Časopis pro pěstování matematiky a fysiky

E. Bunický

O jedné soustavě kongruencí, související s Wilsonovou větou

Časopis pro pěstování matematiky a fysiky, Vol. 69 (1940), No. 3-4, 97--109

Persistent URL: http://dml.cz/dmlcz/123327

ČASOPIS PRO PĚSTOVÁNÍ MATEMATIKY A FYSIKY

ČÁST MATEMATICKÁ

O jedné soustavě kongruencí, související s Wilsonovou větou.

E. Bunický, Praha.

(Došlo dne 3. února 1940.)

§ 1. Budeme častěji vyšetřovati základní symetrické funkce $s_1, s_2, \ldots, s_{m-1}$ čísel

$$1, 2, \ldots, m-1, \qquad (1)$$

kdež m je jisté celé kladné číslo, t. j. součet s_1 čísel (1), součty $s_2, s_3, \ldots, s_{m-2}$ všech součinů čísel (1) po dvou, po třech, ..., po $m-2$ a konečně součin $(m-1)! = s_{m-1}$. Symbol s_ν značí v následujícím vždy základní symetrickou funkci řady čísel tvaru (1) (při čemž index ν jest roven některému členu řady (1)), definovanou číslem ν, jež musí býti dáno v každém jednotlivém případě. Tvar řady (1), jež obsahuje všechna přirozená čísla menší než m, naznačuje, že m má býti větší než 1. Přes to, užíváme-li výrazů s_ν, jest vhodno, zdůrazniti výslovně nerovnost $m > 1$, zvláště vzhledem k tomu, že se v kombinatorických vzorcích připisuje symbolu $(m-1)! = s_{m-1}$ pro $m = 1$ hodnota $0! = 1$.

Je známo, že kongruence

$$(p-1)! + 1 \equiv 0 \pmod{p} \qquad (2)$$

vyjadřuje — podle Wilsonovy věty — nutnou a postačující podmínku, aby číslo p, celé a větší než 1, bylo prvočíslem (v čemž jest zahrnuto i sudé prvočíslo 2). Můžeme tedy říci, že kongruence (2) *charakterisuje* všechna prvočísla. Z kongruence

$$(x-1)(x-2)\ldots(x-(p-1)) - (x^{p-1}-1) \equiv 0 \pmod{p},$$

platné identicky, když p je prvočíslo, je dále patrno, že každé *liché* prvočíslo p splňuje vedle kongruence (2) ještě také soustavu kongruencí

$$s_1 \equiv 0 \pmod{p}, \; s_2 \equiv 0 \pmod{p}, \ldots, s_{p-2} \equiv 0 \pmod{p}, \qquad (3)$$

kde výrazy $s_1, s_2, \ldots, s_{p-2}$ jsou vytvořeny pro řadu čísel $1, 2, \ldots,$

$\ldots, p-1$. Tato soustava se redukuje na jedinou kongruenci tehdy a jen tehdy, je-li $p = 3$.

Dokažme nyní tuto větu: *soustava kongruencí* (3) *charakterisuje všechna lichá prvočísla, to jest: tato soustava vyjadřuje podmínku nutnou a postačující k tomu, aby celé číslo p, větší než* 1, *bylo lichým prvočíslem.* Předně každé liché prvočíslo p vyhovuje soustavě kongruencí (3). Budiž za druhé p celé číslo větší než 1, splňující soustavu (3). Podle první kongruence této soustavy je podíl $s_1 : p = \frac{1}{2}p\,(p-1) : p = \frac{1}{2}\,(p-1)$ číslo celé, takže p je liché. Vyšetřujme nyní kongruenci

$$(x-1)\,(x-2)\ldots(x-(p-1)) \equiv 0 \pmod{p}, \tag{4}$$

kterou lze psáti ve tvaru

$$x^{p-1} - s_1 x^{p-2} + s_2 x^{p-3} - \ldots + (-1)^k s_k x^{p-k-1} + \ldots + \\ + (-1)^{p-2} s_{p-2} x + (-1)^{p-1} \cdot (p-1)! \equiv 0 \pmod{p},$$

nebo, přihlížíme-li k soustavě kongruencí (3) a k okolnosti, že p je liché, v ekvivalentním tvaru

$$x^{p-1} + (p-1)! \equiv 0 \pmod{p}. \tag{4'}$$

Kongruence (4), a tedy i ekvivalentní kongruence (4'), má zřejmě kořen $x = 1$, z čehož plyne $(p-1)! + 1 \equiv 0 \pmod{p}$. Liché číslo p je tedy prvočíslem, čímž věta dokázána.

§ 2. Zjistíme za chvíli, že jest možno, nahraditi soustavu (3) soustavou kongruencí, která jest pouze částí soustavy (3), a která přes to charakterisuje všechna lichá prvočísla. Napřed však dokážeme tuto větu[1]): *Každé číslo celé M, větší než* 1, *splňuje vztah*

$$2s_{2k+1} \equiv 0 \pmod{M}, \tag{5}$$

kdež k je celé nezáporné číslo a $2k+1$ *je kterékoliv liché kladné číslo, jež není větší než* $M-1$; *při tom značí* s_{2k+1} *základní symetrickou funkci čísel*

$$1, 2, \ldots, M-1, \tag{6}$$

definovanou indexem $2k+1$.

