Универзитет у Београду

Математички факултет

Мастер рад

Тема:

Факторизација бројева и полинома у школском програму математике

Ментор:

др Александар Липковски

Студент:

Маја Ђорђевић

Београд, 2020.

Садржај

Предговор

Факторизација бројева и полинома представља важан садржај у школском програму математике. У овом мастер раду је описана факторизација природних бројева у нижим разредима основне школе, описани су прости бројеви и њихова факторизација у старијим разредима основне школе, затим факторизација полинома у средњој школи и поменута је општа алгебарска теорија факторизације.

Рад се састоји из четири поглавља.

У првом поглављу је прича о парним и непарним бројевима и дељењу са остатком.

У другом поглављу обрађују се прости и сложени бројеви и даје се предлог како ученике основне школе на редовној настави увести у свет ових бројева. Дати су и решени задаци за додатни рад који могу послужити као припрема за такмичење.

Треће поглавље је посвећено операцијама са полиномима: сабирању, одузимању и множењу полинома као и разлици квадрата и квадрату бинома. Посебна пажња се посвећује растављању полинома на чиниоце.

У последњем поглављу говори се о прстенима са једнозначном факторизацијом, као и о Еуклидским прстенима.

Овом приликом бих се захвалила свом ментору др Александру Липковском, на подршци и корисним саветима приликом израде овог мастер рада.

1. ПОЈАМ ФАКТОРИЗАЦИЈЕ

Факторизација у математици је разлагање неког објекта (на пример, броја,полинома, или матрице) на факторе, који када се међусобно помноже дају ориганал.

На пример, број 21 факторишемо на просте бројеве 3×7, а полином $x^2 - 1$ на

$(x - 1)(x + 1)$. У сваком случају је добијен једноставнији облик.

Циљ факторисања је обично, поједностављење нечега на "његове полазне елементе", као што су за бројеве, прости бројеви, или за полиноме нерастављиви полиноми.. Факторисање целих бројева покривено је у оквиру основне теореме аритметике и факторисање полинома у оквиру основне теореме алгебре. Вијетове формуле везују коефицијенте полинома са њиховим коренима.

Растављање на факторе за велике бројеве се испоставило као велики проблем. Не постоји позната метода која би могла да изврши то за кратко време. Њена сложеност је основа заштите неких асиметрично криптографских алгоритама, као што је RSA алгоритам.

Матрица може такође бити факторисана у продукт специјалних типова матрица.

Још један пример је фаткорисање функција као композиције других функција које имају одређене особине; на пример, свака функција се може посматрати као композиција сурјективне функције са неком инјективном функцијом.

1.1. ФАКТОРИЗАЦИЈА ПРИРОДНИХ БРОЈЕВА

Прво математичко знање које стичемо је знање о природним бројевима. У току школовања, у основној и средњој школи, стечено знање не подвргавамо критици. Радимо са неким конкретним природним бројевима, испитујемо својства која имају и приписујемо их свим природним бројевима. Уверени смо да можемо сабрати и помножити било која два природна броја, да за сабирање и множење важе комутативни и асоцијативни закон и слично.

Природни бројеви су познат објекат $\mathbb{N} = \{1, 2, 3, \dots\}$. Интуитивно се подразумева да иза сваког броја следи број, те да се набрајање може одвијати без ограничења.

У математици је пребројив скуп онај чија је кардиналност (тј. број елемената) једнака кардиналности неког подскупа скупа природних бројева. Овај термин потиче из чињенице да за бројање користимо природне бројеве. Скуп који није пребројив, називамо непребројив скуп. Под пребројивим скуповима најчешће се подразумевају и коначни скупови, па зато када желимо да нагласимо да је скуп бесконачан и пребројив, називамо га пребројиво бесконачан скуп. Пребројиве скупове можемо замислити као неки скуп чије елементе можемо поређати у низ. Дакле, пребројиве скупове можемо преуредити тако да имамо тачно један први елемент, тачно један други, тачно један трећи итд. Као код природних бројева $\{1, 2, 3, \dots\}$. Приметимо, како и бесконачни скупови могу бити пребројиви, да не захтевамо да се може одредити (коначан) број елемената, само треба да сваком броју можемо рећи који је он у низу елемената тог скупа.

Највећи природан број не постоји. Сваки непразан подскуп скупа природних бројева има најмањи елемент.

Збир и производ природних бројева је природан број, док разлика и количник не морају бити, што доводи у шестом разреду до проширења скупа природних бројева и увођење скупа целих бројева.

1.2. ДЕЉЕЊЕ СА ОСТАТКОМ

Дефиниција: Нека су a и b произвољни природни бројеви. Највећи број q такав да је $qb \leq a$ назива се количник при дељењу a са b. Разлика $a - qb$ назива се остатак при дељењу a са b.

Остатак при дељењу неког броја са 2 може бити једнак 0 или 1. У зависности од тога бројеве из скупа N_0 делимо на парне и непарне.

Парни су они који при дељењу са 2 дају остатак 0. Сваки паран број се може записати у облику $2q$, за неки број q из N_0.

Непарни су они који при дељењу са 2 дају остатак 1. Сваки непаран број се може записати у облику $2q + 1$, за неки број q из N_0.

Ако је $n > 1$, остаци при дељењу бројева из N_0 саn припадају скупу $\{0, 1, 2, \dots, n - 1\}$.

Пример: Колико има бројева у првој стотини који при дељењу са 5 дају остатак 2?

Решење: Највећи број прве стотине који при дељењу са 5 даје остатак 2 јесте 97, 97= 19*5+2.

Сви бројеви прве стотине који при дељењу са 5 дају отатак 2 јесу облика $5q + 2$, када је $0 \leq q \leq 19$:

$5 * 0 + 2, 5 * 1 + 2, 5 * 2 + 2, 5 * 3 + 2, \dots, 5 * 19 + 2.$

Дакле, постоји 20 бројева прве стотине који при дељењу са 5 дају остатак 2.

1.3. ДЕЉИВОСТ ПРИРОДНИХ БРОЈЕВА

Ако је остатак при дељењу броја a са b $(b \neq 0)$ једнак нули, кажемо да се a може поделити са b без остатка.

Дефиниција: Број a из N_0 је дељив природним бројем b ако постоји q из N_0 такав да је $a = qb$. Кажемо и да b дели број a, односно, a је дељиво са b, и пишемо $b|a$.

Дељивост је релација међу бројевима која се односи на могућност да се један број подели другим без остатка.

$$b|a \leftrightarrow a = b * q, \text{за неко } q \text{ из } N_0.$$

Дељење је рачунска операција, што значи да $a:b$ представља израз, или терм. Када a и b заменимо бројевима, вредност израза може бити неки број, а може бити и недефинисана (на пример, за b=0). Дељивост је релација, што значи да $b|a$ представља исказ. Када a и b заменимо бројевима, овај исказ постаје тачан или нетачан.

1.4. ДЕЛИОЦИ И САДРЖАОЦИ ПРИРОДНИХ БРОЈЕВА

Ако $b|a$, онда је b делилац броја a, а број a је садржалац броја b.

Скуп свих делилаца броја n означавамо са D_n. Очигледно, број 1 је делилац било ког природног броја n, $1 \mid n$. Такође, сваки број n је сопствени делилац, $n \mid n$.

За сваки природан број n, скуп D_n је коначан, јер ако $d \mid n$, онда је $d \leq n$. Најмањи делилац било ког природног броја n јесте 1, а највећи његов делилац јесте сам n.

Пример: Одреди скупове D_8 и D_9.

Решење. $D_8 = \{1, 2, 4, 8\}$, $D_9 = \{1, 3, 9\}$

Број 0 је садржалац сваког природног броја n, јер је $0 = n * 0$.

Скуп свих природних садржалаца броја n означавамо са S_n.

За сваки природан број n, скуп S_n је бесконачан. Најмањи природни садржалац било ког природног броја n јесте n, а највећи његов садржалац не постоји.

