1 Prsten celih brojeva

$$\mathbb{Z} := -\mathbb{N}^+ \cup \{0\} \cup \mathbb{N}^+ = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Osnovni primer. $(\mathbb{Z}, +, \cdot, -, 0, 1)$ je komutativan *prsten* sa jedinicom:

sabiranje	množenje
(S1) asocijativnost $x + (y + z) = (x + y) + z$	(M1) asocijativnost $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
(S2) komutativnost $x + y = y + x$	(M2) komutativnost $x \cdot y = y \cdot x$
(S3) 0 je neutral, *nula* $x + 0 = x = 0 + x$	(M3) 1 je neutral, *jedinica* $x \cdot 1 = x = 1 \cdot x$
(S4) svaki element x ima *suprotni* $-x$ $x + (-x) = 0 = -x + x$	( ) samo 1 i -1 imaju *inverz* $1 \cdot 1 = 1,\ -1 \cdot (-1) = 1$
množenje je distributivno prema sabiranju	
(D1) $x \cdot (y + z) = x \cdot y + x \cdot z$	(D2) $(x + y) \cdot z = x \cdot z + y \cdot z$

2 Grupe, prsteni, polja

Definicija. *$(G, *, ^-, e)$, gde je G neprazan skup, $*$ binarna operacija skupa G, $^-$ je unarna operacija skupa G, a $e \in G$ je fiksiran element, je **grupa** akko:*
(Asoc) $*$ je asocijativna operacija (množenje),
(Neutral) e je neutral(ni element) u odnosu na množenje (operaciju $*$),
(Inverz) $\overline{x}$ je inverz elementa x ($x * \overline{x} = e = \overline{x} * x$).

Definicija. *Grupa $(G, *, ^-, e)$ je **komutativna** akko*
(Kom) $*$ je komutativna operacija.

Definicija. *$(P, +, \cdot, -, 0, 1)$ je **komutativni prsten sa jedinicom** akko:*
(Sab) $(P, +, -, 0)$ je komutativna grupa,
(Mno) Množenje $\cdot$ je komutativno i asocijativno, a 1 je neutral (jedinica),
(Dist) Množenje $\cdot$ je distributivno prema sabiranju $+$.

Definicija. *Komutativni prsten sa jedinicom $(P, +, \cdot, -, 0, 1)$ je **polje** akko svaki ne-nula element ima inverz, u odnosu na množenje.*

Primeri. Polja: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
Prsteni (komutativni sa jedinicom), koji nisu polja: $\mathbb{Z}$, $\quad \mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x]$.

Svi navedeni prsteni su euklidski, to jest prsteni sa euklidskim deljenjem.

3 Euklidsko deljenje u $\mathbb{Z}$

Lema o euklidskom deljenju u $\mathbb{Z}$. Za svaki $m \in \mathbb{Z}$, i svaki $n \in \mathbb{N}^+$ postoje jedinstveni $q \in \mathbb{Z}$ i $r \in \{0, 1, \ldots, n-1\}$ takvi da je $m = n \cdot q + r$. Formulski:
$(\forall m \in \mathbb{Z})(\forall n \in \mathbb{N}^+)(\exists! q \in \mathbb{Z})(\exists! r \in \mathbb{Z})\ (\ m = n \cdot q + r\ ,\ 0 \leq r < n\ )$. Ovo je ekv:
$(\forall n \in \mathbb{N}^+)(\forall m \in \mathbb{Z})(\exists! r \in \mathbb{Z})\ (\ n \mid m - r\ ,\ 0 \leq r < n\ )$.

Definicija. *a) Za $n \in \mathbb{N}^+$, uvodimo $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$.*
b) ***Ostatak pri euklidskom deljenju brojem*** *$n \in \mathbb{N}^+$ je funkcija $\varrho_n : \mathbb{Z} \to \mathbb{Z}_n$ definisana implicitno: $(\forall m \in \mathbb{Z})\ (\ \varrho_n(m) = r \Leftrightarrow (\ r \in \mathbb{Z}_n\ \wedge\ n \mid m - r\ )\ )$.*

4 Prsten ostataka

Definicija. *Neka je $n \in \mathbb{N}^+$, $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$.*
Definišemo dve binarne $+_n$, $\cdot_n$ i jednu unarnu operaciju $-_n$ na $\mathbb{Z}_n$:

$$\boxed{x +_n y := \varrho_n(x + y)}\ , \quad \boxed{x \cdot_n y := \varrho_n(x \cdot y)}\ , \quad -_n x := \begin{cases} 0, & \text{ako je } x = 0; \\ n - x, & \text{ako } 0 < x < n. \end{cases}$$

Teorema 1. $(\mathbb{Z}_n, +_n, \cdot_n, -_n, 0, 1)$ je komutativan prsten sa jedinicom.

