Lerch, Matyáš: About Matyáš Lerch

Karel Koutský

K Lerchovým pracím o Fermatově kvocientu

Práce Moravské přírodovědecké společnosti 18, Brno 1947, 1-7

Persistent URL: http://dml.cz/dmlcz/501904

Terms of use:

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

PRÁCE
MORAVSKÉ PŘÍRODOVĚDECKÉ SPOLEČNOSTI
SVAZEK XVIII., SPIS 8. 1947 SIGNATURA: F 195.
BRNO, MORAVA.

ACTA SOCIETATIS SCIENTIARUM NATURALIUM MORAVICAE.
TOMUS XVIII.; FASCICULUS 8.; SIGNATURA: F 195.; BRNO, MORAVIA; 1947.

Dr. KAREL KOUTSKÝ, BRNO.

K Lerchovým pracím o Fermatově kvocientu.

Z početného množství matematických pojednání věnoval † prof. M. Lerch dvě své práce[1]) též theorii t. zv. Fermatova kvocientu, v nichž odvodil řadu velmi zajímavých vztahů. Na popud prof. O. Borůvky zabýval jsem se podrobnějším studiem Lerchových pracovních method a tu se mi podařilo nalézti obecné řešení jednoho, Lerchem pouze částečně řešeného problému.

Nechť $p \geqq 3$ je prvočíslo. Nechť a je celé číslo, nedělitelné p. Potom výraz

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

se nazývá Fermatův kvocient. Podle známé poučky je $q(a)$ vždy celým číslem.

V prvé ze svých prací zabývá se Lerch (kromě jiného) též určováním součtů tvaru

$$Q_k(p) = \sum_{a=1}^{p-1} a^k \cdot q(a), \tag{2}$$

při čemž k je dané celé číslo. Problém tento neřeší však obecně, nýbrž omezuje se pouze na případy $k = 0, 1, 2, \frac{p-1}{2}, \frac{p+1}{2}$. Postup, jehož užívá, jest dosti komplikovaný, ačkoliv vcelku užívá pouze elementárních prostředků. Nevýhodou pak je, že Lerchův postup podstatně závisí na volbě čísla k. Ukáži nyní, jak k jeho výsledkům lze dojíti mnohem schůd-

[1]) Jedná se o tyto dvě práce:

1. Lerch: Zur Theorie des Fermatschen Quotienten [Math. Ann. LX (1905), str. 471—490].

2. Lerch: Sur les théorèmes de Sylvester concernant le quotient de Fermat [Comptes rendus, tome 102 (Paris 1906), str. 35—38].

nější cestou, a to v případě *zcela libovolného* indexu k. Především si dokážeme větu

(3) Nechť $k_1 \equiv k_2 \pmod{p-1}$. Potom $Q_{k_1}(p) \equiv Q_{k_2}(p) \pmod{p}$.

Důkaz: Nechť $k_1 \equiv k_2 \pmod{p-1}$. Pak existuje celé číslo t, pro něž $k_1 = k_2 + t \,.\, (p-1)$. Ježto v součtu $Q_{k_1}(p)$ jsou čísla a vesměs v mezích $1 \leqq a \leqq p-1$, žádné z nich není dělitelno prvočíslem p. A pak vzhledem k Fermatově poučce bude:

$$Q_{k_1}(p) = \sum_{a=1}^{p-1} a^{k_1} \,.\, q(a) = \sum_{a=1}^{p-1} a^{k_2 + t(p-1)} \,.\, q(a) = \sum_{a=1}^{p-1} a^{k_2} \,.\, (a^{p-1})^t \,.\, q(a) =$$

$$\equiv \sum_{a=1}^{p-1} a^{k_2} \,.\, q(a) = Q_{k_2}(p) \pmod{p}, \; c \,.\, b \,.\, d.$$

Z věty (3) následuje, že pokud uvažujeme výrazy $Q_k(p) \pmod{p}$, stačí se omeziti pouze na ty indexy k, pro něž

(4) $$0 \leqq k < p-1.$$

Nyní pro dané přirozené číslo n a dané celé číslo $i \geqq 0$ zaveďme si označení

(5) $$s_i(n) = 1^i + 2^i + 3^i + \ldots + n^i.$$

Budiž dále $\sigma(i)$ funkce, definovaná pro každé celé $i \geqq 0$ tak, že platí:

(6) $$\sigma(0) = 1, \; \sigma(1) = p, \; \sigma(i) = 0 \text{ pro } i > 1.$$

Potom platí kongruence

(7) $$p \,.\, Q_k(p) - \sigma(k) \equiv s_{p-1+k}(p) - s_k(p) \pmod{p^2}.$$

Důkaz: Z (1) a (2) plyne rovnice $p\,Q_k(p) = s_{p-1+k}(p-1) - s_k(p-1)$. Z (5) a (6) se pro každé celé $i \geqq 0$ odvodí kongruence $s_i(p-1) \equiv s_i(p) - \sigma(i) \pmod{p^2}$, takže bude: $p \,.\, Q_k(p) \equiv s_{p-1+k}(p) - s_k(p) - \sigma(p-1+k) + \sigma(k) \pmod{p^2}$. Ježto $p \geqq 3$, $k \geqq 0$, bude $p-1+k \geqq 2$. Podle (6) je tedy $\sigma(p-1+k) = 0$ a pak z poslední kongruence okamžitě následuje (7), c.b.d.

Pro součty $s_i(p)$ ale platí známé vyjádření pomocí Bernoulliských čísel[2]):

---

[2]) Viz Pascal: Repertorium der höheren Mathematik I. 1. (Leipzig 1910), str. 422. Čísla B_i jsou definována rekurentním vztahem

$$\binom{i+1}{1} B_i + \binom{i+1}{2} B_{i-1} + \ldots\ldots\ldots + \binom{i+1}{i} B_1 = i$$

(viz tamtéž, str. 520). Snadno se zjistí, že je $B_1 = \frac{1}{2}$, $B_3 = B_5 = \ldots\ldots = 0$. Proto slovem »Bernoulliská čísla« bývají někdy označována pouze čísla B_{2h} se sudým indexem a číslo B_1. Lerch tak skutečně činí, leč tímto označením stávají se jeho výpočty mnohdy ne dosti průzračné.

$$(8)\qquad (i+1)\,.\,s_i(p) = p^{i+1} + \binom{i+1}{1} p^i B_1 + \binom{i+1}{2} p^{i-1} B_2 + \ldots + \binom{i+1}{i} p\, B_i.$$

Další úvahy musíme rozlišovati podle toho, zda jest $k = 0$, resp. $k = 1$, resp. $1 < k < p-1$.

a) Případ $k = 0$. Z (6) a (7) následuje:

$$(9)\qquad p\,.\,Q_0(p) - 1 \equiv s_{p-1}(p) - s_0(p) \pmod{p^2}.$$

V rovnici (8) položme $i = p-1$. Dostaneme:

$$p\,.\,s_{p-1}(p) = p^p + \binom{p}{1} p^{p-1} B_1 + \binom{p}{2} p^{p-2} B_2 + \ldots + \binom{p}{p-2} p^2 B_{p-2} + \binom{p}{p-1} p\, B_{p-1}.$$

Ježto p je prvočíslo, jsou binomické koeficienty $\binom{p}{1}, \binom{p}{2}, \ldots\ldots, \binom{p}{p-1}$ vesměs dělitelny p. Podle známé Staudtovy věty[3]) není jmenovatel žádného z čísel $B_1, B_2, \ldots, B_{p-2}$ dělitelný p. Ježto pak tato čísla jsou racionální, lze s nimi počítati modulo p jako s čísly celými. Ze Staudtovy věty plyne dále, že jmenovatel čísla B_{p-1} je dělitelný p, nikoliv však p^2. Tudíž jmenovatel čísla $p\,B_{p-1}$ není dělitelný p, a poněvadž i toto číslo je racionální, lze s ním při výpočtu (mod p) zacházeti jako s číslem celým. A poněvadž je $p \geqq 3$, jsou tedy všecky členy na pravé straně poslední rovnice, s výjimkou členu posledního, vesměs dělitelny aspoň p^3. Zřejmě tedy z této rovnice následuje kongruence

$$p\,.\,s_{p-1}(p) \equiv p^2 B_{p-1} \pmod{p^3}$$

a z ní pak dále

$$s_{p-1}(p) \equiv p\, B_{p-1} \pmod{p^2}.$$

Z (5) plyne $s_0(p) = p$. Vzhledem k tomu kongruence (9) nabývá následujícího tvaru:

$$(10)\qquad p\,.\,Q_0(p) \equiv (p\, B_{p-1} + 1) - p \pmod{p^2}.$$

---

[3]) Viz: Journal für Mathematik de Crelle, roč. 21 (1840), str. 372—374. Zmíněná věta dá se vyjádřiti vzorcem $B_{2h} = a_{2h} - \Sigma \frac{1}{l}$, kdež součtové znaménko Σ vztahuje se na všechna prvočísla l, pro něž $(l-1)$ je dělitelem indexu $2h$; a_{2h} je pak celé číslo. Platnost Staudtovy věty lze ovšem rozšířiti i na číslo B_1.

