

Глава 7

РАШИРЕЊА ПРСТЕНА ЦЕЛИХ БРОЈЕВА

Оно што рад са целим бројевима чини погодним су есенцијална својства која они имају – пре свега, својство јединственог разлагања на просте чиниоце (основна теорема аритметике). Међутим, моћ аритметике целих бројева је ограничена. Тако се неки полиноми, мада имају нуле, не могу разложити на полиноме са целобројним коефицијентима. Па ипак, они се увек могу разложити у неком ширем пољу. На пример, полином $x^2 + 1$ је нерастављив над скупом целих бројева \mathbf{Z} , али се над скупом тзв. *Гаусових целих* $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$ разлаже као $(x + i)(x - i)$. Испоставиће се да се Гаусови цели понашају готово као обични цели бројеви, дакле између осталог основна теорема аритметике важи и за њих. Пре него што дођемо до тога, позабавићемо се неким основним појмовима више алгебре. Следеће је прецизирање дефиниција 5 и 6 главе 6.

Дефиниција 1. Кажемо да је број $\alpha \in \mathbf{C}$ **алгебарски** ако постоји полином $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ са целобројним коефицијентима такав да је $p(\alpha) = 0$. Ако је $a_n = 1$, кажемо да је α **алгебарски цео број**.

Такође, $p(x)$ је **минимални полином** броја α ако је нерастављив над \mathbf{Z} (тј. не може бити написан у облику производа неконстантних полинома са целобројним коефицијентима).

ПРИМЕР 1. Број i је алгебарски цео, јер је корен полинома $x^2 + 1$, а његов минимални полином је $x^2 + 1$. Такође, $\sqrt{2} + \sqrt{3}$ је алгебарски цео, а његов минимални полином је $x^4 - 10x^2 + 1$ (проверите!). \triangle

ПРИМЕР 2. Минимални полином рационалног броја $q = a/b$ ($a \in \mathbf{Z}$, $b \in \mathbf{N}$) је $bx - a$. По дефиницији, q је алгебарски цео ако и само ако је $b = 1$, тј. ако и само ако је q цео. \triangle

Дефиниција 2. Нека је α алгебарски цео број и $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ ($a_i \in \mathbf{Z}$) његов минимални полином. **Раширење прстена \mathbf{Z} елементом α** је скуп $\mathbf{Z}[\alpha]$ свих комплексних бројева облика

$$(1) \quad c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} \quad (c_i \in \mathbf{Z}),$$

са свим операцијама наслеђеним из скупа \mathbf{C} . **Степен** раширења је степен n полинома $p(x)$.

Тема ове главе су раширења прстена \mathbf{Z} степена 2, тзв. **квадратна раширења**. Тако нпр. полиномима $x^2 + 1$ и $x^2 + x + 1$ одговарају раширења $\mathbf{Z}[i]$ и $\mathbf{Z}[\omega]$, где је $\omega = \frac{-1 + i\sqrt{3}}{2}$ (ова ознака ће и убудуће бити коришћена).

Сви елементи квадратног раширења су алгебарски цели бројеви са минималним полиномом другог степена. За два елемента који имају заједнички минимални полином кажемо да су **конјуговани**. За сваки елемент z квадратног раширења који није цео постоји још тачно један елемент који му је конјугован. Овај елемент зовемо конјугатом елемента z и означавамо \bar{z} . За цео број z дефинишемо $\bar{z} = z$.

ДЕФИНИЦИЈА 3. **Норма** елемента z квадратног раширења \mathbf{Z} је $N(z) = z\bar{z}$.

Норма елемента квадратног раширења је увек цео број. Грубо речено, њена улога слична је улози апсолутне вредности у скупу целих бројева.

ПРИМЕР 3. Ако је $z \in \mathbf{Z}[\sqrt{d}]$, $z = a + b\sqrt{d}$ ($a, b \in \mathbf{Z}$), онда је $\bar{z} = a - b\sqrt{d}$ и $N(z) = a^2 - db^2$. Специјално, у $\mathbf{Z}[i]$ норма елемента $a + bi$ ($a, b \in \mathbf{N}$) је $N(a + bi) = a^2 + b^2$.