Předpokládejme napřed, že jest $1 < 2k+1 < M-1$, čili, což značí totéž, $0 < k < \frac{1}{2}\,(M-2)$. V tomto případě značí s_{2k+1} součet všech součinů po $2k+1$ z čísel (6). Budiž

$$\alpha_1 \alpha_2 \ldots \alpha_{2k+1} \tag{7}$$

součin $2k+1$ různých čísel $\alpha_1, \alpha_2, \ldots, \alpha_{2k+1}$, vybraných libovolně mezi čísly (6). Výraz

$$(M-\alpha_1)\,(M-\alpha_2)\ldots(M-\alpha_{2k+1}) \tag{7'}$$

[1]) Tato věta byla dokázána autorem v článku „Zamečanije po povodu teoremy Wilsona", Učenyja Zapisky, Praha 1925.

je také jedním z těchto součinů, a systém všech výrazů (7'), příslušných ke všem součinům (7), je zřejmě totožný se systémem všech součinů (7). Následkem toho jest

$$s_{2k+1} = \Sigma \alpha_1\alpha_2 \ldots \alpha_{2k+1} = \Sigma (M - \alpha_1)(M - \alpha_2) \ldots (M - \alpha_{2k+1}),$$

kdež součty Σ se vztahují ke všem $\binom{M}{2k+1}$ kombinacím čísel (6) po $2k + 1$. Odtud plyne

$$s_{2k+1} = \Sigma \alpha_1\alpha_2 \ldots \alpha_{2k+1} = \Sigma (M - \alpha_1)(M - \alpha_2) \ldots (M - \alpha_{2k+1}) \equiv$$
$$\equiv (-1)^{2k+1} \Sigma \alpha_1\alpha_2 \ldots \alpha_{2k+1} = -s_{2k+1} \pmod{M},$$

čímž kongruence (5) dokázána. Podobně se dokáže kongruence (5) v obou krajních případech, kdy jest buďto $2k + 1 = 1$, t. j. $k = 0$ nebo $1 < 2k + 1 = M - 1$, t. j. $0 < k = \frac{1}{2}(M - 2)$. V prvním případě stačí nahraditi $\Sigma \alpha_1\alpha_2 \ldots \alpha_{2k+1}$ a $\Sigma (M - \alpha_1) \ldots (M - \alpha_2) \ldots (M - \alpha_{2k+1})$ výrazy $\Sigma \alpha$ resp. $\Sigma (M - \alpha)$, kdež se sčítá přes všechna čísla řady (6). V druhém krajním případě nahradíme součty

$\Sigma \alpha_1\alpha_2 \ldots \alpha_{2k+1}$ a $\Sigma (M - \alpha_1)(M - \alpha_2) \ldots (M - \alpha_{2k+1})$ resp. součiny $\alpha_1\alpha_2 \ldots \alpha_{2k+1} = \alpha_1\alpha_2 \ldots \alpha_{M-1}$ a $(M - \alpha_1)(M - \alpha_2) \ldots (M - \alpha_{2k+1}) = (M - \alpha_1)(M - \alpha_2) \ldots (M - \alpha_{M-1})$,

kdež řada čísel $\alpha_1, \alpha_2, \ldots, \alpha_{M-1}$ splývá s řadou (6).

Poznámka. Předpoklad $1 < 2k + 1 < M - 1$ čili $0 < k < \frac{1}{2}(M - 2)$ je splnitelný pouze pro $M > 2$ a předpoklad $1 < 2k + 1 = M - 1$ čili $0 < k = \frac{1}{2}(M - 2)$ je splnitelný pouze pro M sudé a větší než 2.

Je-li M liché, můžeme nahraditi kongruenci (5) ekvivalentní kongruencí

$$s_{2k+1} \equiv 0 \pmod{M}. \qquad (5')$$

Tím dostáváme větu: *Každé celé liché číslo M větší než 1 splňuje kongruence (5'), kde index $2k + 1$ probíhá všechny liché hodnoty $1, 3, 5, \ldots, M - 2$ a kde symetrické funkce s_{2k+1} jsou vytvořeny pro řadu čísel $1, 2, \ldots, M - 1$.* Této pomocné věty užijeme k důkazu následující věty.

Věta I. a) *Buďte $s_1, s_2, \ldots, s_{p-1}$ základní symetrické funkce $p - 1$ čísel*

$$1, 2, \ldots, p - 1. \qquad (8)$$

Vyšetřujme systém kongruencí

$$s_1 \equiv 0, s_2 \equiv 0, s_4 \equiv 0, \ldots, s_{2l} \equiv 0 \pmod{p}, \qquad (3')$$

kde p je celé číslo větší než 1 a kde indexy $2, 4, \ldots, 2l$ probíhají všechny sudé hodnoty, ležící v uzavřeném intervalu $\langle 2, 2l \rangle$, kde $2l$

je největší sudé číslo splňující nerovnost

$$2l < p - 1. \qquad (9)$$

Pro $p = 2$ *a pro* $p = 3$ *redukujeme systém* (3′) *na první kongruenci* $s_1 \equiv 0 \pmod{p}$. *Jest dokázati, že systém* (3′) *dává nutnou a postačující podmínku pro to, aby číslo* p, *větší než* 1, *bylo lichým prvočíslem; jinak řečeno, systém kongruencí* (3′) *charakterisuje všechna lichá prvočísla.*

b) *Vyhovuje-li celé číslo* p, *větší než* 1, *systému* (3′), *je* p *liché, a systém* (3′), *je-li* $p > 3$, *splývá se systémem kongruencí*

$$s_1 \equiv 0, s_2 \equiv 0, s_4 \equiv 0, \ldots, s_{p-3} \equiv 0 \pmod{p}. \qquad (3^*)$$

