SOME REAL PROBLEMS AND APPLICATION OF THE GREATEST COMMON DIVISOR, THE LEAST COMMON MULTIPLE

Hoang Minh Giang, Nguyen Thi Thu Hoa, Nguyen Thi Hong*

Hanoi Metropolitan University

Abstract: *One of the contemporary learning and teaching orientations in the general education curriculum in 2018 is to connect math to everyday lives and focus on applying mathematics concepts to solve real-world issues. As a result, we studied a variety of practical problems involving the greatest common divisor and least common multiple. Furthermore, we analyzed typical application problems and the RSA algorithm in cryptography. In particular, we came up with real-life problems involving the greatest common divisor and least common multiple and implemented the RSA algorithm in Maple.*

Keywords: *cryptosystem, RSA algorithm, key generation, key distribution, encryption, decryption, greatest common divisor, least common multiple, common divisor, common multiple, common factor, prime factor.*

Received 8 May 2022

Revised and accepted for publication 26 July 2022

(*) Email: nthong@daihocthudo.edu.vn

1. INTRODUCTION

The greatest common divisor and the least common multiple have many applications in practice as well as in mathematics. For example in finding the common denominator of two or more fractions; finding a way to evenly distribute the number of gifts to the students; queuing in sports,… More recently, its applications have also been found in cryptography, and computer science (see [2;3;5] and the reference therein). Here are some definitions and how to find the greatest common divisor and least multiple.

1.1. Divisor and multiple

Definition 1.1 *([2],p.1)*

If natural number a is divisible by natural number b, we say a is a multiple of b and we also call that b is a divisor of a.

Notation: $D(a)$ is the set of divisors of a.

$M(a)$ is the set of multiples of a.

1.2. Common divisor and greatest common divisor

Definition 1.2 *([6],p.51 &p.54)*

A common divisor of two or more numbers is the divisor of all the numbers.

The greatest common divisor of two or more numbers is the greatest number in the set of their common divisors.

Notation: $CD(a;b)$ is the set of common divisors of a and b.

$GCD(a;b)$ is the greatest common divisor of a and b.

How to find the greatest common divisor *([6],p.55)*

We find the greatest common divisor by factoring numbers into prime factors. So finding GCD of two or more numbers greater than 1, we do the three steps as follows:

Step 1: Factor each number into prime factors

Step 2: Choose common factors

Step 3: Make a product of chosen factors, with the smallest exponent for each factor.

That product is GCD which we have to find

1.3. Common multiple and least common multiple

Definition 1.3 *([6], p.52 &p.57)*

A common multiple of two or more numbers is the multiple of all the numbers.

The least common multiple of two or more numbers is the leasr non-zero number in the set of their common multiples.

Notation: $CM(a;b)$ is the set of common multiples of a and b.

$LCM(a;b)$ is the least common multiple of a and b.

How to find the least common multiple *([6], p.58)*

We find the least common multiple by factoring numbers into prime factors. So finding LCM of two or more numbers greater than 1, we do the three steps as follows:

Step 1: Factor each number into prime factors

Step 2: Choose common and individual factors

Step 3: Make a product of chosen factors, take for each factor with its highest exponent.

That product is LCM which we have to find.

2. SOME REAL PROBLEMS ABOUT THE GREATEST COMMON DIVISOR AND THE LEAST COMMON MULTIPLE

2.1. Problem about "the area"

Example 1: Uncle Tan has a rectangular field with $70m$ long and $42m$ wide. He wants to divide this field into the equal squares with the units of meters in order to grow flowers and fruits. So with this division, what is the maximum length of this square side?

Analysis: Uncle Tan wants to divide the rectangular field into the equal squares so the length and the width of the rectangle field is divisible by the length of the square side. Therefore, the length of the square side is the common divisor of 70 and 42.

Solution:

Let a be the length of the square side $(meter; 0 < a < 42)$.

According to the exercise 1, uncle Tan divides the rectangular field into the equal squares in order to grow flowers and fruits so a is the common divisor of 70 and 42.

If the length of the square side is the maximum, then a must be the greatest common divisor of 70 and 42. $So\ a = GCD(70; 42)$.

Now, we find the greatest common divisor of 70 and 42. We have: $70 = 2.5.7;\ 42 = 2.3.7.$

Hence $GCD(70; 42) = 2.7 = 14 \Rightarrow a = 14$ (satisfied).So the length of the largest square side is 14 meters.

