Abelova cena v roce 2018 udělena za Langlandsův program

Vítězslav Kala

Abstrakt. V článku motivujeme a vysvětlíme základy Langlandsova programu, sítě domněnek propojujících řadu různých oblastí matematiky. Během toho se také setkáme s Riemannovou hypotézou a domněnkou Birche a Swinnerton-Dyera, dvěma ze sedmi problémů tisíciletí vyhlášených Clayovým matematickým institutem.

1. Langlands a Abelova cena

Abelovu cenu za rok 2018 obdržel 22. května v Oslu Robert Langlands „za svůj vizionářský program propojující teorii reprezentací s teorií čísel“. Jedná se o další z řady významných ocenění pro tohoto kanadsko-amerického matematika, narozeného 6. října 1936 v provincii Britská Kolumbie na západě Kanady. Titul Ph.D. získal roku 1960 na Yaleově univerzitě pod vedením nepříliš známého rumunsko-amerického matematika jménem Cassius Ionescu-Tulcea; už ve své disertaci se Langlands věnoval studiu Lieových grup, jež pak hrály zásadní roli i v jeho dalším výzkumu. Většinu svého života strávil v Princetonu na východě Spojených států, kde od roku 1972 působí jako profesor na Institutu pro pokročilá studia. Jeho pracovna zde dříve patřila i Albertu Einsteinovi. Přestože Langlands vedl jen osm doktorandů, několik z nich je také špičkovými matematiky, například James Arthur a Thomas Hales, známý pro svůj důkaz Keplerovy domněnky o skládání koulí v trojrozměrném prostoru.

Základy své vize Langlands vypracoval v 60. letech minulého století a poprvé je zformuloval v roce 1967 ve svém slavném dopise André Weilovi [8]. Šlo o revoluční myšlenky díky své míře obecnosti, navazovaly ale zároveň na řadu dřívějších výsledků včetně Tanijamovy–Šimurovy–Weilovy domněnky o modularitě eliptických křivek. Když tedy v 90. letech Andrew Wiles a Richard Taylor prokázali v rámci důkazu velké Fermatovy věty platnost speciálního případu této domněnky, ověřili tím také jednu z lehčích predikcí v Langlandsově programu.

Langlandsův program je velmi náročnou a rozsáhlou oblastí matematiky, sahající od algebry a teorie čísel přes analýzu, diferenciální (ale také algebraickou) geometrii a teorii reprezentací až k teoretické fyzice! Jeho reputaci a (ne)přístupnosti ale také neprospěl Langlandsův hutný, poměrně obtížně čitelný způsob psaní článků: viz například vlivný článek [9] a jeho shrnutí [6] od Rogera Howea, jež končí slovy „Můžeme být nadšení, když nám průvodce ukáže horské štíty; ale také musíme doufat, že nám ukáže stupy a poskytne pár skob, abychom se dostali na další římsu.“ Během 50 let rozvoje tohoto programu samozřejmě vznikla řada přístupnějších úvodů, přesto ale proniknutí do této oblasti vyžaduje přinejmenším několik let intenzivního studia.

Mgr. Vítězslav Kala, Ph.D., Katedra algebry, Matematicko-fyzikální fakulta, Univerzita Karlova, Sokolovská 83, 186 00 Praha 8, e-mail: vita.kala@gmail.com

Obr. 1. Robert Langlands (vlevo) krátce po převzetí Abelovy ceny od norského krále Haralda V. (foto Thomas Brun/NTB)

Cílem tohoto přehledového článku je představit čtenářům Langlandsův program. Pokusíme se zde vysvětlit některé z jeho hlavních nástrojů a cílů, přičemž se místy dopustíme nevyhnutelných nepřesností a zjednodušení. Jednotlivé kapitoly v tomto článku na sebe sice navazují, pro četbu těch pozdějších by ale zdaleka nemělo být nutné porozumět všemu z kapitol dřívějších: všeobecná představa získaná rychlým pročtením by měla stačit. Pro usnadnění orientace v článku také některé myšlenky opakujeme víckrát na různých místech v lehce rozdílných formulacích.

2. L-funkce

V tomto článku Langlandsův program motivujeme a zformulujeme pomocí L-funkcí, které nejen že ve své základní podobě představují klíčový nástroj analytické teorie čísel, ale jako červená nit propojují různé oblasti Langlandsovy korespondence. Zhruba řečeno, L-funkce jsou komplexní funkce, které zachycují aritmetické informace (rozložení prvočísel nebo počty řešení diofantických rovnic) a které zároveň splňují několik důležitých, silných tvrzení: lze je vyjádřit ve tvaru Eulerova součinu a vyhovují jisté funkcionální rovnici. Tyto vlastnosti a jejich význam nejprve ilustrujme na příkladu Riemannovy ζ-funkce, odkud je pak dále budeme rozšiřovat.

Pro jiné přístupy k Langlandsovu programu viz například [11], [5], [4], [3] (přibližně v pořadí podle přístupnosti).

2.1. Riemannova ζ-funkce a existence prvočísel

Prvním příkladem L-funkce je *Riemannova ζ-funkce*. Jako funkci reálné proměnné ji studoval již Leonhard Euler v první polovině 18. století; její hlavní využití jako komplexní funkce ale rozvinul až Bernhard Riemann v roce 1859 za účelem zkoumání rozložení prvočísel. Jedná se o funkci komplexní proměnné s, která je v polorovině $\mathrm{Re}(s) > 1$ definována absolutně konvergentní řadou

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{1}$$

a dává tedy v této oblasti funkci, jež má komplexní derivaci (čili je tzv. holomorfní). S některými hodnotami ζ-funkce se matematik běžně potká na přednáškách z analýzy, například při výpočtu součtu řady $\sum \frac{1}{n^2}$ neboli vlastně hodnoty $\zeta(2) = \pi^2/6$.

