Квадратна раширења поља рационалних бројева

Душан Ђукић

0° Увод

У аритметици на коју смо навикли радимо са рационалним бројевима из скупа $\mathbb{Q}$ и целим из скупа $\mathbb{Z}$. Осим што је савршено интуитивна, оваква аритметика има веома пожељна својства: поредак, добро дефинисану дељивост, просте бројеве и, најзад, јединствено разлагање на просте чиниоце.

Међутим, моћ аритметике над $\mathbb{Q}$ је ограничена. Зато нам је понекад потребно да радимо са другим скуповима. Очигледан пример је свођење по модулу простог броја p - тј. аритметика у скупу $\mathbb{Z}_p$.

Пример. Решити једначине (а) $4x^2 - 1 = y^3$; (б) $6x^3 + 3 = y^3$; (в) $x^2 + 1 = y^3$ у скупу $\mathbb{Z}$.

(а) Леву страну факторишемо: добијамо $(2x-1)(2x+1) = y^3$. Бројеви $2x-1$ и $2x+1$ су узајамно прости, њихов производ је куб, дакле сваки од њих је куб: $2x - 1 = u^3$ и $2x + 1 = v^3$ ($u, v \in \mathbb{Z}$. Али тада је $v^3 - u^3 = 2$, што је једино могуће за $(u, v) = (-1, 1)$ и $(x, y) = (0, -1)$.

(б) Уместо у $\mathbb{Z}$, посматрајмо једначину у $\mathbb{Z}_7$, тј. по модулу 7. Имамо $y^3 \in \{0, 1, 6\} \pmod 7$, али $6x^3 + 3 \in \{2, 3, 4\} \pmod 7$, дакле дата једначина нема решења.

(в) Ово изгледа теже. Рачун по било ком модулу не пролази, а леву страну нажалост можемо да раставимо само као $x^2 + 1 = (x + i)(x - i)$. Можда нам треба аритметика у неком скупу који садржи i?

Да бисмо могли да говоримо о аритметици, није неопходно да радимо у скупу $\mathbb{Q}$ или $\mathbb{Z}_p$. То може да буде било који скуп $\mathbb{F}$ у коме можемо да сабирамо, одузимамо, множимо и делимо. Другим речима, $\mathbb{F}$ може да буде било које поље.

Подсетимо се шта је то поље:

- Скуп F на коме су дефинисане бинарне операције сабирања и множења је *поље* ако:
  - (i) за све $a, b \in F$, збир $a + b$ и производ ab су такође у скупу F;
  - (ii) $a + b = b + a$, $(a + b) + c = a + (b + c)$, $ab = ba$, $a(bc) = (ab)c$ и $(a + b)c = ac + bc$ за свака три елемента $a, b, c \in F$;
  - (iii) постоје елементи $0, 1 \in F$ такви да је $a + 0 = a \cdot 1 = a$ за свако $a \in F$;
  - (iv) за свако $a \in F$, постоји елемент $-a \in F$ такав да је $a + (-a) = 0$;
  - (v) за свако $a \in F \setminus \{0\}$ постоји елемент $a^{-1} \in F$ такав да је $a \cdot a^{-1} = 1$.

Пример. Скупови $\mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ и $\mathbb{Z}_p$ (p је прост број) са уобичајеним операцијама сабирања и множења су поља.

Раширење поља $\mathbb{Q}$ је свако поље које садржи поље $\mathbb{Q}$. То раширење зовемо *алгебарским* ако су сви његови елементи алгебарски бројеви:

Дефиниција. Број $\alpha \in \mathbb{C}$ је *алгебарски* ако је нула неког неконстантног полинома са целим коефицијентима.

Полином $P(x)$ са целим коефицијентима најмањег степена и најмањег позитивног водећег коефицијента за који је $P(\alpha) = 0$ је *минимални* полином броја α.

Пример. Број $\frac{1}{2}i$ је алгебарски, а његов минимални полином је $4x^2 + 1$.

Број $\sqrt{2} + \sqrt{3}$ је алгебарски; његов минимални полином је $x^4 - 10x^2 + 1$ (проверите!).

За нас ће бити посебно значајно поље у следећем примеру:

Пример. Нека је $d \neq 1$ цео број. Скуп $\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$ са уобичајеним операцијама сабирања и множења је поље. Заиста:

$a = a_1 + a_2\sqrt{d}, \quad b = b_1 + b_2\sqrt{d}, \quad a_1, a_2, b_1, b_2 \in \mathbb{Q}:$
(i) $a + b = (a_1 + b_1) + (a_2 + b_2)\sqrt{d}$, $ab = (a_1b_1 + da_2b_2) + (a_1b_2 + a_2b_1)\sqrt{d}$;
(ii) и (iii) тривијално важе на основу особина уобичајеног сабирања;
(iv) $-a = -a_1 - a_2\sqrt{d}$; (v) $a^{-1} = \frac{a_1 - a_2\sqrt{d}}{a_1^2 - da_2^2}$.

Дефиниција. Квадратно раширење поља $\mathbb{Q}$ је поље облика $\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$, где је $d \neq 1$ цео број који није дељив квадратом већим од 1.

Тема овог текста је пре свега аритметика у квадратним проширењима $\mathbb{Q}$. То значи да нам елементи скупа $\mathbb{Q}[\sqrt{d}]$ играју улогу "рационалних" бројева. Може ли аритметика у оваквом пољу да функционише попут аритметике у $\mathbb{Q}$ на коју смо навикли? Одговор ће зависити од одговора на следећа питања:

А Ако су елементи $\mathbb{Q}[\sqrt{d}]$ "рационални", како дефинисати "целе" елементе?

Б Имамо ли погодну релацију поретка, знак и апсолутну вредност на овом пољу?

В Како увести дељивост, конгруенције и просте бројеве у овом пољу?

Г Важе ли и овде основна теорема аритметике и њене последице?

Идемо редом.

1° Цели елементи у $\mathbb{Q}[\sqrt{d}]$.

Тзв. цели елементи унутар поља $\mathbb{F}$ (у нашем случају, $\mathbb{F} = \mathbb{Q}[\sqrt{d}]$) морају да допуштају сабирање, одузимање и множење, и да садрже јединицу. Другим речима, они треба да чине *интегрални домен*:

- Подскуп R поља $\mathbb{F}$ је *интегрални домен* ако:
  (i) елементи 0 и 1 припадају скупу R;
  (ii) за све $a, b \in R$, елементи $-a$, $a + b$ и ab су такође у скупу R.

Интегрални домен је комутативни *прстен* са јединицом и без делилаца нуле. Прстени су скупови са дефинисаним операцијама сабирања и множења у којима у општем случају не мора да важи $ab = ba$, не мора да постоји елемент 1, и могу да постоје ненула елементи са производом нула.

Интегрални домен који садржи R зовемо *интегралним проширењем* R.

Скуп количника $\{\frac{x}{y} \mid x, y \in R\}$ интегралног домена R је поље, тзв. *количничко поље*. Природно захтевамо да количничко поље скупа целих елемената унутар $\mathbb{F}$ буде читаво поље $\mathbb{F}$.

Напомена. Овим је аутоматски искључена неинвентивна могућност да једини цели елементи буду они из $\mathbb{Z}$.

Који критеријум имамо на располагању да разликујемо целе од нецелих елемената? Уводимо појам алгебарски целих бројева:

Дефиниција. Алгебарски број α је *алгебарски цео* ако је његов минималан полином моничан.

Пример. Минимални полином рационалног броја $q = a/b$ ($a \in \mathbb{Z}$, $b \in \mathbb{N}$) је $bx - a$. По дефиницији, q је алгебарски цео ако и само ако је $b = 1$, тј. ако и само ако је q цео.

Пример. Број $\alpha = 2\cos 40^\circ$ је алгебарски цео јер је његов минимални полином $x^3 - 3x + 1$, док $\frac{1}{2}\alpha$ то није.

Управо на овоме заснивамо нашу дефиницију целог елемента у квадратном раширењу.

Дефиниција. Елемент $z \in \mathbb{Q}[\sqrt{d}]$ је *цео* ако и само ако је алгебарски цео.

По Гаусовој леми (зашто?), z је цео елемент ако и само ако постоји неконстантан моничан полином $P(x)$ за који је $P(z) = 0$.

Сваки елемент $z = a + b\sqrt{d}$ са $a, b \in \mathbb{Z}$ је цео, јер је нула полинома $x^2 - 2ax + (a^2 - db^2)$. Међутим, следећи пример показује да то нису обавезно једини цели елементи.

Пример. У пољу $\mathbb{Q}[\sqrt{-3}]$, елемент $\omega = \frac{-1+\sqrt{-3}}{2}$ је цео јер је $\omega^2 + \omega + 1 = 0$, али $\omega \notin \mathbb{Z}[\sqrt{-3}]$.

Претпоставимо да је $z = a + b\sqrt{d}$ цео елемент $(a, b \in \mathbb{Q})$.

(i) Ако је $b = 0$, онда је $P_z(x) = x - a$, дакле $a \in \mathbb{Z}$

(ii) Ако је $b \neq 0$, онда је $P_z(x) = x^2 - 2ax + (a^2 - db^2)$, дакле $2a$ и $a^2 - db^2$ су цели бројеви. Шта више, и број $2b$ је цео јер је $d(2b)^2 = (2a)^2 - 4(a^2 - db^2)$ цео. Ако је један од бројева a, b цео, онда је то и други. Остаје случај када су $2a$ и $2b$ непарни, а тада $4 \mid 4a^2 - 4db^2 \equiv 1 - d \pmod 4$, дакле $d \equiv 1 \pmod 4$ и $a \equiv b \equiv \frac{1}{2} \pmod 1$.

Показали смо ово, уз ознаку $\mathbb{Z}[\alpha] = \{m + n\alpha \mid m, n \in \mathbb{Z}\}$ за $\alpha \in \mathbb{Q}[\sqrt{d}]$:

Теорема 1. За $d \equiv 2, 3 \pmod 4$, скуп целих елемената у $\mathbb{Q}[\sqrt{d}]$ је $\mathbb{Z}[\sqrt{d}]$.
За $d \equiv 1 \pmod 4$, скуп целих елемената у $\mathbb{Q}[\sqrt{d}]$ је $\mathbb{Z}[\frac{-1+\sqrt{d}}{2}]$. □

Уверимо се да је скуп целих елемената заиста интегрални домен. Он садржи нулу и јединицу, затворен је у односу на сабирање и одузимање, остаје само да покажемо да је затворен у односу на множење.
За $d \equiv 2, 3 \pmod 4$ имамо $(m + n\sqrt{d})(p + q\sqrt{d}) = (mn + dpq) + (mq + np)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.
За $d \equiv 1 \pmod 4$, означимо $\tau = \frac{-1+\sqrt{d}}{2}$. Тада је $\tau^2 = \frac{d-1}{4} - \tau$, одакле је $(m + n\tau)(p + q\tau) = mp + nq\frac{d-1}{4} + (mq + np - nq)\tau \in \mathbb{Z}[\tau]$.

