Werk

Label: Article

Jahr: 1946

PURL: https://resolver.sub.uni-goettingen.de/purl?31311028X_0071|log10

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Časopis pro pěstování matematiky a fysiky, roč. 71 (1946)

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

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

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

1. pro ta k, pro která jest $a^{\frac{p^k-1}{d_k}} \not\equiv 1 \pmod{p}$,

$$\text{je } k\sigma_k + k'\sigma_{k'} + k''\sigma_{k''} + \ldots + \sigma_1 \equiv 0 \pmod{p}; \tag{2}$$

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

$$\text{je } k\sigma_k + k'\sigma_{k'} + k''\sigma_{k''} + \ldots + \sigma_1 \equiv d_k \pmod{p}. \tag{3}$$

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

Důkaz: Nechť $\varphi(x)$ 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 $k', k'', k''', \ldots, 1$, kde $k', k'', k''', \ldots, 1$ mají nahoře zavedený význam. Těleso $K_p(j)$ obsahuje p^k elementů tvaru

$$\xi = c_0 + c_1 j + c_2 j^2 + \ldots + c_{k-1} j^{k-1} \; (0 \leqq c_i \leqq p - 1). \tag{4}$$

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

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

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'', ... atd.

Ježto součet obsahuje p^k sčítanců, jest zřejmě

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

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 potenční 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

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

Zbývající členy můžeme vynechati.

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

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

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

$$\binom{p^k - 1}{l \cdot \frac{p^k-1}{d_k}} = \frac{(p^k-1)(p^k-2)\ldots\left(p^k - l \cdot \frac{p^k-1}{d_k}\right)}{l \cdot \frac{p^k-1}{d_k}\left(l \cdot \frac{p^k-1}{d_k} - 1\right)\ldots 2 \cdot 1} \equiv$$

$$\equiv (-1)^{l \cdot \frac{p^k-1}{d_k}} \pmod{p}.$$

Tedy

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

Nyní nutno rozeznávati dva případy:

1. Je-li

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

je

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

t. j.

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

jinak

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

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.

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

Tím jest naše věta dokázána.

II.

Z rovnic (2) a (3) lze vypočísti explicitně veličiny $\sigma_1, \sigma_2, \ldots, \sigma_n$. K vůli jednoduchosti zaveďme symbol δ_k, který definujeme takto:

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

Systém rekurentních relací vypadá takto:

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

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

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

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

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

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

$\alpha)$ $a^{\frac{p^q-1}{d_q}} \not\equiv 1 \pmod p$, je $\sigma_q \equiv 0 \pmod p$.

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

Při tom: Případ 2β může (ale nemusí) nastati jenom tenkráte, platí-li $q \mid p-1$. 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 $n = \alpha \,.\, d_1$, $p - 1 = \beta \,.\, d_1$, kde $(\alpha, \beta) = 1$. Tedy jest

$$\frac{p^q - 1}{d_q} : \frac{p-1}{d_1} = \frac{p^q - 1}{(p^q - 1, n)} : \frac{p-1}{(p-1, n)} = \frac{(p-1)\,.\,\Sigma}{(p-1\,.\,\Sigma, n)} :$$

$$: \frac{p-1}{d_1} = \frac{\Sigma}{(\beta d_1\,.\,\Sigma, \alpha d_1)} : \frac{1}{d_1} = \frac{\Sigma}{(\beta\,.\,\Sigma, \alpha)},$$

kde znakem Σ jsme označili $\Sigma = 1 + p + p^2 + \ldots + p^{q-1}$. 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. Nechť jest dále $a^{\frac{p-1}{d_1}} \not\equiv 1 \pmod p$. 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 2α. Předpokládejme, že platí $a^{\frac{p^q-1}{d_q}} \equiv 1$, $a^{\frac{p-1}{d_1}} \not\equiv 1 \pmod p$ a ptejme se, jaké důsledky z toho plynou pro číslo q. Viděli jsme, že lze psáti

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

kde s je celým číslem. Vzhledem k předpokladu $a^{\frac{p-1}{d_1}} \not\equiv 1 \pmod p$ může býti číslo $a^{\frac{p-1}{d_1}\,.\,s}$ shodno s 1 (mod p) jenom tenkráte, 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

$$1 + p + p^2 + \ldots + p^{q-1} \equiv 0 \pmod m,$$

t. j.
$$1 + 1 + 1 + \ldots + 1 \equiv 0 \pmod m,$$

$$q \equiv 0 \pmod m.$$

Ježto je $q > 1$ prvočíslem, je $q = m$, tedy $q/p - 1$. Případ 2β je tedy možný jenom tenkráte, 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

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

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

$$\begin{aligned} \sigma_1 &\equiv 0, \\ 2\sigma_2 + \sigma_1 &\equiv 0, \\ 3\sigma_3 + \sigma_1 &\equiv 0, \\ &\cdots\cdots\cdots \\ n\sigma_n + n'\sigma_{n'} + \ldots + \sigma_1 &\equiv d_n \not\equiv 0. \end{aligned}$$

