Lerchův přínos k teorii Fermatových kvocientů

In: Karel Lepka (author): Historie Fermatových kvocientů (Fermat – Lerch). (Czech). Praha: Prometheus, 2000. pp. 42–69.

Persistent URL: http://dml.cz/dmlcz/401889

Kapitola 4

Lerchův přínos k teorii Fermatových kvocientů

Tato kapitola je věnována přednímu českému matematiku Matyáši Lerchovi, jehož dílo významným způsobem přispělo k pokroku v různých oblastech matematiky. Kromě jeho životopisu je zde uveden přehled nejdůležitějších výsledků, jichž dosáhl v teorii čísel. Hlavní část této kapitoly je věnována Lerchovu přínosu k teorii Fermatova kvocientu.

4.1 Životopis Matyáše Lercha

Matyáš Lerch se narodil 20. února 1860 ve vesnici Milínov poblíž Sušice. Jeho otec Vojtěch Lerch byl drobný zemědělec. Malý Matyáš byl velmi čilý a bystrý, ale v šesti letech utrpěl vážný úraz a po vyléčení zůstala jeho levá noha ohnuta v koleně, takže mohl chodit jen s pomocí jedné berle. Následkem tohoto úrazu začal chodit do školy až v devíti letech, když se jeho rodiče přestěhovali do Sušice. Lerch byl od počátku výborným žákem a záhy se začalo projevovat jeho mimořádné nadání pro matematiku. Po skončení měšťanské školy nastoupil krátce v továrně Františka Scheinosta v Sušici, kde se měl stát úředníkem.

Přestože finanční situace jeho rodičů nebyla nejlepší, úřednická kariéra byla lákavá a mladý Matyáš by byl finančně zabezpečen, rozhodl se pro další studium. Složil úspěšně přijímací zkoušky a pro mimořádně dobré výsledky mu byla udělena výjimka, takže mohl nastoupit hned do pátého ročníku. Studium začal na reálném gymnáziu v Plzni, maturitu složil v roce 1880 na reálce v Rakovníku. Již během středoškolského studia se Lerch začal věnovat matematice a samostatně studoval tehdy dostupné učebnice. Svědčí o tom dopis ze dne 17. května 1878, který poslal tehdy jako kvintán svému učiteli Emilu Seifertovi.[1] V tomto listě Lerch mimo jiné píše: *Weyrovy Základy vyšší geometrie jsem pročetl až do involuce, o kteréž jsem sice začátky probral, avšak ustal jsem od dalšího studia jejího,*

[1] Syn E. Seiferta Ladislav Seifert (1883–1956), český matematik a profesor Masarykovy university v Brně, byl naopak žákem M. Lercha.

byv vytržen ze studování koncem prázdnin velikonočních. Teď daří se mi dobře. Myslím, že budu moci objednati sobě Studničkovy Základy vyšší matematiky, čímž se dovrší blaženost má.

Po prázdninách roku 1880 se dal zapsat na České vysoké škole technické v Praze jako řádný posluchač odboru inženýrského stavitelství. Na technice studoval tři roky, jeho učiteli byli mj. i Eduard Weyr, Gabriel Blažek a František Tilšer. Lerch měl v úmyslu vykonat učitelskou zkoušku a stát se středoškolským učitelem. Jak však později zjistil, toto by mu vzhledem k jeho tělesné vadě nebylo umožněno, a tak se začal plně věnovat pouze matematice. Ve školním roce 1883–1884 se stal mimořádným posluchačem české univerzity, jeho profesorem byl František J. Studnička, který si nadaného studenta velice oblíbil. V dalším školním roce studoval v Berlíně, neboť získal státní stipendium 800 zlatých. Zde byli jeho profesory nejlepší němečtí matematici té doby—Weierstrass, Kronecker, Fuchs a Runge. Zde také poznal některé mladé matematiky, mezi nimi byli Kovalevská, Runge, Heffter, Köhler a další.

Po návratu do Prahy se Lerch v roce 1886 habilitoval a byl jmenován soukromým docentem pražské české techniky. V této době začala také jeho rozsáhlá publikační činnost. V období 1886–1896 uveřejnil kolem 110 článků, a to nejen v časopisech domácích, ale také v renomovaných časopisech zahraničních, jako byly *Comptes rendus, Acta mathematica, Journal für die reine und angewandte Mathematik* a jiné. Seznam evropských a amerických matematiků, jimž Lerch posílal separáty svých prací, obsahuje více než sto adres. Zvláštního uznání se Lerchovi dostalo od vynikajícího francouzského matematika *Ch. Hermita*, který vysoce oceňoval Lerchovu vědeckou práci. Již výpočet Raabeova integrálu $\int_0^1 \log\Gamma(x)\mathrm{d}x$, který Lerch uveřejnil v roce 1888 v časopise *Giornale di matematiche*, Hermitea tak nadchl, že ho ve svých přednáškách uváděl slovy: *Voici pour y parvenir la méthode ingénieuse et élégante de Mr. Matyas Lerch, docent a l'Ecole Polytechnique Tchèque de Prague.*[2] Jak ukazuje jejich vzájemná korespondence, Hermite měl k Lerchovi vřelý vztah.

Přestože se Lerch stal světově uznávaným matematikem, nepodařilo se mu získat profesuru na některé vysoké škole v českých zemích, ačkoliv o to velice usiloval. Příležitost na jmenování profesorem se pro Lercha naskytla několikrát, ale vždy byl jmenován někdo jiný. Dne 30. dubna 1890 zemřel profesor druhé stolice matematiky na německé technice v Brně Franz Unferdinger, který na této škole působil v letech 1873–1890. Na uvolněné místo se hlásilo těchto sedm zájemců: profesor na gymnáziu v Klagenfurtu Otto Biermann, soukromý docent na německé technice v Praze Karl Bobek, profesor státního gymnázia v Innsbrucku a soukromý docent na univerzitě v tomto městě Franz Hočevar, soukromý docent na technice ve Vídni Gustav Kohn, soukromý docent na české technice v Praze Matyáš Lerch, profesor na zemské reálce v Rýmařově Reinhard Mildner a soukromý docent na technice ve Vídni a soukromý docent na univerzitě tamtéž Oscar Peithner. Hodnocení na všechny přihlášené kandidáty vypracoval profesor matematiky Emanuel Czuber. Z hodnocení M. Lercha odcitujeme pasáž, týkající se jeho odborných kvalit: *Lerch ist wissenschaftlich sehr tätig, seine za-*

[2]Zde předkládám důmyslnou a elegantní metodu, ke které dospěl pan Matyáš Lerch, docent pražské techniky.

hlreichen Arbeiten, in deutscher, böhmischer, französischer und portugieschischer Sprache geschrieben, betreffen allgemeine Funktionentheorie, Theorie der elliptischen Integrale und Funktionen, Zahlentheorie, Differentialgleichungen, neuere synthetische Geometrie. Wenn sich dadurch seine Vielseitigheit ausspricht, so berechtig der Inhalt der Arbeiten zu dem Schlusse, dass Lerch ein sehr begabter Mathematiker ist. Seine didaktische Bafähigung wird günstig beurtheilt.[3]

Lerchova přihláška do konkursu byla zaslána prostřednictvím rektora české techniky v Praze dne 14. července 1890. Profesorský sbor zasedal 7. července téhož roku a výsledek hlasování byl následující: Celý sbor dal na první místo Peithnera, Biermann byl desetkrát druhý, Mildner čtyřikrát druhý a třináctkrát třetí a jedno třetí místo získal Kohn. Lerchovo jméno se v hlasování vůbec neobjevilo. Dne 6. října 1890 jmenoval císař František Josef I. Dr. Oscara Peithnera, svobodného pána z Lichtenfelsu, mimořádným profesorem matematiky na německé technice v Brně.[4]

Lerchovi se nepodařilo získat jmenování profesorem ani na české univerzitě v Praze, ačkoliv zde bylo na rozdíl od německé univerzity pouze jedno profesorské místo[5] a možná by nebylo pro příslušná místa velkým problémem zasadit se o zřízení druhé profesorské stolice, k tomu však nedošlo. Karel Petr se domnívá, že jednou z možných příčin této situace bylo i Lerchovo sebevědomé vystupování a jeho sklon k přeceňování vlastních výsledků [Pe]. Další příčinou byla možná závist, neboť Lerch se stal již v devadesátých letech světově uznávaným matematikem.

Lerchovo další působení na českých vysokých školách bylo nejisté,[6] proto přijal v roce 1896 nabídku na jmenování profesorem na univerzitě ve švýcarském Freiburgu. Lerch působil ve Švýcarsku deset let a v tomto období došlo v jeho životě k řadě významných změn. Kromě toho, že se podstatně zlepšila jeho hmotná situace, podstoupil v roce 1900 náročnou operaci u doktora Hessinga, takže po ní mohl odložit berlu a chodit jenom o holi, na kratší vzdálenosti i bez hole. V roce 1897 za ním přijela jeho čtrnáctiletá neteř Růžena Sejpková, která mu vedla domácnost, takže se mohl věnovat plně pedagogické a publikační činnosti, která v tomto období vyvrcholila a dostalo se jí i významného mezinárodního ocenění, jak o tom bude ještě zmíněno.