(Za jmenovatele čísel $B_3, B_5, \ldots\ldots$ pokládáme vždy číslo 1. Pro tato Bernoulliská čísla Staudtova věta sice neplatí, nicméně jejich »jmenovatel« není dělitelný p.)

Snadno se však nahlédne, že platí kongruence

$$p\,B_{p-1} \equiv -1 \pmod{p}. \tag{11}$$

Stačí v rekurentním vztahu pro Bernoulliská čísla [viz poznámku sub 2)] prostě položiti $i = p-1$ a uvážiti, že binomické koeficienty $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ jsou vesměs dělitelny p a současně, že jmenovatel žádného z čísel $B_1, B_2, \ldots, B_{p-2}$ není dělitelný p.

Z (11) následuje, že číslo $p\,B_{p-1}+1$ je dělitelno p, takže $\frac{p\,B_{p-1}+1}{p}$ jest číslo racionální. Lze tedy toto číslo vyjádřiti zlomkem, jehož čitatel i jmenovatel jsou celá, nesoudělná čísla. A lehce se pak dá dokázati, že jmenovatel tohoto čísla není dělitelný p, takže při výpočtu modulo p lze s ním zacházeti jako s číslem celým. Vzhledem k tomu lze kongruenci (10) krátiti p, takže jako konečný výsledek dostáváme:

$$Q_0(p) \equiv \frac{p\,B_{p-1}+1}{p} - 1 \pmod{p}. \tag{12}$$

Poznámka: Vzorec tento sice není v Lerchově práci explicitně uveden, avšak podle jedné jeho poznámky, blíže však nijak odůvodněné, lze souditi, že mu byl znám.

b) Případ $k = 1$. Z (6) a (7) následuje:

$$p \,.\, Q_1(p) \equiv s_p(p) - s_1(p) \pmod{p^2}. \tag{13}$$

V rovnici (8) položme $i = p$. Dostaneme:

$$(p+1)\,s_p(p) = p^{p+1} + \binom{p+1}{1}p^p B_1 + \binom{p+1}{2}p^{p-1}B_2 + \ldots + \binom{p+1}{p-1}p^2 B_{p-1} + \binom{p+1}{p}p\,B_p.$$

Ježto $p \geq 3$ je prvočíslo, je p liché a tedy podle definice Bernoulliských čísel je $B_p = 0$. Podle Staudtovy věty pak čísla $B_1, B_2, \ldots, B_{p-2}, p\,B_{p-1}$ jsou racionální a jmenovatel žádného z nich není dělitelný p. Lze tedy při výpočtu modulo p zacházeti s nimi jako s čísly celými. Kromě toho je $\binom{p+1}{p-1} = \frac{p+1}{2}\,.\,p$ a ježto p je liché, jest $\frac{p+1}{2}$ celé číslo a tedy binomický koeficient $\binom{p+1}{p-1}$ je dělitelný p. Zřejmě tedy všecky členy na pravé straně předešlé rovnice jsou dělitelny p^2, takže po malé úpravě z ní plyne kongruence

$$s_p(p) \equiv 0 \pmod{p^2}.$$

Přímým výpočtem podle (5) nalezneme, že je $s_1(p) = \frac{p(p+1)}{2}$ a poněvadž $p \geqq 3$, tedy $p \neq 2$, získáme odtud další kongruenci:

$$s_1(p) \equiv \frac{p}{2} \pmod{p^2}.$$

Po dosazení do (13) a krácení modulem p, získáme po úpravě kongruenci

$$Q_1(p) \equiv \frac{1}{2} \pmod{p}, \tag{14}$$

kterýžto výsledek se plně kryje s výsledkem Lerchovým.

