Fermatovy kvocienty

In: Karel Lepka (author): Historie Fermatových kvocientů (Fermat – Lerch). (Czech). Praha: Prometheus, 2000. pp. 29–41.

Persistent URL: http://dml.cz/dmlcz/401888

Kapitola 3

Fermatovy kvocienty

V této kapitole jsou uvedeny nejdůležitější výsledky teorie Fermatova kvocientu od roku 1828 až do roku 1905, kdy Lerch publikoval svoji práci [Lr7]. Pozornost je věnována především pracím Jacobiho, Eisensteina, Sylvestera, Sterna a Mirimanoffa. Tyto výsledky byly shrnuty ve výborně napsané Bachmannově učebnici Niedere Zahlentheorie [Ba].

3.1 Abelův problém

Historie Fermatových kvocientů začíná v roce 1828. Tehdy totiž norský matematik N. H. Abel uveřejnil v časopise *Journal für Mathematik* [Ab] následující úlohu: *Může být číslo* $\alpha^{\mu-1}-1$, *kde* μ *je prvočíslo a* $1<\alpha<\mu$ *celé číslo, dělitelné* μ^2*?* Ve stejném roce uveřejnil v tomtéž časopise C. G. J. Jacobi řešení této úlohy [Jc]. Jacobi své řešení podrobně nerozebírá, uvádí pouze, že hledal řešení kongruence

$$x^{\mu-1}\equiv 1 \pmod{\mu^2}$$

a že toto řešení hledal ve tvaru $a+\mu a'$, kde a, a' jsou kladná čísla menší než μ. Řešení provedl pro všechna prvočísla od 3 do 37 včetně. Pokusme se na Jacobiho řešení podívat podrobněji.

Z teorie řešení kongruencí $n-$tého stupně plyne, že je-li x_0 řešením kongruence

$$f(x)\equiv 0 \pmod{\mu^2}, \tag{3.1}$$

kde $f(x)$ je polynom stupně n, potom musí být rovněž řešením kongruence

$$f(x)\equiv 0 \pmod{\mu}. \tag{3.2}$$

Známe-li libovolné řešení a kongruence (3.2), je $x_0=a+a'\mu$. Dále platí

$$f(a+a'\mu)\equiv f(a)+a'\mu f'(a) \pmod{\mu^2},$$

přičemž na pravé straně je Taylorův rozvoj funkce $f(x)$ se středem v bodě a. Zbývající členy tohoto rozvoje jsou totiž kongruentní s nulou podle modulu μ^2.

Vzhledem k tomu, že podle Fermatovy věty má kongruence (3.2) řešení pro všechna přirozená čísla $a < \mu$ a že $f'(a) = (\mu - 1)a^{\mu-2}$ není kongruentní s nulou podle modulu μ, má kongruence

$$x^{\mu-1} - 1 \equiv 0 \pmod{\mu^2}$$

jediné řešení $x_0 = a + a'\mu$, přičemž a' je řešení kongruence

$$a^{\mu-1} - 1 + a'\mu(\mu - 1)a^{\mu-2} \equiv 0 \pmod{\mu^2}.$$

Tato úloha je vlastně řešením kongruence

$$\frac{x^{\mu-1} - 1}{\mu} \equiv 0 \pmod{\mu},$$

jinými slovy řeší otázku, zda je Fermatův kvocient dělitelný číslem μ.

V závěru této části uvedeme zajímavou souvislost mezi Velkou a Malou Fermatovou větou, která úzce souvisí s Abelovým problémem. V roce 1909 dokázal *A. Wieferich* následující větu:

Věta 3.1 *Nechť p je liché prvočíslo a x, y, z jsou celá čísla nedělitelná p, která splňují rovnici*

$$x^p + y^p = z^p.$$[1]

Za těchto předpokladů platí kongruence

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Prvočísla, která tuto kongruenci splňují, se nazývají *Wieferichova prvočísla.* (Tato prvočísla splňují rovněž kongruenci $q(2) \equiv 0 \pmod{p}$, jak plyne z předchozích úvah.) I v tomto případě nám přirozená čísla poskytla pozoruhodný výsledek, neboť do dnešní doby byla objevena pouze dvě Wieferichova prvočísla, a to 1093 Meissnerem v roce 1913 a 3511 Beegerem v roce 1922, tedy ještě v „předpočítačové éře.“ Navíc *D. H. Lehmer* dokázal v roce 1981 [Lh], že pro $p < 6 \cdot 10^9$ neexistuje další Wieferichovo prvočíslo. Tuto hranici posunuli v roce 1997 *R. Crandall*, *K. Dilcher* a *C. Pomerance*, kteří ukázali, že neexistuje žádné další Wieferichovo prvočíslo pro $p < 4 \cdot 10^{12}$ [CDP]. Výzkum těchto prvočísel probíhá v posledních letech velmi intenzívně a je možné, že se dočkáme dalších překvapení. Byly rovněž dokázány věty analogické Wieferichově pro jiná čísla než 2; jelikož tato problematika není tématem této práce, odkazujeme čtenáře na publikaci [Ri2].

