Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Number Theory and Negative Primes in RSA

Biplab Dhar*
M.Sc, National Institute of Technology,
Silchar, Assam, India

Abstract: ***The domain of encryption and decryption algorithm has an important effect of number theory. More importantly, here, an attempt to define Euler's totient function for negative numbers is made. This paper provides importance of negative primes, which was never taken into consideration in RSA cryptosystem. At the end, the positive and negative primes plays the same role with respect to the definition of Euler's totient function.***

Keywords— Divisibility, Prime numbers, Euler's totient function, Cryptosystem, RSA

I. INTRODUCTION

The idea of securing secrets and breaking of codes serves humanity from ancient times. For instance, before the era of advanced knowledge of computer and mathematics, humans used to lock their precious things in some sort of box for which they have the key to unlock it. And this is the encryption scheme which is to be discussed, but of course, in mathematical perspective. Cryptography is a very technology in electronic key systems which can't be unseen. As cryptosystem focus on coding and decoding, we will notice that how numbers (especially the negative prime numbers) influence the whole area of RSA cryptosystem, starting from factoring, which is of great challenge in RSA. On the contrary, there are several methods to check if a number can be factored or not. We will also try to define Euler's totient function for negative integers.

II. NUMBER THEORY

Before going through the core, re-study of requisite concepts of number theory will suffice; including the idea of negative prime numbers.

Divisors and g.c.d:

If "a" is divisible by "b", then the additive inverse of "a" is also divisible by "b". Indeed, a = bq implies a = (-b) (-q), so that divisors of an integer always occur in pairs.
["b divides a" or "b is a divisor of a" or "b is a factor of a", written as b|a]

Now, the greatest common divisor of two integers "a" and "b", both non zero, is denoted by gcd (a, b), is the positive integer "d" satisfying the following: i) d|a , d|b and ii) if for any other integer "c", c|a and c|b, then $c \leq d$. Sometimes it is worth finding the number of divisors (either positive or negative) so as to have a better glimpse regarding divisibility criteria for an integer. In general, if for "a" and "b", both positive, we have gcd (a, b) = d then gcd (-a, -b) = d.

E.g. we know 4|8 and 4|36, so gcd (8, 36) = 4 because there doesn't exist any other integer greater than 4 which divides 8 and 36 simultaneously. In similar way gcd (-8, -36) = 4.

Prime numbers:

An integer $p > 1$ is called a prime number, if it is divisible only by 1 and p. Now, this definition motivates to think that the additive inverse of p possess exactly two negative divisors, which are -1 and –p. Moreover, a prime integer $p > 1$ is exactly divisible by 1, -1, p and –p. Therefore the additive inverse of p is also divisible by these four integers and hence notion of negative prime numbers can be raised.

Congruence's and Euler's totient function, Ø:

By division algorithm, given two integers "a" and "b", both non zero, there exist two unique integers "q" and "r", where $0 \leq r < |b|$, such that a = bq + r. This equality is also written as "$a \equiv r \pmod b$". The definition of Euler's totient function may be stated as, "for any given integer $n \geq 1$, the number of positive integers less than n and greater than 0 those are co-prime to n is denoted by Ø (n)". When n is prime then Ø (n) = n – 1, for which the converse is also true.
[Ø (1) = 1, because gcd (1, 1) = 1]

Let us consider $n < 0$, and Ø (n) be the number of negative integers greater than n and less than 0 those are co-prime to n. Since Ø (n) is a number, so it is free from sign. Hence if n is negative prime then Ø (n) = |n| – 1.
[Ø (-1) = 1, because gcd (-1, -1) = 1]

E.g. Ø (7) = 6, Ø (4) = 2 and Ø (-7) = 6, Ø (-4) = 2.

III. CRYPTOGRAPHY

Mathematically, an encryption scheme is a set of collection of all plaintexts, ciphertexts, keys, encryption functions and decryption functions. The essence of cryptosystem is to convert a plaintext (P) to a ciphertext (C) by

encrypting P with suitable encryption key (e). The C, thus obtained can be converted to again P by decrypting C with suitable decryption key (d). So, for each e in the set of keys there exists unique d in the same set. There are two kinds of cryptosystem: symmetric and asymmetric (also known as public-key cryptosystems).

The RSA with negative primes:

The whole idea of RSA is kept same; instead, we will consider the RSA modulus as a product of negative primes of roughly the same size.

Let us consider two randomly large negative primes of roughly the same size, and evaluate the RSA modulus n = pq. Now Ø (n) = (p – 1)(q – 1), as by the definition of Euler's totient function where p and q are both primes. The encryption key e is so chosen such that $1 < e < Ø(n)$ where Ø (n) and e are co-prime. The decryption key d is calculated in such a manner so that $1 < d < Ø(n)$ and $ed \equiv 1 \bmod (Ø(n))$.

The RSA modulus and the RSA encryption key is published keeping the RSA decryption key, p and q as private.

IV. CONCLUSIONS

In this paper, with the help of established celebrated Euler's totient function for integers greater than or equal to 1, the same function is defined for integers less than zero. Keeping this new definition marked, we seek liberty to take negative primes in RSA and found that the negative and positive prime numbers play the same role in basic steps. Further calculations may produce interesting result, taking negative primes into consideration. With the changing concept in the world of security systems the negative primes may leads us to new path.

REFERENCES

[1] Introduction to Cryptography, second edition, Springer, Johannes A. Buchmann
[2] Elementary number theory, sixth edition, Tata McGraw-Hill, David M. Burton
[3] An introduction to Cryptography, second edition, Chapman & Hall/ CRC Richard A. Mollin