Пример. Цели елементи поља $\mathbb{Q}[\sqrt{-1}]$ су тзв. *Гаусови цели* бројеви $a + bi$ $(a, b \in \mathbb{Z})$.

Цели елементи поља $\mathbb{Q}[\sqrt{-3}]$ су тзв. *Ајзенштајнови цели* бројеви $a + b\omega$, где је $\omega = \frac{-1+i\sqrt{3}}{2}$ примитивни трећи корен јединице.

2° Поредак и норма.

Барем за $d > 0$, увођење поретка је наизглед тривијално, јер су тада елементи поља $\mathbb{Q}[\sqrt{d}]$ реални, па онда можемо да наследимо знак, поредак и апсолутну вредност из $\mathbb{R}$. Али да ли је овај начин "погодан"? Да видимо, имамо ли при оваквом поретку минималан позитиван цео елемент? ... Немамо га, постоје бесконачни опадајући низови позитивних елемената - а то значи да не може бити никакве индукције, Еуклидовог алгоритма, највећег заједничког делиоца, итд, што је са становишта теорије бројева апсолутно непожељно. Дакле, ово није погодан начин.

Можда ћемо боље урадити ако почнемо од случаја $d < 0$. Пошто је $\mathbb{Q}[\sqrt{d}]$ тада комплексно поље, у њему имамо коњуговање $(\overline{z} = a - b\sqrt{d})$ и модул $(|z| = \sqrt{a^2 - db^2})$ елемента $z = a + b\sqrt{d}$. Квадрат модула $|z|^2$ је цео број и погодан кандидат за еквивалент "апсолутне вредности".

Појмове конјугата и модула проширићемо по аналогији и на случај $d > 0$.

Дефиниција. Нека је $z = a + b\sqrt{d}$ елемент поља $\mathbb{Q}[\sqrt{d}]$.
Конјугат елемента z је $\bar{z} = a - b\sqrt{d}$, а његова *норма* је $N(z) = z\bar{z} = a^2 - db^2$.

За $d \equiv 1 \pmod 4$ знамо да је скуп целих елемената $\mathbb{Z}[\tau]$, где је $\tau = \frac{-1+\sqrt{d}}{2}$. Конјугат елемента $x = a + b\tau = a - \frac{1}{2}b + \frac{1}{2}b\sqrt{d}$ $(a, b \in \mathbb{Z})$ је $\bar{x} = a - \frac{1}{2}b - \frac{1}{2}\sqrt{d} = a - b - b\tau$, а његова норма

$$N(a + b\tau) = x\bar{x} = (a - \frac{1}{2}b)^2 - \frac{1}{4}db^2 = a^2 - ab - \frac{d-1}{4}b^2.$$

Следеће тврђење се доказује директно по дефиницији.

Теорема 2. Конјуговање и норма су мултипликативни, тј. за произвољне елементе z_1, z_2 поља $\mathbb{Q}[\sqrt{d}]$ важи $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$ и $N(z_1 z_2) = N(z_1)N(z_2)$. □

Пример. У $\mathbb{Z}[i]$ норма елемента $a + bi$ $(a, b \in \mathbb{N})$ је $N(a + bi) = a^2 + b^2$.

Ако је $z = a + b\omega \in \mathbb{Z}[\omega]$ $(a, b \in \mathbb{Z})$, онда је $\overline{z} = a - b - b\omega$ и $N(z) = a^2 - ab + b^2$.

Сада можемо да уведемо поредак овако: за $x, y \in \mathbb{Q}[\sqrt{d}]$ је $x \prec y$ ако је $|N(x)| < |N(y)|$.

Пример. Пошто је норма целог ненула елемента цео број, "минимални" елементи $\mathbb{Z}[\sqrt{d}]$ при овој релацији поретка су они чија је норма ± 1.

Овај поредак није потпун (нису свака два елемента упоредива), али без тога можемо да живимо јер нама и није толико важан поредак сам по себи. Важно нам је да је норма целог елемента цео број, што значи да је сваки "опадајући" низ целих елемената из R коначан - а без овог својства тешко да бисмо могли.

3° Дељивост.

Дељивост и конгруентност се и у проширењима R прстена $\mathbb{Z}$ дефинишу на уобичајен начин: $x \in R$ је дељиво са $y \in R$ (у ознаци $y \mid x$) ако постоји елемент $z \in R$ такав да је $x = yz$, и $x \equiv y \pmod{z}$ ако $z \mid x - y$.

Главна разлика у односу на $\mathbb{Z}$ је у томе што могу да постоје елементи различити од ± 1 који деле сваки цео елемент: то су тзв. јединични елементи.

Дефиниција. Елемент $\epsilon \in \mathbb{Z}[\alpha]$ зовемо *јединичним* ако дели број 1; тј. ако постоји $\epsilon' \in \mathbb{Z}[\alpha]$ такво да је $\epsilon\epsilon' = 1$.

Ако је ϵ јединичан елемент, важи $N(\epsilon)N(\epsilon') = N(1) = 1$, па је $N(\epsilon) = \pm 1$. У ствари, елемент ϵ је јединичан ако и само ако има норму ± 1: заиста, ако је $N(\epsilon) = \pm 1$ онда је по дефиницији $\pm\epsilon\bar{\epsilon} = 1$.

Пример. (1) Једини јединични елементи у $\mathbb{Z}$ су ± 1.

(2) Нађимо све јединичне елементе у $\mathbb{Z}[i]$. Ако је $a + bi$ $(a, b \in \mathbb{Z})$ јединичан, онда је $N(a + bi) = a^2 + b^2 = \pm 1$, одакле је $a + bi \in \{\pm 1, \pm i\}$.

(3) У $\mathbb{Z}[\omega]$ постоји 6 јединичних елемената: $\pm 1, \pm\omega, \pm(1 + \omega)$. Заиста, ако је $a + b\omega$ јединичан онда је $a^2 - ab + b^2 = 1$, тј. $(2a - b)^2 + 3b^2 = 4$ одакле лако следи резултат. Приметимо да је $1 + \omega = -\omega^2$.

(4) У $\mathbb{Z}[\sqrt{2}]$, елемент $x = a + b\sqrt{2}$ је јединичан ако је $N(x) = a^2 - 2b^2 = \pm 1$. Из теорије Пелових једначина знамо да су то сви елементи облика $x = \pm(1 + \sqrt{2})^n$, $n \in \mathbb{Z}$.

Сваки елемент $x \in R$ је дељив са ϵ и са ϵx, за сваки јединичан елемент ϵ. Зато дефиницију простог елемента морамо да прилагодимо новом окружењу.

Дефиниција. Елемент $y \in R$ је *еквивалентан* елементу x (пишемо $y \sim x$) ако постоји јединични елемент ϵ такав да је $y = \epsilon x$.

Дефиниција. Елемент $x \in R$, који није 0 и није јединичан, је *прост* ако нема других делилаца осим јединичних и себи еквивалентних елемената.

Важи следеће једноставно тврђење.

Теорема 3. Нека је $x \in R$. Ако је $N(x)$ прост цео број, онда је x прост.

Доказ. Претпоставимо да је $x = yz$, $y, z \in K$. Тада је $N(x) = N(y)N(z)$, па је бар један од $N(y), N(z)$ једнак ± 1, тј. или y или z је јединични елемент, док је други од њих (по дефиницији) еквивалентан елементу x. □

Пример. (а) Елемент $2+i$ је прост у $\mathbb{Z}[i]$ јер је $N(2+i)=5$ прост.

(б) Број 3 је прост у $\mathbb{Z}[i]$, иако $N(3)=9$ није прост. Заиста, ако је $3=xy$, где $x,y\in\mathbb{Z}[i]$ нису јединични, онда је $N(x)N(y)=9$, дакле $N(x)=N(y)=3$, али $N(a+bi)=a^2+b^2$ никад не узима вредност 3.

Овај пример показује да други смер теореме 3 не важи.

(в) Број 5 је прост у $\mathbb{Z}$, али је сложен у $\mathbb{Z}[i]$ јер је $5=(2+i)(2-i)$, при чему ниједан од фактора није јединичан.

Очигледно, елемент еквивалентан простом елементу, као и његов конјугат, такође су прости.

Теорема 4. Нека је $z\in R$ прост елемент који није еквивалентан целом броју. Цео број m је дељив са z ако и само ако је дељив са $N(z)$.

Доказ. Нека је $n=zw$ најмањи природан број дељив са z. Тада n дели $N(z)=z\bar{z}$, одакле следи да је $\bar{z}/w\in\mathbb{N}$. Како је $\bar{z}$ прост, мора бити $w=\bar{z}$, дакле $n=N(z)$. Одавде следи тврђење. □

Посматрајмо било који елемент $x\in R$ који није јединични или нула. Ако x није прост, онда постоје нејединични елементи $y,z\in R$ такви да је $yz=x$. При том је $N(y)N(z)=N(x)$ и $N(y),N(z)>1$. Дакле, $N(y),N(z)<N(x)$. Настављајући овај поступак све док је то могуће доћи ћемо до представљања $x=x_1x_2\cdots x_k$ у коме су сви елементи $x_1,x_2,\ldots,x_k$ прости. Овако смо добили:

Теорема 5. Свако $x\in R$ које није нула или јединични елемент може се представити у облику производа простих елемената. □

Теорема 6. За дати ненула елемент $z\in R$, број класа еквиваленције у R по модулу z једнак је $N(z)$.

Доказ. Нека је $R=\mathbb{Z}[\alpha]$, при чему је $\alpha^2=p\alpha+q$, $p,q\in\mathbb{Z}$. Нека је $z=a+b\alpha$ $(a,b\in\mathbb{Z})$. Ако је $b=0$ цео број, онда је $a_1+b_1\alpha\equiv a_2+b_2\alpha \pmod z$ ако и само ако $a_1\equiv a_2$ и $b_1\equiv b_2 \pmod z$. Следи да је број класа еквиваленције једнак $N(z)=z^2$.