3.2 Práce G. Eisensteina

Německý matematik G. Eisenstein publikoval ve *Zprávách Královské Pruské Akademie věd* článek [Ei] nazvaný *Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definirt werden.*[2] Eisenstein zde definuje funkci $f(m, n)$, která je pro libovolná celá čísla m, n a liché prvočíslo p definována následujícím způsobem:

[1] Velká Fermatova věta se obvykle dělí na dva případy. Případ I, kdy ani jedno z čísel x, y, z není dělitelné p a Případ II, kdy právě jedno z čísel x, y, z je dělitelné p.

[2] Nový druh číselně teoretických funkcí dvou proměnných, definovaný pomocí jistých lineárních funkcionálních rovnic.

1. $f(m,n) \equiv f(m,m+n) + f(m+n,n) \pmod{p}$, je-li $m+n \neq p$;
2. $f(m,n) \equiv n \pmod{p}$, je-li $m+n = p$;
3. $f(m,n) \equiv 0 \pmod{p}$, je-li $m+n > p$.

Je-li $(m,n) = 1$, potom dokázal, že platí

$$f(m,n) \equiv \sum \frac{1}{r} \pmod{p}, \tag{3.3}$$

kde r jsou všechna celá čísla daná nerovností $\frac{n_0}{n} < \frac{r}{p} < \frac{m_0}{m}$, přičemž m_0 a n_0 jsou nejmenší celočíselná řešení neurčité rovnice $nm_0 - mn_0 = 1$. Volíme-li $m = 1$, $n = 2$, je $m_0 = n_0 = 1$ a r nabývá všech hodnot od $\frac{p+1}{2}$ do $p-1$. Zde se Eisenstein dopustil menší nepřesnosti, neboť uvádí dolní hodnotu $\frac{p-1}{2}$, tato však uvedené nerovnosti nevyhovuje. Platí tedy kongruence

$$f(1,2) \equiv \sum_{r=\frac{p+1}{2}}^{p-1} \frac{1}{r} \pmod{p}. \tag{3.4}$$

Pravou stranu této kongruence lze vyjádřit poněkud jiným způsobem. Snadno se totiž dokáže, že pro lichá celá čísla $p \geq 3$ platí rovnost

$$1 - \frac{1}{2} + \frac{1}{3} - \cdots - \frac{1}{p-1} = \frac{1}{\frac{p+1}{2}} + \frac{1}{\frac{p+3}{2}} + \cdots + \frac{1}{p-1}.$$

Tato rovnost evidentně platí pro $p = 3$, můžeme tedy předpokládat její platnost pro nějaké liché p. Nyní stačí přičíst k oběma stranám rovnice $\frac{1}{p} - \frac{1}{p+1}$ a snadno se vidí, že za tohoto předpokladu rovnice platí i pro $p+2$. Platí tedy kongruence

$$f(1,2) \equiv 1 - \frac{1}{2} + \frac{1}{3} - \cdots - \frac{1}{p-1} \pmod{p}.$$

Dále platí podle binomické věty

$$(1+u)^p - (1+u^p) = pu + \frac{p(p-1)}{1 \cdot 2}u^2 + \\ + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3}u^3 + \cdots + \frac{p(p-1)\cdots(p-(p-2))}{1 \cdot 2 \cdots (p-1)}u^{p-1}.$$

Vezmeme-li v potaz, že pro libovolné celé číslo i, které splňuje podmínku $1 \leq i \leq p-1$ platí $\frac{p-i}{i} \equiv -1 \pmod{p}$, lze tuto rovnici nahradit kongruencí

$$(1+u)^p - (1+u^p) \equiv pu - \frac{p}{2}u^2 + \frac{p}{3}u^3 - \cdots - \frac{p}{p-1}u^{p-1} \pmod{p^2}$$

a po vydělení modulem p máme

$$\frac{(1+u)^p - (1+u^p)}{p} \equiv u - \frac{u^2}{2} + \frac{u^3}{3} - \cdots - \frac{u^{p-1}}{p-1} \pmod{p}. \tag{3.5}$$

Položíme-li $u = 1$, obdržíme následující tvrzení:

Věta 3.2 *Nechť p je liché prvočíslo. Potom platí*

$$f(1,2) \equiv 1 - \frac{1}{2} + \frac{1}{3} - \cdots - \frac{1}{p-1} \equiv \frac{2^p - 2}{p} = 2q(2) \pmod{p}. \tag{3.6}$$

Eisenstein ještě název Fermatův kvocient nepoužíval, stejně tak jako označení $q(a)$ pro tento kvocient.

