

Štefan Schwarz

Příspěvek k reducibilitě binomických kongruencí

Časopis pro pěstování matematiky a fyziky, Vol. 71 (1946), No. 1-4, 21--31

Persistent URL: <http://dml.cz/dmlcz/121089>

Terms of use:

© Union of Czech Mathematicians and Physicists, 1946

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

Příspěvek k reducibilitě binomických kongruencí.

Štefan Schwarz, Bratislava.

(Došlo 1. listopadu 1945.)

I.

Obsahem této poznámky jest rozřešení otázky po počtu a stupních ireducibilních faktorů binomické kongruence

$$x^n - a \equiv 0 \pmod{p}, \quad (n, p) = (a, p) = 1. \quad (1)$$

Pokud jde o lineární faktory takové kongruence, jest všeobecně znám klasický výsledek, který říká: nutná a postačující podmínka pro to, aby kongruence (1) měla řešení, jest splnění vztahu

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

kde $d = (n, p-1)$. Jestliže jest tato podmínka splněna, má (1) právě d řešení.

V této poznámce ukážeme, jak lze nalézt výsledek podobného rázu i pro faktory k -tého stupně. Nejenom výsledky, nýbrž i postup důkazu sám o sobě, nepostrádá jisté zajímavosti.

Platí věta:

Nechť jest dána kongruence (1) n -tého stupně. Nechť k jest celé číslo, $1 \leq k \leq n$. Položme $d_k = (p^k - 1, n)$. Znakem σ_k označme počet ireducibilních faktorů k -tého stupně kongruence (1). Nechť konečně $k' > k'' > k''' > \dots > 1$ jsou všichni dělitelé čísla k , menší než k . Potom platí

$$1. \text{ pro ta } k, \text{ pro která jest } a^{\frac{p^k-1}{d_k}} \equiv 1 \pmod{p},$$

$$\text{je } k\sigma_k + k'\sigma_{k'} + k''\sigma_{k''} + \dots + \sigma_1 \equiv 0 \pmod{p}; \quad (2)$$

$$2. \text{ pro ta } k, \text{ pro která jest } a^{\frac{p^k-1}{d_k}} \equiv 1 \pmod{p},$$

$$\text{je } k\sigma_k + k'\sigma_{k'} + k''\sigma_{k''} + \dots + \sigma_1 \equiv d_k \pmod{p}. \quad (3)$$

Poznámka: Vztahy (2) a (3) dávají zřejmě rekurentní relace, z nichž lze $\sigma_1, \sigma_2, \dots, \sigma_k$ bezprostředně vypočítati (alespoň pro $n < p$).

Důkaz: Necht $\varphi(x)$ je libovolný (mod p) ireducibilní polynom k -tého stupně s racionálními celými koeficienty. Jeden jeho kořen ležící ve vhodném rozšíření tělesa tříd zbytků (mod p) K_p označme znakem j . Jak jest známo, jsou potom všechny kořeny všech nerozložitelných polynomů k -tého stupně nad tělesem zbytkových tříd mod p obsaženy v tělese $K_p(j)$. V témž tělese jsou dále obsaženy i všechny kořeny všech nerozložitelných polynomů stupňů $k', k'', k''', \dots, 1$, kde $k', k'', k''', \dots, 1$ mají nahoře zavedený význam. Těleso $K_p(j)$ obsahuje p^k elementů tvaru

$$\xi = c_0 + c_1j + c_2j^2 + \dots + c_{k-1}j^{k-1} \quad (0 \leq c_i \leq p-1). \quad (4)$$

Každý element $\xi \not\equiv 0 \pmod{p}$ hoví vztahu

$$\xi^{p^k-1} \equiv 1 \pmod{p}.$$

Pro $\xi \equiv 0 \pmod{p}$ jest ovšem

$$\xi^{p^k-1} \equiv 0 \pmod{p}.^{1)}$$

Uvažujme výraz

$$\sum_{x=\xi} [x^n - a]^{p^k-1} \pmod{p},$$

kde součet se vztahuje na všechny elementy (4) v počtu p^k . V tomto součtu bude (mod p) tolik jedniček, kolik jest závorek různých od nuly a tolik nul (mod p), kolik má kongruence (1) kořenů mezi elementy (4).

