Hrvatski matematički elektronički časopis *math.e*
Broj 13
http://e.math.hr/

Ideja jednoznačne faktorizacije I

Ivica Gusić

Sadržaj:

1. Uvod

Većini je prva asocijacija na jednoznačnu faktorizaciju rastavljanje prirodnih brojeva na proste faktore. Naprimjer,

$$30 = 2 \cdot 3 \cdot 5, \quad 60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5.$$

To je i prirodno, tako je i bilo u razvoju matematike. Činjenica da su takvi rastavi jednoznačni (do na poredak prostih faktora) obično se naziva **osnovnim teoremom aritmetike** (OTAr).

Druga je asocijacija rastavljanje polinoma na nerastavljive polinome. Naprimjer,

$$x^3 - x = x(x-1)(x+1), \quad x^4 - x^2 = x \cdot x(x-1)(x+1) = x^2(x-1)(x+1).$$

Činjenica da su takvi rastavi jednoznačni (do na poredak prostih faktora) obično se naziva **osnovnim teoremom algebre** (OTAl).

Naravno, mogu se gledati i rastavi poput

$$13 = (2 - 3i)(2 + 3i), \quad 6 = (1 - \sqrt{5}i)\,(1 + \sqrt{5}i).$$

Mnogi bi se brzo složili s time da i ovakvi rastavi spadaju u aritmetiku. Jednostavno rečeno, aritmetika se odnosi na brojeve (prirodne, cijele, Gaussove…). Prirodno je postavljanje pitanja jesu li $6 = 3 \cdot 2$ i $6 = (1 - \sqrt{5}i)(1 + \sqrt{5}i)$ različiti rastavi broja 6 na nerastavljive faktore i kako to treba tumačiti. Analogno tomu, mogli bismo gledati rastav

$$x - 1 = -\frac{1}{2}(x - 1 - i\sqrt{1 - x^2})\,(x - 1 + i\sqrt{1 - x^2})$$

i pitati se kako ga treba tumačiti. Ili, naprimjer, ako gledamo prsten $\mathbf{C}[x,y]$ gdje su varijable x, y povezane relacijom $x^2 + y^2 = 1$, pitamo se je li

$$y^2 = (1 - x)(1 + x)$$

primjer nejednoznačnosti rastava na nerastavljive faktore ili nije. I je li isto s prstenom $\mathbf{C}[x,y]$ gdje su varijable x, y povezane relacijom $y^2 = (x - e_1)(x - e_2)(x - e_3)$, za različite (kompleksne) brojeve e_1, e_2, e_3, tj. treba li tu relaciju tumačiti kao nejednoznačnost rastava? Kako bilo da bilo, ove posljednje primjere dovodimo u vezu s osnovnim teoremom algebre i to bi, dakle, spadalo u algebru. Češće se govori da je to **funkcijski slučaj** (jer se polinomi mogu razmatrati i kao funkcije), pa ćemo i mi tako govoriti. Dakle, uočava se analogija između aritmetičkog i funkcijskog slučaja (brojeva i funkcija-polinoma). To je jedna od najplodonosnijih analogija u razvoju matematike. Osvrnut ćemo se na neke njezine aspekte bez pretenzije da sve dokažemo i istjeramo načistac. Počet ćemo s aritmetičkim, ali više ćemo prostora posvetiti funkcijskom slučaju jer je on manje zastupljen na dodiplomskoj razini. Većina pojmova i tvrdnja kojima ćemo se koristiti mogu se naći u Langovoj *Algebri* [La] i u knjizi [IR]. Za sada recimo još to da gore postavljena pitanja nisu samo zanimljive glavolomke za razonodu i kraćenje vremena, već se, naprotiv, uklapaju u same temelje matematike.