Teorema 2. $(\mathbb{Z}_n, +_n, \cdot_n, -_n, 0, 1)$ je polje akko n je prost.

Teorema (L). Ako je $(G, \cdot, ^{-1}, 1)$ grupa, $n := |G|$, i $\ x \in G$, onda $x^n = e$.

Mala Fermaova teorema. Ako je p prost broj, onda je $(\mathbb{Z}_p \setminus \{0\}, \cdot_p, 1)$ grupa u kojoj važi $\boxed{x^{p-1} = 1}$.

5 Tablice sabiranja i množenja u prstenu ostataka

Tablice komutativnih operacija su simetrične. Iz tablice se lako čita neutral (nula i jedinica), pa čak i inverzibilnost elementa. Asocijativnost i distributivnost se ne mogu neposredno videti. Treća tablica predstavlja Ojlerovu grupu.

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

$\cdot_2$	0	1
0		
1		1

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\cdot_3$	0	1	2
0			
1		1	2
2		2	1

$x^{3-1} = 1$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\cdot_4$	0	1	2	3
0				
1		1		3
2				
3		3		1

$x^2 = 1$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\cdot_5$	0	1	2	3	4
0					
1		1	2	3	4
2		2	4	1	3
3		3	1	4	2
4		4	3	2	1

$x^{5-1} = 1$

Napomena. U svakom polju važi $xy = 0 \Rightarrow x = 0 \vee y = 0$. Otuda sledi: ako je $n = m \cdot k$ složen, onda $\mathbb{Z}_n$ nije polje (jer $m \cdot_n k = 0,\ m \neq 0,\ k \neq 0$). Zato, ako je $\mathbb{Z}_n$ polje, onda n mora biti prost.

6 Ojlerova grupa

Definicija. *Neka je* $n \in \mathbb{N}^+$, $\Phi_n := \{x \in \mathbb{Z}_n \mid (x, n) = 1\}$.

Teorema 3. Ako je $n \in \mathbb{N}^+$, onda je $(\Phi_n, \cdot_n, 1)$ grupa.
Zapravo $\Phi_n = \{x \in \mathbb{Z}_n \mid (\exists y \in \mathbb{Z}_n)\ x \cdot_n y = 1\}$.

Definicija. *Za grupu* $(\Phi_n, \cdot_n, 1)$ *kažemo da je* ***Ojlerova grupa****.*

Tablice još nekih Ojlerovih (Euler) grupa

$\cdot_6$	1	5
1	1	5
5	5	1

$x^{(2-1)(3-1)} = 1$

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$x^{2^{3-2}} = x^2 = 1$

Teorema 4. (Ova teorema je jedno uopštenje Male Fermaove teoreme; ali je malo slabija od Ojlerove teoreme, iako je deo pod a) zapravo precizniji od nje.)

a) Neka je $k > 2$. Tada u grupi Φ_{2^k} za svako x važi $x^{2^{k-2}} = x^{2^{k-1}-2^{k-2}} = 1$.

Ovo je ekvivalentno sa $\boxed{(x, 2) = 1 \ \Rightarrow\ 2^k \mid x^{2^{k-2}} - 1 = x^{2^{k-1}-2^{k-2}} - 1}$.

b) Neka je $p > 2$ prost broj. Ako $k > 0$, onda u grupi Φ_{p^k} važi $x^{p^k - p^{k-1}} = 1$.

Ovo je ekvivalentno sa $\boxed{(x, p) = 1 \ \Rightarrow\ p^k \mid x^{p^k - p^{k-1}} - 1}$.

Primeri.

$\cdot_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

x^6	$= 1$
1^1	$= 1$
2^3	$= 1$
3^6	$= 1$
4^3	$= 1$
5^6	$= 1$
6^2	$= 1$

$\cdot_9$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

x^6	$= 1$
1^1	$= 1$
2^6	$= 1$
4^3	$= 1$
5^6	$= 1$
7^3	$= 1$
8^2	$= 1$

7 Jednakost ostataka

Sada, za $n \in \mathbb{N}^+$, definišemo jednu binarnu relaciju na skupu $\mathbb{Z}$, tako da su dva cela broja x, y u relaciji akko imaju jednake ostatke pri euklidskom deljenju sa n.