Souvislost se zkoumáním prvočísel začne být zřejmá z vyjádření ζ-funkce ve tvaru *Eulerova součinu*

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}},$$

opět pro $\mathrm{Re}(s) > 1$, přičemž p probíhá přes všechna prvočísla. K důkazu stačí použít vzorec pro součet geometrické řady

$$\prod_p \frac{1}{1 - \frac{1}{p^s}} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right)$$

a poté roznásobit a přeuspořádat pravou stranu tak, abychom dostali ζ-funkci (1).

Z Eulerova součinu ihned vyplývá existence nekonečně mnoha prvočísel: kdyby jich bylo jen konečně mnoho, konvergovala by v bodě $s = 1$ jeho pravá strana

$$\prod_p \frac{1}{1 - \frac{1}{p}},$$

což by ale odporovalo známému faktu o divergenci harmonické řady, který se dá vyjádřit jako $\zeta(1) = \infty$.

Vedle Eulerova součinu je druhou klíčovou vlastností ζ-funkce její *meromorfní rozšíření*: existuje meromorfní funkce $\tilde{\zeta}(s)$, která ji rozšiřuje, čili $\tilde{\zeta}(s) = \zeta(s)$ pro $\mathrm{Re}(s) > 1$.

Připomeňme, že funkce $f\colon \mathbb{C} \to \mathbb{C}$ je meromorfní, pokud je definována a má komplexní derivaci ve všech bodech $s \in \mathbb{C}$ s výjimkou diskrétní množiny pólů s_0, v nichž se chová jako $a/(s-s_0)^k$ pro nějaké $k \in \mathbb{N}$ a $a \in \mathbb{C}$. Rozšíření Riemannovy ζ-funkce má ve skutečnosti pouze jeden pól řádu $k = 1$ (s reziduem $a = 1$), a sice v nám známém bodě $s_0 = 1$. Pokud existuje, tak je meromorfní rozšíření dané funkce jednoznačné, a proto je běžné nerozlišovat mezi původní funkcí a jejím rozšířením – dále tedy budeme značit meromorfní rozšíření jen jako $\zeta(s)$.

Posledním, a možná nejdůležitějším, tvrzením o Riemannově ζ-funkci je *funkcionální rovnice*, kterou splňuje, a sice

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s),$$

kde

$$\Gamma(z) = \int_0^\infty x^{z-1} \mathrm{e}^{-x}\,\mathrm{d}x$$

je obvyklá Γ-funkce, jež spojitě rozšiřuje faktoriál tak, že $\Gamma(n) = (n-1)!$ pro přirozené číslo n. Funkcionální rovnice vypadá na první pohled složitě, to důležité na ní ale je, že dává explicitní vztah mezi hodnotami $\zeta(s)$ a $\zeta(1-s)$. Například tedy umožňuje využít absolutně konvergentní řady (1) pro $\mathrm{Re}(s) > 1$ k výpočtu hodnot ζ-funkce v polorovině $\mathrm{Re}(s) < 0$. Populárním příkladem je Ramanujanova „identita“

$$1 + 2 + 3 + 4 + 5 + \ldots = \sum_{n=1}^{\infty} \frac{1}{n^{-1}} = \zeta(-1) = -\frac{1}{12}.$$

Mezi těmito dvěma polorovinami zbývá *kritický pás* $0 < \mathrm{Re}(s) < 1$. V něm je chování nejzáhadnější; týká se jej také slavná Riemannova hypotéza, která říká, že pokud s je nulový bod ζ-funkce ležící v kritickém pásu, čili $\zeta(s) = 0$ pro $0 < \mathrm{Re}(s) < 1$, pak s leží uprostřed tohoto pásu na přímce $\mathrm{Re}(s) = \frac{1}{2}$. To se zdá být velmi neužitečnou a náhodnou domněnkou, opak je ale pravdou: Nuly v kritickém pásu mají zásadní vliv na rozložení prvočísel.

Už jen nenulovost ζ-funkce na kraji kritického pásu $\mathrm{Re}(s) = 1$ je ekvivalentní *prvočíselné větě*, tedy tomu, že počet prvočísel menších než reálné číslo X je asymptoticky roven $X/\log X$. Znalost Riemannovy hypotézy by potom toto tvrzení uměla zpřesnit o členy nižších řádů. Jak si znalci komplexní analýzy nejspíš dovedou představit, v těchto důkazech hrají zásadní roli reziduová věta a vhodné přesuny integrační křivky. Proto je také důležité uvažovat $\zeta(s)$ vskutku jako funkci komplexní, a ne jen reálné, proměnné s.

2.2. Dirichletovy L-funkce a aritmetické posloupnosti

Riemannova ζ-funkce velmi přesně zachycuje asymptotické rozložení prvočísel, neumí ale dobře popsat jejich chování modulo n, kde n je dané přirozené číslo. Zejména se nehodí k důkazu *Dirichletovy věty o aritmetické posloupnosti*, jež říká, že pro všechna nesoudělná přirozená čísla n, a existuje nekonečně mnoho prvočísel tvaru $nx + a$ pro $x \in \mathbb{N}$.

K důkazu této věty Peter Gustav Lejeune Dirichlet roku 1837 zavedl pojem L-funkce pro charakter χ (včetně jejich značení písmenem L, které se dodnes používá; jednalo se z jeho strany nejspíš o poměrně náhodnou volbu).

Dirichletovým charakterem modulo n budeme rozumět zobrazení $\chi\colon \mathbb{N} \to \mathbb{C}$, které splňuje následující podmínky pro všechna přirozená čísla u, v a k:

- χ je periodické modulo n: $\chi(u + kn) = \chi(u)$,
- χ je multiplikativní: $\chi(uv) = \chi(u)\chi(v)$ a
- platí $\chi(u) = 0$, právě když u je soudělné s n.