Veličiny (4) hoví však pouze ired. polynomům stupně k , resp. k' , resp. k'' , ... atd. Při tom ke každému ired. polynomu stupně k -tého přísluší skupina k veličin ξ ze skupiny veličin (4). Podobně pro dělitele k', k'', \dots atd.

Ježto součet obsahuje p^k sčítanců, jest zřejmě

$$\sum_{\xi} [x^n - a]^{p^k-1} \equiv p^k - k\sigma_k - k'\sigma_{k'} - k''\sigma_{k''} - \dots - \sigma_1 \pmod{p}. \quad (5)$$

Abychom upravili součet na levé straně, připomeňme si: ze vztahu

$$x^{p^k-1} - 1 \equiv \prod_{\xi \neq 0} (x - \xi) \pmod{p}$$

plyne elementárními algebraickými úpravami pro potenění součty

$$s_i \equiv \sum_{\xi} \xi^i \equiv \begin{cases} 0 \pmod{p}, & \text{pro } p^k - 1 \nmid i, \\ -1 \pmod{p}, & \text{pro } p^k - 1 \mid i. \end{cases}$$

¹⁾ Jinak lze také říci: Platí $x^{p^k} - x \equiv \Pi \varphi(x) \pmod{p}$, kde součin se vztahuje na všechny (mod p) ired. polynomy $\varphi(x)$, jichž stupeň dělí k .

Vztah (5) upravujeme umocněním závorky. Ježto budeme dle x sčítati, budou nás zajímati pouze členy s x^i , kde exponent i jest dělitelný číslem $p^k - 1$. To jsou členy, v nichž exponent u x jest tvaru

$$n \left(p^k - 1 - l \cdot \frac{p^k - 1}{d_k} \right) \quad (l = 0, 1, \dots, d_k - 1).$$

Zbývající členy můžeme vynechati.

Jest tedy, označíme-li k vůli přehlednosti na chvíli $\sigma = k\sigma_k + \dots + \sigma_1$,

$$-\sigma \equiv \sum_{\xi} \sum_{l=0}^{d_k-1} (-1)^l \cdot \frac{p^k-1}{d_k} \binom{p^k-1}{l \cdot \frac{p^k-1}{d_k}} \cdot x^{n \left(p^k-1-l \cdot \frac{p^k-1}{d_k} \right)} \cdot a^{l \cdot \frac{p^k-1}{d_k}} \pmod{p}.$$

Provedeme-li sumaci dle ξ , jest

$$\sigma \equiv \sum_{l=0}^{d_k-1} (-1)^l \cdot \frac{p^k-1}{d_k} \binom{p^k-1}{l \cdot \frac{p^k-1}{d_k}} a^{l \cdot \frac{p^k-1}{d_k}} \pmod{p}.$$

Dále je však

$$\begin{aligned} \binom{p^k-1}{l \cdot \frac{p^k-1}{d_k}} &= \frac{(p^k-1)(p^k-2)\dots\left(p^k-l \cdot \frac{p^k-1}{d_k}\right)}{l \cdot \frac{p^k-1}{d_k} \left(l \cdot \frac{p^k-1}{d_k} - 1\right) \dots 2 \cdot 1} \equiv \\ &\equiv (-1)^l \frac{p^k-1}{d_k} \pmod{p}. \end{aligned}$$

Tedy

$$\sigma \equiv \sum_{l=0}^{d_k-1} a^{l \cdot \frac{p^k-1}{d_k}} \pmod{p}. \quad (6)$$

Nyní nutno rozeznávati dva případy:

1. Je-li

$$a^{\frac{p^k-1}{d_k}} \not\equiv 1 \pmod{p},$$

je

$$\sigma \equiv \frac{a^{\frac{p^k-1}{d_k}} - 1}{a^{\frac{p^k-1}{d_k}} - 1} \pmod{p},$$

t. j.

$$\sigma \equiv 0 \pmod{p},$$

jinak

$$k\sigma_k + k'\sigma_{k'} + \dots + \sigma_1 \equiv 0 \pmod{p}.$$

2. Je-li

$$a^{\frac{p^k-1}{d_k}} \equiv 1 \pmod{p},$$

plyne z relace (6)

$$\sigma \sum_{l=0}^{d_k-1} 1 \pmod{p},$$

t. j.

$$k\sigma_k + k'\sigma_{k'} + \dots + \sigma_1 \equiv d_k \pmod{p}.$$

Tím jest naše věta dokázána.

