Václav Veselý

Elementární důkaz Hurwitzovy identity

Časopis pro pěstování matematiky a fysiky, Vol. 62 (1933), No. 4-5, 117--122

Persistent URL: http://dml.cz/dmlcz/123917

Elementární důkaz Hurwitzovy identity.

Napsal *Václav Veselý*.

(Došlo 2. října 1932.)

Bude dobře, budou-li zde uvedeny alespoň nejdůležitější informace o Waringově problému, při kterém se Hurwitzova identita objevila. Je to problém: *Najíti jest nejmenší číslo celé a kladné* $g(k)$ *takové, že každé číslo celé a kladné lze vyjádřiti jako součet* $g(k)$ *anebo méně* k*-tých mocnin celých kladných čísel. Při tom* k *je celé číslo* > 0. Jmenuje se Waringovým, protože Edward Waring v I. vydání svých Meditationes algebraicae (r. 1770) na str. 204 prvý, patrně z pouhé zkušenosti, prohlásil, že každé celé kladné číslo je součtem 9 anebo méně celých kladných krychlí a 19 anebo méně celých čtyřmocí atd.

Problém na počátku nevzbudil takřka zájmu, teprve od roku 1835 začínají se v literatuře objevovati rozmanitá pojednání o tomto problému. Velmi zevrubný, ač ne zcela úplný soupis této literatury do r. 1920 spolu se stručným resumé každého pojednání podává L. E. Dickson: History of the theory of numbers, II. díl, str. 717—729. Zde alespoň buď konstatováno, že metody, kterými bylo postupováno, jsou v podstatě tyto: metoda empirická, metoda identit (vycházející právě z identity Hurwitzovy) a pak analytické metody Hardy-Littlewoodovy a Winogradovovy.

Co do výsledků lze říci, že dosud je problém vyřešen v triviálním případě $k = 1$, kdy $g(1) = 1$, dále $g(2) = 4$ a $g(3) = 9$. Pro další k jsou pouhé odhady čísla $g(k)$. Velmi pěkný odhad pro libovolné k odvodili Hardy a Littlewood, ale jejich odhad netýká se čísla $g(k)$ samotného, nýbrž velmi blízkého čísla $G(k)$. Bylo-li by ale známo $G(k)$ pro nějaké k, pak ustanovení $g(k)$ pro totéž k je již věcí pouze počtářské trpělivosti.

Vedle těchto odhadů je ze starších prací důležitým výsledkem věta o existenci čísla $g(k)$. Je to věta Waring-Hilbertova: *Každé celé kladné číslo je součtem* N *anebo méně* k*-tých mocnin celých kladných čísel, při čemž* N *závisí jen na* k. Dokázal ji po prvé D. Hilbert r. 1909. Podstatnou částí jeho důkazu je důkaz identity Hurwitzovy, který podal s užitím integrálního počtu. Hurwitzova identita pro libovolné k, ale pouze pro $r = 4$, se po prvé objevila v Hurwitzově článku z r. 1908, před tím ovšem již byly známy některé její zvláštní případy. Téhož roku jako Hilbertův důkaz vyšel i Hausdorffův důkaz Hurwitzovy identity, provedený ale

také s užitím integrálního počtu. Důkaz Hausdorffův zjednodušil Stridsberg zavedením symbolické mocniny

$$h^\nu = \begin{cases} \dfrac{\nu!}{(\frac{1}{2}\nu)!} & \text{pro } \nu \equiv 0 \pmod 2 \\ 0 & \text{pro } \nu \equiv 1 \pmod 2 \end{cases}$$

ale při tom užití integrálního počtu zcela neodstranil. Nutno podotknouti, že podal celý důkaz Waring-Hilbertovy věty, a to způsobem odlišným od Hilbertova. Konečně jak Remak, tak i Frobenius upravili Stridsbergův důkaz Hurwitzovy identity tak, že odstranili vůbec užití integrálního počtu. Oppenheim r. 1930 podal celý důkaz Waring-Hilbertovy věty, a to v konečné fázi, k jaké se došlo ze Stridsbergova důkazu. Neužil ale symbolické mocniny h^ν, nýbrž vrátil se k užití integrálního počtu.

V dalším bude podán pouze důkaz Hurwitzovy identity na podkladě myšlenky Stridsbergovy a Frobeniovy. Bude ale potud jednodušší, že nebude užívati ani integrálního počtu ani symbolické mocniny.

