# Ligjerata per Javet 6-11

David Kalaj, Davidkalaj@gmail.com

April 18, 2020

## 1 Plotpjesëtueshmeria

Themi se numri natyror $a$ plotpjesëtohet me numrin natyror $b$ nëse ekziston numri natyror $c$ i tillë që $a = b \cdot c$. Këte fakt e shënojmë simbolikisht $a \vdots b$ ose $b|a$.

**Vetitë**.

1. Nëse $a \vdots b$ dhe $a \neq 0$ atëherë $a \geqslant b$.
2. Nëse $a \vdots b$ dhe $b \vdots a$ atëherë $a = b$.
3. Nëse $a \vdots 3$ dhe $b \vdots 3$ atëhere $a \vdots c$.
4. Nëse $a \vdots c$ dhe $b \vdots c$ atëherë $(a + b) \vdots c$ dhe $(a - b) \vdots c$ për $a \geqslant b$.
5. Nëse $a \vdots b$ dhe $c \in \mathbf{N}$, atëhere $ac \vdots b$.
6. Nëse $a_1, \dots a_n \vdots b$ dhe $c_1, \dots c_n \in \mathbf{N}$, atëhere $(a_1b_1 + \dots a_nb_n) \vdots b$,

Le të vertetojmë p.sh. vetiné e 3). Meqenëse $a \vdots b$, rrjedh se $a = a_1b$. Meqenëse $b \vdots c$, rrjedh se $b = b_1c$. Nga këtu rrjedh se $a = a_1b_1c$, ku $a_1b_1$ është numër natyror si prodhim i dy numrave natyrorë. Në mënyrë të ngjashme vërtetohen edhe vetitë e tjera.

## 2 Pjesëtuesi më i madh i përbashkët i dy numrave $PMP$.

**Përkufizim**. Themi se numci $c$ është pjesëtuesi më i madh i përbashkët i numrave natytorë $a$ dhe $b$ në qoftë se numri $c$ i plotëson këto dy veti.

1. $a \vdots c$ dhe $b \vdots c$.
2. Nëse $a \vdots d$ dhe $b \vdots d$, atëherë $c \vdots d$.

Pjesëtuesim më të madh të peprbashkët te numrave $a$ dhe $b$ e shënojmë me $c = PMP(a, b)$ ose shkurtimisht nëprmjet simbolit $(a, b)$.

**Shembulli 2.1** *Le të jetë* $a = 120$ *dhe* $b = 300$*. Të percaktojmë* $PMP(a, b)$*. Pjesëtuesit e numrit a janë* $A = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 18, 20, 24, 30, 40, 60, 120\}$*, kurse pjesëtuesit e numrit b janë* $B = \{1, 2, 3, 4, 5, 6, 10, \ldots, 60, 100, 150, 300\}$*. Numri më i madh i përbashët i bashkësive A dhe B është numri* 60*, prandaj* $PMP(a, b) = 60$*.*

Metoda e zbatuar paraprakisht nuk është praktike prandaj zbatojmë dy metoda të tjera që bazohen në:

1. Teoremën themelore të aritmetikës
2. Algoritmin e Euklidit.

Qe te formulojmë teoremën themelore të aritmetikës le të perkufizojmë numrat e thjeshtë.

**Perkufizimi 2.2** *Themi se numri natyror* $n \neq 1$ *është i thjeshtë, në qoftë se plotpjesëtohet vetëm me numrat* 1 *dhe* $n$*.*

Numrat e thjeshtë i shënojmë me $P$. Pra

$$P = \{p_1, p_2, \ldots, p_k, \ldots\} = \{2, 3, 5, 7, 11, 13, \ldots\}.$$

Kjo bashkësi numrash është bashkësi e pafundme. Vërtetimi mund të bëhet nëpërmjet

**Theorem 2.3 (Teorema themelore e aritmetikes)** *Çdo numër natyror* $n$ *mund të shënohet në trajtën e produktit të numrave të thjeshtë. Me fjalë të tjera, ekzistojnë numrat e thjeshtë* $p_1 < p_2 < \ldots, p_k$ *dhe numrat natyrorë ose zero* $q_1, \ldots q_k$ *ashtu që*

$$n = p_1^{q_1} \cdot \ldots p_k^{q_k}.$$

*Representimi paraprak eshte i vetem.*

**Theorem 2.4** *Nese*

$$n = p_1^{q_1} \cdot \ldots p_k^{q_k},$$

*dhe*

$$m = p_1^{r_1} \cdot \ldots p_k^{r_k},$$

*atëherë*

$$PMP(m, n) = p_1^{\min\{q_1, r_1\}} \cdot \ldots p_k^{\min\{q_k, r_k\}}.$$

Le te percaktojme $PMP(120, 300)$ duke zhatuar teoremen paraprake. Kemi

$$120 = 2 \cdot 60 = 2^2 \cdot 30 = 2^3 \cdot 15 = 2^3 \cdot 3^1 \cdot 5^1$$

dhe

$$300 = 2^2 \cdot 3^1 \cdot 5^2.$$

Prandaj

$$PMP(120, 300) = 2^{\min\{2,3\}} \cdot 3^{\min\{1,1\}} \cdot 5^{\min\{1,2\}} = 2^2 \cdot 3^1 \cdot 5^1 = 60.$$

**Theorem 2.5** *Bashkësi e numrave të thjeshtë është e pafundme.*

**Vertetimi.** Le te jete $n$ nje numer i çfarëdoshëm dhe marrim numrat $p_1 < p_2 \cdots < p_n$ e thjeshte te renditur prej me te voglit deri te me i madhi duke i kyçur te gjithe numrat e thjeshtë . Numri $x = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$, eshte më i madh se secili nga numrat $p_1, \ldots, p_n$. Madje numri $x$ nuk plotpjesëtohet me asnjenin nga keta numra $p_1, \ldots, p_n$ sepse mbetja e pjesetimit te numrit $x$ me $p_k$ eshte gjithmone 1. Pra numri $x$ eshte i thjeshte ose ne baze te teoremes themelore te aritmetikes pjesetohet me numra te thjeshte te ndryshem nga numrat $p_1, \ldots, p_n$. Nga ketu rrjedh se ekzsiton edhe numri i thjeshte $p_{n+1}$. Si rrjedhim perfundojme se bashkesia $P$ eshte pambarimisht e madhe.

## 2.1 Algoritmi i Euklidit

Ky algoritem bazohet ne teoremen e meposhtme

**Theorem 2.6** *Per çdo dy numra natyrore $a$ dhe $b$ per te cilet vlen $a > b$ ekzistojne numrat natyror te vetem $a_1$ dhe $q_1$ ashtu qe*

$$a = bq_1 + a_1, \quad 0 \leqslant a_1 < b. \tag{2.1}$$

**Vërtetimi**.

Le te perkufizojme bashkesine $A$ siç vijon:

$$A = \{q \in \mathbf{N} : a - bq \geqslant 0\}.$$

Kjo bashkesi eshte bashkesi jo-boshe, sepse $q = 1 \in A$. Ne anen tjeter nese $q > a$, atehere $a - bq < a - ab = a(1 - b) \leqslant 0$, prandaj $q \notin A$. Rrjedhimisht, $A$ eshte nenbashkesi e bashkesise $\{1, \ldots, a\}$. Meqe $A$ eshte bashkesi e fundme, rrjedh se $q_1 = \max A \in A$. Tani kemi $0 \leqslant a_1 = a - bq_1 + a_1$ dhe $a_1 < b$. Sikur mosbarazimi i fundit nuk eshte i sakte, atehere $a - b(q_1 + 1) = a - bq_1 - b \geqslant 0$, prandaj $q_1 + 1 \in A$, qe eshte ne kundershtim me faktin se $a_1$ eshte elementi maksimal i bashkesise $A$.