Dokažme tvrzení a); současně obdržíme během důkazu tvrzení b). Podmínky (3′) jsou nutné, aby p bylo liché prvočíslo. Vskutku, je-li p liché prvočíslo větší než 3, vyhovuje kongruencím (3) a v tomto případě největší sudé číslo $2l$, vyhovující nerovnosti (9), je $p - 3$; tedy systém (3′) splývá se systémem (3*). Dále prvočíslo $p > 3$ vyhovuje jistě systému (3*), jehož všechny kongruence patří k systému (3). Ale systémy (3*), (3′) jsou totožné. Tedy každé liché prvočíslo větší než 3 vyhovuje systému (3′). Liché prvočíslo $p = 3$ vyhovuje kongruenci $s_1 = \tilde{1} + 2 \equiv 0 \pmod{p = 3}$, na kterou se redukuje v tomto případě systém (3) a tedy, podle naší úmluvy, učiněné ve znění věty I, číslo $p = 3$ vyhovuje systému kongruencí (3′). Tedy všechna lichá prvočísla p vyhovují systému (3′).

Budiž za druhé p celé číslo větší než 1, vyhovující systému (3′). Podle první z těchto kongruencí je číslo p liché a tedy větší než 2. Je-li liché číslo p větší než 3, potom největší sudé číslo $2l$ hovící nerovnosti (9) je $p - 3$ a tedy systém (3′) nabývá pro takové p tvaru (3*); tím je tvrzení b) dokázáno. Vraťme se k tvrzení a). Celé číslo $p > 1$, vyhovující systému (3′), je, jak jsme viděli, liché; je tedy buďto $p > 3$ nebo $p = 3$. Je-li $p > 3$, potom systém (3′), kterému p podle předpokladu vyhovuje, má tvar (3*), jak jsme seznali. Podle poslední pomocné věty vyhovuje liché číslo p také všem kongruencím $s_3 \equiv 0$, $s_5 \equiv 0, \ldots, s_{p-2} \equiv 0 \pmod{p}$, které dohromady se systémem (3*) dávají právě celý systém (3). Tedy vyšetřované číslo p, vyhovující systému (3′) a větší než 3, vyhovuje také všem kongruencím systému (3) a tedy je číslo p liché prvočíslo. Zbývá případ $p = 3$. Číslo $p = 3$ vyhovuje systému (3′), který se v tomto případě redukuje na jedinou kongruenci $s_1 \equiv 0 \pmod{p = 3}$ a vedle toho je $p = 3$ liché prvočíslo. Tedy platí ve všech případech: jestliže celé číslo $p > 1$ vyhovuje systému (3′), je p liché prvočíslo.[2])

[2]) Formálně lze systém (3′) napsati pro každé celé číslo $p > 1$. Ale pro sudé prvočíslo 2 a pro složená čísla není tento systém splněn; je právě splněn pouze pro lichá prvočísla.

§ 3. Je možno si položiti otázku, zda není možno vynechati ze systému (3′) některé kongruence tak, aby zbývající systém stále ještě charakterisoval všechna lichá prvočísla. Nerozřešíme úplně tuto otázku, budeme však vyšetřovati některé zvláštní případy. Napřed dokážeme některé pomocné věty. Buďte s_ϱ ($\varrho = 1, 2, \ldots, n$) základní symetrické funkce n čísel

$$1, 2, \ldots, n, \tag{10}$$

kde n je jakékoliv celé číslo větší než 1. Položme nadto $s_\varrho = \sigma(\varrho, n)$, abychom jasněji vyznačili závislost funkcí s_ϱ na obou parametrech ϱ, n. Funkce $\sigma(\varrho, n)$ vyhovují zřejmě vztahům

$$\sigma(k+1, n+1) = \sigma(k+1, n) + (n+1)\,\sigma(k, n) \qquad (k = 1, 2, \ldots, n-1),$$

které lze psáti ve tvaru[3])

$$\Delta\sigma(k+1, n) = (n+1)\,\sigma(k, n) \quad (k = 1, 2, \ldots, n-1), \tag{11}$$

kde znamení diferenční Δ se vztahuje na proměnnou n, jež má obdržeti přírůstek 1. Označme znakem $(n+1)^{l|1}$ faktoriál

$$(n+1)\,n\,(n-1)\ldots(n+1-(l-1)) = (n+1)\,n\,(n-1)\ldots \ldots(n-l+2),$$

kde l je libovolné celé kladné číslo. Pro tento faktoriál platí

$$(n+1)\,(n+1)^{l|1} = l\,(n+1)^{l|1} + (n+1)^{l+1|1}. \tag{12}$$

Ze známé formule

$$\sigma(1, n) = \tfrac{1}{2}\,(n+1)\,n = \tfrac{1}{2}\,(n+1)^{2|1} \tag{13}$$

a ze vztahu (12) můžeme počítati postupně výrazy $\sigma(2, n), \sigma(3, n), \ldots \ldots, \sigma(k, n)$ ($k \leqq n$), užívajíce rovnice (11). Tak jest

$$\Delta\sigma(2, n) = (n+1)\,\sigma(1, n) = \tfrac{1}{2}\,(n+1)\,(n+1)^{2|1} = \\ = \tfrac{1}{2}\,(2\,(n+1)^{2|1} + (n+1)^{3|1}).$$