Претпоставимо да је $b\neq 0$ и да је $(a,b)=d$. Тада је $\alpha z=(a+pb)\alpha+qb$. Како је $(a+pb,b)=d$, коефицијент уз α у xz $(x\in R)$ може бити произвољан цео број дељив са d и ниједан други. Такође, најмањи природан број дељив са z је $|(a+b\alpha)(\overline{a+b\alpha})|/d=|N(z)|/d$. Закључујемо да за свако $x\in R$ постоји јединствено $X=A+B\alpha\in R$ са $A,B\in\mathbb{Z}$, $0\leq A<|N(z)|/d$, $0\leq B<d$ такав да је $x\equiv X \pmod z$. Одавде добијамо да је тражени број класа еквиваленције једнак $|N(z)|$. □

4° Јединственост растављања на просте чиниоце.

По теореми 5, сваки елемент скупа R се може раставити на просте чиниоце. Међутим, не знамо да ли је то растављање јединствено, тј. да ли важи основна теорема аритметике, а знамо колико нам је она значајна.

Прости елементи $\mathbb{Z}$ су $\pm2,\pm3,\pm5$, итд, па разлагање на просте чиниоце у $\mathbb{Z}$ заправо није сасвим јединствено - нпр. $6=2\cdot3=(-3)(-2)$. Ипак, прости чиниоци -2 и -3 су еквивалентни бројевима 2 и 3 редом, тј. та два растављања су иста до на *редослед* и *еквивалентност* чинилаца.

Тако у случају општег интегралног домена R основна теорема аритметике (ако важи) треба да гласи овако:

ОТА (Основна Теорема Аритметике) Сваки елемент скупа R који није нула или јединичан може се написати у облику производа простих елемената. Ово разлагање је јединствено до на редослед чинилаца и еквивалентност између одговарајућих чинилаца.

Пример. Разлагања елемента $4-\omega$ у $\mathbb{Z}[\omega]$ као $(1-\omega)(3+\omega) = (-2-3\omega)(1+2\omega)$ сматрамо истим, јер је $1+2\omega = \omega(1-\omega) \sim 1-\omega$ и $-2-3\omega = -(1+\omega)(3+\omega) \sim 3+\omega$. Касније ћемо показати да ОТА важи у $\mathbb{Z}[\omega]$.

У скупу целих бројева, ОТА је последица Еуклидовог алгоритма, који је опет последица *дељења са остатком*.

Дељење са остатком у квадратном раширењу R прстена $\mathbb{Z}$ се може формулисати на следећи начин:

ДСО За свако $a, b \in R$, $b \neq 0$ постоје $p, q \in R$ такви да је $a = pb + q$ и $|N(q)| < |N(b)|$.

Овакво дељење не мора бити јединствено, и могуће га је спровести у неким (али не свим!) пољима $\mathbb{Q}[\sqrt{d}]$. Поља у којима је дељење са остатком увек изводљиво зову се *еуклидска*.

Пример. У пољу $\mathbb{Q}[\sqrt{-10}]$ ДСО не важи. Ако ставимо $a = 1+\sqrt{-10}$ и $b = 3$, ма како одабрали цео елемент p, важиће $N(a-pb) \geq N(b) = 9$ (проверите!).

Претпоставимо да се у R може делити са остатком. Нека су $a, b \in R$, $b \neq 0$. Означимо $r_0 = a$, $r_1 = b$ и за $i \geq 2$, на основу ДСО, индуктивно дефинишимо $q_i, r_i \in R$ тако да је $r_{i-2} = q_i r_{i-1} + r_i$ и $|N(r_i)| < |N(r_{i-1})|$. Постоји n тако да је $r_{n+1} = r_{n+2} = \cdots = 0$; тада је $r_n = (a, b)$. Ово је Еуклидов алгоритам у R.

Највећи заједнички делилац (НЗД) је јединствен до на еквивалентност (на пример, $(4, 6)$ може бити било који од бројева ± 2). Међутим, ако ДСО не важи у R, можемо да говоримо само о *максималном* заједничком делиоцу (МЗД).

Пример. У пољу $\mathbb{Q}[\sqrt{-2}]$ услов ДСО важи. Одредимо (a, b) за $a = 7+10\sqrt{-2}$ и $b = 8+5\sqrt{-2}$ Еуклидовим алгоритмом. Имамо $N(a) = 249$ и $N(b) = 114$.

$$\begin{array}{lll} a = 1 \cdot b + r_2, & r_2 = -1 + 5\sqrt{-2}: & N(r_2) = 51; \\ b = (1-\sqrt{-2})r_2 + r_3, & r_3 = -1 - \sqrt{-2}: & N(r_3) = 3; \\ r_2 = (-3-2\sqrt{-2})r_3, & r_4 = 0. & \end{array}$$

Према томе, $(a, b) = r_3 = -1 - \sqrt{-2}$.

Ако у Еуклидовом алгоритму елементе a, b заменимо са ac, bc ($c \in R \setminus \{0\}$), чланови низа q_i се не мењају, а сви r_i се множе са c. Одавде следи да је $(ac, bc) = cr_n = c(a, b)$.

Одавде се показује да ако је $p \in R$ прост и $a, b \in R$ такви да $p \mid ab$, онда $p \mid a$ или $p \mid b$. Заиста, ако претпоставимо супротно, имамо $p \mid (ab, ap) = a(b, p) = a$, контрадикција.

Теорема 7. Ако је у R дељење са остатком могуће, онда у R важи ОТА.

Доказ. Претпоставимо да $x \in R$ ($x \neq 0$) елемент са минималним $|N(x)|$ за који не важи ОТА. Нека је $x = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_l$, где су p_i, q_j прости елементи у R. На основу горњег разматрања, $p_1 \mid q_1 q_2 \ldots q_l \Rightarrow p_1 \mid q_j$ за неко j, тј. $q_j \sim p_1$. Скраћивањем p_1 на обе стране закључујемо да x/p_1 такође има две различите факторизације на просте чиниоце, али $|N(x/p_1)| < |N(x)|$, контрадикција. □

Постоје примери квадратних раширења у којима дељење са остатком није могуће, али ОТА ипак важи.

Пажња! ОТА није тачна у свим квадратним раширењима R.

Пример. (а) ОТА не важи у $\mathbb{Z}[\sqrt{-6}]$, јер се 6 може разложити на просте чиниоце на два начина: $6 = 2 \cdot 3 = -\sqrt{-6} \cdot \sqrt{-6}$.

(б) ОТА не важи у $\mathbb{Z}[\sqrt{-5}]$, јер се 9 може разложити на просте чиниоце на два начина: $9 = 3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5})$, али они се не сматрају истим јер $2 \pm \sqrt{-5} \not\sim 3$.

Сада ћемо доказати ОТА за неколико малих вредности d.

Теорема 8. (а) ОТА важи за $d \in \{-2, -1, 2, 3\}$.
(б) ОТА важи за $d \in \{-11, -7, -3, 5, 13\}$.

Доказ. Довољно је показати да је услов ДСО задовољен у оба случаја: посматрајмо $x, y \in R$ и покажимо да постоје $q, r \in R$ такви да је $x = qy + r$ и $|N(r)| < |N(y)|$.

(а) За дате d је $R = \mathbb{Z}[\sqrt{d}]$. Нека је $\frac{x}{y} = \alpha + \beta\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, $\alpha, \beta \in \mathbb{Q}$. Постоје цели бројеви a, b такви да је $|a - \alpha| \leq \frac{1}{2}$ и $|b - \beta| \leq \frac{1}{2}$; ставимо $q = a + b\sqrt{d}$ и $r = x - qy$. Тада је $|N(\frac{x}{y} - q)| = |(a - \alpha)^2 - d(b - \beta)^2| < 1$, одакле следи $|N(r)| = |N(y)N(\frac{x}{y} - q)| < |N(y)|$.

(б) За ове вредности d је $R = \mathbb{Z}[\tau]$, где је $\tau = \frac{-1+\sqrt{d}}{2}$. Нека је $\frac{x}{y} = \alpha + \beta\tau \in \mathbb{Q}[\sqrt{d}]$, $\alpha, \beta \in \mathbb{Q}$. Постоје цели бројеви a, b такви да је $|\nu| \leq \frac{1}{2}$ и $|\mu - \frac{1}{2}\nu| \leq \frac{1}{2}$, где је $\mu = a - \alpha$ и $\nu = b - \beta$; ставимо $q = a + b\tau$ и $r = x - qy$. Тада је $|N(\frac{x}{y} - q)| = |(\mu - \frac{1}{2}\nu)^2 - \frac{d}{4}\nu^2| < 1$, одакле следи $|N(r)| = |N(y)N(\frac{x}{y} - q)| < |N(y)|$. □

Напомена. Показује се да ДСО важи само за следеће вредности d: $-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

За $d < 0$, ОТА важи још само за $d \in \{-19, -43, -67, -163\}$. С друге стране, за позитивно d, ОТА је прилично чест феномен и, осим наведених вредности, за $d < 50$, важи и за $d \in \{14, 22, 23, 31, 38, 43, 46, 47\}$. Још је Гаус претпоставио да оваквих d има бесконачно много. Овај проблем је до данас остао нерешен.

5° Последице основне теореме аритметике.

У овом одељку претпостављамо да је d такво да у прстену целих елемената R у $\mathbb{Q}[\sqrt{d}]$ важи ОТА. Многа тврђења која важе у $\mathbb{Z}$ се лако преносе у R. За почетак, поменимо једно једноставно али важно такво тврђење.

Теорема 9. Ако су $x, y \in R$ узајамно прости и $xy = z^n$, где је $z \in R$ и $n \in \mathbb{N}$, онда су x и y еквивалентни n-тим степенима неких елемената у R. □

Још једно тврђење чији доказ користи ОТА је Кинеска теорема о остацима:

Теорема 10. Нека су $n_1, \ldots, n_k \in R$ узајамно прости по паровима и $r_1, \ldots, r_k$ произвољни елементи R. Тада постоји $x \in R$ такво да је $x \equiv r_i \pmod{n_i}$ за $i = 1, \ldots, k$. Ово x је јединствено по модулу $n_1 n_2 \ldots n_k$.

Доказ. Довољно је доказати случај $k = 2$. За произвољно k тврђење следи индукцијом.

Означимо $x_i = r_1 + in_1$; довољно је показати да је $x_i \equiv r_2 \pmod{n_2}$ за бар једно $i \in \{0, 1, \ldots, N(n_2) - 1\}$. Претпоставимо супротно. Како има тачно $N(n_2)$ класа остатака по модулу n_2, постоје различити $i, j \in \{0, 1, \ldots, N(n_2) - 1\}$ $(i > j)$ такви да је $x_i \equiv x_j \pmod{n_2}$. Тада $n_2 \mid x_i - x_j = (i - j)n_1$. На основу ОТА, због $(n_1, n_2) = 1$ следи $n_2 \mid i - j$, контрадикција. □

Сада ћемо описати све просте елементе у прстену R.