II.

Z rovnic (2) a (3) lze vypočítati explicitně veličiny $\sigma_1, \sigma_2, \dots, \sigma_n$. Kvůli jednoduchosti zavedme symbol δ_k , který definujeme takto:

$$\delta_k = \begin{cases} 0, & \text{pro ta } k, \text{ pro která jest } a^{\frac{p^k-1}{d_k}} \equiv 1 \pmod{p}, \\ d_k, & \text{pro ta } k, \text{ pro která jest } a^{\frac{p^k-1}{d_k}} \not\equiv 1 \pmod{p}. \end{cases}$$

Systém rekurentních relací vypadá takto:

$$\begin{aligned} \sigma_1 &\equiv \delta_1, \\ 2\sigma_2 + \sigma_1 &\equiv \delta_2, \\ 3\sigma_3 + \sigma_1 &\equiv \delta_3, \\ 4\sigma_4 + 2\sigma_2 + \sigma_1 &\equiv \delta_4, \pmod{p} \\ 5\sigma_5 + \sigma_1 &\equiv \delta_5, \\ 6\sigma_6 + 3\sigma_3 + 2\sigma_2 + \sigma_1 &\equiv \delta_6, \\ &\dots \end{aligned} \quad (7)$$

Odtud plyne přímo (pokud index u příslušného σ_k není dělitelný p)

$$\begin{aligned} \sigma_1 &\equiv \delta_1, \\ \sigma_2 &\equiv \frac{1}{2}(\delta_2 - \delta_1), \\ \sigma_3 &\equiv \frac{1}{3}(\delta_3 - \delta_1), \\ \sigma_4 &\equiv \frac{1}{4}(\delta_4 - \delta_2), \\ \sigma_5 &\equiv \frac{1}{5}(\delta_5 - \delta_1), \\ \sigma_6 &\equiv \frac{1}{6}(\delta_6 - \delta_3 - \delta_2 + \delta_1), \\ &\dots \end{aligned} \pmod{p} \quad (8)$$

V případě $n < p$ udává soustava (7) hodnotu veličin $\sigma_1, \sigma_2, \sigma_3, \dots$ jednoznačně. V případě $n > p$ nedává však (7) o číslech $\sigma_p, \sigma_{2p}, \sigma_{3p}, \dots$ žádných informací. Relace pro $\sigma_p, \sigma_{2p}, \sigma_{3p}, \dots$ vypa-
dají totiž takto:

$$\begin{aligned}
 p\sigma_p + \sigma_1 &\equiv \delta_p, \\
 2p\sigma_{2p} + p\sigma_p + 2\sigma_2 + \sigma_1 &\equiv \delta_{2p}, \\
 3p\sigma_{3p} + p\sigma_p + 3\sigma_3 + \sigma_1 &\equiv \delta_{3p}, \\
 &\dots\dots\dots
 \end{aligned}
 \tag{9}$$

atd.

Sčítanci obsahující $\sigma_p, \sigma_{2p}, \sigma_{3p}, \dots$ jsou $\equiv 0 \pmod{p}$, v relacích vypadnou a vztahy (9) dávají pak první relace (7) zároveň se shodami $\delta_1 \equiv \delta_p, \delta_2 \equiv \delta_{2p}, \dots$, jež lze dokázati ostatně také přímo. Veličiny $\sigma_1, \sigma_2, \sigma_3, \dots$, které nejsou tvaru σ_{kp} , nejsou pak relacemi (8) také určeny jednoznačně (jsouce udány pouze mod p). (Přirozeně v konkrétních případech lze je vzhledem ke vztahu $\sigma_1 + 2\sigma_2 + 3\sigma_3 + \dots + n\sigma_n = n$ určit zpravidla bez námahy.)

