MATEMATICKO-FYZIKÁLNY ČASOPIS SAV, 13, 2, 1963

O JEDNEJ SÚSTAVE KONGRUENCIÍ

POZNÁMKA K PREDCHÁDZAJÚCEMU ČLÁNKU J. SEDLÁČKA

ŠTEFAN SCHWARZ, Bratislava

V predchádzajúcom článku [1] položil J. Sedláček túto otázku: Nech T_p je teleso tried zvyškov (mod p). Pýtame sa, či sústava rovníc

$$x + y + z = 1, \qquad (1)$$
$$xyz = 1,$$

má riešenie v telese T_p.

Sedláček ukázal elementárnou úvahou, že pre prvočísla tvaru $4k + 1$ a prvočísla tvaru $8k + 7$ riešenie vždy existuje. Pre prvočísla tvaru $8k + 3$ našiel, že riešenie neexistuje pre $p = 3$, ale existuje pre $p = 11$ a $p = 19$.

V tejto poznámke ukážeme, používajúc pritom veľmi neelementárne výsledky z teórie kongruencií, že prípad $p = 3$ je celkom výnimočný. Platí totiž:

Veta. *Pre každé $p \neq 3$ má sústava* (1) *riešenie v telese T_p.*

Dôkaz. V prípade $p = 2$ je úloha triviálna. V ďalšom budeme preto predpokladať $p \neq 2$.

Sústava (1) je ekvivalentná s rovnicou $xy(1 - x - y) = 1$, t. j. s rovnicou

$$yx^2 + (y^2 - y)\,x + 1 = 0. \qquad (2)$$

Pri pevnom $y \neq 0$ (z telesa T_p) má táto kvadratická rovnica v x riešenie v telese T_p vtedy a len vtedy, ak jej diskriminant $(y^2 - y)^2 - 4y$ je štvorcom nejakého elementu z T_p. To nastane vtedy a len vtedy, ak rovnica

$$y^4 - 2y^3 + y^2 - 4y = t^2 \qquad (3)$$

má v telese T_p riešenie (y, t), v ktorom $y \neq 0$. Označme znakom N počet riešení rovnice (3) v telese T_p. Nutná a postačujúca podmienka pre riešiteľnosť sústavy (1) je teda splnenie podmienky $N > 1$.

Teraz použijeme jeden hlboký výsledok z teórie kongruencií, ktorý znie takto: Nech je daná kongruencia

$$a_0y^4 + a_1y^3 + a_2y^2 + a_3y + a_4 \equiv t^2 \pmod{p}, \qquad a_0 \neq 0. \qquad (4)$$

Nech polynóm 4. stupňa na ľavej strane nie je násobkom štvorca nejakého kvadratického polynómu (mod p). Potom pre počet N_1 (navzájom inkongruentných) riešení kongruencie (4) platí:

$$|N_1 - (p - 1)| \leqq 2\sqrt{p}.$$

Výsledky tohto druhu sú uvedené v knihe H. Hasse [2] (str. 163–188). Podrobné dôkazy možno nájsť v literatúre citovanej v tejto knihe.(¹)

Polynóm na ľavej strane rovnice (3) sa nedá písať v tvare násobku štvorca kvadratického polynómu nad T_p, lebo z rovnosti

$$y^4 - 2y^3 + y^2 - 4y = c(y^2 + ay + b)^2$$

by nutne vyplývalo $b = 0$, čo však vedie k rozporu, keďže najnižšia mocnina y na ľavej strane je $-4y$ (a to je v T_p rôzne od nuly), zatiaľ čo na pravej strane vystupuje y až v mocnine $\geqq 2$.

Zo vzťahu (5) vyplýva preto $N \geqq p - 1 - 2\sqrt{p}$. Pre $p \geqq 11$ je $p - 1 - 2\sqrt{p} > 1$, teda sústava (1) má riešenie. Pre $p = 7$ je riešením trojica (4, 5, 6), pre $p = 5$ je riešením (1, 2, 3). Pre $p = 3$ sa bezprostredným dosadením presvedčíme, že riešenie neexistuje. Tým je naše tvrdenie dokázané.

LITERATÚRA

[1] Sedláček J., *Několik poznámek k problému W. Mnicha*, Matematicko-fyzikálny časopis SAV *13* (1963), 97—102.

[2] Haase H., *Лекции по теории чисел* (preklad z nemčiny), Москва 1953.

[3] Mordell L. J., *The number of solutions of some congruences in two variables*, Math. Z. *37* (1933), 193—209.

[4] Mordell L. J., *Note on the linear symetric congruence in n variables*, Canad. J. Math. *5* (1953), 433—438.

(¹) Poznamenajme, že pre náš účel by sme mohli v podstate vystačiť i s menej ostrými odhadmi, ktoré našiel prvý L. J. Mordell ([3]). Mordell sa zaoberal otázkou o počte riešení kongruencií tvaru $f(y) \equiv t^m (\mathrm{mod}\, p)$, $m \geqq 2$. Pri dôkazoch používal jednoduchšie metódy; v prípade $m = 2$ sú, pravda, jeho výsledky slabšie než odhad udaný v texte. Vyplýva z nich však bezprostredne, že existuje také číslo $p_0 > 0$, že pre prvočísla $p > p_0$ má sústava (1) vždy riešenie. (Pozri aj prácu [4].)