Z této definice není těžké dokázat (zkuste si to jako cvičení!), že všechny nenulové hodnoty charakteru χ leží na jednotkové kružnici $|z| = 1$ a že jde dokonce o $\varphi(n)$-té odmocniny z jedné $\mathrm{e}^{2\pi \mathrm{i} r/\varphi(n)}$, kde $\varphi(n)$ je Eulerova funkce a $r \in \mathbb{Z}$.

Pro názornější představu se podívejme na několik příkladů charakterů:

- Triviální charakter modulo n

$$\chi(u) = \begin{cases} 1 & \text{pokud je } \mathrm{nsd}(u,n) = 1, \\ 0 & \text{pokud je } \mathrm{nsd}(u,n) > 1. \end{cases}$$

- Netriviální charakter modulo 5

$$\chi(u) = \begin{cases} 1 & \text{pokud je } u \equiv 1 \pmod 5, \\ \mathrm{i} & \text{pokud je } u \equiv 2 \pmod 5, \\ -\mathrm{i} & \text{pokud je } u \equiv 3 \pmod 5, \\ -1 & \text{pokud je } u \equiv 4 \pmod 5, \\ 0 & \text{pokud je } u \equiv 0 \pmod 5. \end{cases}$$

- Legendreův symbol $\left(\frac{u}{p}\right)$ modulo prvočíslo p.

Charaktery zachycují chování přirozených čísel modulo n, zkusme je tedy spojit s definicí ζ-funkce, jež umí zkoumat prvočísla. *Dirichletova L-funkce* pro charakter χ je

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}, \tag{2}$$

kde jsme rovnou vedle definice uvedli i příslušný Eulerův součin; nekonečná řada i součin opět absolutně konvergují pro $\mathrm{Re}(s) > 1$.

Stejně jako v případě Riemannovy ζ-funkce má tento Eulerův součin *stupeň 1* v tom smyslu, že násobíme členy tvaru $1/P_{p,\chi}(p^{-s})$, kde $P_{p,\chi}(X) = 1 - \chi(p)X$ je polynom stupně 1 (který závisí na charakteru χ a prvočíslu p).

Další analogií s Riemannovou ζ-funkcí je fakt, že Dirichletovy L-funkce mají meromorfní prodloužení na $s \in \mathbb{C}$ (které dokonce je holomorfní neboli nemá žádné póly, je-li χ netriviální charakter). Dále splňují funkcionální rovnici, jež poskytuje vztah mezi hodnotami $L(s,\chi)$ a $L(1-s,\overline{\chi})$, kde $\overline{\chi}$ je komplexně sdružený charakter definovaný jako $\overline{\chi}(u) = \overline{\chi(u)}$. Tato funkcionální rovnice je ještě o něco techničtější než v případě ζ-funkce, proto ji neuvádíme.

Jak už jsme naznačili, Dirichletovy L-funkce se hodí k důkazu existence prvočísel v dané aritmetické posloupnosti. Myšlenkou tohoto důkazu je uvažovat sumu

$$S_{n,a}(s) = \sum_{p \equiv a \pmod n} \frac{1}{p^s},$$

kde sčítáme přes všechna prvočísla kongruentní s a modulo n. Dokážeme-li, že tato funkce má pól v bodě $s = 1$, bude muset takových prvočísel být nekonečně mnoho.

K důkazu existence tohoto pólu použijeme identitu

$$\frac{1}{\varphi(n)} \sum_{\chi} \chi(a)^{-1} \cdot \chi(u) = \begin{cases} 1 & \text{pokud je } u \equiv a \pmod n, \\ 0 & \text{jinak,} \end{cases}$$

kde sčítáme přes všechny charaktery modulo n. Tímto můžeme převést sumu $S_{n,a}(s)$ na součet logaritmů Dirichletových L-funkcí a využít znalosti jejich chování v bodě $s = 1$. Nejtěžším krokem je potom dokázat, že $L(1, \chi) \neq 0$; celý důkaz ale zabere několik (desítek) stran.

2.3. Artinovy L-funkce a předzvěst Langlandsovy korespondence

Není daleko od pravdy, když řekneme, že cílem celého Langlandsova programu je studovat obecnější L-funkce a budovat teorii a nástroje, které je umožní zkoumat a dokazovat tvrzení, jako je funkcionální rovnice. Jak uvidíme později, zajímají nás zejména L-funkce, které zachycují nějakou algebraickou nebo geometrickou informaci. S těmi je ale obecně velmi těžké pracovat, a proto se postupuje tak, že se dokáže rovnost dané L-funkce s nějakou „analytickou“ L-funkcí, pro niž je naopak důkaz platnosti funkcionální rovnice snazší.

Dirichletovy L-funkce a ζ-funkci, o nichž jsme mluvili doposud, je možné považovat právě za příklady těchto analyticky definovaných L-funkcí. Jedním z náznaků, které Langlandse vedly k formulování jeho programu, je fakt, že těmto L-funkcím vskutku odpovídají „algebraické“ Artinovy L-funkce. Jejich přesná definice by nás zavedla poměrně hluboko do Galoisovy teorie, pojďme ji tedy jen naznačit.

Buď $K \supset \mathbb{Q}$ Galoisovo rozšíření těles, čili $K = \mathbb{Q}(\alpha)$ obdržíme přidáním nějakého algebraického čísla α k tělesu $\mathbb{Q}$, přičemž navíc ještě předpokládáme, že všechny kořeny minimálního polynomu prvku α nad $\mathbb{Q}$ také leží v K. Nejjednodušším příkladem je těleso $\mathbb{Q}(\mathrm{i})$, jež je rozšířením $\mathbb{Q}$ stupně 2.

