11. Számelmélet, oszthatóság

**Oszthatóság:**

* Definíció: a,b∈Z. Az a és b számokról azt mondjuk, hogy a osztja b-t, illetve b az a többszöröse, ha b=a\*q valamely q egész számra. Jelölése: a|b
* Triviális osztó: n≠0 esetén +/-1. +/-n|n, ezeket hívjuk triviális osztóknak
* Valódi osztó: n nem triviális osztói. (azok az osztók amik nem 1 és nem maga a szám)
* Maradékos osztás: b szám felírható úgy, hogy 𝑏 = 𝑎 ∗ ⌊ ⌋ + 𝑚, 0 ≤ − ⌊ ⌋ < 1, é𝑠 0 ≤ 𝑚 < 𝑏 maradék adódik.

**LNKO:**

* Definíció: Legyen a,b∈Z olyan, hogy a≠0, vagy b≠0 teljesül. Az a és b számok legnagyobb közös osztója a legnagyobb olyan szám, ami osztója a-nak és b-nek is. Jelölése: (a,b)
* Relatív prímek: ha (a,b)=1

Euklidészi algoritmus:

* Algoritmus
  + Input: a és b egészek (mondjuk 𝑏 ≤ 𝑎)
  + Output: (a,b)
  + Működése: =a, =b, i=1; Ha már meghatároztuk az >=>=….>=, akkor legyen = \*+ , azaz osszuk el maradékosan -t -vel és legyen a maradék, amire tehát 0<=<=teljesül. Az eljárás akkor ér véget, ha =0. Ekkor az algoritmus válasza (a,b)=
* Bizonyítás:

**Prímek és felbonthatatlan számok:**

* Definíció: A p∈Z szám felbonthatatlan, ha |p|≠1 és a p-t csak triviális módon tudjuk egészek szorzataként előállítani. Azaz p=a\*b (a,b∈Z) esetén |a|=1 vagy |b|=1. (csak triviális osztói vannak és |p|≠1)
* Definíció: A p∈Z szám akkor prímszám, ha |p|>1 és csak úgy tud osztani egy szorzatot ha a szorzat valamelyik tényezőjét osztja: p|a\*b →p|a vagy p|b
* Egészek körében a prímek és a felbonthatatlanok ugyanazok.

**Számelmélet alaptétele:**

* Ha az n egész szám és n abszolútértéke nagyobb, mint 1, akkor n felbontható felbonthatatlanok szorzatára, és az a felbontás sorrendtől és előjeltől eltekintve egyértelmű.

**Kanonikus alak:**

* n∈N és n>1 szám kanonikus alakja egy olyan n= \*\*……\* előállítást értünk, amiben ,,… különböző pozitív felbontatlanok és az ,,… számok pedig pozitív egészek.

Osztó kanonikus alakja

* A d∈N szám pontosan akkor osztója az n∈N számnak, ha d kanonikus alakjában kizárólag n kanonikus alakjában megtalálható prímek szerepelnek és minden ilyen pi prím kitevője legfeljebb annyi d-ben, mint n-ben.
* bizonyítás:

LNKO kanonikus alakja:

* ha a= \*\*……\* és b= \*\*……\*,akkor (a,b)= \*\*……\*
* szavakkal: a két szám kanonikus alakját kell venni, és az alakban szereplő közös prímeket kell venni a legkisebb hatványon
* Bizonyítás: ha d közös osztó, akkor d kanonikus alakjában, csak az a és b kanonikus alakjában szereplő, közös prímek szerepelhetnek, legfeljebb a kisebbik kitevőn, ezért az lnko-ra adott képlet helyes.

Osztók száma:

* n∈Z és d(n) jelöli n pozitív osztóinak darabszámát. n=, ahol az n szám felbonthatatlanokból állók szorzat tényezői az pedig azt jelöli, hogy ezek a szorzat tényezők hányszor fordulnak elő a felbontásban (hányadikon vannak). (Úgy számolhatjuk ki, hogy a kanonikus alakjából a kitevőket plusz egy összeszorozzuk) d(n)=π(
* példa: 12= \*3 -> d(12)= (2+1)\*(1+1)=3\*2=6
* Bizonyítás:

Nevezetes tételek prímszámokról:

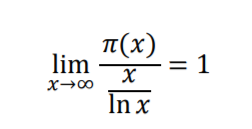
**Prímek száma:**

* Tétel: Prímszámok száma végtelen.
* Bizonyítás: mivel n! az 1,2,…n számok mindegyikével osztható, igy N:=n!+1 az 1,2…n számok mindegyikéhez relatív prím, tehát N nem osztható semelyik n-nél kisebb prímmel sem. N kanonikus alakjában, csak n-nél nagyobb prímek fordulhatnak elő.

**Prímek közti hézag:**

* Tétel: Tetszőlegesen hosszú sorozat képezhető szomszédos összetett számokból, azaz bármely n∈N-re létezik olyan N, amire az N+1, N+2,….N+n számok mindegyike összetett.
* Bizonyítás:

**Prímszámtétel:**

ahol 𝜋(𝑥) az x-nél nem nagyobb prímek számát jelöli.

Csebisev tétel: Tetszőleges n pozitív egészre létezik p prím, n <p <= 2n

Dirichlet tétel: Ha a és d relatív prím, az a, a+d, a+2d,…. számtani sorozatban végtelen sok prím fordul elő.