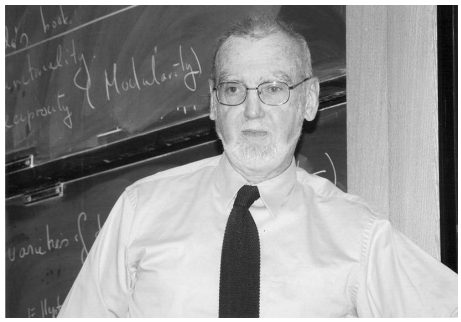
Robert Langlands dobio Abelovu nagradu za 2018. g.

Ivica Gusić[1]

Uvod



Kanadsko-američki matematičar Robert Langlands dobio je Abelovu nagradu iz matematike za 2018. godinu, kako je odbor za nagradu istakao "for his visionary program connecting representation theory to number theory" (za njegov vizionarski program koji povezuje teoriju reprezentacija s teorijom brojeva). Svoje ideje Langlands je 1967. u rukom pisanom pismu od sedamnaest stranica izložio André Weilu. Weil, jedan od najvećih matematičara 20. stoljeća, dao je pretipkati pismo. Kopija je sljedećih desetak godina kružila među matematičarima [6]. Vremenom su te ideje postale poznate kao Langlandsove slutnje, Langlandsov program, katkad i kao Langlandsova filozofija. Imale su velik utjecaj na razvoj matematike posljednjih 50 godina, napose na njenu unifikaciju. Prije dvije godine Abelovu je nagradu dobio Andrew Wiles za rješenje Fermatova teorema [3]. Metode njegova dokaza prirodno se uklapaju u Langlandsov program.

Langlands je rođen 1936. u New Westminsteru, Kanada, u znaku vage. Početkom školovanja ništa nije upućivalo na to da će postati slavan matematičar. Bio je bliži jezicima i književnosti. Uz engleski jezik, Langlands dobro govori francuski, njemački i ruski, ali i turski i talijanski. Kada je imao dvanaest godina na njega i njegov budući život velik je utjecaj izvršio učitelj engleske književnosti. U to je doba upoznao djevojčicu Charlotte s kojom se oženio u devetnaestoj godini za vrijeme studija matematike na Sveučilištu Britanske Kolumbije. Često je znao reći da je vrijeme studiranja najznačajnije prijelazno razdoblje njegova života. Ipak, s četvero male djece i suprugom koja nije dobila pravo rada u SAD-u, bio je na rubu odluke da napusti matematiku. To nije učinio zahvaljujući Charlottinoj podršci [6].

Abel, Galoisova grupa i jedinstvo matematike

Abelovu nagradu dodjeljuje Norveška akademija znanosti za izvanredne doprinose u matematici. Osnovana je 2002. u spomen na velikog norveškog matematičara Nielsa Henrika Abela (1802.–1829.). Dodjeljuje se svake godine, a prvu je 2003. dobio Jean-Pierre Serre, koji se u dobrom dijelu svoje matematičke karijere bavio problematikom

[1] Autor je profesor matematike na Fakultetu kemijskog inženjerstva i tehnologije Sveučilišta u Zagrebu; e-pošta: igusic@fkit.hr

povezanom s Langlandsovim slutnjama. Abel je možda najpoznatiji po dokazu da opća jednadžba 5. stupnja nije rješiva u radikalima. Drugim riječima, ne postoji formula za rješenje jednadžbe

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0 \tag{1}$$

zapisana pomoću koeficijenata a, b, c, d, e koristeći osnovne računske operacije i korjenovanje. Takve formule postoje za jednadžbe stupnja jedan, dva, tri i četiri. Početkom 19. stoljeća još uvijek nije bilo poznato postoje li i za jednadžbu petog stupnja. Prvi potpun dokaz da ne postoje dao je Abel 1824. kad je imao samo 22 godine [7]. U dokazu, a naročito u daljnjem istraživanju doveo je u vezu algebru s teorijom kompleksnih funkcija koja je tada bila tek u začetku. Abel je bio jedan od pionira ideja koje su vodile do Langlandsova programa.