Pro nás bude důležitý obecnější příklad *cyklotomických těles* $\mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/m})$ pro $m \in \mathbb{N}$. Jejich zásadní vlastností je fakt, že Galoisova grupa $Gal(\mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/m})/\mathbb{Q})$ neboli grupa všech automorfismů tělesa $\mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/m})$ je izomorfní grupě

$$\mathbb{Z}_m^* = \{a \in \mathbb{Z} | 0 < a < m, \mathrm{nsd}(a, m) = 1\}$$

invertibilních prvků modulo m. Tento izomorfismus je poměrně jednoduché popsat, prvku $a \in \mathbb{Z}_m^*$ totiž odpovídá automorfismus

$$\varphi_a \colon \mathbb{Q}\left(\mathrm{e}^{\frac{2\pi\mathrm{i}}{m}}\right) \to \mathbb{Q}\left(\mathrm{e}^{\frac{2\pi\mathrm{i}}{m}}\right), \varphi_a\left(\mathrm{e}^{\frac{2\pi\mathrm{i}}{m}}\right) = \mathrm{e}^{\frac{2\pi\mathrm{i}a}{m}}.$$

Artinova L-funkce $L(s, \rho)$ je přiřazena Galoisovu rozšíření $K \supset \mathbb{Q}$ a grupovému homomorfismu

$$\rho \colon Gal(K/\mathbb{Q}) \to GL_n(\mathbb{C}),$$

kde $GL_n(\mathbb{C})$ je grupa invertibilních matic $n \times n$. Obecně se homomorfismus do grupy $GL_n(\mathbb{C})$ nazývá reprezentace, v našem případě tedy mluvíme o *Galoisově reprezentaci* ρ. Takovéto reprezentace jsou užitečné proto, že zatímco $Gal(K/\mathbb{Q})$ je poměrně abstraktní grupa, její reprezentace realizuje prvky této grupy jako konkrétní matice, takže například umožňuje uvažovat jejich determinant, stopu nebo vlastní čísla, jež potom nesou informaci i o prvcích původní Galoisovy grupy.

Obecná definice Artinovy L-funkce je složitější (viz odstavec 4.1), zaměřme se tedy zatím na případ cyklotomického tělesa $K = \mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/m})$ a 1-dimenzionální reprezentace $\rho \colon Gal(K/\mathbb{Q}) \to \mathbb{C}^*$, kde $\mathbb{C}^*$ je multiplikativní grupa $\mathbb{C} \setminus \{0\}$. Povšimněme si, že $GL_1(\mathbb{C}) = \mathbb{C}^*$, a tedy ρ je vskutku speciálním případem Galoisovy reprezentace.

V tomto případě můžeme využít zmíněného izomorfismu $\mathbb{Z}_m^* \simeq Gal(K/\mathbb{Q})$ k tomu, abychom homomorfismu ρ přiřadili Dirichletův charakter modulo m

$$\chi(u) = \begin{cases} \rho(\varphi_u), & \text{pokud je nsd}(u,m) = 1, \\ 0, & \text{pokud je nsd}(u,m) > 1. \end{cases}$$

Artinova L-funkce se potom rovná Dirichletově L-funkci charakteru χ

$$L(s,\rho) = L(s,\chi).$$

Tato obecná korespondence Dirichletových a Artinových L-funkcí byla jedním ze základních kamenů, na nichž Langlands vystavěl svůj program.

Skutečnost, že tato rovnost L-funkcí stupně 1 obecně platí pro všechna Galoisova rozšíření $K \supset \mathbb{Q}$, je zásadní důsledek *teorie třídových těles*, jež je jedním z nejkrásnějších matematických výsledků první poloviny dvacátého století spojeným se jmény jako Emil Artin, Helmut Hasse a John Tate. Stručně řečeno, tato teorie popisuje všechna rozšíření, jejichž Galoisova grupa je komutativní, pomocí podobných izomorfismů jako v cyklotomickém případě $\mathbb{Z}_m^* \simeq Gal(\mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/m})/\mathbb{Q})$.

Z teorie třídových těles se také dá jako speciální případ odvodit zákon kvadratické reciprocity, který dává vztah mezi Legendrovými symboly $\left(\frac{p}{q}\right)$ a $\left(\frac{q}{p}\right)$ pro různá prvočísla p a q, neboli mezi řešitelností kongruencí $x^2 \equiv p \pmod{q}$ a $x^2 \equiv q \pmod{p}$. Nejen to, teorie třídových těles dokonce zahrnuje i reciprocity vyšších stupňů, jež se podobně týkají řešitelnosti kongruencí n-tého stupně. Proto se její hlavní věta nazývá Artinův zákon reciprocity – a proto se také mluví o hypotetické, výrazně obecnější Langlandsově reciprocitě.

3. Eliptické křivky a modulární formy

V předchozí kapitole jsme představili Dirichletovy a Artinovy L-funkce, které mají společné nejen to, že jde o L-funkce stupně 1 (tedy že součinitele příslušného Eulerova součinu obsahují polynomy stupně 1), ale hlavně to, že si díky teorii třídových těles navzájem odpovídají.

Pojďme se nyní zaměřit na případ L-funkcí stupně 2, jenž je také do značné míry dokázán v podobě Tanijamovy–Šimurovy–Weilovy domněnky o modularitě eliptických křivek. Za svou práci na tomto problému (a za související důkaz velké Fermatovy věty) získal Abelovu cenu za rok 2016 Andrew Wiles, jehož práce byla detailně představena v přehledovém článku [7]. Budeme tedy v této kapitole poněkud stručnější a zájemcům o více detailů vřele doporučíme zmíněný článek. Výrazně více podrobností směřujících k větě o modularitě obsahuje například kniha [2].

