Eduard Weyr
O jisté větě číselné

Časopis pro pěstování mathematiky a fysiky, Vol. 11 (1882), No. 1, 39--47

Persistent URL: http://dml.cz/dmlcz/122131

O jisté větě číselné.

Napsal **Ed. Weyr.**

Budiž v libovolné celistvé číslo a mějme

$$v = q_1^{n_1} q_2^{n_2} \dots q_m^{n_m},$$

kdež $q_1, q_2, \dots q_m$ značí různá čísla kmenná. Je-li p číslem kmenným, pak je z theorie čísel známo, že výraz

$$p^v - \Sigma p^{\overline{q_1}} + \Sigma p^{\overline{q_1 q_2}} - \dots + (-1)^{m-1} \Sigma p^{\overline{q_1 q_2 \dots q_{m-1}}} + (-1)^m p^{\overline{q_1 q_2 \dots q_m}}$$

je dělitelný číslem v. Napsaný výraz podává totiž stupeň součinu všech celistvých funkcí stupně v, jež jsou kmenné (irréductible) dle modulu p, a rovná se tudíž výraz ten součinu $N v$, značí-li N počet oněch funkcí (v. *Serret*, Cours d'Algèbre supérieure, Section III, Chap. III). Hledaje v rovině body, jež vyhovují jisté podmínce, nalezl p. *S. Kantor*, priv. docent při c. k. něm. vys. škole technické v Praze, že jich počet jest dán výrazem právě napsaným nechť je p jakékoli číslo, a poněvadž se body ty nutně řadily do skupin po v, soudil, že onen výraz je dělitelný číslem v (v. Annali di Mat. pura ed appl., ser. II^a t. X. pag. 71). Speciálný případ $p = 2$ uvažovaný týmž autorem ibid. pag. 64 v pojednání „Wie viele cyclische Gruppen gibt es in einer quadratischen Transformation der Ebene?“ prozkoumal p. *Hirst* již před lety a uveřejnil tehdejší výsledky teprve nedávno v The Quarterly Journal of Pure and Appl. Math. 1881 s titulem *On quadric transformation*, načež mě pan S. Kantor sám laskavě upozornil.

Ač souvislost takto vytknutá mezi geometrií a theorií čísel je zajímava, přece se mi zdálo, že dokazování vět číselných pomocí dosti složitých úvah geometrických jest postup velice nepřímý, z něhož as theorie čísel, držící co do přesnosti první místo v mathematice, mnoho těžiti nemůže. Hledaje ryze číselný důkaz oné věty pro případ obecný — kdy p jest číslem libovolným — měl jsem za to, že důkaz takový i vůči případu

již odůvodněnému — kdy p je kmenné — nebude bez ceny, poněvadž úvahy o kmenných funkcích, jež k onomu theorému mimochodem vedly, jsou, ač velmi zajímavé, nad míru abstraktní a poměrně rozsáhlé. Nalezl jsem přímý důkaz oné věty, jež v následujících řádcích čtenářům předkládám.

1. Buďte a a ν dva libovolná celistvá čísla.*) Položme

$$M = a^\nu - 1$$

a zvolme M za modul, k němuž čísla vztahujeme.

Utvoříme-li pomocí čísla a, jež patrně je nesoudělné s modulem, a pomocí libovolného čísla x řadu

$$x, xa, xa^2, xa^3, \ldots . xa^{\nu-1}, xa^\nu, \ldots,$$

tu je rozdíl $xa^\nu - x$ dělitelný modulem t. j. $\nu + 1^{ni}$ člen je shodný s prvním, tedy $\nu + 2^{ý}$ s druhým atd. Obmezíme se tudíž na ν členů

$$(1) \qquad x, xa, xa^2, \ldots xa^{\nu-1}.$$

Nejsou-li žádné dvě z těchto hodnot shodné dle mod. M, nazveme x číslem řádu ν. Jde nyní o to, abychom ustanovili počet čísel řádu ν.

Je-li x číslem řádu ν, jest každé z čísel (1) též řádu ν, neboť čísla

$$xa^\varrho, xa^{\varrho+1}, \ldots xa^{\varrho+\nu-1}$$

jsou resp. shodna s čísly (1). Z toho jde snadno, *že je počet čísel řádu ν násobkem čísla ν.* Existuje-li totiž jedno takové číslo, máme jich hned ν t. všecka čísla řady (1). Existuje-li mimo tato jiné na př. y, tu budou

$$y, ya, ya^2, \ldots ya^{\nu-1}$$

zase čísla řádu ν a s. vesměs nová a různá. Nebo kdyby na př.

$$ya^h \equiv xa^\varrho \pmod{M},$$

měli bysme

$$ya^{h+\nu-h} \equiv xa^{\varrho+\nu-h}$$

t. j.

$$y \equiv xa^{\varrho+\nu-h},$$

a tedy by y nebylo číslem novým, proti supposici.

