Malá Fermatova věta

In: Karel Lepka (author): Historie Fermatových kvocientů (Fermat – Lerch). (Czech). Praha: Prometheus, 2000. pp. 14–28.

Persistent URL: http://dml.cz/dmlcz/401887

Kapitola 2

Malá Fermatova věta

Tato kapitola bude věnována jednomu z nejdůležitějších tvrzení elementární teorie čísel, které je nyní v česky psané literatuře uváděno jako Malá Fermatova věta. Nejdříve se budeme věnovat okolnostem vzniku tohoto tvrzení a důkazům, které Fermat pravděpodobně znal. V další části uvedeme některé další důkazy této věty a na závěr pojednáme o důkazu amerických fyziků. Tento důkaz je sice jen modifikací Mac Mahonova důkazu a nespadá do období, kterému je věnována tato práce, udává však zajímavou aplikaci této věty v teoretické fyzice.

2.1 Dokonalá čísla

Jeden ze svých největších objevů v teorii čísel učinil Fermat na přelomu třicátých a čtyřicátých let 17. století. V této době byly totiž v módě různé „hrátky s čísly“. Těmito problémy se zabývali mj. M. Mersenne, P. Bruslart de Saint-Martin, A. Jumeau de Sainte-Croix a B. Frenicle de Bessy. Tento pařížský matematik se rovněž věnoval teorii čísel. Byl obdařen schopností snadno počítat s velkými čísly a měl rovněž velký cit pro vlastnosti čísel. Ze všech Fermatových současníků, kteří se zabývali teorií čísel, byl Frenicle jediný, kdo se svými znalostmi mohl přiblížit Fermatově úrovni. Fermat se již během svého pobytu v Bordeaux zabýval „magickými čtverci“, což vlastně byly čtvercové matice sestavené z přirozených čísel tak, aby součet čísel v každém řádku, sloupci a úhlopříčkách byl stejný. V roce 1640 zjistil prostřednictvím Mersenna, že o problémy spojené s přirozenými čísly má zájem i Frenicle, a od této doby začala mezi nimi čilá korespondence. Právě tato korespondence nám pomohla porozumět Fermatovu stylu práce, neboť Fermat jinak své metody, alespoň co se teorie čísel týče, velice pečlivě tajil.

Fermat směřoval svůj zájem především na *dokonalá* čísla. Označíme-li $s(n)$ součet všech dělitelů čísla n s výjimkou n samotného a $S(n)$ součet všech dělitelů čísla n, potom číslo n, které splňuje podmínku $s(n) = n$, resp. $S(n) = 2n$ se nazývá *dokonalé*. [1]

Do problémů s hledáním dokonalých čísel byl vtažen kolem roku 1638 i René

[1] Nejmenší dokonalé číslo je $6 = 1 + 2 + 3$, v 17. století byla známa i další taková čísla.

Descartes, jenž odvodil rekurzívní vzorec pro součet dělitelů složených čísel ([Ma], str. 290–291):

Věta 2.1 *Nechť $N = ab$, přičemž $(a, b) = 1$. Potom*

$$s(N) = s(ab) = s(a)s(b) + as(b) + bs(a).$$

Při zkoumání dokonalých čísel je však výhodnější používat funkci $S(n)$, pro niž zřejmě platí následující tvrzení:

Věta 2.2 *Nechť $n = ab$, přičemž $(a, b) = 1$. Potom*

$$S(n) = S(ab) = S(a)S(b).$$

Nyní uvedeme a dokážeme nutnou a postačující podmínku pro to, aby sudé číslo bylo dokonalé.

Věta 2.3 *Sudé číslo n je dokonalé právě tehdy, když ho můžeme psát ve tvaru $n = 2^{k-1}(2^k - 1)$, kde $k > 1$ je přirozené číslo a $2^k - 1$ je prvočíslo.*

Abychom dokázali nutnost podmínky, předpokládejme, že číslo $n = 2^{k-1}l$, kde l je liché číslo, je dokonalé. Potom platí

$$S(n) = S(2^{k-1})S(l).$$

Využijeme-li známý vzorec pro součet geometrické posloupnosti, obdržíme

$$S(n) = (2^k - 1)S(l).$$

Jelikož n je dokonalé, platí

$$S(n) = 2n = 2^k l$$

a porovnáme-li tyto dvě rovnice, obdržíme

$$\frac{l}{S(l)} = \frac{2^k - 1}{2^k}.$$

Protože $(2^k - 1, 2^k) = 1$, je $l = (2^k - 1)q$ a $S(l) = 2^k q$, kde q je přirozené číslo. Pokud by bylo $q > 1$, číslo l by mělo přinejmenším čtyři dělitele, a sice $l, 2^k - 1, q, 1$. Potom by platilo

$$S(l) \geq l + 2^k - 1 + q + 1 = 2^k(q + 1) > 2^k q = S(l),$$

což je spor a je tedy $q = 1$, $l = 2^k - 1$ a $S(l) = 2^k$. Navíc je zřejmé, že l musí být prvočíslo, protože kdyby mělo jiné dělitele kromě jedničky a sebe sama, platilo by $S(l) > 2^k$, což je opět spor.

Nyní dokážeme dostatečnost tohoto tvrzení. Předpokládejme, že číslo n je tvaru $n = 2^{k-1}(2^k - 1)$, přičemž $2^k - 1$ je prvočíslo. Potom platí

$$S(n) = S(2^{k-1})S(2^k - 1)$$

Použijeme-li vzorec pro součet geometrické posloupnosti a vezmeme-li v úvahu, že $S(2^k - 1) = 2^k$, obdržíme $S(n) = 2n$.