Věta 1.: *Jestliže*

$$\mathrm{H}_n(x) = n! \cdot \sum_{i=0}^{[\frac{n}{2}]} (-1)^i \cdot \frac{x^{n-2i}}{i! \cdot (n-2 \cdot i)!} \qquad \text{pro celé } n \geqq 0 \tag{1}$$

a $\mathrm{H}_n(x) = 0$ pro celé $n < 0$,

pak je pro $n \geqq 1$ *derivace*

$$\mathrm{H}'_n(x) = n \cdot \mathrm{H}_{n-1}(x) \tag{2}$$

a $$\mathrm{H}_n(x) - x \cdot \mathrm{H}_{n-1}(x) + 2 \cdot (n-1) \cdot \mathrm{H}_{n-2}(x) = 0. \tag{3}$$

Důkaz: 1. Z (1) derivováním podle x plyne

$$\mathrm{H}'_n(x) = n! \cdot \sum_{i=0}^{[\frac{n-1}{2}]} (-1)^i \cdot \frac{x^{n-2i-1}}{i! \cdot (n-2 \cdot i-1)!} = n \cdot \mathrm{H}_{n-1}(x),$$

c. b. d.

2. Po uspořádání členů podle mocnin x na levé straně (3) je koeficient u x^{n-2r} pro $1 \leqq r \leqq \frac{1}{2}n$

$$\frac{n! \cdot (-1)^r}{r! \cdot (n-2 \cdot r)!} - \frac{(n-1)! \cdot (-1)^r}{r! \cdot (n-1-2 \cdot r)!} + \\ + \frac{2 \cdot (n-1) \cdot \{(n-2)!\} \cdot (-1)^{r-1}}{(r-1)! \cdot (n-2 \cdot r)!} = 0$$

a u x^n: $\dfrac{n!}{n!} - \dfrac{(n-1)!}{(n-1)!} = 0,$ c. b. d.

Věta 2.: *Jestliže pro všechna* $n \geqq 1$ *je*

$$(x-y) \cdot \mathrm{G}_n(x, y) = \mathrm{H}_n(x) \cdot \mathrm{H}_{n-1}(y) - \mathrm{H}_{n-1}(x) \cdot \mathrm{H}_n(y), \tag{4}$$

kdež x, y jsou nezávisle proměnné, pak

$$G_n(x, y) = (n-1)! \cdot \sum_{i=1}^{n} \frac{2^{i-1}}{(n-i)!} \cdot H_{n-i}(x) \cdot H_{n-i}(y). \qquad (5)$$

Důkaz: Dosadí-li se do (4) za $H_n(x)$ a $H_n(y)$ výrazy plynoucí z (3), je po úpravě

$$(x-y) \cdot G_n(x, y) = (x-y) \cdot H_{n-1}(x) \cdot H_{n-1}(y) + 2 \cdot (n-1) \cdot (x-y) \cdot G_{n-1}(x, y),$$

čili $$G_n(x, y) = H_{n-1}(x) \cdot H_{n-1}(y) + 2 \cdot (n-1) \cdot G_{n-1}(x, y),$$

což dává (5) vzhledem k tomu, že $G_1(x, y) = 1$, c. b. d.

Věta 3.: *Rovnice $H_n(x) = 0$ má n reálných navzájem různých kořenů.*

Důkaz: 1. Nechť má kořeny komplexní. Pak, značí-li α_1, α_2 dva její komplexně sdružené kořeny, je podle (5)

$$G_n(\alpha_1, \alpha_2) > 0 \text{ a podle (4) } (\alpha_1 - \alpha_2) \cdot G_n(\alpha_1, \alpha_2) = 0,$$

což je ve sporu. Rovnice $H_n(x) = 0$ nemůže tedy míti komplexní kořeny.

2. Že nemá ani kořeny vícenásobné, dokáže se úplnou indukcí. *a*) Nechť tvrzení platí pro $n = n_1$. Kdyby rovnice $H_{n_1+1}(x) = 0$ měla p-násobný kořen α, $p \geqq 2$, pak by jeho derivace musila míti týž kořen $(p-1)$-násobný, což vzhledem k (2), znamená, že $H_{n_1}(x) = 0$ má $(p-1)$-násobný kořen α. Pak z (3) pro $n = n_1 + 1$ plyne, že i $H_{n_1-1}(x) = 0$ má $(p-1)$-násobný kořen α. To znamená vzhledem k (2), že polynom $H_{n_1}(x)$ a jeho derivace mají společnou míru $(x-\alpha)^{p-1}$ čili, že $H_{n_1}(x) = 0$ musí míti kořen α p-násobný. To je ve sporu s předpokladem. Platí tedy tvrzení i pro $n = n_1 + 1$.

b) Rovnice $H_2(x) = 0$, t. j. $2 \cdot \frac{1}{2}x^2 - 2 = 0$ má kořeny reálné různé $x_1 = +\sqrt{2}$, $x_2 = -\sqrt{2}$. Tedy pro $n_1 = 2$ věta platí.

