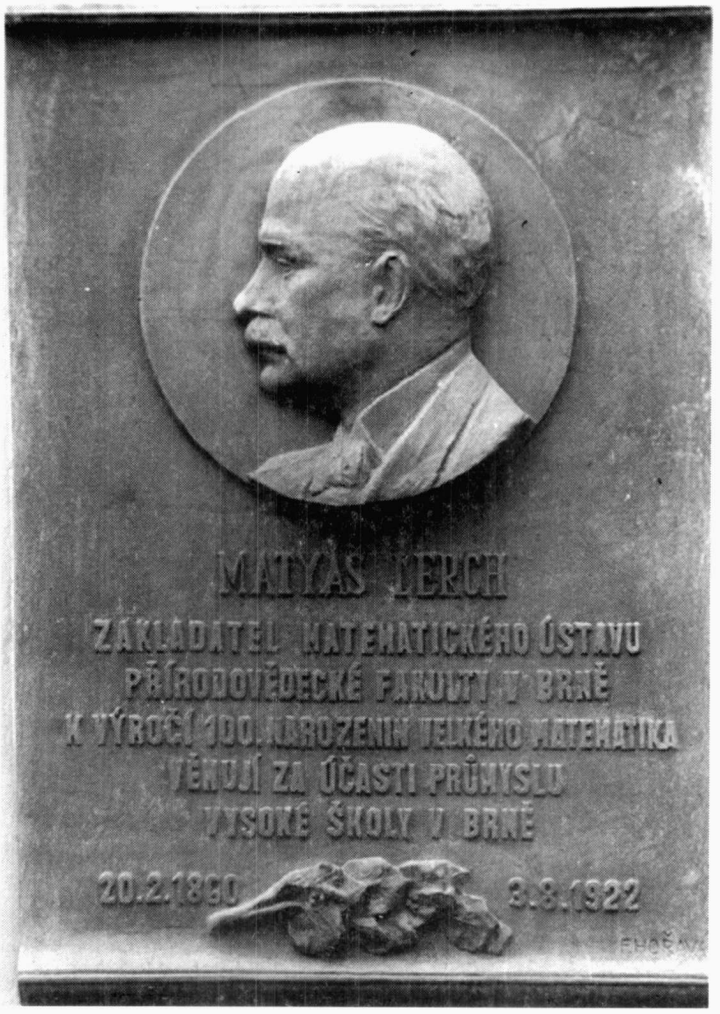
Karel Lepka

Souvislost mezi Fermatovými kvocienty a kvocientem Wilsonovým

In: Jindřich Bečvář (editor); Eduard Fuchs (editor): Matematika v proměnách věků. I. Sborník. (Czech). Praha: Prometheus, 1998. pp. 142–146.

Persistent URL: http://dml.cz/dmlcz/401615



Pamětní deska Matyáše Lercha (1862 - 1922)
na Přírodovědecké fakultě MU v Brně

SOUVISLOST MEZI FERMATOVÝMI KVOCIENTY A KVOCIENTEM WILSONOVÝM

KAREL LEPKA

(Článek je věnován 75. výročí úmrtí M. Lercha)

3. srpna 1997 uplynulo již 75 let od chvíle, kdy v Sušici zemřel vynikající český matematik Matyáš Lerch. Tento článek chce čtenářům přiblížit tuto významnou osobnost naší vědy malou ukázkou z jeho díla.

Úvodem mi však dovolte přece jen několik základních životopisných údajů. Lerch se narodil 20. února 1862 v Milínově v jihozápadních Čechách. Když mu bylo šest roků, utrpěl vážný úraz nohy s trvalými následky, takže se mohl pohybovat pouze s pomocí berle. Tento úraz mu sice překazil jeho původní záměr stát se středoškolským profesorem, mimořádnou osobnost tím však získala česká věda. Lerch byl naším prvním matematikem, který se výrazně prosadil mimo naši vlast a jemuž se dostalo uznání světové matematické veřejnosti. Z mnoha poct, které se mu během jeho života dostalo, připomínám Cenu Pařížské Akademie, kterou Lerch získal v roce 1900 za svou práci o kvadratických formách. Poslední třetina Lerchova života je spojena s Brnem; nejdříve působil jako profesor na brněnské technice, od roku 1920 až do své smrti vedl matematický ústav nově založené Masarykovy univerzity. Podrobnější údaje o jeho životě lze nalézt v publikacích, které jsou uvedeny v seznamu literatury.