Z odvozených výsledků lze činiti různé zajímavé závěry pro ired. faktory k -tého stupně dané kongruence. Pro lineární faktory dává $\sigma_1 \equiv \delta_1$, pro $n < p$ přímo výsledek v úvodu zmíněný. Pro faktory kvadratické, kubické a obecněji pro faktory prvočíselného stupně q platí tato věta:

Nechť n, σ_k, d_k mají nahoře zavedený význam. Nechť $q > 1$ je prvočíslem, $(p, q) = 1$. Potom pro číslo σ_q platí tyto vztahy:

1. Je-li

$$a^{\frac{p-1}{d_1}} \equiv 1 \pmod{p},$$

je

$$\sigma_q \equiv \frac{1}{q} \{(p^q - 1, n) - (p - 1, n)\} \pmod{p}.$$

2. Je-li

$$a^{\frac{p-1}{d_1}} \not\equiv 1 \pmod{p} \tag{*}$$

a kromě toho

$$\alpha) a^{\frac{p^q-1}{d_q}} \equiv 1 \pmod{p}, \text{ je } \sigma_q \equiv 0 \pmod{p}.$$

$$\beta) a^{\frac{p^q-1}{d_q}} \equiv 1 \pmod{p}, \text{ je } \sigma_p \equiv \frac{1}{q} (p^q - 1, n).$$

Při tom: Případ 2β může (ale nemusí) nastati jenom tenkrát, platí-li $q / p - 1$. Je-li $q \nmid p - 1$, nastane buď případ 2α , anebo případ 1.

Důkaz: 1. Nechť $a^{\frac{p-1}{d_1}} \equiv 1 \pmod{p}$. Pak je též $a^{\frac{p^q-1}{d_q}} \equiv 1 \pmod{p}$. K důkazu tohoto tvrzení stačí dokázati, že číslo $\frac{p^q-1}{d_q}$

jest násobkem čísla $\frac{p-1}{d_1}$, t. j. že podíl

$$\frac{p^q - 1}{d_q} : \frac{p - 1}{d_1}$$

jest číslem celým. Jelikož $(n, p - 1) = d_1$, je $n = \alpha \cdot d_1$, $p - 1 = \beta \cdot d_1$, kde $(\alpha, \beta) = 1$. Tedy jest

$$\begin{aligned} \frac{p^q - 1}{d_q} : \frac{p - 1}{d_1} &= \frac{p^q - 1}{(p^q - 1, n)} : \frac{p - 1}{(p - 1, n)} = \frac{(p - 1) \cdot \Sigma}{(p - 1, \Sigma, n)} \\ &: \frac{p - 1}{d_1} = \frac{\Sigma}{(\beta d_1 \cdot \Sigma, \alpha d_1)} : \frac{1}{d_1} = \frac{\Sigma}{(\beta \cdot \Sigma, \alpha)}, \end{aligned}$$

kde znakem Σ jsme označili $\Sigma = 1 + p + p^2 + \dots + p^{q-1}$. Ježto dále $(\alpha, \beta) = 1$, jest $(\beta \Sigma, \alpha)$ dělitelem čísla Σ a podíl $\frac{\Sigma}{(\beta \Sigma, \alpha)}$ jest číslem celým.

V rovnicích $\sigma_1 \equiv \delta_1$, $\sigma_q \equiv \frac{1}{q} (\delta_q - \delta_1)$ jest tedy $\delta_1 = d_1$, $\delta_q = d_q$, což dává horní vzorec.

2. Necht jest dále $a^{\frac{p-1}{d_1}} \equiv 1 \pmod{p}$. První rovnice dává $\sigma_1 \equiv 0 \pmod{p}$. Je-li nadto $a^{\frac{p^q-1}{d_q}} \equiv 1 \pmod{p}$, jest $\delta_q = d_q = (p^q - 1, n)$, tedy $\sigma_q \equiv \frac{1}{q} (p^q - 1, n)$.