Qe te vertetojme se cifti $(a_1, q_1)$ eshte i vetem, e zeme se vlen e kunderta. D.m.th. e zeme se

$$a = bq_2 + a_2, \quad 0 \leqslant a_2 < b. \tag{2.2}$$

Duke zbritur (2.1) dhe (2.2), perftojme $b(q_1 - q_2) = a_2 - a_1$. E zeme se $a_2 > a_1$, atehere edhe $q_2 > q_1$. Nga ketu rrjedh se $a_2 > a_2 - a_1 = b(q_1 - q_2) \geqslant b$, gjegjesisht $a_2 > b$, qe eshte kunderthenie me relacionin (2.2). Me kaq u vertetua reprezentimi unik (2.1).

Qe te formulojmë algoritmin e Euklidit le te vertetojmë nje veti te PMP.

**Theorem 2.7** *Le te jete $a > b$ dhe $a = bq + r$, ku $0 \leqslant r < b$. Atehere $PMP(a, b) = PMP(b, r)$.*

**Vertetim**

Le te jete $c = PMP(a, b)$ dhe $d = PMP(b, r)$. Nga fakti se $a \vdots c$ dhe $b \vdots c$ dhe barazimi $r = a - bq$, rrjedh se $r \vdots c$. Prandaj $d \vdots c$ qe domethene $d \geqslant c$.

ne anen tjeter meqenese $b \vdots d$ dhe $r \vdots d$ rrjedh se $a = bq + r \vdots d$, qe domethene se edhe $c \vdots d$. Perfundojme se $c \geqslant d$. Rrjedhimisht $c = d$.

Nga teorema paraprake kemi

$$c = PMP(a, b) = PMP(b, a_1).$$

Pastaj $b = a_1 q_2 + a_2$, ku $0 \leqslant a_2 < a_1$. Prandaj

$$c = PMP(a_1, a_2).$$

Duke vazhduar proceduren paraprake, mbas nje numri te fundme hapash arrijme deri te numri $a_{k+1} = 0$. Ne ate rast $a_{k-1} = a_k q_k$ the

$$c = PMP(a_1, a_2) = PMP(a_2, a_3) = \cdots = PMP(a_{k-1}, a_k) = a_k.$$

Ja te ilustrojme algoritmin paraprak ne rastin e numrave $a = 300$ dhe $b = 120$. Kemi $a > b$ dhe $a = 2 \cdot b + 60$, gjegjesisht $300 = 2 \cdot 120 + 60$ ku $60 < 120$.

ne fund $120 = 2 \cdot 60$. Nga ketu rrjedh se

$$PMP(300, 120) = PMP(120, 60) = 60.$$

### 2.2 Edhe disa veti te PMP

1. $PMP(a, b) = PMP(b, a)$.
2. Nëse $PMP(a, b) = c$, atëhere $PMP(ak, bk) = ck$.
3. Nése $PMP(a, b) = k$, atëhere $PMP(a/k, b/k) = 1$.

## 3 Shumëfishi më i vogël i përbashkët i dy numrave $SHVP$.

**Përkufizim**. Themi se numri $c$ është shumëfishi më i vogël i përbashkët i numrave natytorë $a$ dhe $b$ në qoftë se numri $c$ i plotëson këto dy veti.

1. $c \vdots a$ dhe $c \vdots b$.
2. Nëse $d \vdots a$ dhe $d \vdots b$, atëherë $d \vdots c$.

Shumëfishin më të vogël të përbashkët të dy numrave $a$ dhe $b$ e shënojmë me $c = SHVP(a, b)$ ose shkurtimisht nëprmjet simbolit $[a, b]$.

**Theorem 3.1** *Për dy numra të çfarëdoshëm natyrorë $a$ dhe $b$ ka vend barazimi*

$$[a, b] \cdot (a, b) = ab.$$

**Vërtetimi.**
Le të jetë

$$x = \frac{ab}{(a,b)}.$$

Tani kemi $x \vdots a$ dhe $x \vdots b$, prandaj nga përkufizimi i shumëfishit më të vogël të përbashkét rrjedh se $x \vdots [a,b]$. Prandaj ekziston numri natyror $k$ i tillë që

$$x = k[a,b].$$

Nga barazimi

$$\frac{ab}{(a,b)} = k[a,b]$$

rrjedh se

$$a = \frac{[a,b]}{b} \cdot k(a,b)$$

dhe

$$b = \frac{[a,b]}{a} \cdot k(a,b).$$

Prandaj

$$a \vdots k(a,b) \text{ dhe } b \vdots k(a,b).$$

Nga vetia e dytë perkufizuese e PMP rrjedh se

$$(a,b) \vdots k(a,b).$$

Prandaj $(a,b) \geqslant k(a,b)$. Rrjedhimisht $k = 1$, çfarë duhej të vërtetohet sepse në ketë rast kemi $x = [a,b]$.

**Shembulli 3.2** *Le të jetë $a = 24$ dhe $b = 30$. Te gjejme $[a,b]$. Nga barazimi $[a,b] = ab/(a,b)$, dhe $(a,b) = 6$, rrjedh se $[a,b] = 4 \cdot 30 = 120$.*

**Theorem 3.3** *Nese*

$$n = p_1^{q_1} \cdot \dots \cdot p_k^{q_k},$$

*dhe*

$$m = p_1^{r_1} \cdot \dots \cdot p_k^{r_k},$$

*atëherë*

$$SHVP(m,n) = p_1^{\max\{q_1,r_1\}} \cdot \dots \cdot p_k^{\max\{q_k,r_k\}}.$$

Le te percaktojme $SHVP(120,300)$ duke zbatuar teoremen paraprake. Kemi

$$120 = 2 \cdot 60 = 2^2 \cdot 30 = 2^3 \cdot 15 = 2^3 \cdot 3^1 \cdot 5^1$$

dhe

$$300 = 2^2 \cdot 3^1 \cdot 5^2.$$

Prandaj

$$SHVP(120,300) = 2^{\max\{2,3\}} \cdot 3^{\max\{1,1\}} \cdot 5^{\max\{1,2\}} = 2^3 \cdot 3^1 \cdot 5^2 = 600.$$

# 4 Disa kritere plotpjesëtimit

Ne kete njesi mesimore kemi $x = a_n a_{n-1} \dots a_1 a_0 = \sum_{k=0}^{n} a_k 10^k$.

## 4.1 Plotpjesëtueshmëria me numrin 2

Numri $x$ plotpjesëtohet me numrin 2 atehere dhe vetem atehere kur shifra e fundit (gjegjesisht shifra e njesheve) e keti numrit $a_0$ eshte numer çift, d.m.th. $a_0 \in \{0, 2, 4, 6, 8\}$. Qe te vertetojme nje gje te tille vime re se $x = a_n a_{n-1} \dots a_1 \cdot 10 + a_0 = 2 \cdot (a_n a_{n-1} \dots a_1 \cdot 5) + a_0$. Meqenese $2 \cdot (a_n a_{n-1} \dots a_1 \cdot 5)$ eshte numer çift, sepse eshte faktor i numrit 2, rrhedh se ai plotpjesetohet me 2. Mbetet qe te verifikohet pohimi nese $a_0 \vdots 2$. Pra $a_0 \vdots 2$ atehere dhe vetem atehere kur $a_0 \in \{0, 2, 4, 6, 8\}$. Numri $x$ plotpjesëtohet qe plotpjesetohet me numrin 2 eshte çift.