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

У сваком комплексном квадратном раширењу конјуговање одговара комплексном конјуговању. \triangle

Следећа два тврђења се доказују директно по дефиницији.

ТЕОРЕМА 1. *Конјуговање је мултипликативно, тј. за произвољне елементе z_1, z_2 квадратног раширења скупа \mathbf{Z} важи $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$.* ■

ТЕОРЕМА 2. *Норма је мултипликативна, тј. за произвољне елементе z_1, z_2 квадратног раширења скупа \mathbf{Z} важи $N(z_1 z_2) = N(z_1)N(z_2)$.* ■

Елемент $\varepsilon \in \mathbf{Z}[\alpha]$ зовемо **јединичним** ако постоји $\varepsilon' \in \mathbf{Z}[\alpha]$ такво да је $\varepsilon\varepsilon' = 1$. У том случају је $N(\varepsilon)N(\varepsilon') = N(1) = 1$, па је $N(\varepsilon) = \pm 1$. У ствари, елемент ε је јединичан ако и само ако има норму ± 1 : заиста, ако је $N(\varepsilon) = \pm 1$ онда је по дефиницији $\varepsilon\bar{\varepsilon} = \pm 1$.

ПРИМЕР 4. Једини јединични елементи у \mathbf{Z} су ± 1 .

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

Сви јединични елементи у $\mathbf{Z}[\omega]$ су $\pm 1, \pm\omega, \pm(1 + \omega)$. 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. Напоменимо да је ω^2 управо једнако $-(1 + \omega)$. \triangle

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

Решење. Означимо $P(x) = (1+x)(2+x)\cdots(p-1+x)$. 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

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

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

Због чињенице да је сваки не-нула елемент квадратног раширења дељив ма којим јединичним елементом, дефиницију појма простог елемента морамо да прилагодимо новом окружењу. Тако дефинишемо

Дефиниција 4. Елемент y квадратног раширења K је **еквивалентан** елементу x (пишемо $y \sim x$) ако постоји јединични елемент ε такав да је $y = \varepsilon x$.

Дефиниција 5. Елемент $x \in K$, који није 0 и није јединичан, јесте **прост** ако нема других делилаца осим јединичних и себи еквивалентних елемената.

Следеће очекивано тврђење се једноставно доказује. Међутим, обратно тврђење не важи, јер је нпр. 3 прост елемент у $\mathbf{Z}[i]$ (проверите!), али $N(3) = 9$ није прост.

ТЕОРЕМА 3. Нека је $x \in K$. 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 . ■

Наравно, елемент еквивалентан простом елементу је такође прост. Такође, елемент конјугован простом елементу је прост, па лако закључујемо да је најмањи природан број дељив простим z једнак $z\bar{z} = N(z)$.

Посматрајмо сада било који елемент $x \in K$ који није јединични нити нула. Ако x није прост, онда постоје елементи $y, z \in K$ који такође нису јединични 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, \dots, x_k прости. Овако смо добили да важи

ТЕОРЕМА 4. Свако $x \in K$ које није нула нити јединични елемент може се представити у облику производа простих елемената. ■

ЗАДАТАК 2. Дат је елемент $z \in K$ који није нула нити јединични. Колико има класа еквиваленције у K по модулу z ?

Решење. Нека је $K = \mathbf{Z}[\alpha]$, при чему је $\alpha^2 = p\alpha + q$, $p, q \in \mathbf{Z}$. Нека је $z = a + b\alpha$ ($a, b \in \mathbf{Z}$). 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 ($x \in K$) 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 $x \in K$ постоји јединствено $X = A + B\alpha \in K$ са $A, B \in \mathbf{Z}$, $0 \leq A < |N(z)|/d$, $0 \leq B < d$ такав да је $x \equiv X \pmod{z}$. Одавде добијамо да је тражени број класа еквиваленције једнак $|N(z)|$. \triangle

Природно се поставља питање када је растављање на просте елементе јединствено, тј. када важи основна теорема аритметике. По горњој дефиницији, прости елементи у \mathbf{Z} су $\pm 2, \pm 3, \pm 5$, итд. Међутим, разлагање на просте чиниоце више није јединствено, јер важи нпр. $2 \cdot 3 = (-2)(-3)$. У овом случају основна теорема аритметике у \mathbf{Z} важи у следећем облику.

