АЛГЕБРА 1

Комутативни прстени са јединицом; поља

Зоран Петровић

25. децембар 2012.

Ову лекцију започињемо дефиницијом појма комутативног прстена са јединицом.

Дефиниција 1 Комутативан прстен са јединицом је структура $(A, +, \cdot)$ за коју важи:

1. $(A, +)$ је Абелова група;
2. $(A, \cdot)$ је комунативан моноид;
3. за све $x, y, z \in A$: $x \cdot (y + z) = x \cdot y + x \cdot z$.

Неутрал у односу на сабирање означавамо са 0, или са 0_A уколико је потребно да избегнемо недоумице, док неутрал у односу на множење означавамо са 1, односно 1_A. Неутрал у односу на сабирање зове се нула, а неутрал у односу на множење јединица прстена. Како ћемо се искључиво бавити комутативним прстенима са јединицом, то ћемо, ради краткоће, понекад користити само термин прстем (подразумевајући да се ради о комутативном пстену са јединицом).

Приметимо да је производ ма ког елемента прстена и нуле једнак нули. Наиме, $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Како је прстен Абелова група у односу на сабирање, то елемент $a \cdot 0$ има инверз (у односу на сабирање) и добијамо да је $0 = a \cdot 0$. Поставља се питање: може ли у неком прстену A важити једнакост $0_A = 1_A$? Уколико је то тако и ако је $x \in A$ произвољан елемент, добијамо да је

$$x = x \cdot 1_A = x \cdot 0_A = 0_A.$$

Дакле, у том случају бисмо добили да је $A = \{0_A\}$. Такав прстен називамо и нула прстен. У даљем ћемо претпоставити да прстени са којима радимо нису нула прстени, тј. да је $0 \neq 1$ у прстену.

У произвољном прстену може се десити да је $x \cdot y = 0$, а да је и $x \neq 0$ и $y \neq 0$. На пример, у прстену $\mathbb{Z}_6$ (у коме су операције сабирање по модулу 6 и множење по модулу 6) важи: $2 \cdot 3 = 0$, а $2, 3 \neq 0$. Имамо посебан назив за такве елементе.

Дефиниција 2 Елемент a прстена A је делитељ нуле уколико постоји елемент $b \neq 0$ за који је $a \cdot b = 0$. Уколико је a делитељ нуле и $a \neq 0$, онда је a прави делитељ нуле.

Скуп свих делитеља нуле у прстену A означавамо са $Z(A)$.

Дефиниција 3 Елемент a прстена A је регуларан уколико за све $x, y \in A$ важи: ако је $a \cdot x = a \cdot y$, онда је $x = y$.

Дакле, регуларни су они елементи које можемо да „скратимо". Приметимо да је елемент регуларан ако и само ако он није делитељ нуле. Наиме, претпоставимо да је a регуларан елемент. Уколико би он био делитељ нуле, онда би следило да је $a \cdot b = 0$ за неки $b \neq 0$. Но, из једнакости $a \cdot b = a \cdot 0$ следи да је $b = 0$. С друге стране, ако a није делитељ нуле и ако је $a \cdot x = a \cdot y$, добијамо да је $a \cdot (x - y) = 0$. Из чињенице да a није делитељ нуле, следи да мора бити $x - y = 0$, те закључујемо да је a регуларан елемент.

Скуп свих регуларних елемената прстена A означавамо са $R(A)$. На основу претходне анализе, добијамо да је $A = Z(A) \sqcup R(A)$.

Дефиниција 4 Елемент a прстена A је инвертибилан уколико постоји елемент $b \in A$ за који је $a \cdot b = 1$.

Уколико је a инвертибилан, онда је елемент b за који важи $a \cdot b = 1$ јединствено одређен (зашто?) и означавамо га са a^{-1}. Скуп свих инвертибилних елемената прстена A означавамо са $U(A)$. Јасно је да је $(U(A), \cdot)$ једна Абелова група. Зовемо је мултипликативна група прстена. Приметимо да је $U(A) \subseteq R(A)$. Наиме, ако је $a \in U(A)$ и $a \cdot x = a \cdot y$, онда је $a^{-1} \cdot a \cdot x = a^{-1} \cdot a \cdot y$, па је $1 \cdot x = 1 \cdot y$, те је $x = y$.