Toto tvrzení, včetně důkazu dostatečnosti, uvádí už Eukleides ve svých *Základech* [Ek] (IX, 36). Euler dokázal, že každé sudé dokonalé číslo má tvar, který uvádí Eukleides [Eu1].[2] Tato věta neudává funkci, která by generovala sudá dokonalá čísla, ale redukuje tento problém na rozřešení otázky, zda číslo $M_n = 2^n - 1$ je prvočíslo nebo číslo složené. Tato čísla byla na Mersennovu počest nazvána *Mersennova čísla*. První čtyři Mersennova prvočísla (M_2, M_3, M_5, M_7) byla známa již ve starověku. Do roku 1985 bylo známo 31 Mersennových prvočísel, největší z nich s indexem 216091 objevil v roce 1985 D. Slowinski. Mersennovo prvočíslo M_{127} má 39 míst a je největší, které bylo objeveno bez použití počítače. Přehled všech dosud známých Mersennových prvočísel lze nalézt v [Ri2].[3]

Abychom si uvědomili složitost tohoto problému pro Fermatovy současníky, je třeba se zmínit o tom, že Mersenne se ptal Saint-Martina, jak najít počet všech dělitelů čísla 49000 a jejich součet, aniž bychom je vypočítávali jeden po druhém. V tomto ohledu má velký význam algebraická notace, kterou už Fermat a Descartes měli k dispozici. V roce 1640 se Frenicle otázal Fermata prostřednictvím Mersenna, zda existuje dokonalé číslo mezi 10^{20} a 10^{22}. Tato otázka se samozřejmě týkala sudých dokonalých čísel. Nerovnice

$$10^{20} < 2^{n-1}(2^n - 1) < 10^{22}$$

má řešení $34 \leq n \leq 37$. Pro nás je velmi zajímavé, jak Fermat při řešení tohoto problému postupoval. Jak oznámil v červnu roku 1640 Mersennovi, jeho metoda byla založena na následujících třech předpokladech:

(I) Je-li n složené, je i $2^n - 1$ složené

(II) Je-li n prvočíslo, potom $2^n - 2$ je násobek $2n$.

(III) Je-li n prvočíslo a p je prvočíselný dělitel $2^n - 1$, potom $p - 1$ je násobek n.

Podmínka (I) je důsledek obecné identity

$$x^{ab} - 1 = (x^a - 1)(x^{a(b-1)} + x^{a(b-2)} + \cdots + 1) \tag{2.1}$$

[2] Existence lichých dokonalých čísel nebyla dosud ani potvrzena, ani vyvrácena.

[3] Devadesátá léta jsou ve znamení nástupu výkonných počítačů při zkoumání velkých čísel. Pro studium Mersennových čísel byl realizován projekt G I M P S, neboli The Great Internet Mersenne prime Search. Vedoucí tohoto projektu Georege Woltmann sestavil velmi efektivní program, který Scott Kurowski se svými spolupracovníky přizpůsobil pro Internet, takže se do tohoto projektu mohlo zapojit několik tisíc lidí. V síti Internet se objevila zpráva, že bylo objeveno již 36. dokonalé číslo, které má tvar $2^{2976220} \cdot (2^{2976221} - 1)$ a které má 1 791 864 míst. Toto číslo objevil Gordon Spence; David Slowinski ukončil ověření 29. 8. 1997. Další, v pořadí již 37. dokonalé číslo je tvaru $2^{3021376} \cdot (2^{3021377} - 1)$ a objevil je devatenáctiletý student California State University v Dominguez Hills. Toto číslo má 1 819 050 míst; ověření ukončil David Slowinski 30. 1. 1998. Informace lze získat na následujících adresách: http://www.utm.edu/research/primes/notes/2976221 resp. 3021377 nebo http://www.mersenne.org/prime.htm.

pro případ $x = 2$. Skutečnost, že to Fermat uvádí jako objev svědčí o tom, že jeho znalosti algebry nebyly v té době příliš velké. Podmínky (II) a (III) jsou ovšem typické případy toho, co se dnes označuje jako *Malá Fermatova věta.* Tato tvrzení uvádí Fermat bez důkazu. V dopise Freniclovi z 18. října 1640, v němž Fermat píše o „la propositon fondamentale de parties aliquotes" neboli o základní větě o dělitelích, Fermat poodhalil i způsob, kterým ke svým závěrům přišel: *Jeli dáno libovolné prvočíslo p a libovolná geometrická posloupnost $1, a, a^2$, etc., p musí dělit některé číslo $a^n - 1$, pro něž n dělí $p-1$; jestliže potom N je libovolný násobek nejmenšího n pro něž toto platí, p dělí také $a^N - 1$. Toto tvrzení platí pro všechny řady a všechna prvočísla. Poslal bych Vám jeho důkaz, obávám se však, že je příliš dlouhý.*

Na závěr této části si dovolíme ještě menší odbočku. Jak uvádí L. E. Dickson v [Di] (Vol. I, str. 59), je možné, že tuto poučku znali již staří Číňané v 5. stol. př. Kr. pro $n = 2$ [Di]. Jiní historikové, ([Ri2], str.86), s tím však nesouhlasí a poukazují zejména na skutečnost, že staří Číňané neznali pojem prvočísla. Tato tzv. „čínská věta" bývá často uváděna jako test na prvočíselnost, tedy n je prvočíslo, pokud $n|2^n - 2$; jedná se tedy o konverzi Malé Fermatovy věty, ta však není správná jak ukázal Sarrus protipříkladem $341 = 11 \cdot 31|2^{341} - 2$. Podle jedné verze se tato chyba poprvé objevila v článku J. H. Jeanse v časopise *Messenger of Mathematics* (vol. 27, 1897–98) a vznikla nepřesným překladem starého čínského textu *Devět knih matematického umění.* Tuto chybu poté převzal Dickson a další matematikové.