Теорема 11. Прост број $p \in \mathbb{N}$ је прост у R ако и само ако d није квадратни остатак по модулу p.

Доказ. Претпоставимо да је p сложен у R и да је $\pi = a + b\sqrt{d}$ $(a, b \in \mathbb{Q})$ његов прост делилац. По теореми 4, p је дељиво са $N(\pi)$, па је $p = \pm N(\pi) = \pm\pi\bar{\pi} = a^2 - db^2$, дакле $a^2 \equiv db^2 \pmod{p}$. Како су $2a$ и $2b$ цели бројеви, следи да је d квадратни остатак по модулу p.

Сада претпоставимо да је d квадратни остатак $\pmod{p}$. Постоји $\pi = a + b\sqrt{d}$ $(a, b \in \mathbb{Z})$ такво да $p \mid \pi\bar{\pi} = N(\pi) = a^2 - db^2$ и $p \nmid ab$. Међутим, $p \nmid \pi, \bar{\pi}$, одакле због ОТА следи да је p сложен у R. □

Последица. (а) Елемент $x \in \mathbb{Z}[i]$ је прост ако и само ако је $N(x)$ прост или је $x = \epsilon p$ за неки прост број $p \equiv 3 \pmod{4}$ и $\epsilon \in \{\pm 1, \pm i\}$.

(б) Елемент $x \in \mathbb{Z}[\omega]$ је прост ако и само ако је $N(x)$ прост или је $x = \epsilon p$ за неки прост број $p \equiv 2 \pmod{3}$ и $\epsilon \in \{\pm 1, \pm\omega, \pm\omega^2\}$.

Посматрајмо неки прост елемент $x \in R$. Елемент $\bar{x}$ је такође прост, па је $N(x) = x\bar{x}$ (јединствена) канонска факторизација броја $N(x)$.

Претпоставимо да је $N(x)$ сложен број, тј. $N(x) = mn$ за неке $m, n \in \mathbb{Z} \setminus \{-1, 1\}$. Из $x\bar{x} = mn$ следи без смањења општости да је $x \sim m$, дакле m је прост број који је такође прост као елемент R. Одавде и из теореме 11 следи:

Теорема 12. Елемент $x \in R$ је прост ако и само ако је $N(x)$ прост број или је $x \sim m$ за неки прост број m такав да је $\left(\frac{d}{m}\right) = -1$. □

Директна последица теореме 11 за $d = -1$ је Фермаова теорема о представљању простог броја $p \equiv 1 \pmod 4$ у облику збира два квадрата. Шта више:

Теорема 13. Нека ОТА важи у пољу $\mathbb{Q}[\sqrt{d}]$ и нека је p прост број са $\left(\frac{d}{p}\right) = 1$.

(а) Ако је $d \not\equiv 1 \pmod 4$, онда постоје $x, y \in \mathbb{Z}$ такви да је $x^2 - dy^2 = \pm p$.

(б) Ако је $d = 4k + 1$, $k \in \mathbb{Z}$, онда постоје $x, y \in \mathbb{Z}$ такви да је $x^2 - xy - ky^2 = \pm p$.

Доказ. По теореми 11, p је сложен у $\mathbb{Q}[\sqrt{d}]$, дељив неким простим елементом π. Норма π је прави делилац $N(p)$, дакле $N(\pi) = \pm p$, одакле следи тврђење. □

Последица. За прост број $p \equiv 1 \pmod 4$ постоје $x, y \in \mathbb{Z}$ такви да је $x^2 + y^2 = p$.

За прост број $p \equiv 1 \pmod 6$ постоје $x, y \in \mathbb{Z}$ такви да је $x^2 - xy + y^2 = p$.

За прост број $p \equiv 1, 3 \pmod 8$ постоје $x, y \in \mathbb{Z}$ такви да је $x^2 + 2y^2 = p$.

У доказу теореме 13, елемент π је једнозначно одређен до на конјуговање и множење јединичним елементом. Одавде се лако закључује нпр. да је представљање простог броја $p \equiv 1 \pmod 4$ у облику збира два квадрата јединствено.

Пример. Број $2^{2^5} + 1$ се може написати као збир два квадрата на два различита начина: као $65536^2 + 1^2 = 62264^2 + 20449^2$. Одавде следи да је он сложен.

Нажалост, наћи ова растављања није ништа лакше него факторисати број $2^{2^5} + 1$.

6° Велика Фермаова теорема за $n = 3$.

Можда најпознатија теорема која се доказује коришћењем елементарне аритметике скупа $\mathbb{Z}[\omega]$ је случај велике Фермаове теореме за експонент $n = 3$. Ово није неочекивано, с обзиром на чињеницу да се $x^3 + y^3$ растављa у $\mathbb{Z}[\omega]$ на линеарне чиниоце као

$$x^3 + y^3 = (x + y)(x + \omega y)(x + \omega^2 y) = (x + y)(\omega x + \omega^2 y)(\omega^2 x + \omega y).$$

Доказ који дајемо је дело Гауса.

Теорема 14. Једначина

$$x^3 + y^3 + z^3 = 0 \qquad (*)$$

нема нетривијалних решења у $\mathbb{Z}[\omega]$, а самим тим ни у $\mathbb{Z}$.

Доказ. Претпоставимо да за три елемента x, y, z из $\mathbb{Z}[\omega]$, различита од нуле, важи $(*)$. Јасно је да можемо да претпоставимо да су x, y, z узајамно прости по паровима.

Посматрајмо елемент $\rho = 1 - \omega$: он је прост јер је $N(\rho) = 3$. Примећујемо да је $\bar{\rho} = 1 - \omega^2 = (1 - \omega)(1 + \omega) \sim \rho$, одакле следи да, за $\alpha \in \mathbb{Z}[\omega]$, $\rho \mid \alpha$ ако и само ако $\rho \mid \bar{\alpha}$. Како је $a + b\omega \equiv a + b \pmod \rho$, сваки елемент $\mathbb{Z}[\omega]$ је конгруентан са $-1, 0$ или $1 \pmod \rho$.

Посебно је битна следећа особина броја ρ:

$$\alpha \equiv \pm 1 \pmod \rho \ (\alpha \in \mathbb{Z}[\omega]) \text{ повлачи } \alpha^3 \equiv \pm 1 \pmod{\rho^4}. \qquad (1)$$

Заиста, ако је $\alpha = \pm 1 + b\rho$, имамо $a^3 \mp 1 = (a \mp 1)(a \mp \omega)(a \mp \omega^2) = \rho^3 b(b \pm 1)(b \pm (1+\omega))$, при чему елементи b, $b \pm 1$, $b \pm (1+\omega)$ дају три различита остатка по модулу ρ, па је један од њих такође дељив са ρ што потврђује ову особину.

Међу бројевима x, y, z, (тачно) један мора бити дељив са ρ: у супротном бисмо свођењем једначине (1) по модулу ρ^4 добили $\pm 1 \pm 1 \pm 1 \equiv 0$ што није тачно. Без смањења општости, нека $\rho \mid z$. Шта више, из (1) такође закључујемо да $\rho^2 \mid z$.

Нека је $k \geq 2$ најмањи природан број за који постоји решење једначине $(*)$ у коме је $(x, y, z) = 1$ и $\rho^k \mid z$, $\rho^{k+1} \nmid z$. Посматрајмо ово решење (x, y, z).

Нека је $A = x + y$, $B = \omega x + \omega^2 y$ и $C = \omega^2 x + \omega y$. Како је $A \equiv B \equiv C \pmod{\rho}$ и $\rho \mid ABC = -z^3$, следи $\rho \mid A, B, C$, при чему је $(A, B, C) = \rho$, дакле $(\frac{A}{\rho}, \frac{B}{\rho}, \frac{C}{\rho}) = 1$. Како је $\frac{A}{\rho} \cdot \frac{B}{\rho} \cdot \frac{C}{\rho}$ потпун куб, на основу ОТА следи да су $\frac{A}{\rho}, \frac{B}{\rho}, \frac{C}{\rho}$ еквивалентни кубовима:

$$A = \rho\alpha\zeta^3, \quad B = \rho\beta\eta^3, \quad C = \rho\gamma\xi^3$$

за неке $\zeta, \eta, \xi \in \mathbb{Z}[\omega]$ узајамно просте по паровима и јединичне елементе α, β, γ. Како је $A + B + C = 0$, добијамо

$$\alpha\zeta^3 + \beta\eta^3 + \gamma\xi^3 = 0. \tag{2}$$

Пошто је $\alpha\beta\gamma$ јединични елемент и потпун куб, имамо $\alpha\beta\gamma = \pm 1$. Даље, $ABC = -z^3$ је дељиво са ρ^6 (јер $\rho^2 \mid z$), па је (тачно) један од бројева ζ, η, ξ дељив са ρ: рецимо да је то ξ. Због $\rho \nmid \zeta, \eta$, из (1) следи $\zeta^3, \eta^3 \equiv \pm 1 \pmod{\rho^4}$, што убацивањем у (2) даје $\pm\alpha \pm \beta \equiv 0 \pmod{\rho^3}$. Одавде је $\beta = \pm\alpha$, па из $\alpha\beta\gamma = \pm 1$ следи и $\gamma = \pm\alpha$. Скраћивањем α у (2) добијамо $\zeta^3 \pm \eta^3 \pm \xi^3 = 0$, што даје још једно нетривијално решење $(*)$ са $(\zeta, \eta, \xi) = 1$.

Међутим, $\rho^3\xi^3$ дели $ABC = -z^3$ што је тачно дељиво са ρ^{3k}, па је ρ^{k-1} највећи степен ρ који дели ξ, што је у контрадикцији са избором броја k. □

7° Конгруенције вишег степена.

Овде није неопходно да поље $\mathbb{Q}[\sqrt{d}]$ буде еуклидско.

Један од основних појмова је ред елемента по датом модулу. (Мала) Фермаова теорема каже да ред целог броја a по модулу простог броја p дели $p - 1$. У квадратном проширењу R прстена $\mathbb{Z}$ ово не мора да важи:

Пример. Нека је $a = i \in \mathbb{Z}[i]$ и $p = 3$. Како је $a^2 = -1$, $a^3 = -i$ и $a^4 = 1$, ред $a \pmod 3$ је 4.

Пример. Елемент $a = 2 + \sqrt{-5} \in \mathbb{Z}[i]$ нема коначан ред по модулу $p = 3$, иако је $(a, p) = 1$. Заиста, $a^2 = -1 + 4\sqrt{-5} \equiv a \pmod 3$, и зато $a^n \equiv a \pmod 3$ за све n.