Odtud plyne po řadě

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

tedy

$$n\sigma_n \not\equiv 0 \pmod{p}.$$

Užitím rovnice

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

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

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

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

kdežto pro $k < \varkappa$ je

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

Potom ze vztahů (2), (3) plyne opět

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

$$\varkappa \,.\, \sigma_\varkappa \not\equiv 0 \pmod{p}.$$

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

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		$d_1 \equiv (p^1 - 1,4)$	$d_2 \equiv (p^2 - 1,4)$	$d_3 \equiv (p^3 - 1,4)$	$d_4 \equiv (p^4 - 1,4)$	$(-1)^{\frac{p^1-1}{d_1}}$	$(-1)^{\frac{p^2-1}{d_2}}$	$(-1)^{\frac{p^3-1}{d_3}}$	$(-1)^{\frac{p^4-1}{d_4}}$
$p = 4k + 3$		2	4	2	4	-1	1	-1	1
$p = 4k + 1$	$p = 8k + 1$	4	4	4	4	1	1	1	1
	$p = 8k + 5$	4	4	4	4	-1	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 Galoisovou grupou jest Kleinova čtyřková grupa.[2]) Ostatně plyne bezprostředně z teorie třídních 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

$$x^q - a \pmod{p}, \tag{10}$$

je-li q prvočíslem, $q < p$.

Zde jest číslo $d_k = (p^k - 1, q)$ 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 $k = 1, 2, \ldots, q$.

α) Je-li

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

pak jest také

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

Systém kongruencí (7) je tvaru

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

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

β) Je-li

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

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

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

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

Zřejmě platí

$$a^{\frac{p^k-1}{q}} = a^{\frac{p-1}{q}(1+p+p^2+\ldots+p^{k-1})} \equiv a^{\frac{p-1}{q}\cdot k} \pmod{p}.$$

[Poslední relace plyne z toho, že je $1 + p + p^2 + \ldots + p^{k-1} \equiv k \pmod{p-1}$.] Avšak vzhledem k předpokladu $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$ může býti číslo $a^{\frac{p-1}{q}\cdot k}$ shodno s 1 $(\mathrm{mod}\ p)$ jenom tehdy, je-li q dělitelem čísla k. Nejmenší takové číslo jest $k = q$. Tedy v tomto případě jest

$$a^{\frac{p-1}{q}} \not\equiv 1, \quad a^{\frac{p^2-1}{q}} \not\equiv 1, \quad \ldots, \quad a^{\frac{p^{q-1}-1}{q}} \not\equiv 1, \quad a^{\frac{p^q-1}{q}} \equiv 1 \pmod{p}.$$

Podle věty sub II dokázané jest tedy polynom $x^q - a \pmod{p}$ ireducibilní.

b) Nechť jest za druhé $l > 1$. Pak jest

$$d_1 = 1, \quad d_2 = 1, \quad \ldots, \quad d_{l-1} = 1, \quad d_l = q.$$

Ukážeme nejdříve, že jest nyní splněn vztah

$$a^{\frac{p^k-1}{d_k}} \equiv 1 \pmod{p}, \quad (k = 1, 2, \ldots, l).$$

Pro $k = 1, 2, \ldots, l-1$ je to zřejmé. Pro $k = l$ uvažme, že celé číslo $\frac{p^l-1}{d_l} = \frac{p^l-1}{q}$ lze psáti ve tvaru

$$(p-1)\cdot\frac{1+p+\ldots+p^{l-1}}{q}.$$

Při tom jest naznačený podíl celým číslem. Kdyby totiž q dělilo $p-1$ a nikoliv vypsaný součet, bylo by $l = 1$, což je proti předpokladu. Tedy jest též $a^{\frac{p^l-1}{q}} \equiv 1 \pmod{p}$.

Systém kongruencí pro čísla $\sigma_1, \sigma_2, \ldots, \sigma_l$ vypadá tedy takto:

$$\begin{aligned} \sigma_1 &\equiv 1, \\ 2\sigma_2 + \sigma_1 &\equiv 1, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ (l-1)\,\sigma_{l-1} + \ldots + \sigma_1 &\equiv 1, \\ l\sigma_l + \ldots + \sigma_1 &\equiv q. \end{aligned} \pmod{p}.$$

Odtud plyne

$$\sigma_1 \equiv 1, \quad 2\sigma_2 \equiv 0, \quad 3\sigma_3 \equiv 0, \quad \ldots, \quad (l-1)\,\sigma_{l-1} \equiv 0, \quad l\sigma_l \equiv q - 1.,$$

Ježto je $q < p$ a ježto platí $\sigma_1 + 2\sigma_2 + \ldots + l\sigma_l + \ldots + q\sigma_q = q$, je jediné řešení

$$\sigma_1 = 1, \quad l\sigma_l = q - 1, \quad \sigma_2 = \sigma_3 = \ldots = \sigma_{l-1} = 0.$$