Se zajímavou hypotézou přišel ve své doktorské práci Han Qi z *Institutu historie přírodních věd Čínské Akademie* v Pekingu. Podle jeho verze k této chybě došlo přenesením znalostí západní matematiky do čínských textů v 18. století a jejich vlivů na rozvoj čínské matematiky. Čínský matematik Li Shanlan (1811–1882) věřil, že obdržel kritérium pro testování prvočíselnosti ($n|2^n - 2$) a tuto skutečnost sdělil svému spolupracovníku v překládání západních textů anglickému misionáři Alexanderu Wyliemu kolem roku 1869 v Šanghaji. Wylie, který nebyl příliš dobrý matematik, tuto tezi pochopil jako významný objev a publikoval ji v časopise *Notes and Queries on Chine and Japan* v roce 1869 pod názvem „Čínský teorém". V následujících číslech tohoto časopisu někteří čtenáři poukázali na chybnost tohoto tvrzení. Li si uvědomil, že se dopustil omylu, a na tuto skutečnost upozornil v jednom ze svých článků o teorii čísel v roce 1872. Jeho mladší kolega a spolupracovník Hua Hengtang si tuto chybu neuvědomil a toto „kritérium" uvedl ve své knize o teorii čísel z roku 1882, přičemž autorství připsal Liovi. Souvislost mezi těmito publikacemi a článkem J. H. Jeanse není zřejmá. [4]

2.2 První důkazy Malé Fermatovy věty

V dnešní době existuje řada důkazů této věty, v této části se však soustředíme na dva, které Fermat zřejmě znal nebo alespoň mohl znát. V dnešní době se tato

[4] Tuto zajímavou hypotézu publikoval Man-Keung Siu z katedry matematiky Univerzity v Hongkongu v rámci konference o historii matematiky v síti Internet v červnu 1997 . Pro krátkost času a poměrnou nedostupnost písemných materiálů se ji autorovi nepodařilo ověřit jiným způsobem.

věta obvykle uvádí v následujícím znění:

Věta 2.4 *Nechť p je prvočíslo, a celé číslo. Pak platí*

$$a^p \equiv a \pmod{p}. \tag{2.2}$$

Je-li navíc splněna podmínka $p \nmid a$, pak platí

$$a^{p-1} \equiv 1 \pmod{p}. \tag{2.3}$$

Vezmeme-li v úvahu formulaci (2.2), lze provést tzv. *aditivní důkaz*. Použijeme binomickou větu

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-1}xy^{p-1} + y^p.$$

Položíme-li $x = y = 1$ a vezmeme-li v úvahu, že pro prvočíselné p jsou všechny binomické koeficienty s výjimkou $\binom{p}{0}$ a $\binom{p}{p}$ násobky p, obdržíme

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

Nyní můžeme předpokládat, že existuje alespoň jedno číslo a, které splňuje podmínku

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

Použijeme-li opět binomickou větu s volbou $x = a, y = 1$, obdržíme

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1.$$

Přejdeme-li ke kongruenci a vezmeme-li do úvahy indukční předpoklad, obdržíme

$$(a+1)^p \equiv a + 1 \pmod{p}.$$

Vzhledem k tomu, co Fermat bezpečně znal o binomických koeficientech již v roce 1636, lze předpokládat, že tento důkaz, přinejmenším pro případ $a = 2$, který je pro hledání dokonalých čísel rozhodující, znal. Tento důkaz však nesouvisí s problémy dělitelnosti a navíc z Fermatovy korespondence plyne, že se jeho úvahy ubíraly poněkud jiným směrem. Fermat si zřejmě všimnul, že dělíme-li členy posloupnosti $1, a, a^2, \ldots$ prvočíslem p, zbytky se opakují. Je totiž možných nejvýše $p-1$ zbytků, existují tedy nejméně dva exponenty, řekněme n a $n+m$, které při dělení čísel a^n a a^{m+n} prvočíslem p dávají týž zbytek. Platí tedy

$$a^{m+n} - a^n \equiv 0 \pmod{p}.$$

S ohledem na předpoklad $p \nmid a$ dostáváme

$$a^m \equiv 1 \pmod{p},$$

tedy číslo 1 je vždy členem posloupnosti zbytků. Nechť d je nejmenší exponent, který při dělení čísla a^d číslem p dává zbytek 1. Potom i při dělení čísla a^{kd} číslem p dostaneme zbytek 1, neboť výraz

$$a^{kd} - 1 = (a^d - 1)(a^{(k-1)d} + \cdots + a^d + 1)$$

je dělitelný p. Naopak jedinými mocniteli čísla a, které při dělení číslem p dávají zbytek 1, jsou násobky d. Nechť číslo m, které napíšeme ve tvaru

$$m = qd + r, \quad q \geq 0, \quad 0 \leq r < d$$

dá při dělení p rovněž zbytek 1. Jelikož čísla $a^m = a^{qd}a^r$ a a^{qd} dávají zbytek 1, musí být jejich rozdíl $a^{qd}(a^r - 1)$ dělitelný p. Protože $p \nmid a^{qd}$, musí platit $p|a^r - 1$, což je však spor s definicí čísla d s výjimkou $r = 0$, tedy m je násobkem d. Navíc čísla a^{n+m} a a^n dávají týž zbytek pouze v případě, že a^m dává zbytek 1. Jinými slovy při dělení čísel a^n prvočíslem p dostaneme d zbytků, které se cyklicky opakují. Pokud $d = p - 1$, potom samozřejmě platí $d|p - 1$. V opačném případě existuje alespoň jedno číslo k, které není členem posloupnosti zbytků. Uvažujme množinu zbytků, které obdržíme při dělení čísel $k, ka, ka^2, \ldots$ prvočíslem p. Tato množina má opět d prvků, neboť čísla ka^{m+n} a ka^n dají týž zbytek tehdy a jen tehdy, když $p|ka^n(a^m - 1)$ a to platí pouze v případě $d|m$. Kromě toho platí, že žádný prvek této množiny není prvkem množiny původní, což snadno dokážeme sporem. Předpokládejme, že a^n a ka^m dávají týž zbytek. Potom stejnou vlastnost mají i čísla a^{n+1} a ka^{m+1}, neboť $a^n - a^m k$ je dělitelné p právě tehdy, když $a(a^n - a^m k)$ je dělitelné p. Tak postupujeme dál, až narazíme na případ, kdy $d|m + j$. Potom ovšem čísla a^n a k dávají týž zbytek, což je spor s definicí čísla k. Pokud jsme nevyčerpali všechny možné zbytky, volíme k', které nepatří do žádné z výše uvedených množin a postupujeme stejným způsobem, dokud nevyčerpáme všechny možné zbytky. Musí tedy platit $d|p - 1$, což jsme chtěli dokázat.

