Number Theory
نظرية الاعداد

The part of mathematics involving the integers and their properties belongs to the branch of mathematics called **number theory**.

1. Division

Definition// If a and b are integers with a # 0, we say that a divides b if there is an integer c such that b = ac. When a divides b we say that a is a factor of b and that b is a multiple of a . The notation a | b denotes that a divides b. We write a |/ b when a does not divide b.

EX//Determine whether 3 |7 and whether 3 |12.

<u>Solution:</u>

It follows that 3 |/7, because 7/3 is not an integer. On the other hand, 3 |12 because 12/3 = 4.

Definition// In the equality given in the division algorithm, d is called the divisor, a is called the dividend, q is called the quotient, and r is called the remainder. this notation is used to express the quotient and remainder:

$q = a \text{ div } d,\ r = a \bmod d.$

EX// What are the quotient and remainder when 101 is divided by 11?

Solution: We have $101 = 99 + 2.$

Hence, the quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \bmod 11$.

2. Primes

Every positive integer greater than 1 is divisible by at least two integers, because a positive integer is divisible by 1 and by itself. Positive integers that have exactly two different positive integer factors are called primes.

- A positive integer that is greater than 1 and is not prime is called **composite**.

Remark: The integer n is composite if and only if there exists an integer a such that $a|n$ and $1 < a < n$.

EX// The integer 7 is prime because its only positive factors are 1 and 7, whereas the integer 9 is composite because it is divisible by 3 .

The primes less than 100 are 2, 3 , 5, 7, 11 , 13 , 17, 19, 23, 29, 31 , 37, 41 , 43, 47, 53, 59, 61 ,67, 71 , 73, 79, 83, 89, and 97.

EX// The prime factorizations of 100, 999, and 1024 are given by

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 . 5^2 ,$
$999 = 3 . 3 \cdot 3 \cdot 37 = 3^3 \cdot 37,$
$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10} .$

EX// Find the prime factorization of 7007.

Solution:

To find the prime factorization of 7007, first perform divisions of 7007 by successive primes, beginning with 2. None of the primes 2, 3 , and 5 divides 7007.

However, 7 divides 7007, with 7007/7 = 1001 . Next, divide 1001 by successive primes, beginning with 7. It is immediately seen that 7 also divides 1001 , because 1001 /7 = 143 .

Continue by dividing 143 by successive primes, beginning with 7.

Although 7 does not divide 143, 11 does divide 143, and 143 / 11 = 13 .

Because 13 is prime, the procedure is completed. It follows that the prime factorization of 7007 is $7 . 7 . 11 . 13 = 7^2 . 11 . 13$.

Greatest Common Divisors (GCD)

The largest integer that divides both of two integers is called the greatest common divisor of these integers.

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by $\gcd(a , b)$.

EX// What is the greatest common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1 , 2, 3 , 4, 6, and 12 . Hence, gcd(24, 36) = 12 .

2	24
2	12
2	6
3	3
	1

2	36
2	18
3	9
3	3
	1

24=2*2*2*3
36=2*2*3*3
GCD(24,36)=2*2*3
GCD(24,36)=12

EX// What is the greatest common divisor of 17 and 22?

Solution: The integers 17 and 22 have no positive common divisors other than 1 , so that gcd(17, 22) = 1 .

17	17
	1

2	22
11	11
	1

- **The second way** to find the greatest common divisor of two integers is to use the **prime factorizations** of these integers. Suppose that the prime factorizations of the integers a and b, neither equal to zero, are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \; b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each exponent is a nonnegative integer, and where all primes occuring in the prime factorization of either a or b are included in both factorizations, with zero exponents if necessary. Then gcd(a , b) is given by

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)},$$

EX/ Because the prime factorizations of 120 and 500 are $120 = 2^3 . 3 . 5$ and $500 = 2^2 . 5^3$, the greatest common divisor is

120	2
60	2
30	2
15	3
5	5
1	

500	2
250	2
125	5
25	5
5	5
1	

$$\gcd(120, 500) = 2^{\min(3,\,2)}3^{\min(1,\,0)}5^{\min(1,\,3)} = 2^2 3^0 5^1 = 20.$$

EX// Find GCD of each by finding the prime factorizations?