Eisenstein se dále zmiňuje o funkci $u' = \Lambda(u)$, která je definovaná kongruencí

$$u^{p-1} \equiv 1 + pu' \pmod{p^2}.$$

Napíšeme-li tuto kongruenci ve tvaru

$$\frac{u^{p-1} - 1}{p} \equiv u' \pmod{p},$$

je zřejmé, že $u' \equiv q(u) \pmod{p}$, proto budeme dále používat označení $q(u)$, resp. $q(a)$. Vlastnosti této funkce lze vyjádřit následující větou:

Věta 3.3 *Nechť a, b, c jsou celá kladná čísla taková, že $(a,p) = (b,p) = (c,p) = 1$. Potom pro libovolné m přirozené a z celé platí*

$$q(ab) \equiv q(a) + q(b) \pmod{p}, \tag{3.7}$$

$$q(a^m) \equiv mq(a) \pmod{p}, \tag{3.8}$$

$$q(c + pz) \equiv q(c) - \frac{z}{c} \pmod{p}. \tag{3.9}$$

První dvě vlastnosti jsou shodné s vlastnostmi logaritmu. Eisenstein neuvádí důkaz, ten však plyne bezprostředně z definice Fermatova kvocientu. Je totiž

$$a^{p-1} \equiv 1 + pq(a) \pmod{p^2} \quad \text{a} \quad b^{p-1} \equiv 1 + pq(b) \pmod{p^2}$$

a tudíž

$$(ab)^{p-1} \equiv 1 + pq(a) + pq(b) + p^2 q(a)q(b) \pmod{p^2},$$

což po menší úpravě dává

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

Druhá vlastnost je důsledkem první, volíme-li $b = a$ atd.

Třetí vlastnost dokážeme rozvinutím $(c+pz)^{p-1}$ podle binomické věty. Protože všechny členy s výjimkou prvních dvou jsou násobky p^2, lze přejít ke kongruenci podle modulu p^2, čímž obdržíme

$$(c + pz)^{p-1} \equiv c^{p-1} + (p-1)pc^{p-2}z \pmod{p^2},$$

což po úpravě dává

$$(c + pz)^{p-1} \equiv c^{p-1} - p \cdot \frac{z}{c} \cdot c^{p-1} \pmod{p^2}.$$

Z definice Fermatova kvocientu je

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

a po dosazení

$$(c + pz)^{p-1} \equiv 1 + pq(c) - \frac{pz}{c} \pmod{p^2}.$$

Po vydělení p a úpravě obdržíme požadovaný vztah.

Podívejme se na tato tvrzení z hlediska moderní algebry. Platí totiž následující tvrzení:

Věta 3.4 *Nechť p je prvočíslo a $a \equiv b \pmod{p^2}$ jsou libovolná celá kladná čísla splňující podmínku $(a, p) = (b, p) = 1$. Potom platí $q(a) \equiv q(b) \pmod{p}$.*

Fermatův kvocient tedy zobrazuje množinu $(\mathbb{Z}/p^2\mathbb{Z})^*$ na množinu $\mathbb{Z}/p\mathbb{Z}$. Toto zobrazení je surjekce, neboť platí

$$q(p-1) = \frac{(p-1)^{p-1} - 1}{p} = \frac{p^{p-1} - \binom{p-1}{1}p^{p-2} + \cdots - \binom{p-1}{p-2}p + 1 - 1}{p}.$$

Přejdeme-li ke kongruenci podle modulu p, lze vypustit všechny členy kromě posledního, neboť jsou násobky p^2. Poslední člen má tvar $\frac{-(p-1)p}{p}$ a platí tedy

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

Obraz $\mathrm{Im}(q) = \mathbb{Z}/p\mathbb{Z}$. Jádro je

$$\mathrm{Ker}(q) = \{\alpha \in (\mathbb{Z}/p^2\mathbb{Z})^* : Q(\alpha) \equiv 0 \pmod{p}\}$$

a protože platí

$$|\ \mathrm{Ker}(q)\ | \cdot |\ \mathrm{Im}(q)\ | = |\ (\mathbb{Z}/p^2\mathbb{Z})^*\ | = p(p-1),$$

je

$$|\ \mathrm{Ker}(q)\ | = p - 1.$$

Logaritmická vlastnost zase dokazuje existenci homomorfizmu grupy $(\mathbb{Z}/p^2\mathbb{Z}, .)^*$ na grupu $(\mathbb{Z}/p\mathbb{Z}, +)$.

V závěru svého článku se Eisenstein ještě vrací k Abelovu problému ([Ab]), kdy uvádí, že všechna řešení jsou tvaru

$$x \equiv a + pa\Lambda(a) \pmod{p^2},$$

kde $a < p$ je libovolné celé kladné číslo.