Platí tedy věta pro každé n, c. b. d.

Věta 4.: *Lze ustanoviti n reálných navzájem různých čísel β_i tak, že soustava n lineárních rovnic*

$$\sum_{i=1}^{n} \varrho_i \cdot \beta_i^{\nu} = c_\nu, \quad \nu = 0, 1, \ldots, n-1, \qquad (6)$$

kdež

$$c_\nu = \left\{ \begin{array}{ll} \dfrac{\nu!}{(\frac{1}{2}\nu)!} & \text{pro } \nu \equiv 0 \\ 0 & \text{pro } \nu \equiv 1 \end{array} \right\} \pmod 2 \qquad (7)$$

má řešení v číslech ϱ_i kladných.

Důkaz: Nechť čísla β_i jsou kořeny rovnice $H_n(x) = 0$. Pak determinant soustavy (6) je $\neq 0$ a tedy čísla ϱ_i jsou jednoznačně určena.

Buď dále n polynomů stupně $n - 1$

$$\mathrm{F}_r(x) = \frac{\mathrm{H}_n(x) \,.\, \mathrm{H}'_n(\beta_r)}{x - \beta_r} = \sum_{l=0}^{n-1} d_{r,l} \,.\, x^l, \quad r = 1, \ldots, n. \tag{8}$$

Protože podle (2) a (4) je $\mathrm{F}_r(x) = n \,.\, \mathrm{G}_n(x, \beta_r)$, je též

$$\mathrm{F}_r(x) = n! \,.\, \sum_{j=1}^{n} \frac{2^{j-1}}{(n-j)!} \,.\, \mathrm{H}_{n-j}(x) \,.\, \mathrm{H}_{n-j}(\beta_r), \quad r = 1, \ldots, n. \tag{9}$$

Porovnáním koeficientů u x^l na pravých stranách rovnic (8) a (9) dostane se

$$d_{r,l} = n! \,.\, \sum_{\substack{j=1 \\ n-j-l \equiv 0 \,(\mathrm{mod.}\, 2)}}^{n-l} \frac{2^{j-1}}{(n-j)!} \,.\, \frac{(n-j)! \,.\, (-1)^{\frac{n-j-l}{2}}}{\left(\frac{n-j-l}{2}\right)! \,.\, l!} \, H_{n-j}(\beta_r),$$

$$l = 0, 1, \ldots, n-1, \qquad r = 1, 2, \ldots, n$$

čili po úpravě, klade-li se $j = n - l - 2 \,.\, h$

$$d_{r,l} = \frac{n!}{l!} \,.\, \sum_{h=0}^{\left[\frac{n-l-1}{2}\right]} (-1)^h \,.\, \frac{2^{n-l-2h-1}}{h!} \,.\, H_{2h+l}(\beta_r), \quad \begin{matrix} l = 0, 1, \ldots, n-1 \\ r = 1, 2, \ldots, n \end{matrix} \tag{10}$$

Jestliže se nyní první rovnice soustavy (6) násobí číslem $d_{r,0}$, druhá $d_{r,1}$, třetí $d_{r,2}$, ..., n-tá $d_{r,n-1}$ a sečte-li se všech těch n rovnic, bude na levé straně výsledné rovnice vzhledem k (8)

$$\sum_{i=1}^{n} \frac{\mathrm{H}_n(\beta_i) \,.\, \mathrm{H}'_n(\beta_r)}{\beta_i - \beta_r} \,.\, \varrho_i = \varrho_r \,.\, \{\mathrm{H}'_n(\beta_r)\}^2$$

a na pravé

$$P = \sum_{\nu=0}^{n-1} c_\nu \,.\, d_{r,\nu} = \sum_{\mu=0}^{\left[\frac{n-1}{2}\right]} c_{2\mu} \,.\, d_{r,2\mu} =$$

$$= \sum_{\mu=0}^{\left[\frac{n-1}{2}\right]} \sum_{h=0}^{\left[\frac{n-2\mu-1}{2}\right]} \frac{(2\mu)! \, n!}{\mu! \, (2\mu)!} \,.\, (-1)^h \,.\, \frac{2^{n-2\mu-1-2h}}{h!} \,.\, \mathrm{H}_{2h+2\mu}(\beta_r).$$