Na tyto úvahy se můžeme podívat i z hlediska moderní algebry. Je-li a nesoudělné s p, potom zbytky po dělení čísel a^n číslem p tvoří uzavřenou množinu vzhledem k násobení a tato množina je podmnožinou množiny všech možných zbytků, které vzniknou při dělení přirozených čísel nesoudělných s číslem p. Ale množina všech možných zbytků tvoří multiplikativní grupu, jejíž řád je $p - 1$. Podle Lagrangeovy věty je řád každé konečné multiplikativní grupy násobkem řádu libovolné podgrupy, tedy platí $d|p - 1$.

Je-li $a = 2$, potom Malá Fermatova věta dává důležitý důsledek, který urychlí faktorizaci Mersennových čísel:

Věta 2.5 *Nechť p je liché prvočíslo. Potom každý dělitel čísla $2^p - 1$ je tvaru $2kp + 1$, přičemž k je celé číslo.*

Protože součin dvou či více čísel tvaru $2kp + 1$ je opět tohoto tvaru a jedničku obdržíme volbou $k = 0$, stačí dokázat, že každý prvočíselný dělitel čísla $2^p - 1$ je tohoto tvaru. Nechť $q|2^p - 1$. Potom platí $2^p \equiv 1 \pmod{q}$ a $p|q - 1$. Je tedy $q - 1 = k'p$, kde k' je přirozené číslo. Jelikož q je dělitel lichého čísla, je liché a $q - 1$ je sudé a $2|k'n$. Protože p je liché, je k' sudé a $k' = 2k$. Prvočíselní dělitelé čísel $2^p - 1$ jsou tudíž tvaru $q = 2kp + 1$.

Fermat tento důsledek znal, jak vyplývá z jeho doisu Freniclovi, a nebylo pro něho problém faktorizovat číslo $2^{37} - 1$. Pokud existuje prvočíselný dělitel p, potom 37 musí dělit $p - 1$. Jelikož p je liché, musíme je hledat mezi prvočísly tvaru $74n + 1$; první kandidát 149 nevyhovuje, druhý 223 ale ano. Fermat se však zde nezastavil. Pokud faktorizujeme čísla $a^n - 1$, lze faktorizovat i čísla $a^m + 1$

pro $m = 2n$. Fermat se ptal, zda pro libovolné a a libovolné prvočíslo p existuje vždy takové m, že $p|a^m + 1$. Odpověď je ovšem záporná a Fermat má pro to i zdůvodnění. Tehdy a jen tehdy, je-li nejmenší n, pro něž p dělí $a^n - 1$ liché, existuje m takové, že p dělí $a^m + 1$. Nejmenší takové m je $\frac{n}{2}$.

Fermat se také zabýval otázkou, kdy je $2^m + 1$ prvočíslo. Toto nemůže nastat, jestliže m má lichého dělitele $d > 1$. Platí-li totiž $m = ed$ a položíme-li $N = 2^e$, potom $2^m + 1 = N^d + 1$ a toto číslo je dělitelné $N + 1$. K důkazu stačí použít známé identity, která platí pro lichá čísla k:

$$x^k + 1 = (x + 1)(x^{k-1} - x^{k-2} + \cdots + 1).$$

V případě, že m nemá lichého dělitele, je $m = 2^n$ a pro $n = 0, 1, 2, 3, 4$ je číslo $2^m + 1$ prvočíslo. V dopise Freniclovi z roku 1640 Fermat vypočítal všechna tato čísla až po $n = 6$ a odhadoval, že se jedná o prvočísla. Čísla tvaru $F_n = 2^{2^n} + 1$ se nazývají *Fermatova čísla.*[5] Fermat znal způsob, jak urychlit faktorizaci těchto čísel. Platí totiž následující věta:

Věta 2.6 *Nechť n je přirozené číslo a p je liché prvočíslo pro něž platí $p|2^{2^n} + 1$. Potom $p = 2^{n+1}k + 1$, kde k je přirozené číslo.*

Podle předpokladu $p \mid (2^{2^n} + 1)(2^{2^n} - 1) = 2^{2^{n+1}} - 1$, přičemž $p \nmid 2^{2^n} - 1)$, neboť by došlo ke sporu s předpokladem $(2, p) = 1$. Označme d nejmenší exponent, pro nějž platí $2^d \equiv 1 \pmod{p}$. Protože platí $p \mid 2^{2^{n+1}}$, máme $d \mid 2^{n+1}$. Poněvadž na druhé straně $d \nmid 2^n$, jelikož $p \nmid 2^{2^n} - 1$, máme $d = 2^{n+1}$. Podle Malé Fermatovy věty platí $p \mid 2^{p-1} - 1$, platí i $2^{n+1} \mid p - 1$ a odtud $p = 2^{n+1}k + 1$.