3.3 Sylvesterovy práce

Sylvester uvádí při různých příležitostech ([Sy1], [Sy2] a [Sy3]) další kongruence pro Fermatovy kvocienty, tyto své výsledky však uvádí bez důkazů a v podstatě bez sebemenšího náznaku, jakou cestou k nim dospěl. Sylvester jako první používá pojem Fermatův kvocient. Sylvesterovy výsledky uvedeme jen v přehledu.

Věta 3.5 *Nechť p je prvočíslo, r celé kladné číslo splňující podmínku $(r,p)=1$. Potom platí*

$$\frac{r^{p-1}-1}{p} \equiv \frac{c_1}{p-1}+\frac{c_2}{p-2}+\cdots+\frac{c_{p-1}}{1} \pmod p, \tag{3.10}$$

kde koeficienty $c_1, c_2, \ldots, c_{p-1}$ jsou opakující se čísla $1, 2, \ldots, r$, přičemž celý cyklus začíná číslem r', které splňuje podmínku $pr' \equiv 1 \pmod r$.

Na základě této obecné kongruence odvodil některé kongruence pro speciální volbu r. Z nich uvádíme

$$q(5) \equiv \frac{1}{p-1}+\frac{2}{p-2}+\frac{3}{p-3}+\frac{4}{p-4}+\frac{5}{p-5}+\frac{1}{p-6}+\cdots \pmod p, \tag{3.11}$$

je-li $p = 10k+1$ a

$$q(5) \equiv \frac{3}{p-1}+\frac{1}{p-2}+\frac{4}{p-3}+\frac{2}{p-4}+\frac{5}{p-5}+\frac{3}{p-6}+\cdots \pmod p, \tag{3.12}$$

je-li $p = 10k+7$.

Dále uvádí kongruence

$$q(2) \equiv 2\left(\frac{1}{p-3}+\frac{1}{p-4}+\frac{1}{p-7}+\frac{1}{p-8}+\frac{1}{p-11}+\cdots\right) \pmod p, \tag{3.13}$$

je-li $p = 4k+1$ a

$$q(2) \equiv -2\left(\frac{1}{p-2}+\frac{1}{p-3}+\frac{1}{p-6}+\frac{1}{p-7}+\frac{1}{p-10}+\cdots\right) \pmod p, \tag{3.14}$$

je-li $p = 4k-1$. Pro libovolné p platí

$$q(2) \equiv -\frac{1}{p-1}+\frac{1}{p-2}-\frac{1}{p-3}+\cdots \pmod p. \tag{3.15}$$

Tyto výsledky byly později dokázány Sternem [St] a Mirimanoffem [Mi].

3.4 Sternův přínos

V roce 1895 publikoval Moritz Stern práci [St], v níž odvodil řadu zajímavých kongruencí pro Fermatovy kvocienty. Stern předpokládal, že p je liché prvočíslo. Přičteme-li k oběma stranám Eisensteinovy kongruence (3.5) výraz $\frac{u^p-u}{p}$, obdržíme novou kongruenci

$$\frac{(1+u)^p-(1+u)}{p} \equiv u-\frac{u^2}{2}+\cdots-\frac{u^{p-1}}{p-1}+\frac{u^p-u}{p} \pmod p$$

a po substituci $1+u=r$ je

$$\frac{r^p-r}{p} \equiv (r-1) - \frac{(r-1)^2}{2} + \frac{(r-1)^3}{3} - \cdots - \\ -\frac{(r-1)^{p-1}}{p-1} + \frac{(r-1)^p-(r-1)}{p} \pmod p. \tag{3.16}$$

Dosadíme-li do této kongruence $r-1$ místo r, obdržíme

$$\frac{(r-1)^p-(r-1)}{p} \equiv (r-2) - \frac{(r-2)^2}{2} + \frac{(r-2)^3}{3} - \cdots \\ -\frac{(r-2)^{p-1}}{p-1} + \frac{(r-2)^p-(r-2)}{p} \pmod p. \tag{3.17}$$

Do takto vzniklé kongruence dosadíme $r-2$ místo $r-1$ a tak postupujeme dál, až nakonec obdržíme kongruenci podle modulu p

$$\frac{r^p-r}{p} \equiv \begin{cases} 1+2+\cdots+r-1- \\ -\frac{1}{2}[1+2^2+\cdots+(r-1)^2]+ \\ +\frac{1}{3}[1+2^3+\cdots+(r-1)^3]- \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ -\frac{1}{p-1}[1+2^{p-1}+\cdots+(r-1)^{p-1}]. \end{cases} \tag{3.18}$$