---

*) Jednám zde jen o celistvých číslech, což k vůli dalšímu připomínám jednou pro vždy.

Existují-li mimo nalezená 2ν čísla řádu ν ještě jiná, tu nechť je z jedno z nich, i budou z důvodů obdobných

$$z,\ za,\ za^2,\ \ldots\ za^{\nu-1}$$

samá nová čísla řádu ν, čímž jich již máme 3ν, atd. až do vyčerpání všech.

2. Nechť x není číslem řádu ν t. j. nechť nejsou čísla v řadě (1) naskrze neshodna dle mod. M. Mějmež tedy na př.

$$xa^g \equiv xa^h, \qquad g < h < \nu.$$

Z toho jde

$$xa^{g+\nu-h} \equiv xa^\nu \equiv x,$$

t. j. v řadě (1) se vyskytne nutně člen shodný s prvním.

Buď xa^g *první* člen, který v řadě (1) je shodný s x t. j. mějme teprve při exponentu g shodu

$$xa^g \equiv x, \qquad g < \nu.$$

Pak jsou čísla

$$x,\ xa,\ xa^2,\ \ldots\ xa^{g-1} \tag{2}$$

vesměs neshodna dle mod. M; neboť v případu opačném bysme měli

$$xa^h \equiv xa^k, \qquad h < k < g,$$

t. j.

$$xa^{h+g-k} \equiv xa^g \equiv x,$$

což odporuje supposici, jelikož

$$h + g - k < g.$$

Číslo x, jež podává řadu (2) naskrz neshodných čísel, jež však činí xa^g shodným s x, nazveme číslem řádu g. Jest patrno, že v řadě

$$x,\ xa,\ xa^2,\ \ldots$$

budou jen čísla

$$x,\ xa^g,\ xa^{2g},\ a^{3g},\ \ldots$$

shodna s x, pročež jest ν nutně násobkem čísla g, t. j. *řád libovolného čísla jest dělitelem čísla* ν.

3. Vyšetřme kolik jest čísel x vyhovujících shodě

$$xa^g \equiv x \pmod{M},$$

v níž g značí dělitel čísla ν. — Napišme shodu ve tvaru

$$x(a^g - 1) \equiv 0 \pmod{M}$$

aneb

$$x \equiv 0 \pmod{M_1},$$

klademe-li

$$M_1 = \frac{M}{a^g - 1} = \frac{a^\nu - 1}{a^g - 1},$$

kteráž divise algebraicky beze zbytku vyjde, poněvadž je g dělitelem čísla ν. Obdržíme tedy za x tato čísla

$$x = 0,\ M_1,\ 2M_1,\ 3M_1,\ \ldots\ (a^g - 2)M_1,$$

jichž počet jest

$$a^g - 1.$$

4. Buďte g a h dva dělitelé čísla ν, a vyšetřme kolik čísel x vyhovuje současně shodám

$$xa^g \equiv x,\quad xa^h \equiv x \pmod{M}.$$

Položivše

$$M_1 = \frac{M}{a^g - 1},\quad M_2 = \frac{M}{a^h - 1},$$

bude

$$x \equiv 0 \pmod{M_1},\quad x \equiv 0 \pmod{M_2}.$$

Musí tedy x býti násobkem čísel M_1 a M_2 t. j. násobkem jich nejmenšího společného násobku. Označme literou d největší společný dělitel čísel g a h; *pak jest* $a^d - 1$ *největší společný dělitel čísel* $a^g - 1$, $a^h - 1$, o čemž důkaz připojím na konci této úvahy. Tedy jest

$$M_3 = \frac{M}{a^d - 1}$$

nejmenší společný násobek čísel M_1 a M_2. Tím máme tyto společné kořeny obou shod

$$x = 0,\ M_3,\ 2M_3,\ 3M_3,\ \ldots\ (a^d - 2)M_3,$$

jichž počet jest $a^d - 1$.

Zcela obdobně lze stanoviti společné kořeny tří shod

$$xa^g \equiv x,\quad xa^h \equiv x,\quad xa^k \equiv x,\ \pmod{M}$$

v nichž g, h, k jsou dělitelé čísla ν. Vyskytne se společných kořenů $a^d - 1$, značí-li d největší společný dělitel čísel g, h, k; a p. pro více shod.