У општем случају је $R(A) \neq U(A)$. На пример, $R(\mathbb{Z}) = \mathbb{Z} \setminus \{0\}$, док је $U(\mathbb{Z}) = \{-1, 1\}$. Но, занимљив је следећи став.

Став 5 У коначном прстену сваки регуларан елемент је инвертибилан.

Доказ. Нека је прстен A коначан и $a \in R(A)$. Дефинишимо $L_a \colon A \to A$ са: $L_a(x) := a \cdot x$. Из регуларности елемента a следи да је L_a „1–1". Наиме, ако је $L_a(x) = L_a(y)$, то значи да је $a \cdot x = a \cdot y$, а како је a регуларан, добијамо да је $x = y$. Како је A коначан, из чињенице да је $L_a \colon A \to A$ „1–1" следи да је L_a и „на". Стога постоји $b \in A$ за које је $L_a(b) = 1$, тј. $a \cdot b = 1$, те закључујемо да је a инвертибилан. □

Дефиниција 6 Комутативан прстен са јединицом A је домен, ако он не садржи праве делитеље нуле, тј. ако је $Z(A) = \{0\}$. Комутативан прстен са јединицом A је поље уколико је сваки ненула елемент у A инвертибилан, тј. ако је $U(A) = A \setminus \{0\}$.

Очигледно је да је свако поље и домен, док као последицу претходног става добијамо да је сваки коначан домен и поље. Наравно, у општем

случају та два појма се не поклапају. На пример, $\mathbb{Z}$ јесте домен, али није поље. У наредном курсу видећемо како се сваком домену може придружити једно поље, али то остаје за касније.

Приметимо да је $U(\mathbb{Z}_n) = \Phi(n)$ и да је $\mathbb{Z}_n$ поље ако и само ако је n прост број (уверите се да је то заиста тако!).

Пређимо сада на појам потпрстена.

Дефиниција 7 Нека су $(A, +_A, \cdot_A)$ и $(B, +_b, \cdot_B)$ два комутативна прстена са јединицом при чему је $B \subseteq A$. Кажемо да је B потпрстен са јединицом прстена A уколико је B уколико је

1. за све $x, y \in B$: $x +_B y = x +_A y$;
2. за све $x, y \in B$: $x \cdot_B y = x \cdot_A y$;
3. $1_B = 1_A$.

Добро нам је познато (зар не?) да из првог услова следи да је $0_B = 0_A$. Но, морамо додати услов да је $1_B = 1_A$. Наиме, то не следи из претходна два услова, као што следећи пример јасно показује.

Пример 8 Нека је $A = \{(0,0), (0,1), (1,0), (1,1)\}$, $B = \{(0,0), (1,0)\}$, а операције су дефинисане по координатама, користећи сабирање и множење по модулу 2. Прецизније:

$$(a, b) + (c, d) := (a +_2 c, b +_2 d);$$

$$(a, b) \cdot (c, d) := (a \cdot_2 c, b \cdot_2 d);$$

Операције на B су рестрикције операција на A. Тада су и A и B комутативни прстени са јединицом, но, док је $0_A = (0,0) = 0_B$, то је $1_A = (1,1) \neq (1,0) = 1_B$. □

Размотримо сада директан производ прстена.

Дефиниција 9 Нека су $(A_1, +^1, \cdot^1), (A_1, +^2, \cdot^2) \ldots, (A_n, +^n, \cdot^n)$ комутативни прстени са јединицом. На скупу $A = A_1 \times A_2 \times \cdots \times A_n$ дефинишемо структуру $(A, +, \cdot)$ са:

$$\begin{aligned}(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) &:= (x_1 +^1 y_1, x_2 +^2 y_2, \ldots, x_n +^n y_n)\\ (x_1, x_2, \ldots, x_n) \cdot (y_1, y_2, \ldots, y_n) &:= (x_1 \cdot^1 y_1, x_2 \cdot^2 y_2, \ldots, x_n \cdot^n y_n)\end{aligned}$$