čili

$$\Delta\sigma(2, n) = (n+1)^{2|1} + \tfrac{1}{2}\,(n+1)^{3|1}.$$

Sčítáme-li obě strany, dostaneme

$$\sigma(2, n) = \tfrac{1}{3}\,(n+1)^{3|1} + \tfrac{1}{8}\,(n+1)^{4|1} + c,$$

kde c je konstanta; pro $n = 2$ obdržíme (poznamenejme, že $(n+1)^{l|1}$ vymizí pro $n = 0, 1, 2, \ldots, l-2$)

$$\sigma(2, 2) = 2! = \tfrac{1}{8}\,3^{4|1} + \tfrac{1}{8}\,3^{3|1} + c = 2! + c,$$

odkud $c = 0$ a

[3]) Můžeme potlačiti podmínku $n > 1$ a připustiti pro n všechna celá kladná čísla, klademe-li $\sigma(0, n) = 1$ pro každé n. Tato úmluva dovoluje psáti rovnici (11) pro $k = 0$ ve tvaru $\Delta\sigma(1, n) = n + 1$, i když $n = 1$. Sečteme-li obě strany a použijeme rovnice $\sigma(1, 1) = 1$, obdržíme známý vzorec (13).

$$\sigma(2, n) = \tfrac{1}{3}(n+1)^{3|1} + \tfrac{1}{8}(n+1)^{4|1} = \frac{n(n^2-1)(3n+2)}{24}. \qquad (14)$$

Podobně obdržíme postupně

$$\Delta\sigma(3, n) = (n+1)\,\sigma(2, n) = (n+1)\left[\tfrac{1}{3}(n+1)^{3|1} + \tfrac{1}{8}(n+1)^{4|1}\right] =$$
$$= (n+1)^{3|1} + \tfrac{1}{3}(n+1)^{4|1} + \tfrac{1}{2}(n+1)^{4|1} + \tfrac{1}{8}(n+1)^{5|1} =$$
$$= (n+1)^{3|1} + \tfrac{5}{6}(n+1)^{4|1} + \tfrac{1}{8}(n+1)^{5|1},$$
$$\sigma(3, n) = \tfrac{1}{4}(n+1)^{4|1} + \tfrac{1}{6}(n+1)^{5|1} + \tfrac{1}{48}(n+1)^{6|1} + c.$$

Položíme-li $n = 3$, obdržíme

$$\sigma(3, 3) = 3! = \tfrac{1}{4}\,4! + c = 3! + c,\ c = 0,$$

odkudž

$$\sigma(3, n) = \tfrac{1}{4}(n+1)^{4|1} + \tfrac{1}{6}(n+1)^{5|1} + \tfrac{1}{48}(n+1)^{6|1} =$$
$$= \tfrac{1}{48}n^2(n+1)^2(n^2-3n+2). \qquad (15)$$

Dokážeme, že se funkce $\sigma(k, n)$ $(k = 1, 2, \ldots, n)$ dá vyjádřiti mnohočlenem v n stupně $2k$ tvaru

$$\sigma(k, n) = a_{k,k+1}(n+1)^{k+1|1} + \sum_{\nu=k+2}^{2k-1} a_{k\nu}(n+1)^{\nu|1} + a_{k,2k}(n+1)^{2k|1}, \qquad (16)$$

kde a_{kl} $(l = k+1,\ k+2, \ldots, 2k-1,\ 2k)$ jsou racionální konstanty. První a poslední z těchto koeficientů jsou dány rovnicemi

$$a_{k,k+1} = \frac{1}{k+1}, \qquad (17)$$

$$a_{k,2k} = \frac{1}{2^k \cdot k!}; \qquad (17')$$

ostatní koeficienty jsou, pro $k > 1$, dány rekurentním vzorcem

$$a_{k+1,\nu} = \frac{(\nu-1)\,a_{k,\nu-1} + a_{k,\nu-2}}{\nu} \qquad (18)$$
$$(k > 1;\ \nu = k+3, k+4, \ldots, 2k, 2k+1).$$

Abychom tyto vzorce dokázali, poznamenejme především, že vzorce (16), (17), (17′) jsou podle rovnic (14), (15) správné pro $k = 2$ a $k = 3$. Zůstávají správnými též pro $k = 1$: neboť v tomto případě podle (13) platí $a_{1,2} = \frac{1}{2} = \frac{1}{1+1} = \frac{1}{2^1 \cdot 1!}$. Pro $k = 1$ a $k = 2$ stačí vzorce (17), (17′) k určení koeficientů $a_{k,\nu}$; pro $k = 3$ potřebujeme vedle vzorců (17), (17′) ještě $a_{3,5}$; příslušná rovnice (18) se redukuje na $a_{3,5} = \frac{1}{5}(4a_{2,4} + a_{2,3})$, kterážto je správná, neboť $a_{3,5} = \frac{1}{6}$, $a_{2,4} = \frac{1}{8}$, $a_{2,3} = \frac{1}{3}$. Předpokládejme tedy,