5. Mějme nyní

$$\nu = p^\alpha,$$

kdež p jest číslem kmenným. Čísla 0, 1, 2, ... $M - 1$ jsou buď řádu 1 neb p, neb p^2, p^3, ... $p^{\alpha-1}$, aneb konečně řádu ν. Z toho jde, že všecka, která nejsou řádu ν, podává shoda

$$x^{p^{\alpha-1}} \equiv x, \text{ (mod. M)}$$

jež má $a^{p^{\alpha-1}} - 1$ kořenů. Máme tedy čísel řádu ν

$$M - (a^{p^{\alpha-1}} - 1)$$

t. j.

$$a^{\nu} - a^{\frac{\nu}{p}},$$

a jest tudíž dle odst. 1. číslo to dělitelno číslem ν.*)

Mějme dále

$$\nu = p^{\alpha} q^{\beta},$$

kde p a q značí různá čísla kmenná. Čísla, která nejsou řádu ν, jsou řádu g, značí-li g dělitel čísla ν, pročež jest g buď dělitelem čísla $p^{\alpha-1}q^{\beta}$ aneb čísla $p^{\alpha}q^{\beta-1}$, aneb obou. Vyhovují tedy tato čísla jedné neb druhé aneb oběma shodám

$$x^{\frac{\nu}{p}} \equiv x \text{ (mod. M)}, \quad x^{\frac{\nu}{q}} \equiv x \text{ (mod. M)}.$$

Počet kořenů první shody jest $a^{\frac{\nu}{p}} - 1$, druhé $a^{\frac{\nu}{q}} - 1$, oběma společných je $a^{d} - 1$, je-li d největší společný dělitel čísel $\frac{\nu}{p}$ a $\frac{\nu}{q}$, tedy $d = \frac{\nu}{pq}$. Jest tedy počet všech čísel, která nejsou řádu ν

$$a^{\frac{\nu}{p}} - 1 + a^{\frac{\nu}{q}} - 1 - (a^{\frac{\nu}{pq}} - 1)$$

a tedy počet čísel řádu ν

$$M - (a^{\frac{\nu}{p}} + a^{\frac{\nu}{q}} - a^{\frac{\nu}{pq}} - 1)$$

t. j.

$$a^{\nu} - \left(a^{\frac{\nu}{p}} + a^{\frac{\nu}{q}}\right) + a^{\frac{\nu}{pq}}.$$

Dle odst. 1. jest číslo to dělitelno číslem ν.

Mějme dále

$$\nu = p^{\alpha} q^{\beta} r^{\gamma},$$

---

*) Jsou-li a a ν nesoudělná, vychází ihned, že $a^{\nu - \frac{\nu}{p}} - 1$ je dělitelno číslem ν a to je patrně speciálný případ rozšířené věty Fermatovy.

kdež p, q, r značí různá čísla kmenná. Čísla, která nejsou řádu ν, jsou jistých řádů g, jež jsou děliteli čísla ν a tedy dělí jedno z čísel $\frac{\nu}{p}$, $\frac{\nu}{q}$, $\frac{\nu}{r}$, aneb dvě z nich aneb všecka tři. Čísla zmíněná podává jedna ze shod

$$x^{\frac{\nu}{p}} \equiv x, \quad x^{\frac{\nu}{q}} \equiv x, \quad x^{\frac{\nu}{r}} \equiv x \pmod{M},$$

aneb dvě aneb všecky tři. Všem třem vyhovuje dle odst. 4. $Q_{123} = a^{\frac{\nu}{pqr}} - 1$ čísel, prvním dvěma $Q_{12} = a^{\frac{\nu}{pq}} - 1$ čísel, první a třetí $Q_{13} = a^{\frac{\nu}{pr}} - 1$, druhé a třetí $Q_{23} = a^{\frac{\nu}{qr}} - 1$ čísel, první $Q_1 = a^{\frac{\nu}{p}} - 1$ čísel, druhé $Q_2 = a^{\frac{\nu}{q}} - 1$ čísel a třetí $Q_3 = a^{\frac{\nu}{r}} - 1$ čísel.

