Dorota Krajňáková

Poznámka k teórii potenčných zvyškov (mod p^α)

Matematicko-fyzikálny časopis, Vol. 4 (1954), No. 4, 212--217

Persistent URL: http://dml.cz/dmlcz/126858

POZNÁMKA K TEÓRII POTENČNÝCH ZVYŠKOV (mod p^α)

DOROTA KRAJŇÁKOVÁ, Bratislava

Pri riešení istého problému o potenčných zvyškoch (mod p^α) vyskytla sa mi táto otázka: „Koľko je k-tych potenčných zvyškov (mod p^α)?“ V monografiách o teórii čísel nenašla som na túto otázku nikde odpoveď.

Počet k-tych potenčných zvyškov (mod p^α) *nesúdelných* s p a menších ako p^α je, pravda, známy a daný týmto vzorcom:

$$P_k^*(p^\alpha) = \frac{\varphi(p^\alpha)}{(k, \varphi(p^\alpha))} = \frac{p^{\alpha-1}(p-1)}{[k, p^{\alpha-1}(p-1)]} .$$

(Pozri napr.: Vinogradov „Osnovy teórie čísel“, vydanie 6, 1949, str. 99.)

Hlavným obsahom tejto poznámky je dôkaz vety 1. Záverom uvádzam niekoľko poznámok o „hustote rozloženia“ k-tych potenčných zvyškov (mod p^α).

I.

Veta 1. *Nech $k \geqq 1$, $\alpha \geqq 1$ sú ľubovoľné prirodzené čísla. Nech p je prvočíslo, $p > 2$. Nech $(k, p) = 1$. Položme $s = \left[\frac{\alpha - 1}{k}\right]$. Potom počet nenulových k-tych potenčných zvyškov* (mod p^α) *je daný vzorcom*

$$P_k(p^\alpha) = \frac{p-1}{(k, p-1)} \cdot p^{\alpha-1-sk} \cdot \frac{1 - p^{k(s+1)}}{1 - p^k} . \qquad (A)$$

Dôkaz. Reprezentant každej triedy (mod p^α) sa dá písať v tvare

$$a = a_0 + a_1 p + a_2 p^2 + \ldots + a_{\alpha-1} p^{\alpha-1},$$

kde $a_i = 0, 1, 2, \ldots, p-1$. V ďalšom budeme zvyšky vždy predpokladať v tomto tvare. Hľadajme k-te potenčné zvyšky deliteľné p. Zvyšky (mod p^α) deliteľné p sú tie a len tie, pri ktorých je $a_0 = 0$. Teda majú tvar:

$$a = a_1 p + a_2 p^2 + \ldots + a_{\alpha-1} p^{\alpha-1}.$$

(Prípad $a = 0$ nebudeme uvažovať, pretože 0 je zvyškom ľubovoľného stupňa podľa ľubovoľného modulu m.)

Ak má byť toto číslo a k-tou mocninou (mod p^α), musí existovať také číslo b,

$$b = \xi_0 + \xi_1 p + \xi_2 p^2 + \ldots + \xi_{\alpha-1} p^{\alpha-1},$$

že platí:

$$a_1 p + a_2 p^2 + \ldots + a_k p^k + \ldots + a_{\alpha-1} p^{\alpha-1} \equiv (\xi_0 + \xi_1 p + \xi_2 p^2 + \ldots + \xi_{\alpha-1} p^{\alpha-1})^k \pmod{p^\alpha}.$$

Z tejto kongruencie vyplýva, že musí byť nevyhnutne $\xi_0 = 0$. Potom však číslo a je deliteľné najmenej k-tou mocninou p a má tvar:

$$a = a_k p^k + a_{k+1} p^{k+1} + \ldots + a_{\alpha-1} p^{\alpha-1}.$$

To znamená, že k-te potenčné zvyšky deliteľné p môžu existovať len vtedy, keď je $\alpha - 1 \geqq k$, t. j. $\alpha > k$.