Přes všechny pocty, kterých se mu v cizině dostalo, se Lerch chtěl vrátit do vlasti, a proto ho velice mrzelo, že byl několikrát opomenut při jmenování profesorů na českých vysokých školách. Návrat z ciziny se mu zdařil až v roce 1906, kdy byl jmenován řádným profesorem české brněnské techniky. Na této škole působil až do roku 1920, kdy přešel jako profesor na nově zřízenou Masarykovu

[3] Lerch je vědecky velmi činný, jeho četné práce psané německy, česky, francouzsky a portugalsky jsou věnovány obecné teorii funkcí, teorii eliptických funkcí a eliptických integrálů, teorii čísel, diferenciálním rovnicím a novější syntetické geometrii. Obsah jeho prací ukazuje, že Lerch je všestranný a velmi nadaný matematik. Jeho pedagogické schopnosti jsou hodnoceny příznivě.

[4] Veškeré materiály týkající se tohoto konkursního řízení lze nalézt v Moravském zemském archívu v Brně, složka B 34–638.

[5] Toto místo zastával Lerchův učitel F. J. Studnička; jejich vzájemné vztahy však po roce 1885 značně ochladly.

[6] Asistentské místo mohlo být tehdy zastáváno nejvýš deset let a soukromý docent neměl nárok na služební požitky.

univerzitu v Brně. Po příchodu do Brna se Lerch dočkal uznání i doma. Byl zvolen čestným členem Jednoty českých matematiků a fyziků, v roce 1909 získal čestný doktorát filosofie pražské univerzity a ve školním roce 1908–1909 byl děkanem odboru strojního inženýrství brněnské techniky. V té době se však jeho zdravotní stav postupně zhoršoval. Lerch totiž trpěl cukrovkou, která se tehdy prakticky nedala léčit, neboť inzulín ještě nebyl objeven. Ze zdravotních důvodů musel odmítnout jmenování rektorem brněnské techniky a také jeho publikační činnost poklesla.

Nahlédneme-li do studijních plánů brněnské techniky, zjistíme, že Lerch přednášel střídavě základní kurs matematiky v prvním a druhém ročníku. Obsah těchto přednášek byl následující:

1. Mathematika I. Základové vyšší mathematiky

   Algebra a analysis. Pojem funkce. Rozdělení funkcí. Sppojitost a mezní hodnoty funkcí o jedné proměnné. Pojem diferenciálního poměru a neurčitého integrálu. Pravidla pro differencování a určování neomezených integrálů funkcí algebraických a elementárních funkcí transcendentních. Maxima a minima, neurčité tvary. Rozvinování funkcí v řady, řady rozdílové; interpolace. Konvergence nekonečných řad; řada Taylorova. Některá užití diferenciálního počtu v geometrii. Nejhlavnější vlastnosti omezených integrálů a užití jejich v geometrii v případech jednoduchých. Přibližná integrace, pravidlo Simpsonovo. Algebraické rovnice o jedné neznámé. Řešení rovnic prvních čtyř stupňů. Přibližné methody řešení rovnic číselných. Rovnice o několika neznámých. Eliminace.

   Geometrie a) v rovině: bod, přímka, křivky stupně druhého a některé jiné křivky v souřadnicích bodových a polárních; b) v prostoru: bod, rovina, přímka, koule, plochy rotační. Některé křivky prostorové.

   Přednáška 5 hod., repet. 2 hod. po oba semestry I. ročníku.

2. Mathematika II. Analytická geometrie v prostoru; omezené integrály. Integrály dvojité a mnohonásobné. Differenciální rovnice. Základy počtu variačního. Upotřebení počtu differenciálního a integrálního v theorii křivek a ploch.

   Přednáška 5 hod., repet. 2 hodin po oba semestry II. ročníku.

Kromě těchto základních přednášek Lerch občas vypisoval i přednášky mimořádné, jejichž témata byla následující:

1. Vybrané kapitoly z mathematické analyse. Úryvky z filozofie. Singularity analytických výrazů. Stanovení derivace různých řad. Věty z nauky o funkcích komplexní proměnné. Různé otázky počtu integrálního.

   Mimořádná přednáška 2 hod. v LS.

2. Úvod do theorie funkcí elliptických.

   Mimořádná přednáška 1 hod. v ZS.

3. Základové theorie funkcí elliptických s úvodem do nauky o funkcích komplexní proměnné.

   Mimořádná přednáška po 1 hod. v obou semestrech.

4. Vybrané části z nauky o číslech.

   Dělitelnost. Shody. Aritmetické funkce. Zákon reciprocity. Kvadratické formy.

   Mimořádná přednáška 1 hodinu týdně v obou semestrech.

Závěr svého neobyčejného života strávil Lerch budováním matematického ústavu Masarykovy univerzity. Zde se stal jeho asistentem Otakar Borůvka, který se stal pokračovatelem v jeho díle a také dosáhl světového věhlasu. Při prázdninovém pobytu v Sušici dostal Lerch zápal plic a dne 3. srpna 1922 zemřel.

4.2 Dílo M. Lercha z teorie čísel

Matyáš Lerch publikoval během svého života 238 prací. Většina z nich se týká matematické analýzy; Lerch se věnoval především obecné teorii funkcí, nekonečným řadám, eliptickým funkcím, funkci gama a integrálnímu počtu. Lerchovo dílo v této oblasti bylo podrobně zpracováno v publikaci [Bo1]. V geometrii publikoval práce o rovnicích křivek, transformaci kuželoseček a věnoval se rovněž projektivní geometrii. Lerchovy geometrické práce nebyly dosud souhrnně zhodnoceny.

Matyáš Lerch publikoval v teorii čísel 52 prací, jež jsou psány česky, německy, francouzsky a polsky a jsou publikovány jak v renomovaných zahraničních časopisech, tak i v časopisech domácích. V tomto seznamu nalezneme řadu významných prací, které významným způsobem přispěly k rozvoji teorie čísel. Zpočátku se Lerch věnoval aritmetickým funkcím, kde dokázal řadu zajímavých tvrzení. Tak např. v práci [Lr1] odvodil vzorce

$$\sum_{\varrho=0}^{\left[\frac{n}{2}\right]} \psi(n-\varrho,\varrho) = n$$

a

$$\sum_{\varrho=0}^{n} \psi(n+\varrho,\varrho) = 2n.$$

V pracích [Lr2] a [Lr3] dokázal různými způsoby vzorec

$$\sum_{a=0}^{\left[\frac{m-1}{n}\right]} \psi(m-an,a) = \sum_{a=0}^{\left[\frac{m-1}{n}\right]} \chi(m-an,a),$$

kde $\psi(a,b)$ je počet přirozených dělitelů čísla a, které jsou větší než b, $\chi(a,b)$ je počet přirozených dělitelů čísla a, které jsou menší než b.

V roce 1895 publikoval článek [Lr4], ve kterém se poprvé věnoval kvadratickým formám; v této problematice dosáhl největších úspěchů. Jeho stěžejní dílo

v této oblasti, *Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers*[7], bylo v roce 1900 oceněna Velkou cenou francouzské akademie věd v Paříži.[8] Toto ocenění získal Lerch jako jediný. Originál této práce je [Lr11], zkrácenou a upravenou verzi publikoval v *Acta Mathematica* [Lr8] a [Lr10].

Binární kvadratická forma má tvar

$$ax^2 + bxy + cy^2,$$

její diskriminant je $D = b^2 - 4ac$, pro $D < 0$ klademe $-\Delta = D$. Zavedeme-li substituci

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y', \quad \alpha\delta - \beta\gamma = 1,$$

vznikne nová forma

$$a'x'^2 + b'x'y' + c'y'^2.$$

Tyto dvě formy se nazývají ekvivalentní. Všechny formy navzájem ekvivalentní tvoří určitou třídu kvadratických forem. Formy téže třídy mají stejný diskriminant. Naopak dvě formy, které mají stejný diskriminant, mohou patřit do různých tříd. Počet tříd kvadratických forem příslušných k danému diskriminantu je konečný. Symbol $Cl(-\Delta)$, resp. $Cl(D)$ označuje potom *počet tříd kvadratické formy* se záporným, resp. kladným diskriminantem. V práci [Lr6] dokázal Lerch vzorce

$$\frac{2}{\tau}\left[m - \left(\frac{-\Delta}{m}\right)\right] Cl(-\Delta) = -\sum_{\alpha=1}^{\Delta-1}\left(-\frac{\Delta}{\alpha}\right) E\left(\frac{\alpha m}{\Delta}\right),$$

kde m je libovolné celé číslo nedělitelné Δ, $\tau = 6$ pro $\Delta = 3$, $\tau = 4$ pro $\Delta = 4$, $\tau = 2$ jinak a $E(x)$ je celá část x, a

$$Cl(-\Delta) = \frac{\tau\sqrt{\Delta}}{2\pi}\sum_{\nu=1}^{\infty}\left(-\frac{\Delta}{\nu}\right)\cos\frac{2\nu x\pi}{\nu},$$

kde $0 \le x \le \frac{1}{\Delta}$. (Pro $x = 0$ dostáváme známou Dirichletovu rovnici.)