Aplikací binomické věty získáme kongruenci

$$\frac{(r-1)^p}{p} \equiv \frac{r^p-1}{p} - \left(r^{p-1} + \frac{r^{p-2}}{2} + \cdots + \frac{r}{p-1}\right) \pmod p$$

a odečteme-li od obou stran této kongruence výraz $\frac{r-1}{p}$, obdržíme

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

Dosadíme-li tuto kongruenci do (3.16), obdržíme

$$r-1-\frac{(r-1)^2}{2} - \cdots - \frac{(r-1)^{p-1}}{p-1} \equiv r^{p-1} + \frac{r^{p-2}}{2} + \cdots + \frac{r}{p-1} \pmod p. \tag{3.19}$$

Volba $r=1$ dává následující důležitou kongruenci:

Věta 3.6 *Nechť p je liché prvočíslo. Potom platí*

$$\sum_{\nu=1}^{p-1} \frac{1}{\nu} \equiv 0 \pmod p. \tag{3.20}$$

Kongruence (3.16) se dá psát ve tvaru

$$\frac{r^p-r}{p} \equiv r^{p-1} + \frac{r^{p-2}}{2} + \cdots + \frac{r}{p-1} + \frac{(r-1)^p-(r-1)}{p} \pmod p;$$

pokud sem budeme postupně dosazovat $r-1$, $r-2$ atd. místo r, obdržíme

$$\frac{r^p-r}{p} \equiv \begin{cases} 1+2^{p-1}+\cdots+(r-1)^{p-1}+r^{p-1}+ \\ +\frac{1}{2}[1+2^{p-2}+\cdots+(r-1)^{p-2}+r^{p-2}]+ \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ +\frac{1}{p-1}[1+2^{p-1}+\cdots+(r-1)^{p-1}]. \end{cases} \tag{3.21}$$

Sečtením kongruencí (3.18) a (3.21) a s ohledem na zřejmé kongruence

$$\frac{1}{k}+\frac{1}{p-k} \equiv 0, \qquad \frac{1}{p-k}-\frac{1}{k} \equiv \frac{2}{p-k} \pmod{p}$$

obdržíme

$$\frac{r^p-r}{p} \equiv \begin{cases} \frac{1}{2}\left[\frac{r}{p-1}+\frac{r^2}{p-2}+\cdots+r^{p-1}\right]+ \\ +\frac{1}{p-2}\left[1+2^2+\cdots+(r-1)^2\right]+ \\ +\frac{1}{p-4}\left[1+2^4+\cdots+(r-1)^4\right]+ \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ +[1+2^{p-1}+\cdots+(r-1)^{p-1}]. \end{cases} \tag{3.22}$$

Odečteme-li (3.18) od (3.21), obdržíme

$$0 \equiv \begin{cases} \frac{1}{2}\left[\frac{r}{p-1}+\frac{r^2}{p-2}+\cdots+r^{p-1}\right]+ \\ +\frac{1}{p-1}\left[1+2+\cdots+(r-1)\right]+ \\ +\frac{1}{p-3}\left[1+2^3+\cdots+(r-1)^3\right]+ \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ +\frac{1}{2}\left[1+2^{p-2}+\cdots+(r-1)^{p-2}\right]. \end{cases}$$

Dosadíme-li do (3.18) $r=2$, obdržíme Eisensteinovu kongruenci (3.6), kterou však s ohledem na (3.20) můžeme psát ve tvaru

$$\frac{2^{p-1}-1}{p} \equiv 1+\frac{1}{3}+\cdots+\frac{1}{p-2} \pmod{p}. \tag{3.23}$$

Je-li k liché, potom se snadno ověří platnost kongruence

$$\frac{1}{k}-\frac{1}{p-k} \equiv \frac{1}{\frac{p+k}{2}} \pmod{p},$$

naproti tomu pro k sudé platí

$$-\frac{1}{k}+\frac{1}{p-k} \equiv \frac{1}{p-\frac{k}{2}} \pmod{p}.$$

Je tedy

$$1-\frac{1}{p-1} \equiv \frac{1}{\frac{p+1}{2}} \pmod{p}, \quad \frac{1}{3}-\frac{1}{p-3} \equiv \frac{1}{\frac{p+3}{2}} \pmod{p} \quad \text{a.t.d.}$$

a pro $p = 4n + 1$ dojdeme nakonec ke kongruenci

$$\frac{1}{\frac{p-3}{2}} - \frac{1}{\frac{p+3}{2}} \equiv \frac{1}{\frac{3p-3}{4}} \pmod{p};$$

dále platí

$$-\frac{1}{2} + \frac{1}{p-2} \equiv \frac{1}{p-1} \pmod{p}, \quad -\frac{1}{4} + \frac{1}{p-4} \equiv \frac{1}{p-2} \pmod{p} \quad \text{a.t.d.}$$

až konečně dospějeme ke kongruenci

$$-\frac{1}{\frac{p-1}{2}} + \frac{1}{p - \frac{p-1}{2}} \equiv \frac{1}{\frac{3p+1}{4}} \pmod{p}.$$