Nechce se až věřit, že se Fermatovi nepodařilo faktorizovat alespoň číslo F_5. Podle jím objevené metody mezi možné dělitele tohoto čísla připadají pouze prvočísla tvaru $64n + 1$, z nichž 641 toto číslo skutečně dělí, jak později dokázal Euler. Ani Frenicle se nepokusil toto číslo rozložit, přestože Fermat v dopise vyslovil přání, aby tak učinil; naopak s tímto Fermatovým závěrem vyslovil souhlas. Fermat až do konce života věřil, že tento jeho závěr je správný, ačkoliv obvykle udával, že pro to nemá důkaz. Můžeme si představit, že když poprvé formuloval svůj závěr, byl jím tak unesen, že si nevšiml numerické chyby a své výpočty si nepřekontroloval. Číslo $2^{64} + 1$, které má dělitele 274177 bylo za hranicemi Fermatových možností a zřejmě i Freniclových, přestože tento byl vytrvalejší a lepší počtář.

Dejme však slovo Fermatovi, který ve svém listu Freniclovi z roku 1640 praví: *„1. Nechť je dána například posloupnost 2,4,8,16,32,64,128,256 atd. Říkám, že když zvětšíte čísla této posloupnosti o jedničku, takže dostanete 3,5,9,17 atd; všechna řečená kladná čísla, která budou mít exponent, jenž není členem této posloupnosti a zvětšená o jedničku budou složená.*

2. Ačkoliv je možné udělat podrobný rozbor, který je příliš dlouhý, pro pochopení stačí následující příklad, který uvedu. Nechť je například číslo z dané posloupnosti zvětšené o jedničku rovno 8193, exponent je prvočíslo 13. Říkám, že

[5] Fermatova čísla mají zajímavou souvislost s konstrukcí pravidelných $n-$úhelníků. Jak dokázal Gauss, pravidelný $n-$úhelník lze sestrojit pouze pomocí kružítka a pravítka právě tehdy, když $n = 2^k \cdot p_1 \cdots p_l$, kde $k \geq 0$ a p_i jsou navzájem různá Fermatova prvočísla.

když dělíte 8193 třemi, podíl bude dělitelný pouze číslem, které je buďto dvojnásobkem exponentu 13 zvětšeného o jednu nebo násobkem tohoto dvojnásobku 13 etc. až do nekonečna. Říkám, že když je exponent složené číslo, ale ne mocnina dvojky, mohu velmi snadno najít všechny jeho dělitele.

3. Ale zde je něco, co je nejpodivuhodnější. Jsem téměř přesvědčen, že všechna čísla z této posloupnosti zvětšená o jedničku, jejichž exponenty jsou čísla z posloupnosti mocnin dvojky, jsou prvočísla, jako 3,5,17, 257, 65537, 4 294 967297 a následující dvacetimístné 18 446 744 073 709 551 617 atd. Nemám přesný důkaz, ale vyloučil jsem tak velké množství dělitelů přesným důkazem a vyznám se v této problematice natolik dobře, že toto své tvrzení nemohu vzít zpět."

Fermatova čísla jsou zajímavou ukázkou toho, jak podivuhodné a nevyzpytatelné jsou vlastnosti přirozených čísel. Zejména v posledních letech, kdy byly vyvinuty moderní metody, které umožňují faktorizovat velká čísla za pomoci výkonných počítačů, se podařilo buď faktorizovat či alespoň nalézt některého dělitele řady Fermatových čísel. Nepodařilo se však nalézt žádné další prvočíslo, takže je možné, že zbývající Fermatova čísla jsou složená, ačkoliv důkaz pro toto tvrzení není. Některá složená Fermatova čísla jsou uvedena v příloze na konci této práce.

2.3 Přínos L. Eulera

Fermat se těmito problémy ve čtyřicátých letech přestal zabývat a už se k nim ani později nevrátil. V osmdesátých letech 17. století Malou Fermatovu větu dokázal Wilhelm Leibniz, tento důkaz však nebyl během jeho života publikován a byl objeven až v jeho pozůstalosti ([Di], str. 59). Leibniz využil formuli

$$(1+1+\cdots+1)^p = 1+1+\cdots+1+\sum_{q+r+\cdots+s=p} \frac{p!}{q!r!\ldots s!}.$$

Poněvadž všechny sčítance v sumě jsou násobky p, je a^p násobkem a.

Euler se ve třicátých letech 18. století začal zabývat nejprve problémem Fermatových čísel, později dospěl k mnoha závažným číselně teoretickým objevům. O tom, jak hluboce Fermatovo dílo z teorie čísel upadlo v zapomění, svědčí skutečnost, že Euler považoval Malou Fermatovu větu za svůj objev, teprve později přiznal Fermatovo prvenství. Tato skutečnost je o to zajímavější, že *Varia Opera* byla v té době k dispozici.

Euler se poprvé zabýval Malou Fermatovou větou v roce 1731. Později se k tomuto problému znovu vrátil v souvislosti s vyšetřováním multiplikativní grupy modulo p, kdy mluví o vynikajícím teorému objeveném Fermatem. Začal s objevem, že $2^{p-1}-1$ je násobkem p, pokud p je prvočíslo, nazýval to „theorema non inelegans". Dále objevil, že $a^{p-1}-b^{p-1}$ je násobek p, pokud a, b jsou s p nesoudělná. V téže době rovněž faktorizoval páté Fermatovo číslo a vyvrátil tak Fermatův předpoklad, že se jedná o prvočísla. Do června 1735 byl Euler mlhavě zpraven přinejmenším o Fermatově dopisu Mersennovi z roku 1640, neboť ve svém dopise Ehlerovi v Dantzigu píše: *Věta...není nová, pokud se nemýlím byla*

formulována Fermatem, ale bez důkazu, jelikož byla odvozena pouze indukcí. Euler dále udává poněkud těžkopádný důkaz, který je založen na aplikaci binomické formule $(1+1)^{p-1}$ a vhodného uspořádání členů. Tento důkaz opakuje znovu v roce 1736, ale přidává k němu aditivní důkaz této věty založený na binomické formuli pro $(a+1)^p$ [Eu2].