V práci [Lr11] Lerch odvodil nové, prakticky použitelné vzorce pro počet tříd. Vzorce, které předtím odvodili Kronecker a Dirichlet, byly zejména v případě kladného diskriminantu v praxi nepoužitelné. Nejdůležitější Lerchem odvozené vzorce jsou následující:

$$\frac{2}{\tau}Cl(-\Delta) = \frac{\sqrt{\Delta}}{\pi}\sum_{n=1}^{\infty}\left(\frac{-\Delta}{n}\right)\frac{1}{n}e^{\frac{n^2\pi}{\Delta}} + \frac{2}{\sqrt{\pi}}\sum_{n=1}^{\infty}\left(\frac{-\Delta}{n}\right)\int_{n\sqrt{\frac{\pi}{\Delta}}}^{\infty} e^{-x^2}dx$$

a

$$\frac{1}{\tau}Cl(-\Delta) = \sum_{m=1}^{\infty}\left(-\frac{\Delta}{m}\right)\frac{1}{1+e^{\frac{m\pi\sqrt{2\Delta}}{\Delta}}} + \frac{1}{\sqrt{2}}\sum_{m=1}^{\infty}\left(-\frac{\Delta}{m}\right)\frac{1}{\sinh\frac{2m\pi}{\sqrt{2\Delta}}}$$

[7] Pojednání o výpočtu počtu tříd binárních kvadratických forem s celočíselnými koeficienty

[8] Pařížská Akademie vypisovala pro každý rok téma pro udělení své Velké ceny. Tématem pro rok 1900 bylo „Zdokonalit v některém důležitém směru vyšetřování počtu tříd binárnírních kvadratických forem s celočíselnými koeficienty."

pro $\Delta > 0$. Pro případ kladného diskriminantu D odvodil Lerch následující dva vzorce:

$$Cl(D)\ln E(D) = \frac{2\sqrt{D}}{\sqrt{\pi}} \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \frac{1}{n} \int_{\sqrt[n]{\frac{\pi}{D}}}^{\infty} e^{-x^2} dx + \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \int_{\frac{n^2\pi}{D}}^{\infty} \frac{e^{-x}}{x} dx$$

a

$$\frac{1}{2} Cl(D)\ln E(D) = \sqrt{D} \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \frac{1}{n} \cdot \frac{1}{e^{\frac{2n\pi}{\sqrt{2D}}} + 1} + \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \ln \frac{1 + e^{-\frac{n\pi\sqrt{2D}}{D}}}{1 - e^{-\frac{n\pi\sqrt{2D}}{D}}},$$

kde $E(D) = \frac{T+U\sqrt{D}}{2}$ a $T^2 - DU^2 = 4$, $\left(\frac{D}{n}\right)$ resp. $\left(-\frac{D}{n}\right)$ je Legendreův symbol a $E(D)$ je základní Pellova jednotka k diskriminantu D.

Lerchovu přínosu k teorii Fermatových kvocientů jsou věnovány následující oddíly této kapitoly. Základní přehled o Lerchově díle z teorie čísel je uveden v publikaci [Lp].

Matyáš Lerch se stal prvním českým matematikem, jehož práce získaly věhlas a uznání. Jeho práce jsou i po šedesáti letech, které uplynuly od jeho smrti, přímo citovány v publikacích zahraničních autorů. V referativním časoppise Zentralblatt lze nalézt v letech 1935–1995 72 citací. Z teorie čísel jsou to zejména práce [Lr5], [Lr7] a [Lr11]. Řada výsledků, jichž dosáhl, je dodnes v matematické literatuře označována jeho jménem. Práce, které publikoval, jsou psány srozumitelně a mají i vysokou jazykovou úroveň. Přestože Lerchova publikační činnost byla zejména v mladších letech velmi intenzívní, Lerch nepublikoval žádnou monografii ani učebnici, ačkoliv dosažené výsledky by ho k tomu v mnoha oborech opravňovaly. Zřejmě se i v tomto směru projevil Kroneckerův vliv, neboť Lerch podobně jako Kronecker dával přednost řešení speciálních problémů.

Významná byla i jeho činnost pedagogická. Jeho přednášky měly vysokou úroveň, byl i náročným examinátorem. Lerch sice nezkoušel příliš mnoho látky, ale zato vyžadoval přesné odpovědi. Své žáky vedl k tomu, aby samostatně studovali matematickou literaturu.

Lerchův žák prof. Otakar Borůvka zhodnotil význam M. Lercha těmito slovy: *Význam Matyáše Lercha je především pro vědecké pracovníky všech oborů v přesnosti myšlení a jasnosti výkladu. Dále v tom, že M. Lerch měl široké znalosti z oborů, které byly blízké jeho vlastnímu pracovnímu zaměření, že nově získané výsledky ve svém oboru rozšiřoval podle možností do oborů příbuzných a měl velké porozumění pro aplikaci cizích výsledků, které zpracovával podle svého založení.*

Koncem minulého století se začala rozvíjet teorie množin a Lerch byl první český matematik, který nové myšlenky přenášel do české literatury. Zdá se například velmi pravděpodobné, že název množina pochází od Lercha. Soudíme tak z toho, že Lerch slovo množina běžně používá, kdežto toto slovo u dřívějších autorů nalezeno nebylo.

Velmi význačné se také jeví působení pedagogické na universitách a technikách a z toho plynoucí množství Lerchových následníků.

4.3 Vztah mezi Wilsonovým a Fermatovým kvocientem

Lerch se věnoval Fermatovým kvocientům v článcích [Lr7] a [Lr9]. Zejména v první citované práci dokázal řadu významných tvrzení, o nichž se podrobně zmíníme v této kapitole. Výsledky, jichž dosáhl, významným způsobem obohatily teorii Fermatových kvocientů. V úvodu tohoto článku Lerch dokázal souvislost mezi Fermatovými kvocienty a kvocientem Wilsonovým. Z Wilsonovy věty totiž plyne, že podíl

$$N = \frac{(p-1)! + 1}{p} \tag{4.1}$$

je celé číslo, které se nazývá *Wilsonův kvocient*. Lerch dokázal následující tvrzení:

Věta 4.1 *Nechť a je kladné celé číslo, p je liché prvočíslo. Potom platí*

$$\sum_{a=1}^{p-1} q(a) \equiv N \pmod{p}, \tag{4.2}$$

kde $q(a)$ je Fermatův kvocient a N je Wilsonův kvocient.

Důkaz tohoto tvrzení provádí Lerch poměrně jednoduchými prostředky. 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, dostaneme

$$P^{p-1} \equiv 1 + p \sum_{a=1}^{p-1} q(a) \pmod{p^2}. \tag{4.3}$$

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

$$P^{p-1} \equiv 1 + pN \pmod{p^2}. \tag{4.4}$$

Porovnáním kongruencí (4.3) a (4.4) obdržíme již uvedený vztah mezi Wilsonovými a Fermatovými kvocienty.

Tento Lerchův výsledek, který se dnes udává v poněkud pozměněném tvaru, je citován např. v [Si], kde úloha číslo 5 na straně 225 zní: Dokažte Lerchovu větu, tvrdící, že pro lichá prvočísla platí

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv p + (p-1)! \pmod{p^2}. \tag{4.5}$$

Kongruence (4.5) je důsledek Lerchovy věty 4.1. Stačí totiž v kongruencích (4.3) a (4.4) vyjádřit podle definice $q(a)$, resp. N.

4.4 Vyjádření Fermatova kvocientů pomocí součtu celých částí a jeho důsledky

V další části práce [Lr7] dokázal Lerch následující důležitou kongruenci:

Věta 4.2 *Nechť p je liché prvočíslo, a kladné celé číslo nesoudělné s p. Potom platí*

$$q(a) \equiv \sum_{\nu=1}^{p-1} \frac{1}{\nu a} \left[\frac{\nu a}{p}\right] \pmod{p}, \tag{4.6}$$

kde $\left[\frac{\nu a}{p}\right]$ označuje celou část čísla $\frac{\nu a}{p}$.

K odvození této kongruence využil Lerch Eisensteinem odvozených logaritmických vlastností Fermatových kvocientů. Podle (3.7) platí

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

a po úpravě dostaneme

$$\sum_{\nu=1}^{p-1} q(\nu a) \equiv -q(a) + \sum_{\nu=1}^{p-1} q(\nu) \pmod{p}. \tag{4.7}$$

Levou stranu kongruence (4.7) lze upravit jiným způsobem, uvážíme-li, že každému číslu $\nu \in \{1, 2, \ldots, p-1\}$ odpovídá jisté číslo c téže množiny, pro něž platí

$$\nu a \equiv c \pmod{p},$$

čili

$$\nu a = c + pz, \quad (0 < c < p),$$

kde z je celé číslo. Vydělíme-li tuto rovnici p, obdržíme

$$\frac{\nu a}{p} = \frac{c}{p} + z,$$

kde z je celá část čísla $\frac{\nu a}{p}$. Podle Eisensteinova vztahu (3.9) je

$$q(\nu a) \equiv q(c+pz) \equiv q(c) - \frac{z}{c} \equiv q(c) - \frac{z}{\nu a - pz} \equiv q(c) - \frac{z}{\nu a} \pmod{p},$$

tedy

$$q(\nu a) \equiv q(c) - \frac{1}{\nu a}\left[\frac{\nu a}{p}\right] \pmod{p}. \tag{4.8}$$

Sečteme-li tyto kongruence pro $\nu = 1, 2, \ldots, p-1$ a vezmeme-li v úvahu, že podle definice čísla c platí $\sum q(c) = \sum q(\nu)$, obdržíme

$$\sum_{\nu=1}^{p-1} q(\nu a) \equiv \sum_{\nu=1}^{p-1} q(\nu) - \sum_{\nu=1}^{p-1} \frac{1}{\nu a}\left[\frac{\nu a}{p}\right] \pmod{p}. \tag{4.9}$$

Porovnáme-li kongruenci (4.9) s (4.7), obdržíme tvrzení věty 4.2.

