Sergěj Šišpanov
O větě Leibnizově

Časopis pro pěstování matematiky a fysiky, Vol. 55 (1926), No. 3, 225--233

Persistent URL: http://dml.cz/dmlcz/124053

O větě Leibnizově.

Sergěj Šišpanov.

Podle věty Fermatovy platí kongruence

$$a^{m-1} \equiv 1 \ (mod\ m),$$

při čemž m je prvočíslo a a není dělitelno m.

Je rovněž správná obrácená věta:

Je-li při libovolném kladném čísle a, menším než m, vyhověno kongruenci

$$a^{m-1} \equiv 1 \ (mod\ m),$$

jest m prvočíslem.

Následkem toho je věta výše vyslovená úplně rovnocenná s větou Wilsonovou a spolu s ní slouží za kriterium pro prvočísla.

Lze vysloviti ještě jednu větu obrácenou k větě Fermatově:

Je-li pro libovolné celistvé číslo a, nemající s m společného činitele, vyhověno kongruenci

$$a^{m-1} \equiv 1 \ (mod\ .\ m),$$

jest m prvočíslem.

Tato neúplně obrácená věta se připisuje Leibnizovi. Číselným příkladem snadno seznáme, že není správná. Vezmeme číslo $561 = 3 . 11 . 17$, uvedené Mankem. Libovolné a, nemající s 561 společného činitele, není dělitelno ani 3, ani 11, ani 17 a proto:

$$a^2 \equiv 1 \ (mod\ 3), \quad a^{10} \equiv 1 \ (mod\ 11), \quad a^{16} \equiv 1 \ (mod\ 17).$$

Umocníme-li první kongruenci mocnitelem 40, druhou mocnitelem 8 a třetí mocnitelem 5, dostaneme

$$a^{80} \equiv 1 \ (mod\ 3), \quad a^{80} \equiv 1 \ (mod\ 11), \quad a^{80} \equiv 1 \ (mod\ 17).$$

Ježto moduly těchto kongruencí po dvou nemají společných činitelů, plyne z toho kongruence

$$a^{80} \equiv 1 \ (mod\ 3 . 11 . 17).$$

Rozdíl $561 - 1 = 560$ je dělitelný číslem 80, což znamená, že př. libovolném a, nemajícím s 561 společného dělitele, platí kongruence

$$a^{560} \equiv 1 \ (mod\ 561).$$

Je tedy složené číslo 561, vzhledem k větě Fermatově, analogické prvočíslu.

Vyšetření takovýchto čísel, odporujících větě Leibnizově, je předmětem tohoto článku.

Vezměme složené číslo m a dejme tomu, že při libovolném a, nemajícím s m společných činitelů, je vyhověno kongruenci

$$a^{m-1} \equiv 1 \pmod{m}. \qquad (1)$$

Připusťme nejdříve, že m je číslo sudé. Ježto $m-1$ nemá s m společných činitelů, můžeme vziti

$$a = m - 1.$$

Podmínka (1) nabude pak tvaru

$$(-1)^{m-1} \equiv 1 \pmod{m},$$

poněvadž máme

$$a \equiv -1 \pmod{m}.$$

Ale mocnina $m-1$ v předcházející kongruenci jest číslo liché, a proto tato kongruence dává

$$2 \equiv 0 \pmod{m},$$

což není možno při složeném m. Může tedy m obsahovati jako prvočinitele lichá prvočísla. Oddělíme jeden z takových činitelů, t. j. položíme

$$m = p^{\alpha} . n,$$

kde p je liché prvočíslo, n je číslo liché, nedělitelné p a mocnina $\alpha > 0$. Ježto platí (1), máme

$$a^{m-1} \equiv 1 \pmod{p^{\alpha} n}$$

a tedy tím spíše

$$a^{m-1} \equiv \pmod{p^{\alpha}}. \qquad (2)$$

Označme písmenem g kořen jednotkový pro modul p^{α}. Podle definice kořenu jednotkového při složeném modulu, náleží g k mocniteli $\varphi(p^{\alpha})$, kde φ značí funkci Eulerovu. Jinými slovy, nejmenší kladná hodnota t, při níž je vyhověno kongruenci

$$g^{t} \equiv 1 \pmod{p^{\alpha}},$$

je rovna $\varphi(p^{\alpha})$. Jak vysvítá z poslední kongruence, není g dělitelno p. Podobné vlastnosti má každé číslo a, kongruentní s g podle modulu p^{α}. O jednotkovém kořenu g můžeme učiniti dva předpoklady: buď g a n nemají společných činitelů, nebo mají společnou míru. V prvém případě vezmeme

$$a = g.$$

V druhém případě rozložíme g a n na prvočinitele a vypíšeme ty z nich

$$q_1, q_2, \ldots, q_l,$$

jež obsahují n, ale neobsahují g.