Ова структура јесте комутативан прстен са јединицом и представља директан производ прстена $A_1, \ldots, A_n$. Приметимо да је $0_A = (0_{A_1}, \ldots, 0_{A_n})$ и $1_A = (1_{A_1}, \ldots, 1_{A_n})$. Уколико имамо бар два фактора у производу, у њему увек има правих делитеља нуле: $(0_{A_1}, \ldots, 1_{A_n}) \cdot (1_{A_1}, \ldots, 0_{A_n}) = 0_A$. Како у пољу нема правих делитеља нуле (зашто?) закључујемо да производ бар два комутативна прстена са јединицом (чак и ако су сви фактори поља) не може бити поље.

Следећи став утврђује структуру мултипликативне групе директног производа прстена.

Став 10 Ако је $A = A_1 \times \cdots \times A_n$, онда је $U(A) = U(A_1) \times \cdots \times U(A_n)$.

Доказ. Ово није тешко показати.

$\subseteq$: Нека је $a \in U(A)$. То значи да постоји $b \in A$ такав да је $a \cdot b = 1_A$. Другим речима, ако је $a = (a_1, \ldots, a_n)$, онда постоје $b_i \in A_i$ такви да је

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (1_{A_1}, \ldots, 1_{A_n}).$$

Но, ова једнакост је еквивалентна са: $a_i \cdot^i b_i = 1_{A_i}$ за $i = \overline{1,n}$. То управо значи да $a_i \in U(A_i)$ за $i = \overline{1,n}$, тј. $a \in U(A_1) \times \cdots \times U(A_n)$.

$\supseteq$: Нека $a \in U(A_1) \times \cdots \times U(A_n)$. Дакле, $a = (a_1, \ldots, a_n) \in U(A_1) \times \cdots \times U(A_n)$. Према томе, $a_i \in U(A_i)$ за $i = \overline{1,n}$, па постоје $b_i \in A_i$ такви да је $a_i \cdot^i b_i = 1_{A_i}$, за $i = \overline{1,n}$. Но, одатле следи да за елемент $b - (b_1, \ldots, b_n) \in A$ важи: $a \cdot b = 1_A$, те закључујемо да $a \in U(A)$. □

Став 11 Уколико је $(A, +_A, \cdot_A) \cong (B, +_B, \cdot_B)$, онда је $(U(A), \cdot_A) \cong (U(B), \cdot_B)$.

Доказ. Нека је $f\colon A \to B$ изоморфизам прстена. Доказаћемо да је $f[U(A)] = U(B)$. Одатле следи да рестрикција f на $U(A)$ индукује тражени изоморфизам мултипликативних група датих прстена.

$\subseteq$: Нека је $a \in U(A)$. То значи да постоји $a_1 \in A$ тако да је $a \cdot_A a_1 = 1_A$. Но, тада је $f(a \cdot_A a_1) = f(1_A)$, па је $f(a) \cdot_B f(a_1) = 1_B$. Дакле, $f(a) \in U(B)$.

$\supseteq$: Нека $b \in U(B)$. То значи да постоји $b_1 \in B$ тако да је $b \cdot_B b_1 = 1_B$. Како је f „на", постоје a, a_1 за које је $f(a) = b$ и $f(a_1) = b_1$. Тако добијамо

$$f(1_A) = 1_B = b \cdot_B b_1 = f(a) \cdot_B f(a_1) = f(a \cdot_A a_1).$$

С обзиром на то да је f и „1–1", следи да је $1_A = a \cdot_A a_1$, тј. $a \in U(A)$, па $b \in f[U(A)]$. □

Пређимо на неке конкренте примере прстена. Претходни појмови и резултати даће нам, уз мало рада, неке резултате из елементарне теорије бројева.

Теорема 12 Нека су $m_1, m_2, \ldots, m_n \geqslant 2$ цели бројеви за које је испуњено: $\mathrm{NZD}(m_i, m_j) = 1$ за $i \neq j$. Тада су прстени $\mathbb{Z}_{m_1 m 2 \cdots m_n}$ и $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ изоморфни.