Nyní uvedeme některé důsledky kongruence (4.6). Vynásobíme-li ji číslem a, obdržíme

$$aq(a) = \frac{a^p - a}{p} \equiv \sum_{\nu=1}^{p-1} \frac{1}{\nu}\left[\frac{\nu a}{p}\right] \pmod{p}. \tag{4.10}$$

Položme $a = 2$ a $m = \frac{p-1}{2}$. Potom pro $\nu = 1, 2, \ldots, m$ je $\left[\frac{\nu a}{p}\right] = 0$ a pro $\nu = m+1, m+2, \ldots, 2m$ je $\left[\frac{\nu a}{p}\right] = 1$ a platí

$$\frac{2^p - 2}{p} \equiv \sum_{\nu=m+1}^{2m} \frac{1}{\nu} \equiv -\sum_{\nu=1}^{m} \frac{1}{\nu} \pmod{p}. \tag{4.11}$$

Druhá část je bezprostředním důsledkem Sternovy kongruence (3.20)

Kongruence (4.11) je stejná, jakou již odvodili Sylvester a Stern. Využitím identity

$$\sum_{\nu=1}^{2m} c_\nu - 2\sum_{\nu=1}^{m} c_{2\nu} = \sum_{\nu=1}^{2m} (-1)^{\nu-1} c_\nu$$

ji lze převést na tvar

$$\frac{2^p - 2}{p} \equiv \sum_{1}^{p-1} (-1)^{\nu-1} \frac{1}{\nu} \pmod{p}. \tag{4.12}$$

Lerch rozšířil již známé výsledky na další speciální případy. Volbou $a = 4$ se sumační index rozpadá na tři podmnožiny

$$\left\{\frac{p}{4}, \ldots \frac{p}{2},\right\}, \left\{\frac{p}{2}, \ldots, \frac{3p}{4}\right\}, \left\{\frac{3p}{4}, \ldots p,\right\},$$

které odpovídají hodnotám $1, 2, 3$ celé části $[\frac{4\nu}{p}]$. V druhé a třetí podmnožině zavedeme substituci

$$\frac{1}{\nu} = \frac{1}{p-\mu} \equiv -\frac{1}{\mu} \pmod{p}$$

a po dosazení do kongruence (4.6) obdržíme

$$4q(4) \equiv \sum_{\nu=\frac{1}{4}p}^{\frac{1}{2}p} \frac{1}{\nu} - 2\sum_{\mu=\frac{1}{4}p}^{\frac{1}{2}p} \frac{1}{\mu} - 3\sum_{\varrho=1}^{[\frac{1}{4}p]} \frac{1}{\varrho} \pmod{p};$$

levou stranu této kongruence lze psát ve tvaru $4q(4) = 4[q(2\cdot 2)] = 8q(2) = 4\frac{2^p-2}{p}$, zatímco na pravé straně lze sloučit první dvě sumy, takže obdržíme

$$4\frac{2^p-2}{p} \equiv -\sum_{\mu=\frac{1}{4}p}^{\frac{1}{2}p} \frac{1}{\mu} - 3\sum_{\varrho=1}^{\frac{p}{4}} \frac{1}{\varrho} \pmod{p}.$$

Čísla ϱ doplňují množinu čísel μ v intervalu $(0, \ldots, \frac{1}{2}p)$, můžeme tedy sloučit sumy $\sum \frac{1}{\varrho}$ a $\sum \frac{1}{\mu}$, čímž obdržíme

$$4\frac{2^p-2}{p} \equiv -\sum \nu =_1{}^m \frac{1}{\nu} - 2\sum_{\varrho=1}^{[\frac{1}{4}p]} \frac{1}{\varrho} \pmod{p}. \tag{4.13}$$

Odečteme-li od této kongruence kongruenci (4.11), obdržíme

$$3\frac{2^p-2}{p} \equiv -2\sum_{\varrho=1}^{[\frac{1}{4}p]} \frac{1}{\varrho} \pmod{p}, \tag{4.14}$$

případně pro $p > 3$

$$\frac{2^{p-1}-1}{p} \equiv -\frac{1}{3}\sum_{\nu=1}^{[\frac{1}{4}p]} \frac{1}{\nu} \pmod{p}. \tag{4.15}$$

Kongruenci (4.11) lze psát ve tvaru

$$\frac{2^p-2}{p} \equiv \sum_{1}^{m} \frac{1}{\nu} \equiv -\sum_{\lambda\le m} \frac{1}{\lambda} - \frac{1}{2}\sum_{1}^{[\frac{p}{4}]} \frac{1}{\mu} \pmod{p},$$

kde čísla ν jsou rozdělena na lichá λ a sudá 2μ. Tuto kongruenci lze upravit na tvar

$$2\frac{2^p-2}{p} = 4\frac{2^{p-1}-1}{p} \equiv -2\sum_{\lambda\le m} \frac{1}{\lambda} - \sum_{1}^{[\frac{p}{4}]} \frac{1}{\mu} \pmod{p}. \tag{4.16}$$

Odečteme-li od této kongruence (4.15), obdržíme

$$\frac{2^{p-1}-1}{p} \equiv -2 \sum \frac{1}{\lambda} \pmod{p}, \tag{4.17}$$

kde $\lambda = 1, 3, 5, \ldots$ a $\lambda \leq m$.

Stejným způsobem lze upravit kongruenci (4.12) na tvar

$$\frac{2^p-2}{p} \equiv \sum_1^{p-1} (-1)^{\nu-1} \frac{1}{\nu} \equiv \sum_1^{p-2} \frac{1}{\lambda} - \frac{1}{2} \sum_1^m \frac{1}{\mu} \pmod{p}. \tag{4.18}$$

Vynásobíme-li tuto kongruenci číslem -2 a přičteme-li k ní (4.11), obdržíme po úpravě

$$\frac{2^{p-1}-1}{p} \equiv \sum \frac{1}{\lambda} \pmod{p}, \tag{4.19}$$

kde $\lambda = 1, 3, 5, \ldots, p-2$.

Volba $a = 8$ vede ke kongruenci

$$4\frac{2^p-2}{p} \equiv -\sum \frac{1}{a} - \sum \frac{1}{b} \pmod{p}, \tag{4.20}$$

kde $0 < a < \frac{p}{8}, 0 < b < 3\frac{p}{8}$. Volíme-li $a = 3$, lze odvodit kongruenci

$$\frac{3^p-3}{p} \equiv -2 \sum_1^{[\frac{1}{3}p]} \frac{1}{\nu} \pmod{p} \tag{4.21}$$

a pro $a = 5$

$$\frac{5^p-5}{p} \equiv -2 \sum \frac{1}{a} - 2 \sum \frac{1}{b} \pmod{p}, \quad 0 < a < \frac{p}{5}, \quad 0 < b < \frac{2p}{5}. \tag{4.22}$$

Lerch uvádí ještě jednu kongruenci pro Wilsonův kvocient. Vychází z kongruence (4.6), přičemž tyto kongruence sčítá v mezích od 1 až po $p-1$, takže obdržíme

$$\sum_{a=1}^{p-1} q(a) \equiv \sum_{\mu=1}^{p-1} \sum_{\nu=1}^{p-1} \frac{1}{\mu\nu} \left[\frac{\mu\nu}{p}\right] \pmod{p}. \tag{4.23}$$

Levá strana (4.23) je podle věty 4.1 kongruentní s N. Položíme $\mu\nu = n$ a označíme $\psi(n)$ počet celočíselných řešení této neurčité rovnice. Potom lze (4.23) psát ve tvaru

$$N \equiv \sum_{n=1}^{(p-1)^2} \frac{\psi(n)}{n} \left[\frac{n}{p}\right] \pmod{p}. \tag{4.24}$$

Funkci $\psi(n)$ lze jednoduše určit následující úvahou. Jelikož čísla μ a ν jsou menší než p, je $n < p\mu$. Musí tedy platit nerovnost $\frac{n}{p} < \mu < p$ a komplementární dělitel ν je určen jednoznačně. $\psi(n)$ je tedy počet dělitelů n, které leží v intervalu $(\frac{n}{p}, p)$.

4.5 Vztahy pro $\sum a^k q(a)$

V další části článku [Lr7] Lerch vyšetřuje součty typu

$$Q_k(p) = \sum_{a=1}^{p-1} a^k q(a), \tag{4.25}$$

kde k je celé číslo vyhovující podmínce $0 \leq k < p$. Lerch odvodil několik vět pro různé hodnoty exponentu k, nepodařilo se mu však nalézt obecný vzorec. Dříve než uvedeme Lerchovy výsledky, připomeneme několik pojmů z teorie čísel.