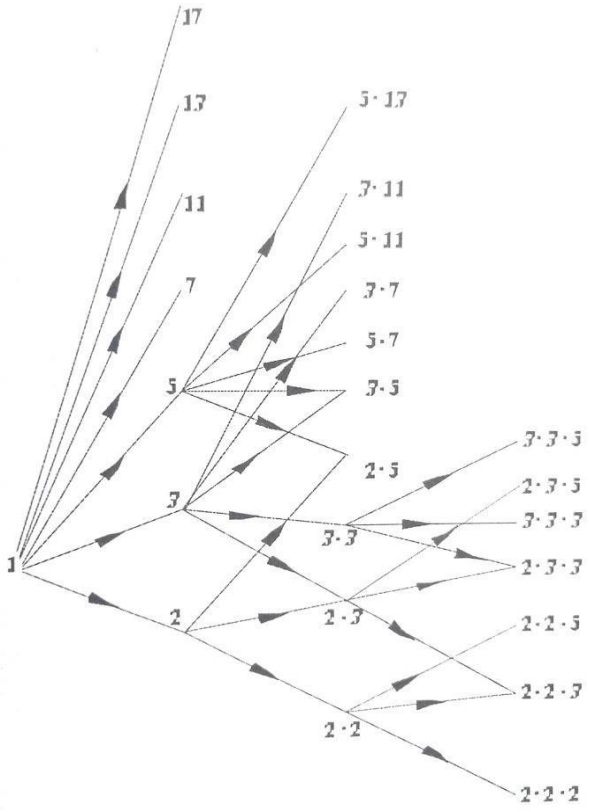
Пример: Напиши бар шест садржалаца броја 6.

Решење: Садржаоци броја 6 су 6, 12, 18, 24, 30, 36 итд. Број 6 има бесконачно много садржалаца који су природни бројеви. То су сви бројеви облика $6q$, за неко $q \in N$.

$$S_6 = \{6, 12, 18, 24, 30, 36, \dots\}$$

2. ПРОСТИ И СЛОЖЕНИ БРОЈЕВИ

Полазну основу читавог развоја математике чини појам природног броја. Приликом разматрања природних бројева примећујемо да међу њима постоје бројеви са веома разноврсним особинама. Осим њиховог природног поретка по величини, релацијом ≤, који је потпун и бројеви се нижу линеарно $1 \leq 2 \leq 3$ ... може се уочити и природни поредак по релацији дељивости. Тај поредак није потпун и њиме се скуп природних бројева преплиће у мрежу. На слици је приказана мрежа за првих 25 природних бројева.



Осим природних бројева, постоје и друге врсте бројева, па ћемо поменути и такозване негативне бројеве тј. бројеве који су за неки природан број мањи од нуле. Њих записујемо тако што испред записа одговарајућег природног броја додамо и знак минус. Дакле, негативне целе бројеве схватамо и као разлике броја нула и неког природног броја, па можемо замишљати да је ознака негативног броја добијена изостављањем нуле из одговарајуће разлике:

0-1=-1, 0-2=-2, 0-3=-3, 0-4=-4, 0-5=-5,...

Како природних бројева има бесконачно много, и негативних целих бројева има бесконачно много.

Сви природни бројеви заједно са нулом и свим негативни целим бројевима образују скуп целих бројева који обележавамо Z. Скуп негативних целих бројева бележава се Z^{-}.

$$\mathrm{Z}^{-} = \{-1, -2, -3, -4, -5, -6, \dots\}$$

$$\mathrm{Z} = \mathrm{Z}^{-} \cup \{0\} \cup N = Z^{-} \cup N_0 = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$$

Када природне бројеве посматрамо у скупу целих бројева, називамо их и позитивним целим бројевима или бројевима позитивног знака.Број нула није ни негативан ни позитиван број. Дакле, нула и сви природни бројеви нису негативни цели бројеви, па их називамо ненегативним целим бројевима.

У вези са овим, скуп целих бројева можемо поделити на 3 дела: просте бројеве, сложене бројеве и бројеве који нису ни прости ни сложени.

Дефиниција: 1) Цео број p је прост ако не припада скупу {-1, 0, 1} и делитељи су му само -1, 1, p и $-p$.

2) Цео број који је различит од -1, 1 и 0, и није прост, јесте сложен.

3) Бројеви 0, 1 и -1 нису ни прости ни сложени.

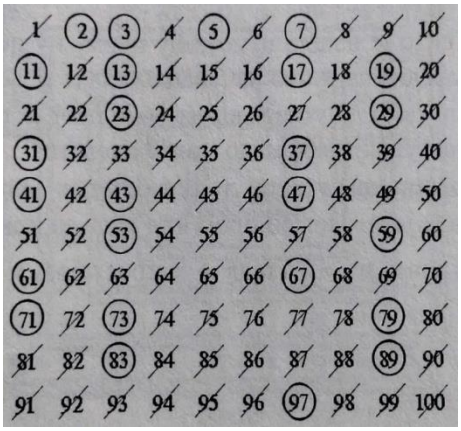
Проблем добијања потпуне листе простих бројева мањих од датог броја n заокупљао је пажњу математичара вековима. Један поступак за утврђивање простоте датог броја и налажење свих простих бројева мањих од датог броја n дао је старогрчки математичар Ератостен.

Најлакши начин да се овај низ настави је метод познат као **Ератостеново сито** (решето): ако желимо да нађемо све просте бројеве мање од n, прво треба да испишемо све природне бројеве од 2 до $n - 1$ и да редом из списка елиминишемо (прецртамо) све парне бројеве изузев броја 2, затим све бројеве дељиве са 3, изузев самог броја 3, затим слично са 5, 7 итд.све до последњег природног броја мањег од $\sqrt{n}$. Приметимо да после елиминације парних бројева није више потребно тражити бројеве дељиве са 4, 6, 8 итд. јер су сви ти бројеви парни. Слично, после елиминације бројева дељивих са 3 није више потребно тражити бројеве дељиве са 6, 9 итд. Дакле, да бисмо одредили просте бројеве мање од n, користимо просте бројеве мање од $\sqrt{n}$.

Пример : Да бисмо помоћу Ератостеновог сита одредили све просте бројеве мање од 100, треба редом да елиминишемо све бројеве дељиве са 2,

3, 5 и 7 ($\sqrt{100}$ = 10 а 7 је највећи прост број мањи од 10).

На тај начин добијамо 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67,71, 73, 79, 83, 89, 97, укупно 25 простих бројева мањих од 100. Ератостенов алгоритам је у том случају приказан на слици.



Ератостеново сито

Није тешко закључити да, чим смо нашли први прост број који прелази $\sqrt{n}$, остали су нам непрецртани само прости бројеви. Ово тврдимо на основу следеће теореме:

Теорема:

Цео број $n > 0$ је сложен ако и само ако је дељив простим бројем p, таквим да је $p \leq \sqrt{n}$.

Доказ:

($\Leftarrow$) Ако је n дељив простим бројем $p \leq \sqrt{n}$,
онда је n очигледно сложен број.

($\Rightarrow$) Ако је p најмањи прост делитељ сложеног броја n, тада је $n = pk$, за неки цео број k, и при томе је $k \geq p$. Тада је $n \geq p * p$, односно $p \leq \sqrt{n}$.

Закон контрапозиције нам омогућава да претходно тврђење формулишемо и на следећи начин:

Последица:

Цео број $n > 1$ је прост ако и само ако није дељив простим бројем $p \leq \sqrt{n}$

2.1. ОСНОВНА ТЕОРЕМА АРИТМЕТИКЕ

У овом одељку доказаћемо да се сваки позитиван цео број може представити у облику производа простих фактора и да је такво представљање јединствено до на поредак фактора.

Теорема :

Ако је n цео број већи од 1, онда је n производ простих фактора.