Рад у скупу целих елемената у $\mathbb{Z}[\sqrt{d}]$ по модулу p значи рад у $\mathbb{Z}_p[\sqrt{d}]$. Треба да имамо у виду да, ако је d квадратни остатак по модулу p, онда и $\sqrt{d}$ лежи у пољу $\mathbb{Z}_p$, али узима две могуће вредности, па тако и елемент a има две могуће вредности у $\mathbb{Z}_p$. Ако је $N(a) \neq 0$, обе ове вредности су различите од нуле, па тако у оба случаја важи $a^{p-1} \equiv 1 \pmod p$.

Пример. У пољу $\mathbb{Z}_3$, норма елемента $a = 2 + \sqrt{-5}$ је $N(a) = 2^2 + 5 \cdot 1^2 = 0$, и зато овај елемент нема инверз нити коначан ред.

С друге стране, ако је d квадратни неостатак по модулу p, онда је $\mathbb{Z}_p[\sqrt{d}]$ поље са p^2 елемената (проверите!), што значи да имамо $p^2 - 1$ ненула елемената који сви имају инверзе у том пољу. У овом случају, мала Фермаова теорема гласи овако:

Теорема 15. Нека је p прост број и $a \neq 0$ цео елемент у $\mathbb{Q}[\sqrt{d}]$ са $p \nmid N(a)$.

(а) Ако је $\left(\frac{d}{p}\right) = 1$, онда је $a^{p-1} \equiv 1 \pmod p$.

(б) Ако је $\left(\frac{d}{p}\right) = -1$, онда је $a^{p^2-1} \equiv 1 \pmod p$.

Доказ. (б) Нека је $\{a_1, a_2, \ldots, a_{p^2-1}\}$ скуп ненула елемената поља $\mathbb{Z}_p[\sqrt{d}]$. Скуп $\{aa_1, \ldots, aa_{p^2-1}\}$ такође садржи све ненула елементе, дакле производи елемената у ова два скупа су једнаки. Следи да је $a_1 \cdots a_{p^2-1} = aa_1 \cdots aa_{p^2-1}$. Скраћивањем са $a_1 \cdots a_{p^2-1}$ добијамо $a^{p^2-1} = 1$ у пољу $\mathbb{Z}_p[\sqrt{d}]$. □

Пример. За $a = 1 + 2\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ и $p = 13$ имамо $a^2 \equiv 4\sqrt{3}$, $a^4 \equiv 9$ и $a^{12} \equiv 1 \pmod{13}$ јер је $d = 3$ квадратни остатак по модулу 13.

Пример. За $a = 1 + 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ и $p = 13$, имамо $a^{12} \equiv 8 + 8\sqrt{2}$, $a^{14} \equiv 6$ и $a^{168} \equiv 1 \pmod{13}$. Показује се да је ред a по модулу 13 једнак $168 = 13^2 - 1$ (проверите!).

Последица. Ако је $a \in \mathbb{Q}[\sqrt{d}]$ цео елемент, p прост број и $\left(\frac{d}{p}\right) = -1$, онда је $a^{p+1} \equiv b \pmod{p}$ за неко $b \in \mathbb{Z}$.

Доказ. Ако означимо $c = a^{p+1}$, на основу теореме 15 је $c^{p-1} = 1$. Како једначина $x^{p-1} = 1$ има $p - 1$ нула $1, 2, \ldots, p - 1$, она нема других нула, дакле $c \in \{1, \ldots, p-1\}$ у $\mathbb{Z}_p[\sqrt{2}]$.

Да бисмо заокружили рад са модулима, треба да испитамо и сложене модуле, пре свега модуле облика p^k за прост број p и $k \in \mathbb{N}$. Следећег важног тврђења се сећамо из теорије конгруенција вишег степена - оно важи и у квадратним проширењима; доказ је потпуно исти и овде га стављамо само ради лакшег читања.

Теорема 16. Нека је p природан прост број, a цео елемент у $\mathbb{Q}[\sqrt{d}]$ и $n, k \in \mathbb{N}$, $l \in \mathbb{N}_0$. Ако $p^k \parallel a - 1$ и $p^l \parallel n$, онда $p^{k+l} \parallel a^n - 1$.

Доказ. Имамо $a = p^k B + 1$ за неко цело $B \in \mathbb{Q}[\sqrt{d}]$ које није дељиво са p. Тада је по биномној формули

$$a^n - 1 = (1 + p^k B)^n - 1 = np^k B + \binom{n}{2} p^{2k} B^2 + \cdots + p^{nk} B^n. \qquad (*)$$

Тврђење показујемо индукцијом по l. За $l = 0$ и $l = 1$, очигледно су сви сабирци на десној страни $(*)$ осим првог дељиви са p^{k+l+1}, док је први тачно дељив са p^{k+l}, одакле следи $p^{k+l} \parallel a^n - 1$.

Нека је $l = t > 1$. На основу случаја $l = 1$ важи $p^{k+1} \parallel a^p - 1$. Пошто $p^{t-1} \parallel N = n/p$, по индуктивној претпоставци за $l = t - 1$ примењеној на $A = a^p$ и N имамо $p^{(k+1)+(t-1)} \parallel A^N - 1$, тј. $p^t \delta \mid n$. □

Последица 1. Ако је ред $a \pmod{p}$ једнак δ и $p^k \parallel a^\delta - 1$, онда је ред $a \pmod{p^{k+l}}$ једнак $p^l \delta$.

Доказ. Следи из теореме 16 примењене на a^δ. □

Случај $p = 2$ се мало разликује од одговарајућег случаја за целе бројеве. Разлог је што у квадратном проширењу не мора да важи $2 \mid a - 1$ ако је $(a, 2) = 1$.

Пример. У $\mathbb{Q}[\sqrt{10}]$, за $a = \sqrt{10}$, $(a, 2) = 1$, али $2 \mid a^n$ за све целе $n > 1$.

У $\mathbb{Q}[\sqrt{2}]$, за $a = 1 + \sqrt{2}$, важи $2^1 \parallel a^2 - 1$ и $2^2 \parallel a^4 - 1$, што се опет никад не дешава у $\mathbb{Z}$.

И овде у доказу морамо да будемо пажљиви, јер не захтевамо да 2 буде прост у $\mathbb{Q}[\sqrt{d}]$, па тако из $2^x \parallel \xi$ и $2^y \parallel \eta$ не смемо да закључимо $2^{x+y} \parallel \xi\eta$.

Теорема 17. Нека је a цео елемент у $\mathbb{Q}[\sqrt{d}]$ такав да $2^k \parallel a - 1$ за неко $k \in \mathbb{N}$, $k \geq 2$. Тада за свако цело $l \geq 0$, $2^{k+l} \mid a^n - 1$ ако и само ако $2^l \mid n$.

Доказ. Нека је $a - 1 = 2^k b$ за цео елемент b, $2 \nmid b$. Показујемо индукцијом по l да је $a^n - 1 = 2^{k+l}(2r + b)$ за неки цео елемент r ако $2^l \parallel n$.

Почињемо од случаја $l = 0$. Тада је $a^n - 1 = (a-1)((2^k b + 2)(a^{n-2} + a^{n-4} + \cdots + a) + 1) = 2^k b(2c + 1) = 2^k(2bc + b)$ за неки цео елемент c.

Претпоставимо да тврђење важи за $l - 1$ ($l \in \mathbb{N}$) и нека $2^l \parallel n$. По индукцијској претпоставци је $a^{\frac{n}{2}} - 1 = 2^{k+l-1}(2r + b)$ за неко r, па праволинијским сређивањем добијамо $a^n - 1 = (a^{\frac{n}{2}} - 1)(a^{\frac{n}{2}} - 1) = 2^{k+l-1}(2r + b)(2^{k+l-1}(2r + b) + 2) = 2^{k+l}(2r' + b)$, где је $r' = 2^{k+l-3}(2r + b)^2 + r$. Индукција је готова. □

8° **Примена на линеарне рекурентне низове другог реда.**

Нека је (a_n) низ целих бројева који задовољава рекурентну везу другог реда $a_{n+1} = ba_n - ca_{n-1}$, где су $b, c \in \mathbb{Z}$. Знамо да је низ a_n периодичан по простом модулу p под претпоставком да $p \nmid c$ (зашто?). То значи да постоји $n > 0$ за које $p \mid a_n$. Осим тога, једноставна индукција нам даје $a_{n+k} \equiv ca_k \pmod{p}$ за свако k, где је $c \in \mathbb{Z}$ такав да је $a_{n+1} \equiv ca_1 \pmod{p}$. Одавде лако закључујемо да $p \mid a_m$ ако и само ако $n \mid m$.

Ако је $d = b^2 - 4c \neq 0$, нуле $a, \bar{a}$ карактеристичног полинома $P(x) = x^2 - bx + c$ су цели елементи поља $\mathbb{Q}[\sqrt{d}]$. Општи члан низа има облик $a_n = k_1 a^n + k_2 \bar{a}^n$ за неке константе $k_1, k_2 \in \mathbb{Q}[\sqrt{d}]$. Директно се добија $k_1 = \frac{a_1 - \bar{a}a_0}{a - \bar{a}}$ и $k_2 = \frac{aa_0 - a_1}{a - \bar{a}}$. Како је $a - \bar{a} = 2\sqrt{d}$, имамо $p \nmid a - \bar{a}$, дакле k_1 и k_2 су добро дефинисани по модулу p.

Теорема 18. Нека низ целих бројева a_n задовољава релацију $a_{n+1} = ba_n - ca_{n-1}$ $(b, c \in \mathbb{Z})$ и нека је $p > 2$ прост број. Означимо $d = b^2 - 4c$.
(а) За $p \nmid d$, период низа (a_n) по модулу p дели $p^2 - 1$.
(б) Ако $p \mid a_0$, онда $p \mid a_{p-(\frac{d}{p})}$.

Доказ. (а) По теореми 15 важи $a^{n+p^2-1} \equiv a^n$ и $\bar{a}^{n+p^2-1} \equiv \bar{a}^n$. Из горњих формула за a_n, k_1, k_2 одмах следи да је $a_{n+p^2-1} \equiv a_n \pmod{p}$.

(б) Због $k_1 + k_2 = a_0 \equiv 0 \pmod{p}$ важи $a_n = k_1 a^n + k_2 \bar{a}^n \equiv k_1(a^n - \bar{a}^n) \pmod{p}$.