3.1. L-funkce eliptických křivek

Eliptickou křivkou rozumějme rovnici

$$E\colon y^2 = x^3 + ax + b,$$

jejíž koeficienty a, b jsou celá čísla. Dává tedy smysl uvažovat množinu jejích řešení nad celými čísly $E(\mathbb{Z}) = \{(x,y) \in \mathbb{Z}^2 | y^2 = x^3 + ax + b\}$ nebo obdobně nad racionálními čísly

$E(\mathbb{Q})$. Můžeme se ale na tuto rovnici také dívat jako na kongruenci modulo prvočíslo p nebo ekvivalentně jako na rovnici nad p-prvkovým tělesem $\mathbb{F}_p$ a brát příslušnou množinu řešení $E(\mathbb{F}_p)$.

Dá se čekat, že množina $E(\mathbb{F}_p)$ bude mít zhruba p prvků (stačí si uvědomit, že polovina možných hodnot modulo p jsou druhé mocniny, a předpokládat coby heuristiku, že hodnoty x^3+ax+b jsou modulo p náhodně rozmístěné), označme tedy $a_p(E)$ odchylku skutečného počtu řešení od této předpovědi,

$$a_p(E) = p - |E(\mathbb{F}_p)|.$$

Těchto koeficientů můžeme využít k tomu, abychom definovali L-funkci přiřazenou eliptické křivce E pomocí jejího Eulerova součinu přes všechna prvočísla p

$$L(s,E) = \prod_p \frac{1}{1 - \frac{a_p(E)}{p^s} + \frac{p}{p^{2s}}}, \tag{3}$$

jenž absolutně konverguje v polorovině $\mathrm{Re}(s) > 3/2$. (Pro úplnost dodejme, že stejně jako naše definice eliptické křivky, ani tato definice její L-funkce není zcela korektní, protože je potřeba ji upravit v konečně mnoha prvočíslech, která dělí diskriminant $-16(4a^3+27b^2)$.)

Všimněme si také, že vskutku jde o L-funkci stupně 2, neboť jmenovatel p-tého součinitele je dán kvadratickým polynomem $P_{p,E}(X) = 1 - a_p(E)X + pX^2$ v bodě $X = p^{-s}$.

L-funkce $L(s,E)$ také má meromorfní rozšíření a splňuje jistou funkcionální rovnici, což je ale extrémně obtížné dokázat. To by nás už nemělo příliš překvapit, protože eliptická křivka je geometrický objekt (můžeme například nakreslit graf množiny jejích reálných řešení $E(\mathbb{R})$), a jak jsme viděli již v odstavci 2.3, s geometrickými a algebraickými L-funkcemi se špatně pracuje. A vskutku, jediný dosud známý důkaz těchto vlastností pro $L(s,E)$ stojí na tom, že se napřed dokáže, že se tato L-funkce rovná L-funkci nějaké modulární formy, jak popíšeme níže.

L-funkce eliptické křivky má řadu dalších důležitých vlastností. Množina řešení křivky (například) nad racionálními čísly $E(\mathbb{Q})$ totiž tvoří konečně generovanou komutativní grupu a domněnka Birche a Swinnerton-Dyera předpovídá, že hodnost této grupy (tedy vlastně počet nezávislých řešení) se rovná řádu pólu funkce $L(s,E)$ v bodě $s=1$. To na první pohled působí překvapivě: L-funkci jsme definovali pouze pomocí „lokálních“ údajů modulo jednotlivá prvočísla, ale přesto je v ní zahrnuta i informace o počtu všech racionálních řešení. Význam této domněnky potvrzuje i skutečnost, že spolu s Riemannovou hypotézou je jedním ze sedmi tzv. problémů tisíciletí (Millenium Prize Problems) vyhlášených Clayovým matematickým institutem, za jejichž vyřešení je vypsaná odměna milion dolarů!

3.2. L-funkce modulárních forem

Co jsou tedy modulární formy, jež nám umožňují zkoumat L-funkce eliptických křivek? Neformálně řečeno, jedná se o jisté holomorfní funkce definované na horní komplexní polorovině $\mathbb{H} = \{z \in \mathbb{C} | \mathrm{Im}(z) > 0\}$, jež splňují silné transformační vlastnosti vůči Möbiovým transformacím $z \mapsto (az+b)/(cz+d)$, kde $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ je celočíselná matice s determinantem ± 1, tedy prvek grupy $SL_2(\mathbb{Z})$.

Formálněji, buď $k \in \mathbb{Z}$ a Γ vhodná podgrupa grupy $SL_2(\mathbb{Z})$. *Modulární forma váhy k a úrovně* Γ je holomorfní funkce $f\colon \mathbb{H} \to \mathbb{C}$ taková, že

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \tag{4}$$

pro všechny matice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ (a jež splňuje jisté asymptotické podmínky omezující rychlost jejího růstu). Tato definice na první pohled působí dost technicky, pro nás ale ani není příliš důležité zcela rozumět jejímu významu. Ostatně ani není jasné, zda vůbec nějaké nekonstantní modulární formy existují. Jako jeden z prvních je objevil Henri Poincaré roku 1880, který k tomu napsal [10, str. 326]: „Po patnáct dní jsem usiloval dokázat, že žádné takové funkce nemohou existovat [...], ale bez výsledků. Jednoho večera jsem, oproti svým zvyklostem, vypil černou kávu a nemohl spát. Davy myšlenek stoupaly a nechával jsem je srážet se, dokud se nezačaly po dvojicích propojovat, vytvářejíce stabilní kombinace. Do příštího rána jsem dokázal existenci třídy těchto funkcí [...]“

Ve skutečnosti ale není příliš těžké uvést příklady modulárních forem, Poincarého citát se totiž týká jiné, komplikovanější, třídy podobných funkcí. Základním příkladem modulární formy je *Eisensteinova řada* váhy k

$$E_k(z) = \sum_{(c,d)} \frac{1}{(cz+d)^k},$$

kde $k \geq 4$ je sudé přirozené číslo a sčítáme přes všechny uspořádané dvojice celých čísel $(c,d) \neq (0,0)$. To, že pro ni platí vztah (4) pro grupu $\Gamma = SL_2(\mathbb{Z})$, je snadné cvičení.