Доказ:

Ако је n прост број, тврђење очигледно важи. Претпоставимо да тврђење важи за сваки сложен број мањи од n. Ако је n сложен број, тада постоји цео број d такав да је $1 < d < n$ и $d \mid n$. Означимо са m најмањи такав број. Број m не може бити сложен, јер би у том случају постојао цео број k такав да је $1 < k < m$

и $k \mid m$, што повлачи да $k \mid n$. То је, међутим, у контрадикцији са претпоставком да је m најмањи цео број већи од 1 који је делитељ од n. Дакле, m је прост број. Обележимо га са p_1. Следи да је $n = p_1 n_1$, где је $1 < n_1 < n$. По претпоставци индукције, број n_1 се може представити у облику производа простих фактора; према томе, може и n.

Групишући једнаке просте факторе броја n, закључујемо да се сваки цео број већи од 1 може представити у облику

$$n = \prod_{i=1}^{k} {p_i}^{\alpha_i}$$

где је $p_1 < p_2 < \cdots < p_k$ и $\alpha_i > 0$, за $i = 1,2, \ldots k$. За такво представљање кажемо да је канонски облик броја n . Из практичних разлога, међутим, ми узимамо да је $\alpha_i \geq 0$, јер онда било који прост број може формално да фигурише у канонском представљању неког броја.

Теорема:

Сваки цео број већи од 1 има јединствен канонски облик

Доказ:

Канонско представљање постоји на основу претходне теореме.

Канонски облик простог броја је, очигледно, јединствен. Претпоставимо да постоји позитиван сложен број већи од 1 који се може на два различита начина представити у канонском облику. Нека је n најмањи такав број, са представљањима

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_m.$$

Не постоји прост број p који се појављује у обе канонске репрезентације броја n, јер би у том случају и број $n' = \frac{n}{p}$,

који је мањи од n имао две различите канонске репрезентације што је у контрадикцији са претпоставком о минималности броја n.

Можемо да претпоставимо даје

$$p_1 \leq p_2 \leq \cdots p_k, q_1 \leq q_2 \leq \cdots q_m$$

За просте факторе p_1 и q_1 важи да је $p_1 \neq q_1$, па можемо узети да је $p_1 < q_1$. Нека је $N = p_1 q_2 \dots q_m$. Како $p_1 \mid N$ и $p_1 \mid n$, следи да $p_1 \mid (n - N)$, где је $n - N = (q_1 - p_1) q_2 \dots q_m > 1$. Следи да се број $n - N$ може написати у облику $n - N = p_1 t_1 \dots t_h$, где су t_i прости бројеви, за $i = 1,2, \dots h$.

С друге стране, ако је $q_1 - p_1 > 1$, онда се $q_1 - p_1$ може написати као производ простих фактора, рецимо $q_1 - p_1 = r_1 r_2 \dots r_s$, па добијамо, на други начин, број $n - N$ у облику производа простих фактора:

$$n - N = r_1 r_2 \dots r_s q_2 \dots q_m.$$

Ова последња факторизација не садржи прост фактор p_1. Наиме, знамо да је $p_1 \neq q_i, i = 1,2, \dots m$; с друге стране $p_1 \neq r_j$, за $j = 1,2, \dots s$, јер p_1 није делитељ од $q_1 - p_1$. Дакле, број $n - N$ има две различите факторизације, јер само једна од њих садржи прост фактор p_1. То важи и у случају кад је $q_1 - p_1 = 1$.

Међутим, $1 < n - N < n$, што је у контрадикцији са претпоставком о минималности броја n. Дакле, не постоји цео број већи од 1, који се може на два начина представити у канонском облику. ■

2.2. ПРОСТИ И СЛОЖЕНИ БРОЈЕВИ У ОСНОВНОЈ ШКОЛИ

Са појмом простог и сложеног броја ученици се први пут сусрећу у основној школи. У наставку дат је предлог – како ученике на редовној настави увести у свет ових бројева, као и избор решених задатака за додатну наставу.

ПРЕДЛОГ ЗА РЕДОВНУ НАСТАВУ

Просте бројеве можемо увести као бројеве који имају тачно два делиоца, а сложене бројеве као бројеве који имају више од два делиоца.

Дефиниција: Прости бројеви су они природни бројеви који имају тачно два делиоца – дељиви су само са самим собом и са 1. Сложени бројеви су природни бројеви који имају више од два делиоца. Број 1 није ни прост ни сложен.

Пример: Број 13 је прост, јер је дељив само са 13 и са 1 (има тачно два делиоца). Број 15 је сложен јер је дељив са 15, 5, 3 и 1 (има више од два делиоца).

Задаци за вежбу:

Задатак 1. Наведи све просте бројеве мање од 30.

Решење: То су бројеви 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Задатак 2. Дат је скуп A = {7, 9, 20, 31, 47, 50, 56, 60, 71, 100, 121}.

Написати елементе скупова P и S ако је: P = {x ⎪ x ∈ A и x је прост број},
S = {x ⎪ x ∈ A и x је сложен број}.

Решење: P = {7, 31, 47, 71}, S = {9, 20, 50, 56, 60, 100, 121}.

Такође, важно је истаћи да је број 2 једини паран прост број јер та чињеница је основа за решавање многих задатака, нарочито на додатној настави.

Неизоставан део часа на ком се обрађују прости и сложени бројеви је и дефинисање узајамно простих бројева. При томе ученицима треба указати на разлику између простих и узајамно простих бројева (да два сложена броја могу бити узајамно проста). Обавезно наводити примере јер ученици то много лакше уоче кроз примере.

2.3. НАЈВЕЋИ ЗАЈЕДНИЧКИ ДЕЛИЛАЦ

Дефиниција: Највећи заједнички делилац бројева a и b јесте највећи природан број који дели и број a и број b. Највећи заједнички делилац бројева a и b означавамо са НЗД(a, b).

Највећи заједнички делилац бројева a и b јесте највећи елемент скупа $D_a \cap D_b$.

Ако $a \mid b$ и $a \neq b$, онда је $D_a \subset D_b$, па је $D_a \cap D_b = D_a$. Тада је највећи заједнички делилац бројева a и b заправо највећи елемент скупа D_a, тј. број a.

Ако $a \mid b$, онда је НЗД$(a, b) = a$.

Највећи заједнички делилац два броја најједноставније налазимо на следећи начин: дата два или више броја напишемо један до другог, поред њих повучемо усправну црту и тражимо редом заједничке делиоце тих бројева. Поступак се завршава кад у истом реду буду узајамно прости бројеви. Највећи заједнички делилац једнак је производу простих чинилаца са десне стране црте.

Пример: Одреди НЗД(72, 90)

Решење:

72,90	2
36,45	3
12,15	3
4,5	

НЗД(72, 90)=2·3·3=18

Пример: Одреди НЗД(210, 315,630)

Решење:

210,315,630	3
70,105,210	5
14,21,42	7
2,3,6	

НЗД(210, 315, 630) = 3·5·7 = 105

2.4. УЗАЈАМНО ПРОСТИ БРОЈЕВИ

Дефиниција: Бројеви који немају заједничке просте делиоце називају се узајамно прости брјеви. Највећи заједнички делилац узајамно простих бројева јесте 1.

Пример: Узајамно прости бројеви су 3 и 5, 20 и 21 итд. Бројеви 3 и 5 су прости бројеви, а уједно и узајамно прости јер је НЗД(3, 5) = 1. Али, бројеви 20 и 21 нису прости, али јесу узајамно прости.

Задаци за вежбу:

Задатак 3. Нађи све а) просте б) сложене бројеве који су делиоци броја 210.

Решење: а) 2, 3,5,7 б) 6, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210.

Задатак 4. Нађи два сложена троцифрена броја који су узајамно прости.

Решење: 104 и 105.

Задатак 5. Нађи по један прост и један сложен број, такве да су: а) њихов збир и разлика прости бројеви; б) њихов збир и разлика сложени бројеви.

