 4$
$\phi(11) = 10$	$\phi(12) = 4$	$\phi(13) = 12$	$\phi(14) = 6$	$\phi(15) = 8$
$\phi(16) = 8$	$\phi(17) = 16$	$\phi(18) = 6$	$\phi(19) = 6$	$\phi(20) = 8$
$\phi(21) = 12$	$\phi(22) = 10$	$\phi(23) = 22$	$\phi(24) = 8$	$\phi(25) = 20$
$\phi(26) = 12$	$\phi(27) = 18$	$\phi(28) = 12$	$\phi(29) = 28$	$\phi(30) = 8$
$\phi(31) = 30$	$\phi(32) = 16$	$\phi(33) = 20$	$\phi(34) = 16$	$\phi(35) = 24$
$\phi(36) = 12$	$\phi(37) = 36$	$\phi(38) = 18$	$\phi(39) = 24$	$\phi(40) = 16$
$\phi(41) = 40$	$\phi(42) = 12$	$\phi(43) = 42$	$\phi(44) = 20$	$\phi(45) = 24$
$\phi(46) = 22$	$\phi(47) = 46$	$\phi(48) = 16$	$\phi(49) = 42$	$\phi(50) = 20$

Theorem 18: A positive integer p is prime if and only if $\phi(n) = p-1$.

Example: Determine $\phi(31)$

Solution: Since 31 is a prime number, then all of the positive integers from 1 to 30 are relatively prime to 31.

Thus, $\phi(31) = 31-1 = 30$.

Theorem 19: If $n = p^k$ is a power of a prime, then $\phi(n) = p^k - p^{k-1} = p^{k-1}(p-1)$

Example: Compute $\phi(24)$ by using the prime power factorization of 24.

Solution:

Let $24 = 2^3 3^1$. Then, $\phi(24) = 2^2.(2-1).3^0.(3-1)$

$$= 4.1.2 = 8$$

To determine $\phi(24)$, we also can check our answer by list all of the positive integers less than 24 and relatively prime to it:

1, 5, 7, 11, 13, 17, 19, 23

There are 8 numbers on the list, thus $\phi(24)$ = 8. Therefore, our answer is right.

Theorem 20

If $\perp$ m, then $\phi(n.m) = \phi(n).\phi(m)$.

Example:

$$\phi(35) = \phi(7)\times\phi(5)$$
$$= (7-1)\times(5-1) = 6\times 4 = 24$$

Where the 24 positive integers are
{1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23,24,26,28,29,31,32,33,34}
Example:

$$\phi(45) = \phi(9)\times\phi(5)$$
$$= 3^2\times(5-1) = 3(3-1)\times(5-1) = 6\times 4 = 24$$

Where the 24 positive integers are
{1,2,4,7,8,11,13,14,16,17,19,22,23,26,28,29,31,32,34,37,38,41,43,44}

Theorem 21: Euler's Theorem

If a $\perp$n, then $a^{\phi(n)} \equiv 1(\mathrm{mod}\, n)$.

Example: Let a = 3 and n = 11,

$$\phi(11) = (11-1) = 10;\ 3^{10} = 59049 \equiv 1(\mathrm{mod}\ 11)$$
$$\therefore 3^{\phi(11)} \equiv 1(\mathrm{mod}\ 11)$$

III. CONCLUSIONS

Number theory is essential for cryptography. Basic concepts of number theory which were introduced in this paper are fundamental tools to understand the mathematical operations in RSA algorithm and hash function.

REFERENCES

[1] Burton, David M. "Elementry Number Theory", 3e, Wm. C. Brown Publishers, 1994.
[2] Dickson, L. E. "History of the Theory of the Numbers", Vol. 1, Carnage Institute of Washington, D.C. 1919, reprinted by Dover, Mineola, NY, 2005.
[3] J. Daemen and C. Clapp, "Fast hashing and stream Encryption with PANAMA", Fast Software Encryption, LNCS 1372, S. Vaudenay, Ed., Springer-Verlag, 1998,pp. 60-74.
[4] Hardy, G.H.,Wright, E. M., " An Introduction to the Theory of Numbers, 5e, Oxford University press, 1989.
[5] Willam Staling "Cryptography and network security-principle and practice", 5e, Prentice Hall, 2010.
[6] B. Schneier, applied cryptography. New York: Wiley, 1999.
[7] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1986.