Uvod u aritmetiku eliptičkih krivulja

L-funkcija eliptičke krivulje (skica) - 25. lekcija

Prototip L-funkcije je (kompleksna) Riemannova zeta funkcija

$$\zeta(s) := \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}$$

za $Res > 1$, a produkt ide po svim prostim brojevima (Eulerov produkt). Riemannova zeta funkcija važna je jer u sebi nosi informaciju o dobrom dijelu tajne o prostim brojevima.
Prva generalizacija Riemannove zeta funkcije (i njoj srodnih) jest takva funkcija kojoj Eulerov produkt u nazivnicima ima kvadratne izraze (u p^{-s}). Takva je L-funkcija eliptičke krivulje E nad $\mathbf{Q}$ (uz izuzetak konačno mnogo faktora za proste p u kojima E ima lošu redukciju). Ona ima važnu ulogu u aritmetici eliptičkih krivulja.
Neka je E eliptička krivulja nad $\mathbf{Q}$ s globalnim minimalnim modelom (tada ona u pravilu ima općenitiju jednadžbu od one $y^2 = x^3 + ax^2 + bx + c$).
Neka je Δ diskriminanta od E i neka je E_p pripadna krivulja dobivena iz E redukcijom njene jednadžbe modulo p. Znamo da vrijedi:
(I) Ako je p ne dijeli Δ onda je E_p opet eliptička krivulja; tada definiramo $a_p := p + 1 - N_p$ gdje je N_p broj točaka na reduciranoj krivulji, s koordinatama iz $\mathbf{F}_p$;
vrijedi $|a_p| < 2\sqrt{p}$ (Hasse-Weilova ocjena - analogon Riemannove slutnje): tada definiramo pripadni Eulerov p-faktor L- funkcije kao

$$L_p(E, s) := \frac{1}{1 - a_p p^{-s} + p \cdot p^{-2s}}$$

(vidimo da je u nazivniku kvadratan faktor - on ima i aritmetičko značenje koje sad ne obradjujemo).
(II) Ako $p|\Delta$ (znači za konačno mnogo p) onda je redukcija loša, reducirana krivulja je singularna kubika (ima genus 0) i imamo dva slučaja.
(i) redukcija je multiplikativna (ili polustabilna) - tipični je primjer $y^2 = x^3 + ax^2$ sa singularnom točkom $(0, 0)$ (dvostruka točka ili node) i opet imamo dva podslučaja:

(A) Rascjepivi slučaj (kad su tangente na grane u singularnoj točki definirane nad $\mathbf{F}_p$, tj. kad je a kvadrat); tada definiramo

$$L_p(E,s) := \frac{1}{1-p^{-s}}$$

(B) Nerascjepivi slučaj (kad tangente na grane u singularnoj točki nisu definirane nad $\mathbf{F}_p$, tj. kad a nije kvadrat); tada definiramo

$$L_p(E,s) := \frac{1}{1+p^{-s}}.$$

(ii) redukcija je aditivna (nestabilna) - tipični je primjer $y^2 = x^3$ sa singularnom točkom $(0,0)$ (šiljak ili kasp); tada definiramo

$$L_p(E,s) = 1$$

Konačno definiramo L- funkciju od eliptičke krivulje E kao

$$L(E,s) := \prod_p L_p(E,s) = \sum_{n\geq 1} \frac{a_n}{n^s}.$$

Ako dodatno definiramo da je $a_p = 1$ za multiplikativni rascjepivi slučaj, $a_p = -1$ za multiplikativni nerascjepivi slučaj i $a_p = 0$ za aditivni, vrijedi

$$L(E,s) = \prod_{p \text{ ne dijeli } \Delta} \frac{1}{1-a_p p^{-s} + p\cdot p^{-2s}} \prod_{p|\Delta} \frac{1}{1-a_p p^{-s}}$$

.

Konstrukcija L-funkcije eliptičke krivulje (nad Q) iz l-adske reprezentacije Galoisove grupe.

Pokazuje se da informacije o L-funkciji eliptičke krivulje nosi pripadna l-adska reprezentacija Galoisove grupe $G := \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Time će se dobiti uniformna definicija L-funkcije, što je osnova njenog suvremenog proučavanja.
Podsjetimo da smo u Teoremu u 24. lekciji naveli da za prosti broj p koji je različit od l i u kojemu je redukcija dobra, vrijedi

$$a_p = tr\rho_{E,l}Frob_p \ i \ det\rho_{E,l}Frob_p = p$$

Podsjetimo, takodjer da tu l-adska reprezentacija $\rho_{E,l}$ nije išla s cijele Galoisove grupe G, veś njene podgrupe $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$, gdje je $K_{E,l}$ polje generirano koordinatama točaka reda l^n za $n \geq 1$.