Je-li konečně $\mu = t - h$, pak

$$P = \sum_{t=0}^{\left[\frac{n-1}{2}\right]} n! \,.\, 2^{n-1-2t} \,.\, \mathrm{H}_{2t}(\beta_r) \,.\, \sum_{h=0}^{t} \frac{(-1)^h}{h! \,.\, (t-h)!} = n! \,.\, 2^{n-1}.$$

Je tedy výsledná rovnice po úpravě

$$\varrho_r \cdot \{H'_n(\beta_r)\}^2 = n! \cdot 2^{n-1}$$

čili

$$\varrho_r = \frac{n! \cdot 2^{n-1}}{\{H'_n(\beta_r)\}^2} > 0.$$

Protože tato úvaha platí pro $r = 1, 2, 3, \ldots, n.$ plyne z toho, že jsou-li čísla β_i kořeny rovnice $H_n(x) = 0.$ má soustava (6) řešení v číslech ϱ_i kladných, c. b. d.

Věta 5.: *Lze ustanoviti n racionálních navzájem různých čísel $\bar{\beta}_i$ tak, že soustava (6) má řešení v číslech $\bar{\varrho}_i$ racionálních kladných.*

Důkaz: Podle (6) jsou ϱ_i spojitými funkcemi proměnných β_i v bodech $[\beta_1, \ldots, \beta_n]$, když determinant soustavy $\neq 0$. To znamená, že lze ustanoviti takové okolí bodu $[\beta_1, \ldots, \beta_n]$, že čísla ϱ_i nebudou měnit znaménko, budou-li β_i v tom okolí. Jsou-li β_i kořeny rovnice $H_n(x) = 0$, pak lze voliti v tom jistém okolí bodu $[\beta_1, \ldots, \beta_n]$ takový bod $[\bar{\beta}_1, \ldots, \bar{\beta}_n]$, že $\bar{\beta}_i$ budou navzájem různá a racionální a $\varrho_i = \bar{\varrho}_i$ jim příslušná podle (6) tudíž racionální a také kladná, c. b. d.

Věta 6.: *Pro všechna celá $m < n$ a všechna celá $r > 0$ platí identita v $x_1, \ldots, x_r$*

$$\sum_{v_1,\ldots,v_r=1}^{n} \varrho_{v_1} \cdot \varrho_{v_2} \cdots \varrho_{v_r} (\beta_{v_1} x_1 + \ldots + \beta_{v_r} x_r)^m = c_m (x_1^2 + \ldots + x_r^2)^{\frac{m}{2}}, \tag{11}$$

kdež $\beta_1, \ldots, \beta_n$ je n navzájem různých reálných čísel a $\varrho_1, \ldots, \varrho_n$ jsou čísla daná rovnicemi (6) a c_i rovnicemi (7).

Důkaz: Podle polynomické věty je levá strana (11)

$$m! \sum_{v_1,\ldots,v_r=1}^{n} \varrho_{v_1} \cdots \varrho_{v_r} \sum_{\substack{\mu_1+\ldots+\mu_r=m \\ \mu_i \geqq 0}} \prod_{i=1}^{r} \frac{x_i^{\mu_i} \beta_{v_i}^{\mu_i}}{\mu_i!} =$$

$$= m! \sum_{\substack{\mu_1+\ldots+\mu_r=m \\ \mu_i \geqq 0}} \prod_{i=1}^{r} \frac{x_i^{\mu_i}}{\mu_i!} \sum_{v=1}^{n} \varrho_v \cdot \beta_v^{\mu_i} .$$

Z toho plyne vzhledem k (6) a (7), že (11) platí pro m liché.

Pro m sudé musí býti vzhledem k (6) a (7) $\mu_i = 2\nu_i$, $i = 1 \ldots r$ a tedy je levá strana (11) rovna

$$m! \sum_{\substack{\nu_1+\ldots+\nu_r=\frac{m}{2} \\ \nu_i \geqq 0}} \prod_{i=1}^{r} \frac{x_i^{2\nu_i}}{(2 \cdot \nu_i)!} \cdot \frac{(2 \cdot \nu_i)!}{\nu_i!} = \frac{m!}{(\frac{1}{2}m)!} \cdot (x_1^2 + \ldots + x_r^2)^{\frac{m}{2}}$$

c. b. d.