2. Aritmetički slučaj

U ovom, prvom dijelu članka, osvrnut ćemo se na aritmetički slučaj, tj. slučaj brojeva. Osnovni teorem aritmetike poznavali su i koristili još stari Grci, samo što nisu smatrali da ga trebaju formulirati kao posebnu tvrdnju, a kamoli dokazivati. Neizravno, taj je teorem korišten kroz Euklidov algoritam (zanimljivo nagađanje o vezi tih dvaju teorema može se pročitati u [Go]). Čini se da je Gauss bio prvi koji je smatrao da (OTAr) treba dokazati (vidi [Ga], gdje ga Gauss dokazuje na samom početku). Vjerojatno je Gauss bio i prvi koji je znao da (OTAr) ne vrijedi u općenitijim prstenima brojeva. Da to pojasnimo, najprije uočimo da se (OTAr) izvorno odnosi na prirodne brojeve 1, 2, 3, 4, 5, 6… i pripadne proste brojeve 2, 3, 5, 7, 11… (OTAr) tvrdi da se svaki prirodni broj n različit od 1 jednoznačno rastavlja na umnožak prostih brojeva, tj. da postoje jedinstveni prosti brojevi $p_1, \ldots, p_k$ i jedinstveni prirodni brojevi $r_1, \ldots, r_k$ tako da bude

$$n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}.$$

Pokazuje se da je korisno gledati nešto veći skup: **prsten cijelih brojeva** $\{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$.

Tu je nula za sebe, -1, 1 su invertibilni elementi (čine multiplikativnu grupu), a $-p$, p parovi su međusobno pridruženih (asociranih) prostih brojeva. Sad (OTAr) postaje tvrdnja da svaki cijeli m različit od $0, -1, 1$ ima jedinstven prikaz

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

gdje su p_j međusobno neasocirani prosti brojevi, a $\varepsilon = \pm 1$ (u pravilu, od dvaju međusobno asociranih prostih brojeva, u ovakvim rastavima biramo onaj pozitivni, ali to nije nužno).

Jedna od glavnih posljedica jednoznačne faktorizacije jest tvrdnja da neki prosti broj dijeli umnožak dvaju cijelih brojeva ako i samo ako dijeli bar jednog od njih. Kao ilustraciju primjene teorema o jednoznačnoj faktorizaciji navedimo primjer određivanja cjelobrojnih točaka na jednoj eliptičkoj krivulji.

Primjer 1. Jedina cjelobrojna rješenja jednadžbe $y^2 - y = x^3$ jesu $(0, 0)$ i $(0, 1)$.

Uputa. Jednadžbu treba napisati u obliku $y(y-1) = x^3$.

Prihvaćanje prstena (komutativnih s jedinicom) prirodnim okvirom razmatranja problema jednoznačne faktorizacije, pogodno je u složenijim okolnostima, naprimjer, za prsten cijelih Gaussovih brojeva

$$A = \mathbf{Z}[i] := \{a + bi, \quad a, b \in \mathbf{Z}\}.$$

Tu je opet 0 za sebe, $1, -1, i, -i$ čine grupu invertibilnih elemenata (tj. to su jedini Gaussovi cijeli brojevi kojima je i inverz cijeli Gaussov broj). To se lako vidi, a mnogo je teže pokazati sljedeće (za ovo i dio daljnjeg razmatranja vidi [IR]):

(F_1) A ima jednoznačnu faktorizaciju na nerastavljive elemente (tj. elemente koji se ne mogu rastaviti na umnožak dvaju neinvertibilnih), koje onda zovemo prostim.

Ovdje napomenimo da uz svaki broj α prstena, različit od nule, idu njemu pridruženi, $-\alpha$, $i\alpha$, $-i\alpha$, koji zajedno s α čine klasu pridruženosti (asociranosti) broja α.

(F_2) Klase pridruženosti nerastavljivih elemenata su:

(0) Klasa od $1 + i$ koji ima svojstvo da je $2 = -i\,(1 + i)^2$ rastav od 2.

(I) Klase prostih p oblika $4k - 1$, tj. kongruentnih -1 modulo 4, primjerice 3, 7, 11, 19, … (lako se vidi da su takvi nerastavljivi).

(II) Za svaki prosti p oblika $4k + 1$, klase pripadnih kompleksno konjugiranih parova $a + bi$, $a - bi$ gdje su a, b prirodni brojevi sa svojstvom da je $(a + bi)(a - bi) = p$ (napomenimo kako nije tako lako dokazati da takav rastav postoji).