2.2. Problem about dividing the number of people or things

Example 2: The homeroom teacher at class 5A of Cu Khoi primary school wants to divide 36 notebooks, 18 boxes of crayons and 60 ballpoint pens into some equal rewards to give to students on the year-end celebration. What is the greatest number of rewards that can be divided into? How many notebooks, boxes of crayons and ballpoint pens are there for each reward?

Analysis: Because the homeroom teacher at class 5A of Cu Khoi primary school wants to divide 36 notebooks, 18 boxes of crayons and 60 ballpoint pens into some equal rewards so the number of notebooks, boxes of crayons and ballpoint pens in each prize is the common divisor of $36; 18; 60$.

Solution:

Let a be the number of rewards which the homeroom teacher at class 5A of Cu Khoi primary school gives to students on the year-end celebration $(a \in \mathbb{N}^*; a < 18)$.

Because the homeroom teacher at class 5A of Cu Khoi primary school wants to divide 36 notebooks, 18 boxes of crayons and 60 ballpoint pens into some equal rewards so a is the common divisor of 36; 18 and 60.

If the reward is the maximum, then a must be the largest number such that $36 \vdots a; 18 \vdots a; 60 \vdots a$. Therefore: $a = GCD(36; 18; 60)$.

Now, we find the greatest common divisor of 36; 18 and 60. We have:

$$36 = 2^2.3^2;\ 18 = 2.3^2; 60 = 2^2.3.5$$

Thus $GCD(36; 18; 60) = 2.3 = 6 \Rightarrow a = 6$ (satisfied). Therefore, it is possible to divide at most into 6 rewards are 6 notebooks, 3 boxes of crayons and 10 ballpoint pens.

2.3. The problem about queuing

Example 3: The number of students in grade 6 of Cu Khoi middle school is divided into three classes: 6A, 6B and 6C. The class 6A has 45 students, the class 6B has 50 students and the class 6C has 55 students. During the flag-raising ceremony on the first of the week, both of them line up in some equal vertical rows to salute the flag without any odd people in each class. Find the maximum number of vertical rows that can be lined.

Analysis: Because the number of students in grade 6 of Cu Khoi middle school line up in some equal vertical rows to salute the flag without any odd people in each class so the number of vertical rows is the common divisor of 54; 42 and 48.

Solution:

Let a be the number of vertical rows that can be lined $(a \in \mathbb{N}^*; a < 45)$.

According to the exercise 3, the number of students in grade 6 of Cu Khoi middle school is divided into three classes: 6A, 6B, 6C and during the flag-raising ceremony on the first of the week, both of them line up in some equal vertical rows to salute the flag without any odd people in each class so a is the common divisor of 54; 42 amd 48.

If the vertical row is the maximum, a must be the largest number such as $54 \vdots a; 42 \vdots a; 48 \vdots a$. Therefore: $a = GCD(54; 42; 48)$.

Now, we find the greatest common divisor of 54; 42 and 48. We have:

$$54 = 2.3^3;\ 42 = 2.3.7;\ 48 = 2^4.3$$

Hence $GCD(54; 42; 48) = 2.3 = 6 \Rightarrow a = 6$ (satisfied). So the maximum number of vertical rows is 6.

2.4. Mathematics problems about calculating the number of days or hours for some objects to work together.

Example 4: Mai and Lan are students of Bat Trang middle school but in two different classes. Mai scans the classroom every 15 days and Lan scans the classroom every 9 days. At the first time, both of them scan the classroom on the same day. At least how many days do they scan the classroom on the same day again?

Analysis: Because Mai and Lan are students of Bat Trang middle school but in two different classes, Mai scans the classroom every 15 days and Lan scans the classroom every 9 days so the number of days which both of them scan the classroom on the same day is the common multiple of 15 and 9.

Solution:

Let a be the number of days which both of them scan the classroom on the same day $(a \in \mathbb{N}^*; a > 15)$.

Because Mai and Lan are students of Bat Trang middle school but in two different classes, Mai scans the classroom every 15 days and Lan scans the classroom every 9 days so a is the common multiple of 15 and 9.