Shrneme-li tyto výsledky, obdržíme kongruenci

$$1 - \frac{1}{2} + \frac{1}{3} - \cdots - \frac{1}{p-1} \equiv \frac{1}{\frac{p+1}{2}} + \frac{1}{\frac{p+3}{2}} + \cdots + \frac{1}{p-1} \pmod{p}. \tag{3.24}$$

Obdobným postupem lze pro $p = 4n + 3$ odvodit tutéž kongruenci, rozdíl je pouze v tom, že poslední dvojice jsou

$$\frac{1}{\frac{p-1}{2}} - \frac{1}{p - \frac{p-1}{2}} \quad \text{a} \quad -\frac{1}{\frac{p-3}{2}} + \frac{1}{p+3} 2.$$

Z kongruence (3.24) plynou zároveň kongruence

$$1 - \frac{1}{2} + \frac{1}{3} - \cdots - \frac{1}{\frac{p-1}{2}} \equiv 2\left[\frac{1}{\frac{p+3}{2}} + \frac{1}{\frac{p+7}{2}} + \cdots + \frac{1}{p-1}\right] \pmod{p},$$

je-li $p = 4n + 1$ a

$$1 - \frac{1}{2} + \cdots + \frac{1}{\frac{p-5}{2}} - \frac{1}{\frac{p-3}{2}} + \frac{1}{\frac{p-1}{2}} \equiv 2\left[\frac{1}{\frac{p+1}{2}} + \frac{1}{\frac{p+5}{2}} + \cdots + \frac{1}{p-1}\right] \pmod{p},$$

je-li $p = 4n + 3$. V originále článku je tisková chyba, třetí člen této kongruence má ve jmenovateli $\frac{p+5}{2}$.

Další kongruence Stern odvozuje pomocí komplexních čísel, přitom tato metoda zde byla použita poprvé. Platí totiž kongruence

$$\frac{(1+i)^{2p} - (1+i^{2p})}{p} \equiv 2i - \frac{2i^2}{2} + \frac{2i^3}{3} \cdots - \frac{2i^{2p-2}}{2} + 2i^{2p-1} \pmod{p}.$$

Každé dva členy se sudými exponenty jako $\frac{2i^2}{2}$ a $\frac{2i^{2p-2}}{2}$ se ruší, zatímco členy s lichým exponentem jako $2i$ a $2i^{2p-1}$ jsou stejné a člen $\frac{2i^p}{p}$ je osamocený, takže obdržíme

$$\frac{(1+i)^{2p} - (1+i^{2p}) - 2i^p}{p} \equiv 2 \cdot 2i \left(1 - \frac{1}{3} + \frac{1}{5} \cdots \mp \frac{1}{p-2}\right) \pmod{p},$$

přičemž znaménko $-$ platí pro $p = 4n+1$ a znaménko $+$ pro $p = 4n+3$. Podle stejných předpokladů platí

$$(1+i)^{2p} - i^{2p} - 1 - 2i^p = \pm 2i(2^{p-1} - 1),$$

což porovnáním dává výslednou kongruenci

$$\pm\frac{2^{p-1}-1}{p} \equiv 2\left(1 - \frac{1}{3} + \frac{1}{5} - \cdots \mp \frac{1}{p-2}\right) \pmod{p}. \tag{3.25}$$

Závěrem této práce Stern odvozuje některé zajímavé kongruence. Je-li $p = 4n+1$, odečtením (3.25) od dvojnásobku (3.23) obdržíme

$$\frac{2^{p-1}-1}{p} \equiv 4\left(\frac{1}{3} + \frac{1}{7} + \cdots \frac{1}{p-2}\right) \pmod{p}, \tag{3.26}$$

pokud takto upravené kongruence sečteme, máme

$$\frac{2^{p-1}-1}{p} \equiv \frac{4}{3}\left(1 + \frac{1}{5} + \cdots + \frac{1}{p-4}\right) \pmod{p}. \tag{3.27}$$

Stejným způsobem obdržíme pro $p = 4n+3$ kongruence

$$\frac{2^{p-1}-1}{p} \equiv \frac{4}{3}\left(\frac{1}{3} + \frac{1}{7} + \cdots + \frac{1}{p-4}\right) \pmod{p}, \tag{3.28}$$

respektive

$$\frac{2^{p-1}-1}{p} \equiv 4\left(1 + \frac{1}{5} + \cdots + \frac{1}{p-2}\right) \pmod{p}.$$

Přičteme-li k (3.25) dvojnásobek (3.20), obdržíme pro $p = 4n+1$

$$\frac{2^{p-1}-1}{p} \equiv 2\left(\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{p-1}\right) + 4\left(1 + \frac{1}{5} + \cdots + \frac{1}{p-4}\right) \pmod{p}. \tag{3.29}$$