Доказ. Нека је $m = m_1 m_2 \cdots m_n$. Приметимо да оба прстена имају m елемената. Стога је, за доказ постојања изоморфизма, довољно конструисати једну „1–1" функцију из једног у други, која се слаже са операцијама, јер ће та функција сигурно бити и „на", тј. изоморфизам (то су коначни скупови са истим бројем елемената). Ако са $\rho_k(x)$ означимо остатак при (еуклидском) дељењу x са k, онда је тражена функција $f\colon \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ дефинисана са:

$$f(x) := (\rho_{m_1}(x), \rho_{m_2}(x), \ldots, \rho_{m_n}(x)).$$

Докажимо да је f „1–1”. Нека је $f(x) = f(y)$. То значи да за $i = \overline{1,n}$ важи: $\rho_{m_i}(x) = \rho_{m_i}(y)$. Но, ако два броја имају исти остатак при дељењу бројем m_i, онда је њихова разлика дељива са m_i. Дакле, за $i = \overline{1,n}$ важи: $m_i \mid (x-y)$. Како су бројеви m_i узајамно прости, следи да $m \mid (x-y)$. С обзиром да $x, y \in Z_m = \{0, 1, \ldots, m-1\}$, добијамо да је $x - y = 0$, тј. $x = y$.

Докажимо да се f слаже са операцијама, тј. да је за све $x, y \in Z_m$: $f(x +_m y) = f(x) + f(y)$ и $f(x \cdot_m y) = f(x) \cdot f(y)$ (где је са $+$, односно $\cdot$ означена операција у директном производу, за коју знамо како се дефинише). Доказаћемо то за операцију множења, док сличан доказ за сабирање остављамо за вежбу.

Дакле, треба доказати да је $f(x \cdot_m y) = f(x) \cdot f(y)$ за све $x, y \in Z_m$. С обзиром на дефиницију функције f и дефиницију операције $\cdot$, ово се своди на доказ чињенице да је за све $i = \overline{1,n}$ испуњено:

$$\rho_{m_i}(x \cdot_m y) = \rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y).$$

Доказ ћемо извести тако што ћемо показати да су и лева и десна страна ове једнакости заправо остаци при дељењу $x \cdot y$ са m (где је овде $\cdot$ операција множења целих бројева). Наиме, по дефиницији операције $\cdot_m$ имамо да је

$$x \cdot y \equiv x \cdot_m y \,(\mathrm{mod}\ m).$$

Приметимо да важи следеће: ако је $a \equiv b \,(\mathrm{mod}\ m)$ и ако $k \mid m$, онда је и $a \equiv b \,(\mathrm{mod}\ k)$. Наиме, $a \equiv b \,(\mathrm{mod}\ m)$ је еквивалентно са $m \mid (a-b)$. Како $k \mid m$, то следи да је и $k \mid (a-b)$, што је, пак, еквивалентно са $a \equiv b \,(\mathrm{mod}\ k)$. Стога, из

$$x \cdot y \equiv x \cdot_m y \,(\mathrm{mod}\ m),$$

следи да за све $i = \overline{1,n}$ важи:

$$x \cdot y \equiv x \cdot_m y \,(\mathrm{mod}\ m_i).$$

С обзиром да је

$$x \equiv \rho_k(x) \,(\mathrm{mod}\ k),$$

добијамо да је

$$x \cdot_m y \equiv \rho_{m_i}(x \cdot_m y) \,(\mathrm{mod}\ m_i),$$

те, напокон, добијамо да је

$$x \cdot y \equiv \rho_{m_i}(x \cdot_m y) \,(\mathrm{mod}\ m_i).$$

С обзиром да је $\rho_{m_i}(x \cdot_m y) \in Z_{m_i}$, следи да је тај број заправо остатак при дељењу $x \cdot y$ са m_i.