## 4.2 Plotpjesëtueshmëria me numrin 5

Si ne rastin e plotpjesetimit me numrin 2, kemi $x = 5 \cdot (a_n a_{n-1} \dots a_1 \cdot 2) + a_0$. Meqenese $5 \cdot (a_n a_{n-1} \dots a_1 \cdot 2)$ plotpjesëtohet me 5, mbetet te provohet nese $a_0$ plotpjesetohet me 5. Dhe nje gje e tille ndodh atehere dhe vetem atehere kur $a_0 = 0$ ose $a_0 = 5$.

## 4.3 Plotpjesëtueshmëria me numrin 10

Meqense $x = 10 \cdot \cdot (a_n a_{n-1} \dots a_1) + a_0$, rrjedh se $c \vdots 10$ atehere dhe vetem atehere kur $a_0 = 0$.

## 4.4 Plotpjesëtueshmëria me numrin 4

Meqenese $x = 100 \cdot (a_n a_{n-1} \dots a_3) + a_1 a_0 = 4 \cdot 25 \cdot (a_n a_{n-1} \dots a_2)$, rrjedh se $x \vdots 4 \Leftrightarrow a_1 a_0 \vdots 4$. Dmth kriteri i plotpjesetimit me 4 sillet ne kriterin e plotpjestimit te numrit dyshifror te formuar nga dy shifrat e fundit te tij te plotesohet me 4.

Per shembull, numri $x = 873878732x$ plotpestohet me 4 atehere dhe vetem atehere kur $x \in \{0, 4, 8\}$, sepse numrat dyshifrore 20, 24, 28 plotpjesetohen me 4.

## 4.5 Plotpjesëtueshmëria me numrin 8

Meqenese $x = 1000 \cdot (a_n a_{n-1} \dots a_3) + a_2 a_1 a_0 = 8 \cdot 125 \cdot (a_n a_{n-1} \dots a_3)$, rrjedh se $x \vdots 8 \Leftrightarrow a_2 a_1 a_0 \vdots 8$. Dmth kriteri i plotpjesetimit me 8 sillet ne kriterin e plotpjestimit te numrit treshifror te formuar nga tri shifrat e fundit te tij te plotesohet me 8.

**Shembulli 4.1** *Numri $x = 873878732x$ plotpestohet me 8 atehere dhe vetem atehere kur $x \in \{0, 8\}$, sepse numrat treshifror 320, 328 plotpjesetohen me 8.*

## 4.6 Plotpjesetueshmeria me 3 dhe 9

Le te vertetojme paraprakisht nje leme

**Lemma 4.2** *Per çdo numër natyror $n$, $10^n - 1 \vdots 9$.*

**Vertetimi**. Meqenese $10^n - 1 = 9 \dots 9 = 9 \cdot (1 \dots 1)$, ku shifra 9 gjegjesisht 1 paraqitet $n$ here, rrjedh se $10^n - 1 \vdots 9$.

Tani mund te formulojme kriterin e plotpjesëtimit me 9. Ne fillim kemi $x = \sum_{k=0}^{n} a_k 10^k = \sum_{k=0}^{n} a_k((10^k - 1) + 1) = \sum_{k=0}^{n} a_k(10^k - 1) + \sum_{k=0}^{n} a_k = A + B$, ku

$$A = \sum_{k=0}^{n} a_k(10^k - 1)$$

dhe

$$B = \sum_{k=0}^{n} a_k.$$

Meqenese $10^k - 1$ plotpjesetohet me 9 per cdo $k$, rrjedh se numri $A$ plotpjesetohet me 9. Mbetet te kontyrollohet nese numri $B$ qe paraqet shumen e shifrave te ketij numri te plotpjesetohet me 3 ose me 9, meqenese $A$ plotpjesetohet natyrisht me 3, ngase plotpjesetohet me 9.

**Shembulli 4.3** *Te kontrollojme nese numri $x = 126562a3873873b$ plotpjesetohet me 3 ose me 9.*

*Njehsojme shumen e shifrave $B = 1 + 2 + 6 + 5 + 6 + 2 + a + 3 + 8 + 7 + 3 + 8 + 7 + 3 + b = 61 + a + b = 63 + a + b - 2$. Pra duhet te gjejme te gjitha shifrat e numrave $a$ dhe $b$ ashtu qe $a + b - 2$ te plotpjesetohet me 3. Pastaj te gjejme te gjithe chiftet e numrave $a$ dhe $b$ ashtu qe numri $a + b - 2$ te plotpjesetohet me 9.*

*Per 3 kemi me shume zgjidhje:*

$(a, b) \in \{(0, 2), (0, 5), (0, 8), (1, 1), (1, 4), (1, 7), (2, 0), (2, 3), (2, 5),$
$(2, 8), (3, 2), (3, 5), (3, 8), (4, 1), (4, 4), (4, 7), (5, 0), (5, 3), (5, 6),$
$(5, 9), (6, 2), (6, 5), (6, 8), (7, 1),$
$(7, 4), (7, 7), (8, 0), (8, 3), (8, 6), (8, 9), (9, 1), (9, 4), (9, 7)\}$.

*Per numrin 9 kemi me pak zgjidhje dhe ato jane*

$(a, b) \in \{(0, 2), (1, 1), (2, 0), (2, 9), (3, 8), (4, 7), (5, 6), (6, 5), (7, 4), (8, 3), (9, 2)\}$.

# 5 Numrat e plotë

Ekuacioni

$$b + x = a \tag{5.1}$$

per $b > a$ nuk ka zgjidhje ne bashkesine $\mathbf{N}$, gjegjesusht nuk ekziston numri natyror $x$ i tille qe barazimi (5.1) te jete i sakte. Ky eshte motivi i pare qe bashkesia e numrave natyrore te plotesohet (zgjerohet) me nje bashkesi numrash, ashtu qe ekuacioni (5.1) te kete zgjidhje. Zgjidhjen e ekuacionit (5.1) do ta shenojme me $x = a - b$, mirepo nje veprim i tille tani nuk esht i lejueshem, qe

si rrjedhim na detyron qe shprehjen $a-b$ ta zevendesojme me çiftin $(a,b)$. Per chfar behet fjale do te lexoni ne vazhdim.

Le të jete $\sim$ relacioni ne bashkësine $\mathbf{N}_0 \times \mathbf{N}_0$ i perkufizuar siç vijon

$$(a,b) \sim (a',b') \Leftrightarrow a+b' = b+a'.$$

Le te vertetojme se reacioni $\sim$ eshte relacion ekuivalence ne bashesine $\mathbf{N}_0 \times \mathbf{N}_0$.

1. Vetia refleksive. $(a,b) \sim (a,b)$ sepse $a+b = b+a$ (nga vetia komutative e mbledhjes se numrave).

2. Vetia simetrike. $(a,b) \sim (a',b') \Rightarrow (a',b') \sim (a,b)$ sepse $a+b' = b+a' \Rightarrow a'+b = b'+a$.

3. Vetia tranzitive. $(a,b) \sim (a',b') \wedge (a',b') \sim (a'',b'') \Rightarrow (a,b) \sim (a'',b'')$ sepse $a+b' = b+a' \wedge a'+b'' = b'+a'' \Rightarrow a+b'+a'+b'' = b+a'+b'+a''$. Prandaj $a+b'' = b+a''$.