Modulární formy každopádně existují a nám bude stačit si všimnout, že pokud $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma$ pro nějaké $h \in \mathbb{N}$ (je třeba předpokládat, že takové h existuje), pak podle (4) platí $f(z+h) = f\left((z+h)/(0\cdot z+1)\right) \overset{(4)}{=} (0\cdot z+1)^k f(z) = f(z)$, neboli modulární forma $f(z)$ je periodická s periodou h. Můžeme ji tedy vyjádřit pomocí Fourierova rozvoje

$$f(z) = \sum_{n=0}^{\infty} a_n(f) \mathrm{e}^{2\pi \mathrm{i} n/h}.$$

Když jsme takto zkonstruovali posloupnost koeficientů $a_n(f) \in \mathbb{C}$, využijeme jí k definici příslušné L-funkce

$$L(s,f) = \sum_{n=0}^{\infty} \frac{a_n(f)}{n^s} = \prod_p \frac{1}{1 - \frac{a_p(f)}{p^s} + \frac{p^{k-1}}{p^{2s}}}, \tag{5}$$

jež konverguje absolutně pro $\mathrm{Re}(s) > k$, přičemž vyjádření ve tvaru Eulerova součinu platí, pokud $a_0(f) = 0$ a $f(z)$ je tzv. normalizovaná vlastní špicová forma. Opět jde o L-funkci stupně 2, přičemž nelineární člen se ve jmenovateli Eulerova součinu vyskytuje proto, že posloupnost koeficientů $a_n(f)$ není úplně multiplikativní, ale splňuje $a_{mn}(f) = a_m(f)a_n(f)$ pouze pro nesoudělná čísla m a n. Nelineární člen p^{k-1}/p^{2s} potom odpovídá vztahu, který platí mezi koeficienty $a_{p^j}(f)$ pro různé exponenty j.

Pomocí komplexní analýzy není příliš těžké dokázat ani existenci meromorfního rozšíření pro $L(s, f)$ a vhodnou funkcionální rovnici, jež dává vztah mezi hodnotami $L(s, f)$ a $L(k-s, f)$. Tyto důkazy spočívají v tom, že se L-funkce vyjádří jako Mellinova transformace modulární formy f. Všeobecně řečeno, věci fungují pěkně, neboť v tomto případě pracujeme s analytickou L-funkcí.

Všimněme si také hlavně toho, že Eulerovy součiny L-funkcí (3) a (5) si jsou velmi podobné, zejména v případě, kdy váha modulární formy je $k = 2$! Nemuselo by možná jít o zcela náhodnou souvislost...

Tím se zabývá věta o modularitě, která byla známá jako Tanijamova–Šimurova–Weilova domněnka předtím, než ji roku 2001 dokázali Breuil, Conrad, Diamond a Taylor v návaznosti na důkaz jejího speciálního případu Wilesem a Taylorem z roku 1995, jenž byl třeba k důkazu platnosti velké Fermatovy věty. Věta o modularitě říká, že každá eliptická křivka E je modulární v tom smyslu, že existuje modulární forma f váhy 2 (a vhodné úrovně určené diskriminantem eliptické křivky) taková, že se jejich L-funkce shodují, čili

$$L(s, E) = L(s, f).$$

Pomocí toho je pak možné přenést všechny známé vlastnosti z modulární L-funkce $L(s, f)$ na $L(s, E)$, a tím například dokázat meromorfní rozšíření a funkcionální rovnici pro $L(s, E)$.

Zároveň jde o druhou, už mnohem jasnější, inkarnaci Langlandsova programu: Existuje bijekce mezi množinami jistých geometrických a analytických objektů, jež zachovává jejich L-funkce. V tomto případě jde o eliptické křivky a modulární formy, zatímco v odstavci 2.3 jsme viděli korespondenci mezi Artinovými a Dirichletovými L-funkcemi.

Poznamenejme ještě, že ani tento případ zdaleka není zcela dořešen. Jedním z významných problémů zůstává to, že modulárních forem je mnohem více než eliptických křivek, mimo jiné proto, že mohou mít i jinou váhu než 2. Pro některé z nich jsou známé odpovídající geometrické (nebo algebraické) objekty, pro jiné, např. Maaßovy formy, se naopak očekává, že jim korespondující objekty jsou velmi komplikované (pokud vůbec existují). Jedná se ale nejspíš o velmi těžké otázky.

4. Langlandsova reciprocita

Pojďme se nyní podívat na obecné Langlandsovy domněnky, jež předpovídají vztahy mezi L-funkcemi stupně n podobné, jako jsme už viděli ve stupních 1 a 2. Opět se zejména zaměříme na Langlandsovu reciprocitu (neboli korespondenci), zmíníme se ale také o důležitém principu funktoriality. Poměrně čitelným úvodem k tomuto tématu je kniha [1].

Podobně jako tomu bylo v předchozích kapitolách, je snazší definovat příslušné algebraicko-geometrické objekty (v tomto případě Galoisovy reprezentace), ale dokazovat vlastnosti L-funkcí ale naopak umíme jen pro analytické objekty (automorfní formy, respektive reprezentace).

