K O N G R U E N C I J E

1. Pojam i osnovna svojstva kongruencija

Ako su a,b(Z i m(Z i ako m|a-b, onda kažemo da su a i b kongruentni po modulu m i to pišemo ovako: a(b (mod m). Poslednji zapis zovemo još i kongruencijom. Svaka kongruencija po modulu m definisana je za jednu relaciju na Z ovako: a~mb <=> a(b (mod m).

~m je relacija ekvivalencije

Dokaz:

Refleksivnost: a(Z a~ma <=> a(a (mod m) <=> m|a-a <=> m|0 a ovo je tačno.

Simetričnost: a,b(Z

a~mb => a(b (mod m) => m|a-b => a-b=km|(-1) =>b-a=m*(-k) =>m|b-a =>

b(a (mod m) => b~ma

Tranzitivnost: a,b,c(Z

a~mb /\ b~mc => a(b (mod m) /\ b(c (mod m) =>m|a-b /\ m|b-c =>

a-b=mk /\ b-c=ml; k,l(Z => a-b+b-c=mk=ml => a-c=m(k+l) =>

m|a-c => a(c (mod m) =>a~mc.

Svaku klasu Z/~m zovemo klasom ostatka mod m. Skup svih klasa zovemo potpunim sistemom ostatka mod m. Kako svaka relacija ekvivalencije vrši particiju skupa na disjunktne klase, to su klase ostataka disjunktne i njihova unija je čitav Z. Potpun sistem ostataka zadajemo pomoću predstavnika klasa. Obično se biraju: 0,1,2,...,m-1; 1,2,...,m;...Izbor može biti po želji. Nekad je zgodno birati negativne predstavnike.

Izvedimo sada neka svojstva kongruencija:

Teorema 1: Ako je a(b (mod m) i c(d (mod m), onda je:

a+c(b+d (mod m)

a*c(b*d (mod m)

ka(kb (mod m),(k(Z

Dokaz:

1) a(b (mod m) /\ c(d (mod m) => m|a-b /\ m|c-d => m|(a-b+c-d) =>

m|(a+c-(b+d)) => a+c(b+d (mod m).

2) a(b (mod m) /\ c(d (mod m)

=> m|a-b /\ m|c-d

=> m|(a-b)(c-d)

=> m|ac-ad-bc+bd

=> m|ac-bd-ad-bc+bd+bd

=> m|ac-bd-d(a-b)-b(c-d)

=> m|ac-bd

=>ac(bd (mod m)

3) a(b (mod m)

=> m|a-b

=>m|k(a-b)

=> m|ka-kb

=>ka(kb (mod m)

Napomena:Videli smo da kongruencija ostaje istinita ako levu i desnu stranu pomnožimo istim brojem. Postavlja se pitanje da li se ona može deliti celim brojem različitim od nule.Da to ne može pokazuje ovaj primer: 35(20 (mod m) ne povlači 7(4 (mod m).