Çdo relacion ekuivalence e ndan bashkesine perkatese ne klasa ekuivalence. Bashkesia e klasave te ekuivalences e formojne bashkesine faktor e cila ne kete rast paraqet bashkesine e numrave te plote te cilen e shenojme nepermjet simbolit $\mathbb{Z}$. Pra

$$\mathbb{Z} = \mathbf{N}_0 \times \mathbf{N}_0 /_\sim = \{\overline{(n,m)} : n,m \in \mathbf{N}_0\} = \{\overline{(n,0)} : n \in \mathbf{N}_0\} \bigcup \{\overline{(0,n)} : n \in \mathbf{N}_0\}.$$

Elementin $\overline{(0,0)}$ e shenojme shkurtimisht me 0

Elementi $\overline{(0,0)} \subset \mathbf{N}_0 \times \mathbf{N}_0$ formalisht perfshin kete bashkesi pambarimisht te madhe $\{(0,0),(1,1),\dots,(n,n),\dots\}$ dhe e shenojme shkurtimisht me 0 (ky element nuk perputhet formalisht me elementin zero nga bashkesia $\mathbf{N}_0$).

Elementi $\overline{(1,0)} \subset \mathbf{N}_0 \times \mathbf{N}_0$ formalisht perfshin kete bashkesi pambarimisht te madhe $\{(1,0),(2,1),\dots,(n+1,n),\dots\}$, Kete numer e shenojme shkurtimish me 1.

E keshtu me radhe, elementi $\overline{(m,0)} \subset \mathbf{N}_0 \times \mathbf{N}_0$ formalisht perfshin kete bashkesi pambarimisht te madhe $\{(m,0),(m+1,1),\dots,(m+n,n),\dots\}$, Kete numer e shenojme shkurtimish me $m$.

Elementi $\overline{(0,1)} \subset \mathbf{N}_0 \times \mathbf{N}_0$ formalisht perfshin kete bashkesi pambarimisht te madhe $\{(0,1),(1,2),\dots,(n,n+1),\dots\}$, Kete numer e shenojme shkurtimish me $-1$. Elementi $\overline{(0,m)} \subset \mathbf{N}_0 \times \mathbf{N}_0$ formalisht perfshin kete bashkesi pambarimisht te madhe $\{(0,m),(1,1+m),\dots,(n,n+m),\dots\}$, Kete numer e shenojme shkurtimish me $-m$.

Prandaj

$$\mathbb{Z} = \{0,1,-1,2,-2,\dots,m,-m,\dots\}.$$

Bashkesia $\mathbb{Z}$ e *numvae te plotë* e perbehet nga bashkesia e numrave pozitivë, negativë dhe zero.

### 5.0.1 Shtrirja e bashkesise N ne bashkesine $\mathbb{Z}$.

Nenbashkesia $\mathbf{N}' = \{\overline{(n,0)} : n \in \mathbf{N}\}$ e bashkesise $\mathbb{Z}$ identifikohet me bashkesine $\mathbf{N}$, ashtu qe numrat e plote $\overline{(n,0)}$ identifikonen me numrat $n$ per cdo $n$.

## 5.1 Mbledhja e numrave të plotë

Shuma e numrave te plote $a = \overline{(n,m)}$ dhe $b = \overline{(k,l)}$ eshte numri i plote

$$c = a + b = \overline{(n+k, m+l)}.$$

Le te vertetojme se ky perkufizim eshte korrekt, dmth nuk varet nga perfaqesuesi i klases.

E zeme se $a = \overline{(n',m')}$ dhe $b = \overline{(k',l')}$ d.m.th.

$$n + m' = m + n', \quad k + l' = l + k'. \tag{5.2}$$

Duhet te vertetojme se

$$\overline{(n+k, m+l)} = \overline{(n'+k', m'+l')}.$$

Relacioni i fundit eshte ekuivalent me barazimin

$$n + k + m' + l' = m + l + n' + k',$$

i cili rrjedh nga relacionet (5.2).

## 5.2 Vetite e mbledhjes

1. Vetia komutative. $\forall a, b \in \mathbb{Z}$, $a + b = b + a$. E zeme se $a = \overline{(n,m)}$ dhe $b = \overline{(k,l)}$. Barazimi $a + b = b + a$ eshte ekuivalent me barazimet

   $$n + k = k + n, \quad m + l = l + m.$$

   Barazimet e efundit rrjedhin nga vetia komutative e mbledhjes se numrave nagtyrorë.

2. Vetia asociative. $\forall a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$.

3. Elementi neutral. $\forall a \in \mathbf{Z}$, $a + 0 = a = 0 + a$.

4. Elementi invers i mbledhjes. $\forall a \in \mathbf{Z}$, ekziston $b = -a \in \mathbf{Z}$, i tille qe $a + b = 0$. Nese $a = \overline{(m,n)}$, atehere $b = -a = \overline{(n,m)}$. Ne te vertete $a + b = \overline{(m+n, n+m)} = 0$.

## 5.3 Shumezimi i numrave te plote

.

Prodhimi i numrave te plote $a = \overline{(n,m)}$ dhe $b = \overline{(k,l)}$ eshte numri i plote

$$c = a \cdot b = \overline{(nk + ml, nl + mk)}.$$

Le te vertetojme se ky perkufizim eshte korrekt, dmth nuk varet nga perfaqesuesi i klases.

E zeme se $a = \overline{(n',m')}$ dhe $b = \overline{(k',l')}$ d.m.th.

$$n + m' = m + n', \quad k + l' = l + k'. \tag{5.3}$$

Nga (5.3) rrjedh se
$n(k + l') = n(l + k')$, $m(l + k') = m(k + l')$,
$(m + n')l' = (n + m')l'$, $(n + m')k' = (m + n')k'$.
Duke i mbledh keto barazime perftojme

$$nk + ml + n'l' + m'k' = nl + mk + n'k' + m'l'.$$

Nga ketu perftojme

$$\overline{(nk + ml, nl + mk)} = \overline{(n'k' + m'l', n'l' + m'k')}.$$

Keshtu vertetuam se shumezimi eshte korrekt.

## 5.4 Vetite e shumezimit

1. Vetia komutative. $\forall a, b \in \mathbb{Z}$, $ab = ba$. E zeme se $a = \overline{(n,m)}$ dhe $b = \overline{(k,l)}$. Barazimi $ab = ba$ eshte ekuivalent me barazimet

   $$\overline{(nk + ml, nl + mk)} = \overline{(kn + lm, ln + km)}$$

   qe eshte barazim i thjeshte.

2. Vetia asociative. $\forall a, b, c \in \mathbb{Z}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. Edhe ky barazim vertetohet ne menyere te ngjashme si ai paraprak

3. Elementi neutral. $\forall a \in \mathbf{Z}$, $a \cdot 1 = a = 1 \cdot a$. Nese $a = \overline{(n,m)}$, dhe $1 = \overline{(1,0)}$, atehere $a \cdot 1 = \overline{(n \cdot 1 + m \cdot 0, m \cdot 1 + n \cdot 0)} = \overline{(n,m)}$.

4. Vetia shperndarese. Per çdo tre numra natyrorë $a, b, c \in \mathbb{Z}$ kemi $a \cdot (b + c) = a \cdot b + a \cdot c$. Barazimi paraprak rrjedh nga barazimi i ngjashem per numrat natyrorë prandaj nuk e vertetojme.