Dakle 3 je prost, ali i -3, $3i$, $-3i$ i oni čine klasu međusobno pridruženih. Slično je s $2 + 3i$, $-2 - 3i$, $-3 + 2i$, $3 - 2i$.

Za ilustraciju funkcioniranja jednoznačne faktorizacije u $\mathbf{Z}[i]$ skicirat ćemo dokaz Fermatova teorema o prostim brojevima koji su sume dvaju kvadrata.

Teorem (Fermat). Svaki prosti broj oblika $4k + 1$, $k \in \mathbf{N}$ suma je dvaju kvadrata prirodnih brojeva.

Naprimjer, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$ itd. Još je $2 = 1^2 + 1^2$, a prosti brojevi oblika $4k - 1$ ne mogu biti zbroj dvaju kvadrata (to je lako) i time je tvrdnja kompletirana.

Uočite da je traženi teorem upravo tvrdnja (F_2)(II). Dakle, pretpostavljamo da vrijedi (F_1), a dokazujemo (F_2)(II). To i nije tako neobično jer standardni dokazi najprije pokazuju jednoznačnost faktorizacije, potom opisuju nerastavljive elemente.

Za dokaz će nam biti dovoljno pokazati da je svaki prosti p koji je oblika $4k + 1$ rastavljiv u $A = \mathbf{Z}[i]$, tj. da je

$$p = \varepsilon\,(a + bi)(c + di)$$

gdje je $\varepsilon = \pm 1, \pm i$ jedinica u A, a a, b, c, d su cijeli brojevi uz $ab \neq 0$, i $cd \neq 0$. Naime, tada bismo konjugiranjem i množenjem dobili

$$p^2 = (a^2 + b^2)(c^2 + d^2)$$

pa bi bilo $p = a^2 + b^2$.

Ostaje pokazati da je p rastavljiv u A. Za to nam dobro dođe poznata karakterizacija prostih brojeva oblika $4k + 1$ - to su upravo oni p za koje jednadžba $x^2 + 1 = 0$ ima dva različita rješenja modulo p (naprimjer, modulo 5 to su klase od ± 2, a modulo 13 klase od ± 5). To znači da postoji cijeli broj m tako da bude $p \mid m^2 + 1$ u $\mathbf{Z}$, pa će biti $p \mid (m - i)(m + i)$ u A. Ako je p nerastavljiv u A, a faktorizacija jednoznačna (to je jedino mjesto gdje nam to treba), onda $p \mid m + i$, što je nemoguće. Zato je p rastavljiv u A.

Primjer 2. Koristeći se jednoznačnošću faktorizacije u prstenu $\mathbf{Z}[\sqrt{-2}]$ pokazuje se da su $(3, \pm 5)$ jedine cjelobrojne točke na eliptičkoj krivulji $y^2 = x^3 - 2$ (Fermatov zadatak). Dovoljno je jednadžbu napisati u obliku $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$ i analizirati rastave.

Situacija općenito nije takva. Ako se usredotočimo samo na kvadratna proširenja polja racionalnih brojeva, a nije teško uvidjeti da su to polja $K := \mathbf{Q}(\sqrt{d})$ gdje su d cijeli brojevi slobodni od kvadrata (tj. koji su prosti, umnošci različitih prostih ili broj -1; također, drugi korijen gledamo u kompleksnom području i smatramo da smo izabrali jednu od dviju mogućih vrijednosti od $\sqrt{d}$), prvo se postavlja pitanje koje je prstene A analogne prstenu cijelih brojeva potrebno razmatrati. Pokazuje se da tzv. **prstene cijelih brojeva** u $\mathbf{Q}(\sqrt{d})$ čine oni elementi od $\mathbf{Q}(\sqrt{d})$ koji su korijeni polinoma s cjelobrojnim koefcijentima, ali tako da je koefcijent uz najvišu potenciju jednak 1. Tada se dobije da je

$$A = \{a + b\sqrt{d},\ a, b \in \mathbf{Z}\} \text{ ako je } d \equiv 2, 3 \text{ modulo } 4;$$

$$A = \{a + b\omega,\ a, b \in \mathbf{Z}, \omega := \frac{1+\sqrt{d}}{2}\} \text{ ako je } d \equiv 1 \text{ modulo } 4.$$