že vzorce (16), (17), (17′) platí pro jistou hodnotu k, kde $3 \leqq k < n$, a dokažme, že tyto formule platí i tehdy, píšeme-li $k+1$ místo k a že koeficienty $a_{k+1,\nu}$ ($\nu = k+3, k+4, \ldots, 2k+1$) vyhovují vztahům (18). K tomu cíli dosaďme do rovnice (11) místo $\sigma(k, n)$ pravou stranu rovnice (16). Obdržíme postupně, užívajíce vztahu (12),

$$\Delta\sigma(k+1, n) = (n+1) \sum_{\lambda=k+1}^{2k} a_{k,\lambda} (n+1)^{\lambda|1} =$$

$$= \sum_{\lambda=k+1}^{2k} a_{k,\lambda} (\lambda (n+1)^{\lambda|1} + (n+1)^{\lambda+1|1}),$$

$$\Delta\sigma(k+1, n) = (k+1)\, a_{k,k+1} (n+1)^{k+1|1} +$$

$$+ \sum_{\varrho=k+2}^{2k} (\varrho a_{k,\varrho} + a_{k,\varrho-1}) (n+1)^{\varrho|1} + a_{k,2k} (n+1)^{2k+1|1}.$$

Sčítáme-li na obou stranách, obdržíme

$$\sigma(k+1, n) = \frac{k+1}{k+2} a_{k,k+1} (n+1)^{k+2|1} +$$

$$+ \sum_{\varrho=k+2}^{2k} \frac{\varrho a_{k,\varrho} + a_{k,\varrho-1}}{\varrho+1} \cdot (n+1)^{\varrho+1|1} + \frac{a_{k,2k}}{2k+2} (n+1)^{2k+2|1} + c,$$

kde c je konstanta. Položíme-li $n = k+1$, užijeme-li vzorce (17) a vynecháme členy, které se rovnají nule pro $n = k+1$, obdržíme $\sigma(k+1, k+1) = (k+1)! = \frac{k+1}{k+2} a_{k,k+1}(k+2)! + c =$ $= (k+1)! + c$, takže $c = 0$. Dále máme podle vzorců (17), (17′)

$$\frac{k+1}{k+2} a_{k,k+1} = \frac{1}{k+2}, \quad \frac{a_{k,2k}}{2k+2} = \frac{1}{2^{k+1} \cdot (k+1)!}.$$

Položíme-li tedy $\varrho + 1 = \nu$, vychází

$$\sigma(k+1, n) = \frac{1}{k+2} (n+1)^{k+2|1} + \sum_{\nu=k+3}^{2k+1} \frac{(\nu-1)\, a_{k,\nu-1} + a_{k,\nu-2}}{\nu} \cdot$$

$$\cdot (n+1)^{\nu|1} + \frac{1}{2^{k+1} \cdot (k+1)!} (n+1)^{2k+2|1}.$$

Můžeme tedy psáti $\sigma(k+1, n)$ ve tvaru

$$\sigma(k+1, n) = a_{k+1,k+2} (n+1)^{k+2|1} + \sum_{\nu=k+3}^{2k+1} a_{k+1,\nu} (n+1)^{\nu|1} + \tag{19}$$

$$+ a_{k+1,2k+2} (n+1)^{2k+2|1},$$

kde koeficienty $a_{k+1,\lambda}$ ($\lambda = k+2, k+3, \ldots, 2k+2$) vyhovují

rovnicím

$$a_{k+1,k+2} = \frac{1}{k+2}, \quad a_{k+1,2k+2} = \frac{1}{2^{k+1} \cdot (k+1)!},$$

$$a_{k+1,\nu} = \frac{(\nu - 1)\, a_{k,\nu-1} + a_{k,\nu-2}}{\nu} \quad (\nu = k+3, k+4, \ldots, 2k+1). \tag{19'}$$

Z toho je patrno, že vzorce (16), (17), (17'), (18) platí obecně. Neboť podle (19), (19') obdržíme obecný tvar funkce $\sigma(k+1, n)$ a výrazy pro první a poslední koeficient na pravé straně, nahradíme-li ve vzorcích (16), (17), (17') (jež pro naši hodnotu k považujeme za správné) číslo k číslem $k+1$; mimo to, podle poslední rovnice (19'), vyhovují koeficienty $a_{k+1,\nu}$ ($\nu = k+3$, $k+4, \ldots, 2k+1$) rekurentním relacím (18).

Poznamenejme, že pravá strana vzorce (16) je dělitelna mnohočlenem $(n+1)^{k+1|1}$. Z toho plyne

$$\sigma(k, n) = \frac{(n+1)^{k+1}\, \psi_{k-1}(n)}{\delta_k}$$

nebo

$$\sigma(k, n) = \frac{(n+1)\, n\, (n-1) \ldots (n-k+1)\, \psi_{k-1}(n)}{\delta_k}, \tag{20}$$

kde $\psi_{k-1}(n)$ je polynom stupně $k-1$ v proměnné n s celými součiniteli, kteří mají pro danou hodnotu k hodnoty úplně určené rovnicemi (17), (17'), (18) a kde δ_k je celé kladné číslo, které podle vzorců (16), (17') je násobkem čísla $2 \cdot 4 \ldots 2k = 2^k \cdot k!$. Ježto celistvé číslo k je nejméně rovno jedné, lze psáti rovnici (20) pro všechny přípustné hodnoty $1, 2, \ldots, n$ čísla k ve tvaru

$$\sigma(k, n) = \frac{(n+1)\, n\, \eta_{2k-2}(n)}{\delta_k}, \tag{20*}$$

kde $\eta_{2k-2}(n)$ je mnohočlen stupně $2k-2$ v proměnné n, s celistvými koeficienty, určenými pro každou hodnotu čísla k.