Potom sestavíme součin

$$\pi = q_1 \cdot q_2 \cdot \ldots \cdot q_l$$

a položíme

$$a = g + \pi \cdot p^{\alpha}.$$

Ve zvláštním případě, kdy všechny prvočíselné dělitelé čísla n jsou zahrnuty již v g, položíme $\pi = 1$.

Dokážeme, že a a n nemají společných dělitelů. Je-li totiž nějaké prvočíslo obsaženo zároveň v n i v g, nemůže již býti obsaženo v πp^{α}. Je-li nějakým prvočíslem dělitelno pouze n, je toto číslo obsaženo v řadě

$$q_1, q_2, \ldots, q_l,$$

a je proto obsaženo v $\pi \cdot p^{\alpha}$ a nikoliv v g. Takovým způsobem najde se vždycky číslo α, náležející mocniteli $\varphi(p^{\alpha})$ podle modulu p^{α}, které nemá s m společných činitelů. Ježto pak vztah (2) má platiti při libovolném a, nemajícím s m společných činitelů, musí podle věty známé z teorie čísel $m-1$ býti dělitelno minimálním mocnitelem $\varphi(p^{\alpha})$, t. j.

$$\frac{p^{\alpha} n - 1}{p^{\alpha-1}(p-1)} = \text{číslu celému},$$

a to je možno pouze za podmínky, že $\alpha = 1$ a $pn - 1$ je dělitelno $p-1$.

Opakujeme-li tyto úvahy pro všechny prvočíselné dělitele p čísla m, seznáme, že má tvar

$$m = p_1 \cdot p_2 \cdot \ldots \cdot p_k,$$

kde $p_1, p_2, \ldots p_k$ jsou vesměs různá lichá prvočísla a $k \geq 2$, poněvadž podle předpokladu m je složené. Mimo to, musí $m-1$ býti dělitelno každým z rozdílů

$$p_1 - 1, p_2 - 1, \ldots, p_k - 1,$$

a tedy i jejich nejmenším společným násobkem

$$[p_1 - 1, p_2 - 1, \ldots, p_k - 1],$$

který pro stručnost označíme λ.

Setrvávajíce při obecném výkladu, můžeme ovšem předpokládati, že činitelé jsou seřaděni v stoupající řadu, t. j. že

$$p_1 < p_2 < \ldots < p_k.$$

Ke konci zjistíme, že číslo m, sestavené uvedeným způsobem, vyhovuje podmínce (1). Jsou-li totiž $m = p_1 \cdot p_2 \ldots p_k$ a $m - 1$ dělitelna číslem λ, platí podle věty Fermatovy při libovolném a, nemajícím s m společných činitelů, kongruence

$$a^{p_1 - 1} \equiv 1 \pmod{p_1}, \; a^{p_2 - 1} \equiv 1 \pmod{p_2}, \; \ldots \ldots \ldots \ldots,$$
$$a^{p_k - 1} \equiv 1 \pmod{p_k}.$$

Umocníme-li první z obdržených kongruencí mocnitelem $\frac{\lambda}{p_1 - 1}$ druhou m mocnitelem $\frac{\lambda}{p_2 - 1}$ atd., najdeme

$$a^\lambda \equiv 1 \ (mod\ p_1),\ a^\lambda \equiv 1 \ (mod\ p_2),\ \ldots\ldots\ldots\ldots,\ a^\lambda \equiv 1 \ (mod\ p_k).$$

Z toho plyne, že $a^\lambda \equiv 1 \ (mod\ p_1 p_2 \ldots . p_k)$

a tím spíše $a^{m-1} \equiv 1 \ (mod\ m)$,

poněvadž λ jest dělitelno $m - 1$.