Naprimjer, za Gaussove brojeve $d = -1 \equiv 3$ modulo 4, pa je prsten cijelih $A = \{a + b\sqrt{-1},\ a, b \in \mathbf{Z}\}$, što je upravo prsten cijelih Gaussovih brojeva $\mathbf{Z}[i]$, kako smo i očekivali (treba uočiti da je broj i rješenje jednadžbe $x^2 + 1 = 0$). Kako je pak $-3 \equiv 1$ modulo 4, prsten cijelih brojeva u polju $\mathbf{Q}(\sqrt{-3})$ je $\mathbf{Z}[\rho]$ gdje je ρ jedan od netrivijalnih trećih korijena iz 1, naprimjer $\rho := ½(-1 + \sqrt{-3})$ (treba uočiti da je ρ rješenje jednadžbe $x^2 + x + 1 = 0$). Taj prsten ima jednoznačnu faktorizaciju (na osnovi toga lako je odrediti nerastavljive elemente, kao i kod $\mathbf{Z}[i]$). Također, vidi se da je grupa invertibilnih elemenata $\{1, -1, \rho, -\rho, \rho^2, -\rho^2\}$. Detalji se mogu vidjeti u [IR].

Prsten $\mathbf{Z}[\sqrt{-3}]$ potprsten je prstena $\mathbf{Z}[\rho]$ i ne sadržava ρ. Euler je, dokazujući Fermatov teorem za $n = 3$, pogrješno, bez dokaza, na njega primijenio svojstvo: *ako su brojevi relativno prosti (tj. nemaju zajedničkih pravih djelitelja) i njihov umnožak je kub, onda je svaki od njih kub.* Pogrješno je to što je za takav zaključak potrebna jednoznačna faktorizacija, a $\mathbf{Z}[\sqrt{-3}]$ je nema, naprimjer, u tom su prstenu brojevi 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ nerastavljivi, a vrijedi

$$4 = 2^2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Za $d = -5$ pojavljuje se novi moment: odabran je pravi prsten, ali je jednoznačna faktorizacija izostala.

Primjer 3. Budući da je $d = -5 \equiv 3$ modulo 4, dobijemo da je $A := \mathbf{Z}(\sqrt{-5})$ prsten cijelih u polju $\mathbf{Q}(\sqrt{-5})$. Grupa invertibilnih elemenata je $\{-1, 1\}$. Tu je $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ i nije teško provjeriti da su 2, 3, $1 + \sqrt{-5}$, $1- \sqrt{-5}$ nerastavljivi elementi u A pa je to primjer nejednoznačne faktorizacije.

O tom ćemo fenomenu nešto više reći poslije, a sad uočimo da su prsteni $\mathbf{Z}[i]$ i $\mathbf{Z}[\rho]$ povezani i time što su generirani korijenima iz jedinice (četvrtim, odnosno trećim). Općenito, za svaki prirodni broj n, primitivni n-ti korijen iz jedinice izvodnica je grupe n-tih korijena iz 1, naprimjer $\zeta_n := e^{2\pi i/n}$. Pripadno ciklotomsko (kružno) polje je $\mathbf{Q}(\zeta_n)$, a pokazuje se da je pripadni prsten cijelih brojeva $A := \mathbf{Z}[\zeta_n]$ (to općenito nije tako lako pokazati, za proste n vidi [IR], Prop. 13.2.10). Kako za $n = 3$ i $n = 4$ prsten cijelih A ima jednoznačnu faktorizaciju, može se pomisliti da to vrijedi općenito, i zaista, vrijedi za mnoge male n. Prvi prirodni broj za koji ne vrijedi je $n = 23$. Francuski matematičar Lame 1847. uputio je Pariškoj akademiji podnesak s "rješenjem" Fermatova teorema, a rješenje se zasnivalo na pretpostavci da prsten cijelih ciklotomskih brojeva ima jednoznačnu faktorizaciju. Taj je prsten ulazio u raspravu tako što se hipotetska diofantska jednadžba $X^n + Y^n = Z^n$ u tom prstenu, za neparne n (a samo su takvi bitni) rastavlja kao

$$(X + Y)(X + \zeta_n Y)(X + \zeta_n^2 Y) \cdot \ldots \cdot (X + \zeta_n^{n-1} Y) = Z^n,$$