Како је $x \equiv \rho_{m_i}(x) \,(\mathrm{mod}\ m_i)$ и $y \equiv \rho_{m_i}(y) \,(\mathrm{mod}\ m_i)$, то је

$$\rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) \equiv x \cdot_{m_i} y \,(\mathrm{mod}\ m_i).$$

Но,

$$x \cdot_{m_i} y \equiv x \cdot y \,(\mathrm{mod}\ m_i),$$

те је и

$$x \cdot y \equiv \rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) \,(\mathrm{mod}\ m_i).$$

С обзиром да $\rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) \in \{0, \ldots, m_i - 1\}$, следи да је $\rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) \in \{0, \ldots, m_i - 1\}$ остатак при дељењу $x \cdot y$ са m_i. Закључујемо да мора бити

$$\rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) = \rho_{m_i}(x \cdot_m y),$$

јер је и један и други број остатак при дељењу $x \cdot y$ са m_i. □

Последица 13 (Кинеска теорема о остацима) Нека су $m_1, m_2, \ldots, m_n \geqslant 2$ цели бројеви за које је $\mathrm{NZD}(m_i, m_j) = 1$ за $i \neq j$. Тада за произвољне $x_i \in \mathbb{Z}$, $i = \overline{1,n}$, систем конгруенција

$$\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ x &\equiv x_2 \pmod{m_2} \\ &\vdots \\ x &\equiv x_n \pmod{m_n} \end{aligned} \tag{1}$$

има јединствено решење по модулу $m_1 m_2 \cdots m_n$.

Доказ. Функција f, дефинисана у претходној теореми, је изоморфизам. Ми ћемо искористити чињеницу да је она „на". Нека су $x_1, x_2, \ldots, x_n \in \mathbb{Z}$. Са r_i означимо остатак при дељењу броја x_i са m_i. Јасно је да тада важи $x_i \equiv r_i \,(\mathrm{mod}\ m_i)$, за $i = \overline{1,n}$. Формирајмо n-торку $(r_1, r_2, \ldots, r_n) \in Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_n}$. Како је f „на", то постоји $x \in Z_m$ (где је $m = m_1 m_2 \cdots m_n$) за које је $f(x) = (r_1, r_2, \ldots, r_n)$. Но, с обзиром на дефиницију f, то заправо значи да је $x \equiv r_i \,(\mathrm{mod}\ m_i)$ за $i = \overline{1,n}$ (уверите се да је то заиста тако!), те је и $x \equiv x_i \,(\mathrm{mod}\ m_i)$ за $i = \overline{1,n}$. Дакле, систем конгруенција има решење. Проверимо и јединственост решења. Нека је $x' \in \mathbb{Z}$ неки други цео број за који је $x' \equiv x_i \,(\mathrm{mod}\ m_i)$ за $i = \overline{1,n}$. Добијамо да је $x \equiv x' \,(\mathrm{mod}\ m_i)$ за $i = \overline{1,n}$. То значи да $m_i \mid (x - x')$ за $i = \overline{1,n}$. Како су m_i узајамно прости то даје: $m \mid (x - x')$, те је решење заиста јединствено по модулу m (јединственост решења следи и из чињенице да је f „1–1" – проверите како следи). □

Последица 14 Ако су $m_1, m_2, \ldots, m_n$ цели бројеви за које је $\mathrm{NZD}(m_i, m_j) = 1$, за $i \neq j$, онда је $\varphi(m_1 m_2 \cdots m_n) = \varphi(m_1)\varphi(m_2) \cdots \varphi(m_n)$.

Доказ. На основу претпоставки из доказане теореме следи да важи изоморфизам прстена $\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$. На основу става 11 и става 10 добијамо да је $U(\mathbb{Z}_m) \cong U(\mathbb{Z}_{m_1}) \times \cdots \times U(Z_{m_n})$. С обзиром да је $U(\mathbb{Z}_k) = \Phi(k)$ и да је $\varphi(k) = |\Phi(k)|$, тражени резултат следи (уверите се у то!). □

Као што знамо, уколико је F поље, онда је $U(F) = F \setminus \{0\}$. Поље наравно може бити и коначно и бесконачно, те и $U(F)$ може бити коначна и бесконачна. Оно што је занимљиво је да имамо врло једноставан опис за коначне подгрупе групе $U(F)$. Најпре докажимо један помоћни став.

Став 15 Нека је A Абелова група реда m и нека је за сваки позитиван цео број d такав да $d \mid m$ број решења једначине $dx = 0$ у групи A највише d, тј.

$$|\{x \in A : dx = 0\}| \leqslant d. \qquad (*)$$

Тада је група A циклична.