Def. 4.1 *Nechť p je liché prvočíslo, a libovolné celé číslo splňující podmínku $(a,p)=1$. Má-li kongruence $x^2 \equiv a \pmod p$ řešení, pak a nazýváme kvadratický zbytek modulo p, v opačném případě kvadratický nezbytek modulo p. Legendrův symbol $\left(\frac{a}{p}\right)$ je roven ± 1, přičemž znaménko $+$ platí v případě, že a je kvadratický zbytek modulo p a znaménko $-$ v případě opačném.*

Pro Legendreův symbol platí následující věta:

Věta 4.3 *(Euler) Nechť p je liché prvočíslo a a libovolné celé číslo nesoudělné s p. Potom platí*

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

Def. 4.2 *Racionální čísla B_m, kde $m \geq 1$ je celé číslo, která jsou definována rovnicí*

$$\frac{t}{e^t - 1} = 1 + \sum_{m=1}^{\infty} \frac{B_m}{m!} t^m,$$

se nazývají Bernoulliova čísla.

Pro Bernoulliova čísla platí následující tvrzení:

Věta 4.4 *Všechna Bernoulliova čísla s lichými indexy jsou rovna nule s výjimkou $B_1 = \frac{1}{2}$.*[9]

Věta 4.5 *(Staudt) Nechť p je prvočíslo a m je sudé číslo. Jestliže $(p-1) \nmid m$, je B_m $p-$celé, tedy neobsahuje p ve jmenovateli. Jestliže $(p-1)|m$, potom je pB_m $p-$celé číslo a platí $pB_m \equiv -1 \pmod p$.*

Věta 4.6 *(Dirichlet) Nechť $Cl(-p)$ je počet primitivních kladných tříd kvadratické formy $ax^2+bxy+cy^2$ se záporným diskriminantem $b^2-4ac=-p$. Potom platí*

$$\left(2 - \left(\frac{2}{p}\right)\right) Cl(-p) = \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right).$$

[9] Zejména ve starší literatuře bývala za Bernoulliova čísla považována pouze čísla B_{2m} se sudým indexem a B_1.

Def. 4.3 *Nechť p je prvočíslo, α je celé číslo. Multiplikativní funkce definovaná vztahy*

$$\mu(p^\alpha) = \begin{cases} -1 & \text{je} - \text{li} \quad \alpha = 1 \\ 0 & \text{je} - \text{li} \quad \alpha > 1 \end{cases}$$

se nazývá Möbiova funkce.

Lerch nejdříve vyšetřuje součet $Q_1(p)$. Stačí totiž vynásobit kongruenci (4.6) číslem a a tyto výsledky sečíst přes všechna $a = 1, 2, \ldots, p-1$, čímž obdržíme

$$\sum_{a=1}^{p-1} aq(a) \equiv \sum_{a=1}^{p-1} \sum_{\nu=1}^{p-1} \frac{1}{\nu} \left[\frac{a\nu}{p} \right] \pmod{p}. \tag{4.26}$$

Platí

$$\sum_{a=1}^{p-1} \left[\frac{a\nu}{p} \right] = \sum_{a=1}^{p-1} \frac{a\nu}{p} - \sum_{b=1}^{p-1} \frac{b}{p}.$$

Využijeme-li vzorec pro součet aritmetické posloupnosti, je

$$\sum_{a=1}^{p-1} \frac{a}{p} = \sum_{b=1}^{p-1} \frac{b}{p} = \frac{p-1}{2}$$

a

$$\nu \sum_{a=1}^{p-1} \frac{a}{p} - \sum_{b=1}^{p-1} \frac{b}{p} = \frac{(\nu-1)(p-1)}{2}.$$

Po dosazení do (4.26) máme

$$\sum_{a=1}^{p-1} aq(a) \equiv \sum_{\nu=1}^{p-1} \frac{\nu-1}{\nu} \cdot \frac{p-1}{2} \pmod{p}.$$

Využitím Sternovy kongruence (3.20) lze tuto kongruenci zjednodušit na tvar

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

a po úpravě

$$\sum_{a=1}^{p-1} aq(a) \equiv \frac{1}{2} \pmod{p}. \tag{4.27}$$

Lerch dále vyšetřuje součet

$$S = \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p} \right) q(\nu). \tag{4.28}$$

Nejdříve předpokládá prvočíslo p tvaru $4k+3$. V tomto případě je $\left(\frac{p-\nu}{p}\right) = -\left(\frac{\nu}{p}\right)$ a můžeme zavést substituci $\nu = p-\mu$, takže

$$S = -\sum_{\mu=1}^{p-1}\left(\frac{\mu}{p}\right) q(p-\mu).$$

Protože $q(-a) = q(a)$, je

$$q(p-a) \equiv q(a) + \frac{1}{a} \pmod{p}.$$

Tato kongruence je důsledkem (3.9) a umožňuje nám přepsat součet S na tvar

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

odkud bezprostředně plyne

$$2S \equiv -\sum_{\mu=1}^{p-1}\left(\frac{\mu}{p}\right)\frac{1}{\mu} \pmod{p}.$$

Podle Eulerovy věty 4.3. můžeme psát tuto kongruenci ve tvaru

$$2S \equiv -\sum_{\mu=1}^{p-1}\mu^{m-1} \pmod{p},$$

kde $m = \frac{p-1}{2}$. Užijeme-li známé formule z diferenčního počtu

$$u_0 + u_1 + \cdots + u_{n-1} = \sum_{\nu=0}^{n-1}\binom{n}{\nu+1}\Delta^\nu u_0 \tag{4.29}$$

s volbou $u_\nu = \nu^{m-1}$, $n = p$ obdržíme

$$\sum_{1}^{p-1}\mu^{m-1} = \sum_{\nu=0}^{p-1}\binom{p}{\nu+1}\Delta^\nu O^{m-1} = \sum_{\nu=0}^{m-1}\binom{p}{\nu+1}\Delta^\nu O^{m-1},$$

neboť $m-$té a vyšší diference $(m-1)-$mocniny přirozených čísel se spolu vyruší. Vzhledem k tomu, že každý předcházející binomický koeficient $\binom{p}{\nu+1}$ je dělitelný p, je

$$\sum \mu^{m-1} \equiv 0 \pmod{p}$$

a můžeme zformulovat první Lerchův výsledek:

Věta 4.7 *Nechť $p > 3$ je prvočíslo, přičemž platí $p \equiv 3 \pmod 4$. Potom je*

$$\sum_{\nu=1}^{p-1}\left(\frac{\nu}{p}\right) q(\nu) \equiv 0 \pmod{p}. \tag{4.30}$$

Zde se však Lerch dopustil nepřesnosti, neboť pro $p = 3$ je $m = 1$ a vzorec (4.29) nelze použít. Vzhledem k tomu, že $\left(\frac{1}{p}\right) \equiv 1 \pmod 3$ a $\left(\frac{2}{p}\right) \equiv 2 \pmod 3$, je podle (4.27) $S \equiv \frac{1}{2} \pmod p$.

Pro prvočísla tvaru $4k + 1$ tento postup nelze použít, proto Lerch zvolil při vyšetřování součtu S jiné prostředky. Vychází opět z věty 4.3. a definuje celé číslo $q'(\nu)$, které je určeno rovnicí

$$\nu^m = \left(\frac{\nu}{p}\right)[1 + pq'(\nu)]. \tag{4.31}$$

Vztah mezi $q(\nu)$ a $q'(\nu)$ se odvodí snadno, jestliže rovnici (4.31) umocníme na druhou. Obdržíme

$$1 + 2pq'(\nu) + p^2 q'(\nu)^2 = 1 + pq(\nu)$$

a tedy

$$q(\nu) \equiv 2q'(\nu) \pmod p.$$

Protože $p = 4n + 1$ je $m = 2n$ a

$$\sum_{\nu=1}^{p-1} \nu^m = p \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) q'(nu), \tag{4.32}$$

neboť v řadě čísel $1, 2, \ldots, p-1$ je počet kvadratických zbytků a nezbytků stejný a tedy

$$\sum_{1}^{p-1} \left(\frac{\nu}{p}\right) = 0.$$

Levou stranu můžeme vyjádřit pomocí vzorce

$$S_{2n}(x) = \frac{x^{2n+1}}{2n+1} - \frac{1}{2}x^{2n} + \sum_{\nu=1}^{n} (-1)^{\nu-1} \frac{B_\nu}{2\nu} \binom{2n}{2\nu-1} x^{2n-2\nu+1}, \tag{4.33}$$

tedy je

$$\sum_{\nu=1}^{p-1} \nu^m = S_{2n}(p), \quad 2n = m.$$

Vydělíme-li tuto rovnici číslem p, obdržíme

$$\frac{p^m}{m+1} - \frac{1}{2}p^{m-1} + \sum_{\nu=1}^{n} (-1)^{\nu-1} \frac{B_\nu}{2\nu} \binom{2n}{2\nu-1} p^{2n-2\nu} = \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) q'(\nu).$$

Podle Staudtovy věty platí

$$(-1)^{n-1} B_n \equiv \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) q'(\nu) \pmod p$$

a můžeme zformulovat druhý Lerchův výsledek:

Věta 4.8 *Nechť p je prvočíslo splňující podmínku $p \equiv 1 \pmod 4$. Potom platí*

$$S = \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) q(\nu) \equiv (-1)^{n-1} 2B_n \pmod p. \tag{4.34}$$

