

Komentář k přednášce Kena Ribeta o velké Fermatově větě

<https://www.youtube.com/watch?v=mq9BS6S2E2k>

Tento text je komentářem ke zmíněné přednášce pro studenty předmětu Proseminář z algebry (verze 24/25).

Ken Ribet je slavným matematikem, působícím na jednom z nejlepších matematických pracovišť na světě na University of California v Berkeley. Proslavil se zejména svými výsledky v algebraické teorii čísel a algebraické geometrii v 80. a 90. letech: jeho výsledky byly klíčovou komponentou Wilesova důkazu velké Fermatovy věty a zároveň patřil mezi úzkou skupinu matematiků, která Wilesovu práci ověřila a rozšířila. V letech 2017-19 sloužil jako prezident American Mathematical Society.

Přednáška je z roku 2020 a pronesl ji na konferenci zvané Joint Mathematical Meeting obou největších amerických matematických společností, konané v Denveru. Na přednášku přišlo kolem 3000 diváků. Cílem bylo oslovit všechny účastníky konference, od specialistů v oboru až po učitele kalkulu z malých škol (kteří nerozumí algebře o nic víc než vy). Pozorujte, jak se taková přednáška dělá, podle mého názoru se to povedlo velmi dobře. (Pozorování můžete aplikovat například na obhajobu své bakalářské práce, kde také nebudou všichni specialisty na vaše téma.)

Přednáška má několik fází:

- 2:30-11:30 úvod: znění problému, motivace, historie, ...
- 11:30-17:00 osnova důkazu velké Fermatovy věty (princip byste měli pochopit, pojmy budou dovysvětleny)
- 17:00-28:30 terminologie, vztah křivek k modulárním formám, ... (většinu pojmů a principů byste měli pochopit)
- 28:30-33:00 více o eliptických křivkách (již znáte!)
- 33:00-42:00 shrnutí Ribetova důkazu, že Freyovy křivky nejsou modulární
- 43:00-47:00 shrnutí Wilesova důkazu, že Freyovy křivky jsou modulární
- 47:00-51:00 co se dělo po Wilesovi (zde už Ribet spěchal, některé slajdy jsou vynechané, rozumět se tomu nedá)

Do času 33:00 byste měli víceméně všechno nějak pobrat, pak už asi moc ne. Přesto doporučuji shlédnout video celé. Pozorujte, jaké pojmy se ve výkladu vyskytují, které oblasti algebry (a geometrie) se v důkazu využívají. I když nebudete důkazu rozumět, bude pro vás motivací k dalšímu studiu, až se uvedené pojmy a metody někde objeví. Například Galoisovy grupy budou na přednášce z algebry ještě letos (i když ne v rozsahu, který by umožnil videu porozumět).

Až do času 33:00 přednáška nepředpokládá žádné hluboké znalosti. Zde je pár definic, které se vám budou hodit.

Perfektní mocnina je číslo, které je k -tou mocninou přirozeného čísla, $k > 1$.

Diskriminant. Znáte pro kvadratický polynom $f = ax^2 + bx + c$: jeho diskriminant je roven $b^2 - 4ac$. Jeho nulovost indikuje vícenásobný kořen. Přednáška využívá diskriminant pro kubický polynom $f = ax^3 + bx^2 + cx + d$: jeho diskriminant je roven

$$b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

Opět platí, že f má vícenásobný kořen právě tehdy když je diskriminant nulový. Viz též sekce 26.1 ve skriptech algebra22.

Diskriminant křivky $y^2 - f(x) = 0$ se definuje jako diskriminant polynomu f . Tato křivka je eliptická, tj. nesingulární, právě tehdy, když je diskriminant nenulový. To je ihned vidět z parciálních derivací: derivace podle y je nulová pouze pro $y = 0$ a derivace podle x je potom nulová v bodě $(u, 0)$ právě tehdy, když $f(u) = f'(u) = 0$, čili když má f vícenásobný kořen u .

Konduktor eliptické křivky. Nesnažte se hledat, Ribet si dobře rozmyslel, proč definici vynechat. Prostě to berte tak, že ke každé eliptické křivce je přiřazen jakýsi číselný objekt zvaný konduktor, ze kterého se dají vykukat lecjaké vlastnosti té křivky.

Modulární forma je komplexní funkce $f : H \rightarrow \mathbb{C}$, kde $H = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$ je horní polorovina, splňující tři podmínky:

- f je holomorfní na H (tj. ve všech bodech diferencovatelná – bude v kurzu komplexní analýzy)
- pro každé $z \in H$ a každou celočíselnou matici $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ s jednotkovým determinanem platí

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

- f je holomorfní ve špičce (radši se ani nebudu pokoušet vysvětlit).

Pro účely přednášky si zapamatujte, že modulární formy jsou hladké komplexní funkce splňující jistou funkcionální rovnici. Tyto funkce mají velmi zajímavé vlastnosti, které teď ovšem neoceníte.

Reprezentace grup. Ve skriptech algebra22 je věta 15.11, která se na přednášce většinou vynechává: pro každou konečnou grupu G , libovolné těleso T a dostatečně velké n existuje prostý homomorfismus $\varphi : G \rightarrow \text{GL}(n, T)$, tj. grupa G je izomorfní nějaké podgrupě $\text{GL}(n, T)$. Jinými slovy, každou konečnou grupu lze reprezentovat pomocí (dostatečně velkých) regulárních matic nad T , přičemž prvky grupy G se násobí stejně jako korespondující matice, $\varphi(gh) = \varphi(g)\varphi(h)$.

Základní reprezentací každé grupy jsou tzv. permutační matice odpovídající translacím $x \mapsto gx$, tato reprezentace je popsána ve větě 15.11; výsledkem jsou matice řádu $|G|$. Jde to dělat i efektivněji, například dihedralní grupy D_{2n} mají reprezentaci řádu 2 nad tělesem \mathbb{R} (uvažujte matice příslušných izometrií v rovině), ale obecně jde o složitý problém, kterým se zabývá algebraický obor zvaný *teorie reprezentací*. Reprezentace pomocí permutačních matic translací funguje pro každé těleso, ale existence a vlastnosti „lepší“ reprezentací záleží na zvoleném tělese. Pro teorii čísel mají význam reprezentace nad tělesy \mathbb{C} , \mathbb{Q} i \mathbb{F}_p (tzv. modulární reprezentace).

Před lety napsal Víťa Kala pěkný a poměrně přístupný článek o Langlandsově programu, který obsahuje mimo jiné také výklad souvislosti velké Fermatovy věty a modulárních forem. Zájemce o podrobnější informace odkazují na něj: <https://dml.cz/handle/10338.dmlcz/147325>