c) Případ $1 < k < p-1$. Z (6) a (7) následuje:

$$p \,.\, Q_k(p) \equiv s_{p-1+k}(p) - s_k(p) \pmod{p^2}. \tag{15}$$

Podle předpokladu je $p - 1 + k < 2(p-1)$. Je tedy patrno, že mezi všemi celými čísly j, pro něž $1 \leqq j \leqq p - 1 + k$, existuje pouze jediné, které je dělitelno $(p-1)$, totiž číslo $(p-1)$ samo. Podle Staudtovy věty tedy všechna čísla B_j, pro něž $1 \leqq j \leqq p - 1 + k$, $j \neq p-1$, jsou racionální a jmenovatel žádného z nich není dělitelný p; obdobnou vlastnost má podle Staudtovy věty i součin $p\,B_{p-1}$. Lze tudíž se všemi těmito čísly zacházeti při výpočtu modulo p jako s čísly celými.

V rovnici (8) položme nyní jednak $i = k$, jednak $i = p - 1 + k$. Jest $k > 1$, tedy tím spíš bude $p - 1 + k > 1$. Každá ze vzniklých rovnic bude tedy míti na své pravé straně aspoň tři členy. A vzhledem k tomu, co před chvilkou bylo řečeno, snadno nahlédneme, že v obou případech jsou všechny členy na pravých stranách těchto rovnic, s výjimkou vždy členu posledního, dělitelny p^2.

Jakási pochybnost by snad mohla nastati v případě $i = p - 1 + k$ u členu, který obsahuje B_{p-1}. Tento člen však je $\binom{p+k}{p-1} p^{k+1} B_{p-1} = \binom{p+k}{p-1} \,.\, p^k \,.\, p\,B_{p-1}$ a tudíž vzhledem k tomu, co bylo řečeno, je tento člen dělitelný p^k. Ježto však $k > 1$, t. j. $k \geqq 2$, je i tento člen zcela jistě dělitelný p^2.

Utvoříme-li tedy z obou vzniklých rovnic kongruence (mod p^2), dostaneme:

$$(k+1) \,.\, s_k(p) \equiv \binom{k+1}{k} p\,B_k \pmod{p^2},$$

$$\text{resp. } (p+k)\, s_{p-1+k}(p) \equiv \binom{p+k}{p+k-1} p\,B_{p+k-1} \pmod{p^2}.$$

Ježto podle předpokladu je $1 < k < p-1$, není číslo k, a tedy ani číslo $(p+k)$ dělitelno p. Zřejmě ale je $2 < k+1 < p$, takže ani číslo k

není dělitelno p. Lze tedy obě předešlé kongruence bez obav krátiti — první číslem $(k+1)$, druhou číslem $(p+k)$ — čímž po úpravě dostaneme:

$$s_k(p) \equiv p\,B_k \pmod{p^2}, \text{ resp. } s_{p-1-k}(p) \equiv p\,B_{p+k-1} \pmod{p^2}.$$

Po dosazení do (15) a krácení modulem p dostáváme pak konečný výsledek:

(16) $$\underline{Q_k(p) \equiv B_{p+k-1} - B_k \pmod{p}.}$$

Zajímavým důsledkem předešlého vzorce je věta

(17) K d y ž $k > 1$ j e l i c h é č í s l o, p o t o m $Q_k(p) \equiv 0 \pmod{p}$.

D ů k a z: Ježto $p \geqq 3$ je prvočíslo, je p liché. Když tedy $k > 1$ je liché, bude též $p+k-1$ liché a zřejmě bude $p+k-1 > 1$. Podle definice Bernoulliských čísel je tedy $B_{p+k-1} = B_k = 0$ a tudíž věta (17) okamžitě plyne z kongruence (16).

P o z n á m k y: Vzorce (16) a (17) nejsou v Lerchově práci vůbec uvedeny. Jest však zajímavé porovnati je s výsledky jím získanými.