Definicija. *Neka je $n \in \mathbb{N}^+$. Definišemo binarnu relaciju, $=_n$, na skupu $\mathbb{Z}$:*

$$(\forall x, y \in \mathbb{Z})\ (\ x =_n y \ \Leftrightarrow\ n \mid x - y \ \Leftrightarrow\ \varrho_n(x) = \varrho_n(y)\ ).$$

Osobine. a) $=_n$ je relacija ekvivalencije, $x =_n \varrho_n(x)$;

b) $x =_n y,\ \ x_1 =_n y_1 \ \Rightarrow\ x + x_1 =_n y + y_1,\ \ x \cdot x_1 =_n y \cdot y_1$;

c) $x =_n y \ \Rightarrow\ -x =_n -y,\ \ x^k =_n y^k$, za $k \geq 0$.

Teorema 4'. Teoremu 4. možemo formulisati i na sledeći način:

a) Neka je $k > 2$. Tada $\boxed{(x, 2) = 1 \ \Rightarrow\ x^{2^{k-2}} =_{2^k} 1 =_{2^k} x^{2^{k-1}-2^{k-2}}}$.

b) Neka je $p > 2$ prost broj, $k > 0$. Tada $\boxed{(x, p) = 1 \ \Rightarrow\ x^{p^k - p^{k-1}} =_{p^k} 1}$.

8 Zadaci

1. Izračunati $\varrho_{77}(2222^{5555} + 5555^{2222})$.

(1) $2222^{5555} + 5555^{2222} =_{11} 0^{5555} + 0^{2222} =_{11} 0$;

(2) $2222 =_7 122 =_7 52 =_7 \boxed{3}$, $\quad 5555 =_7 655 =_7 25 =_7 \boxed{4}$;

(3) $3^2 =_7 2,\ 3^3 =_7 6,\ 3^4 =_7 4,\ 3^5 =_7 5,\ \boxed{3^6 =_7 1}$, $\quad 4^2 =_7 2,\ \boxed{4^3 =_7 1}$;

(4) $5555 =_6 155 =_6 35 =_6 \boxed{5}$, $\quad 2222 =_3 122 =_3 \boxed{2}$, računamo zbog (3);

(5) $2222^{5555} + 5555^{2222} =_7 1 \cdot \boxed{3^5} + 1 \cdot \boxed{4^2} =_7 5 + 2 =_7 0$, iz (2), (3), (4);

(6) $\varrho_{77}(2222^{5555} + 5555^{2222}) = \boxed{0}$, $\quad$ iz (1), (5), jer $(7, 11) = 1$.

2. Izračunati $\varrho_{1001}(2012^{2012})$. Napomena: $1001 = 7 \cdot 11 \cdot 13$.

(1) $2012 =_{1001} 10$, zato ne čudi: $2012 =_7 612 =_7 52 =_7 \boxed{3}$,

$2012 =_{11} 912 =_{11} 32 =_{11} \boxed{-1}$, $2012 =_{13} 712 =_{13} 62 =_{13} \boxed{-3}$;

(2) $3^2 =_7 2$, $3^3 =_7 6$, $3^4 =_7 4$, $3^5 =_7 5$, $\boxed{3^6 =_7 1}$, $\boxed{(-1)^2 =_{11} 1}$,

$(-3)^2 =_{13} 9$, $(-3)^3 =_{13} -1$, $(-3)^4 =_{13} 3$, $(-3)^5 =_{13} 4$, $\boxed{(-3)^6 =_{13} 1}$;

(3) $2012 =_6 212 =_6 \boxed{2}$, $2012 =_2 \boxed{0}$, $2012 =_6 212 =_6 \boxed{2}$,

računamo zbog (2);

(4) $2012^{2012} =_7 3^2 =_7 \boxed{2}$, $2012^{2012} =_{11} (-1)^0 =_{11} \boxed{1}$,

$2012^{2012} =_{13} (-3)^2 =_{13} \boxed{9}$, dobijamo iz (1), (2), (3).

(5) Ako je $a = \varrho_{11\cdot13}(2012^{2012})$, onda $a =_{11\cdot13} 2012^{2012}$. Otuda i iz (4) sledi $a =_{11} 2012^{2012} =_{11} 1$ i $a =_{13} 2012^{2012} =_{13} 9$. Iz drugog uslova imamo $a \in \{9, 22, 35, 48, 61, 74, 87, 100, 113, 126, 139\}$, ali jedino $\boxed{a = 100}$ zadovoljava i prvi uslov.

(6) Ako je $b = \varrho_{1001}(2012^{2012})$, onda $b =_{1001} 2012^{2012}$. Otuda i iz (4), (5) sledi $b =_7 2012^{2012} =_7 2$ i $b =_{11\cdot13} 2012^{2012} =_{11\cdot13} 100$. Iz drugog uslova imamo $b \in \{100, 243, 386, 529, 672, 815, 958\}$, ali jedino $\boxed{b = 100}$ zadovoljava i prvi uslov.

(7) $\varrho_{1001}(2012^{2012}) = \boxed{100}$, iz (6).