Probereme podrobněji také podmínku dělitelnosti $m - 1$ číslem λ. Dejme tomu, že rozdíly

$$p_1 - 1,\ p_2 - 1,\ \ldots.,\ p_k - 1$$

mají největší společnou míru $2t$. Tato je určitě sudé kladné číslo, poněvadž všechna p jsou lichá prvočísla. Dělíme-li všechny rozdíly jejich největší společnou měrou, dostaneme

$$p_1 - 1 = 2t \,.\, x_1,\ p_2 - 1 = 2t \,.\, x_2, \ldots.,\ p_k - 1 = 2t \,.\, x_k$$

nebo

$$p_1 = 2t \,.\, x_1 + 1,\ p_2 = 2t \,.\, x_2 + 1, \ldots.,\ p_k = 2t \,.\, x_k + 1, \quad (3)$$

kde čísla

$$x_1 < x_2 < \ldots . < x_k$$

nemají společné míry. Výraz pro společný nejmenší násobek zmíněných rozdílů můžeme přepsati takto:

$$[p_1 - 1,\ p_2 - 1, \ldots.,\ p_k - 1] = [2t\,x_1,\ 2t\,x_2, \ldots.,\ 2t x_k] =$$
$$= 2t \,.\, [x_1,\ x_2, \ldots.,\ x_k].$$

Označíme-li společný nejmenší násobek

$$[x_1,\ x_2, \ldots.,\ x_k]$$

písmenem μ, budeme míti

$$\lambda = 2t \,.\, \mu\,.$$

Podmínku dělitelnosti

$$p_1 p_2 \ldots . p_k - 1 \equiv 0 \ (mod\ \lambda)$$

můžeme pak vyjádřiti takto

$$(1 + 2tx_1) \,.\, (1 + 2tx_2) \ldots . (1 + 2tx_k) \equiv 0 \ (mod\ 2t\mu).$$

Vykonáme-li násobení binomů na levé straně a zavedeme-li pro souměrné funkce zkrácená označení

$$\sum x_1 = a_1,\ \sum x_1 x_2 = a_2,\ \ldots\ldots\ldots,\ \sum x_1 x_2 \ldots . x_k = a_k,$$

obdržíme

$$a_1 \,.\, 2t + a_2 \,.\, (2t)^2 + \ldots . + a_{k-1} \,.\, (2t)^{k-1} + a_k \,.\, (2t)^k \equiv 0 \ (mod\ 2t\mu).$$

Odtud, po zkrácení číslem $2t$ a vzhledem k tomu, že a_k je dělitelno μ, obdržíme pro určení $2t$ kongruenci

$$a_1 + a_2 \cdot 2t + \cdots + a_{k-1} \cdot (2t)^{k-2} \equiv 0 \ (mod\ \mu). \qquad (4)$$

Ve zvláštním případě, kdy $k = 2$, platí

$$a_1 = x_1 + x_2, \qquad \mu = x_1 x_2,$$

poněvadž čísla x_1 a x_2 nemají společných činitelů. Kongruence (4) neobsahuje t a nabývá tvaru

$$x_1 + x_2 \equiv 0 \ (mod\ x_1 x_2).$$

Odtud plynou dvě kongruence

$$x_1 \equiv 0 \ (mod\ x_2), \qquad x_2 \equiv 0 \ (mod\ x_1),$$

které si při našich podmínkách odporují. Vidíme tedy, že číslo m musí obsahovati více než dva prvočíselné činitele.

Abychom se vyhnuli zbytečnému zkoušení při vyhledávání čísel zkoumaného tvaru, dokážeme, že libovolná $k-1$ z čísel $x_1, x_2, \ldots, x_k$ nemají společné míry. Neboť kdyby kterákoliv z výše uvedených čísel, na příklad $x_1, x_2, \ldots, x_{k-1}$ byla dělitelna d, musely by všechny koeficienty $a_2, a_3, \ldots$, počínajíc druhým, býti dělitelné d. Modul

$$\mu = [x_1, x_2, \ldots, x_k]$$

je také dělitelný d. To znamená, že první člen kongruence (4) musí býti dělitelen d. Připomeneme-li si výraz pro a_1:

$$a_1 = x_1 + x_2 + \cdots + x_{k-1} + x_k$$

a uvážíme-li, že v posledním součtu všechny sčítance, mimo poslední, jsou dělitelny d, usoudíme, že x_k je také dělitelno d, což však není možno při $x_1, x_2, \ldots, x_k$, nemajících společné míry jak bylo zmíněno. Ve zvláštním případě, pro $k = 3$, mají býti čísla x_1, x_2, x_3 nesoudělná a tedy

$$\mu = x_1 x_2 x_3.$$

Po těchto výkladech docházíme k této větě:

Je-li při libovolném a, nemajícím s m společných činitelů, vyhověno kongruenci

$$a^{m-1} \equiv 1 \ (mod\ m),$$

je m buď prvočíslem, nebo součinem nejméně tří navzájem různých, lichých prvočísel.

