On the Divisor of Numbers

Ishaan Gupta, Saumya Gautam

Abstract – We analyze theories related to divisibility and divisors of numbers as currently understood. We then elucidate the different kinds of typical mathematical problems where they can be useful.

Keywords – Division Algorithm, Fundamental theorem of arithmetic, Divisibilty tests, Fermat's Little theorem, divisibility, applications of divisibility

1 INTRODUCTION

Consider the set of integers denoted by symbol **Z**. If a, d ∈ **Z**, d ≠ 0, we say that d is a divisor of a if ∃ a_1 ∈ **Z** such that a= a_1 d and we write d|a i.e. d divides a. The set N of positive integers is contained in **Z**, the definition of division is the same as in **Z**. But the divisors of a positive integer present some interesting results.

2 PREREQUISITES

2.1 Division Algorithm

If a, b ∈ **Z**, b >0, ∃ integers q and r such that a= bq +r when 0≤ r < b;q is called the quotient and r the remainder in the division of a and b. In case r= 0, we say b|a in **Z**. The set N of numbers is partially ordered with respect to relation of division i.e. it is reflexive, asymmetric and transitive.

If a, b are integers, not both zero, greatest common divisor (GCD) of a and b is the unique +ve integer d such that (i) d|a and d|b (ii) if c|a and c|b, then c|d and we write d=(a, b). In case d=1, we say a and b are co-prime. In case p>1 ∈ N and p and 1 are only divisors of p, then p is called a prime, otherwise called composite.

The following result is quite useful:

Let a, b ∈ **Z** not both of which are zero and d=(a, b), then ∃ integers x and y such that ax+ by =d

2.2 Fundamental theorem of arithmetic

Each integer a >1 can be expressed as a product of primes in one and only one way (except of the order of factors).[1]

2.3 Divisibility tests

Next we discuss divisibility test:
It is useful when we have to decide a number consist of large number of digits divisible or not by a prescribed number
without carrying out actual division i.e. by simple inspection or by small calculations. We present divisibility test as follows –

- A number is divisible by 2 if and only if last (units) digit is divisible by 2.
- A number is divisible by 3 if and only if the sum of its digits is divisible by 3.
- A number is divisible by 4 if and only if its units digit plus twice its tens digit is divisible by 4
- A number is divisible by 5 if and only if its units digit is 5 or 0.
- A number is divisible by 6 if and only if its units digit is even and sum of its digits is divisible by 3.
- A number is divisible by 7 if and only if 3 times units digit + 2 times tens digit -1 times hundreds digit -3 times thousands digit -2 times ten thousands digit + 1 times hundred thousands digit (if there are more digits present, the sequence of multiples 3, 2, -1, -3, -2, 1 is repeated as often as necessary) is divisible by 7.
- A number consists of 24 digits, each digit same, is divisible by 7.
- A number is divisible by 8 if and only if unit digit +2 times tens digit + 4 times hundreds digit is divisible by 8.

- A number is divisible by 9 if and only if sum of its digit is divisible by 9.
- A number is divisible by 10 if and only if its last digit is 0.
- A number is divisible by 11 if and only if unit digit –tens digit + hundred digit – thousands digit and so on is divisible by 11.
- A number is divisible by 12 if it is divisible by 3 and 4.
- A number is divisible by 13 if and only if 10 times unit digit -4 times tens digit -1 times hundreds digit +3 times thousands digit +4 times ten thousands digit + 1 times hundred thousands digit (if there are more digits present, the sequence of multiplication 10, -4, -1, 3, 4, 1 is repeated as often as necessary.)

If (a, b)=1, and n is divisible by a as well as b , then n is also divisible by ab.

As an illustration of the proof of divisibility we take a three digit number and 7 as divisor i.e. n=abc

2.1 =100a +10b +c

be the three digit number if s= 3c+ 2b –a , say, so that

2.2 2s= 6c +4b -2a

n+2s= 98a + 14b +7c
= 7(14a +2b +c)
=7m

Say, in case n is divisible by 7, then n=7k, say 7k + 2s =7m => 7(m-k) =2s
But (2, 7) =1, i.e 7∣s
Conversely if s is multiple of 7 say r=7q, then
n ≠2s=7m
n=7m - 14q
=7(m-2q)
i.e. n is multiple of 7.

2.4 Modulo function

Let m>1 be a positive integer.
If a, b ∈ $\mathbb{Z}$ are such that m(a-b),we write it as a ≡ b (mod m) and say a is congruent to b modulo m. Clearly it is a relation on $\mathbb{Z}$, called congruence relation. Also when both a, b are divided by m, the remainder is same. Then we can verify the elementary properties of the congruence relation:-
(i) it is an equivalent relation and splits $\mathbb{Z}$ into m congruence
(ii) if a≡ a′ (mod m)
b ≡ b′ (mod m), then
a ± b ≡ a′ ± b′ (mod m)
(iii) ab ≡ a′ b′ (mod m)
(iv) pa ≡ pa′ (mod m)
(v) if (k, m) = d, then ka ≡ ka′ (mod m) ⇔ a ≡ a′ mod (m/d)

3 DIVISOR FUNCTION

Let d denote the divisor function i.e. d: N → N such that d(n) is the number of divisors of n including 1 and itself.