Protože evidentně platí kongruence

$$\frac{2}{p-k} + 2 \equiv 0 \pmod{p}, \quad \frac{2}{p-5} + \frac{2}{5} \equiv 0 \pmod{p}, \quad \text{a.t.d.},$$

lze kongruenci (3.29) upravit na tvar

$$\frac{2^{p-1}-1}{p} \equiv 2\left(\frac{1}{p-3} + \frac{1}{p-4} + \frac{1}{p-7} + \frac{1}{p-8} + \cdots + \frac{1}{2} + 1\right) \pmod{p}. \tag{3.30}$$

Pro $p = 4n+3$ lze od dvojnásobku (3.20) odečíst (3.25) a po přerovnání členů obdržíme kongruenci

$$\frac{2^{p-1}-1}{p} \equiv 2\left(\frac{1}{p-1} + \frac{1}{p-4} + \frac{1}{p-5} + \frac{1}{p-8} + \cdots + \frac{1}{3} + \frac{1}{2}\right) \pmod{p}. \tag{3.31}$$

Protože podle (3.20) platí

$$\frac{1}{p-3}+\frac{1}{p-4}+\frac{1}{p-7}+\frac{1}{p-8}+\cdots+\frac{1}{2}+1\equiv$$
$$-\left(\frac{1}{p-1}+\frac{1}{p-2}+\cdots+\frac{1}{4}+\frac{1}{3}\right)\pmod p,$$

lze (3.30) upravit na tvar

$$\frac{2^{p-1}-1}{p}\equiv -2\left(\frac{1}{p-1}+\frac{1}{p-2}+\cdots+\frac{1}{4}+\frac{1}{3}\right)\pmod p \tag{3.32}$$

a (3.31) na tvar

(3.33)
$$\frac{2^{p-1}-1}{p}\equiv -2\left(\frac{1}{p-2}+\frac{1}{p-3}+\frac{1}{p-6}+\frac{1}{p-7}+\cdots+\frac{1}{5}+\frac{1}{4}+1\right)\pmod p.$$

Kongruenci (3.6) lze psát ve tvaru

$$\frac{2^{p-1}-1}{p}\equiv\frac{1}{2}\left(1-\frac{1}{2}+\frac{1}{3}-\cdots-\frac{1}{p-1}\right)\pmod p$$

a využitím kongruencí $1+\frac{1}{p-1}\equiv 0 \pmod p$, $\frac{1}{2}+\frac{1}{p-2}\equiv 0 \pmod p$ atd. ji lze upravit na tvar

$$\frac{2^{p-1}-1}{p}\equiv -\frac{1}{p-1}+\frac{1}{p-2}-\cdots\pm\frac{1}{\frac{p+1}{2}}\pmod p, \tag{3.34}$$

přičemž znaménko + platí pro případ $p=4n+1$ a znaménko − pro případ $p=4n+3$. Kongruence (3.30), (3.33) (3.34) jsou Sylvesterovy kongruence (3.13), (3.14) a (3.15).

3.5 Práce D. Mirimanoffa

Odlišný způsob při studiu vlastností Fermatových kvocientů zvolil Dmitrij Mirimanoff [Mi]. Vychází z Eisensteinova pojetí kvocientu $\frac{r^{p-1}-1}{p}\equiv q_r \pmod p$, kde r a p jsou nesoudělná a uplatňuje jím odvozené vzorce (např. věta 3.2).

Nechť a_0 je nejmenší kladné číslo takové, že a_0p+1 je dělitelné p. Položme $a_0p+1=r^{e_0}b_1$, b_1 je nesoudělné s r. Nechť obecně a_i je nejmenší kladné číslo splňující podmínku $a_ip+b_i\equiv 0 \pmod r$. Je tedy

$$\begin{cases} a_0p+1 &= r^{e_0}b_1,\\ a_1p+b_1 &= r^{e_1}b_2,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ a_ip+b_i &= r^{e_i}b_{i+1},\\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases} \tag{3.35}$$

Po určitém počtu kroků obdržíme

$$a_{n-1}p + b_{n-1} = r^{e_{n-1}},$$

kde $b_n = 1$, $b_{n+1} = b_1$ atd.

Vzorce (3.9) a (3.7) dávají

$$q(a_i p + b_i) \equiv q(b_i) - \frac{a_i}{b_i} \pmod{p}$$

a

$$q(r^{e_i} b_{i+1}) \equiv e_i q(r) + q(b_{i+1}) \pmod{p}.$$

Z definice čísel a_i, b_i a e_i plyne kongruence

$$q(b_i) - \frac{a_i}{b_i} \equiv e - iq(r) + q(b_{i+1}) \pmod{p}.$$

Sečteme-li tyto kongruence, obdržíme

$$-\sum_{i=0}^{n-1} \frac{a_i}{b_i} \equiv q(r) \sum_{i=0}^{n-1} e_i \pmod{p}. \tag{3.36}$$