1. gcd (2415,3289)
2415=3.5.7.23
3289=11.13.23
gcd (2415,3289) =23

2. gcd (406,555)
406=2.7.29
555=3.5.37
gcd (406,555) =1

3. gcd (4278,8602)
4278=2.3.23.31
8602=2.11.17.23
gcd (4278,8602) =2.23=46

➢ **The third way to find GCD is Euclidean Algorithm**

The Euclidean Algorithm

This method asks you to perform successive division:

1. The smaller of 2 number into the larger
2. The resulting remainder divided into divisor until the remainder is equal zero, of that point look to the remainder of the previous division that will be the greatest common divisor.

The Euclidean Algorithm.

```
procedure gcd(a , b: positive integers)
{x := a
y := b
while (y =! 0)
begin
r := x mod y
x := y
y := r
end (gcd(a , b) is x }
```

In Algorithm , the initial values o f x and y are a and b, respectively. At each stage of the procedure, x is replaced by y, and y is replaced by x mod y, which is the remainder when x is divided by y. This process is repeated as long as $y \neq 0$. The algorithm terminates when $y = 0$, and the value of x at that point, the last nonzero remainder in the procedure, is the greatest common divisor of a and b.

EX// Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution:

Successive uses of the division algorithm give:

x =662, y =414, r =248

x =414, y =248, r =166

x =248, y =166, r =82

x =166, y =82 , r =2

x =82, y =2, r =0

x =2, y =0

Hence, gcd(414, 662) = 2, because 2 is the last nonzero remainder.

EX// Find the gcd (1424,3084) using Euclidean

Solution:

Successive uses of the division algorithm give:

$x = 3084$, $y = 1424$, $r = 236$

$x = 1424$, $y = 236$, $r = 8$

$x = 236$, $y = 8$, $r = 4$

$x = 8$, $y = 4$, $r = 0$

$x = 4$, $y = 0$

Hence, gcd(1424,3084) = 4, because 4 is the last nonzero remainder.

Applications of Number Theory

Congruence's have many applications to discrete mathematics and computer science. One of these is cryptology, which is the study of secret messages. One of the earliest is Julius Caesar by shifting each letter three letters forward in the alphabet.

In the encrypted version of the message, the letter represented by p is replaced with the letter represented by (p + 3) mod 26.

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

a b c d e f g h i j............z K l m n o p q r s t u v w x y z

The P integer p<=25 can be replaced by

£(p)=(p+3)mod 26

Let p= 6 which is the char 9

£(p)= (6+3) mod 26

=9 which is the char j

Then we replace g by j

EX// What is the secret message produced from the message "MEET YOU IN THE PARK" using the Caesar cipher?

Solution: First replace the letters in the message with numbers.

This produces

12 4 4 19   24 14 20   8 13   19 7 4   15 0 17 10.

Now replace each of these numbers p by

$f(p) = (p + 3) \bmod 26.$

This gives

I5 7 7 22   1 17 23   11 16   22 10 7   18 3 20 13 .