## 5.5 Zbritja e numrave te plote

Le te jete $a = \overline{(n,m)}$ dhe $b = \overline{(k,l)}$. Bëjmë pekufizimin

$$a - b = \overline{(n+l, m+k)}.$$

Tani te kthehemi te ekuacioni (5.1) dhe vime re se ky ekuacion ka zgjidhje ne bashkesine $\mathbb{Z}$, sepse $a - b \in \mathbb{Z}$, ne qofte se $a, b \in \mathbb{Z}$. Meqense $\mathbf{N} \subset \mathbb{Z}$, rrjedh se ja kemi arritur qellimit fillestar qe te zgjidhim ekuacionin (5.1).

Në bazë te pohimeve paraprake mund te formulojme teoremen e mëposhtme.

**Theorem 5.1** *Struktura $(\mathbb{Z}, +, \cdot, 0, 1)$ është unazë me element njesh (me elementin neutral ne lidhje me shumezimin).*

*Me fjalë te tjera. Per çdo tre numra te plote $a, b, c$ kane vend barazimet e meposhtme.*

1. $a + b \in \mathbb{Z}$, *(Mbledhja eshte veprim i mbyllur)*
2. $(a + b) + c = a + (b + c)$, *(Mbledhja eshte shoqeruese)*
3. $a + 0 = 0 + a = a$, *(Elementi neutral i mbledhjes eshte numri 0)*
4. $a - a = 0$, *(Ekziston elementi i anasjellet i secilit numer)*
5. $a \cdot b \in \mathbb{Z}$, *(Shumezimi eshte veprim i mbyllur)*
6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, *(Shumezimi ploteson vetine shoqeruese)*
7. $a \cdot b = b \cdot a$, *(Shumezimi eshte komutativ)*
8. $a \cdot 1 = a$, *(Numri 1 eshte elementi neutral i shumezimit)*
9. $a \cdot (b + c) = a \cdot b + a \cdot c$ *(Vlen vetia shperdnarese)*
10. $(a + b) \cdot c = a \cdot c + b \cdot c$. *(Vlen vetia shperdnarese)*

## 5.6 Radhitja e numrave te plote dhe boshti numerik

Themi se numri i plote $a = \overline{(n,m)}$ eshte me i vogel ose i barabarte se numri i plote $b = \overline{(k,l)}$ dhe shenojme $a \leqslant b$, ne qofte se $n + l \leqslant m + k$.

Ky relacion eshte relacion radhitjeje ne bashkesine $\mathbb{Z}$.

Ne te vertet, kane vend vetite ne vazhdim

1. Vetia refleksive. Per $a = \overline{(n,m)}$, $a \leqslant a$, sepse $n + m \leqslant m + n$.
2. Vetia antisimetrike. Per $a = \overline{(n,m)}$ dhe $b = \overline{(k,l)}$, kemi $a \leqslant b \wedge b \leqslant a \Rightarrow a = b$, sepse, $n + l \leqslant m + k$ dhe $k + m \leqslant l + n$, rrjedh se $n + l = m + k$, gjegjesisht $a = b$.
3. Vetia tranzitive. Per $a = \overline{(n,m)}$, $b = \overline{(k,l)}$ dhe $c = \overline{(i,j)}$, $a \leqslant b \wedge b \leqslant c \Rightarrow a \leqslant c$. Ne te vertet, nga $n + l \leqslant m + k \wedge k + j \leqslant l + i$, rrjedh se $n + l + k + j \leqslant m + k + l + i$ d.m.th. $n + j \leqslant m + k$

Numrat me te vegjel se 0 jane negative, kurse ata me te medhenj se 0 jane pozitive. Numrat zakonisht shenohen ne nje drejtez (qe e quajme bosht numerik) te drejtuar me nje shigjete nga ana e majte ne te djathte.




## 5.7 Vetitë e radhitjes së numrave te plotë

E zëmë se $z, w, t$ janë numra të plotë. Atehere kane vend keto veti

1. $z + w < z + t \Leftrightarrow w < t$,
2. $z + w > z + t \Leftrightarrow w > t$,
3. Ne qoftë se $z > 0$ atëherë $z \cdot w < z \cdot t \Leftrightarrow w < t$,
4. Ne qoftë se $z > 0$ atëherë $z \cdot w > z \cdot t \Leftrightarrow w > t$,
5. Ne qoftë se $z < 0$ atëherë $z \cdot w < z \cdot t \Leftrightarrow w > t$,
6. Ne qoftë se $z < 0$ atëherë $z \cdot w > z \cdot t \Leftrightarrow w < t$,

Le te provojmë pë shembull, vetine e parë. E zeme se $z = \overline{(a, b)}$, $w = \overline{(c, d)}$ dhe $t = \overline{(e, f)}$. Atehere $z+w = \overline{(a + c, b + d)}$ dhe $z+t = \overline{(a + e, b + f)}$. Nga ketu rrjedh se $z+w < z+t$ atehere dhe vetem atehere kur $a+c+b+f < b+d+a+e$, dhe nga monotoniteti i numrave natyrorë relacioni i fundit është ekuivalent me relacionin $c + f < d + e$ gjegjesisht me relacionin $w < t$.

## 5.8 Pjesëtimi pa mbetje i numrave të plotë

Themi se numri i plotë $z$ plotpjesëtohet me numrin e plotë $w$ ne qoftë se ekziston numri i plotë $t$ i tillë që $z = w \cdot t$. Shenojmë simbolikisht $z \vdots w$. Numrin $t$ e shenojme $t = z : w$ ose $t = \frac{z}{w}$.

**Disa veti**

1. Nese $z \vdots w$, atehere kemi $(z : w) \cdot w = z$.
2. $(z \cdot w)/w = z$,
3. Nese $z \vdots t$ dhe $w \vdots t$ atehere edhe $(w \pm w) \vdots t$ dhe kemi $\frac{z \pm w}{t} = \frac{z}{t} \pm \frac{w}{t}$.

## 5.9 Vlera absolute e numrit të plotë

E zeme se $z \in \mathbb{Z}$ është numër i plotë i çvarëdoshëm. Vlera absolute e numrit $z$ shënohet me simbolin $|z|$. Numri $|z|$ është i barabartë me numrin $z$ nese $z \geqslant 0$, dhe është i barabartë me numrin $-z$ nese $z < 0$. Këtë fjali përkufizuese të vlerës absolute e shënojmë shkurtimisht siç vijon:

$$|z| = \begin{cases} z, & \text{nese } z \geqslant 0; \\ -z, & \text{nese } z < 0. \end{cases}$$

### 5.9.1 Vetitë e vlerës absolute

E zeme se $z, w, t \in \mathbb{Z}$. Atëherë kemi:

1. $|z \cdot w| = |z| \cdot |w|$,
2. $|z + w| \leqslant |z| + |w|$,
3. $|z - w| \leqslant |z| + |w|$,
4. $|z| - |w| \leqslant |z| + |w|$,
5. Nese $z \vdots w$ atehere edhe $|z| \vdots |w|$ dhe kemi
$$\left|\frac{z}{w}\right| = \frac{|z|}{|w|}.$$
6. $|z| \leqslant y \Leftrightarrow -y \leqslant z \leqslant y$

Le te vertetojme per shembull vetine e dyte (e cila ke emertimin *mosbarazimi i trekendeshit*). Sipar perkufizimit kemi $|z+w| = \begin{cases} z+w, & \text{nese } z+w \geqslant 0; \\ -(z+w), & \text{nese } z+w < 0. \end{cases}$ Meqenese $z \leqslant |z|$ dhe $w \leqslant |w|$, rrjedh se $z + w \leqslant |z| + |w|$. Ngjashem, $-z \leqslant |z|$ dhe $-w \leqslant |w|$, prandaj $-(z + w) \leqslant |z| + |w|$. Nga keto dy mosbarazime rrjedh se $|z + w| \leqslant |z| + |w|$.