If we take a pair of coprimes, m and n, each factor of mn has to be a product of one factor of m and one factor of n. Thus, d(mn) is equal to the total number of ways to multiply one of d(m) number of factors of m with one of d(n) number of factors of n, which is d(m) x d(n). Thus d (mn) = d (m) d(n) when (m, n)=1; i.e, divisor function is multiplicative for 2 coprimes. If n is any number >1, by Fundamental Theorem of Arithmetic

3.1 $n= p_1^{\alpha 1}.........p_k^{\alpha k}$,

p_i's are distinct primes and

α_i's are exponent

We know

3.2 $d(n)= \prod_{i=1}^{k} (\alpha_i +1)$

3.3 $\sigma(n)=\prod_{i=1}^{k} \frac{(p_i^{(\alpha i+1)}-1)}{(p_i-1)}$ $=\sum_{d\mid n} d$ i.e. sum of all divisors of n taken individually.

Def: let p be a fixed given prime, a>1 be a positive integer, then k (a) is the largest integer t such that $p^t \mid a$ and

3.4 $k(n!)=\sum_{s=1} \left[\frac{n}{p^s}\right]$

Where $\left[\frac{n}{p^s}\right]$ is greatest integer function of $\frac{n}{p^s}$

4 Euler's theorem, Fe
theorem

Def: the Euler function [2] is defined as (m), is the number of numbers m and co-prime to m
The Euler function is multiplicative

Euler's theorem [2]
if (a, m) =1, then $a^{d(m)} \equiv 1 (\text{mod } m)$

Fermat's little theorem [3]
if p is a prime, p does not divide a, then $a^{p-1} \equiv 1 (\text{mod } p)$

5 APPLICATIONS IN PROBLEMS

We apply above stated results in the following problems-

Q1- Find the number of digits in $2^{14} \times 3^2 \times 5^{12} \times 7$

Sol. $= 2^{14} \times 3^2 \times 5^{12} \times 7$
$= (2\times5)^{12} \times 2^2 \times 3^2 \times 7$
$= 10^{12} \times 252$
Therefore, number of digits in the given number is 15.

Q2- Find digits a and b so that the number n=a759b is divisible by both 8 and 9.

Sol. n is divisible by 8 if b+ 18 +20 is divisible by 8, i.e. b + 38 is divisible by 8 b = 2 n=a7592 and it is divisible by 9 a + 7 + 5 + 9 + 2 is also divisible by 9, i.e. a +23 is divisible by 9.
a= 4

Q3. Show that the fraction $\frac{21n+4}{14n+3}$ is irreducible for all natural numbers n.

Sol. let g be a common divisor of 21n+4 and 14n+ 3.denote 21n+4 = gA, 14n +3=gB. Then g(3B-2A) =1. Then the factorization is not reducible.

Q4- Show for every positive integer n, $11^{n+2} + 122^{n+1}$ is divisible by 133.

Sol. The result is true for n=0 and n=1

Let the result hold true for positive integer k
$M_k = 11^{k+2}+122^{k+1}$ is divisible by 133.
Consider $M_{k+1}=11^{k+3}+12^{2k+3}$
$=11 (11^{k+2}+122^{k+1})+133 \times 12^{2k+1}$
$=11 M_k+133 \times 12^{2k+1}$
Since M_k is divisible by 133 and $133 \times 12^{2k+1}$ is divisible by 133, M_{k+1} is divisible by 133.
Thus by principal of mathematical induction, for every positive integer n, $11^{n+2} + 122^{n+1}$ is divisible by 133

Q5-Show that 1-1/2+1/3-1/4.........+1/199-1/200 = 1/101+1/102+..........+1/200.

Sol. 1/101+1/102+..........+1/200
=(1+1/2+1/3+1/4.........+1/199+1/200) - (1+1/2+1/3+1/4.........+1/99+1/100)
=(1+1/3+1/5.........+1/199) + 1/2(1+1/2+1/3+1/4.........+1/99+1/100) - (1+1/2+1/3+1/4.........+1/99+1/100)
=1+1/3+1/5.........+1/199-1/2-1/4…...-1/200
=1-1/2+1/3-1/4.........+1/199-1/200

Q6- Find the remainder when 2^{2003} is divided by 17.

Sol. We have (2, 17) = 1, 17 is a prime by fermat's theorem,
$2^{16} \equiv 1 (\text{mod } 17)$
$2^{2003}=(2^{16})^{125}.2^3$
$\equiv 2^3 (\text{mod } 17)$
$=8$
Thus remainder obtained when 22003is divided by 17 is 8.

Q7- Find the units digit of 7^{87}.

