13. Kongruencia

Ha egy számot elosztunk m-mel, m darab maradékosztály képezhető, 0->m-1 ig (m maradék olyan, mintha 0 lenne a maradék)

**Kongruencia fogalma:**

* a,b,m Z, m>0 esetén azt mondjuk, hogy a kongruens b modulo m, ha m|a-b
* Jelölése: ab(mod m) -> ab(m)
* Úgy is mondhatjuk, hogy a és b ugyanabba a maradékosztályba tartozik.

**Műveletek kongruenciákkal**

* adott ab(m) és cd(m)
* összeadás: a+cb+d(m)
  + bizonyítás: Tudjuk, hogy m|a-b és m|c-d. Ezért m|a-b+c-d=a+c-(b+d), azaz a+cb+d(m)
* kivonás: a-cb-d(m)
* szorzás: a\*cb\*d(m)
  + bizonyítás: m|c(a-b) + b(c-d)=ac-bd, azaz acbd (m)
* osztás: ha d|a és d|b és ab(m), akkor (), azaz kongruencia osztáskor nemcsak a konruencia két oldalát osztjuk el, hanem a modulust is az osztó és a modulus LNKO-val
  + bizonyítás:
* Következmény:
  1. ab(m) kongruencia, akkor teljesül, ha a+kb+k (m), tehát a k számnak m szorosnak kell hogy legyen (m|k)
     + bizonyítás: kk(m) hozzáadása (mint az összeadás bizonyítása)
  2. ha d relatív prím az m-hez, akkor ab(m) kongruencia ekvivalens adbd(m) kongruenciával, tehát kongruencia szorzása csak akkor ekvivalens átalakítás, ha a modulushoz relatív prímszámmal szorzunk
     + bizonyítás: ab(m) kongruenciát dd(m) kongruenciával beszorozva adbd(m) adódik. Az osztásra vonatkozó állítás miatt pedig ab(m) kongruenciából ab () következik, ahol (m,d)=1 miatt ab(m) alakot ölt.
  3. A d>0 rögzített egész szám, akkor az ab(m) kongruencia ekvivalens az adbd(md) kongruenciával.
     + a≡b(m) re igaz, hogy m|a-b akkor md|(a-b)d = md|ad-bd -> adbd(md)

**Teljes maradékrendszer:**

* Rögzített m>1 egész szám esetén az m elemű T= = {𝑎1,𝑎2, … , 𝑎𝑚} halmazt modulo m teljes maradékrendszernek (TMR-nek) nevezzük, ha T minden m szerinti maradékosztályból pontosan egy elemet tartalmaz.
* TMR modulo m a{0,1,2…..,m-1} vagy az {1,2,3,….m} halmaz. Modulo 10 TMR a{100,11,22,33,44,55,66,77,88,99} halmaz

**Redukált maradékrendszer:**

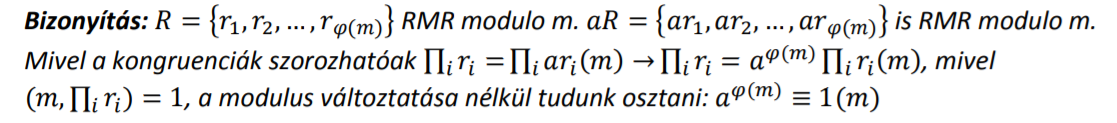
* 𝑅 ⊂ ℤ halmaz redukált maradékrendszer (RMR) modulo m, ha R minden m-hez relatív prím m szerinti maradékosztályból pontosan egy elemet tartalmaz.
* A modulo PMP méretét, azaz azoknak az m szerinti maradékosztályoknak a számát, amelyek m-hez relatív prím számot tartalmaznak ϕ(m)-mel jelöljük.
* Úgy is megkaphatjuk az RMR-t, ha a TMR-ből elhagyjuk a modulushoz nem relatív prím elemeket. Ezek szerint RMR-t alkotnak az 1 és m közötti, m-hez relatív prím egészek.

**Euler féle ϕ függvény:**

* Egy adott egész számhoz megadja, a nála kisebb relatív prímszámok darab számát. (RMR mérete)
* ϕ(n) kiszámítása:
  + p prímre ϕ(=-/p-1
  + ha egy szám nem prím, de fel tudjuk bontani relatív prímszámok szorzatára (kanonikus alakra), akkor: 𝜑(𝑎 ∗ 𝑏) = 𝜑(𝑎) ∗ 𝜑(𝑏)

**Euler-Fermat tétel**

* Ha (a,m)=1, akkor ≡ 1(𝑚)



**Kis Fermat tétel**

* Ha p prím, akkor bármely a egészre igaz, hogy a(p).
* bizonyítása: Világos, hogy ϕ(=p-1 (hisz 1től p-1 ig minden egész szám relatív prím p-hez), ezért ha (a,p)=1, akkor 1(p), ahonnan a(p), Ha (a,p) 1, akkor p prímtulajdonsága miatt p|a, azaz 0(p), és a(p)

**Lineáris kongruenciák**

* Lineáris kongruencián egy axb(m) kongruenciát értünk, ahol a és b adott egészek, m>0. A lineáris kongruencia megoldása azt jelneti, hogy meghatározzuk mindazon egészeket, amelyeket x helyére írva a kongruencia igaz lesz.

**Lineáris kongruenciák megoldása**

* Tétel: Az axb(m) kongruencia esetén pontosan akkor oldható meg, ha (a,m)|b. A kongruencia megoldáshalmaza (a,m) darab maradékosztály modulo m.
* bizonyítás:

**Konkrét módszer a megoldásra**

1. Az a együttható abszolút értékét csökkentjük egészen 1-ig ekvivalens átalakításokkal

* a vagy b helyettesítése vele kongruens számmal
* osztás (modulót is)
* m-hez relatív prímmel szorzás (modulushoz nem nyúlunk)

1. Euklidészi algoritmus használata
2. ha a modulus kellően kicsi, akkor TMR minden elemét behelyettesítve, pontosan azok a maradékosztályok alkotják a megoldáshalmazt, amelyeknek reprezentásait behelyettesítve teljesül a kongruencia
3. ha ismert m kanonikus alakja, akkor 𝜑(𝑚)-et kiszámítva, az Euler-Fermat tételt kihasználva tudjuk megoldani a kongruenciát, a leosztás után, amikor is már (a,m)=1 teljesül. Így beszorozhatjuk mindkét oldalt 𝑎 𝜑(𝑚)−1 , m-hez relatív prím számmal. 𝑎 𝜑(𝑚)−1𝑎𝑥 ≡ 𝑎 𝜑(𝑚)−1𝑏(𝑚), azaz megkapjuk a lineáris kongruencia egyértelmű megoldását.