If the number of days is the maximum, a must be the least common multiple of 15 and 9. Therefore: $a = LCM(15; 9)$.

Now, we find the least common multiple of 15 and 9. We have:$15 = 1.3.5; 9 = 1.3^2$.

Therefore $LCM(15; 9) = 1.3^2.5 = 9.5 = 45$. Hence $a = 45$ (satisfied).

So at least 45 days they scan the classroom on the same day again.

3. APPLICATION OF THE GREATEST COMMON DIVISOR AND THE LEAST COMMON MULTIPLE

RSA algorithm

GCD can be used for several applications in modular arithmetic. One of the applications is RSA algorithm. Derived in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman, RSA has become a commonly used public-key cryptosystem.

There are four steps in implementing RSA algorithm: key generation, key distribution, encryption and decryption.

Key generation.

Being an asymmetric cryptosystem, RSA involves a public key and a private key.

The key generation is based on idea of creating a one-way function with intention that the ciphertext would only be decrypted in a 28hần2828ntial amount of time using the private key (see Fig.1).

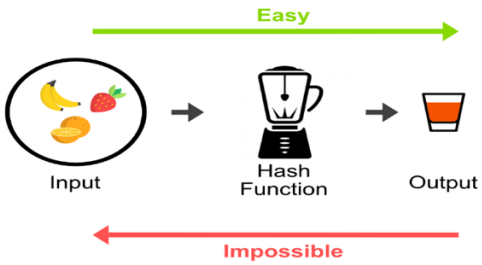

Fig 1. One way functions are easy to compute but it is extremely hard to compute their inverse functions. (© Bill MacKenty)

The keys are generated as follow:

1. Choose distinct large prime numbers p and q. These numbers are kept secret.
2. Compute $n = pq$. This is the modulus for public key and private key.
3. Calculate $\phi(n)$ and $\phi(n)$ is kept secret.
4. Choose e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.
   e is the public key exponent.
5. Determine the private key exponent $d = e^{-1}\ (mod\ \phi(n))$ using the extended Euclidean algorithm. According to Bézout's identity, there exist s, t such that $s \cdot e + t \cdot \phi(n) = \gcd(e, \phi(n)) = 1$.

We can set $d = s$ if $s > 0$ and $d = \phi(n) - s$ if $s < 0$.

The public key is (n, e) and the private key is (p, q, d).

Key distribution

We suppose that Bob wants to send a message to Alice and among them, there are intermediaries such as wifi points, internet service providers and their email servers and eavesdroppers. To use RSA, Alice transmits her public key (n, e) to Bob and keeps her private key d. Bob then uses Alice's public key to encrypt the message. After receiving the ciphertext, Alice can use her private key to decrypt it.

Encryption

The message is encoded to an integer m such that $0 \leq m < n$.

Using Alice's public exponent key e, the ciphertext $c = m^e \ (mod\ n)$.

Bob then transmits the ciphertext to Alice.

Decryption

Alice can decrypt the ciphertext c by using her private key exponent d by computing $c^d = (m^e)^d = m \ (mod\ n)$.

Then, Alice can decode m to get the original message. [7][9]