Решење: а) 23 и 6 (23 + 6 = 29, 23 – 6=17) б)31 и 4 (31+4=35,31–4

= 27)

2.5. ЕУКЛИДОВ АЛГОРИТАМ

Еуклидов алгоритам је ефикасан начин за одређивање највећег заједничког делиоца два природна броја, који не захтева њихову претходну факторизацију. То је најстарији нетривијални алгоритам који је преживео до данас. Први пут се у писаном облику појављује у Еуклидовим „Елементима“ (300.год пре нове ере) и то у VII књизи где је исказан за природне бројеве и у X књизи где је дата његова примена на дужи. Иако се налази у Еуклидовим „Елементима“ верује се да алгоритам није његово дело, већ да је био познат више од 200 година раније. Алгоритам је заснован на чињеници да се највећи заједнички делилац два природна броја неће променити ако се од већег одузме мањи па се затим посматра највећи заједнички делилац новодобијеног броја и мањег од два претходно посматрана. Понављајући тај поступак, а како скуп природних бројева има најмањи елемент, то се алгоритам завршава у коначно много корака.

Теорема: Нека су a, b, q и r цели бројеви такви да је $b > 0$, $0 \leq r < b$ и $a = bq + r$. Тада је НЗД$(a, b) =$ НЗД(b, r).

Теорема: (Еуклидов алгоритам):

Нека су $a, b > 0$ цели бројеви. Претпоставимо да је узастопном применом теореме о дељењу са остатком добијен низ једнакости:

$$a = bq_1 + r_1, \quad 0 < r_1 < b,$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2,$$

...

$$r_{j-2} = r_{j-1}q_j + r_j, \quad 0 < r_j < r_{j-1},$$

$$r_{j-1} = r_jq_{j+1}.$$

Тада је НЗД(a, b) једнак r_j, тј. последњем остатку различитом од нуле.

Пример: Применом Еуклидовог алгоритма одреди НЗД(196, 154)

Решење:

$$196 = 154 \cdot 1 + 42$$

$$154 = 42 \cdot 3 + 28$$

$$42 = 28 \cdot 1 + 14$$

$$28 = 14 \cdot 2$$

Добили смо да је НЗД(196, 154) = 14.

2.6. НАЈМАЊИ ЗАЈЕДНИЧКИ САДРЖАЛАЦ

Дефиниција: Најмањи заједнички садржалац бројева a и b јесте најмањи природан број који је дељив и бројем a и бројем b. Најмањи заједнички садржалац бројева a и b означавамо са НЗС(a, b).

Најмањи заједнички садржалац бројева a и b јесте најмањи елемент скупа $S_a \cap S_b$.

Ако $a \mid b$, онда је НЗС$(a, b) = b$.

Најмањи заједнички садржалац два броја најједноставније налазимо на следећи начин: дата два или више броја напишемо један до другог, поред њих повучемо усправну црту и тражимо редом делиоце сваког од тих бројева. Поступак се завршава кад у истом реду буду само јединице. Најмањи заједнички садржалац једнак је производу простих чинилаца са десне стране црте.

Пример: Одредити НЗС(18, 24)

Решење:

18,24	2
9,12	2
9,6	2
9,3	3
3,1	3
1,1	

НЗС(18, 24) = $2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 72$

Пример: Одредити НЗС(15, 12, 20)

Решење:

15,12,20	2
15,6,10	2
15,3,5	3
5,1,5	5
1,1,1	

НЗС(15, 12, 20) = $2 \cdot 2 \cdot 3 \cdot 5 = 60$

2.7. ВЕЗА ИЗМЕЂУ НЗД-а И НЗС-а

За свака два природна броја a и b важи НЗС$(a, b) \cdot$ НЗД$(a, b) = a \cdot b$.

Ако су a и b узајамно прости бројеви, тј. ако је НЗД$(a, b) = 1$, онда је НЗС$(a, b) = a \cdot b$.

Пример: НЗД$(84, 90) = 6$, НЗС$(84, 90) = 1260$

НЗД$(84, 90) \cdot$НЗС$(84, 90) = 6 \cdot 1260 = 7560$ и $84 \cdot 90 = 7560$.

2.8. ПРЕДЛОГ ЗА ДОДАТНУ НАСТАВУ

Прости и сложени бројеви су неизоставна тема за додатни рад у свим вишим разредима основне школе. Следи избор решених задатака који се могу користити као припрема за такмичења. Предложени задаци илуструју неке од стандардних идеја за решавање проблема у основношколској настави математике.

Задатак 6. Одредити све просте бројеве p за које су и бројеви $p + 3$, $p^2 + 3$, $p^3 + 3$ и $p^4 + 3$ такође прости.

Решење: Разликујемо два случаја.

Ако је $p = 2$ онда је $p + 3 = 5$, $p^2 + 3 = 7$, $p^3 + 3 = 11$, $p^4 + 3 = 19$ и све су то прости бројеви па је 2 једно решење.

Ако је $p > 2$, онда је p непаран број па је p^2 такође непаран број. Тада је p^2+3 паран, што значи и сложен. Дакле $p = 2$ је једино решење.

Задатак 7.Ако је p прост број већи од 3 доказати да је $p^2 – 1$ дељив са 24.

Решење: С обзиром да је по претпоставци p прост број већи од 3, он је и непаран, па је $p^2 – 1 = (p + 1)(p – 1)$ производ два парна броја, који су и узастопни парни бројеви, па је један од њих дељив са 2, а други са 4. Зато је њихов производ $(p + 1)(p – 1)$ дељив са 8.

Такође, пошто је p прост број он сигурно није дељив са 3, а $p – 1$ и $p + 1$ су му претходник и следбеник од којих је један сигурно дељив са 3. Пошто смо показали да је овај производ дељив и са 8 и са 3, следи да је он дељив и са 24 и тиме је доказ завршен.

Задатак 8. За који прост број p је и број $8p^2 + 1$ такође прост?

Решење: Разликујемо 3 случаја.

Ако је $p = 2$ тада је $8 \cdot 2^2 + 1 = 33$ а ово је сложен број. Ако је $p = 3$ онда је $8 \cdot 3^2 + 1 = 73$ прост број.

Нека је сада p прост број већи од 3. Он ће тада бити облика $p = 3k + 1$ или $p = 3k – 1$. Сада је: $8(3k \pm 1)^2 + 1 = 72k^2 \pm 48k + 9$ а овај број је сложен јер је дељив са 3. Закључујемо да је $8p^2 + 1$ прост број једино када је $p = 3$.

3. ФАКТОРИЗАЦИЈА ПОЛИНОМА

3.1. ПОЈАМ И ВРСТЕ ПОЛИНОМА

Полиноми су алгебарски изрази добијени помоћу знакова бројева, знакова променљивих и знакова операција сабирања, одузимања и множења (+, -, (·)).

Мономи су полиноми које добијамо од знакова бројева, знакова променљивих и знака за множење (·).

Пример: Изрази $7, x, y, 5x, 9y^2, x^2y^3, -10a^5b^2c^3$ јесу мономи, док изрази

$x - 5, 8x^2 - 4y$ нису мономи.

Бројевна константа у моному се назива коефицијент монома. Све променљиве одређеног степена које учествују у моному чине променљиви део. Збир изложилаца променљивих које учествују у моному називамо степен тог монома. Ако је моном константа, кажемо да је његов степен нула. За мономе који се разликују само у коефицијенту (имају једнак променљиви део) кажемо да су слични.

Пример: $3x, \frac{5}{8}x, -10x$ су слични мономи са једном променљивом, $7a^4b^2, -11a^4b^2, \frac{3}{4}a^4b^2$ су слични мономи са две променљиве.

Ако су A и B два неслична монома, онда израз $A + B$ називамо биномом, а за мономе A и B кажемо да су чланови бинома $A + B$. За бином се каже да је двочлани полином.

Пример: Изрази: $x + y, \frac{14}{25}a + b, 4x + 5yz, 10x^3 - 7$ су биноми, где су x, y, z, a, b променљиве.

Ако су A, B и C три неслична монома, онда израз $A + B + C$ називамо трином, а за мономе A, B и C кажемо да су чланови тринома $A + B + C$. За трином се каже да је трочлани полином.

Пример: Изрази: $x + y + 15, 7 + 13x - 25x^2, x - 3y + 42z^3,$ су примери тринома, где су x, y, z променљиве.

За полиноме са више од три члана не постоји посебан назив.