ОТА (Основна Теорема Аритметике). Сваки елемент \mathbf{Z} , односно квадратног раширења K , који није нула нити јединичан, може се написати у облику производа простих елемената. Ово разлагање је јединствено до на редослед чинилаца и еквивалентност између одговарајућих чинилаца.

Дељење са остатком у квадратном раширењу K се може формулисати на следећи начин:

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

Овакво дељење не мора бити јединствено; могуће га је спровести у неким (али не свим!) квадратним раширењима, као што ћемо касније видети. Значај дељења са остатком, онда када је оно могуће, огледа се у следећој теорему.

ТЕОРЕМА 5. Ако је у квадратном раширењу K дељење са остатком могуће, онда у K важи ОТА.

Доказ. Ако је дељење са остатком у K могуће, онда се Еуклидов алгоритам завршава у коначном броју корака. Једноставна последица Еуклидовога алгоритма је да ако је p прост, $a, b \in \mathbf{Z}$ и $p \mid ab$, онда $p \mid a$ или $p \mid b$. Одавде лако следи јединственост растављања на просте чиниоце (видети доказ ОТА у првој глави). ■

Постоје примери квадратних раширења у којима дељење са остатком није могуће, али ОТА ипак важи. Ипак, ОТА није тачна у свим квадратним раширењима.

ПРИМЕР 5. ОТА не важи у $\mathbf{Z}[\sqrt{-5}]$, 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 $2 \pm \sqrt{-5} \not\sim 3$. \triangle

ПРИМЕР 6. Разлагања елемента $4 - \omega$ у $\mathbf{Z}[\omega]$ 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 $\mathbf{Z}[\omega]$. \triangle

Аритметика у скупу Гаусових целих $\mathbf{Z}[i]$

Као што смо већ констатовали, норма елемента $a + bi \in \mathbf{Z}[i]$ ($a, b \in \mathbf{Z}$) је $N(a + bi) = a^2 + b^2$. Јединични елементи су ± 1 и $\pm i$. Према томе, сви делиоци простог елемента $\pi \in \mathbf{Z}[i]$ су $\pm 1, \pm i, \pm \pi, \pm i\pi$.

ТЕОРЕМА 6. У скупу Гаусових целих $\mathbf{Z}[i]$ важи основна теорема аритметике (ОТА).

Доказ. На основу теореме 5, довољно је показати да за све $a, b \in \mathbf{Z}[i]$, $b \neq 0$ постоји $p \in \mathbf{Z}[i]$ такво да је $N(a - pb) < N(b)$.

Нека су $\sigma, \tau \in \mathbf{R}$ такви да је $a/b = \sigma + \tau i$, и нека су $s, t \in \mathbf{Z}$ такви да је $|\sigma - s| \leq 1/2$ и $|\tau - t| \leq 1/2$. Ставимо $p = s + ti$. Тада је $a - pb = (\sigma + \tau i)b - pb = [(\sigma - s) + (\tau - t)i]b$, одакле добијамо

$$\begin{aligned} N(a - pb) &= N[(\sigma - s) + (\tau - t)i]N(b) \\ &= [(\sigma - s)^2 + (\tau - t)^2]N(b) \leq N(b)/2 < N(b). \end{aligned}$$

Овим је тврђење доказано. \blacksquare

Следеће тврђење описује све просте елементе у скупу Гаусових целих.