Fig 2. Encrypting and decrypting data using RSA

We implemented RSA algorithm in Maple 2020 as follow:

```
# RSA(Rivest-Shamir-Adleman) algorithm
restart:
with(StringTools):
list_to_str := proc(list_of_int)
local list_of_str:
list_of_str := map(x -> convert(x, string),  list_of_int):
return Join(list_of_str, "")
end proc:
list_hex_format:= proc(dec_list)
local list_of_hex:
list_of_hex := map(x -> convert(x, 'hex'), dec_list):
```

```
return  Join(list_of_hex, “”)
end proc:
min_public_exp := proc(totient_n)
local min_exponent_e:
for min_exponent_e from 2 to totient_n do
      if gcd(min_exponent_e, totient_n) = 1 then
            break
      end if:
end do:
return min_exponent_e
end proc:
private_exponent := proc(public_exponent, totient)
local s, t, private_exp_key:
description “compute private key exponent d:” \
          “d * e = 1 (mod phi_n) using extended Euclidean algorithm” \
          “Bezout’s identity gcd(e, phi_n) = 1 = d * e + t * phi_n”:
igcdex(public_exponent, totient, ‘s’, ‘t’):
if s > 0 then
      private_exp_key := s:
else
      private_exp_key := totient  +  s:
end if:
return private_exp_key
end proc:
encrypting_str := proc(msg, pub_key)
description “description function f(message, public_key) “:
return  msg ^ pub_key[2] mod modulus_n:
end proc:
decrypting_str := proc(cipher, private_exp)
description “decrypting function g(c, k’) = c^d mod n = original_msg” \
          “private key k’ = (p, q, d) or (n, d) -> decrypt” :
return  cipher^private_exp mod modulus_n
end proc:
```

```
decrypted_txt := proc(decrypted_dec)
description “convert list of decimal equivalents back to text”:
return Join(map(x -> Char(x), decrypted_dec), “”);
end proc:
# RSA algorithm
# secret message m
# msg_str := “The quick brown fox jumps over the lazy dog”;
# convert the message to decimal equivalents
msg_decimal := map(Ord, Explode(msg_str));
msg_decimal_str := list_to_str(msg_decimal);
“Message in hex format” = list_hex_format(msg_decimal);
# 1. Choose different large random prime numbers p & q
private_key_p := 257;
private_key_q := 263;
# 2. Calculate n = p * q = modulus for public key & private key
modulus_n := private_key_p * private_key_q;
# 3. Euler’s totient function: (private) phi(n) = (p – 1) * (q – 1)
phi_n := (private_key_p – 1) * (private_key_q – 1);
# phi_n := NumberTheory:-Totient(n);
# 4. Choose public key exponent 1 < e < phi(n), gcd(e, phi(n)) = 1
# short bit-length, small Hamming weight -> more efficient encryption
# (smallest/fastest/ least secure) public key exponent
public_exponent_key := min_public_exp(phi_n);
# 5. Compute private key exponent d:   d * e = 1 (mod phi_n)
private_exponent_key := private_exponent(public_exponent_key, phi_n);
# 6. Public_key k = (modulus_n, public_exponent_key) -> encrypt
public_key := [modulus_n, public_exponent_key]:
public_key_hex := map(x -> convert(x, ‘hex’), public_key);
# 7. Apply the encrypting function on (message, public_key)
encrypted_decimals := map(x -> encrypting_str(x, public_key), msg_decimal);
encrypted_decimal_str := list_to_str(encrypted_decimals);
“Cipher text” = list_hex_format(encrypted_decimals);
# 8. Apply the decrypting function on (c, d)
```

```
# the same as msg_decimal
decrypted_decimals := map(x -> decrypting_str(x, private_exponent_key),
                                    encrypted_decimals);
"Decrypted message" =  list_hex_format(decrypted_decimals);
decrypted_str = decrypted_txt(decrypted_decimals);
```

The important results obtained are in Fig 4 and Fig 5. Here, the message to be sent is "The quick brown fox jumps over the lazy dog". It is a popular English pangram that contains all English alphabets. We then convert the alphabets to its ASCII decimal equivalents and display the message in hex format. The public key is $(n, e) = (67591,\ 3)$ is used to encrypt the message, then the cipher text is displayed in hex format. After using the private exponent key is $d = 44715$, we obtain the original message.