Vertetojme tani vetine e fundit. Nga $|z| \leqslant y$, rrjedh se $z \leqslant y$ dhe $-z \leqslant y$. Prandaj $z \leqslant y$ dhe $z \geqslant -y$. Prandaj $-y \leqslant z \leqslant y$.

## 5.10 Fuqia dhe rrenja katrore e numrave te plote

Per numrin e plote $z$ dhe numrin natyror $n$, e perkufizojme $z^n = z \cdot \cdots \cdot n$, ku prodhimi paraqitet $n$ here. Per shembull $z^1 = z$, $z^2 = z \cdot z$, $z^3 = z \cdot z \cdot z$.

Ja disa veti:

1. $(z \cdot w)^n = z^n \cdot w^n$.
2. Nese $z \vdots w$, atehere $\left(\frac{z}{w}\right)^n = \frac{z^n}{w^n}$.
3. $z^{n+m} = z^n \cdot z^m$,
4. $(z^n)^m = z^{nm}$.

## 5.11 Rrenja katrore e numrave te plote

Themi se numri natyror $x$ eshte rrenja katrore e numrit te plot $y$ nese $x^2 = y$. Kete numer e shenojme me $x = \sqrt{y}$.

# 6 Pjesëtuesi më i madh i përbashkët i dy numrave te plotë $PMP$.

**Përkufizim**. Themi se numri natyror $c$ është pjesëtuesi më i madh i përbashkët i numrave te plotë $a$ dhe $b$ në qoftë se numri $c$ i plotëson këto dy veti.

1. $a \vdots c$ dhe $b \vdots c$.
2. Nëse $a \vdots d$ dhe $b \vdots d$, atëherë $c \vdots d$.

Pjesëtuesim më të madh të peprbashkët te numrave $a$ dhe $b$ e shënojmë me $c = PMP(a, b)$ ose shkurtimisht nëprmjet simbolit $(a, b)$.

**Shembulli 6.1** *Le të jetë $a = -120$ dhe $b = 300$. Të percaktojmë $PMP(a, b)$. Pjesëtuesit e numrit a janë $A = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 18, 20, 24, 30, 40, 60, 120\}$, $\cup\{-1, -2, -3, -4, -5, -6, -8, -10, -12, -15, -16, -18, -20, -24, -30, -40, -60, -120\}$, kurse pjesëtuesit e numrit b janë $B = \{1, 2, 3, 4, 5, 6, 10, \ldots, 60, 100, 150, 300\}$ $\cup\{-1, -2, -3, -4, -5, -6, -10, \ldots, -60, -100, -150, -300\}$. Numri më i madh i përbashët i bashkësive $A$ dhe $B$ është numri 60, prandaj $PMP(a, b) = 60$.*

Metoda e zbatuar paraprakisht nuk është praktike prandaj, si tek numrat natyrore zbatojmë dy metoda të tjera që bazohen në:

1. Teoremën themelore të aritmetikës
2. Algoritmin e Euklidit.

Qe te formulojmë teoremën themelore të aritmetikës le të perkufizojmë numrat e thjeshtë.

**Perkufizimi 6.2** *Themi se numri natyror $n \neq 1$ është i thjeshtë, në qoftë se plotpjesëtohet vetëm me numrat $1, -1, n$ dhe $-n$.*

Numrat e thjeshtë i shënojmë me $P$. Pra

$$P = \{p_1, p_2, \ldots, p_k, \ldots\} = \{\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \ldots\}.$$

Kjo bashkësi numrash është bashkësi e pafundme. Vĭtetimi mund të bëhet nëpĭrmjet

**Theorem 6.3 (Teorema themelore e aritmetikes)** *Çdo numër i plotë $n$ mund të shënohet në trajtën e produktit të numrave të thjeshtë pozitiv dhe eventualisht numrit $-1$. Me fjalë të tjera, ekzistojnë numrat e thjeshtë $p_1 < p_2 < \ldots, p_k$ dhe numrat natyrorë ose zero $q_1, \ldots q_k$ ashtu që*

$$n = \pm p_1^{q_1} \cdot \ldots p_k^{q_k}.$$

*Representimi paraprak eshte i vetem.*

**Theorem 6.4** *Nese*

$$n = \pm p_1^{q_1} \cdot \ldots p_k^{q_k},$$

*dhe*

$$m = \pm p_1^{r_1} \cdot \ldots p_k^{r_k},$$

*atëherë*

$$PMP(m,n) = p_1^{\min\{q_1,r_1\}} \cdot \ldots p_k^{\min\{q_k,r_k\}}.$$

Le te percaktojme $PMP(-120, 300)$ duke zhatuar teoremen paraprake. Kemi

$$-120 = -2 \cdot 60 = 2^2 \cdot 30 = 2^3 \cdot 15 = 2^3 \cdot 3^1 \cdot 5^1$$

dhe

$$300 = 2^2 \cdot 3^1 \cdot 5^2.$$

Prandaj

$$PMP(-120, 300) = 2^{\min\{2,3\}} \cdot 3^{\min\{1,1\}} \cdot 5^{\min\{1,2\}} = 2^2 \cdot 3^1 \cdot 5^1 = 60.$$

**Theorem 6.5** *Bashkësi e numrave të thjeshtë të plotë është e pafundme.*

**Vertetimi.** Meqenese kjo bashkesi i permban te gjithe numrat e thjeshte pozitiv, eshte e qarte se kjo bashkesi eshte e pafundme, ne baze te teoremes perkatese te numrave natyrore (shiko Teorema 2.5).

## 6.1 Algoritmi i Euklidit

Ky algoritem bazohet ne teoremen e meposhtme

**Theorem 6.6** *Per çdo dy numra te plote $a$ dhe $b$ per te cilet vlen $|a| > |b|$ ekzistojne numrat e plote te vetem $a_1$ dhe $q_1$ ashtu qe*

$$a = bq_1 + a_1, \quad 0 \leqslant a_1 < |b|.$$

Qe te formulojmë algoritmin e Euklidit le te vertetojmë nje veti te PMP.

**Theorem 6.7** *Le te jete $|a| > |b|$ dhe $a = bq + r$, ku $0 \leqslant r < b$. Atehere $PMP(a,b) = PMP(b,r)$.*

**Vertetim**

Le te jete $c = PMP(a,b)$ dhe $d = PMP(b,r)$. Nga fakti se $a \vdots c$ dhe $b \vdots c$ dhe barazimi $r = a - bq$, rrjedh se $r \vdots c$. Prandaj $d \vdots c$ qe domethene $d \geqslant c$.

ne anen tjeter meqenese $b \vdots d$ dhe $r \vdots d$ rrjedh se $a = bq + r \vdots d$, qe domethene se edhe $c \vdots d$. Perfundojme se $c \geqslant d$. Rrjedhimisht $c = d$.