ТЕОРЕМА 7. Елемент $x \in \mathbf{Z}[i]$ је прост ако и само ако је $N(x)$ прост број или је $|x|$ прост цео број облика $4k + 3$, $k \in \mathbf{Z}$.

Доказ. Посматрајмо произвољан прост елемент $x = a + bi \in \mathbf{Z}[i]$ ($a, b \in \mathbf{Z}$). Елемент \bar{x} је такође прост (ако $\bar{x} = yz$, онда $x = \bar{y}\bar{z}$), тако да је $N(x) = x\bar{x}$ једно (на основу ОТА, уједно и једино) растављање броја $N(x)$ на просте чиниоце у скупу Гаусових целих.

Претпоставимо да је $N(x)$ сложен број и $N(x) = mn$ за нека два природна броја m, n . Из $x\bar{x} = mn$ следи да је $x \sim m$ или $x \sim n$, па x мора бити цео прост број. Ако је $x = 2$ или $x \equiv 1 \pmod{4}$, онда постоје цели бројеви $a, b \in \mathbf{Z}$ такви да је $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2 = x$, па је x сложен у $\mathbf{Z}[i]$. С друге стране, ако је x прост број и $x \equiv 3 \pmod{4}$, онда је x прост и у $\mathbf{Z}[i]$. Заиста, ако је $x = uv$ за неке не-јединичне елементе $\mathbf{Z}[i]$, онда из $x^2 = N(x) = N(u)N(v)$ следи $N(u) = N(v) = x$, што није могуће (зашто?). Овим је доказ теореме завршен. \blacksquare

ЗАДАТАК 3. 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 $\mathbf{Z}[i]$. Како је $(y+i)(y-i)$ пети степен, следи да су $y+i$ и $y-i$ оба пети степени (зашто?). Нека су $a, b \in \mathbf{Z}$ 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 $b = \pm 1$. Лако се проверава да долази у обзир једино $b = 1$ и $a = 0$, а самим тим и $y = 0$, па је $(1, 0)$ једино решење. \triangle

Аритметика у скупу $\mathbf{Z}[\omega]$

Норма елемента $a + b\omega \in \mathbf{Z}[\omega]$ ($a, b \in \mathbf{Z}$) је $N(a + b\omega) = a^2 - ab + b^2$. Јединични елементи су ± 1 , $\pm\omega$ и $\pm(1 + \omega) = \mp\omega^2$.

ТЕОРЕМА 8. У скупу $\mathbf{Z}[\omega]$ важи основна теорема аритметике (ОТА).

Доказ. По теореме 5, довољно је показати да за све $a, b \in \mathbf{Z}[\omega]$, $b \neq 0$ постоји $p \in \mathbf{Z}[\omega]$ такво да је $N(a - pb) < N(b)$.

Слично као у скупу Гаусових целих бројева, нека су $\sigma, \tau \in \mathbf{R}$ такви да је $a/b = \sigma + \tau i$, и нека су $s, t \in \mathbf{Z}$ такви да је $|\sigma - s| \leq 1/2$ и $|\tau - t| \leq 1/2$. Ставимо $p = s + ti$. Сада добијамо $N(a - pb) \leq 3N(b)/4 < N(b)$, што доказује тврђење. ■

ЗАДАТАК 4. Нека је дат прост број $p \equiv 1 \pmod{6}$. Доказати да постоје $a, b \in \mathbf{Z}$ такви да је $p = a^2 - ab + b^2$.

Решење. Довољно је показати да је p сложен број у $\mathbf{Z}[\omega]$. Заиста, ако постоји прост елемент $z = a + b\omega \in \mathbf{Z}[\omega]$ ($a, b \in \mathbf{Z}$) такав да $z \mid p$, тада и $\bar{z} \mid \bar{p} = p$. Приметимо да је $(z, \bar{z}) = 1$: у супротном $z \mid \bar{z}$, па би морао да постоји јединични елемент ε такав да је $\bar{z} = \varepsilon z$, одакле би се лако добило $z \sim (1 - \omega) \mid 3$, што у овом случају није тачно. Следи $a^2 - ab + b^2 = z\bar{z} \mid p$, а самим тим и $a^2 - ab + b^2 = p$.