Sol. Units digit of 7^{87} is equivalent to 7^{87}(mod 10)
7 is a prime and (10,7) = 1 by Euler's theorem
$7^{d(10)} \equiv 1 (\text{mod } 10)$
$7^4 \equiv 1 (\text{mod } 10)$
$7^{87}=(7^4)^{21}. 7^3$
$=343 (\text{mod } 10)$
$=3$
Thus, the units digit of 7^{87} is 3.

Q8- If x,y are distinct primes, find the remainder when xy divides $y^{x-1} + x^{y-1}$.

Sol.

(x,y)=1and both are primes. Thus, by fermat's little theorem,

x^{y-1}-1=my

y^{x-1}-1=nx, where m,n are positive integers

$[(x^{y-1}-1)(y^{x-1}-1)] \pmod{xy}=0$

$(x^{y-1}.y^{x-1}+1-y^{x-1}-x^{y-1}) \bmod (xy) = 0$

$y^{x-1} + x^{y-1} = 1 \pmod{xy}$

Thus the remainder obtained when when xy divides $y^{x-1} + x^{y-1}$ is 1.

Q9- Find the remainder when 5^{99} is divided by 13

Sol. (5,13) = 1, and 13 is prime. By Fermat's theorem

$5^{12} \pmod{13} = 1 \pmod{13}$

$5^{99}=(5^{12})^8.\ 5^3$

$5^3 \pmod{13}$

=8

Thus, the remainder is 8

Q10- Let m, n be the natural numbers, m<n and last three digits of 1978^n and 1978^m are equal. Find m and n such that m +n is least.

Sol. given the last three digits are equal we have $1978^n - 1978^m$ is divisible by 10^3 i.e. $(1978)^m (1978^{n-m}$ - 1) is divisible by 1000 $=2^3 \times 5^3$ but second factor 1978^{n-m} -1 is odd therefore,$1978^m = (2{\times}989)^m = 2^m$ 989^m=m3

We can express m+n =(n-m) + 2m and to minimise their sum, we take m=3 and seek the smallest value of n-m and 1978^{n-m} -1 is divisible by 5^3. Denote d=n-m and the least value 1978^d -1 is divisible by 5^3 i.e. $1978^d \equiv 1 \pmod{125}$

Now by ferments theorem $1978^n \equiv 1 \pmod 5$

$(1978)^{d(125)} \equiv 1 \pmod{125}$

$(1978)^{100} \equiv 1 \pmod{125}$

Given 1978^d -1 is divisible by 125 we must have d= n-m = 100

As m=3

n +m = 106 is the least value

Q11-Show that A=101010…101 is not a prime unless A=101.

Sol. $A=10^{2n}+10^{2n-2}\ldots.10^2+1$; clearly A is sum of terms from a GP. Hence,

$100A=10^{2n+2}+10^{2n}\ldots.10^4+10^2$

$99A=10^{2n+2}-1$

$99A=(10^{n+1}+1)(10^{n+1}-1)$

For n>1, $10^{n+1}+1>10^{n+1}-1>99$

If n is odd (but n>1), 10^{n+1}-1=9999, 999999, … (99 99…. 99)….

Such a number would be divisible by 99

Thus A can be expressed as a product of two numbers greater than one if n is odd.

If n is even, 10^{n+1}+1= 1001, 100001,…. (The first digit is 1 on an even place, and the last digit is 1 on an odd place; the rest are zeroes)

Such a number would always be divisible by 11

Thus A can be expressed as a product of two numbers greater than one if n is even.

Thus a number of form 10101010…101 cannot be prime unless 101.

6 CONCLUSION

Typically, formula for divisor function, Euler's theorem and Fermat's little theorem help in finding-the-remainder problems involving numbers with many digits. In fact, the subject theorems also help finding the number of digits. Since the units digit of a number is the remainder obtained on dividing that number by 10, the subject theorems can be used to find the units digit as well. Furthermore, by making the remainder 0, we can also use the subject theorems in making suitable adjustments in a long number to make it divisible by a given value (as seen in Q2). Finally, the theorems can give us insight on not only whether a bulky number is divisible by a value, but also if it is a prime (as seen in Q11). Thus, it can be inferred that these theorems have potential for application in cryptography.

7 REFERENCES

[1] Euclid (1956), *The thirteen books of the Elements*, 2 (Books III-IX), Translated by Thomas Little Heath (Second Edition Unabridged ed.), New York: Dover, ISBN 978-0-486-60089-5.

[2] Gauss, Carl Friedrich; Clarke, Arthur A. (translator into English) (1986), Disquisitiones Arithmeticae (Second, corrected edition), New York: Springer, ISBN 0-387-96254-9.

[3] D. Mahnke, Leibniz auf der Suche nach einer allgemeinen Primzahlgleichung, Bibliotheca mathematica. Zeitschrift für Geschichte der Mathematischen Wissenschaften, 13, 1912, 29-61.