Nga teorema paraprake kemi

$$c = PMP(a,b) = PMP(b,a_1).$$

Pastaj $b = a_1q_2 + a_2$, ku $0 \leqslant a_2 < a_1$. Prandaj

$$c = PMP(a_1, a_2).$$

Duke vazhduar proceduren paraprake, mbas nje numri te fundme hapash arrijme deri te numri $a_{k+1} = 0$. Ne ate rast $a_{k-1} = a_k q_k$ dhe

$$c = PMP(a_1, a_2) = PMP(a_2, a_3) = \cdots = PMP(a_{k-1}, a_k) = a_k.$$

Ja te ilustrojme algoritmin paraprak ne rastin e numrave $a = -300$ dhe $b = 120$. Kemi $|a| > |b|$ dhe $a = (-3) \cdot b + 60$, gjegjesisht $-300 = (-3) \cdot 120 + 60$ ku $60 < |120|$.

Ne fund $120 = 2 \cdot 60$. Nga ketu rrjedh se

$$PMP(300, 120) = PMP(120, 60) = 60.$$

## 6.2 Edhe disa veti te PMP

1. $PMP(a, b) = PMP(|a|, |b|)$.
2. Nëse $PMP(a, b) = 1$, atëhere $PMP(ak, bk) = ck$.
3. Nése $PMP(a, b) = k$, dhe $a \vdots m$ dhe $b \vdots m$ atëhere $PMP(a/m, b/m) = k/m$.

# 7 Shumëfishi më i vogël i përbashkët i dy numrave te plotë $SHVP$.

**Përkufizim**. Themi se numci pozitiv $c$ është shumëfishi më i vogël i përbashkët i numrave natytorë $a$ dhe $b$ në qoftë se numri $c$ i plotëson këto dy veti.

1. $c \vdots a$ dhe $c \vdots b$.
2. Nëse $d \vdots a$ dhe $d \vdots b$, atëherë $d \vdots c$.

Shumëfishin më të vogël të përbashkët të dy numrave $a$ dhe $b$ e shënojmë me $c = SHVP(a, b)$ ose shkurtimisht nëprmjet simbolit $[a, b]$.

**Theorem 7.1** *Për dy numra të çfarëdoshëm të plotë $a$ dhe $b$ ka vend barazimi*

$$[a, b] \cdot (a, b) = |a||b|.$$

**Vërtetimi behet si ne rastin e teoremes perkatese per numrat e natyrorë.**

**Shembulli 7.2** *Le të jetë $a = -24$ dhe $b = -30$. Te gjejme $[a, b]$. Nga barazimi $[a, b] = |a||b|/(a, b)$, dhe $(a, b) = 6$, rrjedh se $[a, b] = 4 \cdot 30 = 120$.*

# 8 Kongruenca

**Perkufizimi 8.1** *Le te jete $m$ nje numer natyror $m > 1$. Themi se numri i plote $a$ eshte kongruent me numrin e plotë $b$ sipas modulit $m$ nese $(a-b) \vdots m$. Kete fakt e shenojme simbolikisht $a \equiv b \mod m$.*

**Theorem 8.2** *Kongruenca sipas modulit $m$ është relacion ekuivalence.*

**Vertetimi.**

Duhet te vertetojme tri veti (R (Refleksive), S (Simetrike) dhe T (Tranzitive)).

Vetia refleksive vlen sepse nese $x$ eshte numer i plote, atehere $x - x = 0$, dhe numri 0 plotepjesetohet me çdo numer sepse $0 = 0 \cdot m$. Prandaj $x \equiv x \mod m$.

Vetia simetrike vlen sepse nese $x - y \vdots m$ atehere ekziston numri i plote $k$ i tille qe $x - y = k \cdot m$. Prandaj $y - x = (-k) \cdot m$. meqenese $-k$ eshte gjithashtu i plote, rrjedh se $y - x \vdots m$. Prandaj $x \equiv y \mod m \Rightarrow y \equiv x \mod m$.

Ne fund vetia tranzitive gjithashtu vlen. E zeme se $x \equiv y \mod m$ dhe $y \equiv z \mod m$. Nga ketu rrjedh se $x - y \vdots m$ dhe $y - z \vdots m$. Prandaj edhe shuma e ketyre numrave: $(x - y) + (y - z) = x - z \vdots m$. Perfundojme se $x \equiv z \mod m$.

Relacioni $\mod m$ e ndan bashkesine e numrave te plote $\mathbf{Z}$ ne $m$ klasa ekuivalence. Keto jane $\overline{0}, \overline{1}, \ldots, \overline{m-1}$, qe paraqesin mbetjet e mundeshme te pjesetimit me $m$. Ne te vertet ne bashkesine faktor $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ mund te perkufizojme mbledhjen dhe shumezimin sipas formulave ne vazhdim.

$$\overline{x} \oplus \overline{y} = \overline{x + y} \tag{8.1}$$

dhe

$$\overline{x} \odot \overline{y} = \overline{x \cdot y}. \tag{8.2}$$

Keto dy veprime algjebrike ne $\mathbb{Z}_m$ jane perkufizuar mirë. Ne te vertet, e zeme se $x \equiv x' \mod m$ dhe $y \equiv y' \mod m$. Ne kete rast kemi $x = x' + km$ dhe $y = y' + k_1 m$, per dy numra te plote $k$ dhe $k_1$. Prandaj $x + y = x' + y' + (k + k_1)m$, qe domethene se $x + y \equiv (x' + y') \mod m$. Me fjale te tjera, ne perkufizimin (8.1), nuk eshte e rendesishme se cilet perfaqesues te klasave marrim.

Ngjashem edhe (8.2) eshte i perkufizuar mire. Ne te vertet, duke perdor simbolet paraprake, perkftojme: $x \cdot y = x' \cdot y' + m(kk_1 + x' + y')$, qe domethene $x \cdot y = x' \cdot y' \mod m$. Le te konstatojme se $\overline{0}$ eshte elementi neutral i mbledhjes dhe $\overline{1}$ eshte elementi neutral i shumezimit. Qe te vertetojme nje gje te tille marrim $\overline{x} \in \mathbb{Z}_m$. Per mbledhjen kemi

$$\overline{0} \oplus \overline{x} = \overline{0 + x} = \overline{x} = \overline{x + 0} = \overline{x} \oplus \overline{0},$$

kurse per shumezimin

$$\overline{1} \odot \overline{x} = \overline{1 \cdot x} = \overline{x} = \overline{x \cdot 1} = \overline{x} \odot \overline{1}.$$

Tani formulojme teoremen.

**Theorem 8.3** *Struktura* $(\mathbb{Z}_m, \oplus, \odot, \overline{0}, \overline{1})$ *eshte unaze me element neutral te shumezimit. Ne qofte se* $m$ *eshte numer i thjeshte atehere kjo unaze eshte fushë.*

**Vertetimi**

Duhet te vertetojme se $(\mathbb{Z}_m, \oplus, \overline{0})$ është grup abelian.

1. $\forall \overline{x}, \overline{y} \in \mathbb{Z}_m$ kemi $\overline{x} \oplus \overline{y} \in \mathbb{Z}_m$. Kemi vertetuar paraprakisht.
2. $\forall \overline{x}, \overline{y} \in \mathbb{Z}_m$ kemi $\overline{x} \oplus \overline{y} = \overline{y} \oplus \overline{x}$, sepse $x + y = y + x$. Prandaj vlen vetia nderruese e mbledhjes.
3. $\forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_m$ kemi $(\overline{x} \oplus \overline{y}) \oplus \overline{z} = \overline{y} \oplus (\overline{x} \oplus \overline{z})$, sepse $(\overline{x} \oplus \overline{y}) \oplus \overline{z} = (\overline{x \oplus y} \oplus \overline{z}) = \overline{(x + y) + z} = \overline{x + (y + x)} = \overline{x} \oplus \overline{(y + z)} = \overline{x} \oplus (\overline{y} \oplus \overline{z})$. Prandaj vlen vetia asosciative e mbledhjes.
4. $\forall \overline{x} \in \mathbb{Z}_m$ vlen $\overline{x} \oplus \overline{0} = \overline{0}$, prandaj ekziston elementi neutral i mbledhjes.
5. $\forall \overline{x} \in \mathbb{Z}_m$, $\overline{m - x} \in \mathbb{Z}_m$ dhe kemi $\overline{x} \oplus \overline{m - x} = \overline{m} = \overline{0}$. Prandaj ekziston elementi neutral i secilit numer nga bashkesia faktor.

