Práce navazující na Lercha

In: Karel Lepka (author): Historie Fermatových kvocientů (Fermat – Lerch). (Czech). Praha: Prometheus, 2000. pp. 70–73.

Persistent URL: http://dml.cz/dmlcz/401890

Kapitola 5

Práce navazující na Lercha

V této kapitole se stručně zmíníme o pracích, které bezprostředně navazují na Lerchovu práci [Lr7]. Lerch odvodil několik kongruencí pro součty

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

přičemž při odvozování těchto kongruencí používal různé postupy pro různé případy a navíc jeho odvozování nepostihuje všechny hodnoty čísla k. Naskýtá se otázka, zda nelze odvodit obecný vzorec pro sumu $Q_k(p)$. Tento problém vyřešili již v roce 1908 A. Friedmann a J. Tamarkine, kteří tuto metodu publikovali v [FT]. Jak ukazují četné citace, inspirací jim byla právě Lerchova práce [Lr7].

V této práci nejdříve dokázali následující tvrzení:

Věta 5.1 *Nechť* $(a,p) = 1$. *Potom platí*

$$\left[\frac{a}{p}\right] \equiv -aq(a) - 1 - \sum_{k=1}^{p-1} \alpha_k a^k \pmod{p}, \tag{5.1}$$

kde

$$\alpha_k = \begin{cases} \frac{(p-1)!+1}{p} = N & \text{pro } k = 1, \\ (-1)^{\frac{p-1}{2}} \frac{B_{\frac{p-k}{2}}}{p-k} & \text{pro } 1 < k < p-1, \\ -\frac{1}{2} & \text{pro } k = p-1. \end{cases}$$

Abychom dokázali toto tvrzení, je nutné si uvědomit, že výraz $1 - y^{p-1}$ je kongruentní podle modulu p buď s nulou, jsou-li čísla y a p nesoudělná, nebo s jedničkou v opačném případě. Platí tedy kongruence

$$\left[\frac{a}{p}\right] \equiv \sum_{y=1}^{a} 1 - y^{p-1} \pmod{p}.$$

Vzhledem k předpokladu můžeme tedy psát

$$\left[\frac{a}{p}\right] \equiv \sum_{y=1}^{a} 1 - y^{p-1} \equiv a - 1 - \sum_{y=1}^{a-1} y^{p-1} \pmod{p}.$$

Sumu na pravé straně vyjádříme pomocí Markovova vzorce

$$\sum_{y=1}^{a-1} y^{p-1} = \frac{a^p}{p} + A_1 a^{p-1} + A_2(p-1)a^{p-2} + \cdots + A_k(p-1) + \cdots$$
$$+(p-k+1)a^{p-k} + \cdots + A_{p-1}(p-1) + \cdots + 2a,$$

kde

$$A_m = \frac{(-1)^{\frac{m}{2}} - 1}{m!} B_{\frac{m}{2}}, \quad A_1 = -\frac{1}{2}.^{1}$$

První a poslední člen můžeme upravit následujícím způsobem:

$$\frac{a^p}{p} - \frac{a}{p} + \frac{a}{p} + A_{p-1}(p-1)!a = aq(a) + La,$$

kde je pro zjednodušení

$$L = \frac{(p-1)!A_{p-1}p + 1}{p}.$$

Zavedeme-li Fermatův kvocient, máme

$$\sum_{y=1}^{a-1} y^{p-1} = aq(a) + La + A_1 a^{p-1} + A_2(p-1)a^{p-2} + \cdots$$
$$+A_k(p-1) + \cdots + (p-k+1)a^{p-k} + \cdots + A_{p-2}(p-1) + \cdots + 3a^2.$$

Odsud plyne tvrzení věty 5.1, kde $\alpha_1 = -1 + L$. Vynásobíme-li obě strany kongruence (5.1) číslem a^{m-1} a vytvoříme-li sumu v mezích od $a = 1$ do $a = p-1$, obdržíme obecný vzorec pro součty typu $Q_k(p)$, který můžeme formulovat následujícím způsobem:

Věta 5.2 *Nechť p je prvočíslo, a, k jsou kladná celá čísla nesoudělná s p. Potom platí*

(5.2)

$$\sum_{a=1}^{p-1} a^k q(a) \equiv \begin{cases} -\frac{(-1)^{\frac{k}{2}} B_{\frac{k}{2}}}{k} & \text{pro } k \text{ sudé} \quad 0 < k < p-1 \\ -\frac{(-1)^{\frac{k}{2}} B_{\frac{k}{2}}}{k} \equiv 0 & \text{pro } k \text{ liché} \quad 1 < k < p-1 \end{cases} \pmod{p},$$

kde $B_{\frac{k}{2}}$ je $k-$té Bernoulliovo číslo.

[1] Definice A_1 v původním článku chybí.

Při důkazu této věty se využívá skutečnosti, že

$$\sum_{a=1}^{p-1} a^{k-1} \left[\frac{a}{p}\right] = 0$$

a věty 5.1.

V roce 1947 publikoval Karel Koutský práci [Ko], ve které se věnuje stejnému problému. Tato práce byla součástí semináře věnovaného studiu Lerchova díla. Tento seminář byl veden prof. Borůvkou. Koutský zřejmě neznal práci [FT], neboť se o ní vůbec nezmiňuje. Jeho postup nebudeme podrobně rozebírat, uvedeme pouze výsledky.