Jednadžbu (1) obično se razmatra nad $\mathbb{Q}$, što znači da su koeficijenti racionalni brojevi. Tada su rješenja algebarski brojevi. U ovom kontekstu nerješivost u radikalima znači da postoji izbor koeficijenata takav da se rješenja ne mogu dobiti iz racionalnih brojeva pomoću osnovnih računskih operacija i korjenovanja. Najmanje polje koje sadrži rješenja zove se *polje razlaganja* jednadžbe. Automorfizmi tog polja čine grupu s obzirom na kompoziciju. Na primjer, polje razlaganja jednadžbe

$$x^2 + 1 = 0$$

kojoj su rješenja $\pm i$, je $\mathbb{Q}(i)$ koje se sastoji od svih kompleksnih brojeva oblika $a + bi$, gdje su a, b racionalni brojevi. Prema definiciji, automorfizam ostavlja na miru racionalne brojeve i čuva operacije. Zato pripadna grupa ima dva elementa: trivijalni automorfizam koji sve ostavlja na miru i kompleksno konjugiranje (ono permutira i i $-i$). Naime, ako je ψ automorfizam, onda je $\psi(i)^2 = \psi(i^2) = \psi(-1) = -1$. Zato je $\psi(i) = i$ ili $-i$.

Jednadžbe koje se mogu rastaviti svode se na pripadne jednadžbe povezane s faktorima. Na primjer, jednadžba $x^5 - 1 = 0$ može se zapisati kao $(x-1)(x^4+x^3+x^2+x+1) = 0$, što je ekvivalentno s $x - 1 = 0$ ili $x^4 + x^3 + x^2 + x + 1 = 0$. Druga se jednadžba ne može dalje rastavljati. Takve se jednadžbe nazivaju *ireducibilnim* (nad $\mathbb{Q}$). Pri razmatranju rješivosti uvijek se može pretpostaviti da su jednadžbe ireducibilne, makar to nije nužno.

Abel je dokazao da postoje jednadžbe petog stupnja koje nisu rješive u radikalima. S druge strane, za svaki n postoje ireducibilne jednadžbe n-tog stupnja rješive u radikalima, primjerice $x^n - 2 = 0$. Postavlja se pitanje postoji li kriterij za rješivost jednadžbe u radikalima. Odgovor je dao genijalni francuski matematičar Évariste Galois (1811.–1832.): jednadžba je rješiva u radikalima ako i samo ako joj je grupa automorfizama polja razlaganja rješiva. U njegovu čast ta se grupa naziva *Galoisova grupa*. Tako je teško pitanje o jednadžbama svedeno na jednostavnije pitanje o (konačnim) grupama. Galoisova grupa opće jednadžbe stupnja većeg ili jednakog 5 nije rješiva pa opća jednadžba stupnja ≥ 5 nije rješiva u radikalima.

Abel je dokazao da je svaka jednadžba kojoj je Galoisova grupa komutativna nužno rješiva u radikalima. Zato se komutativne grupe i nazivaju abelovim. Taj rezultat poseban je slučaj Galoisova jer je svaka abelova grupa rješiva, dok obratno ne vrijedi. Intuitivno, grupa je rješiva ako se može izgraditi iz blokova koji su abelove grupe (to se može i preciznije izreći).

Značaj Galoisova rezultata daleko je nadmašio njegovu ulogu u pitanju rješenja u radikalima. Njegove ideje (Galoisova teorija) postale su važne i u drugim pitanjima algebre, teorije brojeva, algebarske geometrije, topologije pa čak i diferencijalnih jednadžba. One su bile naznaka i dubljih veza između različitih matematičkih područja, odnosno jedinstva matematike. Jedna od takvih dubokih veza je i u Langlandsovu programu kojemu je Galoisova teorija jedna od glavnih sastojnica. Pokazalo se da je slučaj abelovih Galoisovih grupa bitno jednostavniji i dostižan, dok je opći slučaj još uvijek nerazriješen.

Primjer nekomutativne Galoisove grupe

Jednadžba $x^3 - 2 = 0$ ima rješenja $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$, gdje je $\sqrt[3]{2}$ realni treći korijen iz 2, a $\omega = \dfrac{-1+\sqrt{-3}}{2}$, kompleksni treći korijen iz jedinice. Vrijedi $\omega^2 = \bar{\omega} = -\omega - 1$. Polje razlaganja jednadžbe čine svi brojevi oblika $a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4} + b_1\omega + b_2\sqrt[3]{2}\omega + b_3\sqrt[3]{4}\omega$, gdje su a_1, a_2, a_3, b_1, b_2, b_3 racionalni brojevi.

Galoisova grupa ima 6 elemenata: e, τ, τ^2, σ, $\tau\sigma$, $\tau^2\sigma$, gdje je e neutralni element, dok se τ i σ definirani na sljedeći način. Rješenja $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ označimo redom kao 1, 2, 3. Tada je $\tau = (123)$, što znači da 1 ide u 2, 2 u 3, a 3 u 1. Tada je $\tau^2 = (132)$. Dalje, $\sigma = (1)(23)$ što znači da 1 ostaje na mjestu, a 2, 3 se permutiraju. Uz dogovor da $\tau\sigma$ znači da najprije djeluje τ, potom σ, vrijedi $\tau\sigma = (13)(2)$ i $\tau^2\sigma = (12)(3) = \sigma\tau$ iz čega se vidi da je $\tau\sigma \neq \sigma\tau$ pa je grupa nekomutativna.