Полином по променљивој x је израз $P = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, при чему је $n \in \mathbb{N}$, и $a_0, a_1, \ldots, a_{n-1}, a_n \in \mathbb{R}$. Ако је $a_n \neq 0$ број n се назива степеном полинома, коефицијент a_n је најстарији или водећи коефицијент, сабирак $a_n x^n$ је најстарији члан тог полинома или водећи моном, а сабирак a_0 слободан члан тог полинома. Ако је $a_n = 1$ полином се назива монични полином. Полином је линеаран ако је $n = 1$.

Полином P по комплексној променљивој $z = x + iy$је $P(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0 = \sum_{k=0}^{n} a_k z^k$, где су коефицијенти $a_k \in \mathbb{C}$ и $n \in \mathbb{N} \cup \{0\}$. Елементи $a_n z^n, a_{n-1} z^{n-1}, \dots, a_1 z, a_0$ су чланови полинома P.

3.2. ОПЕРАЦИЈЕ СА ПОЛИНОМИМА

3.2.1. Сабирање полинома

Збир сличних монома је њима сличан моном чији је коефицијент једнак збиру коефицијената датих монома или нула ако је збир коефицијената датих монома нула.

Збир сличних монома одређујемо примењујући дистрибутивност операције множења према сабирању.

Пример: Одредити збир следећих монома:

$$\text{а) } 5x + 8x$$

$$\text{б) } 8{,}3ab + 4{,}6ab$$

$$\text{в) } \frac{3}{4}xy^2 + \frac{1}{2}xy^2$$

Решење:

$$\text{а) } 5x + 8x = (5 + 8)x = 13x$$

$$\text{б) } 8{,}3ab + 4{,}6ab = (8{,}3 + 4{,}6)ab = 12{,}9ab$$

$$\text{в) } \frac{3}{4}xy^2 + \frac{1}{2}xy^2 = \left(\frac{3}{4} + \frac{1}{2}\right)xy^2 = \left(\frac{3}{4} + \frac{2}{4}\right)xy^2 = \frac{5}{4}xy^2 = 1\frac{1}{4}xy^2$$

Претходно правило важи и у случајевима када сабирамо више сличних монома.

За дати моном P њему супротан моном је –P. Важи да је P + (-P) = 0. Коефицијент два узајамно супротна монома су узајамно супротни бројеви.

Разлика два монома једнака је збиру првог монома и монома супротног другом.

Пример: Одредити разлику монома:

$$-\frac{5}{7}xy^2 - \frac{3}{21}xy^2$$

Решење:

$$-\frac{5}{7}xy^2 - \frac{3}{21}xy^2 = \left(-\frac{5}{7} - \frac{3}{21}\right)xy^2 = \left(-\frac{15}{21} - \frac{3}{21}\right)xy^2 = -\frac{18}{21}xy^2 = -\frac{6}{7}xy^2.$$

Неслични мономи се не могу сабирати.Збир несличних монома је полином.

Кажемо да је полином у сређеном облику ако је записан у облику збира међусобно несличних монома.

Ако је полином у сређеном облику, степен тог полинома је једнак највећем од степена монома који чине тај полином.

Сабирање полинома вршимо применом закона комутативности и асоцијативности операције сабирања, док је пре сабирања погодно полиноме написати у сређеном облику.

Збир два полинома одређујемо тако што саберемо сличне мономе, а преостале мономе из оба полинома препишемо, ово правило важи и у случајевима када сабирамо више полинома.

Пример: Одредити збир полинома

$$M = x^2 + 3x - 5 \text{ и } N = -7x^2 + 1$$

Решење:

$$M + N = (x^2 + 3x - 5) + (-7x^2 + 1)$$

$$= x^2 + 3x - 5 - 7x^2 + 1 \text{ ослобађање од заграда}$$

$$= x^2 - 7x^2 + 3x + (-5) + 1 \text{ комутативност}$$

$$= (x^2 - 7x^2) + 3x + (-5 + 1) \text{ асоцијативност}$$

$$= (1 - 7)x^2 + 3x + (-4) \text{ дистрибутивност}$$

$$= -6x^2 + 3x - 4$$

За дати полином P њему супротан полином је $-P$. Важи да је $P + (-P) = 0$. Парови одговарајућих коефицијената (коефицијенти сличних монома из ова два полинома) два узајамно супротна поллинома су међусобно супротни бројеви.

Разлика два полинома једнака је збиру првог полинома и полинома супротног другом.

Пример: Одредити разлику полинома

$$P = 3x^6 + x^5 - 10x^4 - 7x^2 + 2 \text{ и } Q = 4\,x^5 - 5x^4 + 8x^2 - 6x$$

$$P - Q = (3x^6 + x^5 - 10x^4 - 7x^2 + 2) - (4\,x^5 - 5x^4 + 8x^2 - 6x)$$

$$P - Q = 3x^6 + x^5 - 10x^4 - 7x^2 + 2 - 4\,x^5 + 5x^4 - 8x^2 + 6x$$

$$P - Q = 3x^6 - 3\,x^5 - 5x^4 - 15x^2 + 6x + 2$$

3.2.2. Множење полинома

Производ два монома одређујемо примењујући комутативни и асоцијативни закон операције множења и својства степена.

Производ монома је моном чији је коефицијент једнак производу коефицијената, а променљиви део производу променљивих делова чинилаца.Производ произвољног броја монома је нови моном.

Пример: Помножити следеће мономе:

$$A = 3x^2, B = -5x^3$$

Решење:

$$A \cdot B = 3x^2 \cdot (-5x^3)$$

$$A \cdot B = 3 \cdot (-5) \cdot x^2 \cdot x^3$$

$$A \cdot B = -15x^5$$

Полином множимо мономом тако што сваки члан полинома помножимо мономом, па добијене производе саберемо.

Пример: Помножити полином P мономом M ако је:

$$P = 2x^3 + 4x^2 - 6x, M = 3x$$

Решење:

$$P \cdot M = (2x^3 + 4x^2 - 6x) \cdot 3x$$

$$P \cdot M = \ 2x^3 \cdot 3x + 4x^2 \cdot 3x - 6x \cdot 3x \ \text{дистрибутивност}$$

$$P \cdot M = 6x^4 + 12x^3 - 18x^2$$

Полином множимо полиномом тако што сваки члан једног полинома помножимо сваким чланом другог полинома, па добијене производе саберемо.

Пример: Помножити полином R полиномом S ако је:

$$R = x^2 - 5x + 4, S = \ 2x^3 - 7x - 3$$

Решење:

$$R \cdot S = (x^2 - 5x + 4) \cdot (2x^3 - 7x - 3)$$

$$R \cdot S = \ x^2 \cdot (2x^3 - 7x - 3) - 5x \cdot (2x^3 - 7x - 3) + 4 \cdot (2x^3 - 7x - 3)$$

$$R \cdot S = 2x^5 - 7x^3 - 3x^2 - 10x^4 + 35x^2 + 15x + 8x^3 - 28x - 12 \ \text{дистрибутивност}$$

$$R \cdot S = 2x^5 - 10x^4 + x^3 + 32x^2 - 13x - 12 \ \text{сређени облик полинома}$$

3.2.3. Квадрат бинома

Израз облика $(A+B)^2$представља квадрат збира монома A и B.

Општи образац за квадрат збира (формула за квадрат бинома) је:

$$(A+B)^2 = (A+B)\cdot(A+B) = A\cdot A + A\cdot B + B\cdot A + B\cdot B = A^2 + 2AB + B^2$$

Квадрат бинома једнак је збиру квадрата првог члана, двоструког производа првог и другог члана и квадрата другог члана тог бинома.

Израз облика $(A-B)^2$представља квадрат разлике монома A и B.