Kako se ta polja mijenjaju za različite E i l, dobro je to izbjeći proširenjem reprezentacija na G (a i inače, G je središnji objekt suvremene aritmetike, pa ovo gledamo tako da variranjem E ili, općenito, abelovih mnogostrukosti i sličnih geometrijskih objekata, dobivamo familije reprezentacija od G za sve proste l). Kako smo vidjeli, to se prirodno provodi tako da najprije napravimo restrikciju s G na $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$, potom komponira s $\rho_{E,l}$; kompoziciju opet označimo kao $\rho_{E,l}$ (što ne bi trebalo stvarati zabunu). Naravno, uz ovaj dobitak, dolazi i do gubitaka; prvi je što l-adska reprezentacija s G nije više vjerna (injektivna), a drugi je što sad ni jedan p nije nerazgranat. Zato nastaje problem s tragom i determinantom Frobeniusovih elemenata. Posljednja se poteškoća tu može razriješiti.
(I) Neka je u p redukcija dobra i $p \neq l$. Tada je, prema teoremu Serrea i Tatea, $\rho_{E,l}$ djeluje trivijalno na sve elemente od I_p - to je inače definicija nerazgranatosti reprezentacije u p (jer je restrikcija te grupe na $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$ trivijalna grupa); zato ni trag ni determinanta matrica koje pripadaju elementima koje čine $Frob_p$ ne ovise o reprezentantima, pa su oni jednoznačno definirani i vrijedi

$$a_p = tr\rho_{E,l}Frob_p \ i \ det\rho_{E,l}Frob_p = p$$

(gdje, za razliku od prijašnjih idfentičnih formula po izgledu, $Frob_p$ se odnosi na cijelu grupu G). Uočite da se sad p faktor L-funkcije može zapisati kao

$$L_p(E,s) = \frac{1}{\det(I - (\rho_{E,l}Frob_p)p^{-s})}$$

(II) Neka je u p redukcija loša i neka je $p \neq l$.
Tada $\rho_{E,l}$ djeluje trivijalno na sve elemente od I_p, tj. matrice koje su pridružene elementima inercijske grupe u p nisu sve jedinične matrice. Podsjetimo da su matrice $\rho_{E,l}(\sigma)$ za $\sigma \in G$ kvadratne drugog reda jer prirodno djeluju na slobodni $\mathbf{Z}_l$ modul $T_l(E)$ ranga 2, što se prirodno proširuje na djelovanje na $\mathbf{Q}_l$ vektorski prostor $V_l(E)$ dimenzije 2.
Sad činjenica da je $\rho_{E,l}(I_p)$ grupa matrica koja sadrži bar jednu nejediničnu matricu povlači da je fiksni podprostor od I_p

$$V_l(E)^{I_p} := \{v \in V_l(E) : \rho_{E,l}(\sigma)(v) = v, \text{ za sve } \sigma \in I_p\}$$

vektorski podprostor od $V_l(E)$ različit od $V_l(E)$, pa je jednodimenzionalan ili nul-dimenzionalan.

Pokazuje se da je $V_l(E)^{I_p}$ jednodimenzionalan ako i samo ako je redukcija u p multiplikativna. Nadalje, $Frob_p$ djeluje na $V_l(E)^{I_p}$ kao množenje s 1 u rascjepivom slučaju, a kao množenje s -1 u nerascjepivom. Zato dobijemo:
$\frac{1}{\det(I-(\rho_{E,l}Frob_p|V_l(E)^{I_p})p^{-s})} = \frac{1}{1-p^{-s}}$ u rascjepivom, a
$\frac{1}{\det(I-(\rho_{E,l}Frob_p|V_l(E)^{I_p})p^{-s})} = \frac{1}{1+p^{-s}}$ u nerascjepivom slučaju.
Naravno, $V_l(E)^{I_p}$ je nul-dimenzionalan akko je redukcija aditivna. Uočite da je tada trivijalno $\frac{1}{\det(I-(\rho_{E,l}Frob_p|V_l(E)^{I_p})p^{-s})} = 1$
Uočimo još da je $V_l(E)^{I_p} = V_l(E)$ akko je u p redukcija dobra.
Zaključujemo da za sve $p \neq l$ imamo uniformnu formulu

$$L_p(E,s) = \frac{1}{\det(I-(\rho_{E,l}Frob_p|V_l(E)^{I_p})p^{-s})}$$

(ovdje $|$ znači restrikciju djelovanja operatora).
Uočite, posebno, da ovo vrijedi za sve proste l i rezultati ne ovise o izboru prostog broja l (osim što za svaki l treba izključiti jedan p, naime $p = l$). Takvu familiju l-adskih reprezentacija zovemo uskladjenom.