Ova je grupa rješiva: može se izgraditi iz abelovih grupa $\{e, \tau, \tau^2\}$ i $\{e, \sigma\}$ kao umnožak svakog elementa iz prve grupe sa svakim elementom druge, uz relaciju $\sigma\tau = \tau^2\sigma$.

Prosti brojevi i Riemannova zeta funkcija

Prirodni brojevi jednoznačno se rastavljaju na umnožak prostih, odatle njihov značaj u teoriji brojeva. Još je Euklid dokazao da ima beskonačno mnogo prostih brojeva, ali mnoge su druge zagonetke ostale, primjerice pitanje koliko ima prostih brojeva do zadanog broja. Uobičajena je oznaka $\pi(x)$ za broj prostih brojeva manjih ili jednakih x [8]. Na primjer $\pi(10) = 4$ (prosti brojevi 2, 3, 5, 7). Slično, $\pi(1000) = 168$ i $\pi(10\,000) = 1229$. Legendre i Gauss su na osnovi primjera primijetili da je

$$\pi(x) \approx \frac{x}{\ln x}. \tag{2}$$

Zaista, $\dfrac{1000}{\ln(1000)} \approx 144.8$, što nije daleko od 168. Slično $\dfrac{10\,000}{\ln(10\,000)} \approx 1085.7$, što je blizu 1229. Makar je tu apsolutna pogreška veća, relativna je manja. Naime $\dfrac{168}{144.8} \approx 1.16$, dok je $\dfrac{1229}{1085.7} \approx 1.13$. Gauss je postavio slutnju da omjer između $\pi(x)$ i $\dfrac{x}{\ln x}$ teži prema 1 kad x teži u $+\infty$ (odnosno da su $\pi(x)$ i $\dfrac{x}{\ln x}$ *asimptotski jednaki*). To je dokazano koncem 19. stoljeća koristeći svojstva Riemannove zeta funkcije koje na prvi pogled nemaju nikakve veze s prostim brojevima.

Riemannova zeta funkcija

Riemannova zeta funkcija izvire iz formule

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots \tag{3}$$

gdje je s na početku bio realan broj veći od 1 (za $s = 1$ ili $s < 1$ izraz na desnoj strani je beskonačan). Bernhard Riemann (1826.–1866.) prvi je počeo razmatrati taj izraz za kompleksne vrijednosti s uz uvjet da je realni dio od s veći od 1 ($\mathrm{Re}\,(s) > 1$). U formulu

(3) ne mogu se uvrstiti brojevi s kojima je realni dio manji ili jednak od 1. Riemann je pokazao da je njome ipak određena kompleksna analitička funkcija definirana za svaki s osim za $s = 1$. Tako proširena funkcija $\zeta(s)$ naziva se Riemannovom zeta funkcijom. Ona ima vrijednost 0 u negativnim parnim brojevima (trivijalne nultočke). Riemann je postavio slutnju da su ostale (netrivijalne) nultočke unutar pravca $\mathrm{Re}\,(s) = 1/2$ i obrazložio kako bi posljedica njene istinitosti bila vrlo precizna približna formula za $\pi(x)$. To je možda najslavnija neriješena slutnja u matematici.

Koliko je ta slutnja važna za proste brojeve vidi se i iz toga što rečeni dokaz da omjer između $\pi(x)$ i $\dfrac{x}{\ln x}$ teži prema 1 slijedi iz dokaza da $\zeta(s)$ nema nultočaka na pravcu $\mathrm{Re}\,(s) = 1$.

Prosti brojevi u aritmetičkim nizovima i Dirichletove L-funkcije

Beskonačni red (3) može se napisati u obliku beskonačnog produkta

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots = \frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdots \tag{4}$$

koji se zove *Eulerov produkt*. Faktori na desnoj strani indeksirani su prostim brojevima: uz prosti broj p ide faktor $\dfrac{1}{1-p^{-s}}$. To djelomice objašnjava zašto $\zeta(s)$ ima veze s prostim brojevima.