Všeobecně je tato kapitola náročnější než dřívější kapitoly, ale snad si z ní čtenář i přesto odnese základní představu o šíři a obecnosti Langlandsova programu.

4.1. Artinovy L-funkce Galoisových reprezentací

S Artinovými L-funkcemi jsme se již potkali v odstavci 2.3, zde budeme potřebovat jen jejich zobecnění na stupeň n. Opět buď $K \supset \mathbb{Q}$ Galoisovo rozšíření těles a uvažujme grupový homomorfismus

$$\rho\colon Gal(K/\mathbb{Q}) \to GL_n(\mathbb{C}).$$

Galoisově reprezentaci ρ pak přiřadíme *Artinovu L-funkci* pomocí Eulerova součinu

$$L(s,\rho) = \prod_p \frac{1}{\det(I - p^{-s}\rho(Frob_p))},$$

kde $Frob_p$ je *Frobeniův prvek* (příslušný prvočíslu p) dané Galoisovy grupy, který zde nebudeme přesně definovat.

Co se děje ve jmenovateli zlomku odpovídajícího prvočíslu p? $\rho(Frob_p)$ je matice $n \times n$, jejíž každý prvek vynásobíme komplexním číslem p^{-s}. Výslednou matici pak odečteme od jednotkové matice I a spočítáme determinant, což je polynom celkového stupně n. Výsledek $\det(I - p^{-s}\rho(Frob_p))$ tedy bude polynomem stupně n v p^{-s}; povšimněme si, že jde v podstatě o charakteristický polynom matice $\rho(Frob_p)$. Ověřili jsme, že Artinova L-funkce má vskutku stupeň n, jak jsme chtěli!

Tím jsme definovali algebraickou stranu obecné Langlandsovy korespondence, a sice reprezentace ρ Galoisových grup rozšíření $K \supset \mathbb{Q}$. Opět jsme přitom vynechali řadu technických detailů, například to, že je lepší pracovat s algebraickým uzávěrem $\overline{\mathbb{Q}}$ a reprezentacemi jeho nekonečné Galoisovy grupy $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.

Předtím než se podíváme na jejich analytický protějšek, se ještě zmiňme o vztahu geometrických a algebraických L-funkcí. Společné mají to, že kódují informace, které chceme studovat: třeba u eliptických křivek to byly počty jejích řešení, tedy v zásadě řešení jisté diofantické rovnice. V případě Galoisových reprezentací je jejich zajímavost méně zřejmá, jde ale o to, že struktura Galoisových grup, zachycená příslušnou reprezentací, je klíčová pro porozumění řadě dalších otázek, jako jsou například zobecnění zákona kvadratické reciprocity.

Zároveň je také často poměrně snadné mezi geometrickými a algebraickými objekty přecházet, například Tateův modul eliptické křivky jí přiřazuje dvourozměrnou Galoisovu reprezentaci. A jak jsme již víckrát viděli, bývá poměrně snadné definovat jejich L-funkce, ale nesmírně obtížné dokazovat analytické vlastnosti těchto L-funkcí. Obecné Langlandsovy domněnky se snáze formulují pro algebraické L-funkce přiřazené Galoisovým reprezentacím, proto jsme zde zvolili tento přístup (obecné geometrické objekty ale také existují, jsou jimi Šimurovy variety).

4.2. Automorfní formy a reprezentace

Abychom mohli zobecnit modulární formy na vhodné n-rozměrné analytické objekty, musíme poupravit jejich definici. Jak jsme již viděli, maticová grupa $SL_2(\mathbb{R})$ působí na horní polorovině $\mathbb{H}$ pomocí Möbiových transformací, přičemž není těžké si rozmyslet, že toto působení je tranzitivní a že pomocí něj dostáváme bijekci (dokonce homeomorfismus) mezi $\mathbb{H}$ a množinou rozkladových tříd $SL_2(\mathbb{R})/O(2)$. Můžeme se tedy dívat na modulární formy jako na funkce $f\colon SL_2(\mathbb{R}) \to \mathbb{C}$, jež splňují řadu transformačních rovností (vůči grupám $O(2)$ a Γ) a také jistou diferenciální rovnici odpovídající jejich holomorfnosti.

Tato definice modulární formy se přímo nabízí ke zobecnění: *automorfní forma* je funkce $f\colon SL_n(\mathbb{R}) \to \mathbb{C}$, jež leží v prostoru $L^2(SL_n(\mathbb{R}))$ funkcí integrovatelných s kvadrátem a splňuje vhodné transformační a diferenciální rovnice. Přesná definice je poměrně technická, a proto ji vynecháme. Už pro automorfní formy lze definovat L-funkce a zformulovat Langlandsovu reciprocitu, lepší je ale pracovat s obecnějším pojmem – automorfními reprezentacemi.

Jde o to, že grupa $SL_n(\mathbb{R})$ působí na prostoru $L^2(SL_n(\mathbb{R}))$ pravou regulární akcí, kterou pro $g \in SL_n(\mathbb{R})$ definujeme vztahem $R_g(f)(x) = f(xg)$ pro $f \in L^2(SL_n(\mathbb{R}))$. To dává nekonečněrozměrnou reprezentaci grupy $SL_n(\mathbb{R})$, která obsahuje nekonečně mnoho ireducibilních podreprezentací (chce-li být člověk přesný, je toto velmi delikátní záležitost, protože regulární reprezentace se nerozkládá na direktní součet svých ireducibilních komponent, ale obsahuje také velkou spojitou část). Tyto ireducibilní podreprezentace π pak odpovídají automorfním formám, v zásadě totiž vypadají jako $A_f = \{R_g(f) | g \in SL_n(\mathbb{R})\}$ pro automorfní formu f.