Je-li však $a^{\frac{p^q-1}{d_q}} \not\equiv 1 \pmod{p}$ jest $\delta_q = 0$, tedy $\sigma_q \equiv 0 \pmod{p}$, c. b. d.

Ukážeme nyní, že platí-li $q \nmid p - 1$ a relace (*), nastane nutně případ 2 α . Předpokládejme, že platí $a^{\frac{p^q-1}{d_q}} \equiv 1$, $a^{\frac{p-1}{d_1}} \equiv 1 \pmod{p}$ a ptejme se, jaké důsledky z toho plynou pro číslo q . Viděli jsme, že lze psáti

$$\frac{p^q - 1}{d_q} = \frac{p - 1}{d_1} \cdot s,$$

kde s je celým číslem. Vzhledem k předpokladu $a^{\frac{p-1}{d_1}} \equiv 1 \pmod{p}$ může být číslo $a^{\frac{p-1}{d_1} \cdot s}$ shodno s 1 (mod p) jenom tenkrát, mají-li s a d_1 společného dělitele $m > 1$. Ježto je $d_1/p - 1$ a s/Σ , platí také $m/p - 1$ a m/Σ . Z první relace plyne $p \equiv 1 \pmod{m}$. Ze vztahu m/Σ plyne však

$$\begin{aligned} \text{t. j.} \quad & 1 + p + p^2 + \dots + p^{q-1} \equiv 0 \pmod{m}, \\ & 1 + 1 + 1 + \dots + 1 \equiv 0 \pmod{m}, \\ & q \equiv 0 \pmod{m}. \end{aligned}$$

Ježto je $q > 1$ prvočíslem, je $q = m$, tedy $q/p = 1$. Příklad 2β je tedy možný jenom tenkrát, platí-li $q/p = 1$, c. b. d.

Z odvozené věty lze činiti různé závěry. Jednoduchým důsledkem jest na příklad tato věta:

Polynom $x^n - a$, $(a, p) = (n, p) = 1$ jest mod p nerozložitelný tehdy a jen tehdy, je-li pro každé $k < n$ splněn vztah

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

a platí-li pro $k = n$

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

Důkaz: a) Je-li podmínka ve větě uvedená splněna, je systém (2) a (3) tvaru

$$\begin{aligned} \sigma_1 &\equiv 0, \\ 2\sigma_2 + \sigma_1 &\equiv 0, \\ 3\sigma_3 + \sigma_1 &\equiv 0, \\ &\dots\dots\dots \end{aligned}$$

$$n\sigma_n + n'\sigma_{n'} + \dots + \sigma_1 \equiv d_n \equiv 0.$$

Odtud plyne po řadě

$$\sigma_1 \equiv 2\sigma_2 \equiv 3\sigma_3 \equiv \dots \equiv (n-1)\sigma_{n-1} \equiv 0,$$

tedy

$$n\sigma_n \equiv 0 \pmod{p}.$$

Užitím rovnice

$$\sigma_1 + 2\sigma_2 + 3\sigma_3 + \dots + n\sigma_n = n$$

plyne pak, že je nutně $\sigma_n = 1$, tedy $\sigma_1 = \sigma_2 = \dots = \sigma_{n-1} = 0$.

b) Budiž obráceně $k = \kappa < n$ první index takový, že

$$a^{\frac{p^\kappa-1}{d_\kappa}} \equiv 1 \pmod{p},$$

kdežto pro $k < \kappa$ je

$$a^{\frac{p^k-1}{d_k}} \not\equiv 1 \pmod{p}.$$

Potom ze vztahů (2), (3) plyne opět

$$\sigma_1 \equiv 2\sigma_2 \equiv 3\sigma_3 \equiv \dots \equiv (\kappa-1)\sigma_{\kappa-1} \equiv 0,$$

$$\kappa \cdot \sigma_\kappa \equiv 0 \pmod{p}.$$

Tedy je $\sigma_\kappa \not\equiv 0$, t. j. polynom $x^n - a$ jest modulo p rozložitelný, má ireducibilní faktor stupně $\kappa < n$. Nadto vychází rovněž, že je $\kappa \not\equiv 0 \pmod{p}$.