Lako je zamisliti da umjesto $1 - p^{-s}$ može stajati $1 - a_p \cdot p^{-s}$, gdje su a_p nekakvi kompleksni brojevi. Kad bi se izvršilo množenje dobila bi se jednakost oblika

$$1 + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \frac{a_4}{4^s} + \ldots = \frac{1}{1-a_2 \cdot 2^{-s}} \cdot \frac{1}{1-a_3 \cdot 3^{-s}} \cdot \frac{1}{1-a_5 \cdot 5^{-s}} \cdots \tag{5}$$

kojoj je s lijeve strane *Dirichletov red*, a s desne njegov Eulerov produkt. Riemannova zeta funkcija isto je Dirichletov red. Kod nje je $a_n = 1$ za sve n.

Nije svaki izbor koeficijenata a_p zanimljiv za teoriju brojeva, već samo neki posebni. Prve takve otkrio je Dirichlet 1837. i pomoću njih dokazao teorem o prostim brojevima u aritmetičkim nizovima. Na primjer, taj teorem tvrdi da ima beskonačno mnogo prostih brojeva oblika $4k + 1$, a također oblika $4k + 3$, za $k = 0, 1, 2, 3, 4, \ldots$. Dirichletova metoda dokaza primijenjena na ovaj slučaj svodi se na to kao da je izabrano $a_p = 1$ za $p \equiv 1 \pmod 4$ i $a_p = -1$ za $p \equiv 3 \pmod 4$, te $a_2 = 0$. Pripadni Dirichletov red dobio bi se množenjem izraza $\dfrac{1}{1 \pm p^{-s}}$ za $p \neq 2$. Taj se red zove Dirichletova L-funkcija (za ovaj izbor koeficijenata a_p). Ona ima slična svojstva kao i Riemannova, samo se proširuje na cijelu kompleksnu ravninu, dakle ima vrijednost i u $s = 1$. Nadalje, vrijednost u 1 različita je od nule. Koristeći svojstva ove L-funkcije i Riemannove zeta funkcije dokazuje se ne samo da ima beskonačno mnogo prostih brojeva oblika $4k + 1$, kao i oblika $4k + 3$, već da tih brojeva ima u prosjeku jednako. Na primjer, do $x = 100$ za 11 prostih brojeva p je $p \equiv 1 \pmod 4$, a za 13 je $p \equiv 3 \pmod 4$.

Za druge module m zaključuje se analogno kao i za $m = 4$, samo što je tehnički složenije. Tada umjesto dviju L-funkcija ima ih $\phi(m)$ (broj prirodnih brojeva manjih od m, relativno prostih s m). Kad je Dirichlet objavio dokaz, Riemann je još bio dječak i nije postajala njegova zeta funkcija. Dirichlet je razmatrao samo realne vrijednosti varijable s veće od 1. Za dokaz je presudno bilo najprije dokazati da postoji limes kad s ide u 1 i da je taj limes različit od nule.

Dirichletove L-funkcije za ostatke modulo 5

Skicirat ćemo konstrukciju Dirichletovih L-funkcija za ostatke modulo 5. Prosti brojevi različiti od 5 mogu imati ostatak 1, 2, 3 ili 4 modulo 5. Ovi se ostatci mogu množiti modulo 5 tako da se dobije komutativna grupa. Na primjer $3 \cdot 4 = 12 = 2$, inverz od 2 je 3 jer je $2 \cdot 3 = 6 = 1$, itd. Da bi dobio obične brojeve, Dirichlet je gledao homomorfizme (karaktere) χ grupe ostataka u multiplikativnu grupu kompleksnih brojeva, dakle $\chi(ab) = \chi(a)\chi(b)$ za svaka dva ostatka. Rezultati moraju biti unutar četvrtih korijena iz 1. Karakter je određen čim se zna $\chi(2)$, jer je $2^2 = 4$, $2^3 = 3$, $2^4 = 1$. Zato ima četiri mogućnosti: χ_1 kad su sve vrijednosti 1 (trivijalni karakter), χ_2 kad je $\chi_2(2) = \chi_2(3) = -1$ i $\chi_2(1) = \chi_2(4) = 1$ (kvadratni karakter), χ_4 kad je $\chi_4(2) = i$, $\chi_4(3) = -i$, $\chi_4(1) = 1$, $\chi_4(4) = -1$, te $\bar{\chi}_4$ (rezultati se kompleksno konjugiraju).

Za svaki karakter χ postoji Dirichletova L-funkcija $L(\chi, s)$ prema pravilu: ako je $p \equiv k \pmod 5$, onda je $a_p = \chi(k)$, $k = 1, 2, 3, 4$. Na primjer, za $L(\chi_4, s)$ vrijedi:

(i) ako je $p \equiv 1 \pmod 5$, onda je Eulerov faktor $\dfrac{1}{1 - p^{-s}}$.

(ii) ako je $p \equiv 2 \pmod 5$, onda je Eulerov faktor $\dfrac{1}{1 - i \cdot p^{-s}}$.