Predpokladajme teraz, že je $\alpha > k$ a $a_k \neq 0$. Potom môžeme písať:

$$a = p^k (a_k + a_{k+1} p + \ldots + a_{\alpha-1} p^{\alpha-k-1}).$$

Keď je toto číslo a k-tou mocninou (mod p^α), je:

$$p^k (a_k + a_{k+1} p + \ldots + a_{\alpha-1} p^{\alpha-k-1}) \equiv (\xi_1 p + \xi_2 p^2 + \ldots + \xi_{\alpha-1} p^{\alpha-1})^k \pmod{p^\alpha},$$

$$a_k + a_{k+1} p + \ldots + a_{\alpha-1} p^{\alpha-k-1} \equiv (\xi_1 + \xi_2 p + \ldots + \xi_{\alpha-1} p^{\alpha-2})^k \pmod{p^{\alpha-k}}.$$

To značí: číslo

$$a_k + a_{k+1} p + a_{k+2} p^2 + \ldots + a_{\alpha-1} p^{\alpha-k-1}$$

musí byť k-tou mocninou (mod $p^{\alpha-k}$).

Podľa predpokladu $a_k \neq 0$, čiže je to nesúdelný zvyšok (mod $p^{\alpha-k}$). Medzi takýmito číslami je k-tych mocnín (mod $p^{\alpha-k}$) presne:

$$P_k^*(p^{\alpha-k}) = \frac{\varphi(p^{\alpha-k})}{[k, \varphi(p^{\alpha-k})]} = \frac{p^{\alpha-k} - p^{\alpha-k-1}}{[k, p^{\alpha-k-1}(p-1)]}.$$

Teda existuje najviac $P_k^*(p^{\alpha-k})$ k-tych potenčných zvyškov (mod p^α), ktoré sú deliteľné práve p^k, a nie vyššou mocninou p.

Teraz ukážeme, že je ich presne toľko. Ukážeme totiž: ak číslo

$$\beta = a_k + a_{k+1} p + \ldots + a_{\alpha-1} p^{\alpha-k-1}$$

je k-tou mocninou (mod $p^{\alpha-k}$), je aj k-tou mocninou (mod p^α).

Podľa predpokladu existuje také η, [$\eta \not\equiv 0 \pmod{p}$], že je

$$\beta \equiv \eta^k \pmod{p^{\alpha-k}}. \tag{1}$$

Hľadajme t také, aby bolo:

$$\beta \equiv (\eta + t p^{\alpha-k})^k \pmod{p^{\alpha-k+1}}.$$

Musí byť:

$$\beta \equiv \eta^k + \binom{k}{1} \eta^{k-1} \cdot t \cdot p^{\alpha-k} + \binom{k}{2} \eta^{k-2} \cdot t^2 \cdot p^{(\alpha-k)2} + \ldots + \binom{k}{k} t^k p^{k(\alpha-k)} \pmod{p^{\alpha-k+1}}.$$

Podľa predpokladu je $\alpha - 1 \geqq k$, teda je: $0 \leqq \alpha - k - 1$ a ďalej:

$$\alpha - k - 1 \leqq 2(\alpha - k - 1) = 2(\alpha - k) - 2 < 2(\alpha - k).$$

Preto musí platiť:

$$\beta - \eta^k \equiv k\eta^{k-1} \,.\, t \,.\, p^{\alpha-k} \pmod{p^{\alpha-k+1}}.$$

Ale z kongruencie (1) vyplýva, že ľavá strana, t. j. $\beta - \eta^k$, je deliteľná $p^{\alpha-k}$. Teda musí platiť:

$$\frac{\beta - \eta^k}{p^{\alpha-k}} \equiv k\eta^{k-1} \,.\, t \pmod{p}. \tag{2}$$

Uvažujme teraz takto: Keďže je $(k, p) = 1$, lineárna kongruencia (2) má riešenie $t = t_1$. Položme $\eta_1 = \eta + t_1 p^{\alpha-k}$. Dosadením a umocnením sa presvedčíme, že toto číslo vyhovuje kongruencii

$$\beta \equiv \eta_1^k \pmod{p^{\alpha-k+1}}.$$

Ak postup opakujeme, dokážeme, že existuje také η_2, že platí:

$$\beta \equiv \eta_2^k \pmod{p^{\alpha-k+2}} \text{ atď.}$$

Nakoniec dokážeme, že existuje také η_k, že je:

$$\beta \equiv \eta_k^k \pmod{p^{\alpha}}.$$

Teda medzi číslami tvaru:

$$a_k + a_{k+1}p + \ldots + a_{\alpha-1}p^{\alpha-k-1}, \quad a_k \neq 0$$

je presne

$$P_k^*(p^{\alpha-k}) = \frac{p^{\alpha-k-1}(p-1)}{[k, p^{\alpha-k-1}(p-1)]}$$

k-tych potenčných zvyškov (mod p^{α}).