što se dalje pokušava razriješiti koristeći se djeljivošću u tom prstenu. Sve bi bilo dobro da je faktorizacija jednoznačna, ali nije. Tek se od sedamdesetih godina 20. st. zna potpun popis onih n za koji to vrijedi (vidi [Po], str. 14). Jedan od načina prevladavanja nejednoznačnosti faktorizacije u spomenutim prstenima jest njihovo dovođenje u vezu s objektima u kojima je ona jednoznačna. Podsjetimo se najprije pojma ideala.

Ideal I prstena A (komutativnog i s jedinicom) neprazan je podskup od A koji je zatvoren na zbrajanje (dakle je Abelova grupa) i na množenje s elementima iz A. Sam prsten A ima ta svojstva, ali ga ne smatramo idealom (odnosno kažemo da nije pravi ideal). Prototipovi ideala su svi višekratnici nekog cijelog broja m, tj. skupovi oblika $\{\ldots, -2m, -m, 0, m, 2m, \ldots\} = \{mk : k \in \mathbf{Z}\}$.

Općenito, ako $\beta \in A$ nije invertibilan, onda je $(\beta) := \{\beta a : a \in A\}$ ideal u A. Kažemo da je to glavni ideal generiran s β (da je β bio invertibilan ispalo bi $(\beta) = A$). Mnogi prsteni imaju samo glavne ideale (naprimjer, prsten cijelih brojeva $\mathbf{Z}$ ili prsten polinoma $k[X]$ s koeficijentima u polju k), ali to ne vrijedi općenito. Najjednostavniji primjer takvog prstena možda je prsten polinoma s dvjema varijablama s koeficijentima u nekom polju, primjerice u $\mathbf{C}$. Tu su glavni ideali oblika (f) gdje je f neki nekonstantni polinom, ali je, naprimjer skup

$$I := \{(x-a)f(x, y) + (y-b)g(x, y) : f, g \in \mathbf{C}[x, y]\}$$

ideal koji nije glavni. Kažemo da je taj ideal generiran s $x - a$ i $y - b$ i označavamo ga kao $(x - a, y - b)$ (da taj ideal nije generiran s jednim elementom vidimo po tome što je zajednički korijen svih njegovih elemenata upravo (a, b), a elementi ideala (f) imaju beskonačno mnogo zajedničkih korijena).

Kažemo da je ideal I prost, ako iz $ab \in I$ za $a, b \in A$ vrijedi $a \in I$ ili $b \in I$. Vidjet ćemo da taj pojam dobro generalizira pojam prostog broja.

Na skupu ideala nekog prstena možemo uvesti operaciju množenja. Kada bi svi ideali bili glavni, to bi bilo jednostavno, naime

$$(a)(b) := (ab),$$

a umnožak ideala bio bi upravo umnožak pripadajućih skupova (pomnožili bismo svaki element sa svakim). Općenito, tj. kad nisu svi ideali glavni, to ne bi bilo dovoljno, tj. umnožak dvaju ideala kao skupova nije nužno ideal. Zato definiramo:

$$I \cdot J := \text{najmanji ideal koji sadržava umnožak skupova } I \text{ i } J.$$

To je isto kao da kažemo

$$I \cdot J := \{\textstyle\sum a_i b_i : a_i \in I, b_i \in J\}$$

gdje su sume konačne.

Ideja je da umjesto rastava na nerastavljive elemente gledamo rastav na proste ideale (vidi [IR], 12. poglavlje).