III.

Abychom správně odhadli dosah odvozených vět, provedeme ještě dva instruktivní příklady.

Příklad 1. Jest vyšetřiti rozklad polynomu

$$x^4 + 1$$

dle modulu p .

Potřebné veličiny jsou sestaveny v tabulku:

p je tvaru	$d_1 \equiv (p^1 - 1, 4)$	$d_2 \equiv (p^2 - 1, 4)$	$d_3 \equiv (p^3 - 1, 4)$	$d_4 \equiv (p^4 - 1, 4)$	$\frac{p^1 - 1}{(-1) d_1}$	$\frac{p^2 - 1}{(-1) d_2}$	$\frac{p^3 - 1}{(-1) d_3}$	$\frac{p^4 - 1}{(-1) d_4}$
$p = 4k + 3$	2	4	2	4	-1	1	-1	1
$p = 4k + 1$	$p = 8k + 1$	4	4	4	4	1	1	1
	$p = 8k + 5$	4	4	4	4	-1	1	-1

Systémy kongruencí (2) a (3) jsou tyto:

a) pro p tvaru $4k + 3$

$$\sigma_1 \equiv 0, \quad 2\sigma_2 + \sigma_1 \equiv 4, \quad 3\sigma_3 + \sigma_1 \equiv 0, \quad 4\sigma_4 + 2\sigma_2 + \sigma_1 \equiv 4,$$

t. j.

$$\sigma_1 = \sigma_3 = \sigma_4 = 0, \quad \sigma_2 = 2;$$

b) pro p tvaru $8k + 1$

$$\sigma_1 \equiv 4, \quad 2\sigma_2 + \sigma_1 \equiv 4, \quad 3\sigma_3 + \sigma_1 \equiv 4, \quad 4\sigma_4 + 2\sigma_2 + \sigma_1 \equiv 4,$$

t. j.

$$\sigma_1 = 4, \quad \sigma_2 = \sigma_3 = \sigma_4 = 0;$$

c) pro p tvaru $8k + 5$

$$\sigma_1 \equiv 0, \quad 2\sigma_2 + \sigma_1 \equiv 4, \quad 3\sigma_3 + \sigma_1 \equiv 0, \quad 4\sigma_4 + 2\sigma_2 + \sigma_1 \equiv 4,$$

t. j.

$$\sigma_1 = \sigma_3 = \sigma_4 = 0, \quad \sigma_2 = 2.$$

Dokázali jsme tedy tuto větu:

Polynom $x^4 + 1$ jest modulo každého prvočísla p rozložitelný a to: je-li p tvaru $8k + 3, 5, 7$ na dva faktory druhého stupně; je-li p tvaru $8k + 1$ na čtyři faktory lineární.

Poznámka: Existence racionálně nerozložitelných polynomů, jež jsou rozložitelné dle každého prvočíselného modulu p , jest známa. Dá se na příklad jednoduše dokázati, že má tuto vlastnost každý ired. polynom s rac. koeficienty 4. stupně, jehož Galoisovu grupou jest Kleinova čtyřková grupa.²⁾ Ostatně plyne bezprostředně z teorie třídnicích těles, že totéž platí (s eventuální výjimkou konečného počtu prvočísel) pro každý abelovský polynom, jehož Galoisova grupa má tu vlastnost, že řád každého elementu jest menší než řád grupy, t. j. není cyklickou. (Na příklad jest tomu tak pro každou rovnici pro dělení kruhu n -tého stupně, je-li $n \neq 2, 4, p^t, 2p^t$, kde p je liché číslo.)

Příklad 2. Ptejme se, jak se rozpadne polynom

$$x^q - a \pmod{p}, \quad (10)$$

je-li q prvočíslem, $q < p$.

Zde jest číslo $d_k = \nu(p^k - 1, q)$ rovné buď číslu q nebo číslu 1. Nechť p patří mod q k exponentu l .

a) Nechť jest nejdříve $l = 1$. Pak jest $d_k = (p^k - 1, q) = q$ pro každé $k = 1, 2, \dots, q$.