Општи образац за квадрат разлике који ћемо користити је:

$$(A-B)^2 = (A-B)\cdot(A-B) = A\cdot A - A\cdot B - B\cdot A + B\cdot B = A^2 - 2AB + B^2$$

Пример: Одредити квадрате следећих бинома:

$$\text{а) } (6x+y),\ \text{б) } (3a-4b)$$

Решење:

$$\text{а) } (6x+y)^2 = (6x)^2 + 2\cdot 6x\cdot y + y^2 = 36x^2 + 12xy + y^2$$

$$\text{б) } (3a-4b)^2 = (3a)^2 - 2\cdot 3a\cdot 4b + (4b)^2 = 9a^2 - 24ab + 16b^2$$

3.2.4. Разлика квадрата

Израз облика $A^2 - B^2$ представља разлику квадрата монома A и B.

Множењем полинома добијамо да за било које мономе Aи B важи:

$$(A-B)\cdot(A+B) = A^2 + AB - BA + B^2 = A^2 - B^2$$

Разлика квадрата два неслична монома једнака је производу њиховог збира и њихове разлике, тј.

$$A^2 - B^2 = (A+B)\cdot(A-B)$$

Пример: Разлику квадрата напиши у облику производа:

$$x^2 - 4$$

Решење:

$$x^2 - 4 = (x-2)\cdot(x+2)$$

Пример: Применом разлике квадрата дати производ напиши у облику сређеног полинома

$$(a-5)\cdot(a+5)$$

Решење:

$$(a-5)\cdot(a+5) = a^2 - 5^2 = a^2 - 25$$

3.3. РАСТАВЉАЊЕ ПОЛИНОМА НА ЧИНИОЦЕ

За полином који је представљен у облику производа других полинома кажемо да је растављен (разложен на чиниоце). Раставити полином на просте чиниоце (факторе) значи написати га у облику производа простих полинома (полинома који се не могу даље раставити).

Пример:

1) моном $2x^3y^2z = 2 \cdot x \cdot x \cdot x \cdot y \cdot y \cdot z$ је растављен на чиниоце $2, x, x, x, y, y, z$.
2) бином $3a + 9$ се применом дистрибутивног закона $3a + 9 = 3 \cdot a + 3 \cdot 3 = \ 3 \cdot (a + 3)$ растаља на чиниоце 3 и $a + 3$.
3) бином $9x^2 - 16y^2 = (3x)^2 - (4y)^2 = (3x - 4y) \cdot (3x + 4y)$ се применом формуле за разлику квадрата растаља на чиниоце $3x - 4y$ и $3x + 4y$.
4) трином $a^2 + 8a + 16 = a^2 + 2 \cdot a \cdot 4 + 4^2 = (a + 4)^2$ се применом формуле за квадрат бинома растаља на чиниоце $a + 4$ и $a + 4$.

Ако за полином $P = P_1 + P_2 + \ ... + P_n$ важи да се сваки од сабирака $P_1, P_2, ..., P_n$, $n \in N$, може написати у облику $P_1 = B_1 \cdot C$, $P_2 = B_2 \cdot C$, ... , $P_n = \ B_n \cdot C$, при чему је C полином, тада се применом дистрибутивног закона, полином P може раставити на чиниоце на следећи начин $P = (B_1 + B_2 + \ ... + B_n) \cdot \ C$ или $\ P = C \cdot (B_1 + B_2 + \ ... + B_n)$. За овај начин кажемо и да извлачимо заједнички чинилац испред заграде.

Пример: Применом закона дистрибутивности растави на просте чиниоце дате полиноме:

$$\text{а) } 32z + 4z^2$$

$$\text{б) } 7x^2y^3 - 28xy$$

Решење:

$$\text{а) } 32z + 4z^2 = 4z \cdot 8 + 4z \cdot z = 4z \cdot (8 + z)$$

$$\text{б) } 7x^2y^3 - 28xy = 7x \cdot x \cdot y \cdot y \cdot y - 7x \cdot 4y = 7xy \cdot (xy^2 - 4)$$

Метод груписања: Ако полином нема тзв. заједнички моном који се може извући испред заграде, али га можемо довести на облик у којем се може извући испред заграде неки бином, трином или полином, груписањем монома долазимо до решења.

Пример: Растави на просте чиниоце дати полином груписањем чланова:

$$5x - 5y - 12x + 12y$$

Решење:

$$5x - 5y - 12x + 12y = (5x - 5y) + (-12x + 12y) = 5 \cdot (x - y) + 12(-x + y)$$
$$= 5 \cdot (x - y) - 12(x - y) = (x - y) \cdot (5 - 12) = -7 \cdot (x - y)$$

Полином P комплексној променљивој $z = x + iy$ је

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \ \dots + a_1 z + a_0 = \sum_{k=0}^{n} a_k z^k$$

Где су коефицијенти $a_k \in \mathbb{C}$ и $n \in N \cup \{0\}$.

Елементи : $a_n z^n, a_{n-1} z^{n-1}, \dots, a_1 z, a_0$ су чланови полинома P.

Ако је водећи коефицијент $a_n \neq 0$ тада је полином P n-тог степена, тј.$st(P) = n$.

Број 0 се назива нула полином.

3.3.1. БЕЗУОВА ТЕОРЕМА И ХОРНЕРОВА ШЕМА

Безуов став је једна од алгебарских теорама која дефинише дељивост два полинома при специјалном случају када је делилац облика $x - \alpha$. Употребљава се за растављање полинома на чиниоце.

Теорема: (Безуов став): Нека је дат полином

$$P(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \ (a_0, a_1, a_2, \dots, a_n \in \mathbb{R})$$

И нека је дат полином $Q(x) = x - \alpha \ (\alpha \in \mathbb{R})$, тада полином $P(x)$ при дељењу полиномом $Q(x)$ даје остатак $P(\alpha)$. Специјално, ако је $P(\alpha) = 0$, полином $P(x)$је дељив полиномом $Q(x)$.

Доказ: У општем случају, дељење два полинома можемо записати као:

$$P(x) = B(x)\, Q(x) + R,$$

где је $B(x)$ неки полином који представља количник, а R остатак при дељењу полинома $P(x)$ са $Q(x)$. Заменом $Q(x) = x - \alpha$ се добија:

$$P(x) = B(x)(x - \alpha) \ + R,$$

У случају $x - \alpha = 0$, тј. $x = \alpha$ добија се:

$$P(\alpha) = B(x)(\alpha - \alpha) + R,$$

односно, $P(x) = R$, што је и требало доказати.

Хорнерова шема (Хорнеров метод или Хорнерово правило) представља једну од наведених ствари: алгоритам за израчунавање полинома, који се састоји из трансформације полинома у облик погоднији за израчунавање, или метод за одређивање корена полинома.

Нека је дат полином:

$$p(x) = \sum_{i=0}^{n} a_i\, x^i = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0, (a_0, a_1, a_2, \dots, a_n \in \mathbb{R}),$$

а потребно је израчунати вредност полинома за одређену вредност променљиве x, на пример x_0.

Да бисмо то постигли, дефинисаћемо низ нових константи:

$$b_n \coloneqq a_n$$

$$b_{n-1} \coloneqq a_{n-1} + b_n x_0$$

$$\dots.$$

$$b_0 = a_0 + b_1 x_0 \,.$$

Тада b_0 има вредност $p(x_0)$.

Како бисмо показали да је ово тачно, приметимо да се полином може записати у следећем облику:

$$p(x) = a_0 + x\big(a_1 + x(a_2 + \ \dots + x(a_{n-1} + a_n x) \dots)\big)$$

На овај начин, замењујући b_i у претходном изразу, добијамо:

$$p(x_0) = a_0 + x_0\big(a_1 + x_0(a_2 + \ \dots + x_0(a_{n-1} + b_n x_0) \dots)\big)$$

$$= a_0 + x_0\big(a_1 + x_0(a_2 + \ \dots + x_0(b_{n-1}) \dots)\big)$$

$$\dots$$

$$= a_0 + x_0(b_1)$$

$$= b_0$$

Пример: Одредити $P(2)$ по Хорнеровој шеми ако је $P(z) = 2z^5 - 3z^2 + 5z - 4$

Решење: $P(z) = 2z^5 - 3z^2 + 5z - 4 = \ 2z^5 + 0z^4 + 0z^3 - 3z^2 + 5z - 4$

2	2	0	0	−3	5	−4
	2	4	8	13	31	58

Дакле, $P(2) = 58$.