- Ако је $(\frac{d}{p}) = 1$, по теореми 15 је $a^{p-1} \equiv \bar{a}^{p-1} \equiv 1 \pmod{p}$, дакле $p \mid a_{p-1}$.
- Ако је $(\frac{d}{p}) = -1$, по последици теореме 15 је $a^{p+1} \equiv b \pmod{p}$ за неки цео број b; такође $\bar{a}^{p+1} \equiv b$, дакле $a_{p+1} \equiv 0 \pmod{p}$.
- Најзад, ако $(\frac{d}{p}) = 0$, тј. $p \mid d$, важи $x^2 - bx + c \equiv (x - \frac{b}{2})^2$ и једноставна индукција даје $a_n \equiv na_1(\frac{b}{2})^{n-1}$, дакле $a_p \equiv 0 \pmod{p}$. □

Пример. Фибоначијев низ F_n је дат са $F_0 = 0$, $F_1 = 1$ и $F_{n+1} = F_n + F_{n-1}$ за све n. По теореми 18, прост број $p \neq 5$ дели $F_{p-(\frac{5}{p})}$, што доказује тврђење које нам је познато: $p \mid F_{p+1}$ за $p \equiv \pm 2 \pmod{5}$ и $p \mid F_{p-1}$ за $p \equiv \pm 1 \pmod{5}$.

Теореме 16 и 17 могу да нам кажу понешто о дељивости a_n степеном простог броја - видети нпр. задатак 19.

9° **Мало о општим алгебарским проширењима.**

Степен алгебарског броја α је степен његовог минималног полинома.

Да бисмо направили проширење поља $\mathbb{Q}$ алгебарским бројем α степена већег од 2, није довољно да посматрамо само бројеве облика $a + b\alpha$ $(a, b \in \mathbb{Q})$.

Дефиниција. Нека је α алгебарски број степена n. *Проширење поља* $\mathbb{Q}$ *елементом* α је скуп $\mathbb{Q}[\alpha]$ свих комплексних бројева облика $c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$ $(c_i \in \mathbb{Q})$, са свим операцијама наслеђеним из скупа $\mathbb{C}$. *Степен* проширења је степен n полинома $p(x)$.

Као и у квадратним проширењима, целим елементима поља $\mathbb{Q}[\alpha]$ проглашавамо оне елементе који су алгебарски цели. Скуп целих елемената у пољу је интегрални домен.

У проширењима произвољног коначног степена могу се дефинисати конјугати и норма. Међутим, конјугат датог елемента у општем случају није јединствен. За два алгебарска поља кажемо да су конјуговани кад год имају исти (монични) минимални полином. Једна од неколико еквивалентних дефиниција норме је следећа:

Дефиниција. Нека је $\mathbb{F}$ проширење поља $\mathbb{Q}$ степена n, и $\xi \in \mathbb{F}$. Ако су $\xi = \xi_1, \xi_2, \ldots, \xi_d$ сви конјугати ξ, *норма* елемента ξ се дефинише као $N(\xi) = (\xi_1\xi_2 \cdots \xi_d)^{n/d}$.

Показује се да $d \mid n$, па је норма целог елемента проширења увек цео број. Као и у квадратним проширењима, норма је мултипликативна: $N(\xi\eta) = N(\xi)N(\eta)$.

Пример. Поље $\mathbb{F} = \mathbb{Q}[\sqrt[3]{2}]$ је степена 4. Минимални полином елемента $\xi = 1 + \sqrt[3]{2}$ је $x^3 - 3x^2 + 3x - 3 = 0$, а његови коњугати су $\xi_1 = \xi$, $\xi_2 = 1 + \omega\xi$ и $\xi_3 = 1 + \omega^2\xi$ (приметимо да су $\xi_2, \xi_3 \notin \mathbb{F}$). Норма $N(\xi)$ је $\xi_1\xi_2\xi_3 = 3$.

Једини коњугат елемента $\eta = 2$ у $\mathbb{F}$ је он сам: $\eta_1 = 2$. Дакле, $N(\eta) = \eta_1^3 = 8$.

Означимо са R скуп целих елемената раширења $\mathbb{F}$ поља $\mathbb{Q}$. Сваки елемент $x \in R$ одредјује тзв. идеал $I = xR = \{xy \mid y \in R\}$ прстена R.

Дефиниција. Подскуп I интегралног домена R је *идеал* ако, за све $x, y \in I$ и $a \in R$, елементи $x + y$ и ax такође припадају I.

У прстенима R попут $\mathbb{Z}$ и $\mathbb{Z}[i]$, једини идеали су они облика xR, где је $x \in R$. Овакве прстене зовемо *главноидеалским доменима*.

Норма идеала I је број класа еквиваленције R/I, ако је овај број коначан. Норма идеала xR је управо $N(x)$.

Показује се да су главноидеалски домени увек еуклидски. Ипак, у општем случају, интегрални домен не мора да буде главноидеалски.

Пример. У прстену $R = \mathbb{Z}[\sqrt{-5}]$, скуп $I = \{3a + (2 + \sqrt{-5})b \mid a, b \in \mathbb{Z}\}$ је идеал норме 3. Овај идеал није облика xR ни за једно $x \in R$, јер у R нема елемената норме 3.

Идеали прстена R се могу множити као и његови елементи. Наиме, ако су I и J идеали, производ IJ је идеал који се дефинише као $\{xy \mid x \in I, y \in J\}$. Овако и међу идеалима можемо увести релацију дељивости, и она је компатибилна са већ уведеном дељивошћу за елементе: идеал xR дели идеал yR ако и само ако $x \mid y$. У складу са дељивошћу, уводимо и *просте* идеале као оне који се не могу написати као производи два идеала различита од R.

Испоставља се да се посматрањем идеала уместо елемената скуп R донекле може превазићи недостатак ОТА:

Теорема. Сваки идеал прстена R се растављa на производ простих идеала на јединствен начин, до на редослед.

Пример. Видели смо да у скупу R целих елемената у $\mathbb{Q}[\sqrt{5}]$ број $9 = 3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5})$ има две нееквивалентне канонске факторизације. Ипак, посматран као идеал $9R$, он има јединствену факторизацију на просте идеале: $9 = \mathfrak{p}^2\mathfrak{q}^2$, где је $\mathfrak{p} = \langle 3, 2 + \sqrt{-5}\rangle$ и $\mathfrak{q} = \langle 3, 2 - \sqrt{-5}\rangle$. Као идеали, елементи $2 \pm \sqrt{-5}$ и 3 су сложени, јер је $2 + \sqrt{-5} = \mathfrak{p}^2$, $2 - \sqrt{-5} = \mathfrak{q}^2$ и $3 = \mathfrak{pq}$.

10° Задаци

1. Доказати да не постоје $m, n \in \mathbb{Z}$ такви да је $(3 + i)^m = (7 + i)^n$.

   Решење. Ако такви m и n постоје, онда је $10^m = N((3 + i)^m) = N((7 + i)^n) = 50^n$, што је немогуће.

2. Одредити све парове (x, y) елемената из $\mathbb{Z}[\sqrt{2}]$ за које је $\frac{1}{x} + \frac{1}{y} = 2$.

   Решење. Дата једначина је еквивалентна са $(2y - 1)(2x - 1) = 1$. Према томе, елемент $2x - 1$ јединичан у $\mathbb{Z}[\sqrt{2}]$. Знамо да су сви јединични елементи у $\mathbb{Z}[\sqrt{2}]$ облика $\pm(1 + \sqrt{2})^n$, дакле $2x - 1 = \pm(1 + \sqrt{2})^n$ и $2y - 1 = \pm(1 + \sqrt{2})^{-n}$ за неко $n \in \mathbb{Z}$. Да би x и y били цели елементи, још је потребно да буде $a + b\sqrt{2} = (1 + \sqrt{2})^n \equiv 1 \pmod 2$, тј. $a \equiv 1$ и $b \equiv 0 \pmod 2$, што важи ако и само ако $n = 2k$ за неко $k \in \mathbb{Z}$.

3. Нека су x, y цели елементи неког квадратног раширења $\mathbb{Q}$ такви да је $N(x) = 1$ и $N(y) = 2$. Ако је $N(x + y) > 0$, наћи најмању могућу вредност $N(x + y)$.

   Решење. Означимо $x = x_1 + x_2\sqrt{d}$ и $y = y_1 + y_2\sqrt{d}$. Имамо $N(x + y) = (x_1 + y_1)^2 - d(x_2 + y_2)^2 = N(x) + N(y) + 2(x_1y_1 - dx_2y_2)$. Како је $(x_1y_1 - dx_2y_2)^2 = N(x)N(y) +$

$d(x_1y_2 - x_2y_1)^2 \geq N(x)N(y)$, следи $N(x+y) \geq (N(x)^{1/2} + N(y)^{1/2})^2 = (\sqrt{2}+1)^2 > 5$ или $N(x+y) \leq (N(x)^{1/2} - N(y)^{1/2})^2 = (\sqrt{2}-1)^2 < 1$. Друга могућност отпада, па мора да буде $N(x+y) \geq 6$.

Ако је $N(x+y) = 6$, из горњих једнакости добијамо $x_1y_1 - dx_2y_2 = \frac{3}{2}$ и $(x_1y_2 - x_2y_1)^2 = \frac{1}{4d}$, што није могуће јер d није дељиво квадратом. Према томе, $N(x+y) \geq 7$.

Минимална вредност $N(x+y)$ је 7, и достиже се нпр. у $\mathbb{Q}[\sqrt{2}]$ за $x = 1$ и $y = 2 - \sqrt{2}$.

4. Показати на примеру да максимални заједнички делилац два елемента $x, y \in R$ не мора да буде јединствен до на еквивалентност ако у R не важи ОТА.

   Решење. Нека је $x = 9$ и $y = 6 + 3\sqrt{-5}$ у $\mathbb{Z}[\sqrt{-5}]$. Оба елемента имају норму 81 и нису еквивалентни, па њихов МЗД има норму $1, 3, 9$ или 27. У $\mathbb{Z}[\sqrt{-5}]$ нема елемената норме 27. С друге стране, постоје два нееквивалентна елемента норме 9 који деле x и y: то су 3 и $2 + \sqrt{-5}$, и сваки од њих је МЗД елемената x, y.

5. Нека је a цео број и $n = a^4 + a^2 - 1$. Одредити (бар један) максимални заједнички делилац елемената $x = a + \sqrt{n}$ и $y = 1 + a\sqrt{n}$ у пољу $\mathbb{Q}[\sqrt{n}]$.

   Решење. Нека је $d = (x, y)$. Како је $N(d) \mid N(x) = -(a^4 - 1)$ и $d \mid ax - y = a^2 - 1$, одакле $N(d) \mid (a^2-1)^2$, следи $N(d) \mid a^2 - 1$.