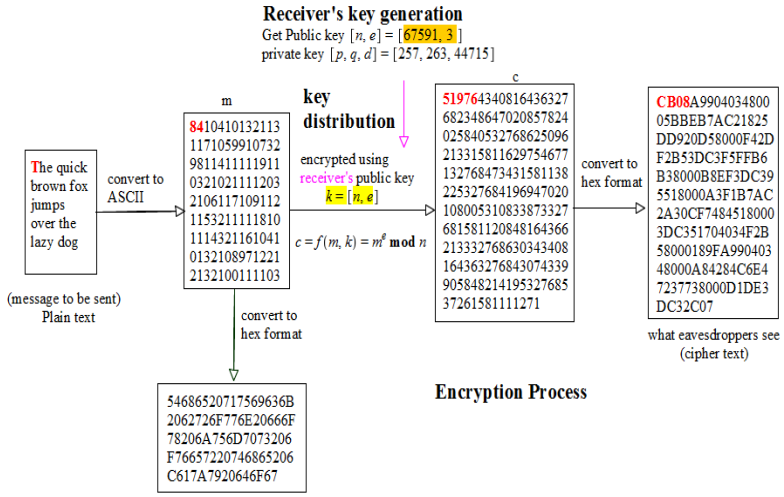

Fig 4. Encryption process

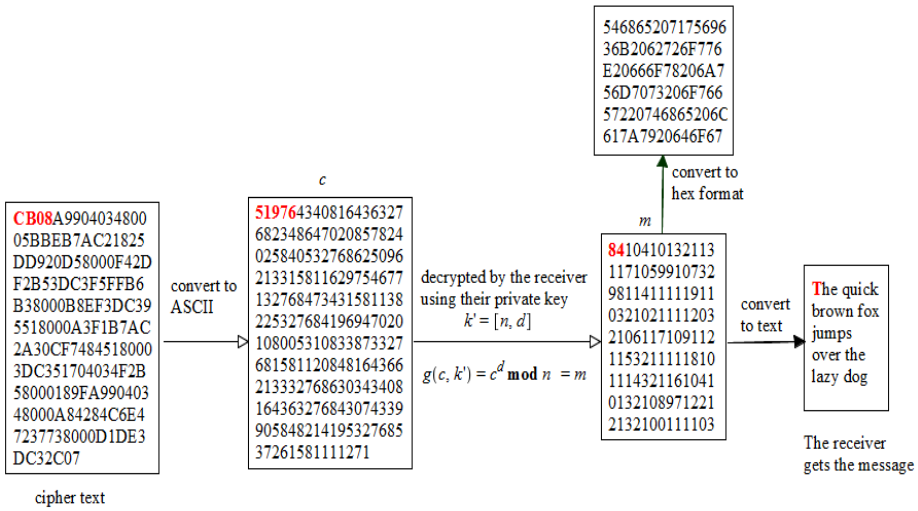

Fig 5. Decryption process

4. CONCLUSION

The article presents some real problems about the greatest common divisor and the least common multiple in practice. Moreover we analyzed typical application problems and the RSA algorithm in cryptography.

REFERENCE

1. R.L. Rivest, A. Shamir, and L.M. Adleman (1978), "A Method for Obtaining Digital Signature and Public-key Cryptosystems", *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126.
2. Hengki Tamando Sihotang et al (2020), "Design and Implementation of Rivest Shamir Adleman's (RSA) Cryptography Algorithm in Text File Data Security", *Journal of Physics: Conference Series.*
3. George E. Andrews (1971), *Number theory,* Saunders company.
4. Hà Huy Khoái (tổng chủ biên*), sách giáo khoa toán 6 tập 1 bộ kết nối tri thức với cuộc sống*, Nhà xuất bản giáo dục Việt Nam.
5. Lê Đức Thuận – Tạ Ngọc Trí (đồng chủ biên), *Sách củng cố và ôn luyện Toán 6 tập 1*, Nhà xuất bản đại học quốc gia Hà Nội.
6. Bộ Giáo Dục và Đào Tạo, *sách song ngữ việt – anh toán 6 tập 1*, Nhà xuất bản giáo dục Việt Nam.

MỘT SỐ BÀI TOÁN THỰC TẾ VÀ ÁP DỤNG CỦA ƯỚC CHUNG LỚN NHẤT, BỘI CHUNG NHỎ NHẤT

Tóm tắt: *Một trong những định hướng của chương trình giáo dục phổ thông môn toán năm 2018 đó chính là kết nối toán học với thực tiễn, vận dụng toán học vào thực tiễn. Nhằm góp phần phát triển mục tiêu của chương trình giáo dục phổ thông, chúng tôi nghiên cứu một số bài toán thực tiễn và áp dụng của ước chung lớn nhất và bội chung nhỏ nhất. Hơn nữa, chúng tôi trình bày năm dạng bài toán thực tế liên quan đến ước chung lớn nhất, bội chung nhỏ nhất và một áp dụng của ước chung lớn nhất trong thuật toán RSA trong ngành mật mã học. Cụ thể chúng tôi xây dựng được các ví dụ về các bài toán thực tế và triển khai được thuật toán RSA trong 33hần33.*

Từ khoá: *hệ thống mật mã, thuật toán RSA, tạo khóa, 33hần phối khóa, mã hóa, giải mã, ước chung lớn nhất, bội chung nhỏ nhất, ước chung, bội chung, thừa số chung, thừa số nguyên tố.*