Qe te vertetojme se struktura e dhene eshte unaze, na duhet qe te vertetojme se $(\mathbb{Z}_m, \odot, \overline{1})$ është gjysmegrup me element neutral.

1. $\forall \overline{x}, \overline{y} \in \mathbb{Z}_m$ kemi $\overline{x} \odot \overline{y} \in \mathbb{Z}_m$. Kemi vertetuar paraprakisht.
2. $\forall \overline{x}, \overline{y} \in \mathbb{Z}_m$ kemi $\overline{x} \odot \overline{y} = \overline{y} \odot \overline{x}$, sepse $x \cdot y = y \cdot x$. Prandaj vlen vetia nderruese e shumezimit.
3. $\forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_m$ kemi $(\overline{x} \odot \overline{y}) \odot \overline{z} = \overline{x} \odot (\overline{y} \odot \overline{z})$, sepse $(x \cdot y) \cdot z = x \cdot (y \cdot x)$. Prandaj vlen vetia asosciative e shumezimit.
4. $\forall \overline{x} \in \mathbb{Z}_m$ vlen $\overline{x} \odot \overline{1} = \overline{x} = \overline{1} \odot \overline{x}$, prandaj ekziston elementi neutral i mbledhjes.

Mbetet qe te vertetojme vetite distributive, gjegjesisht shpendarese.

1. $\forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_m$, $(\overline{x} \oplus \overline{y}) \odot \overline{z} = (\overline{x} \odot \overline{y}) \oplus (\overline{y} \odot \overline{z})$. Sepse $(x + y) \cdot z = x \cdot z + y \cdot z$.
2. $\forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_m$, $\overline{x} \odot (\overline{y} \oplus \overline{z}) = \overline{x} \odot \overline{y} \oplus \overline{x} \odot \overline{z}$. Sepse $x(y + z) = x \cdot y + x \cdot z$.

Me kaq vertetuam se struktura ne fjale eshte unaze.

Mbetet qe te vertetohet se struktura ne fjale eshte fushe nese numri $m$ është i thjeshtë. E zeme se $\overline{x} \in \mathbb{Z}_m \setminus \{\overline{0}\}$. Duhet te gjejme numrin $y$ te tille qe $xy = 1$ mod $m$. Le te jete $q$ mbetja e numrit $x$ gjate pjesetimit me numrin $m$. Dmth $x = x_1 m + q$. Ne kete rast kemi $0 \leqslant q < m$. Meqe $\overline{x} \neq \overline{0}$, rrjedh se $q > 0$. Meqenese numri $m$ eshte i thjeshte, rrjedh se $1 = PMP(x, m) = PMP(m, q)$ (Teorema 6.7). Duke vazhduar pjesetimin me mbetje, perftojme $m = m_1 \cdot q + q_1$, ku $0 < q_1 < q$. Nga ketu rrjedh se

$$PMP(m, q) = PMP(q, q_1) = PMP(q_1, q_2)$$

$$= \cdots = PMP(q_{k-2}, q_{k-1}) = PMP(q_{k-1}, q_k) = PMP(q_k, 1).$$

Duke zbatuar Analizen e anasjellet perftojme $q_{k-1} = x_k q_k + 1$. Nga ketu rrjedh se

$$q_{k-2} = x_{k-1}q_{k-1} + q_k, \ldots, \ q_1 = x_2 q_2 + q_3$$

$$1 = q_{k-1} - x_k q_k = q_{k-1} - x_k(q_{k-2} - x_{k-1}q_{k-1}) = a_1 q_{k-1} + b_1 q_{k-2}$$

$$= \cdots = a_2 q_{k-2} + b_2 q_{k-3} = \cdots = a_{k-1}q_1 + b_{k-1}q = a_k q + b_k m = a_{k+1}m + b_{k+1}x$$

Pra

$$xy = 1 + zm,$$

ku $y = b_{k+1}$, kurse $z = -a_{k+1}$. Perfundojme se $\overline{xy} = \bar{1}$. Prandaj numri $x$ ka inversin e vete. Perfundojme se struktura ne fjale eshte fushe

**Shembulli 8.4** *Le te jete $m = 5$. Ne kete rast per mbledhje kemi*

| $\oplus$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |

*Ketu kemi $-\bar{0} = \bar{0}$, $-\bar{1} = \bar{4}$, $-\bar{2} = \bar{3}$, $-\bar{3} = \bar{2}$ dhe $-\bar{4} = \bar{1}$.*
*Per shumezim kemi*

| $\odot$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|---|---|---|---|---|
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{4}$ | $\bar{1}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{1}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

*ne kete rast kemi $\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{3}$, $\bar{3}^{-1} = \bar{2}$ dhe $\bar{4}^{-1} = \bar{4}$. Sepse per shembull* $3 \cdot 2 = 1 + 5 \equiv 1 \mod 5$.

**Shembulli 8.5** *Te gjendet $m$ dhe $n$ ashtu qe $m \cdot 10 + n \cdot 27 = 1 = PMP(m, n)$.*
*Kemi $27 = 2 \cdot 10 + 7$, $10 = 1 \cdot 7 + 3$, $7 = 2 \cdot 3 + 1$.*
*Tani anasjlelltas perftojme* $1 = 7 - 2 \cdot 3 = 7 - 2(10 - 1 \cdot 7) = (1 - 2 \cdot (-1)) \cdot 7 - 2 \cdot 10 = 3 \cdot 7 + (-2) \cdot 10 = 3 \cdot (27 - 2 \cdot 10) + (-2) \cdot 10 = 3 \cdot 27 + (-8) \cdot 10$.
*Pra $m = -8$ dhe $n = 3$.*

### 8.0.1 Detyra shtepije

1. Plotesoni tabelat perkatese per mbledhjen dhe shumezimin per $m = 7$.
2. Plotesoni tabelat perkatese per mbledhjen dhe shumezimin per $m = 11$.
3. Gjeni numrat e plotë $m$ dhe $n$ ashtu që $n \cdot 30 + m \cdot 47 = 1$.
4. Gjeni numrat e plotë $m$ dhe $n$ ashtu që $n \cdot 30 + m \cdot 45 = 5$.

Le te jete $a$ dita e lindjes, dhe $b$ numri i indeksit

### 8.0.2 Detyra shtepije

1. Plotesoni tabelat perkatese per mbledhjen dhe shumezimin per $m = a \mod 7$.
2. Plotesoni tabelat perkatese per mbledhjen dhe shumezimin per $m = b \mod 7$.
3. Gjeni numrat e plotë $m$ dhe $n$ ashtu që $n \cdot a + m \cdot b = PMP(a, b)$.
4. Gjeni numrat e plotë $m$ dhe $n$ ashtu që $n \cdot a \cdot 75 + m \cdot (a + 1) \cdot 95 = 5$.