Připojíme-li požadavek, aby $m-1$ bylo dělitelno λ, dostaneme nutné a postačující podmínky existence hledaných čísel.

K jejich vyšetřování volíme hodnoty $x_1, x_2, \ldots, x_k$, tak, aby žádných $k-1$ z nich nemělo společného dělitele. Pak řešíme kongruenci (4) a dosadíme výrazy pro $2t$, lineárně závislé na jednom

celistvém parametru do vztahu (3). Klademe-li za tento parametr hodnoty, při nichž všechna p jsou prvočísla, obdržíme podle vzorce

$$m = p_1 \cdot p_2 \ldots . p_k$$

všechna hledaná čísla, určená systémem

$$x_1, x_2, \ldots, x_k.$$

Nemá-li kongruence (4) kořenů, znamená to, že při takto volených hodnotách $x_1, x_2, \ldots, x_k$ není čísel splňujících podmínku (1).

Propočítejme číselný příklad.

Nechť $x_1 = 1, \quad x_2 = 2, \quad x_3 = 3,$

takže $\mu = 1 \,.\, 2 \,.\, 3 = 6.$

Dále $a_1 = 1 + 2 + 3 \equiv 0 \ (mod\ 6),$

$a_2 = 2 + 3 + 6 \equiv -1 \ (mod\ 6).$

Kongruence pro určení $2t$ nabývá tvaru

$$2t \equiv 0 \ (mod\ 6).$$

Odtud $2t = 6\tau,$

kde τ je celistvým parametrem.

Podle vzorců (3) obdržíme

$$p_1 = 6\tau + 1, \quad p_2 = 12\tau + 1, \quad p_3 = 18\tau + 1.$$

Při $\tau = 1$ máme: $p_1 = 7, \ p_2 = 13, \ p_3 = 19.$ Ježto všechna p jsou prvočísla, je číslo

$$m = 7 \,.\, 13 \,.\, 19 = 1729$$

číslem hledaným.

Nejblíže příští hodnota τ, vedoucí k prvočíselným činitelům, je 6. Zde

$$m = 37 \,.\, 73 \,.\, 109 = 294409 \text{ atd.}$$

Z tohoto příkladu je patrno, že otázka o počtu řešení úlohy je v souvislosti s větou Dirichletovou, rozšířenou na několik řad aritmetických. — V případech, kdy takové zobecnění je možno, obdržíme nekonečný počet řešení. V případě opačném, počet řešení je omezen.

Udaný způsob pro vyhledávání čísel odporujících větě Leibnizově, je možno přeměniti takto: Vezmeme dvě nebo několik lichých prvočísel $p_1, p_2, \ldots, p_k$, navzájem nerovných a sestavíme součin

$$n = p_1 p_2 \ldots . p_k.$$

Potom násobíme obě části poslední rovnosti nějakým lichým prvočíslem p, různým od $p_1, p_2, \ldots . p_k$.

Číslo $m = n \,.\, p = p \cdot p_1 \,.\, p_2 \ldots . p_{k-1} \,.\, p_k$

musí splňovati podmínku (1). K tomu je nutno a stačí, aby $m-1$ bylo dělitelno $p-1$ a

$$\lambda = [p_1 - 1,\ p_2 - 1, \ldots, p_k - 1].$$

Vyjádříme-li $m-1$ ve tvaru

$$m-1 = np-1 = n(p-1)+(n-1),$$

vidíme, že dělitelnost číslem $p-1$ vede ke kongruenci

$$n-1 \equiv 0 \pmod{p-1}. \qquad (5)$$

Dělíme n číslem λ a máme

$$n = q\lambda + r,$$

kde q je podíl a r zbytek. Zde r nemůže se rovnati nule, poněvadž n je liché a λ sudé.

Číslo $m-1$ lze psáti:

$$m-1 = p(q\lambda + r) - 1 = pq\lambda + (pr-1).$$

Připomeneme-li, že poslední výraz je dělitelný λ, přijdeme ke kongruenci

$$pr-1 \equiv 0 \pmod{\lambda} \text{ nebo } pr \equiv 1 \pmod{\lambda}. \qquad (6)$$

Je-li možno splniti současně kongruence (5) a (6) za platnosti uvedených omezení vzhledem k číslu p, je p číslem hledaným. V opačném případě, není možno vyhovět podmínce (1), při hodnotách $p_1, p_2, \ldots, p_k$, takto volených.