§ 4. **Věta II.** a) *Žádná kongruence tvaru*

$$s_k \equiv 0 \pmod{p}, \tag{21}$$

kde k je dané celé kladné číslo a kde s_k značí základní symetrickou funkci čísel

$$1, 2, \ldots, p-1, \tag{8'}$$

nemůže charakterisovati všechna prvočísla p, hovící nerovnosti

$$p > k+1. \tag{22}$$

b) *Budiž m celé číslo větší než 1, libovolně dané. Žádný systém kongruencí*

$$s_{k_\nu} \equiv 0 \pmod{p} \quad (\nu = 1, 2, \ldots, m), \tag{23}$$

kde $k_1, k_2, \ldots, k_m$ je m různých celých kladných čísel a kde s_{k_ν} značí základní symetrické funkce čísel (8'), *nemůže charakterisovati všechna prvočísla p, hovící nerovnosti*

$$p > \text{maximum}\,(k_1, k_2, \ldots, k_m) + 1. \qquad (22')$$

Poznámka. Podle definice funkce $s_k = \sigma(k, p-1)$ je $k \leqq p-1$. Ale rovnost $k = p-1$ je v části a) věty II nemožná, neboť pro prvočíslo p a pro $k = p-1$ by platil místo kongruence (21), jež má tvar $s_k = s_{p-1} \equiv 0 \pmod p$, vztah $s_{p-1} \equiv -1 \pmod p$. Je tedy nutno omeziti číslo p podmínkou $k < p-1$, t. j. nerovností (22). Podobně je p v části b) omezeno analogickou nerovností (22').

Důkaz. Abychom dokázali tvrzení a), stačí, najdeme-li složené číslo p, které vyhovuje kongruenci (21) a nerovnosti (22). Položíme-li[4]) ve vzorci (20*) $n = p-1$ a označíme $\eta_{2k-2}(p-1)$ znakem $f(p)$, kde $f(p)$ je stejně jako $\eta_{2k-2}(p-1)$ mnohočlen v p s celistvými součiniteli, můžeme psáti kongruenci (21) ve tvaru

$$\frac{p\,(p-1)\,f(p)}{\delta_k} \equiv 0 \pmod p, \text{ čili } (p-1)\,f(p) \equiv 0 \pmod{\delta_k}.$$

Tato kongruence má kořen $p \equiv 1 \pmod{\delta_k}$. Položíme-li tedy $p = (1+\delta_k)^\varrho$, kde ϱ je libovolné celé číslo větší než 1, bude $p \equiv 1 \pmod{\delta_k}$. Takto sestrojené číslo p je složené. Za druhé, ježto δ_k je násobkem součinu $2 \cdot 4 \ldots 2k$, je $p = (1+\delta_k)^\varrho > \delta_k + 1 > k+1$. Tedy $p = (1+\delta_k)^\varrho$ je číslo složené, vyhovující kongruenci (21) a nerovnosti (22).

b) Abychom dokázali tvrzení b), sestrojme složené číslo p, které vyhovuje systému (23) a nerovnosti (22'). Podle rovnice (20*) lze psáti systém (23) ve tvaru

$$s_{k_\nu} = \sigma(k_\nu, p-1) = \frac{p\,(p-1)\,f_\nu(p)}{\delta_{k_\nu}} \equiv 0 \pmod p \qquad (23')$$
$$(\nu = 1, 2, \ldots, m),$$

čili jednodušeji

$$(p-1)\,f_\nu(p) \equiv 0 \pmod{\delta_{k_\nu}} \quad (\nu = 1, 2, \ldots, m), \qquad (23^*)$$

kde $f_\nu(p)$ jsou jisté mnohočleny v p s celistvými součiniteli a kde čísla δ_{k_ν} závisí pouze na daných číslech k_ν $(\nu = 1, 2, \ldots, m)$. Označme znakem δ nejmenší společný násobek čísel $\delta_{k_1}, \ldots, \delta_{k_m}$. Čísla p, vyhovující kongruenci $p \equiv 1 \pmod\delta$, vyhovují zřejmě systému (23*) čili ekvivalentnímu systému (23'). Speciálně lze

[4]) Položíme-li $n = p-1$ a užijeme vzorce (20*) z paragrafu 3., můžeme podržeti předpoklad $n > 1$, Vskutku, ježto číslo k je celé kladné, je číslo p vzhledem k (22) nejméně rovno 3, takže $p-1 = n > 1$.

zvoliti $p = (1 + \delta)^\varrho$, kde ϱ je celé číslo větší než 1, jinak libovolné. Takové číslo p je složené číslo, vyhovující systému (23′). Ježto δ_k je násobkem čísla $2 \cdot 4 \ldots 2k$, je

$$p = (1 + \delta)^\varrho > \delta + 1 \geqq \delta_{k_\nu} + 1 > k_\nu + 1 \quad (\nu = 1, 2, \ldots, m).$$

Tedy složené číslo $p = (1 + \delta)^\varrho$, vyhovující systému (23′) a tedy i ekvivalentnímu systému (23), splňuje nerovnosti $p > k_\nu + 1$ $(\nu = 1, 2, \ldots, m)$ a tedy i nerovnost (22′).