Vezmime teraz ďalšie čísla deliteľné p, ktoré prichádzajú do úvahy ako k-te mocniny (mod p^{α}). To sú čísla tvaru

$$a_{2k}p^{2k} + a_{2k+1}p^{2k+1} + \ldots + a_{\alpha-1}p^{\alpha-1}.$$

Predpokladajme $a_{2k} \neq 0$ a $\alpha - 1 \geqq 2k$. Aby toto číslo bolo k-tou mocninou, musí byť:

$$p^{2k}(a_{2k} + a_{2k+1}p + \ldots + a_{\alpha-1}p^{\alpha-2k-1}) \equiv (\xi_2 p^2 + \xi_3 p^3 + \ldots + \xi_{\alpha-1}p^{\alpha-1})^k \pmod{p^{\alpha}},$$

t. j.

$$a_{2k} + a_{2k+1}p + \ldots + a_{\alpha-1}p^{\alpha-2k-1} \equiv (\xi_2 + \xi_3 p + \ldots + \xi_{\alpha-1}p^{\alpha-3})^k \pmod{p^{\alpha-2k}}.$$

Čísel tvaru:

$$a_{2k} + a_{2k+1}p + \ldots + a_{\alpha-1}p^{\alpha-2k-1}, \; a_{2k} \neq 0,$$

ktoré sú k-tou mocninou (mod $p^{\alpha-2k}$), je $P_k^*(p^{\alpha-2k})$. Teda najviac je $P_k^*(p^{\alpha-2k})$ k-tych mocnín (mod p^{α}), ktoré sú deliteľné práve p^{2k}. Práve tak ako hore

sa dokáže, že každé číslo práve napísaného tvaru, ktoré je k-tou mocninou (mod $p^{\alpha-2k}$), je tiež k-tou mocninou (mod p^{α}). Teda existuje presne

$$P_k^*(p^{\alpha-2k}) = \frac{\varphi(p^{\alpha-2k})}{[k, \varphi(p^{\alpha-2k})]} = \frac{p^{\alpha-2k-1}(p-1)}{[k, p^{\alpha-2k-1}(p-1)]}$$

k-tych mocnín (mod p^{α}) deliteľných práve p^{2k}.

Keď opakujeme vykonanú úvahu, pre počet všetkých k-tych mocnín (mod p^{α}) dostaneme tento vzorec:

$$P_k(p^{\alpha}) = P_k^*(p^{\alpha}) + P_k^*(p^{\alpha-k}) + P_k^*(p^{\alpha-2k}) + \ldots + P_k^*(p^{\alpha-sk}).$$

Pritom za číslo s volíme najväčšie nezáporné celé číslo, ktoré spĺňuje podmienku $1 \leqq \alpha - sk \leqq k$, t. j. volíme $s = \left[\frac{\alpha-1}{k}\right]$. Dosadením dostávame:

$$P_k(p^{\alpha}) = \frac{p^{\alpha-1}(p-1)}{[k, p^{\alpha-1}(p-1)]} + \frac{p^{\alpha-k-1}(p-1)}{[k, p^{\alpha-k-1}(p-1)]} + \frac{p^{\alpha-2k-1}(p-1)}{[k, p^{\alpha-2k-1}(p-1)]} + \ldots + \frac{p^{\alpha-sk-1}(p-1)}{[k, p^{\alpha-sk-1}(p-1)]}.$$

Keďže je $(k, p) = 1$, menovateľ je v každom výraze rovný $(k, p-1)$. Je teda

$$P_k(p^{\alpha}) = \frac{p-1}{(k, p-1)} \cdot [p^{\alpha-1} + p^{\alpha-k-1} + p^{\alpha-2k-1} + \ldots + p^{\alpha-sk-1}].$$

Sčítaním dostávame:

$$P_k(p^{\alpha}) = \frac{p-1}{(k, p-1)} \cdot p^{\alpha-1-sk} \cdot \frac{1-p^{k(s+1)}}{1-p^k}.$$

Tým je veta 1 dokázaná.