Dále je studován součet

$$H = \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) \nu q(\nu). \tag{4.35}$$

Nechť $p = 4k + 1$, takže

$$\left(\frac{p-a}{p}\right) = \left(\frac{a}{p}\right).$$

Je-li $a \leq m$, potom lze sumu na pravé straně v rovnici (4.35) rozdělit ve dvě a máme

$$H = \sum \left(\frac{a}{p}\right) aq(a) + \sum \left(\frac{p-a}{p}\right) (p-a)q(p-a).$$

Dále přejdeme ke kongruenci modulo p, čímž obdržíme

$$H \equiv \sum \left(\frac{a}{p}\right) a[q(a) - q(p-a)] \pmod p.$$

Výraz v hranaté závorce je ale podle důsledku (3.9) kongruentní s $-\frac{1}{a}$, takže je

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

tedy platí následující tvrzení:

Věta 4.9 *Nechť p je prvočíslo, přičemž platí $p \equiv 1 \pmod 4$. Potom je*

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) \nu q(\nu) \equiv 0 \pmod p. \tag{4.36}$$

Je-li $p = 4k + 3$, má první dělení součtu H tvar

$$H = \sum \left(\frac{a}{p}\right) aq(a) + \sum \left(\frac{p-a}{p}\right) (p-a)q(p-a).$$

Vezmeme-li opět v úvahu, že $\left(\frac{p-\nu}{p}\right) = -\left(\frac{\nu}{p}\right)$ a přejdeme-li ke kongruenci modulo p, můžeme psát

$$H \equiv 2 \sum \left(\frac{a}{p}\right) aq(a) + \sum \left(\frac{a}{p}\right) \pmod p. \tag{4.37}$$

Nyní se provede nové rozdělení čísel ν na sudá $2a$ a lichá $p-2a$, takže součet H má tvar

$$H = \sum \left(\frac{2a}{p}\right) aq(2a) + \sum \left(\frac{p-2a}{p}\right)(p-2a)q(p-2a)$$

a stejným postupem získáme

$$H \equiv 4\sum \left(\frac{2a}{p}\right) aq(2a) + \sum \left(\frac{2a}{p}\right) \pmod{p}.$$

Vzhledem k tomu, že je

$$q(2a) \equiv q(a) + q(2) \pmod{p},$$

lze tuto sumu psát ve tvaru

$$H \equiv 4\left(\frac{2}{p}\right)\sum \left(\frac{a}{p}\right) aq(a) + \left(\frac{2}{p}\right)\sum \left(\frac{a}{p}\right) + 4\left(\frac{2}{p}\right) q(2)\sum \left(\frac{a}{p}\right) a \pmod{p}.$$

Suma

$$\sum \left(\frac{a}{p}\right) a$$

je dělitelná p a v poslední kongruenci odpadá, takže máme

$$H \equiv 4\left(\frac{2}{p}\right)\sum \left(\frac{a}{p}\right) aq(a) + \left(\frac{2}{p}\right)\sum \left(\frac{a}{p}\right) \pmod{p}. \tag{4.38}$$

Vynásobíme-li (4.37) dvojkou a (4.38) $\left(\frac{2}{p}\right)$ a odečteme-li je od sebe, obdržíme

$$\left(2 - \left(\frac{2}{p}\right)\right) H \equiv \sum \left(\frac{a}{p}\right) \pmod{p}.$$

Vezmeme-li v úvahu Dirichletovu větu 4.6, Lerchův čtvrtý výsledek zní:

Věta 4.10 *Nechť p je prvočíslo splňující podmínku $p \equiv 3 \pmod 4$. Potom platí*

$$\sum_{\nu=1}^{p-1} \left(\frac{2}{p}\right) \nu q(\nu) \equiv Cl(-p) \pmod{p}. \tag{4.39}$$

Lerch dále odvodil vzorec pro $k = 2$, přičemž využil uvedených výsledků. Vrací se k součtu S, který značí A.[10] Nechť ϱ je celé číslo vyhovující podmínce $0 < \varrho < p$. Potom existuje celé číslo b takové, že platí $\nu b \equiv \varrho \pmod{p}$ a Lerchův vzorec (4.6) lze psát ve tvaru

$$q(\nu b) \equiv q(\varrho) - \frac{1}{\nu b}\left[\frac{\nu b}{p}\right] \pmod{p}.$$

[10] Toto přeznačení samozřejmě nemá žádný význam a není jasné, proč k němu Lerch přistoupil.

Eisensteinův vzorec (3.7) zase dává

$$q(\nu b) \equiv q(\nu) + q(b) \pmod{p},$$

platí tedy

$$q(\varrho) - \frac{1}{\nu b}\left[\frac{\nu b}{p}\right] \equiv q(\nu) + q(b) \pmod{p}. \tag{4.40}$$

Podle definice čísel b, ν, ϱ platí

$$\left(\frac{\nu b}{p}\right) = \left(\frac{\varrho}{p}\right);$$

kongruenci (4.40) lze po vynásobení $(\frac{\nu b}{p})$ psát ve tvaru

$$\left(\frac{b}{p}\right)\left(\frac{\nu}{p}\right) q(\nu) + \left(\frac{b}{p}\right) q(b) \left(\frac{\nu}{p}\right) \equiv \left(\frac{\varrho}{p}\right) q(\varrho) - \left(\frac{\nu b}{p}\right) \frac{1}{\nu b}\left[\frac{\nu b}{p}\right] \pmod{p}. \tag{4.41}$$

Na levé straně je využito skutečnosti, že pro Legendreův symbol platí $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$. Nyní provedeme součet pro $\nu = 1, 2, \ldots, p-1$. Vzhledem k podmínce $\nu b \equiv \varrho \pmod{p}$ musí pro pevné b nabývat ϱ týchž hodnot jako ν a součet druhých členů na levé straně dá 0, neboť je stejný počet zbytků a nezbytků. Kongruence (4.40) má tedy tvar

$$\left(\frac{b}{p}\right) A \equiv A - \sum_{\nu=1}^{p-1} \left(\frac{\nu b}{p}\right) \frac{1}{\nu b}\left[\frac{\nu b}{p}\right] \pmod{p}$$

a po zkrácení $\left(\frac{b}{p}\right)$ a násobení b

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right)\left[\frac{b\nu}{p}\right]\frac{1}{\nu} \equiv -\left(1 - \left(\frac{b}{p}\right)\right) bA \pmod{p}. \tag{4.42}$$

Je-li b kvadratický zbytek modulo p, je $\left(\frac{b}{p}\right) = 1$ a suma

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right)\left[\frac{b\nu}{p}\right]\frac{1}{\nu}$$

je dělitelná p. Je-li b kvadratický nezbytek, musíme rozlišit dva případy. Pro $p = 4n+3$ je tato suma rovněž dělitelná p (viz věta 4.7) a pro $p = 4n+1$ je s ohledem na tvrzení věty 4.8 tato suma kongruentní podle modulu p s číslem $(-1)^n 4 B_n b$.

Násobíme-li kongruenci (4.40) $b^2\nu^2 \equiv \varrho^2$ a užijeme-li logaritmické vlastnosti (3.7), obdržíme

$$b^2 q(b) \cdot \nu^2 + b^2 \cdot \nu^2 q(\nu) \equiv \varrho^2 q(\varrho) - b\nu\left[\frac{b\nu}{p}\right] \pmod{p}.$$

Tyto kongruence opět sečteme pro $\nu = 1, 2, \ldots, p-1$, přičemž opět využijeme skutečnosti, že sčítací indexy pro ν a ϱ jsou stejné. Při dalších úvahách využijeme tvrzení následující věty:

Věta 4.11 *Nechť p je prvočíslo, ν a k jsou kladná celá čísla. Potom platí*

$$\sum_{\nu=1}^{p-1} \nu^k \equiv \begin{cases} 0 & \text{jestliže } (p-1) \nmid k, \\ -1 & \text{jestliže } (p-1) | k. \end{cases} \tag{4.43}$$

Abychom dokázali tuto větu, předpokládejme, že $(p-1) \nmid k$ a g je primitivní kořen, potom g^k není kongruentní s 1 modulo p. Jelikož množiny $g, 2g, \ldots, g(p-1)$ a $1, 2, \ldots, p-1$ jsou ekvivalentní modulo p, platí

$$\sum_{\nu=1}^{p-1} (\nu g)^k \equiv \sum \nu = 1^{p-1} \nu^k \pmod{p};$$

po úpravě obdržíme

$$(g^k - 1) \sum_{\nu=1}^{p-1} \nu^k \equiv 0 \pmod{p}$$

a odsud plyne první část tvrzení. V případě $(p-1)|k$ je druhá část tvrzení důsledkem Malé Fermatovy věty.