Lerch publikoval během svého života asi 230 prací, a to jak v renomovaných zahraničních časopisech, tak i v časopisech domácích. Jeho doménou byla především analýza, zabýval se také teorií čísel a projektivní geometrií. Lerch však bohužel nenapsal žádnou monografii či učebnici, ačkoliv dosažené výsledky by ho k tomu plně opravňovaly.

V roce 1905, krátce před koncem svého švýcarského působení, publikoval Lerch práci [Le], v níž významným způsobem přispěl k pokroku v teorii Fermatova kvocientu. V úvodu této práce dokázal vztah mezi Fermatovými kvocienty a kvocientem Wilsonovým a na tento problém se podíváme podrobněji.

Nejdříve uvedeme několik pojmů z elementární teorie čísel.

Věta 1 (Fermat)[1]: *Nechť p je prvočíslo, a kladné celé číslo nesoudělné s p. Potom platí*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Definice 1: *Celé číslo*

$$q(a) = \frac{a^{p-1} - 1}{p}$$

se nazývá Fermatův kvocient.

[1]Pierre de Fermat (1601–1665); francouzský matematik. Zakladatel teorie čísel, analytické geometrie a počtu pravděpodobnosti.

Věta 2 (Wilson)[2]: *Nechť p je prvočíslo. Potom platí*

$$(p-1)! \equiv -1 \pmod{p}.$$

Definice 2: *Celé číslo*

$$N = \frac{(p-1)!+1}{p}$$

se nazývá Wilsonův kvocient.

Dnes je známa řada důkazů obou těchto vět.[3] Zajímavý důkaz podal Lagrange[4]; jeho specifičnost spočívá v tom, že dokazuje současně jak Wilsonovu, tak Malou Fermatovu větu. Podívejme se na tento důkaz podrobněji. Předpokládejme, že p je liché prvočíslo (pro $p = 2$ je tvrzení Wilsonovy věty evidentní) a uvažujme rovnici

$$(1) \qquad (x+1)(x+2)\cdots(x+p-1) = x^{p-1} + A_1 x^{p-2} + A_2 x^{p-3} + \cdots + A_{p-2}x + A_{p-1},$$

kde

$$(2) \qquad \begin{aligned} A_1 &= 1+2+3+\cdots+(p-1) \\ A_2 &= 1\cdot 2 + 1\cdot 3 + \cdots + 2\cdot 3 + \cdots + (p-2)(p-1) \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ A_{p-1} &= 1\cdot 2\cdot 3\cdots(p-1) \end{aligned}$$

Dosadíme-li do (1) $x+1$ místo x, obdržíme

$$(x+2)(x+3)\cdots(x+p) = (x+1)^{p-1} + A_1(x+1)^{p-2} + \cdots + A_{p-2}(x+1) + A_{p-1}.$$

Vynásobíme-li obě strany této rovnice výrazem $x+1$ a dosadíme-li do pravé strany z rovnice (1), dostaneme

$$(3) \qquad \begin{aligned} &(x+p)[x^{p-1} + A_1 x^{p-2} + \cdots + A_{p-2}x + A_{p-1}] = \\ &(x+1)^p + A_1(x+1)^{p-1} + \cdots + A_{p-2}(x+1)^2 + A_{p-1}(x+1), \end{aligned}$$

odkud porovnáním koeficientů u stejných mocnin x obdržíme následující rekurentní vzorce pro koeficienty A_i.

$$(4) \qquad \begin{aligned} A_1 &= \binom{p}{2} \\ 2A_2 &= \binom{p}{3} + \binom{p-1}{2} A_1 \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ (p-1)A_{p-1} &= 1 + A_1 + A_2 + \cdots + A_{p-3} + A_{p-2}. \end{aligned}$$

[2]John Wilson (1741–1793); člen britské Royal Society.

[3]O Malé Fermatově větě pojednává mj. i článek [Lp2].

[4]Joseph Louis Lagrange (1736–1813); působil jako profesor v Turíně, Berlíně a Paříži. Vynikal jak v matematice (variační počet, algebra, analýza a teorie čísel), tak v mechanice. Podílel se i na reformě měrového systému za francouzské revoluce.