II.

Vyšetrujme teraz „hustotu rozloženia" k-tych potenčných zvyškov (mod p^{α}) za predpokladu $(k, p) = 1$.

Vyšetrujme najprv pomer $\frac{P_k^*(p^{\alpha})}{p^{\alpha}}$ a $\frac{P_k(p^{\alpha})}{p^{\alpha}}$. Je

$$\frac{P_k^*(p^{\alpha})}{p^{\alpha}} = \frac{1}{p^{\alpha}} \cdot \frac{p^{\alpha-1}(p-1)}{[k, p^{\alpha-1}(p-1)]} = \frac{1}{(k, p-1)} \cdot \left(1 - \frac{1}{p}\right).$$

Tento pomer je teda nezávislý od α.

Pre druhý výraz dostaneme:

$$\frac{P_k(p^{\alpha})}{p^{\alpha}} = \frac{1}{p^{\alpha}} \cdot \frac{p-1}{(k, p-1)} \cdot p^{\alpha-1-sk} \cdot \frac{1-p^{k(s+1)}}{1-p^k} = \frac{p-1}{p(k, p-1)} \cdot \frac{p^k - p^{-sk}}{p^k - 1}.$$

Tento výraz je závislý od α. Z vyjadrenia však vidieť, že keď p je pevné a $\alpha \to \infty$ (a teda $s \to \infty$), existuje $\lim_{\alpha\to\infty} \frac{P_k(p^\alpha)}{p^\alpha}$ a platí:

$$\lim_{\alpha\to\infty} \frac{P_k(p^\alpha)}{p^\alpha} = \frac{p^k - p^{k-1}}{p^k - 1} \cdot \frac{1}{(k, p-1)} .$$

Rýchlosť konvergencie je daná touto vetou:

Veta 2. *Nech* $(k, p) = 1$. *Potom*

$$\frac{P_k(p^\alpha)}{p^\alpha} = \frac{p^k - p^{k-1}}{p^k - 1} \cdot \frac{1}{(k, p-1)} + 0\left(\frac{1}{p^\alpha}\right),$$

pričom konštanty obsažené v symbole 0 *nezávisia od* α.

Dôkaz. Platí:

$$\left|\frac{P_k(p^\alpha)}{p^\alpha} - \frac{p^k - p^{k-1}}{p^k - 1} \cdot \frac{1}{(k, p-1)}\right| = \left|\frac{p-1}{p(k, p-1)} \cdot \frac{p^k - p^{-sk}}{p^k - 1} - \frac{p^k - p^{k-1}}{p^k - 1} \cdot \right.$$

$$\left. \cdot \frac{1}{(k, p-1)}\right| = \frac{1}{(k, p-1)} \left|\frac{1-p}{p} \cdot \frac{1}{p^{sk}} \cdot \frac{1}{p^k - 1}\right| = \frac{1}{(k, p-1)} \cdot \left|\frac{1-p}{p(p^k - 1)}\right| \cdot$$

$$\cdot \frac{1}{p^{sk}} < c_1 \cdot \frac{1}{p^{sk}} = c_1 \cdot p^{-\left[\frac{\alpha-1}{k}\right] \cdot k} < c_1 p^{-\left(\frac{\alpha-1}{k} - 1\right) k} = c_2 \cdot \frac{1}{p^\alpha},$$

kde c_1 a c_2 sú konštanty nezávislé od α. Z toho ihneď vyplýva tvrdenie našej vety.