α) Je-li

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

pak jest také

$$\frac{p^2-1}{a^q} \equiv 1, \quad \frac{p^3-1}{a^q} \equiv 1, \dots \text{ atd.}$$

Systém kongruencí (7) je tvaru

$$\begin{aligned} \sigma_1 &\equiv q, \\ 2\sigma_2 + \sigma_1 &\equiv q, \\ \dots &\dots \dots \dots \\ q\sigma_q + \sigma_1 &\equiv q. \end{aligned} \pmod{p}$$

Ježto je $q < p$, plyne z první kongruence $\sigma_1 = q$ a tedy $\sigma_2 = \sigma_3 = \dots = \sigma_q = 0$. Polynom (10) se úplně rozpadne:

β) Je-li

$$\frac{p-1}{a^q} \not\equiv 1 \pmod{p},$$

pak k sestavení kongruencí musíme věděti, které jest nejnižší číslo k , pro které jest

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

²⁾ Na to upozornil na speciálním případě již Frobenius (Berl. Berichte 1896, I, str. 689, srovnej Pólya - Szegő, Aufgaben aus der Analysis II, str. 351) a Hilbert (Gött. Nachrichten 1897, str. 53, Werke II, str. 388-9.)

Máme výsledek: náš polynom se rozpadl na faktor stupně prvního a na $\frac{q-1}{l}$ faktorů stupně l -tého.

Uhrnem máme větu:

Je dána kongruence $x^q - a \pmod{p}$, $q < p$. Nechť p a q jsou dvě různá prvočísla. Nechť p patří mod q k exponentu l .

Je-li $l = 1$ a $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$, rozpadne se kongruence na samé lineární faktory. Je-li $l = 1$ a $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$, jest polynom ireducibilní. Je-li $l > 1$, rozpadne se $x^q - a \pmod{p}$ na jeden faktor lineární a na $\frac{q-1}{l}$ faktorů stupně l -tého.³⁾

*

Contribution à la réductibilité des congruences binomiques.

(Résumé de l'article précédent.)

Soit (1) une congruence du degré n , $(n, p) = (a, p) = 1$. Soit k un nombre entier, $1 \leq k \leq n$. Posons $d_k = (p^k - 1, n)$. Soit σ_k le nombre des facteurs irréductibles du degré k de la congruence (1). Soient enfin $k' > k'' > \dots > 1$ tous les diviseurs de k plus petits que k . Alors les relations suivantes ont lieu:

1. pour les k , pour lesquels

$$a^{\frac{p^k-1}{d_k}} \not\equiv 1 \pmod{p},$$

on a

$$k\sigma_k + k'\sigma_{k'} + k''\sigma_{k''} + \dots + \sigma_1 \equiv 0 \pmod{p};$$

2. pour les k , pour lesquels

$$a^{\frac{p^k-1}{d_k}} \equiv 1 \pmod{p},$$

on a

$$k\sigma_k + k'\sigma_{k'} + k''\sigma_{k''} + \dots + \sigma_1 \equiv d_k \pmod{p}.$$

Ces relations forment une généralisation d'un résultat classique bien connu concernant le nombre des racines rationnelles de la congruence (1). Elles donnent des formules récurrentes, qui fournissent — en général — les nombres $\sigma_1, \sigma_2, \dots, \sigma_n \pmod{p}$.

Quelques applications aux équations spéciales servent à illustrer la portée des résultats trouvés.

³⁾ Jako speciální případ obsažen jest v této větě známý rozklad rovnice pro dělení kruhu $x^q - 1 \equiv 0 \pmod{p}$. Tady jest vždy $a^{\frac{p-1}{q}} \equiv 1$. Příklad $l = 1$ a $l > 1$ lze formulovati jednotně: $x^q - 1 \equiv 0 \pmod{p}$ rozpadne se na jeden faktor lineární a $\frac{q-1}{l}$ faktorů stupně l -tého. (Lehce se dokáže, že platí ovšem i v případě $p < q$.)