Nechť ω patří r a označme $\frac{p-1}{\omega} = e$. Fermatův kvocient lze vyjádřit ve tvaru

$$\frac{r^\omega - 1}{p} = u_0 + u_1 r^{m_1} + u_2 r^{m_2} + \cdots + u_k r^{m_k},$$

kde koeficienty $u_i < r$ jsou kladná čísla a pro exponenty platí $m_1 < m_2 < \cdots < m_k$. Tuto rovnici upravíme na tvar

$$r^\omega = 1 + pu_0 + pu_1 r^{m_1} + \cdots + pu_k r^{m_k}. \tag{3.37}$$

Položíme

$$u_0 p + 1 = r^{m_1} b_1,$$

kde b_1 je kladné číslo nesoudělné s r a u_0 je nejmenší kladné řešení kongruence

$$xp + 1 \equiv 0 \pmod{r}.$$

Rovnici (3.37) upravíme na tvar

$$r^{\omega - m_1} = b_1 + pu_1 + pu_2 r^{m_2 - m_1} + \cdots + pu_k r^{m_k - m_1}.$$

Položíme opět

$$u_1 p + b_1 = r^{m_2 - m_1} b_2,$$

kde u_1 je nejmenší kladné řešení kongruence

$$xp + b_1 \equiv 0 \pmod{r}.$$

Stejným způsobem postupujeme dále, až dojdeme k poslední rovnici

$$u_k p + b_n = r^{\omega - m_k} \cdot 1.$$

Porovnáme-li tyto rovnice se soustavou (3.35), zřejmě platí

$$u_k = a_{n-1} \quad \text{a} \quad e_0 = m_1, \quad e_1 = m_2 - m_1, \cdots, \omega - m_k = e_{n-1},$$

takže je $\sum e_i = e$.

Kongruence (3.36) se dá upravit na tvar

$$q(r) \equiv e \sum_{i=0}^{n-1} \frac{a_i}{b_i} \pmod{p}. \tag{3.38}$$

Volba $r = 2$ dává

$$q(2) \equiv e \sum_{i=0}^{n-1} \frac{1}{b_i} \pmod{p},$$

neboť všechna a_i jsou rovna 1. Je-li r primitivní kořen podle modulu p, máme

$$q(r) \equiv \sum_{i=0}^{n-1} \frac{a_i}{b_i} \pmod{p}. \tag{3.39}$$

Uvažujme dále sumu

$$U = \sum_{\beta=1}^{p-1} q(\beta) \cdot (\beta^{2k} - (r\beta)^{2k}) = \sum_{\beta=1}^{p-1} q(\beta) \cdot \beta^{2k} - \sum_{\beta=1}^{p-1} q(\beta) \cdot (r\beta)^{2k},$$

kde k je celé číslo. Množina čísel β se rozpadá na r podmnožin, přičemž do podmnožiny označené β_i padnou všechna $\beta \equiv i \pmod{r}$, $i = 0, 1, 2, \ldots, r-1$.

Čísla $r\beta$, která jsou kongruentní s $\beta_i \pmod{p}$, jsou tvaru $\beta_i + \alpha_i p$, kde α_i je nejmenší kladné řešení kongruence $xp + i \equiv 0 \pmod{r}$.

Protože podle (3.9) platí

$$q(\frac{\beta_i + \alpha_i p}{r}) \equiv q(\beta_i) - \frac{\alpha_i}{\beta_i} - q(r) \pmod{p},$$

a koeficient β^{2k} v U je kongruentní s $\frac{\alpha_i}{\beta_i} + q(r)$, je

$$U \equiv \sum_{\beta=1}^{p-1} \frac{\alpha_i \beta^{2k}}{\beta_i} + \sum_{\beta=1}^{p-1} q(r)\beta^{2k} \pmod{p}.$$

Je-li $2k = p - 1$, první člen se anuluje $\bmod p$ a dostaneme

$$q(r) \equiv \sum_{\beta=1}^{p-1} \frac{\alpha_i}{\beta_i} \pmod{p}. \tag{3.40}$$

Položíme-li $\beta_i = p - \delta_i$ a označíme-li p' nejmenší kladný zbytek $\frac{1}{p} \pmod{r}$, je $\alpha_i \equiv p'\delta_i - 1 \pmod{r}$. Dosadíme-li do (3.39), obdržíme kongruenci

$$q(r) \equiv \sum \frac{p'\delta_i}{p - \delta_i} \pmod{p}, \tag{3.41}$$

kde jmenovatelé jsou čísla $p-1, p-2, \ldots, 2, 1$. Čitatelé tvoří v případě $p' = 1$ cyklus $1, 2, \ldots, r$ a v případě $p' > 1$ cyklus $p', 2p', \ldots, rp' \equiv r \pmod{r}$. Tato kongruence je v podstatě kongruence (3.10), kterou odvodil Sylvester.