Takvo nešto može se provesti za dosta široku klasu prstena (Dedekindove prstene - vidi [Mi], 3. poglavlje). Pokazuje se da se u tim okolnostima, poput toga da se obični složeni brojevi mogu rastaviti na umnožak prostih, i ideali mogu rastaviti na umnožak prostih ideala. U situacijama koje mi razmatramo nije problem da ne možemo rastaviti elemente na nerastavljive (tj. da možemo rastavljati sve dalje i dalje - drugim riječima, naši su prsteni noetherski), već je problem što ti rastavi mogu biti bitno različiti.

Međutim, u prstenima cijelih algebarskih brojeva vrijedi (a i šire, u Dedekindovim prstenima):

(I) svaki se ideal rastavlja na umnožak konačno mnogo prostih ideala (koji su upravo oni što se dalje ne mogu rastavljati),

(II) taj rastav je jednoznačan (do na poredak).

Sad imamo sljedeću proceduru.

1. korak. Svakom neinvertibilnom ne-nul elementu α prstena A pridružimo glavni ideal (α).

2. korak. Skup (monoid s obzirom na množenje) glavnih ideala uložimo u skup (monoid s obzirom na množenje) svih ideala.

Kako je svaki ideal umnožak prostih ideala, tako se i svaki glavni ideal (α) jednoznačno rastavlja na umnožak prostih ideala, iako se α općenito ne rastavlja jednoznačno na umnožak nerastavljivih elemenata (rastavlja se, ali možda na bitno različite načine).

Odatle dolazi terminologija u prstenima cijelih algebarskih brojeva, ali i šire.

(i) Kažemo da je element prstena A **nerastavljiv** (ireducibilan) ako nije invertibilan niti 0 i ako se ne može rastaviti na umnožak dvaju neinvertibilnih elemenata.

(ii) Kažemo da je element π prstena A **prost** ako je ideal (π) prost.

Lako se vidi da je svaki prosti element ujedno i nerastavljiv, međutim, suprotno ne vrijedi općenito.

Nejednoznačna faktorizacija u prstenima cijelih algebarskih brojeva manifestira se i tako što ima prostih ideala koji nisu glavni, tj. koji nisu oblika $I = (\alpha) = \alpha \cdot A$ za neki $\alpha \in A$. Tu je, prema definiciji, $\alpha \cdot A = \{\alpha \cdot x : \alpha \in A\}$. Može se dokazati da vrijedi sljedeće (naprimjer, koristeći se Teoremom 3.41 u [Mi]):

1. Ideal P u $A := \mathbf{Z}[\sqrt{-5}]$ generiran s 2 i $1 + \sqrt{-5}$, tj. $P := (2, 1 + \sqrt{-5})$ je prost i u A vrijedi $(2) = P^2$, tj. ideal u A generiran s 2 nije prost (iako je 2 nerastavljiv element u A, on nije prost u A) već je kvadrat prostog ideala.
2. Ideal $Q := (3, 1 + \sqrt{-5})$ u A je prost, pa je i ideal $\overline{Q} = (3, 1 - \sqrt{-5})$ prost i u A vrijedi $(3) = Q \cdot \overline{Q}$ - umnožak različitih prostih ideala (kompleksnokonjugiranih) pa 3 u A ne generira prosti ideal (iako je nerastavljiv, nije prost).

3. U A vrijedi $(1+\sqrt{-5}) = P\cdot Q$ pa vrijedi i $(1-\sqrt{-5}) = P\cdot \overline{Q}$.

Sad za ideale u A vrijedi

$$(2)\cdot(3) = P^2\cdot Q\cdot \overline{Q} = P\cdot Q\cdot P\cdot \overline{Q} = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$$

(ovo posljednje produkt je ideala), pa se različiti rastavi na nerastavljive elemente svode na iste rastave na proste ideale.

Pokažimo izravno na primjeru da 2 i 3 nisu prosti u ovom prstenu A.

Kako je $(1+\sqrt{-5})\cdot(1-\sqrt{-5}) = 6$, taj je umnožak i u idealu (2) i u idealu (3) (u A), ali nijedan od faktora nije ni u (2) ni u (3).

Činjenica da se svaki ideal u prstenu algebarskih brojeva rastavlja jednoznačno na umnožak prostih ideala može se izreći i preciznije. Naprimjer, broj faktora u tom rastavu, ograničen je stupnjem pripadajućeg proširenja. Radi jednostavnosti, izrecimo tvrdnju za kvadratna proširenja.

