Karel Koutský

Obdoba Wilsonovy poučka

Časopis pro pěstování matematiky a fysiky, Vol. 56 (1927), No. 3, 145--147

Persistent URL: http://dml.cz/dmlcz/109046

Obdoba Wilsonovy poučky.

Napsal Dr. *Karel Koutský.*

1. *Vandermondeův determinant:*

$$\Delta \equiv \begin{vmatrix} 1, & 1, & 1^2, & \ldots\ldots & 1^{p-2} \\ 1, & 2, & 2^2, & \ldots\ldots & 2^{p-2} \\ 1, & 3, & 3^2, & \ldots\ldots & 3^{p-2} \\ \vdots & & & & \vdots \\ 1, & (p-1), & (p-1)^2, & \ldots\ldots & (p-1)^{p-2} \end{vmatrix},$$

kdež p *jest liché prvočíslo, jest vždy kořenem kongruence:*

$$x^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Tudíž platí:

$$\Delta^2 \equiv \pm 1 \pmod{p},$$

podle toho, je-li p prvočíslem tvaru $(4n-1)$ resp. $(4n+1)$.

Důkaz: Vyčíslením determinantu Δ obdržíme po úpravě:*)

$$\Delta = 1!\ 2!\ 3!\ \ldots\ldots (p-2)! \qquad (1)$$

Z Wilsonovy poučky:

$$(p-1)! \equiv -1 \pmod{p}$$

plyne jednoduchým obratem:

$$(p-k)!\ (k-1)! \equiv (-1)^k \pmod{p},$$

kdež k jest libovolné celé a kladné číslo, menší než p.

Lze tedy psáti

$$\left.\begin{aligned} (p-2)!\ 1! &\equiv (-1)^2 \\ (p-3)!\ 2! &\equiv (-1)^3 \\ (p-4)!\ 3! &\equiv (-1)^4 \\ \ldots\ldots\ldots & \\ 1!\ (p-2)! &\equiv (-1)^{p-1} \end{aligned}\right\} \pmod{p}.$$

Znásobením těchto kongruencí obdržíme:

$$[1!\,2!\,3!\ldots.(p-1)!]^2 = (-1)^{2+3+4+\ldots.+(p-1)} = (-1)^{(p-2)\frac{p+1}{2}} \pmod{p};$$

*) Pascal: Repertorium I. 1. (1910) str. 68. Úpravou obecného vzorce lze pro tento zvláštní Vandermondeův determinant dosáhnouti hodnoty, kterou jsem uvedl.

poněvadž pak p jest *liché* prvočíslo, tedy $(p-2)$ jest též liché číslo, bude:

$$[1!\ 2!\ 3!\ldots\ldots\ (p-1)!]^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Dosadíme-li do této kongruence z kongruence (1), dostaneme:

$$\Delta^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}, \qquad (2)$$

čímž předložená věta jest dokázána.

2. Z Wilsonovy poučky

$$(p-1)! \equiv -1 \pmod{p}$$

plyne:

$$[(p-1)!]^4 \equiv 1 \pmod{p}.$$

Vzhledem ke kongruenci (2) pak bude:

$$\Delta^4 . [(p-1)!]^4 \equiv (-1)^{p+1} \pmod{p},$$

pokud p bude l i c h é prvočíslo. Poněvadž potom $(p+1)$ jest sudé číslo, lze vzhledem k (1) zapsati tuto kongruenci ve tvaru:

$$\Pi^4 \equiv [1!\ 2!\ 3!\ldots.(p-2)!\ (p-1)!]^4 \equiv 1 \pmod{p}. \qquad (3)$$

Odtud jest však patrno, že tato kongruence platí též pro $p=2$.

K o n g r u e n c e:

$$\Pi^4 - 1 \equiv 0 \pmod{p} \qquad (3')$$

j e s t t e d y v ž d y s p l n ě n a, p o k u d p j e s t p r v o č í s l o. O b r á c e n ě pak, j e - l i t a t o k o n g r u e n c e s p l n ě n a, j e s t p n u t n ě p r v o č í s l e m.

Důkaz: Π tedy i Π^4 jest dělitelno každým číslem menším než p; tedy (Π^4-1) není žádným číslem menším než p dělitelno. Je-li tedy kongruence (3') splněna, platí:

$$\Pi^4 - 1 = p \,.\, s,$$

kdež s jest nějaké číslo celé a větší než p. — Předpokládejme nyní, že p není prvočíslem, ale číslem složeným; p_1 budiž jedním z jeho dělitelů. Potom platí:

$$1 < |p_1| < |p|$$

a

$$p = p_1 p_2,$$

kdež p_2 jest číslo celé. Dosazením obdržíme:

$$\Pi^4 - 1 = p_1 p_2 s,$$

odkudž plyne, že (Π^4-1) jest dělitelno jistým číslem p_1, které co do absolutní hodnoty jest menší než p. To však podle předešlé úvahy jest nemožné. Nemůže tedy p býti nikdy složeným číslem, pokud kongruence (3) jest splněna a musí tedy býti prvočíslem, *c . b . d.*

Kongruence (3) vyjadřuje tedy *poučku obdobnou poučce Wilsonově.*

*

Sur une formule analogue à celle de Wilson.

(Extrait de l'article précédent.)

La formule en question est fournie par la congruence (3) du texte tchèque.