Počet různých kořenů těchto tří shod jest tedy

$$Q = Q_1 + (Q_2 - Q_{12}) + (Q_3 - Q_{13} - Q_{23} + Q_{123})$$

t. j.

$$Q = Q_1 + Q_2 + Q_3 - (Q_{12} + Q_{13} + Q_{23}) + Q_{123}.$$

Jest tedy počet čísel řádu ν

$$M - Q$$

t. j.

$$a^\nu - \left(a^{\frac{\nu}{p}} + a^{\frac{\nu}{q}} + a^{\frac{\nu}{r}}\right) + a^{\frac{\nu}{pq}} + a^{\frac{\nu}{pr}} + a^{\frac{\nu}{qr}} - a^{\frac{\nu}{pqr}},$$

a číslo to tudiž dělitelno číslem ν.

6. Mějme nyní obecně

$$\nu = q_1^{n_1} q_2^{n_2} \ldots q_m^{n_m},$$

kdež $q_1, q_2, \ldots q_m$ značí různá kmenná čísla. Každé číslo x, které není řádu ν, podává některá shoda:

$$x^{\frac{\nu}{q_1}} \equiv x, \; x^{\frac{\nu}{q_2}} \equiv x, \; \ldots \qquad x^{\frac{\nu}{q_m}} \equiv x \pmod{M}.$$

Učinivše

$$Q_1 = a^{\frac{\nu}{q_1}} - 1, \; Q_2 = a^{\frac{\nu}{q_2}} - 1, \ldots Q_m = a^{\frac{\nu}{q_m}} - 1,$$

$$Q_{12} = a^{\overline{q_1 q_2}} - 1, \quad Q_{13} = a^{\overline{q_1 q_3}} - 1, \ldots\ldots\ldots,$$

$$Q_{123} = a^{\overline{q_1 q_2 q_3}} - 1, \text{ atd. atd.,}$$

bude Q_i počet kořenů shody $i^{té}$, Q_{ij} počet kořenů společných shodám $i^{té}$ a $j^{té}$, Q_{ijk} počet kořenů společných shodám těm a shodě $k^{té}$ atd. Všecky shody mají pak dohromady různých kořenů

$$Q = \Sigma Q_i - \Sigma Q_{ij} + \Sigma Q_{ijk} - \ldots + (-1)^{m-1} Q_{12\ldots m}.$$

To dokážeme snadno tím spůsobem, že se přesvědčíme, že každý kořen ve výrazu Q počítán jednou a jen jednou.

Kořeny, které vyhovují *jen* jedné shodě n. př. $i^{té}$ zahrnuty číslem Q_i. Kořeny vyhovující $i^{té}$ a $j^{té}$ shodě a *jen* těmto počítány v Q_i, Q_j a Q_{ij}, tedy $(1+1-1)^{nou}$ t. j. jednou.

Kořeny vyhovující $i^{té}$, $j^{té}$ a $k^{té}$ shodě a *jen* jím, počítány v Q_i, Q_j, Q_k, Q_{ij}, Q_{ik}, Q_{jk}, Q_{ijk}, tedy $(1+1+1-1-1-1+1)^{nou}$ t. j. jednou.

A obecně kořeny vyhovující současně λ shodám a jen těm, vyskytnou se v Q

$$\left[\lambda - \binom{\lambda}{2} + \binom{\lambda}{3} - \binom{\lambda}{4} + \ldots + (-1)^{\lambda-1} \binom{\lambda}{\lambda}\right] - \text{kráte,}$$

kdež $\binom{\lambda}{\mu}$ značí jako obyčejně $\mu^{tý}$ binomiálný koefficient mocniny λ. Avšak

$$(1-1)^\lambda = 0 = 1 - \lambda + \binom{\lambda}{2} - \binom{\lambda}{3} + \ldots + (-1)^\lambda \binom{\lambda}{\lambda},$$

pročež ono číslo se rovná 1 t. j. *každý* kořen počítán ve Q jednou. Máme nyní M — Q kořenů řádu ν t. j.

$$a^\nu - 1 - \Sigma Q_i + \Sigma Q_{ij} - \Sigma Q_{ijk} + \ldots + (-1)^m Q_{12\ldots m}$$

t. j.

$$a^\nu - 1 - \left(\Sigma a^{\overline{q_1}} - m\right) + \Sigma a^{\overline{q_1 q_2}} - \binom{m}{2} - \left(\Sigma a^{\overline{q_1 q_2 q_3}} - \binom{m}{3}\right)$$

$$+ \ldots + (-1)^m \left(a^{\overline{q_1 q_2 \ldots q_m}} - 1\right)$$

t. j.

$$a^\nu - \Sigma a^{\overline{q_1}} + \Sigma a^{\overline{q_1 q_2}} - \ldots + (-1)^m a^{\overline{q_1 q_2 \ldots q_m}}$$

a jest tedy číslo to dle odst. 1. dělitelno číslem ν, čímž důkaz vytčené věty podán.