Na str. 479 prvního svého pojednání tvrdí Lerch, že za p o d m í n k y $p \equiv 3 \pmod 4$ platí kongruence

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) q(a) \equiv 0 \pmod{p},$$

kdež $\left(\frac{a}{p}\right)$ značí Legendrův symbol, dobře známý z theorie kvadratických zbytků. Je tedy $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$, takže levá strana Lerchovy kongruence je totožná $(\mathrm{mod}\, p)$ s výrazem $Q_{\frac{p-1}{2}}(p)$. Je-li nyní $p > 3$, $p \equiv 3 \pmod 4$, jest $\frac{p-1}{2} > 1$, $\frac{p-1}{2} \equiv 1 \pmod 2$ a tudíž Lerchova kongruence plyne okamžitě z věty (17). Je-li však $p = 3$, pak Lerchova kongruence je n e s p r á v n á. V tomto případě je totiž $\frac{p-1}{2} = 1$ a podle (14) správně jest $Q_{\frac{p-1}{2}}(p) \equiv \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) . q(a) \equiv \frac{1}{2} \pmod{p}$. Na tuto výjimku Lerch zřejmě zapomněl.

Na str. 480 téhož pojednání uvádí Lerch další větu, totiž že za p o d m í n k y $p \equiv 1 \pmod 4$ platí (psáno v našem označení) tato kongruence:

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) . q(a) \equiv 2B_{\frac{p-1}{2}} \pmod{p}.$$

Jak před chvílí řečeno, levá strana předešlé kongruence je totožná

(mod p) s výrazem $Q_{\frac{p-1}{2}}(p)$. Když v (16) položíme $k=\frac{p-1}{2}$, dostaneme $Q_{\frac{p-1}{2}}(p) = B_{3\frac{(p-1)}{2}} - B_{\frac{p-1}{2}} \pmod p$. Nyní ale pro každé číslo h, pro něž $0<h<\frac{p-1}{2}$ platí t. zv. Kummerova kongruence: $\frac{B_{2h+p-1}}{2h+p-1} \equiv \frac{B_{2h}}{2h}$ (mod p).[4]) Ježto $p \equiv 1 \pmod 4$, je $\frac{p-1}{4}$ číslo celé a zřejmě platí $0<\frac{p-1}{4}<\frac{p-1}{2}$. Položíme-li tedy $h=\frac{p-1}{4}$, pak Kummerova kongruence přejde po malé úpravě v kongruenci $B_{3\frac{(p-1)}{2}} \equiv 3B_{\frac{p-1}{2}} \pmod p$. A pak dosazením za $B_{3\frac{(p-1)}{2}}$ do poslední naší kongruence pro $Q_{\frac{p-1}{2}}(p)$ získáme $Q_{\frac{p-1}{2}}(p) \equiv 2B_{\frac{p-1}{2}} \pmod p$, kterýžto výsledek přesně souhlasí s výsledkem Lerchovým.

Na str. 481 téhož pojednání uvádí Lerch větu, že za p o d m í n k y $p \equiv 1 \pmod 4$ platí kongruence:

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) a \,.\, q(a) \equiv 0 \pmod p,$$

při čemž $\left(\frac{a}{p}\right)$ je zase Legendreův symbol. Snadno se pak nahlédne, že levá strana předešlého Lerchova vzorce je totožná (mod p) s výrazem $Q_{\frac{p+1}{2}}(p)$. A ježto je $p \geqq 3$, $p \equiv 1 \pmod 4$, je jistě $\frac{p+1}{2} > 1$, $\frac{p+1}{2} \equiv 1 \pmod p$, takže Lerchova kongruence bezprostředně plyne z věty (17).

Na str. 482 téhož pojednání uvádí pak Lerch svůj poslední výsledek, totiž že za p o d m í n k y $p \equiv 3 \pmod 4$ platí kongruence

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) a \,.\, q(a) \equiv Cl(-p) \pmod p,$$

kdež $Cl(-\Delta)$ značí počet tříd primitivních positivních kvadratických forem $\alpha x^2+\beta xy+\gamma y^2$ se záporným diskriminantem $\beta^2-4\alpha\gamma=-\Delta$. Tento Lerchův výsledek se ovšem nedá bezprostředně odvoditi z kongruence (16). Zato však porovnáním kongruence (16) pro $k=\frac{p+1}{2}$ s kongruencí Lerchovou [pravá její strana je totiž totožná (mod p) s výrazem $Q_{\frac{p-1}{2}}(p)$] docházíme k zajímavému vzorci: $Cl(-p) \equiv B_{3\frac{p-1}{2}} - B_{\frac{p+1}{2}} \pmod p$, platnému ovšem pouze za podmínky $p \equiv 3 \pmod 4$.

Seminář pro studium díla M. Lercha, Brno 1947.

[4]) Viz: Journal für Mathematik de Crelle, roč. 41 (1851), str. 368 až 372.