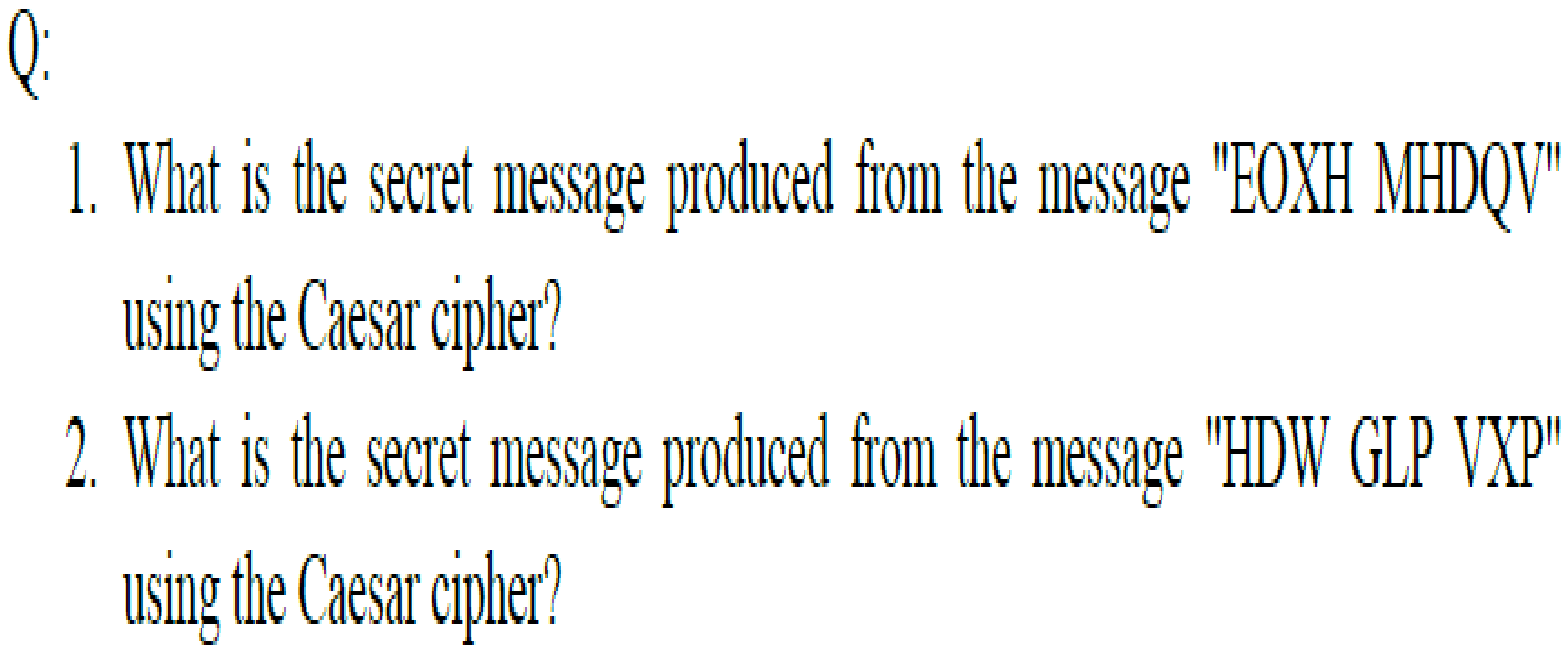
Translating this back to letters produces the encrypted message

"PHHW B RX LQ WKH SDUN."

The decryption

£′(p)= (p-3) mod 26

HOMEWORK :



Q:

1. What is the secret message produced from the message "EOXH MHDQV" using the Caesar cipher?
2. What is the secret message produced from the message "HDW GLP VXP" using the Caesar cipher?

Hashing Functions

The central computer at an insurance company maintains records for each of its customers. How can memory locations be assigned so that customer records can be retrieved quickly? The solution to this problem is to use a suitably chosen hashing function.

Records are identified using a key, which uniquely identifies each customer's records. For instance, customer records are often identified using the Social Security number of the customer as the key. A hashing function h assigns memory location h (k) to the record that has k as its key.

In practice, many different hashing functions are used. One of the most common is the Function $h(k) = k \bmod m$

where m is the number of available memory locations.

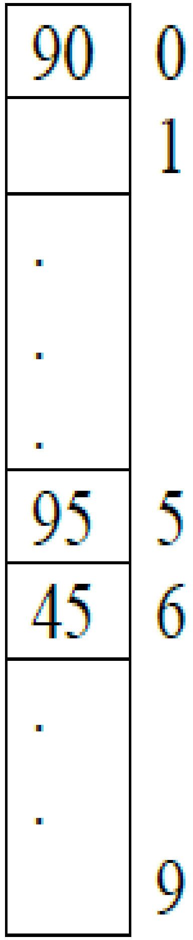
Hashing functions should be easily evaluated so that files can be quickly located. The hashing function $h(k) = k \bmod m$ meets this requirement; to find $h(k)$, we need only compute the remainder when k is divided by m . Furthermore, the hashing function should be onto, so that all memory locations are possible. The function $h(k) = k \bmod m$ also satisfies this property.

EX1// Let m=10, find hashing function to 95,90,45

Solution:

1. H(95)= 95 mod 10= 5
2. H(90)= 90 mod 10= 0
3. H(45)= 45 mod 10= 5

To solve this assign the first free location, the following location 45 set to 6 .



EX2// parking has (31) visitor spaces, numbered from 0 to 30. Visitation use hashing function h(k)= k mod 31, where k is the number of the car : 317, 918, 100, 111, 310.

<u>Solution:</u>

1. h(317)= 317 mod 31= 7
2. h(917)= 917 mod 31= 18
3. h(100)= 100 mod 31= 7
4. h(111)= 111 mod 31= 18
5. h(310)= 310 mod 31= 0

310	0
	1
. .	
317	7
100	8
. .	
918	18
111	19
. .	
	30