Věta 7. (Hurwitzova identita): *Ať jsou m a r jakákoli celá čísla > 0, platí vždy identita v $x_1, \ldots, x_r$*

$$(x_1^2 + \ldots + x_r^2)^m = \sum_{i=1}^{M} R_i (e_{i,1} x_1 + \ldots + e_{i,r} x_r)^{2m}, \tag{12}$$

kdež celá čísla $e_{i,j}$, racionální kladná čísla R_i a celé kladné číslo M jsou závislá pouze na m a r.

Důkaz: Podle věty 5. pro $n = m + 1$ lze určiti racionální čísla $\overline{\beta_i} = \frac{\gamma_i}{\delta_i}$, $i = 1, 2, \ldots, m + 1$, kdež γ_i a δ_i jsou celá čísla, tak, že čísla $\overline{\varrho_i}$ jim příslušná podle (6) jsou racionální a kladná. Z povahy určení čísel $\overline{\beta_i}$ i $\overline{\varrho_i}$ plyne, že čísla γ_i, δ_i i $\overline{\varrho_i}$ jsou závislá jen na m. Jestliže se nyní dosadí do (11) pro $n = m + 1$ za $\beta_i = \overline{\beta_i}$ a $\varrho_i = \overline{\varrho_i}$, dělí-li se rovnice (11) c_m a vytkne-li se z každé závorky na levé straně (11) $\left(\frac{1}{\delta_{v_1} \cdot \delta_{v_2} \ldots \delta_{v_r}}\right)^m$ dostane se identita (12) s čísly

$$R_i = \frac{\varrho_{v_1} \cdot \varrho_{v_2} \ldots \varrho_{v_r}}{(\delta_{v_1} \cdot \delta_{v_2} \ldots \delta_{v_r})^m \cdot c_m}, \quad e_{i,j} = \gamma_{v_j}, \quad i = 1, 2, \ldots, M,$$

kdež $v_1, \ldots, v_r$ je nějaká variace s opakováním r-té třídy z $m + 1$ čísel $1, 2, \ldots, m + 1$. Jsou tedy čísla R_i racionální kladná a závislá jen na m, r, čísla $e_{i,j}$ celá a závislá jen na m.

Konečně číslo $M = (m + 1)^r$ je celé a závislé jen na m, r, c. b. d.

*

Une démonstration élémentaire de l'identité de Hurwitz.

(Extrait de l'article précédent.)

L'auteur démontre l'identité de Hurwitz en se basant sur la démonstration de Stridsberg et de Frobenius, mais sans employer ni le calcul intégral ni la puissance symbolique h^v.

*

Literatura: A. Hurwitz: Über die Darstellung der ganzen Zahlen als Summen von n-ten Potenzen ganzer Zahlen; Math. An., sv. 65 (1908), 424—427.

D. Hilbert: Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsche Problem); vyšlo jednak v Nachrichten v. d. k. Ges. zu Göttingen, 1909, str. 17—36, a jednak s jistými změnami v Math. An., sv. 67 (1909), 281—300.

F. Hausdorff: Zur Hilbertschen Lösung des Waringschen Problems; Math. An., sv. 67. (1909), 301—305.

E. Stridsberg: Öfver Hilberts bevis för Warings sats; Arkiv för Mat., Astr. och Fys., sv. 6 (1910—1911). Výtah z toho: Sur la démonstration de M. Hilbert du théorème de Waring; Math. An., sv. 72 (1912), 145—152.

R. Remak: Bemerkung zu Herren Stridsbergs Beweis des Waringschen Theorems; Math. An., sv. 72 (1912), 153—156.

G. Frobenius: Über den Stridsbergschen Beweis des Waringschen Satzes; Sitzungsberichte d. k. preus. Ak. d. Wis. zu Berlin, 1912, 2. sv., str. 666—670.

E. Schmidt: Zum Hilbertschen Beweise des Waringschen Theorems; Math. An., sv. 74 (1913), 271—274.

A. Oppenheim: Hilbert's proof of Waring's theorem (as improved by Hausdorff and Stridsberg); The Mes. of Math., sv. 58 (1930), 153—158.