INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

(Volume 5, Issue 5)

Available online at: www.ijarnd.com

Three methods of finding remainder on the operation of modular exponentiation by using calculator

[1]Zin Mar Win, [2]Khin Mar Cho

[1]University of Computer Studies, Myitkyina, Myanmar

[2]University of Computer Studies, Pyay, Myanmar

ABSTRACT

The primary purpose of this paper is that the contents of the paper were to become a learning aid for the learners. Learning aids enhance one's learning abilities and help to increase one's learning potential. They may include books, diagram, computer, recordings, notes, strategies, or any other appropriate items. In this paper we would review the types of modulo operations and represent the knowledge which we have been known with the easiest ways. The modulo operation is finding of the remainder when dividing. The modulus operator abbreviated "mod" or "%" in many programming languages is useful in a variety of circumstances. It is commonly used to take a randomly generated number and reduce that number to a random number on a smaller range, and it can also quickly tell us if one number is a factor of another. If we wanted to know if a number was odd or even, we could use modulus to quickly tell us by asking for the remainder of the number when divided by 2. Modular exponentiation is a type of exponentiation performed over a modulus. The operation of modular exponentiation calculates the remainder c when an integer b rose to the eth power, b^e, is divided by a positive integer m such as $c = b^e \bmod m$ [1]. It is useful in computer science, especially in the field of public-key cryptography. The modulo operation is important for cryptography because it can act as a one-way function that the output obscures the input. In this paper we discuss the three methods of finding the remainder in the modular exponentiation based on the formula by using a calculator.

***Key*words**— *Learning Aid, Modulo Operation, Remainder, Modular Exponentiation, Calculator*

I. INTRODUCTION

To propose about our topic, we will first explain about the formula we used in this paper. We would use the formula from the public key data encryption scheme [3]. Data encryption means storing and transmitting sensitive data in encrypted form. The original data is called the plaintext and the encrypted form of the plaintext is called the ciphertext. In the public key encryption (RSA scheme) [3], to encrypt a piece of plaintext P, replace it by the ciphertext C, computed with the following formula:

$$C = P^e \text{ modulo } r.$$

And to decrypt a piece of ciphertext C, replace it by the plaintext P, computed with the following formula:

$$P = C^d \text{ modulo } r.$$

From the above formulae, we have seen that, to encrypt the plaintext and decrypt the ciphertext, we need to find the modulo value of exponentiation. In this paper we do not explain how to compute the value e, r and d because we would be focused only on the methods of finding modulo value. In practice, there are many types of more elaborate modular exponential operations that require more thought. In this paper we would represent the three methods in more clearly to approach on modular exponential operations. And to understand about these methods we displayed with an example that is based on a formula.

2. EXPLANATION OF THE METHODS

We would explain each method with the procedure and give an example to illustrate the foregoing procedure. In each method, we used the same example to prove that there has the same result.

Firstly, some terminologies we would need to know: [2]
If x mod y = r is true and if such an integer q exists, then:

$$y \times q + r = x.$$

In the above equation, the number r is the remainder of the division, where x is the dividend, y is the divisor and q is the quotient.

2.1. Method

The procedure is,

Step 1: Take the dividend
Step 2: Divide the dividend by divisor.
Step 3: Take the fraction value
Step 4: Multiply the step 3 value by divisor.

Example: Let P = 3, e =11, r = 15, d = 3

For encryption,

$$C = P^e \text{ modulo } r$$
$$C = 3^{11} \text{ modulo } 15$$

Step 1: 3^11= 177147
Step 2: 177147 ÷ 15= 11809.8
Step 3: 0.8
Step 4: 0.8×15=12
So, the ciphtertext C = 12

For decryption the ciphtertext C = 12

$$P = C^d \text{ modulo } r$$
$$P = 12^3 \text{ modulo } 15$$

Step 1: 12^3 = 1728
Step 2: 1728 ÷ 15= 115.2
Step 3: 0.2
Step 4: 0.2×15=3
So, we recapture the plaintext P = 3.

2.2 Method (2)

The procedure is,
Step 1: Take the dividend
Step 2: Divide the dividend by divisor.
Step 3: Take the quotient value
Step 4: Multiply the divisor by the quotient
Step 5: Subtract the step 4 value from dividend

Example: Let P = 3, e =11, r = 15, d = 3

For encryption,

$$C = P^e \text{ modulo } r$$
$$C = 3^{11} \text{ modulo } 15$$

Step 1: 3^11 = 177147
Step 2: 177147÷15=11809.8
Step 3: 11809
Step 4: 15×11809= 177135
Step 5: 177147-177135= 12
So, the ciphtertext C = 12

For decryption the ciphtertext C = 12

$$P = C^d \text{ modulo } r$$
$$P = 12^3 \text{ modulo } 15$$

Step 1: 12^3 = 1728
Step 2: 1728 ÷ 15= 115.2
Step 3: 115
Step 4: 115×15=1725
Step 5: 1728-1725 = 3
So, we recapture the plaintext P = 3.

2.3 Method (3)

When we want to calculate the A^B mod C for large values of B, our calculator can't handle numbers as big as this due to overflow. The calculator we have commonly used in our university is handled about up to 15 digits. In this situation, we do not have sufficiently to use only the method (1) or (2). We should also be used, the multiplication properties like the following: [2]

$$3^{40} = 3^{20} \times 3^{20}$$
$$3^{40} \text{ modulo } 5 = (3^{20} \text{modulo } 5 \times 3^{20} \text{ modulo } 5) \text{ modulo } 5$$

Example: Let P = 3, e =11, r = 15, d = 3

For encryption,

$$C = P^e \text{ modulo } r$$
$$C = 3^{11} \text{ modulo } 15$$
$$= (3^5 \text{ modulo } 15 \times 3^6 \text{ modulo } 15) \text{ modulo } 15$$
$$= (3 \times 9) \text{ modulo } 15$$
$$= 27 \text{ modulo } 15$$
$$= 12$$

So, the ciphtertext C = 12

For decryption the ciphtertext C = 12

$$P = C^d \text{ modulo } r$$
$$C = 12^3 \text{ modulo } 15$$
$$= (12 \text{ modulo } 15 \times 12^2 \text{ modulo } 15) \text{ modulo } 15$$
$$= (12 \times 9) \text{ modulo } 15$$
$$= 108 \text{ modulo } 15$$
$$= 3$$

So, we recapture the plaintext P = 3.

3. CONCLUSION

Modulo exponentiation methods are applied in many scientific areas, like computer algebra, cryptography, computer science, or simple school math. The methods in this paper are that may be already known for someone. But we have tried for easily learning to new one and kindly sharing to everyone. These three methods are indeed used for manually step by step but if you want to calculate with online calculator, we could share a website which included 1050 free calculator [2] for various areas such as chemistry, construction, conversion, ecology, etc. For reading this paper we believed that anyone can get some solution in operations of the modular exponentiation and some knowledge in data encryption.

4. ACKNOWLEDGMENT

First of all, I am grateful to the entire person who taught to me directly or indirectly. For encouraging and providing to write this paper, I would like also to thanks my colleagues. And then, I really thanks to all thankworthy person.

5. REFERENCES

[1] www.en.wikipedia.org, Modular exponentiation.
[2] www.omnicalculator.com, Modular Calculator [mod example]-Omni
[3] C.J.Date, 7th edition, An introduction to Database Systems, page 522-524