Доказ. На основу теореме о карактеризацији коначних Абелових група, $A \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k}$ за неко $k \geqslant 1$, при чему је $d_1 > 1$ и $d_i \mid d_{i+1}$ за $i = \overline{1, k-1}$. Да бисмо доказали да је A циклична довољно је (а и потребно) да докажемо да је $k = 1$. На основу раније леме о броју решења једначине $d_1 x = 0$ у оваквом производу, знамо да је тај број једнак $\mathrm{NZD}(d_1, d_1) \cdot \mathrm{NZD}(d_1, d_2) \cdots \mathrm{NZD}(d_1, d_k) = d_1^k$. Но, на основу услова $(*)$, тај број не сме бити већи од d_1, те мора бити $k = 1$. □

Теорема 16 Нека је F поље и $(A, \cdot)$ коначна подгрупа групе $(U(F), \cdot)$. Тада је A циклична група.

Доказ. Нека је ред групе A једнак m и нека $d \mid m$. Како је група A задата мултипликативно, то ћемо у примени претходног става користити мултипликативан запис. Да бисмо доказали да је A циклична, довољно је да докажемо да је

$$\left|\{a \in A : a^d = 1\}\right| \leqslant d.$$

Но, свако решење једначине $a^d = 1$ у пољу F је заправо нула полинома $p(X) = X^d - 1 \in F[X]$. Сада можемо искористити добро познату чињеницу да ненула полином са коефицијентима у пољу не може имати више нула него што је његов степен. С обзиром да је степен овог полинома једнак d, важи тражена неједнакост и резултат следи. □

Како је $\mathbb{Z}_p$ поље уколико је p прост број, то је група $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ циклична група реда $p-1$. На основу јединствености (до на изоморфизам) цикличних група датог реда следи да је ова група изоморфна групи $(\mathbb{Z}_{p-1}, +_{p-1})$. Но, занимљиво је (и корисно) експлицитније задати тај изоморфизам. У ту сврху уводимо следећу дефиницију.

Дефиниција 17 Ма који генератор цикличне групе $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ назива се примитивни корен по модулу p.

Читалац се може запитати „примитивни корен из чега?" Заправо је то примитивни корен из јединице (јер у $\mathbb{Z}_p$ важи: $x^p = 1$ за све $x \in Z_p$). Ово је повезано са „обичним" коренима из јединице (у пољу $\mathbb{C}$) – подсетите се примера групе $\mathbb{C}_n$ са почетка курса!

Став 18 Нека је p прост број и r ма који примитиван корен из јединице по модулу p. Тада је са:

$$\mathrm{ind}_r(a) = x \textbf{ акко } r^x = a,$$

дефинисан један изоморфизам $\mathrm{ind}_r\colon (\mathbb{Z}_p \setminus \{0\}, \cdot_p) \to (\mathbb{Z}_{p-1}, +_{p-1})$.

(Тешко је не приметити сличност са дефиницијом логаритма за основу r, зар не?)

Доказ. Како је $\mathbb{Z}_p \setminus \{0\} = \langle r\rangle = \{r^0, r^1, \ldots, r^{p-2}\}$, то је јасно да је ind_r једна бијекција. Треба показати да се слаже са операцијама, тј. да је

$$\mathrm{ind}_r(a \cdot_p b) = \mathrm{ind}_r +_{p-1} \mathrm{ind}_r(b),$$

за све $a, b \in Z_p$. У ту сврху, нека је $\mathrm{ind}_r(a) = x$ и $\mathrm{ind}_r(b) = y$. То значи да је $r^x = a$ и $r^y = b$. Дакле,

$$a \cdot_p b = r^x \cdot_p r^y = r^{x+y}.$$

С обзиром да је $r^{p-1} = 1$ у групи $\mathbb{Z}_p$, то је и

$$r^{x+y} = r^{x+_{p-1}y}$$

($x + y$ и $x +_{p-1} y$ разликују за умножак броја $p - 1$). Стога је

$$a \cdot_p b = r^{x+_{p-1}y}.$$

На основу дефиниције ind_r, добијамо да је $x +_{p-1} y = \mathrm{ind}_r(a \cdot_p b)$. Ако се подсетимо шта су x и y, добијамо да је заиста $\mathrm{ind}_r(a) +_{p-1} \mathrm{ind}_r(b) = \mathrm{ind}_r(a \cdot_p b)$, што се и тражило. □

Погледајмо један пример примене примивних корена.