У општем случају факторисати полином значи записати га у облику производа полинома нижег степена.

Сваки полином са реалним коефицијентима се на јединствен начин може факторисати у производ полинома првог и полинома другог степена при чему су полиноми другог степена са дискриминантом мањом од нуле.

3.3.2. ЕУКЛИДОВ АЛГОРИТАМ ЗА ОДРЕЂИВАЊЕ НЗД

За било која два не нула полинома P и Q постоји њихов највећи заједнички делилац, одређен са тачношћу до једне мултипликативне константе.

Код Еуклидовог алгоритма за одређивање НЗД најпре поделимо полином P полиномом Q, а затим све док остатак није нула делимо делилац са остатком. Последњи не нула остатак једнак је НЗД(P, Q). Тако добијамо следећи низ једначина у којима су редом $Q, R_1, R_2, \dots, R_k$ делиоци, а редом $R_1, R_2, \dots, 0$ остаци.

$$P(z) = Q(z) \cdot Q_1(z) + R_1(z)$$

$$Q(z) = R_1(z) \cdot Q_2(z) + R_2(z)$$

$$R_1(z) = R_2(z) \cdot Q_3(z) + R_3(z)$$

.....

$$R_{k-3}(z) = R_{k-2}(z) \cdot Q_{k-1}(z) + R_{k-1}(z)$$

$$R_{k-2}(z) = R_{k-1}(z) \cdot Q_k(z) + R_k(z)$$

$$R_{k-1}(z) = R_k(z) \cdot Q_{k+1} + 0$$

дељеник делилац количник остатак

$$R_k(z) = \text{НЗД}(P(z), Q(z)).$$

4. ОПШТА АЛГЕБАРСКА ТЕОРИЈА ФАКТОРИЗАЦИЈЕ

У алгебри, теорија прстена је изучавање прстенова — алгебарских структура у којима су сабирање и множење дефинисани и имају слична својства са тим операцијама дефинисаним за целе бројеве. Теорија прстена изучава структуре прстена, њихове репрезентације, специјалне класе прстена (групе прстена, дељење прстена, универзалне окружујуће алгебре), као и низ својстава за која је доказано да су од интереса унутар саме теорије и за њене примене.

Комутативни прстенови су много боље изучени од оних који нису комутативни. Алгебарска геометрија и алгебарска теорија бројева, које пружају многе природне примере комутативних прстенова, покренули су већи део развоја комутативне теорије прстена, која је сада под именом комутативне алгебре, једно од главних подручја модерне математике. Будући да су ова три поља (алгебарска геометрија, алгебарска теорија бројева и комутативна алгебра) толико блиско повезана, обично је тешко и бесмислено да се разврстава којем пољу припада дати резултат. На пример, теорема Хилбертових нула је фундаментална за алгебарску геометрију, а наведена је и доказана у смислу комутативне алгебре. Слично томе, последња Фермаова теорема је наведена у виду елементарне аритметике, која је део комутативне алгебре, али њен доказ укључује дубоке резултате из алгебарске теорије бројева и алгебарске геометрије.

Некомутативни прстенови имају у знатној мери различит профил, те се стога могу јавити необичније појаве. Мада се та теорија углавном самостално развила, постоји новији тренд који тежи упоређивању са комутативним развојем грађењем теорије извесних класа некомуникативних прстенова на геометријски начин, као да су то прстенови функција на (непостојећим) 'некомутативним просторима'. Овај тренд је започео током 1980-их са развојем некомутативне геометрије и открићем квантних група.То је довело до бољег разумевања некомуникативних прстенова, посебно некомутаторних Нетерових прстенова.

Прстен се назива комутативним ако је његова мултипликација комутативна. Комутативни прстени подсећају на познате бројевне системе, и различите дефиниције комутативних прстенова су дизајниране да формализују својства целих бројева. Комутативни прстенови такође су важни у алгебарској геометрији. У теорији комутативних прстена бројеви се често замењују идеалима, а дефиниција простог идеала настоји да обухвати суштину простих бројева. Интегрални домени, нетривијални комутативни прстенови у којима два ненулта елемента не могу множењем да дају нулу, генерализирају још једно својство целих бројева и служе као одговарајућа област за проучавање дељивости. Главни идеални домени су интегрални домени у којима сваки идеал може бити генерисан једним елементом, још једним својством које је заједничко са целим бројевима. Еуклидски домени су интегрални домени у којима се може спровести еуклидски алгоритам. Важни примери комутативних прстенова могу се конструирати као прстенови полинома и њихови факторски прстенови.

4.1. ТЕОРИЈА ПРСТЕНА

Прстени су алгебарске структуре са којима се ученици прво сређу у свом математичком образовању.

Дефиниција: Алгебарска структура R = $(R, +, \cdot)$ са бинарним операцијама $+$ и $\cdot$ је прстен акко су испуњени следећи услови:

1) $(R, +)$ је Абелова група
2) $(R, \cdot)$ је полугрупа(семигрупа)
3) операција $\cdot$ је и лево и десно дистрибутивна с обзиром на операцију $+$, тј. важи за свако $a, b, c \in R$:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \ \ (b + c) \cdot a = b \cdot a + c \cdot a.$$

Прстен R је комутативан акко је $(R, \cdot)$ је комутативна полугрупа.

Неутрални или нула елемент групе $(R, +)$ обележава се са 0, односно 0_R ако желимо да нагласимо да је у питању нула прстена R. Прстен чији домен садржи само нулу назива се нула прстен. Инверзни елемент елемента a обзиром на сабирање обележавамо са $-a$.

Дефиниција: Ненула елемент e прстена R је леви јединични елемент акко је $e \cdot r = r$ за свако r из R.

Дефиниција: Ненула елемент e прстена R је десни јединични елемент акко је $r \cdot e = r$ за свако r из R.

Ако прстен R има (леви, десни) јединични елемент e кажемо да елемент a има леви (десни) инверзни елемент с обзиром на a акко постоји елемент b такав да је

$$b \cdot a = e \ (a \cdot b = e).$$

Ненула елемент a прстена R је леви (десни) делитељ нуле акко постоји ненула елемент b такав да је $a \cdot b = 0$ ($b \cdot a = 0$). Елемент a је делитељ нуле акко је и леви и десни делитељ нуле. Елемент a је леви (десни) делитељ елемента b акко постоји елемент c такав да је $ac = b$ ($ca = b$). Елемент a је делитељ елемента b акко је и леви и десни делитељ елемента b.

Комутативан прстен са јединицом и без делитеља нуле зове се интегрални .

Елемент a је нилпотентан акко је $a^k = 0$ за неки позитиван природан број k.

Ако прстен има барем један леви и десни јединични елемент онда су ти елементи једнаки и то је јединични елемент прстена.

Прстен може имати највише један јединични елемент.

Ако прстен има јединицу и ако елемент a има и леви и десни инверзни елемент, онда су ти елементи једнаки и то је инверзни елемент елемента a, у ознаци a^{-1}.

Уколико прстен R има јединични елемент, тај се у општој причи обележава са 1 или са 1_R, а за R кажемо да је прстен са јединицом. Како егзистенција јединичног елемента није саставни део

дефиниције прстена, то ћемо увек нагласити када неки прстен има јединицу. Прстен са јединицом има бар два елемента. У прстену са јединицом је $a^0 = 1$ за сваки ненула елемент a.

За елемент који има инверзни кажемо и да је инверзибилан или инвертибилан. Скуп свих инверзибилних елемената прстена R обележавамо са R^*.

4.2. ФАКТОРИЗАЦИЈА У КЛАСИЧНИМ ДОМЕНИМА

Ако се не нагласи другачије домен A биће комутативан прстен са јединицом без делитеља нуле. Инвертибилне елементе домена A означаваћемо са A^*.

Дефиниција: Елементи a, b домена A су асоцирани ако $\exists u \in A^*$ тако да је $a = ub$.

Дефиниција: Идеал P домена A је прост ако је

$$P \neq A \text{ и } ab \in P \Rightarrow (a \in P \vee b \in P).$$

Еквивалентно је рећи да је фактор прстен A / P домен.