V roce 1747, ačkoliv stále lpěl na aditivním důkazu, poukazuje na to, že při zkoumání dělitelnosti číslem p (p nemusí být prvočíslo) mohou být přirozená čísla a, b nahrazena čísly $a \pm \alpha p$, $b \pm \beta p$, tedy jinými čísly, které však po dělení číslem p dávají týž zbytek. Zkoumá zbytky po dělení druhými a třetími mocninami a začíná se zabývat vlastnostmi zbytků, které vzniknou z Fermatovy věty. Konkrétně našel tvrzení, že když $a - f^n$ je dělitelné prvočíslem $p = mn+1$, potom je tímto prvočíslem dělitelné i číslo $a^m - 1$, což je bezprostřední důsledek Fermatovy věty. Dále dokázal i opačné tvrzení.

Počátkem 60. let publikoval multiplikativní důkaz v práci [Eu3], který vzápětí rozšířil i na případ složeného modulu, viz [Eu4]:

Věta 2.7 *Nechť a je celé číslo, m je přirozené číslo, přičemž platí $(a,m) = 1$ a $\varphi(m)$ je počet všech přirozených čísel nesoudělných s m a nepřevyšujících m. Potom platí*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{2.4}$$

Funkce $\varphi(m)$ se dnes nazývá *Eulerova funkce* a její hodnotu lze určit pomocí následující věty:

Věta 2.8 *Nechť $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Potom platí*

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Je-li m prvočíslo, potom je $\varphi(m) = m - 1$ a Eulerova věta přechází v Malou Fermatovu větu. Euler rovněž poznamenává, že $\varphi(m)$ není obecně nejmenší exponent n takový, že m dělí $a^n - 1$ pro všechna a nesoudělná s m. Nejmenší exponent d, pro nějž platí $a^d \equiv 1 \pmod{m}$, je roven nejmenšímu společnému násobku čísel $p_i^{\alpha_i} - p_i^{\alpha_i - 1}$, kde $1 \le i \le k$. Dnešní terminologií říkáme, že a patří d modulo m. Zvláštní význam mají čísla patřící $\pmod{p}$ k mocniteli $p-1$. Nazývají se *primitivní kořeny* $\pmod{p}$ a je jich $\varphi(p-1)$ mezi sebou nekongruentních. Je-li g libovolný primitivní kořen $\pmod{p}$, jsou čísla $g^0, g^1, g^2, \ldots, g^{p-2}$ spolu nekongruentní $\pmod{p}$ a tvoří tudíž redukovanou soustavu zbytků podle modulu p.

2.4 Lagrangeův důkaz

Francouzský matematik Joseph L. Lagrange volil zcela jiný přístup k této problematice. Jeho důkaz je publikován v [La] a uvádíme ho proto, že jako první dal do souvislosti Fermatovu a Wilsonovu větu. Jak bude pojednáno ve čtvrté kapitole, podobnou problematikou se zabýval i M. Lerch. Wilsonovu větu můžeme formulovat následujícím způsobem:

Věta 2.9 *(Wilson) Nechť p je prvočíslo. Potom platí*

$$(p-1)! \equiv -1 \pmod{p}. \tag{2.5}$$

Lagrange vycházel z rovnice

$$(x+1)(x+2)\cdots(x+p-1) = x^{p-1} + A_1 x^{p-2} + A_2 x^{p-3} + \cdots + A_{p-2}x + A_{p-1}, \tag{2.6}$$

kde

$$\begin{aligned} A_1 &= 1+2+3+\cdots+(p-1), \\ A_2 &= 1\cdot 2 + 1\cdot 3 + \cdots + 2\cdot 3 + \cdots + (p-2)(p-1), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ A_{p-1} &= 1\cdot 2\cdot 3\cdots(p-1). \end{aligned} \tag{2.7}$$

Dosadíme-li do (2.6) $x+1$ místo x, obdržíme

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

Vynásobíme-li obě strany této rovnice výrazem $x+1$ a dosadíme-li do pravé strany z (2.6), dostaneme

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

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

$$\begin{aligned} A_1 &= \tbinom{p}{2}, \\ 2A_2 &= \tbinom{p}{3} + \tbinom{p-1}{2} A_1, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ (p-1)A_{p-1} &= 1 + A_1 + A_2 + \cdots + A_{p-3} + A_{p-2}. \end{aligned} \tag{2.8}$$

Jelikož p je prvočíslo, jsou koeficienty $A_1, A_2, \ldots, A_{p-2}$ dělitelné p a platí

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

Roznásobíme-li levou stranu této kongruence a vezmeme-li v potaz, že podle (2.7) je $A_{p-1} = (p-1)!$, obdržíme

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

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

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

Současně je pro libovolné x splňující podmínku $p \nmid x$ jeden z činitelů na levé straně násobkem p a tedy platí

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

2.5 Kombinatorické důkazy

V roce 1892 publikoval Mac Mahon článek [Mh], ve kterém se zabýval permutacemi prvků v lineárním a cyklickém procesu. Mac Mahon navazuje na práce [Ja] a [Lu]; vzorce odvozené v těchto pracech mají zajímavé důsledky i pro teorii čísel.