V předchozích odstavcích jsme se dopustili celé řady nepřesností (jejichž formální vyjasnění by rozsahem zabralo celou knížku!), zmiňme se ale jen o jedné z nich. Místo grupy $SL_n(\mathbb{R})$ je vhodnější uvažovat větší grupu $GL_n(\mathbb{A})$, kde $\mathbb{A}$ je *okruh adelů*, definovaný jako (omezený) direktní součin tělesa reálných čísel $\mathbb{R}$ se všemi p-adickými tělesy $\mathbb{Q}_p$. *Automorfní reprezentace* π je potom ireducibilní reprezentace, jež se vyskytuje v pravé regulární reprezentaci grupy $GL_n(\mathbb{A})$ působící na prostoru funkcí $L^2(GL_n(\mathbb{A}))$. Díky tomu, že je okruh $\mathbb{A}$ součinem $\mathbb{R} \times \prod_p \mathbb{Q}_p$, rozkládá se i reprezentace π na (tenzorový) součin reprezentací $\pi_\mathbb{R} \otimes \bigotimes_p \pi_p$. Pomocí teorie reprezentací pak definujeme lokální faktory Eulerova součinu $L_p(s, \pi_p)$ a z nich příslušnou *automorfní L-funkci*

$$L(s, \pi) = \prod_p L_p(s, \pi_p).$$

Pro tyto analytické L-funkce je potom možné opět dokázat meromorfní prodloužení a funkcionální rovnice.

4.3. Langlandsův program

Hypotetický Langlandsův zákon reciprocity říká, že každé Galoisově reprezentaci ρ stupně n odpovídá automorfní reprezentace π grupy $GL_n(\mathbb{A})$, přičemž se jejich L-funkce shodují, $L(s, \rho) = L(s, \pi)$. Ještě více hypoteticky je možné tuto korespondenci dokonce rozšířit na bijekci, pokud místo Galoisových reprezentací uvažujeme reprezentace větší (domnělé) grupy $L_\mathbb{Q}$. Přesněji řečeno, tato bijekce má být mezi reprezentacemi $\rho\colon L_\mathbb{Q} \to GL_n(\mathbb{C})$ a *L-balíčky* automorfních reprezentací, může se totiž stát, že dvě automorfní reprezentace mají téměř stejnou L-funkci, takže jsou potom v této korespondenci nerozlišitelné.

Tato domněnka je ale velmi daleko od důkazu, neumíme například ani definovat grupu $L_\mathbb{Q}$. Kromě toho však existuje *lokální Langlandsova korespondence*, která se týká složek π_p coby reprezentací grupy $GL_n(\mathbb{Q}_p)$ a již dokázali Harris, Taylor a Henniart kolem roku 2000. To ale pořád ještě není z Langlandsova programu zdaleka všechno! Jednak jsou zajímavé verze Langlandsovy korespondence i pro jiné grupy než GL_n; potom například *Langlandsova funktorialita* říká, že automorfním reprezentacím grupy SO_{2n+1} odpovídají automorfní reprezentace grupy GL_{2n+1}. Také je ale možné uvažovat všechny tyto pojmy nad funkčními tělesy křivek (namísto tělesa racionálních čísel

$\mathbb{Q}$), což vede na *geometrický Langlandsův program* s aplikacemi až v teoretické fyzice. To by ovšem už bylo téma na samostatný článek.

Většinu ze zmíněných domněnek Langlands navrhl koncem 60. let minulého století už v překvapivě precizní podobě. Během uplynulých padesáti let pak sloužily jako vodítko a inspirace pro řadu zásadních matematických výsledků, i přesto se ale ještě ani zdaleka neblížíme k vyčerpání a dořešení Langlandsovy vize. Lze tedy nepochybně očekávat její význam přinejmenším po další půlstoletí!

Poděkování. Děkuji Janě Bartoňové, Martinu Čechovi, Alexandru Kazdovi, Antonínu Slavíkovi a Davidu Stanovskému za cenné komentáře k předběžným verzím tohoto textu.

Článek vznikl za finanční podpory Nadačního fondu Neuron na podporu vědy.

L i t e r a t u r a

[1] Bump, D.: *Automorphic forms and representations.* Cambridge University Press, 1998.

[2] Diamond, F., Shurman, J.: *A first course in modular forms.* Graduate Texts in Mathematics 228. Springer, 2005.

[3] Frenkel, E.: *Lectures on the Langlands program and conformal field theory* [online]. Dostupné z: `https://math.berkeley.edu/~frenkel/houches.pdf`

[4] Friedberg, S.: *What is... the Langlands program?* Notices Amer. Math. Soc. *65* (2018), 663–665.

[5] Gelbart, S.: *An elementary introduction to the Langlands program.* Bull. Amer. Math. Soc. *10* (1984), 177–219.

[6] Howe, R.: shrnutí článku [9] pro mathscinet [online]. Dostupné z : `http://mathscinet.ams.org/mathscinet-getitem?mr=546619`

[7] Kříž ek, M., Somer, L.: *Abelova cena v roce 2016 udělena za důkaz Velké Fermatovy věty.* PMFA *3 (61)* (2016), 169–188.

[8] Langlands, R.: *Letter to André Weil*, 1967 [online]. Dostupné z: `http://publications.ias.edu/rpl/paper/43`

[9] Langlands, R.: *Automorphic representations, Shimura varieties, and motives. Ein Märchen.* Automorphic forms, representations and L-functions. Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, OR, 1977, Part 2, 205–246.

[10] Poincaré, H.: *Mathematical creation.* The Monist *3 (20)* (1910), 321–335.

[11] Sletsjoe, A. B.: *From quadratic reciprocity to Langlands' program* [online]. Dostupné z: `http://www.abelprize.no/c73016/binfil/download.php?tid=73038`