Pro $k = 0$ dospěl Koutský ke vzorci

$$Q_0(p) \equiv \frac{pB_{p-1} + 1}{p} - 1 \pmod{p}. \tag{5.3}$$

K tomuto vzorci připojil následující poznámku: *Vzorec tento sice není v Lerchově práci explicitně uveden, avšak podle jedné jeho poznámky, blíže však nijak odůvodněné, lze souditi, že mu byl znám.* Koutský má zřejmě na mysli stranu 488 v práci [Lr7], kde Lerch uvádí, že při některé jiné příležitosti dokáže pro lichá prvočísla vzorec

$$N \equiv -1 + \frac{1}{p} - (-1)^m B_m \pmod{p}, \tag{5.4}$$

kde $p = 2m+1$. Vzhledem k tomu, že Lerch používá staršího označení Bernoulliových čísel a s ohledem na Lerchem dokázaný vzorec (4.2), lze říci, že tyto dva vzorce jsou prakticky totožné. K uvedené problematice se Lerch však už nevrátil.

Tento vzorec je také citován v práci [CDP], str. 445, kde je však připisován N. G. W. h. Beegerovi. Vzhledem k tomu, že práce [Be] byla publikována až v roce 1913, je zřejmé, že prvenství zde patří Lerchovi.

Pro $k = 1$ odvodil Koutský vzorec

$$Q_1(p) \equiv \frac{1}{2} \pmod{p}, \tag{5.5}$$

což je Lerchova kongruence (4.27) (viz. [Lr7], strana 477, vzorec (17).)

Pro případ $1 < k < p - 1$ odvodil Koutský vzorec

$$Q_k(p) \equiv B_{p+k-1} - B_k \pmod{p}. \tag{5.6}$$

Je-li k liché, je také číslo $p + k - 1$ liché a obě Bernoulliova čísla na pravé straně jsou tudíž rovna nule. Je-li k sudé potom platí Kummerova kongruence

$$\frac{B_{k+p-1}}{k+p-1} \equiv \frac{B_k}{k} \pmod{p} \tag{5.7}$$

a Koutského vzorec (5.6) je totožný s Friedmannovým vzorcem (5.2). Závěrem tohoto článku autor porovnává tyto obecné vzorce s Lerchovými výsledky. Jedná

se o vzorce (4.30) (viz [Lr7], strana 479, vzorec (18)), (4.34) (viz [Lr7], strana 480, vzorec (21)) a (4.36) (viz [Lr7], strana 481, vzorec (22^1)).[2]

Lerchův vzorec (4.39) (viz [Lr7], strana 482 vzorec (22^2)) se ovšem takto odvodit nedá. Koutský však uvádí kongruenci

$$Cl(-p) \equiv B_{\frac{3p-1}{2}} - B_{\frac{p+1}{2}} \pmod{p}, \tag{5.8}$$

která ovšem platí pouze pro $p \equiv 3 \pmod{p}$. Tuto kongruenci obdržíme porovnáním (5.6) s pravou stranou Lerchovy kongruence (4.39), která je modulo p totožná s $Q_{\frac{p-1}{2}}$.

Nakonec se ještě stručně zmíníme o práci [ADS], jejímiž autory jsou T. Agoh, K. Dilcher a L. Skula a která je převážně věnována Fermatovým kvocientům pro složený modul m. Z této práce uvedeme dvě věty, které mají bezprostřední návaznost na Lerchovy práce. První z nich vyjadřuje jiným způsobem Lerchův vzorec (4.10) ([Lr7], vzorec (8^*), strana 474.)

Věta 5.3 *Nechť $a \geq 1$ a $m \geq 2$ jsou nesoudělná celá čísla. Potom platí*

$$aq(a,m) \equiv -\sum_{k=1}^{a-1} S^*\left(\frac{km}{a}\right) \pmod{m},$$

kde

$$S^*(X) = \sum_{\substack{x=1 \\ (x,m)=1}}^{[X]} x^{\phi(m)-1}.$$

Druhá věta, kterou z této práce budeme citovat, je rozšíření Lerchovy věty 4.17 pro složený modul.

Věta 5.4 *Nechť $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ je prvočíselný rozklad libovolného celého čísla $m \geq 2$, a je kladné celé číslo splňující podmínku (m,a)=1. Potom platí*

$$aq(a,m) \equiv -\phi(m) \sum_{r=1}^{k} \frac{n_r n_r'}{\phi(m_r)^2} \sum_{j=1}^{a-1} \left(B_{\phi(m_r)}\left(\frac{j}{a}\right) - B_{\phi(m_r)} \right) \pmod{m},$$

kde $m_r = p_r^{\alpha_r}$, $n_r = m/m_r$ a n_r' je celé číslo vyhovující podmínce $n_r^2 n_r' \equiv 1 \pmod{m_r}$, $(1 \leq r \leq k)$.

[2] Koutský se zde dopustil menší chyby, když uvádí $\frac{p+1}{2} \equiv 1 \pmod{p}$ místo správného $\frac{p+1}{2} \equiv 1 \pmod{2}$.