   Елемент $\delta = a^2 - \sqrt{n}$ има норму $-(a^2-1)$ и дели x и y, па је то МЗД елемената x и y.

6. Показати на примеру да Кинеска теорема о остацима не мора да важи у квадратном проширењу $\mathbb{Z}$ у коме не важи ОТА.

   Решење. Сетимо се да у прстену $\mathbb{Z}[\sqrt{-5}]$ не важи ОТА јер је $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, иако су 3 и $\pi = 2 + \sqrt{-5}$ нееквивалентни прости елементи.

   Покажимо да не постоји $x \in \mathbb{Z}[\sqrt{-5}]$ такво да је $x \equiv 0 \pmod{\pi}$ и $x \equiv 1 \pmod{3}$. Претпоставимо да такво x постоји: тада је $x = (3m+1) + 3n\sqrt{-5}$ за неке $m, n \in \mathbb{Z}$. Ако $\pi \mid x$, онда $\pi \mid x - 3n\pi = 3(m - 2n) + 1$. Како $\pi \mid 9$, следи да $\pi \mid (3(m-2n)+1, 9) = 1$, контрадикција.

7. Нека су α, β, x цели елементи у $\mathbb{Q}[\sqrt{d}]$. Ако $\alpha \mid x$, $\beta \mid x$ и $(N(\alpha), N(\beta)) = 1$, доказати да $\alpha\beta \mid x$.

   Решење. Елемент $y = m + n\sqrt{d} = \bar{\beta}x/\alpha$ је цео. По услову задатка, $N(\beta) = b \mid \alpha y$, а треба показати да $b \mid y$. Стављајући $\alpha = p + q\sqrt{d}$, имамо $b \mid \alpha y = (pm + dqn) + (pn + qm)\sqrt{d}$, дакле b дели $pm + dqn$ и $pn + qm$. Одавде b дели $p(pn+qm) - q(pm+dqn) = n(p^2 - dq^2) = nN(\alpha)$. Како је $(b, N(\alpha)) = 1$, следи да $b \mid n$. Слично, из $b \mid p(pm+dqn) - dq(pn+qm) = m(p^2 - nq^2)$ следи да $b \mid m$. Према томе, $b \mid y$.

8. Нека је p прост број и $N = \prod_{k=1}^{p-1}(k^2+1)$. Одредити остатак N при дељењу са p.

   Решење. Означимо $P(x) = (1+x)(2+x)\ldots(p-1+x)$. Познато нам је да важи $P(x) = x^{p-1} - 1 + pQ(x)$ за неки полином $Q(x)$ са целобројним коефицијентима.

   С друге стране, како је $k^2 + 1 = (k+i)(k-i)$ за свако k, одмах видимо да је

   $$N = P(i)P(-i) = \left(i^{p-1} - 1 + pQ(i)\right)\left((-i)^{p-1} - 1 + pQ(-i)\right) \equiv \begin{cases} 4, & \text{ако } p \equiv 3 \pmod{4}; \\ 0, & \text{иначе.} \end{cases}$$

9. Нека је $p \equiv 3 \pmod{4}$ прост број. Доказати да је бројилац разломка $\sum_{k=0}^{p-2} \frac{1}{k^2+1}$ дељив са p (нпр. за $p = 7$, $\frac{1}{1} + \frac{1}{2} + \frac{1}{5} + \frac{1}{10} + \frac{1}{17} + \frac{1}{26} = \frac{4193}{2210}$, $7 \mid 4193$).

   Решење. Посматрајмо $S = \sum_{k=0}^{p-1} \frac{1}{k^2+1}$. Како је $\frac{2i}{k^2+1} = \frac{1}{k-i} - \frac{1}{k+i}$, имамо $2iS \equiv f(-i) - f(i)$, где је $f(x) = \sum_{k=0}^{p-1} \frac{1}{x+k}$. Даље је $\frac{1}{x+k} = \frac{(x+k)^{p-1}-1}{(x+k)^p - (x+k)} \pmod{p}$, при чему је $(x+k)^p - (x+k) \equiv x^p - x \pmod{p}$ за све k. Према томе, $f(x) \equiv \frac{1}{x^p - x} \sum_{k=0}^{p-1}((x+k)^{p-1} - 1)$.

Полином $\sum_{k=0}^{p-1}((x+k)^{p-1}-1)$ је степена $\leq p-1$ и узима вредност $-1 \pmod p$ за све $x \in \{0,1,\ldots,p-1\}$, дакле идентички је једнак -1 по модулу p. Закључујемо да је $f(x) \equiv -\frac{1}{x^p-x} \pmod p$.

Сада је $2iS \equiv f(-i) - f(i) = -\frac{1}{(-i)^p+i} + \frac{1}{i^p-i} = -\frac{1}{i}$, па најзад добијамо $S \equiv \frac{1}{2} \pmod p$, одакле следи тврђење.

10. Претпоставимо да су x, y, z природни бројеви такви да је $xy = z^2+1$. Доказати да постоје цели бројеви a, b, c, d такви да је $x = a^2+b^2$, $y = c^2+d^2$ и $z = ac+bd$.

Решење. Користићемо следеће важно помоћно тврђење: ако су $m, n, p, q \in \mathbb{Z}[i]$ за које је $mn = pq$, онда постоје $u_1, u_2, v_1, v_2 \in \mathbb{Z}[i]$ такви да је $m = u_1v_1$, $n = u_2v_2$, $p = u_1v_2$, $q = u_2v_1$. Доказ овог тврђења је исти као у случају $m, n, p, q \in \mathbb{Z}$, и следи директно из растављања m, n, p, q на просте чиниоце.

Како је $xy = z^2+1 = (z+i)(z-i)$, помоћно тврђење нам даје

$$x = u_1v_1, \quad y = u_2v_2, \quad z+i = u_1v_2, \quad z-i = u_2v_1 \tag{1}$$

за неке $u_1, u_2, v_1, v_2 \in \mathbb{Z}[i]$. Нека је $u_1 = a+bi$ и $u_2 = c+di$ $(a, b, c, d \in \mathbb{Z}$. Због $u_1 \mid z+i$ важи $(a, b) = 1$, па како је $u_1v_1 \in \mathbb{N}$, следи да је $v_1 = q\bar{u_1}$ за неко $q \in \mathbb{N}$. Даље, из $u_1v_2 = \overline{u_2v_1}$ следи $v_2 = q\bar{u_2}$. Најзад, из $q \mid z+i = qu_1\bar{u_2}$ добијамо $q = 1$. Сада једнакости у (1) постају $x = u_1\bar{u_1} = a^2+b^2$, $y = c^2+d^2$ и $z = ac+bd$.

11. Доказати да за свако природно $n \geq 3$ постоје јединствени непарни природни бројеви x, y такви да је $x^2+7y^2 = 2^n$.

Решење. У пољу $\mathbb{Q}[\sqrt{-7}]$ услов $x^2+7y^2 = 2^n$ се може написати као $N(x+y\sqrt{-7}) = 2^n$. У овом пољу имамо цео елемент $\alpha = \frac{1+\sqrt{-7}}{2}$ норме 2. Пошто је α^n цео елемент за свако n, имамо $2\alpha^n = x_n + y_n\sqrt{-7}$ за неке целе x_n, y_n и $N(2\alpha^n) = x_n^2 + 7y_n^2 = 2^{n+2}$; због $\alpha \equiv 1 \pmod{\bar\alpha}$ је $\alpha^n \equiv \alpha \pmod{\alpha\bar\alpha = 2}$, одакле следи да $2 \nmid \alpha^n$, па су x_n, y_n непарни.

Остаје да покажемо јединственост. Довољно је доказати индукцијом по n да, ако је $\zeta \in \mathbb{Q}[\sqrt{-7}]$ цео елемент са $2 \nmid \zeta$ и $N(\zeta) = 2^n$, онда је $\zeta \in \{\pm\alpha^n, \pm\bar\alpha^n\}$. То је тачно за $n = 1$. Претпоставимо да важи за $n-1$ и покажимо га за n. Како је $\zeta \equiv \alpha$ или $\bar\alpha \pmod 2$, сматраћемо без смањења општости да је $\zeta \equiv \alpha \pmod 2$. Тада $\alpha \mid \zeta$ и $\frac{\zeta}{\alpha} \equiv 1 \pmod{\bar\alpha}$, тј. $\frac{\zeta}{\alpha} = 1+\bar\alpha\beta$ за неки цео елемент β. Тада је $2^{n-1} = N(\frac{\zeta}{\alpha}) = (1+\bar\alpha\beta)(1+\alpha\bar\beta)$. Видимо да је $\alpha \mid \beta$ немогуће, јер би онда било $1+\alpha\bar\beta \equiv 1+\bar\alpha\beta \equiv 1 \pmod 2$ и отуда $2^{n-1} \equiv 1 \pmod 2$. Дакле, $\beta \equiv 1 \pmod\alpha$ и одатле $\frac{\zeta}{\alpha} \equiv 1+\bar\alpha \equiv \alpha \pmod 2$. По индуктивној претпоставци закључујемо да је $\frac{\zeta}{\alpha} = \pm\alpha^{n-1}$, и доказ је завршен.

12. Наћи све природне бројеве m, n за које је $(1+i)^m + (2+i)^n = -1$.

Решење. За $m \leq 5$ једино решење је $(m, n) = (5, 2)$.

Нека је $m \geq 6$. Тада $(1+i)^6 \sim 8 \mid (2+i)^n + 1$. Поредак броја $2+i$ по модулу 8 је 4 јер је $(2+i)^4 = -7+24i \equiv 1 \pmod 8$, па мора бити $n \equiv 2 \pmod 4$, а то није могуће јер је тада $(2+i)^n \equiv (2+i)^2 = 3+4i \not\equiv -1 \pmod 8$.

13. Решити једначину $x^5 - 1 = y^2$ у скупу целих бројева.

Решење. Дата једначина се може написати у облику $x^5 = (y+i)(y-i)$. Приметимо да x није паран број, јер бисмо у супротном имали $y^2 \equiv -1 \pmod 4$. Такође следи да је y парно, одакле добијамо да су елементи $y+i$ и $y-i$ узајамно прости у $\mathbb{Z}[i]$. Како је $(y+i)(y-i)$ пети степен, следи да су $y+i$ и $y-i$ оба пети степени (зашто?). Нека су $a, b \in \mathbb{Z}$ такви да је $y+i = (a+bi)^5 = a(a^4 - 10a^2b^2 + 5b^4) + b(5a^4 - 10a^2b^2 + b^4)i$. Важи $b(5a^4 - 10a^2b^2 + b^4) = 1$, па је $b = \pm1$. Лако се проверава да је у оба случаја $a = 0$, а самим тим и $y = 0$, $x = \pm1$, једино решење.

