VIII. KOLOBARJI IN OBSEGI

1) Osnove

Def.: Kolobar je algebrska struktura $(A,+,\circ,0)$ za katero velja
$+$ = seštevanje
$\circ$ = množenje
0 = ničla

- $(A,+,0)$ je abelova grupa (komutativna)
- $(A,\circ)$ je polgrupa
- distributivnostna zakona:
  - $(a+b)\circ c = a\circ c+b\circ c$
  - $a\circ(b+c) = a\circ b+a\circ c$

Opombe:
Pravimo, da je kolobar komutativen, če je množenje!!! komutativno.
V tem primeru sta oba distributivnostna zakona enakovredna.

Če ima $(A,\circ)$ nevtralni element, ga označimo z 1 in mu pravimo enica.

Zgled: ({soda cela števila},+,$\circ$,0)
$(Z,+,\circ,0)$
$(Q,+,\circ,0)$
$(R,+,\circ,0)$
$(C,+,\circ,0)$
vsi imajo 1

({polinomi z realnimi koeficienti},+,$\circ$,0)

Izrek: 0 je absorbcijski element za $\circ$. Za vse $a\in A$ velja $0\circ a=a\circ 0=0$

Dokaz:
$0+\underline{0\circ a} = 0\circ a = (0+0)\circ a = 0\circ a+\underline{0\circ a}$
$0 = 0\circ a$

Posledica:
Če ima kolobar vsaj dva elementa potem je $1\neq 0$.

Dokaz:
Naj bo $a\in A$
$a\neq 0$
$0\circ a = 0$
$1\circ a = a$
Če bi slučajno veljalo da je 1 = 0, potem bi bilo tudi a = 0, to pa ni res.

2) Kolobar celih števil
(Z,+,◦,0) in enica 1

Izrek: m,n∈Z, m≠0, obstajata enolično določena k,r∈Z, 0≤r<m, za katera velja:
n = k◦m + r
k – kvocient
r – ostanek

Def.: m,n∈Z. Pravimo, da m deli n, m|n, če obstaja k∈Z, za katero je n = k◦m.
Če m,n nista oba 0
greatest common divisor = gcd(m,n) = max{d∈Z; d|m in d|n}
lowest common multiple = lcm(m,n) = min{v∈Z; m|v in n|v}, v pozitiven, če se da

dodatno definiramo: gcd(0,0) = lcm(0,0) = 0

Razširjeni Evklidov algoritem:
Kako izračunamo gcd?

Zgled: gcd(899,812)

1◦899 + 0◦812 =	899	
0◦899 + 1◦812 =	812	
1◦899 + (-1)◦812 =	87	
(-9)◦899 + 10◦812 =	**29**	(0-9◦1 = -9, 1-9◦(-1)=10)
28◦**899** + (-31)◦81 =	0	

899 = 1◦812 + 87
812 = 9◦87 + 29
87 = 3◦29 + 0

Trdimo: 29 deli vse desne strani
Trdimo: 29 je skupni delitelj 812 in 899.
Trdimo: Če število d deli 899 in 812, potem d deli tudi vsako celoštevilsko linearno kombinacijo števil 899 in 812.
a◦899 + b◦812 (a,b∈Z)
Trdimo: 29 je celoštevilska linearna kombinacija 899 in 812.

Torej: gcd(899,812) = 29.

Izrek: Naj bosta m,n∈Z in d=gcd(m,n).
Potem obstajata s,t∈Z, tako da s◦m+t◦n=d.

Def.: Celi števili a in b sta si tuji, a⊥b, če je gcd(a,b)=1.

Izrek: Denimo, da a|b◦c
Če sta a⊥b, potem a|c.

Dokaz:
1) k◦a = b◦c, za nek k∈Z
2) s◦a+t◦b = 1, za neka s,t∈Z

$s \circ a \circ c + t \circ b \circ c = c$
$s \circ a \circ c + t \circ k \circ a = c$
$a \circ (s \circ c + t \circ k) = c$
$a | c$

Izrek: $\gcd(a,b) \circ \mathrm{lcm}(a,b) = a \circ b$

Linearne diofantske enačbe (z dvema neznankama)
Naloga:

Skupina otrok je v slaščičarni jedla torte in kremne rezine. Koliko tort in kremnih rezin so pojedli, če stane torta 540 SIT, kremna rezina 420 SIT, račun pa je znašal 7860 SIT.
(manj tort kot kremnih rezin)

Rešujemo:

$540x + 420y = 7860$ (*)

Def.: Linearna diofantska enačba z dvema neznankama je $ax+by=c$, kjer so $a,b,c \in Z$ in iščemo celoštevilsko rešitev x,y.

Če (*) delimo s 60 dobimo
$9x + 7y = 131$

Uporabimo razširjen Evklidov algoritem (REA):

$1 \circ 9 + 0 \circ 7 = 9$
$0 \circ 9 + 1 \circ 7 = 7$
$1 \circ 9 + (-1) \circ 7 = 2$
$\mathbf{(-3) \circ 9 + 4 \circ 7 = 1 \quad / \circ 131}$
$\mathbf{7 \circ 9 + (-9) \circ 7 = 0 \quad / \circ t}$

$9 \circ (-393) + 7 \circ 524 = 131$
$9 \circ (-393 + 7 \circ t) + 7(524 - 9 \circ t) = 131$

$x_t = -393 + 7t$
$y_t = 524 - 9t$

Določi t, $x_t \geq 0$, $y_t \geq 0$
$t \leq 524/9 = 58.2$
$t \geq 393/7 = 56.1$

$t = 57$
$t = 58$

$x_{57} = 6$
$y_{57} = 11$ √

$x_{58} = 13$
$y_{58} = 2$ //

Izrek: Diofantska enačba $ax+by=c$ je rešljiva natanko tedaj, ko $d=\gcd(a,b)$ deli c.

Če je x^*, y^* rešitev enačbe. potem vse druge rešitve dobimoo z obrazcem
$x_t = x^* + t\circ(b/d)$
$y_t = y^* - t\circ(a/d)$
Dokaz REA.