Neka je A prsten cijelih brojeva u $K := \mathbf{Q}(\sqrt{d})$, gdje je, kako smo i prije rekli, d kvadratno slobodan cijeli broj i neka je:

$D := d$, ako je $d \equiv 1$ modulo 4;

$D := 4d$, ako je $d \equiv 2, 3$ modulo 4.

Tada za (cijele) proste brojeve p vrijedi (vidi [IR], 13. poglavlje):

(i) Ako $p \mid D$ onda je (p) u A kvadrat prostog ideala (koji može biti glavni). To je tzv. slučaj **grananja**.

(ii) Ako je p neparan i p ne dijeli D, onda
(A) (p) je prost u A ako jednadžba $x^2 = d$ modulo p nema rješenja (to je **nerascjepivi** slučaj),
(B) $(p) = P\overline{P}$ je umnožak dvaju različitih prostih ideala u A (koji mogu biti glavni) ako jednadžba $x^2 = d$ modulo p ima dva različita rješenja (to je **rascjepivi** slučaj).

(iii) Ako D nije paran, tj. ako je $d \equiv 1$ modulo 4, onda je
(C) (2) je prost ako je $d \equiv 5$ modulo 8,
(D) $(2) = P\overline{P}$ je umnožak različitih prostih ideala u A (koji mogu biti glavni) ako je $d \equiv 1$ modulo 8.

Pogledajmo gornju tvrdnju za $A := \mathbf{Z}[i]$. Tu je $d = -1$, $D = -4$, pa se samo $p = 2$ grana, kako smo i prije rekli. Za neparne p treba gledati jednadžbu $x^2 = -1$

modulo p, koja očito nema rješenje ako je $p \equiv 3$ modulo 4 (pa takvi p ostaju prosti). Kako smo već rekli, ta jednadžba ima dva rješenja ako je $p \equiv 1$ modulo 4 (pa se takvi (p) rastavljaju na umnožak dvaju prostih ideala - tu se pokazuje da su glavni). Dakle, sve se slaže.

Dok smo ovo obrazlagali, prešutno smo se koristili s relacijom

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

gdje je

$$\left(\frac{\cdot}{p}\right)$$

Legendreov simbol (vidi [IR]), definiran kao

$$\left(\frac{d}{p}\right) = 1 \text{ ili } -1,$$

uz uvjet da prost broj p ne dijeli d, ovisno o tome ima li jednadžba $x^2 = d$ modulo p rješenje ili ne. Gornja jednakost samo je dio tzv. **zakona kvadratnog reciprociteta**

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \ \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}, \ \left(\frac{q}{p}\right) = (-1)^{(p-1)/2\cdot(q-1)/2}\left(\frac{p}{q}\right),$$

za neparne proste p, q (vidi [IR]).

Važnost zakona kvadratnog reciprociteta je u tome što on omogućuje opis razlaganja prostih ideala u kvadratnim poljima u terminima kongruencija modulo D. Provedimo to za $d = -5$.

Tu je $D = -20$ pa se 2 i 5 granaju, s tim da je (5) kvadrat glavnog ideala $(\sqrt{-5})$, a (2) kvadrat neglavnog ideala $(2, 1 + \sqrt{-5})$. Dalje treba gledati samo neparne p različite od 5. Kako je

$$\left(\frac{d}{p}\right)=\left(\frac{-5}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{(p-1)/2} \ (-1)^{(5-1)/2\cdot(p-1)/2}\left(\frac{p}{5}\right)=(-1)^{(p-1)/2}\left(\frac{p}{5}\right)$$

što je jednako

(I) 1 ako je $p \equiv 1$ ili 9 ili 3 ili 7 modulo 20,

a jednako

(II) -1 ako je $p \equiv 13$ ili 17 ili 11 ili 19 modulo 20.