14. Наћи сва целобројна решења једначине $x^2 + 2 = y^3$.

Решење. Напишимо дату једначину у облику $(x+\sqrt{-2})(x-\sqrt{-2}) = y^3$. Ако је x парно, онда $y^3 \equiv 2 \pmod 4$, што је немогуће; следи да је x непарно. Тада су $x+\sqrt{-2}$ и

$x-\sqrt{-2}$ узајамно прости елементи $\mathbb{Z}[\sqrt{-2}]$ чији је производ потпун куб, па на основу ОТА у $\mathbb{Z}[\sqrt{-2}]$ закључујемо да су $x+\sqrt{-2}$ и $x-\sqrt{-2}$ потпуни кубови. Дакле, постоје $a,b\in\mathbb{Z}$ такви да је $(a+b\sqrt{-2})^3 = x+\sqrt{-2}$. Изједначавањем коефицијената уз $\sqrt{-2}$ добијамо $b(3a^2-2b^2)=1$, одакле је $b=1$ и $a=\pm 1$. Сада лако добијамо $x=\pm 5$ и $y=3$, што је и једино целобројно решење постављене једначине.

15. Наћи сва целобројна решења једначине $u^3-2v^3=1$.

Решење. Како је $(2u^3-1)^2 = 4u^3(u^3-1)+1 = (2uv)^3+1$, дату једначину сводимо на $x^2=y^3+1$, где је $x=2u^3-1$ и $y=2uv$. Посматраћемо ову једначину у $\mathbb{Z}[\omega]$. Имамо $x^2=(y+1)(y+\omega)(y+\omega^2)$. Приметимо да је $(y+1,y+\omega)=(y+\omega,y+\omega^2)=(y+\omega^2,y+1)=d\mid 1-\omega$.

Претпоставимо да је $d=1-\omega$ и означимо $y+\omega=(1-\omega)z$. Наша једначина се своди на $z(z+1)(z+\omega^2)=(1-\omega)t^2$. Како је $(z,(z+1)(z+\omega^2))=1$, z је еквивалентно елементу облика m^2 или $(1-\omega)m^2$, $m\in\mathbb{Z}[\omega]$. Како су ω и ω^2 и сами квадрати, следи да је $y+\omega=\pm r^2$ или $y+\omega=\pm(1-\omega)r^2$ за неко r.

(i) $y+\omega=\pm r^2$. Ако ставимо $r=a+b\omega$ $(a,b\in\mathbb{Z})$, добијамо $(a^2-b^2)+(2ab-b^2)\omega=\pm(y+\omega)$, одакле је $y=a^2-b^2$ и $2ab-b^2=\pm 1$. Према томе, $b=\pm 1$ и $a\in\{0,b\}$, што нам даје $y=-1$ или $y=0$. Одавде добијамо решења $(u,v)=(1,0)$.

(ii) $y+\omega=\pm(1-\omega)r^2$. Ако ставимо $r=a+b\omega$ $(a,b\in\mathbb{Z})$, добијамо $(a^2+2ab-2b^2)+(4ab-a^2-b^2)\omega=\pm(y+\omega)$; између осталог, $4ab-a^2-b^2=\pm 1$, али ова једначина нема решења по $a,b\in\mathbb{Z}$. У овом случају полазна једначина нема решења.

Нека је сада $d=1$. Број x^2 је производ три чиниоца узајамно проста по паровима, па је сваки од чинилаца еквивалентан квадрату у $\mathbb{Z}[\omega]$. Опет следи $y+\omega=\pm r^2$ за неко $r\in\mathbb{Z}[\omega]$. Настављамо као у претходном случају и не добијамо нова решења.

Према томе, једино решење је $(u,v)=(1,0)$.

16. Наћи сва целобројна решења (x,y) једначине $y^2=\frac{1}{3}x^4+x^2+1$.

Решење. Пошто $3\mid x$, ставимо $x=3x_1$; једначина постаје $y^2=27x_1^4+8x_1^2+1$. Множењем са 3 добијамо $3y^2=(9x_1^2+1)^2+(9x_1^2+1)+1=\frac{(9x_1^2+1)^3-1}{9x_1^2}$, што за $z=9x_1^2+1$ и $t=3x_1y$ постаје $z^3=3t^2+1$. Десна страна се факторише у $\mathbb{Z}[\omega]$.

Имамо $z^3=(1+t+2t\omega)(1-t-2t\omega)$, при чему је $(1+t+2t\omega,1-t-2t\omega)=(1+t+2t\omega,2)\mid 2$. Приметимо да је 2 прост у $\mathbb{Z}[\omega]$ и да $2\nmid 1+t$, јер би у супротном било $z^3=3t^2+1\equiv 4 \pmod 8$ што није могуће. Следи да су $1+t+2t\omega$ и $1-t-2t\omega$ узајамно прости, а њихов производ је куб, дакле $1+t+2t\omega=\epsilon(a+b\omega)^3$, где су $a,b\in\mathbb{Z}$ и ϵ је јединични елемент. Не умањујући општост, претпостављамо да је $\epsilon\in\{1,\omega\}$.

За $\epsilon=1$ добијамо $1+t+2t\omega=a^3-3ab^2+b^3+3(a^2b-ab^2)\omega$, одакле је $2=2(1+t)-2t=2(a^3-3ab^2+b^3)-6(a^2b-ab^2)=(a+b)(a-2b)(2a-b)$. Лако се добија да је једино решење $(a,b)=(1,0)$ и $(z,t)=(1,0)$, дакле $(x,y)=(0,\pm 1)$.

За $\epsilon=\omega$ слично добијамо $a^3+b^3+3a^2b-6ab^2=-2$. Одавде је, међутим, $(a+b)^3\equiv -2 \pmod 9$, што је немогуће.

17. Доказати да се свако $n\in\mathbb{N}$ може представити у облику $n=\dfrac{x}{2y^2-x^2}$, где су $x,y\in\mathbb{N}$.

Решавањем квадратне једначине по x, услов $n=\frac{x}{2y^2-x^2}$ постаје $(2nx+1)^2-8n^2y^2=1$; према томе, $(u,v)=(2nx+1,2ny)$ је решење Пелове једначине $u^2-2v^2=1$. Сва решења (u,v) задовољавају $u+v\sqrt{2}=(3+2\sqrt{2})^k$ за неко $k\in\mathbb{N}$. Довољно је доказати да постоји решење (u,v) у коме је $u\equiv 1$ и $v\equiv 0 \pmod{2n}$, тј. да постоји k за које је $(3+2\sqrt{2})^k=u+v\sqrt{2}\equiv 1 \pmod{2n}$. Овакво k постоји на основу теореме 15.

Пример. За $n=9$, најмање решење је $(x,y)=(42\,688\,800, 30\,185\,540)$.

18. Нека је $q>5$ прост број и p прост делилац Фибоначијевог броја F_q. Доказати да је $p\equiv\pm 1 \pmod q$.

Решење. По Бинеовој формули је $F_q = \frac{1}{\sqrt{5}}(\phi^q - (-\frac{1}{\phi})^q) = \frac{1}{\phi^q\sqrt{5}}(\phi^{2q}+1)$, где је $\phi = \frac{1+\sqrt{5}}{2}$ цео у $\mathbb{Q}[\sqrt{5}]$. Према томе, поредак ϕ по модулу p дели $4q$, а не дели $2q$, дакле једнак је $4q$. По теореми 15 следи да $4q \mid p^2-1$, одакле следи тврђење.

19. Низ природних бројева (a_n) је дефинисан са $a_0 = 0$, $a_1 = 1$ и $a_n = 2a_{n-1} + a_{n-2}$ за $n > 1$. Доказати да, за сваки природан број k, $2^k \mid a_n$ ако и само ако $2^k \mid n$.

Решење. Директно се добија општи члан: $a_n = \frac{1}{2\sqrt{2}}((1+\sqrt{2})^n - (1-\sqrt{2})^n) = \frac{\alpha^{2n}-(-1)^n}{2\sqrt{2}\alpha^n}$, где је $\alpha = 1+\sqrt{2}$. Лако се показује да је a_n парно ако и само ако је n парно. Надаље претпостављамо да је $k \geq 2$; тада је $2 \mid n$. Из формуле за a_n следи да $2^k \mid a_n$ ако и само ако $2^{k+1} \mid \alpha^{2n} - 1$. Како $2^2 \parallel \alpha^4 - 1 = 16 + 12\sqrt{2}$, по теореми 17 ово важи ако и само ако $2^{k-1} \mid n/2$, тј. $2^k \mid n$.

20. Посматрајмо низ $a_0, a_1, a_2, \ldots$ дат са $a_0 = 2$ и $a_{k+1} = 2a_k^2 - 1$ за $k \geq 0$. Доказати да ако непаран прост број p дели a_n, онда је $p \equiv \pm 1 \pmod{2^{n+2}}$.

Решење. Нека је $p > 2$ прост делилац a_n. Лако се показује индукцијом да је

$$a_n = \frac{(2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}}{2} = \frac{(2+\sqrt{3})^{2^{n+1}}+1}{(2+\sqrt{3})^{2^n}}.$$

Према томе, $(2+\sqrt{3})^{2^{n+1}} \equiv -1 \pmod{p}$. Одавде следи да ред r елемента $2+\sqrt{3}$ по модулу p дели 2^{n+2}, али не дели 2^{n+1}, дакле $r = 2^{n+2}$. Разликујемо два случаја.

Случај 1. 3 је квадратни остатак по модулу p. По теореми 15 је $(2+\sqrt{3})^{p-1} \equiv 1 \pmod{p}$, дакле $2^{n+2} \mid p-1$.

Случај 2. 3 је квадратни неостатак по модулу p. Тада ред сваког елемента $\mathbb{Z}[\sqrt{3}]$ по модулу p дели p^2-1, одакле $2^{n+2} \mid p^2-1$, али ово нам није довољно. За завршетак доказа нам је потребно да нађемо неко $u \in \mathbb{Z}_p(\sqrt{3})$ за које је $u^2 = 2+\sqrt{3}$, јер је тада поредак u једнак 2^{n+3} одакле тврђење једноставно следи.

Приметимо да је $(1+\sqrt{3})^2 = 2(2+\sqrt{3})$. Сада је довољно доказати да је $1/2$ потпун квадрат у $\mathbb{Z}_p(\sqrt{3})$. Међутим, ово одмах следи из чињенице да је у овом пољу $a_n = 0 = 2a_{n-1}^2 - 1$, одакле следи да је $1/2 = a_{n-1}^2$. Овим је доказ завршен.

Београд, 2004-2012