Nechť α je počet prvků prvního druhu, β počet prvků druhého druhu, γ počet prvků třetího druhu, atd. Celkový počet prvků nechť je n, tedy platí

$$\alpha + \beta + \gamma + \cdots = n.$$

Označme N největší společný dělitel čísel α, β, γ atd. Platí

$$N = \frac{\alpha}{\alpha'} = \frac{\beta}{\beta'} = \frac{\gamma}{\gamma'} = \cdots .$$

Dále označme $LP(\alpha, \beta, \gamma, \dots)$ počet permutací procesu a $CP(\alpha, \beta, \gamma, \dots)$ počet cyklických permutací. Platí

$$LP(\alpha, \beta, \gamma, \dots) = \frac{n!}{\alpha!\beta!\gamma!\dots}. \tag{2.9}$$

Je-li d libovolný přirozený dělitel čísla N, je

$$nCP(N\alpha', N\beta', N\gamma', \dots) = \sum_{d|N} \varphi(d) LP\left(\frac{N}{d}\alpha', \frac{N}{d}\beta', \frac{N}{d}\gamma', \cdots\right), \tag{2.10}$$

nebo-li

$$nCP(N\alpha', N\beta', N\gamma', \dots) = \sum_{d|N} \varphi(d) \frac{\left(\frac{n}{d}\right)!}{\left(\frac{N}{d}\alpha'\right)!\left(\frac{N}{d}\beta'\right)!\left(\frac{N}{d}\gamma'\right)!\dots}. \tag{2.11}$$

Je-li n prvočíslo, potom je $N = 1$ a

$$nCP(\alpha, \beta, \gamma, \dots) = \frac{n!}{\alpha!\beta!\gamma!\dots}.$$

Ke stejnému výsledku dojdeme i v případě, že čísla α, β, γ,... nemají kromě jedničky žádného společného dělitele. Platí tedy následující tvrzení:

Věta 2.10 *Nechť podíl* $\frac{n!}{\alpha!\beta!\gamma!\dots}$ *je dělitelný* n. *Potom* $(\alpha, \beta, \gamma, \dots) = 1$.

Předpokládejme dále, že $N = n = \alpha = N\alpha'$. Potom je

$$nCP(n) = \sum_{d|n} \varphi(d)$$

a protože je zřejmě $CP(n) = 1$, platí následující tvrzení:

Věta 2.11 *Nechť d jsou všichni dělitelé čísla n včetně jedničky a n samého. Potom platí*

$$\sum_{d|n} \varphi(d) = n.$$

Toto tvrzení jako první dokázal Gauss [Ga], který rovněž zavedl symbol $\varphi(n)$.

Zkoumejme dále variace $n-$té třídy z r prvků s opakováním, které označíme $RLP(r,n)$; počet cyklických variací nechť je $RCP(r,n)$. Hodnota $RLP(r,n)$ je rovna r^n. V cyklických variacích uvažujme a_1 prvků prvního druhu, a_2 prvků druhého druhu atd., tuto variaci označíme $(a_1, a_2, \ldots, a_r)$, přičemž $a_1 + a_2 + \cdots + a_r = n$.

Protože musíme uvažovat shodnost některých objektů, je lépe pracovat s obecným typem $(a_1^{k_1}, a_2^{k_2}, a_3^{k_3} \ldots)$, kde $k_1 + k_2 + \cdots = r$ a $k_1 a_1 + k_2 a_2 + \cdots = n$. Potom platí

$$RCP(r,n) = \sum \frac{r!}{k_1! k_2! k_3! \cdots} CP(a_1^{k_1}, a_2^{k_2}, a_3^{k_3} \ldots).$$

Využitím vzorce (2.10) obdržíme

$$nCP(a_1^{k_1}, a_2^{k_2}, a_3^{k_3}, \ldots) = \sum \varphi(d) LP \left\{ \left(\frac{a_1}{d}\right)^{k_1} \left(\frac{a_2}{d}\right)^{k_2} \left(\frac{a_3}{d}\right)^{k_3} \cdots \right\},$$

kde d je největší společný dělitel čísel a_i.

Nyní můžeme vyjádřit $RCP(r,n)$ jako lineární funkci LP. Koeficient u $\frac{1}{n}\varphi(d)$ je

$$\sum \frac{r!}{k_1! k_2! k_3! \cdots} LP \left\{ \left(\frac{a_1}{d}\right)^{k_1} \left(\frac{a_2}{d}\right)^{k_2} \left(\frac{a_3}{d}\right)^{k_3} \cdots \right\},$$

a toto je zjevně rovno $RLP(r, \frac{n}{d})$. Odsud

$$RCP(p,n) = \frac{1}{n} \sum \varphi(d) RLP(r, \frac{n}{d}),$$

neboli

$$RCP(p,n) = \frac{1}{n} \sum \varphi(d) r^{\frac{n}{d}},$$

kde sumace probíhá přes všechny dělitele čísla n. Platí tedy věta:

Věta 2.12 *Počet cyklických permutací $n-$té třídy z r prvků s opakováním je*

$$\frac{1}{n} \sum_{d|n} \varphi(d) r^{\frac{n}{d}}.$$

Jelikož počet cyklických permutací je vždy celé číslo, důsledkem této věty je následující tvrzení:

Věta 2.13 *Nechť r a n jsou kladná celá čísla. Potom je*

$$\sum_{d|n} \varphi(d) r^{\frac{n}{d}} \equiv 0 \pmod{n}.$$

Je-li $n = p$ prvočíslo a $r = a$ kladné celé číslo nesoudělné s p, je podle věty 2.12

$$a^p + (p-1)a \equiv 0 \pmod{p}$$

a po vydělení této kongruence číslem a obdržíme

$$a^{p-1} - 1 \equiv 0 \pmod{p},$$

což je Malá Fermatova věta. Navíc podíl

$$q(a) = \frac{a^{p-1} - 1}{p} \tag{2.12}$$

je celé číslo, které nyní nazýváme *Fermatův kvocient*. MacMahon uvádí vztah mezi Fermatovým kvocientem a počtem cyklických permutací

$$q(a) = \frac{1}{a} RCP(a,p) - 1. \tag{2.13}$$

Američtí teoretičtí fyzikové Gutfreund a Little publikovali v roce 1981 důkaz Malé Fermatovy věty, který je modifikací MacMahonova důkazu [GL]. Inspirací jim byl *Isingův spin*, který má možných $a = 2j + 1$ projekcí $(-j, -j+1, \ldots, j)$. Pro zjednodušení matematických úvah posuneme hodnoty projekcí o j, tedy platí $0 \leq s \leq a-1$. Nechť p je liché prvočíslo, a je celé číslo, které vyhovuje podmínkám $(a,p) = 1$ a $2 \leq a \leq p$. Uspořádanou p-tici projekcí