Jelikož p je prvočíslo, jsou koeficienty A_1, A_2 atd. až A_{p-2} dělitelné p a

$$(p-1)A_{p-1} \equiv 1 \pmod{p}.$$

Roznásobíme-li levou stranu a vezmeme-li v potaz, že podle (2) platí $A_{p-1} = (p-1)!$, obdržíme

$$(p-1)! \equiv -1 \pmod{p}.$$

Fermatova věta odsud vyplývá jako důsledek, neboť podle výše uvedených úvah platí

$$(x-1)(x-2)\cdots(x-p+1) \equiv x^{p-1} - 1 \pmod{p}.$$

Současně je pro libovolné x splňující podmínku $(x,p) = 1$ jeden z činitelů na levé straně násobkem p a tedy platí

$$x^{p-1} - 1 \equiv 0 \pmod{p}.$$

Lerch v práci [Le] dokázal následující tvrzení:

Věta 3 (Lerch): *Nechť a je kladné celé číslo, p je liché prvočíslo. Potom platí*

$$\sum_{a=1}^{p-1} q(a) \equiv N \pmod{p}. \tag{4}$$

Z definice Fermatova kvocientu plyne

$$a^{p-1} = 1 + pq(a).$$

Vynásobíme-li tyto rovnice mezi sebou pro $a = 1, 2, \ldots, p-1$ a označíme-li pro jednoduchost $(p-1)! = P$, obdržíme

$$P^{p-1} = \prod_{a=1}^{p-1} (1 + pq(a)).$$

Vypočítáme-li součin na pravé straně a přejdeme-li ke kongruenci podle modulu p^2, odpadají všechny sčítance, které obsahují druhé a vyšší mocniny čísla p, takže dostaneme

$$P^{p-1} \equiv 1 + p\sum_{a=1}^{p-1} q(a) \pmod{p^2}. \tag{5}$$

Z definice Wilsonova kvocientu plyne

$$P = -1 + pN.$$

Umocníme-li obě strany této rovnice číslem $p-1$, a přejdeme-li ke kongruenci podle modulu p^2, obdržíme

$$P^{p-1} \equiv 1 + pN \pmod{p^2}. \tag{6}$$

Porovnáním kongruencí (5) a (6) obdržíme již uvedený vztah mezi Wilsonovými a Fermatovými kvocienty.

Lerchovy výsledky jsou rovněž citovány v publikacích jiných autorů. Uveďme alespoň jednu takovou zajímavou citaci. Úloha číslo 5 na straně 225 v učebnici [Si] zní: Dokažte Lerchovu větu, že pro lichá prvočísla platí

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv p + (p-1)! \pmod{p^2}. \tag{7}$$

Kongruence (7) je důsledek Lerchovy věty 3. Vyjádříme-li v kongruenci (4) $q(a)$ resp. N podle definic, obdržíme

$$\sum_{a=1}^{p-1} \frac{a^{p-1}-1}{p} \equiv \frac{(p-1)!+1}{p} \pmod{p},$$

což po vynásobení číslem p dává

$$\sum_{a=1}^{p-1} (a^{p-1}-1) \equiv (p-1)!+1 \pmod{p^2}$$

a po menší úpravě obdržíme kongruenci (7).

LITERATURA

[Bo1] Borůvka, O. a kol., *Díla Matyáše Lercha v oboru matematická analýza*, Práce brněnské základny ČSAV **39** (1957), 417–450.

[Bo2] Borůvka, O., *O životě a díle českého matematika M. Lercha*, Mat.-fys. rozhledy **38** (1959–60), 271–272.

[Ču] Čupr, K., *Profesor Matyáš Lerch*, Časopis pro pěstování matematiky a fysiky **52** (1923), 301–311.

[Di] Dickson, L. E., *History of the theory of numbers*, Carnegie Institution of Washington, Washington, 1919.

[Fr] Frank, L., *O životě Matyáše Lercha*, Čas. pro pěst. mat. a fys. **78** (1953), 119–137.

[La] Lagrange, J. L., *Nouv. Mém. Acad. Roy. Berlin, 2, 1773, année 1771, 125 (Oeuvres, 3, 1869, 425)*..

[Le] Lerch, M., *Zur Theorie der Fermatschen Quotienten* $\frac{a^{p-1}-1}{p} = q(a)$, Math. Ann. **60**, 471–490.

[Lp1] Lepka, K., *Matyáš Lerch's work on number theory*, MU, Brno, 1995.

[Lp2] Lepka, K., *Malá Fermatova věta*, Učitel matematiky **5** (1997), 143–150.

[Si] Sierpiński, W., *Elementary Theory of Numbers*, Polish Scientific Publishers, Warszawa, 1987.

[Šk] Škrášek, J., *Život a dílo profesora Matyáše Lercha*, Čas. pro pěst. mat. a fys. **85** (1953), 228–240.