(iii) ako je $p \equiv 3 \pmod 5$, onda je Eulerov faktor $\dfrac{1}{1 + i \cdot p^{-s}}$.

(iv) ako je $p \equiv 4 \pmod 5$, onda je Eulerov faktor $\dfrac{1}{1 + p^{-s}}$.

Dirichletov teorem u ovom slučaju kaže da u prosjeku ima jednako prostih brojeva u svakoj od ovih četiriju klasa, posebno ih u svakoj ima beskonačno mnogo.

Zakon reciprociteta i Artinova L-funkcija

Dirichlet je do L-funkcija došao u kontekstu rješavanja problema prostih brojeva u aritmetičkim nizovima. Naime, iako Riemannova zeta funkcija kontrolira mnoga svojstva prostih brojeva, ona nije bila dovoljna za taj problem. Za matematiku je karakteristično da ideje ili metode ne gleda izolirano, već ih pokušava sagledati dijelom veće, savršenije cjeline (i po tome je bliža konceptualnoj umjetnosti nego znanosti). Često širi kontekst nije izravno vidljiv, već izranja tek nakon preformuliranja i reinterpretacije izvorne ideje. Tako koeficijenti a_p iz Dirichletovih L-funkcija imaju važnu interpretaciju u algebarskoj teoriji brojeva. U najjednostavnijem slučaju, prosti brojevi p oblika $4k + 1$ upravo su oni koji se rastavljaju u polju razlaganja $\mathbb{Q}(i)$ jednadžbe $x^2 + 1 = 0$. Na primjer $5 = (2 + i)(2 - i)$. Za njih je $a_p = 1$. Ako je pak $p \equiv 3 \pmod 4$, onda p ostaje prost. Za takve p je $a_p = -1$. Ta je činjenica sadržana u posebnom slučaju Gaussova zakona kvadratnog reciprociteta koji je bio važna tema teorije brojeva 19. stoljeća [2], [5]. Polje razlaganje jednadžbe $x^2 + 1 = 0$ ujedno je i polje razlaganja jednadžbe $x^4 - 1 = 0$. Naime $x^4 - 1 = (x^2 - 1)(x^2 + 1)$, a rješenja od $x^2 - 1 = 0$ ne doprinose polju razlaganja.

Slična je interpretacija za ostale module kada se pojavljuje opći kvadratni zakon reciprociteta. Općenito, za modul m gleda se polje razlaganja jednadžbe $x^m - 1 = 0$, kojoj su rješenja m-ti korijeni iz jedinice (ciklotomsko polje). Galoisova grupa tog polja je abelova. Tako se Dirichletove L-funkcije mogu shvatiti kao funkcije pridružene ciklotomskim poljima. To ćemo ilustrirati na primjeru $m = 5$.

Reinterpretacija Dirichletovih L-funkcija za ostatke modulo 5

Jednadžba $x^5 - 1 = 0$ ima rješenja z, z^2, z^3, z^4 i $z^5 = 1$, gdje je $z = \cos\left(\frac{2\pi}{5}\right) + i \cdot \sin\left(\frac{2\pi}{5}\right)$. Galoisova grupa polja razlaganja ima 4 elementa, ovisno u koju potenciju od z taj automorfizam preslikava z. Naime, automorfizam rješenje mora preslikati u rješenje, a ne može z preslikati u 1 (jer već 1 preslikava u 1). Kompozicija dvaju automorfizama u skladu je s množenjem ostataka modulo 5. Na primjer, kompozicija automorfizma koji z šalje u z^4 s onim koji z šalje u z^3, je automorfizam koji z šalje u $z^{12} = z^2$, što je u skladu s tim da je $4 \cdot 3 = 12 = 2$. Zato se multiplikativna grupa ostataka modulo 5 može interpretirati kao Galoisova grupa ciklotomskog polja za $m = 5$: ostatak k odgovara automorfizmu koji z preslikava u z^k. Sad se (4) može reinterpretirati tako da se prostom broju sa svojstvom $p \equiv k \pmod 5$ pridružuje element Galoisove grupe ciklotomskog polja koji odgovara ostatku k. Pri toj interpretaciji Dirichletovi karakteri postaju homomorfizmi Galoisove grupe u multiplikativnu grupu kompleksnih brojeva. Tako se Dirichletove L-funkcije interpretiraju u terminima Galoisove grupe.

Artinove L-funkcije, komutativni slučaj

Proširujući pristup iz prethodnog, austrijski matematičar Emil Artin (1898.–1962.) dvadesetih godina 20. stoljeća poopćio je Dirichletove L-funkcije na sva polja kojima je Galoisova grupa abelova. Njegov postupak sastoji se od dva koraka.