Poznámka. Místo volby $p = (1 + \delta_k)^\varrho$ resp. $p = (1 + \delta)^\varrho$ mohli jsme voliti obecněji na př. $p = \prod_{i=1}^{\varrho} (1 + t_i \delta_k)$ $\left(\text{resp. } p = \prod_{i=1}^{\varrho} (1 + t_i \delta)\right)$, kde ϱ je libovolné celé číslo větší než 1 a čísla t_i jsou libovolná celá kladná čísla.

§ 5. **Věta III.** a) *Kongruence tvaru*

$$s_{p-k} \equiv 0 \pmod{p}, \tag{24}$$

kde k je dané celé číslo větší než 1 a kde s_{p-k} je základní symetrická funkce čísel (8′) s indexem $p - k$, nemůže charakterisovati všechna prvočísla p, vyhovující nerovnosti

$$p > k. \tag{25}$$

b) *Budiž m celé číslo větší než 1. Žádný systém kongruencí*

$$s_{p-k_\nu} \equiv 0 \pmod{p} \quad (\nu = 1, 2, \ldots, m), \tag{26}$$

kde k_ν jsou navzájem různá celá čísla, větší než 1, a kde s_{p-k_ν} značí základní symetrickou funkci čísel (8′), definovanou indexem $p - k_\nu$, nemůže charakterisovati všechna prvočísla p, vyhovující nerovnosti

$$p > \text{maximum } (k_1, k_2, \ldots, k_m). \tag{25′}$$

Poznámka. Celé číslo k (resp. každé z čísel k_ν) nemůže býti rovno 1, neboť pro prvočíselné p jest $s_{p-1} \equiv -1 \pmod{p}$. Dále musí číslo p býti větší než k (resp. než každé k_ν), ježto podle definice symbolu s_{p-k} má index $p - k$ býti kladný.

Důkaz. a) Abychom dokázali tvrzení a), stačí sestrojiti složené číslo p, vyhovující kongruenci (24) a nerovnosti (25). K tomu cíli položme $p = 2^{k+2}$. Pro takovou hodnotu p řada čísel (8′) má tvar

$$1, 2, 3, \ldots, 2^{k+2} - 1 = p - 1. \tag{8″}$$

Ježto podle předpokladu je k celé a větší než 1, je $k \geqq 2$, odkud

$$2^{k+1} - k > 1 + (k + 1) + \tfrac{1}{2}k(k + 1) - k \geqq 2 + k + \tfrac{1}{2}k(k - 1) > k + 2.$$

Tedy je

$$2^{k+1} - k > k + 2 \tag{27}$$

a tedy $p - k = 2^{k+2} - k > 2^{k+1} - k > k + 2 \geqq 4$,

$$p - k > 4. \tag{28}$$

Symetrická funkce s_{p-k} čísel (8″) je součet *součinů* těchto čísel po $p - k$. Řada $2, 4, \ldots, 2^{k+2} - 2$ obsahuje všechny sudé členy řady (8″). Následkem toho počet všech sudých členů řady (8″) je roven $(2^{k+2} - 2) : 2 = 2^{k+1} - 1$. Z toho plyne, že každý součin $p - k = p - 1 - (k - 1)$ čísel řady (8″) obsahuje nejméně $2^{k+1} - 1 - (k - 1) = 2^{k+1} - k$ sudých činitelů; tedy každý takový součin je dělitelný číslem $2^{2^{k+1}-k}$ a tedy, podle (27), tím spíše dělitelný číslem $p = 2^{k+2}$. Tedy také součet s_{p-k} všech těchto součinů je dělitelný číslem $p = 2^{k+2}$. Tedy $p = 2^{k+2}$ je číslo složené, které vyhovuje kongruenci (24) a vzhledem k nerovnosti (28) také nerovnosti (25).

b) Abychom dokázali tvrzení b), sestrojme jako svrchu složené číslo p, vyhovující systému kongruencí (26) a nerovnosti (25′). Předpokládejme, že je

$$k_1 = \text{maximum } (k_1, k_2, \ldots, k_m), \tag{29}$$

čehož lze vždy dosáhnouti přečíslováním čísel k_ν. Položme $p = 2^{k_1+2}$. Podle důkazu tvrzení a) vyhovuje toto číslo p kongruenci $s_{p-k_1} \equiv 0 \pmod{p}$ a nerovnosti

$$p > k_1. \tag{30}$$

Mimo to, jak bylo dokázáno v důkazu tvrzení a), každý součin $p - k_1$ čísel řady

$$1, 2, 3, \ldots, 2^{k_1+2} - 1 = p - 1 \tag{8*}$$

je dělitelný číslem $p = 2^{k_1+2}$. Vzhledem k nerovnostem $k_1 > k_\nu$ $(\nu = 2, 3, \ldots, m)$ je $p - k_\nu > p - k_1$ $(\nu = 2, 3, \ldots, m)$. Tedy každý součin $p - k_\nu$ čísel řady (8*) je dělitelný jistým součinem $p - k_1$ takových čísel a tento součin je dělitelný, jak jsme zjistili, číslem $p = 2^{k_1+2}$. Tedy každý součin $p - k_\nu$ $(\nu = 1, 2, \ldots, m)$ čísel řady (8*) je dělitelný číslem p a tedy i všechny součty s_{p-k_ν} $(\nu = 1, 2, \ldots, m)$ jsou dělitelny číslem p, čili tyto součty splňují kongruence (26). Tedy složené číslo $p = 2^{k_1+2}$ vyhovuje systému kongruencí (26) a vzhledem ke vztahům (29), (30) též nerovnosti (25′).