Пример 19 а) Наћи све примитивне корене по модулу 13.
б) Решити конгруенцију $x^5 \equiv 7 \pmod{13}$.

Решење. а) Метод је једноставан. Директном провером нађимо један примитивни корен. Нека је то r. Тада су сви остали примитивни корени једнаки r^x, где је x узајамно прост са 12 (мултипликативна група је реда 12, њен генератор је r – подсетите се реда елемента r^x).

У овом случају, директном провером добијамо да је један примитивни корен једнак 2 (рачунамо у $\mathbb{Z}_{13}$):

$$\begin{aligned} 2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 8 \\ 2^4 &= 3 \\ 2^5 &= 6 \\ 2^6 &= 12 \end{aligned}$$

$$\begin{aligned} 2^7 &= 11 \\ 2^8 &= 5 \\ 2^{10} &= 10 \\ 2^{11} &= 7 \\ 2^{12} &= 1. \end{aligned}$$

Дакле, примитивни корени су још и $2^5 = 6$, $2^7 = 11$ и $2^{11} = 7$. Због примене на решавање конгруенција, погодно је направити и следећу табелу.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_r(a)$	0	1	4	2	9	5	11	3	8	10	7	6

б) Нека је $\overline{x}$ остатак при дељењу x са 13 и $y = \mathrm{ind}_2(\overline{x})$. Тада се

$$x^5 \equiv 7 \,(\mathrm{mod}\ 13)$$

своди на

$$5y \equiv \mathrm{ind}_2(7) \,(\mathrm{mod}\ 12),$$

$(x^5 \equiv \overline{x}^5 \,(\mathrm{mod}\ 13))$, тј. на

$$5y \equiv 11 \,(\mathrm{mod}\ 12).$$

С обзиром да је $5 \cdot 5 \equiv 1 \,(\mathrm{mod}\ 12)$ и да је $55 \equiv 7 \,(\mathrm{mod}\ 12)$, добијамо да је $y = 7$ $(y \in \mathbb{Z}_{12})$. С обзиром да из $\mathrm{ind}_2(\overline{x}) = 7$ следи да је $\overline{x} = 11$ (погледајте таблицу), добијамо и тражено решење: $x \equiv 11 \,(\mathrm{mod}\ 13)$ ♣

За сам крај курса оставили смо једну познату теорему из елементарне теорије бројева.

Теорема 20 *(*Вилсонова теорема*)* Нека је p прост број. Тада је

$$(p-1)! \equiv -1 \,(\mathrm{mod}\ p).$$

Доказ. Ако је $p = 2$, све је јасно. Претпоставимо да је p непаран прост број. Уочимо полином $q(X) = X^{p-1} - 1 \in \mathbb{Z}_p[X]$. То је полином степена $p-1$ и у пољу он може имати највише $p-1$ различиту нулу. С обзиром да је за све $a \in \{1, \ldots, p-1\}$: $a^{p-1} \equiv 1 \,(\mathrm{mod}\ p)$, то су све нуле полинома $q(X)$ заправо $1, 2, \ldots, p-1$ (из поља $\mathbb{Z}_p$). Стога је

$$q(X) = (X-1)(X-2)\cdots(X-(p-1)).$$

Добијамо да је

$$q(0) = (0-1)(0-2)\cdots(0-(p-1)),$$

односно

$$-1 = (-1)(-2)\cdots(-(p-1)),$$

у пољу $\mathbb{Z}_p$. Преласком на целе бројеве добијамо да је

$$-1 \equiv (-1)(-2)\cdots(-(p-1)) \,(\mathrm{mod}\ p),$$

тј.

$$-1 \equiv (-1)^{p-1} 1 \cdot 2 \cdots (p-1) \,(\mathrm{mod}\ p),$$

С обзиром да је p непаран, добијамо да је

$$-1 \equiv (p-1)! \,(\mathrm{mod}\ p),$$

што је и тражено. □