Ako je (II) onda je (p) prosti ideal u A. Ako je (I) onda (p) nije prosti već je $(p) = P\overline{P}$. Međutim, u slučajevima s 1 i 9 ideali P, $\overline{P}$ su glavni, u onima s 3 i 7 nisu. Naprimjer:

(a) $41 = (6 + \sqrt{-5})(6 - \sqrt{-5})$ je rastav na proste elemente; slično je za $p = 61, 101, 141\ldots$

(b) $29 = (3 + 2\sqrt{-5})(3 - 2\sqrt{-5})$ je rastav na proste elemente; slično je za $p = 89, 109, 129\ldots$,

dok za 3, 23, 43… niti za 7, 47, 67… nema takvog nečeg.

Matematičari 19. stoljeća pravilno su procijenili da je generalizacija kvadratnog zakona reciprociteta važan problem. I Kummer je došao do jednoznačnog rastava na proste ideale tragajući za zakonom reciprociteta u ciklotomskim poljima, a onda je to primijenio na Posljednji Fermatov teorem i napravio velik prodor. I nedavno konačno rješenje tog teorema može se tumačiti kao posljedica parcijalnog rješenja problema proširenja zakona kvadratnog reciprociteta na neabelova proširenja.

Ilustrirajmo primjenu jednoznačne faktorizacije na proste ideale u prstenu $A := \mathbf{Z}[\sqrt{-5}]$. Trebat će nam još jedna činjenica o tom prstenu. Naime, iako postoje prosti ideali P koji nisu glavni, ipak je kvadrat svakog prostog ideala glavni ideal (vidi, naprimjer [Mi], 3. poglavlje, Primjer 4.6).

Primjer 4. Eliptička krivulja $y^2 = x^3 - 5$ nema cjelobrojnih točaka (tj. jednadžba nema cjelobrojnih rješenja). Jednadžbu pišemo u obliku

$$(y + \sqrt{-5})(y - \sqrt{-5}) = x^3$$

pa imamo i jednakost pripadajućih glavnih ideala u A. Ideali $(y + \sqrt{-5})$ i $(y - \sqrt{-5})$ nemaju zajedničkog prostog ideala u rastavu, osim možda ideala Q sa svojstvom $(2) = Q^2$ u A. Za ideale oblika (p) uz cijele proste p to je jasno, za ideal $(\sqrt{-5})$ također (jer bi onda x bio djeljiv s 5, što je nemoguće). Za ideale P takve da je $\overline{P} \neq P$ također. Naime, kada bi bilo $P|(y + \sqrt{-5})$ i $P|(y - \sqrt{-5})$, onda i $\overline{P}|(y + \sqrt{-5})$, pa bi bilo $P\overline{P}|(y + \sqrt{-5})$, što je nemoguće. Sada dobijemo

$$(y + \sqrt{-5}) = Q^r A \quad \text{i} \quad (y - \sqrt{-5}) = Q^r \overline{A}$$

gdje su A i $\overline{A}$ relativno prosti. Iz $Q^r A Q^r \overline{A} = (x^3) = (x)^3$ vidimo da je $2^r = 2^{3s}$ za neki s, pa je $r = 3s$. Sad je

$$(y + \sqrt{-5}) = Q^{3s} B^3 \quad \text{i} \quad (y - \sqrt{-5}) = Q^{3s} \overline{B}^3$$

za neki ideal B i, konačno, $(y + \sqrt{-5}) = D^3$ za neki ideal D. Kako je D^2 glavni, zaključujemo da je i D glavni, pa je $y + \sqrt{-5} = (a + b\sqrt{-5})^3$ za neke cijele a, b. Lako se vidi da je to nemoguće.

Literatura

[Ga] K. F Gauss, *Disquisitiones Arithmeticae*, 1801.

[Go] T. Gowers, *How to discover a proof of the fundamental theorem of arithmetic*, 2008. http://www.dpmms.cam.ac.uk/~wtg10/FTA.html

[IR] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, 1990.

[La] S. Lang, *Algebra*, Addison-Wesley, 1984.

[Mi] J. Milne, *Algebraic number theory*, 2008. http://www.jmilne.org/math/CourseNotes/ANT301.pdf

[Po] A. van der Poorten, *Notes on Fermat's Last Theorem*, Wiley, 1996.