U prvom se svakom prostom broju p (osim nekih izuzetaka) pridruži element iz Galoisove grupe: Frobeniusov automorfizam od p, oznaka $\mathbf{Fr}_p$ (naziv je prema njemačkom matematičaru Frobeniusu koji je prvi opisao taj postupak).

U drugom koraku primjenjuje se homomorfizam (karakter) Galoisove grupe G u multiplikativnu grupu kompleksnih brojeva, uključujući i trivijalni karakter. Karakter svakom elementu grupe pridružuje neki korijen iz jedinice.

Broj karaktera jednak je broju elemenata grupe. Za svaki se karakter Galoisove grupe svakom prostom broju p (osim nekih izuzetaka) pridružuje korijen iz jedinice. To je a_p koji određuje izraz $\frac{1}{1 - a_p \cdot p^{-s}}$, a množenjem tih izraza dobije se pripadna Artinova L-funkcija (za taj karakter). Sve skupa, dobije se onoliko Artinovih L-funkcija koliko ima elemenata Galoisove grupe. Pri ovoj interpretaciji Dirichletove L-funkcije ujedno su i Artinove. Da se ova dva skupa L-funkcija poklapaju proizlazi iz slavnog Kronecker-Weberova teorema.

Artinove L-funkcije, nekomutativni slučaj

Ovaj pristup Artin je uz neke modifikacije primijenio i na polja razlaganja kojima Galoisova grupa nije abelova. Prva je razlika u tome što se prostom broju ne pridružuje Frobeniusov automorfizam već podskup Galoisove grupe – Frobeniusov element. Druga je što se osim karaktera trebaju uključiti i homomorfizmi kojima su vrijednosti u grupama matrica s kompleksnim koeficijentima: *reprezentacije* Galoisove grupe.

Uobičajeno je multiplikativnu grupu matrica n-tog reda označavati kao $\mathbb{G}\mathrm{l}_n$. Ako se hoće naglasiti da su koeficijenti kompleksni, piše se $\mathbb{G}\mathrm{l}_n(\mathbb{C})$, ako su racionalni $\mathbb{G}\mathrm{l}_n(\mathbb{Q})$ itd. Reprezentacije s vrijednostima u $\mathbb{G}\mathrm{l}_n$ nazivaju se n-dimenzionalnim reprezentacijama.

Ilustrirat ćemo na primjeru Galoisove grupe jednadžbe $x^3 - 2 = 0$ koju smo uveli pri kraju drugog odlomka. Pridruživanje Frobeniusovih elemenata prostim brojevima može se provesti općenito [1]. U ovom primjeru prosti brojevi različiti od 3 dijele se u tri skupine, povezane s time kako se rastavljaju u polju razlaganja

(i) ako je $p \equiv 2 \pmod 3$, onda je $\mathbf{Fr}_p$ klasa $\{\sigma, \tau\sigma, \tau^2\sigma\}$.

(ii) ako je $p \equiv 1 \pmod 3$ i još 2 kub modulo p, onda je $\mathbf{Fr}_p = e$, neutralni element Galoisove grupe.

(iii) ako je $p \equiv 1 \pmod 3$, a 2 nije kub modulo p, onda je $\mathbf{Fr}_p$ klasa $\{\tau, \tau^2\}$.

Na primjer, od prostih brojeva manjih od 100 njih 12 je u skupini (i). To su 2, 5, 11, 17, 23, 41, 47, 53, 59, 71, 83 i 89. Samo dva su u skupini (ii): 31 i 43. Na primjer, $4^3 = 64 = 2 \cdot 31 + 2$ pa je 2 kub modulo 31. Devet ih je u skupini (iii): 7, 13, 19, 37, 61, 67, 73, 79 i 97.

Za ovo polje razlaganja imaju tri temeljne (ireducibilne) reprezentacije Galoisove grupe. Uz trivijalnu (kojoj su svi $a_p = 1$), jednodimenzionalna je i ona koja τ (pa onda i τ^2) preslikava u 1, dok σ (pa onda i $\tau\sigma, \tau^2\sigma$) preslikava u -1. Za nju je $a_p = 1$ ako je $p \equiv 1 \mod 3$, a $a_p = -1$ ako je $p \equiv 2 \mod 3$. Artinove L-funkcije za ove reprezentacije konstruiraju se poput Dirichletovih.