Покажимо, дакле, да је p сложен у $\mathbf{Z}[\omega]$. Из услова задатка закључујемо да је -3 квадратни остатак по модулу p , па зато постоје $m, n \in \mathbf{Z}$ који нису дељиви са p такви да $p \mid (2m - n)^2 + 3n^2 = 4(m^2 - mn + n^2)$, тј. $p \mid (m - n\omega)\overline{m - n\omega}$. Међутим p није делилац ниједног од бројева $(m - n\omega), \overline{m - n\omega}$, па зато мора бити сложен. \triangle

ТЕОРЕМА 9. Елемент $x \in \mathbf{Z}[\omega]$ је прост ако и само ако је $N(x)$ прост број или је $|x|$ прост цео број облика $3k + 2$, $k \in \mathbf{Z}$.

Доказ. Број $x = 3$ је сложен, јер је $N(1 - \omega) = (1 - \omega)(2 + \omega) = 3$. Такође, по задатку 4, сваки цео прост број $p \equiv 1 \pmod{6}$ је сложен у $\mathbf{Z}[\omega]$.

Остали детаљи доказа су аналогни доказу теореме 7, па их препуштамо читаоцу за вежбу. ■

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

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

Доказ који дајемо је дело Гауса.

ТЕОРЕМА 10. *Једначина*

$$(3) \quad x^3 + y^3 = z^3$$

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

Доказ. Претпоставимо да за три елемента x, y, z из $\mathbf{Z}[\omega]$, различита од нуле, важи (3). Јасно је да можемо да претпоставимо да су x, y, z узајамно прости у паровима.

Посматрајмо број $\rho = 1 - \omega$. Нјегова норма је једнака $(1 - \omega)(1 - \omega^2) = 3$, па је он прост. Примећујемо да је $\bar{\rho} = 1 - \omega^2 = (1 - \omega)(1 + \omega) \sim \rho$, одакле следи да је $\alpha \in \mathbf{Z}[\omega]$ дељиво са ρ ако и само ако је то и $\bar{\alpha}$. Сваки елемент $\mathbf{Z}[\omega]$ је конгруентан са $-1, 0$ или $1 \pmod{\rho}$: заиста, $a + b\omega \equiv a + b = 3q + r \equiv r \pmod{\rho}$ за неко $q \in \mathbf{Z}$ и $r \in \{-1, 0, 1\}$.

Посебно је битна следећа особина броја ρ :

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

Заиста, ако је $\alpha = \pm 1 + \beta\rho$, имамо

$$a^3 \mp 1 = (a \mp 1)(a \mp \omega)(a \mp \omega^2) = \rho^3 \beta(\beta \pm 1)(\beta \pm (1 + \omega)),$$

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 би због (4) x^3, y^3, z^3 били конгруентни са $\pm 1 \pmod{\rho^4}$, па би следила једна од нетачних конгруенција $0 \equiv \pm 1, \pm 1 \equiv \pm 2 \pmod{\rho^4}$. Без смањења општости претпостављамо да $\rho \mid z$. Штавише, из (4) такође закључујемо да $\rho^2 \mid z$.

Нека је $k \geq 2$ најмањи природан број за који постоји решење једначине (3) у коме је $(x, y, z) = 1$ и $\rho^k \mid z, \rho^{k+1} \nmid z$. Посматрајмо ово решење (x, y, z) .