V tomto místě se Lerch opět dopustil menší nepřesnosti, neboť předpokládal, že pro lichá prvočísla platí kongruence

$$\sum_{\nu=1}^{p-1} \nu^2 \equiv 0 \pmod{p},$$

ta však podle tvrzení věty 4.11 platí pouze pro prvočísla $p > 3$. Za tohoto předpokladu obdržíme

$$(b^2 - 1) \sum_{\nu=1}^{p-1} \nu^2 q(\nu) \equiv -b \sum_{\nu=1}^{p-1} \nu \left[\frac{b\nu}{p} \right] \pmod{p}. \tag{4.44}$$

Dosadíme-li do (4.44) $b = 2$, máme

$$3 \sum_{\nu=1}^{p-1} \nu^2 q(\nu) \equiv -2 \sum_{\nu=m+1}^{p-1} \nu = -2 \left(\sum_{\nu=1}^{p-1} \nu - \sum_{\nu=1}^{m} \nu \right) \pmod{p},$$

což dává

$$3 \sum \nu^2 q(\nu) \equiv m(m+1) = \frac{p^2 - 1}{4} \equiv -\frac{1}{4} \pmod{p}$$

a po vydělení této kongruence číslem 3 dostaneme následující tvrzení:

Věta 4.12 *Nechť $p > 3$ je prvočíslo. Potom platí*

$$\sum \nu^2 q(\nu) \equiv -\frac{1}{12} \pmod{p}. \tag{4.45}$$

Dosadíme-li kongruenci (4.45) do (4.44), obdržíme zajímavou kongruenci

$$\sum_{\nu=1}^{p-1} \nu \left[\frac{b\nu}{p}\right] \equiv \frac{b^2-1}{12b} \pmod{p},$$

kterou lze přepsat na tvar

$$\frac{1}{b} \equiv b - 12 \sum_{\nu=1}^{p-1} \nu \left[\frac{b\nu}{p}\right] \pmod{p}.$$

Tím je současně nalezeno jedno řešení neurčité rovnice

$$bx - py = 1,$$

přičemž toto řešení má tvar

$$x = b - 12 \sum_{\nu=1}^{p-1} \nu \left[\frac{b\nu}{p}\right].$$

Lerch věnuje v závěru tohoto článku pozornost kvadratickým zbytkům r modulo p. Kongruence (4.8) dává

$$q(\nu^2) \equiv q(r) - \left[\frac{\nu^2}{p}\right] \frac{1}{\nu^2} \pmod{p}.$$

Sečteme-li tyto kongruence od 1 do $p-1$, obdržíme

$$2 \sum_{\nu=1}^{p-1} q(\nu) \equiv 2 \sum_{r} q(r) - \sum_{\nu=1}^{p-1} \left[\frac{\nu^2}{p}\right] \frac{1}{\nu^2} \pmod{p}.$$

Zde bylo použito logaritmické vlastnosti $q(\nu^2) \equiv 2q(\nu)$ a skutečnosti, že pokud ν nabývá všech hodnot od 1 do $p-1$, pak se všech $\frac{p-1}{2}$ kvadratických zbytků vyskytuje dvakrát. Zřejmě platí identita

$$2 \sum_{r} q(r) = \sum \left(1 + \left(\frac{\nu}{p}\right)\right),$$

která s využitím výsledku věty 4.1 a označení (4.28) (Lerch i zde užívá písmene A) dává

$$2 \sum_{r} q(r) \equiv N + A \pmod{p}$$

a tudíž

$$\sum_{\nu=1}^{p-1} \left[\frac{\nu^2}{p}\right] \frac{1}{\nu^2} \equiv A - N \pmod{p}. \tag{4.46}$$

Je-li navíc $p = 4n+3$, je $A \equiv 0$ a tato kongruence dává zajímavé vyjádření zbytků Wilsonových kvocientů.

Označme $a, a', \ldots$ kvadratické zbytky a $b, b', \ldots$ kvadratické nezbytky a položme

$$\sum_a q(a) = A, \qquad \sum_b q(b) = B.$$

Jelikož platí

$$aa' \equiv a' \pmod{p},$$

je

$$aa' = a' + pz \qquad z = \left[\frac{aa'}{p}\right].^{11},$$

Podle kongruence (4.8) platí

$$q(aa') \equiv q(a'') - \frac{1}{aa'}\left[\frac{aa'}{p}\right] \equiv q(a) + q(a').$$

Sčítáme-li přes všechna a', potom a'' nabývá týchž hodnot a máme

$$\frac{p-1}{2}q(a) \equiv -\sum_{a'} \frac{1}{aa'}\left[\frac{aa'}{p}\right] \pmod{p}$$

neboli

$$q(a) \equiv 2\sum_{a'} \frac{1}{aa'}\left[\frac{aa'}{p}\right] \pmod{p}. \tag{4.47}$$

Protože platí

$$ab \equiv b' \pmod{p},$$

je

$$ab = b' + pz$$

a

$$q(ab) \equiv q(b') - \frac{1}{ab}\left[\frac{ab}{p}\right] \equiv q(a) + q(b) \pmod{p}. \tag{4.48}$$

Provedeme-li opět sumaci přes všechny kvadratické nezbytky, obdržíme

$$\frac{p-1}{2}q(a) \equiv -\sum_{b} \frac{1}{ab}\left[\frac{ab}{p}\right] \pmod{p},$$

neboli

$$q(a) \equiv 2\sum_{b} \frac{1}{ab}\left[\frac{ab}{p}\right] \pmod{p}. \tag{4.49}$$

[11] V originále článku je místo této rovnice kongruence podle modulu p. Vzhledem k tomu, že Lerch používá k odvození kongruence (4.49) vztahů (3.7) a (3.9), zdá se být rovnice logičtější (viz odvození kongruence (4.8)). Podobně postupuje při odvozování vzorce (4.50), kdežto při odvozování vzorce (4.51) má již rovnici.

Obě tyto kongruence jsou ovšem důsledkem (4.6) a (4.43).

Sčítáme-li naopak v (4.48) přes všechna a, obdržíme

$$\frac{p-1}{2}q(b) + A \equiv B - \sum_a \frac{1}{ab}\left[\frac{ab}{p}\right],$$

čili

$$q(b) \equiv 2A - 2B + 2\sum_a \frac{1}{ab}\left[\frac{ab}{p}\right] \pmod{p}. \tag{4.50}$$

Vzhledem k tomu, že součin dvou kvadratických nezbytků je kvadratický zbytek, platí

$$bb' = a + pz$$

a z vlastností Fermatových kvocientů máme

$$q(b) + q(b') \equiv q(a) - \frac{1}{bb'}\left[\frac{bb'}{p}\right];$$

sečteme-li tyto kongruence přes všechny b', obdržíme

$$\frac{p-1}{2}q(b) + B \equiv A - \sum_{b'} \frac{1}{bb'}\left[\frac{bb'}{p}\right] \pmod{p},$$

neboli

$$q(b) \equiv -2A + 2B + 2\sum_{b'} \frac{1}{bb'}\left[\frac{bb'}{p}\right] \pmod{p}. \tag{4.51}$$

Porovnáme-li (4.50) a (4.51), obdržíme

$$\sum_a \frac{1}{ab}\left[\frac{ab}{p}\right] - \sum_{b'} \frac{1}{bb'}\left[\frac{bb'}{p}\right] \equiv 2(B - A) \pmod{p}. \tag{4.52}$$

Zde se Lerch dopustil drobného přehlédnutí, neboť v originále článku [Lr7] má na levé straně obrácená znaménka. Tento výsledek je však shodný s kongruencí (4.43), v níž ovšem

$$A = \sum_1^{p-1} \left(\frac{\nu}{p}\right) q(\nu).$$

4.6 Případ složeného modulu

Složenému modulu se Lerch věnoval v obou jím publikovaným článcích. Kvocient $q(a)$ je definován vzorcem

$$q(a) = \frac{a^{\varphi(m)} - 1}{m}, \tag{4.53}$$

kde $\varphi(m)$ je Eulerova funkce. V práci [Lr7] nejdříve rozšiřuje platnost Eisensteinových vzorců (3.7) a (3.9) i pro složený modul m.

Věta 4.13 *Nechť m je liché číslo, a celé číslo vyhovující podmínce $(a,m)=1$. Potom platí*

$$q(ab) \equiv q(a) + q(b) \pmod{m} \tag{4.54}$$

a

$$q(c+mz) \equiv q(c) + \frac{\varphi(m)z}{c} \pmod{m}. \tag{4.55}$$

Lerch neuvádí explicitní důkaz, ale ten je pouze obdobou důkazu pro prvočíselný modul. Lerch připojuje i další kongruenci, kterou lze vyjádřit následující větou:

Věta 4.14 *Nechť $ab \equiv c \pmod{m}$, přičemž $0 < c < m$. Potom platí*

$$q(ab) \equiv q(c) + \frac{\varphi(m)}{ab}\left[\frac{ab}{m}\right] \pmod{m}. \tag{4.56}$$

Toto tvrzení se snadno ověří, uvědomíme-li si, že z předpokladu $ab \equiv c \pmod{m}$ plyne $ab = c + km$, přičemž $k = \left[\frac{ab}{m}\right]$.