$$\sigma = (s_1, \ldots, s_p), \qquad 0 \leq s_i \leq a-1, \quad 1 \leq i \leq p.$$

nazveme *konfigurací*, množinu všech konfigurací označíme S. Definujme zobrazení $T : S \to S$ následujícím způsobem:

$$T(\sigma) = \sigma' = (s'_1, \ldots, s'_p),$$

kde

$$s'_i \equiv s_j + 1 \pmod{a}, \quad j \equiv i - 1 \pmod{p}, \quad 1 \leq j \leq p$$

pro všechna $1 \leq i \leq p$. Toto zobrazení nazveme *operátor translace*. Snadno se vidí, že operátor translace je bijekce. Pro tento operátor platí následující vlastnost:

Věta 2.14 *Nechť r je přirozené číslo, $T^r(\sigma) = \sigma^{(r)} = (s_1^{(r)}, \ldots, s_p^{(r)}) \in S$. Pak pro každé $1 \leq i \leq p$ platí*

$$s_i^{(r)} \equiv s_j + r \pmod{a},$$

kde $j \equiv i - r \pmod{p}, 1 \leq j \leq p$.

Podmnožinu C množiny S tvaru

$$C = \{\sigma, T(\sigma), T^2(\sigma), \ldots, T^{n-1}(\sigma)\}$$

nazveme *cyklem*, jestliže pro $n \in \mathbb{N}$ platí $T^n(\sigma) = \sigma$ a pro všechna $m \in \mathbb{N}, m < n$ platí $T^m(\sigma) \neq \sigma$. Číslo n se nazývá *délka cyklu*.

Mezi všemi cykly existuje jeden speciální, který nazveme *triviální* a který můžeme definovat následujícím způsobem: Nechť

$$\overline{S} = \{\sigma = (s_1, \ldots, s_p) \in S : s_1 = s_2 = \cdots = s_p\}$$

. Zřejmě platí, že délka triviálního cyklu je rovna a.

Věta 2.15 *Nechť* $\sigma \in \overline{S}, \sigma = (s_1, \ldots, s_p), T_a(\sigma) = \sigma' = (s'_1, \ldots, s'_p)$. *Podle (1) pro každé* i, $1 \leq i \leq p$ *platí*

$$s'_i \equiv s_j + a \pmod{a}, \quad j \equiv i - a \pmod{p}, \quad 1 \leq j \leq p.$$

Tudíž $s'_i = s_j = s_i$. *Naopak nechť pro* $1 \leq n \leq ap - 1, \sigma \in S$ *platí* $T^n(\sigma) = \sigma$. *Potom* $n = ka (1 \leq k \leq p-1)$ *a* $\sigma \in \overline{S}$.

Abychom dokázali toto tvrzení, předpokládejme, že $\sigma' = (s'_1, \ldots, s'_p)$, $\sigma' = T^{np}(\sigma) = \sigma$. Pak pro $1 \leq i \leq p$ je podle věty 2.13

$$s_i = s'_i \equiv s_j + np \pmod{a}, \quad j \equiv i - np \pmod{p}, \quad 1 \leq j \leq p.$$

Tudíž pro $j = i$ je $s - i \equiv s_i + np \pmod{a}$ a tedy $n = ka$ pro $1 \leq k \leq p-1$. Předpokládejme, že $1 \leq i, j \leq p, i \neq j, s_i \neq s_j$. Pak existuje přirozené číslo h takové, že $j \equiv i - hka \pmod{p}$, neboť $p \nmid ka$. Pak $\sigma = T^{nk}(\sigma)$, tudíž

$$s_i \equiv s_j + nk \pmod{a}.$$

Jelikož $a|n$, je $s_i \equiv s_j \pmod{a}$ a z toho plyne $s_i = s_j$.

Snadno se dokáže, že platí

$$T^{ap}(\sigma) = \sigma$$

pro každé $\sigma \in S$, jinými slovy délka cyklu je dělitelná ap.

Je-li $\sigma = (s_1, \ldots, s_p) \in S, T^{ap}(\sigma) = \sigma' = (s'_1, \ldots, s'_p) \in S$, pak podle (1) je pro každé i, $1 \leq i \leq p$:

$$s'_i \equiv s_j + ap \pmod{a}, \quad j \equiv i - ap \pmod{p}, \quad 1 \leq j \leq p.$$

Platí tedy

$$\left.\begin{array}{l} s'_i \equiv s_j \pmod{a} \Rightarrow s'_i = s_j \\ j \equiv i \pmod{p} \Rightarrow j = i \end{array}\right\} \Rightarrow s'_i = s_i \Rightarrow \sigma' = \sigma$$

.

Existuje jediný (triviální) cyklus délky a, zbývající cykly mají délku ap. Pro $\alpha, \beta \in S$ položme $\alpha \sim \beta$, jestliže existuje přirozené číslo n takové, že $T^n(\alpha) = \beta$. Pak relace $\sim$ je ekvivalence na S, $\overline{S}$ je třída rozkladu příslušného této ekvivalenci a každá jiná třída tohoto rozkladu má ap prvků. Označme c počet netriviálních cyklů. Potom card$\overline{S}$+cap=card$S$. Po dosazení máme

$$cap = a(a^{p-1} - 1)$$

a odsud plyne

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

Autoři však neuvádějí vztah (2.13) mezi Fermatovým kvocientem a počtem netriviálních cyklů, resp. počtem tříd ekvivalence, který uvádí MacMahon ([Mh], str. 309). Počet netriviálních cyklů je roven $q_a(p)$.