Poznámka. Ve větách IIa, IIb jsou čísla k, resp. $k_1, k_2, \ldots, k_m$ celá kladná; tedy v každém z těchto tvrzení dává nerovnost (22) resp. (22′) $p > 2$. Ve větách IIIa, IIIb čísla k, resp. $k_1, k_2, \ldots, k_m$ jsou celá čísla větší než 1. Nerovnost (25) resp. (25′) dává opět $p > 2$. Ve všech tvrzeních IIa, IIb, IIIa, IIIb jde tedy jen o lichá prvočísla p.

Über ein System von Kongruenzen, welches mit dem Wilsonschen Satz zusammenhängt.

(Auszug aus dem vorstehenden Artikel.)

Kleine lateinische Buchstaben bedeuten natürliche Zahlen, p ist stets > 1; $\sigma(k, n)$ ist die k-te elementarsymmetrische Funktion der Größen $1, 2, \ldots, n$ $(1 \leqq k \leqq n)$. Im § 3 der tschechischen Originalarbeit wird gezeigt, daß sich $\sigma(k, n)$ in der Gestalt

$$\sigma(k, n) = \frac{(n+1)\, n\, \eta_{2k-2}(n)}{d_k} \tag{1}$$

schreiben läßt, wo $\eta_{2k-2}(n)$ ein Polynom in n mit ganzen, nur von k abhängigen Koeffizienten ist; auch d_k hängt nur von k ab (vgl. dort die Formeln (16), (17), (17'), (18), (20), (20*).

1. Genau dann ist p eine Primzahl, wenn

$$(p-1)! + 1 \equiv 0 \pmod{p} \tag{2}$$

(Wilsonscher Satz; alle folgenden Kongruenzen sind auch mod p zu verstehen.)

2. Hier sei $p > 2$; ist p Primzahl, so ist identisch

$$(x-1)(x-2)\ldots(x-(p-1)) \equiv x^{p-1} - 1, \tag{3}$$

also

$$\sigma(1, p-1) \equiv \sigma(2, p-1) \equiv \ldots \equiv \sigma(p-2, p-1) \equiv 0. \tag{4}$$

Gilt umgekehrt (4), so ist $\frac{1}{2}p\,(p-1) \equiv 0$, p ungerade und die Kongruenz (3) ist mit

$$x^{p-1} + (p-1)! \equiv x^{p-1} - 1 \tag{5}$$

identisch. Da (3) die Wurzel 1 hat, so folgt aus (5) mit $x = 1$ die Kongruenz (2), also ist p eine ungerade Primzahl. Unter den $p > 2$ sind also die Primzahlen durch (4) charakterisiert.

3. Zu dieser Charakterisierung ungerader Primzahlen genügt bereits folgendes System:

$$\sigma(1, p-1) \equiv 0,\ \sigma(2l, p-1) \equiv 0 \quad (2l < p-1). \tag{6}$$

Denn die erste Kongruenz charakterisiert ungerade Zahlen p; ist aber p ungerade, so ist

$$\sigma(2k-1, p-1) = \Sigma\, \alpha_1 \ldots \alpha_{2k-1} = \Sigma\,(p-\alpha_1)\ldots(p-\alpha_{2k-1})$$
$$\equiv -\sigma(2k-1, p-1), \text{ also } 2\sigma(2k-1, p-1) \equiv 0,$$

$\sigma(2k-1, p-1) \equiv 0$; daraus und aus (6) folgt also (4).

4. Sind m und $k_1, \ldots, k_m$ gegeben, so genügt weder das System

$$\sigma(k_\nu, p-1) \equiv 0 \quad (\nu = 1, \ldots, m) \tag{7}$$

noch das System

$$\sigma(p - k_\nu, p - 1) \equiv 0 \quad (\nu = 1, \ldots, m) \tag{8}$$

zur Charakterisierung aller hinreichend großen Primzahlen p, d. h. es gibt beliebig große zusammengesetzte p, welche dem System (7) bzw. (8) genügen (für das System (8) kommen nach dem Wilsonschen Satz nur $k_\nu > 1$ in Betracht). Beweis: benutzt man (1), so sieht man, daß die zusammengesetzte Zahl $p = (1 + d_{k_1} \ldots d_{k_m})^r$ $(r > 1)$ den Kongruenzen (7) genügt. Ist zweitens $p = 2^r$ $(r > 1)$, so beachte man, daß die Reihe $1, 2, \ldots, 2^r - 1$ genau $2^{r-1} - 1$ gerade Glieder enthält; also ist $\sigma(p - k_\nu, p - 1)$ durch $2^{2^r - 1 - (k_\nu - 1)}$ teilbar; für hinreichend großes r ist aber $2^r - 1 - (k_\nu - 1) \geqq r$; daher gelten die Kongruenzen (8) für $p = 2^r$, wenn r hinreichend groß ist.