Како је у домену нула идел увек прост, просте идеале различите од нуле звaћемо правим простим идеалима.

Дефиниција: Идеал M домена A је максималан ако је

$$M \neq A \text{ и } M \subseteq I \subseteq A \Rightarrow (I = M \vee I = A).$$

Еквивалентно је рећи даје фактор прстен A / M поље.

Дефиниција: За елемент $p \neq 0$ домена A кажемо да је атом или да је иредуцибилан ако

$$p \notin A^* \text{и } p = ab \Rightarrow a \in A^* \vee b \in A^*.$$

Дефиниција: За елемент $p \neq 0$ домена A кажемо да је прост ако:

$$p \notin A^* \text{и } p \mid ab \Rightarrow p \mid a \vee p \mid b.$$

Теорема: Проста факторизација елемената домена је увек једнозначна.

Доказ: Нека је A домен и $a \in A$ елемент који има две просте факторизације

$$a = p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$$

где су p_i, q_i прости. Из горње једнакости имамо да $p_1 \mid q_1 q_2 \ldots q_m$. Како је p_1 прост, онда $p_1 \mid q_1 \vee \ldots \vee p_1 \mid q_m$. Не умањујући општост доказа претпоставићемо да $p_1 \mid q_1$. Како су p_1 и q_1 прости, па дакле и атоми, онда је p_1 асоциран са q_1, тј. $q_1 = up_1$ за неко $u \in A^*$. На тај горњу факторизацију можемо скратити са p_1, и добијамо

$$p_2 \ldots p_n = uq_2 \ldots q_m.$$

Даље, индукцијом добијамо да је $n = m$ и p_i је асоциран са q_i, тј. факторизација је једнозначна.

Дефиниција: Нека су $a, b \in A, a, b \neq 0$. Елемент $d \in A$ је највећи заједнички делитељ елемената a и b, у ознаци $d = nzd[a, b]$, ако важи:

1) $d \mid a,\ d \mid b$
2) $d' \mid a,\ d' \mid b \Rightarrow d' \mid d$

Дефиниција: Нека су $a, b \in A$. Елемент $m \in A$ је најмањи заједнички садржалац елемената a и b, у ознаци $m = nzs[a, b]$, ако важи:

1) $a \mid m, b \mid m$

2) $a \mid m', b \mid m' \Rightarrow m \mid m'$.

За пар елемената $a, b \in A$, највећи заједнички делитељ, односно, најмањи заједнички садржалац не морају постојати, а ако постоје не морају бити јединствени. Они су одређени једнозначно до на множење инвертибилним фактором. За елементе a, b кажемо да су копрости ако је $nzd[a, b] = 1$. Из дефиниције најмањег заједничког садржаоца следи:

$$m = nzs[a, b] \Leftrightarrow (m) = (a) \cap (b).$$

Егзистенција најмањег заједничког садржаоца за пар елемената $a, b \in A$ еквивалентна је са условом да је пресек главних идеала $(a) \cap (b)$, главни идеал генерисан управо $nzs -$ ом тих елемената.

Теорема: Нека су a, b елементи домена A за које постоји $nzs[a, b]$. Тада постоји и $nzd[a, b]$.

Доказ: Нека је $m = nzs[a, b]$, тј. $(m) = (a) \cap (b)$. Тада је $(ab) \subseteq (a) \cap (b) = (m)$, па $\exists c \in A$ тако да је $ab = cm$. Показаћемо да је $c = nzd[a, b]$. Како $(m) \in (a) \cap (b)$ имамо да је $m = ad_1 = bd_2$ одакле је $ab = cad_1 = cbd_2$. Из последње једнакости добијамо $b = cd_1$, $a = cd_2$, па $c \mid a$ и $c \mid b$. Нека сада $z \mid a$, z $\mid b$. Tada је $a = ze$, $b = zf$, одакле $a \mid zef$, $b \mid zef$, па је zef заједнички садржалац за a и b. Како је $m = nzs[a, b]$ важиће $m \mid zef$ па је $cm = ab = zzef = zmg$, одакле је $c = zg$, тј. $z \mid c$.

У општем случају не важи обрат теореме. Важи следеће: ако за свако x постоји $nzd[xa, xb] = xnzd[a, b]$, тада постоји $nzs[a, b]$.

Дефиниција: Домен A је Еуклидов ако постоји функција φ: $A \setminus \{0\} \to \mathbb{Z}^+$ са особинама:

$$ab \neq 0 \Rightarrow \varphi(ab) \geq \varphi(a)$$

$$(\forall\, a, b \in A, b \neq 0)(\exists\, q, r \in A)\ a = bq + r, \varphi(r) < \varphi(b)$$

Функцију φ из претходне дефиниције зовемо Еуклидским алгоритмом. Еуклидски алгоритам не мора постојати, а и ако постоји, не мора бити једнозначно одређен. Можемо наћи више функција које задовољавају горње услове, на пример ако је φ Еуклидски алгоритам онда је то и функција $\varphi + 1$ па се може говорити о фамилији алгоритама φ_i. Унутрашња карактеритика ових прстена је да у њима важи алгоритам „дељења са остатком“. Елементе q и r из дефиниције функције φ зовемо Еуклидским количником и остатком. Еуклидови прстени су на пример прстен целих бројева $\mathbb{Z}$ са Еуклидском функцијом $\varphi(n) = |n|$.

ЗАКЉУЧАК

У овом раду представљена су прва разматрања о факторизацији природних бројева у нижим разредима основне школе (парни и непарни бројеви, дељење са остатком). Уведен је појам простог броја, говорило се о његовим особинама, дат је пример Ератостеновог сита и објашњено налажење највећег заједничког делиоца и најмањег заједничког садржаоца. Дати су примери за редовну наставу, као и за часове додатног рада. Важно је допустити ученицима да развијају и предлажу неке своје идеје за решавање задатака, јер у противном се може десити да науче шаблон који неће знати да примене на теже проблеме. Неопходно је урадити што више различитих типова задатака и изложити неколико путева решавања. Објашњен је појам полинома као и основне операције са њима: сабирање, одузимање, множење, при чему је за сваку од операција предложен одговарајући пример. Уопштавањем поступака из конкретних примера, подстичемо ученике на индуктивно мишљење. На крају рада дат је и осврт на општу алгебарску теорију факторизације, где су поменути и прстени са једнозначном факторизацијом.

ЛИТЕРАТУРА

[1] Уџбеник из математике за пети разред основне школе – Небојша Икодиновић, Слађана Димитријевић, Klett, Београд, 2015;

[2] Уџбеник из математике за седми разред основне школе – Небојша Икодиновић, Слађана Димитријевић, Klett, Београд, 2015;

[3] Математика за први разред средње школе, Павле Миличић, Владимир Стојановић, Зоран Каделбург, Бранислав Боричић, ЗУНС, Београд, 1991

[4] Збирка задатака из математике за први разред средње школе, Владимир Сотировић, Душан Липовац, Владимир Стојановић, ЗУНС, Београд, 2007

[5] Алгебра - Г. Калајџић, Математички факултет, Београд, 1998;

[6] „Увод у теорију бројева – теорија и примјери“, М. Анђић, Графо Црна Гора д.о.о., Подгорица, 2004;

[7] Б„Алгебра 1“,Б. Шешеља, А. Тепавчевић Природно-математички факултет, Нови Сад, 2004;

[8] „Теорија бројева, збирка задатака“,М. Станић, Н. Икодиновић, Завод за уџбенике и наставна средства, Београд, 2004;

[9] „Линеарна алгебра“, Градимир В. Миловановић, Радосав Ж. Ђорђевић, Ниш, 2004;

[10] „Линеарна алгебра и аналитичка геометрија”, Љ. Кочинац Просвета, Ниш, 1997

[11] http://www.mathtutor.ac.uk/algebra/factorisingquadratics

[12] http://www.opsteobrazovanje.in.rs/matematika/

[13] http://www.dms.org.rs/