Чиниоци $x + y, \omega x + \omega^2 y, \omega^2 x + \omega y$ из (2) су конгруентни по модулу ρ и имају суму једнаку 0. Из $\rho \mid z$ следи да су сви они дељиви са ρ и да им је ρ највећи заједнички делилац. Нека је

$$x + y = A\rho, \quad \omega x + \omega^2 y = B\rho, \quad \omega^2 x + \omega y = C\rho,$$

где су $A, B, C \in \mathbf{Z}[\omega]$ узајамно прости по паровима и $A + B + C = 0$. Производ ABC је потпун куб (једнак $(z/\rho)^3$), одакле из ОТА следи да је сваки од A, B, C еквивалентан неком кубу:

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

за неке $\zeta, \eta, \xi \in \mathbf{Z}[\omega]$ узајамно просте по паровима и јединичне елементе α, β, γ . Према томе,

$$(5) \quad \alpha\zeta^3 + \beta\eta^3 + \gamma\xi^3 = 0.$$

Како је $\alpha\beta\gamma$ јединични елемент и потпун куб, имамо $\alpha\beta\gamma = \pm 1$. Даље, $ABC = (z/\rho)^3$ је дељиво са ρ (јер $\rho^2 \mid z$), па је (тачно) један од бројева ζ, η, ξ дељив са ρ : рецимо да је то ξ . Истовремено ξ^3 дели ABC што је дељиво са ρ^{3k-3} и није дељиво са ρ^{3k-2} , па је ρ^{k-1} највећи степен ρ који дели ξ . Бројеви ζ и η нису дељиви са ρ , па су зато ζ^3 и η^3 конгруентни ± 1 по модулу ρ^4 . Тако из једнакости $A + B + C = 0$ добијамо $\alpha \pm \beta \equiv 0 \pmod{\rho^4}$, значи $\beta = \pm\alpha$, па из $\alpha\beta\gamma = \pm 1$ следи и $\gamma = \pm\alpha$.

Скраћивањем α у једначини (5) добијамо $\zeta^3 \pm \eta^3 \pm \xi^3 = 0$, што даје још једно нетривијално решење једначине (3) са $(\zeta, \eta, \xi) = 1$. Међутим, у овом решењу $\rho^{k-1} \mid \xi$ и $\rho^k \nmid \xi$, што је у контрадикцији са избором броја k . ■

Аритметика у другим квадратним раширењима

Сва квадратна раширења се могу разврстати у две класе:

1° Раширења облика $K = \mathbf{Z}[\sqrt{d}]$, где је $d \neq 1$ цео број који није дељив квадратом већим од 1. Конјуговање и норма су дати формулама $\overline{x + y\sqrt{d}} = x - y\sqrt{d}$ и $N(x + y\sqrt{d}) = x^2 - dy^2$, где су $x, y \in \mathbf{Z}$.

2° Раширења облика $K = \mathbf{Z}[\alpha]$ за $\alpha = \frac{-1 + \sqrt{d}}{2}$, где је $d = 4k + 1$ ($k \in \mathbf{Z}$) цео број који није дељив квадратом већим од 1 и $d \neq 1$ (тада је α алгебарски цео: $\alpha^2 + \alpha - k = 0$). Конјуговање и норма су дати формулама $\overline{x + y\alpha} = x - y - y\alpha$ и $N(x + y\alpha) = x^2 - xy - ky^2$, где су $x, y \in \mathbf{Z}$.

Нека од ових раширења поседују дељење са остатком, и у њима важи ОТА.

Таква су нпр. раширења $\mathbf{Z}[\sqrt{d}]$ за $d = -2, -1, 2, 3, 6, 7$ и $\mathbf{Z}\left[\frac{-1 + \sqrt{d}}{2}\right]$ за $d = -7, -3, 5$.

Питање налажења свих квадратних раширења у којима важи ОТА (дакле, укључујући и она у којима алгоритам дељења са остатком не постоји) је веома озбиљно. Међу раширењима типа 1° и 2° са $d < 0$, ОТА важи у још само пет поред наведених: то су раширења типа 2° за $d = -11, -19, -43, -67, -163$. Још је Гаус претпоставио да ОТА важи у бесконачно много квадратних раширења са позитивним d . Овај проблем је до данас остао нерешен.

З А Д А Ц И

5. 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 $z = ac + bd$.

6. Посматрајмо низ a_0, a_1, a_2, \dots 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 $p \equiv \pm 1 \pmod{2^{n+2}}$.

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