Lerch odvodil následující větu pro složený modul:

Věta 4.15 *Nechť platí $(m, \varphi(m)) = 1$. Potom platí*

$$\frac{1}{a} \equiv a - \frac{12}{P(m)} \sum_b b \left[\frac{ab}{m}\right] \pmod{m}. \tag{4.57}$$

Důkaz této věty vychází z kongruence (4.56). Vynásobíme-li ji $a^2b^2 \equiv c^2$, obdržíme

$$a^2 q(a) \cdot b^2 + a^2 b^2 q(b) \equiv c^2 q(c) + \varphi(m) ab \left[\frac{ab}{m}\right] \pmod{m}.$$

Tyto kongruence sečteme pro všechna b, která jsou nesoudělná s modulem m, těchto čísel je právě $\varphi(m)$. Při pevném a bude c nabývat stejných hodnot jako b. Výsledkem je kongruence

$$a^2 q(a) s_2 + (a^2 - 1) \sum_b b^2 q(b) \equiv \varphi(m) a \sum_b b \left[\frac{ab}{m}\right] \pmod{m}, \tag{4.58}$$

kde s_2 je součet kvadrátů všech čísel nesoudělných s modulem. Volba $a = 2$ dává následující kongruenci

$$4q(2)s_2 + 3\sum b^2 q(b) \equiv 2\varphi(m) \sum b' \pmod{m}, \tag{4.59}$$

přičemž $b' > \frac{m}{2}$. Dále platí

$$\sum b' \equiv \sum (m - \beta) \equiv -\sum \beta \pmod{m},$$

kde β jsou čísla nesoudělná s m splňující podmínku $0 < \beta < \frac{m}{2}$. Označíme-li

$$f(n) = \sum_{\nu=1}^{\left[\frac{n}{2}\right]} \nu,$$

je

$$\sum \beta = \sum \mu(d) df \left(\frac{m}{d}\right),$$

kde d jsou všichni dělitelé m a $\mu(d)$ je Moebiova funkce. Je-li m a tedy i $\frac{m}{d} = d'$ liché a využijeme-li vzorec pro součet aritmetické posloupnosti, obdržíme

$$f(d') = \sum_{1}^{\frac{d'-1}{2}} \nu = \frac{d'^2 - 1}{8},$$

odkud

$$\sum \beta = \frac{1}{8} \sum \mu(d)(md' - d) \tag{4.60}$$

a přejdeme-li ke kongruenci, obdržíme

$$\sum \beta \equiv -\frac{1}{8} \sum d\mu(d).$$

Označíme-li

$$P(m) = \prod (1 - p_i), \tag{4.61}$$

kde p_i jsou prvočinitelé modulu m, je

$$\sum \beta \equiv -\frac{1}{8} P(m). \tag{4.62}$$

Dále musíme vyjádřit součet s_2. Označíme-li pro jednoduchost

$$F(n) = \sum_{\nu=1}^{n-1} \nu^2,$$

je

$$s_2 = \sum_d \mu(d) d^2 F\left(\frac{m}{d}\right),$$

kde d jsou všichni dělitelé čísla m. Pomocí matematické indukce lze dokázat vzorec

$$F(n) = \frac{n^3}{3} - \frac{n^2}{2} + \frac{n}{6},$$

máme tedy

$$s_2 = \frac{m^2}{3} \sum \mu(d) d' - \frac{m^2}{2} \sum \mu(d) + \frac{m}{6} \sum d\mu(d)$$

a protože $\sum \mu(d) = 0$ je

$$s_2 = \frac{m^2}{3}\varphi(m) + \frac{m}{6}P(m). \tag{4.63}$$

Pokud m není dělitelné 3, je

$$s_2 \equiv 0 \pmod{m}$$

a kongruence (4.58) má tvar

$$\sum b^2 q(b) \equiv \frac{1}{12}\varphi(m)P(m) \pmod{m}, \tag{4.64}$$

přičemž sčítací index nabývá všech $\varphi(m)$ hodnot nesoudělných s m. Dosadíme-li (4.64) do kongruence (4.58), dostaneme

$$\left(a - \frac{1}{a}\right)\frac{\varphi(m)P(m)}{12} \equiv \varphi(m)\sum_b b\left[\frac{ab}{m}\right] \pmod{m}.$$

Je-li $(m, \varphi(m)) = 1$, což nastává tehdy, je-li m součin různých prvočísel, potom je i výraz $P(m)$ nesoudělný s kterýmkoliv z nich a tuto kongruenci lze dělit $\varphi(m)P(m)$ a obdržíme tvrzení věty 4.15.

Je-li m dělitelné třemi a má-li být splněna podmínka $(m, \varphi(m)) = 1$, musí musí být všechny prvočinitelé s výjimkou 3 tvaru $3k + 2$, neboť ani jedno z čísel $p_i - 1$ nesmí být dělitelné třemi. Je tedy

$$s - 2 \equiv \frac{m}{6}P(m) \mod m,$$

a po dosazení do (4.59) máme

$$3\sum b^2 q(b) \equiv P(m)\left[\frac{1}{4}\varphi(m) - \frac{2}{3}mq(2)\right] \pmod{m}.$$

Kongruenci (4.59) lze psát ve tvaru

$$\frac{a^2-1}{3}P(m)\left[\frac{1}{4}\varphi(m) - \frac{2}{3}mq(2)\right] + a^2 q(a)\cdot\frac{m}{6}P(m) \equiv \varphi(m)a\sum b\left[\frac{ab}{m}\right] \pmod{m}.$$

Násobíme-li tuto kongruenci číslem 3, obdržíme

$$(a^2-1)P(m)\frac{1}{4}\varphi(m) - (a^2-1)P(m)\frac{2}{3}mq(2) + a^2 q(a)\frac{m}{2}P(m) \equiv \equiv 3\varphi(m)a\sum b\left[\frac{ab}{m}\right] \pmod{m}.$$

Třetí člen odpadá a druhý člen je dělitelný m a tudíž výraz (a^2-1) je dělitelný třemi. Máme tedy

$$\left(a-\frac{1}{a}\right)\frac{P(m)\varphi(m)}{4}\equiv\varphi(m)\cdot 3\sum b\left[\frac{ab}{m}\right]\pmod m$$

a odsud dostaneme tvrzení věty 4.14.

V práci [Lr9] navázal Lerch na práce Sylvestera a Mirimanoffa. Dokázal, že i pro složený modul platí jeho kongruence (4.6).

Věta 4.16 *Nechť a a m jsou celá kladná čísla vyhovující podmínce $(a,m)=1$, $\varphi(m)$ je Eulerova funkce. Potom platí*

$$q(a)=\frac{a^{\varphi(m)}-1}{m}\equiv\sum_{\nu}\frac{1}{a\nu}\left[\frac{a\nu}{m}\right]\pmod m, \tag{4.65}$$

přičemž sčítáme přes všechna $\nu<m$ a $\nu\nmid m$.

Důkaz této věty lze provést využitím identity

$$\prod\nu=\prod\left(a\nu-m\left[\frac{a\nu}{m}\right]\right).$$

Provedeme-li roznásobení na pravé straně, obdržíme

$$\prod\nu=a^{\varphi(m)}\prod\nu-ma^{\varphi(m)-1}\prod\nu\sum\frac{1}{\nu}\left[\frac{a\nu}{m}\right]+m^2K\prod\nu,$$

kde K je celé číslo. Tuto rovnici vydělíme $m\prod\nu$ a po úpravě obdržíme

$$\frac{a^{\varphi(m)}-1}{m}=a^{\varphi(m)-1}\sum\frac{1}{\nu}\left[\frac{a\nu}{m}\right]+mK$$

a odsud plyne kongruence

$$\frac{a^{\varphi(m)}-1}{m}=q(a)\equiv a^{\varphi(m)}\sum\frac{1}{a\nu}\left[\frac{a\nu}{m}\right]\pmod m.$$

Z Eulerovy věty plyne, že $a^{\varphi(m)}=lm+1$ a to dává hledanou kongruenci (4.65).

Závěrem článku [Lr9] uvádí Lerch ještě jednu důležitou kongruenci:

Věta 4.17 *Nechť $m=m_1m_2m_3\ldots m_\nu$, přičemž čísla m_i jsou po dvou nesoudělná. Položme $m=m_in_i$ a nechť n_i' vyhovuje kongruenci $n_i^2n_i'\equiv 1\pmod{m_i}$. Potom platí*

$$q(a,m)\equiv\sum_{1}^{\nu}n_in_i'\varphi(n_i)q(a,m_i)\pmod m. \tag{4.66}$$

Lerch neuvádí důkaz této věty; protože musí být splněna podmínka o nesoudělnosti činitelů, stačí to dokázat pro libovolný z nich. Nechť tedy platí $m = m_i n_i$. Využitím multiplikativnosti Eulerovy funkce a identity (2.1) lze psát

$$a^{\varphi(m)} - 1 = a^{\varphi(m_i)\varphi(n_i)} - 1 = (a^{\varphi(m_i)} - 1) \sum_{k=0}^{\varphi(n_i)-1} a^{\varphi(m_i)k},$$

a po vydělení m máme

$$\frac{a^{\varphi(m)-1}}{m} = \frac{a^{\varphi(m_i)-1}}{m_i} \frac{\sum_{k=0}^{\varphi(n_i)-1} a^{\varphi(m_i)k}}{n_i}.$$

Protože první dva zlomky jsou celá čísla, musí platit

$$a^{\varphi(m_i)} \equiv 1 \pmod{n_i}.$$

Podle Eulerovy věty zase platí

$$\sum_{k=0}^{\varphi(n_i)-1} a^{\varphi(m_i)k} \equiv \varphi(n_i) \pmod{m},$$

což spolu s definicí čísla n_i' dává tvrzení věty (4.15).