Elementary in Number Theory

- Introduction to Number Theory

Number theory is about **integers** and their properties. We will start with the basic principles of :

- Divisibility,
- Greatest common divisors,
- Least common multiples, and
- Modular arithmetic

Division

If a and b are integers with a ≠ 0, we say that a **divides** b, if there is an integer c so that b = ac, or equivalently, if $\frac{b}{a}$ is an integer. When *a* divides *b* we say that *a* is a *factor* or *divisor* of *b*, and that *b* is a *multiple* of *a*.

The notation **a | b** means that a divides b. with no remainder

eg. all of 1,2,3,4,6,8,12,24 divide 24

Divisors

For integer a, b, and c it is true that

- If a | b and a | c, then a | (b+c)

  Example: 3 | 6 and 3 | 9, so 3 | 15
- If a | b and a | bc for all integers c

  Example: 5 | 10, so 5 | 20, 5 | 30, 5 | 40
- If a | b and b | c, then a | c

  Example: 4 | 8 and 8 |24, so 4 | 24

Primes

A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p.

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

The fundamental theorem of arithmetic:

Every positive integer can be written uniquely as the product of primes, where the prime factors are written in order of increasing size.

Examples:

15 = 3*5

48 =2*2*2*2*3 = 2^4*3

17 = 17

100 =2*2*5*5 = 2^2*5^2

512 =2*2*2*2*2*2*2*2*2 = 2^9

515 =5*103

28 =2*2*7

The Division Algorithm

Let **a** be an integer and **d** a positive integer. Then there are unique integers **q** and **r**, with **0** ≤ **r < d**, such that **a = dq + r**. In the above equation,

- **d** is called the divisor, المقسوم عليه
- **a** is called the dividend, المقسوم
- **q** is called the quotient, and
- **r** is called the remainder.

q = *a* **div** *d*, *r* = *a* **mod** *d*.

a **div** *d* = └ a/d ┘

a **mod** *d*= $d\left(\frac{a}{d} - q\right)$

The Division Algorithm

Example: When we divide 17 by 5,

we have 17 = 5*3 + 2.

- 17 is the dividend,
- 5 is the divisor,
- 3 is called the quotient, and
- 2 is called the remainder.

Another example:
What happens when we divide -11 by 3 ?

Note: that the remainder cannot be negative.

-11 = 3*(-4) + 1.

- -11 is the dividend,
- 3 is the divisor,
- -4 is called the quotient, and
- 1 is called the remainder.