7. Dosavadní úvahy podávají snadno novou větu, již stručně vytknu. Především podotýkám, že nalezené číslo jest vždy větší než nulla t. j., že existují vždy čísla řádu ν. Stačí ukázati, že vždy aspoň jedno existuje; a takové číslo řádu ν jest $x \equiv 1$, t. j. čísla

$$1,\ a,\ a^2,\ \ldots\ a^{\nu-1}$$

jsou neshodna vzhledem k mod. M. Neboť v případu opačném by

$$a^g \equiv a^h,\quad g < h < \nu$$

tedy

$$a^g\,(a^{h-g} - 1) \equiv 0,$$

a tedy, poněvadž a a $M = a^\nu - 1$ jsou nesoudělná, musilo číslo $a^{h-g} - 1$ býti dělitelno modulem $a^\nu - 1$, který jest větší, — věc to nemožná. Patří tedy a k exponentu ν vzhledem k modulu $a^{\nu-1}$ dle běžného spůsobu rčení (v. *Serret*, Cours d' Algèbre supérieure, Section III, Chap. II), *a jest tedy v divisorem čísla* $\varphi(a^\nu - 1)$, značí-li $\varphi(M)$ obecně počet čísel nesoudělných s M, která nepřesahují M.

Tím získán tento výsledek. Značí-li ν a a libovolná čísla a je-li

$$M = a^\nu - 1 = p^\alpha q^\beta \ldots r^\gamma,$$

kdež $p, q \ldots r$ jsou různá čísla kmenná, tu číslo

$$M\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\ldots\left(1 - \frac{1}{r}\right)$$

jest dělitelno číslem ν, t. j.

$$\varphi(M) \equiv 0 \pmod{\nu}.$$

8. Zbývá ještě podati důkaz, který jsem v odst. 4. odkázal až na konec, t. důkaz, že největší společný dělitel čísel $a^g - 1$, $a^h - 1$ jest $a^d - 1$, značí-li d největší společný dělitel čísel g a h.

Za $g = h$ jest to patrno; buď tedy $h > g$ a položme

$$G = a^g - 1,\quad H = a^h - 1.$$

Každý číslům G a H společný divisor dělí též rozdíl H — G t. j. dělí

$$a^g\,(a^{h-g} - 1).$$

Každý divisor čísla G neb H jest však patrně nesoudělný s číslem a, pročež společný divisor dělí $a^{h-g} - 1$; t. j.

každý společný dělitel čísel G a H jest též společným dělitelem čísel

$$G \text{ a } a^{h-g} - 1.$$

A naopak jich společný dělitel jest též společným dělitelem čísel

$$G \text{ a } a^g (a^{h-g} - 1)$$

t. j. čísel G a H — G t. j. čísel G a H.

Jest tedy největší společný dělitel čísel G a H týž, jako největší společný dělitel čísel

$$a^g - 1, \quad a^{h-g} - 1,$$

tedy tentýž co největší společný dělitel čísel

$$a^g - 1, \quad a^{h-qg} - 1$$

kdež $h - qg = r < g$.

S čísly $a^g - 1$, $a^r - 1$ jednejme tak jako s G a H atd. atd., čímž správnost věty patrna, uvážíme-li, že divise $\frac{a^m - 1}{a^n - 1}$ algebraicky beze zbytku vyjde, je-li m násobek čísla n.

V Praze, v září 1881.

Věta o binomických součinitelích.

Napsal **Al. Zdrahal.**

O součinitelích binomických platí věta vyjádřená vzorcem

$$\Sigma \binom{a}{\alpha}\binom{b}{\beta}\binom{c}{\gamma}\binom{d}{\delta}\ldots = \binom{a+b+c+d+\ldots}{r},$$

$$\alpha + \beta + \gamma + \delta \ldots = r$$

při čemž a, b, c, d, ... jsou určitá kladná čísla daná, též ukazovatelé α, β, γ, δ, ... kladní a celistvý, tvoříce v každém součinu levé strany určitý daný součet r, který arci musí

$$\leqq a + b + c + d \ldots,$$

a hovíce podmínkám z formule samé taktéž patrným

$$\alpha \leqq a, \quad \beta \leqq b, \quad \gamma \leqq c, \ldots$$

Větu lze přímo dokázati z nauky o kombinacích.

Z $a + b + c + d + \ldots$ prvků jest totiž kombinací třídy $r^{té}$ množství jediné a určité, a kombinace tyto obdržíme, se-