Objasníme úvahy vykonané číselným příkladem:

Nechť $n = 7 \cdot 13 \cdot 19 = 1729.$

Nejdříve najdeme $\lambda = [6, 12, 18] = 36.$

Dělíme-li 1729 číslem 36, obdržíme zbytek $r = 1$. Z kongruencí (5) a (6) plyne, že 1728 je dělitelno $p-1$, a $p-1$ číslem 36.

Položíme-li $p - 1 = 36t,$

kde t je nějaké číslo celé, usoudíme, že t je dělitelem 48 a proto může nabýti jen jedné z hodnot:

$$1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 12,\ 16,\ 24.$$

Při $t = 1$ je součinitel $p = 36t + 1 = 37$

prvočíslem a proto číslo

$$m = 7 \cdot 13 \cdot 19 \cdot 37 = 63973$$

hoví podmínce (1).

Druhá hodnota $t = 2$ dává $p = 73$ a vede k řešení

$$m = 7 \cdot 13 \cdot 19 \cdot 73 = 126217 \text{ atd.}$$

Je patrno, že volíme-li všechny možné hodnoty pro $x_1, x_2, \ldots, x_k$ v prvním z uvedených způsobů, nebo pro $p_1, p_2, \ldots, p_k$ v druhém způsobu, měníme-li k, obdržíme všechna čísla odporující větě Leibnizově, avšak nikoli uspořádaná. Abychom dostali potřebná čísla podle stoupajících hodnot, užijeme tabulky pro rozklad čísel v prvočinitele, volíce pouze lichá čísla rozkládající se nejméně na tři různé prvočíselné činitele. Při tom se otázka o dělitelnosti $m-1$ každým z rozdílů

$$p_1 - 1, \quad p_2 - 1, \ldots, p_k - 1$$

snadno rozřeší podle pravidel dělitelnosti. Takovým způsobem obdržíme v mezích do 10000 tato čísla splňující podmínku (1):

$$561 = 3 \cdot 11 \cdot 17, \quad 1105 = 5 \cdot 13 \cdot 17, \quad 1729 = 7 \cdot 13 \cdot 19,$$
$$2465 = 5 \cdot 17 \cdot 29, \quad 2821 = 7 \cdot 13 \cdot 31, \quad 6601 = 7 \cdot 23 \cdot 41,$$
$$8911 = 7 \cdot 19 \cdot 67.$$

Jak je viděti z tabulky, všechna tato čísla jsou sestavena ze tří součinitelů. Číslo výše uvedené

$$63973 = 7 \cdot 13 \cdot 19 \cdot 37$$

je nejmenším z těch, jež obsahují čtyři součinitele.

Sur un théorème de Leibniz.

(Extrait de l'article précédent.)

1. L'inversion généralisée du théorème de Fermat, exprimée sous la forme suivante: „Si chaque nombre a premier avec m satisfait à la congruence $a^{m-1} \equiv 1 \pmod{m}$, le nombre m est premier“ — n'est pas précise. Il existe des nombres composés satisfaisant à la congruence indiquée, par ex., $m = 561$.

2. L'énoncé exact du théorème est le suivant: „Si chaque nombre a, premier avec m satisfait à la congruence $a^{m-1} \equiv 1 \pmod{m}$, ... (*) le nombre m est, ou premier, ou égal au produit de trois au moins différents nombres premiers et impairs.“

3. La recherche des nombres composés présentant une analogie avec les nombres premiers par rapport au théorème de Fermat conduit à la détermination du nombre t satisfaisant à la congruence

$$\Sigma x_1 . + \Sigma x_1 x_2 . 2t + \cdots + \Sigma x_1 x_2 \cdots x_{k-1} . (2t)^{k-2} \equiv 0 \pmod{\mu}.$$

Les nombres $x_1, x_2, \ldots x_k$ sont arbitraires, sans diviseur commun, μ est leur plus petit commun multiple.

4. Il est possible de ramener la question considerée à la solution d'un système de deux congruences linéaires.

5. Jusqu'à 10000 il n'y a que les nombres suivants satisfaisant à la condition (*)

$$561 = 3 . 11 . 17, \qquad 2821 = 7 . 13 . 31,$$
$$1105 = 5 . 13 . 17, \qquad 6601 = 7 . 23 . 41,$$
$$1729 = 7 . 13 . 19, \qquad 8911 = 7 . 19 . 67.$$
$$2465 = 5 . 17 . 29,$$

Chaque nombre contient trois facteurs.

6. Le plus petit nombre contenant quatre facteurs et satisfaisant à la condition (*) est

$$63973 = 7 . 13 . 19 . 37.$$