Poznámka. Nechajme naopak α konštantné a nech $p \to \infty$. Potom výrazy

$$\frac{P_k(p^\alpha)}{p^\alpha} \quad \text{a} \quad \frac{P_k^*(p^\alpha)}{p^\alpha}$$

nemajú pre $p \to \infty$ vo všeobecnosti limitu. Výrazy $1 - \frac{1}{p}, \frac{p-1}{p} \cdot \frac{p^k - p^{-sk}}{p^k - 1}$ majú síce za limitu číslo 1, ale výraz $(k, p-1)$ kolíše medzi 1 a k. Isté závery možno však získať.

Predne existuje nekonečne mnoho prvočísel takých, že $(k, p-1) = k$. Lebo podľa Dirichletovej vety v aritmetickej postupnosti $nk + 1$ $(n = 1, 2, 3, \ldots)$ existuje nekonečne mnoho prvočísel p_i. Pre každé také prvočíslo je $p_i = n_i k + 1$, t. j. $(p_i - 1, k) = k$. Z toho vyplýva ihneď:

$$\liminf_{p\to\infty} \frac{P_k(p^\alpha)}{p^\alpha} = \liminf_{p\to\infty} \frac{P_k^*(p^\alpha)}{p^\alpha} = \frac{1}{k}. \tag{a}$$

Ďalej nech je k *nepárne*. Potom existuje nekonečne mnoho prvočísel, pre ktoré je $(k, p-1) = 1$. Podľa Dirichletovej vety totiž v aritmetickej postupnosti $nk + 2$ $(n = 1, 2, 3, \ldots)$ existuje nekonečne mnoho prvočísel p_l.

Pre každé také p_l je $p_l = n_l k + 2$, t. j. $p_l - 1 = n_l k + 1$, t. j. nevyhnutne $(p_l - 1, k) = 1$. Teda pre nepárne k je:

$$\limsup_{p\to\infty} \frac{P_k(p^\alpha)}{p^\alpha} = \limsup_{p\to\infty} \frac{P_k^*(p^\alpha)}{p^\alpha} = 1 . \tag{b}$$

Nech je k *párne*. Potom je $(k, p-1) \geqq 2$. Tvrdím, že existuje nekonečne mnoho prvočísel p_m, pre ktoré je $(k, p_m - 1) = 2$. Nech najvyššia mocnina čísla 3, ktorou je číslo k deliteľné, je 3^α, $\alpha \geqq 0$. Potom je $\left(\frac{k}{3^\alpha}, 3\right) = 1$. Teda podľa Dirichletovej vety existuje v postupnosti $n \cdot \frac{k}{3^\alpha} + 3$ $(n = 1, 2, 3, \ldots)$ nekonečne mnoho prvočísel p_m. Pre každé také prvočíslo p_m je:

$$p_m = n_m \cdot \frac{k}{3^\alpha} + 3 , \text{ t. j. } p_m - 1 = n_m \cdot \frac{k}{3^\alpha} + 2 .$$

Nech $d/p_m - 1$ a d/k. Potom je nevyhnutne $d/2$, t. j. $(p_m - 1, k) = 2$. Pre párne k teda je:

$$\limsup_{p\to\infty} \frac{P_k(p^\alpha)}{p^\alpha} = \limsup_{p\to\infty} \frac{P_k^*(p^\alpha)}{p^\alpha} = \frac{1}{2} . \tag{c}$$

Z výsledkov (a), (b), (c) vyplýva, že limita existuje v jedinom prípade, a to pre $k = 2$. Potom je:

$$\lim_{p\to\infty} \frac{P_2(p^\alpha)}{p^\alpha} = \lim_{p\to\infty} \frac{P_2^*(p^\alpha)}{p^\alpha} = \frac{1}{2} .$$

Došlo dňa 30. IV. 1954.

Katedra matematiky SVŠT
v Bratislave

ЗАМЕТКА О ВЫЧЕТАХ СТЕПЕНИ $k \pmod{p^\alpha}$

Д. КРАЙНЯКОВА

Выводы

В статье доказывается между иными следующая теорема.

Пусть $k \geqq 1$, $\alpha \geqq 1$ — натуральные числа, $p > 2$ простое число. Пусть $(k, p) = 1$, $s = \left[\frac{\alpha - 1}{k}\right]$. Обозначим симболом $P_k(p^\alpha)$ число вычетов степени k (отличных от нуля) mod p^α. Потом имеет место уравнение (A).