Ima i jedna ireducibilna dvodimenzionalna reprezentacija ρ ove Galoisove grupe. Ona τ preslikava u $\rho(\tau) = \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}$, gdje je, kao i prije, $\omega = \dfrac{-1 + \sqrt{-3}}{2}$, kompleksni treći korijen iz jedinice, dok σ preslikava u $\rho(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. U ovom slučaju faktor u nazivniku Eulerova produkta nije linearan s obzirom na p^{-s} već kvadratan. Preciznije, oblika je

$$\frac{1}{1 - a_p \cdot p^{-s} + b_p \cdot p^{-2s}} \tag{6}$$

gdje je a_p trag pripadne matrice (zbroj elemenata na glavnoj dijagonali), a b_p determinanta. Slijedi opis Eulerovih faktora za za ovu reprezentaciju.

Neutralni element e preslikava se u jediničnu matricu $\rho(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, kojoj je trag $1 + 1 = 2$, a determinanta $1 \cdot 1 = 1$, pa je, za p iz (ii), Eulerov faktor $\dfrac{1}{1 - 2 \cdot p^{-s} + p^{-2s}} = \dfrac{1}{(1 - p^{-s})^2}$.

Kako je za $\rho(\tau)$ trag $\omega + \bar{\omega} = -1$ i determinanta $\omega \cdot \bar{\omega} = 1$ (a isto je i za $\rho(\tau^2)$ makar su matrice različite), za p iz (iii), Eulerov faktor je $\dfrac{1}{1 + p^{-s} + p^{-2s}}$.

Za $\rho(\sigma)$ trag je 0, a determinanta -1 (isto je za cijelu klasu) pa je, za p iz (i), Eulerov faktor $\dfrac{1}{1 - p^{-2s}} = \dfrac{1}{(1 - p^{-s})(1 + p^{-s})}$.

Pripadna Artinova L-funkcija pridružena ovoj reprezentaciji dobije se množenjem Eulerovih faktora. Artinove L-funkcije definiraju se za sve reprezentacije, a ne samo za ireducibilne. One isto mogu biti važne za teoriju brojeva. Na primjer, umnožak ovih triju L-funkcija je Dedekindova zeta funkcija polja razlaganja jednadžbe $x^3 - 2 = 0$. Kao Artinova L-funkcija ona dolazi od direktne sume ovih triju ireducibilnih reprezentacija.

Langlandsove slutnje

Za dokaz slutnja o L-funkcijama u abelovom slučaju Artin je preformulirao jednu od najznačajnijih teorija algebarske teorije brojeva s kraja 19. i prve polovice 20. stoljeća: teoriju polja klasa. Njegova formulacija naziva se Artinov zakon reciprociteta. On je i za L-funkcije neabelovih proširenja formulirao analogne slutnje. One imaju značenje neabelova zakona reciprociteta (još uvijek nedokazanoga).

L-funkcije eliptičkih krivulja i modularne forme

U međuvremenu je definirano više različitih zeta funkcija i L-funkcija. Sve one imaju slična svojstva, za njih su formulirane slične slutnje i sve su značajne za teoriju brojeva. Ovdje ćemo spomenuti L-funkcije eliptičkih krivulja nad poljem racionalnih brojeva: krivulja koje se mogu zapisati jednadžbom

$$y^2 = x^3 + ax + b, \tag{7}$$

gdje su a, b cijeli brojevi. Eulerovi faktori (osim njih nekoliko) tih L-funkcija su oblika $\dfrac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}}$. Tu je $a_p = p - N_p$, gdje je N_p broj rješenja jednadžbe (7) modulo p. Na primjer jednadžba $y^2 = x^3 - 6x$ modulo 5 postaje $y^2 = x^3 - x$. Njena su rješenja $(0,0)$, $(1,0)$, $(2,1)$, $(2,4)$, $(3,2)$, $(3,3)$, $(4,0)$ pa je $N_5 = 7$, odnosno $a_5 = -2$. Pripadni Eulerov faktor je $\dfrac{1}{1 + 2 \cdot 5^{-s} + 5 \cdot 5^{-2s}}$. Slutnje analogne onima za Artinove L-funkcije formulirane su polovicom 20. stoljeća i za ove funkcije, također s ograničenim uspjehom. Stanje se promjenilo kad su izvorne slutnje preformulirane na način da bi ovi Dirichletovi redovi trebali dolaziti od modularnih forma: vrlo specifičnih analitičkih funkcija definiranih na gornjoj kompleksnoj poluravnini. Nije bilo čvrstih razloga zašto bi tako bilo jer je riječ o, na prvi pogled, potpuno različitim matematičkim objektima. Kad je koncem 20. stoljeća Wiles dokazao tu slutnju za dosta široku klasu eliptičkih krivulja, dokazao je i Fermatov teorem.

Langlandsova intervencija

Šezdesetih godina 20. stoljeća još uvijek nije bilo većih pomaka u rješavanju Artinovih slutnja. Ipak tada su sazrele ideje koje su rezultirale Langlandsovim preformulacijama problema koje su onda omogućile ozbiljan napredak. Sam Langlands često je znao reći kako bi i netko drugi došao do toga da nije on, da se on jednostavno našao na pravom mjestu u pravo vrijeme [6], poglavlje 3. U relativno dugom razdoblju različiti matematičari ili matematičke grupe rade (ili misle da rade) različite stvari. Poslije se ustanovi da su jednu te istu stvar osvjetljavali s različitih gledišta i različitim metodama. Progres koji je vodio do Langlandsovih slutnja rezultat je rada niza matematičara od kojih su mnogi s teorijom brojeva uglavnom imali tek neke dodirne točke. Bili su bliže analizi, poglavito harmonijskoj analizi, teoriji koja je nastala kao široka generalizacija i apstrakcija Fourierove analize. Začetak Fourireve analize je u radu francuskog matematičara i fizičara Fouriera iz 1807. godine, u kojemu je pokazao kako se funkcije mogu razviti u beskonačan red sinusa i kosinusa. Ta je teorija dugo bila povezana s primjenama, na primjer u teoriji valova i glazbe. Sredinom 20. stoljeća iz te je teorije nastala apstraktna harmonijska analiza zasnovana na (beskonačno

dimenzionalnim) reprezentacijama grupa, poput grupa $\mathbb{G}\mathrm{l}_n$. Pokazalo se da je to bio prirodan okvir za preformulaciju Artinovih slutnja.

Langlandsov program, u svom manjem dijelu, predlaže vrlo općenitu konstrukciju Dirichletovih redova i predviđa da su oni važni za teoriju brojeva. Kao specijalni slučaj oni bi trebali sadržavati Artinove L-funkcije. Ta se konstrukcija zasniva na vrlo specifičnim (automorfnim) reprezentacijama tzv. reduktivnih grupa. Najjednostavnije reduktivne grupe su već spomenute grupe $\mathbb{G}\mathrm{l}_n$. Artinove L-funkcije pridružene n-dimenzionalnim reprezentacijama Galoisove grupe trebale bi dolaziti od automorfnih reprezentacija od $\mathbb{G}\mathrm{l}_n$. Kad bi se to dokazalo bile bi dokazane i Artinove slutnje. Langlands je pokazao da Artinove L-funkcije i pripadna teorija u abelovom slučaju koincidira s automorfnim reprezentacijama od $\mathbb{G}\mathrm{l}_1$. Još je daleko od dokaza Langlandsovih slutnja, makar je bilo vrlo ozbiljnih rezultata. Na primjer, gotovo u potpunosti je riješen slučaj $\mathbb{G}\mathrm{l}_2$.

Eulerovi faktori L-funkcija eliptičkih krivulja iz (7), koje su imale presudnu ulogu u dokazu Fermatova teorema, imaju kvadratne faktore u nazivniku (osim nekih). Po tome sliče Artinovim L-funkcijama pridruženim dvodimenzionalnim reprezentacijama. One se mogu i dobiti analogno: preko određenih dvodimenzionalnih (l-adskih) reprezentacija Galoisove grupe. Ipak, one nisu Artinove L-funkcije, ali se uklapaju u Langlandsov program preko automorfnih reprezentacija grupe $\mathbb{G}\mathrm{l}_2$.

Literatura

[1] T. Dokchiters, V. Dokchiters, *Identifying Frobenius Elements in Galois Groups*, Algebra and Number Theory, Vol. 7, No 6 (2013), (1325–1352).

[2] A. Dujella, *Uvod u teoriju brojeva* (skripta), PMF-Matematički odjel Sveučilište u Zagrebu, https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf

[3] I. Gusić, *Andrew Wiles dobio Abelovu nagradu*, MFL, LXVII 1, 7–13, Zagreb, (2016–2017).

[4] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Second edition, GTM, Spinger (1990).

[5] B. Mazur, W. Stein, *Prime Numbers and the Riemann Hypothesis*, Cambridge University Press (2016).

[6] J. Mueller, *On the genesis of Robert P. Langlands' conjectures and his letter to Andreé Weil*, Bull. Amer. Math. Soc., 2018, http://www.ams.org/journals/bull/0000-000-00/S0273-0979-2018-01609-1/home.html

[7] M. Rosen, *Niels Hendrik Abel and Equations of the Fifth Degree*, Amer. Math. Montly, Vol. 2, Issue 6, (1995) (495–505).

[8] *Prime-counting function*, https://en.wikipedia.org/wiki/