Příspěvek k nauce o číslech.

Napsal

Vilém Jung v Pardubicích.

Značí-li a, p čísla nesoudělná a utvoříme-li si

$$Z\left(\frac{a}{p}\right) = \alpha_1$$

$$Z\left(\frac{2a}{p}\right) = \alpha_2$$

$$Z\left(\frac{3a}{p}\right) = \alpha_3$$

$$\vdots$$

$$Z\left(\frac{(p-1)\,a}{p}\right) = \alpha_{p-1}\,,$$

pak jsou α_1, α_2, α_3 ... α_{p-1} zbytky od sebe různé.*)

Zároveň tu platí zákon:

$$\alpha_k = \alpha_1 + \alpha_{k-1} \quad \text{a je-li} \quad \alpha_1 + \alpha_{k-1} > p$$

$$\alpha_k = Z\left(\frac{\alpha_1 + \alpha_{k-1}}{p}\right)$$

neb obecněji

$$Z\left(\frac{\alpha_k}{p}\right) = Z\left(\frac{\alpha_1 + \alpha_{k-1}}{p}\right).$$

Tento zákon jest zvláštním případem všeobecnějšího, jehož odvození krátce tuto podám. Patrno, že

$$Z\left(\frac{(k+i)\,a}{p}\right) - Z\left(\frac{ka}{p}\right) = Z\left(\frac{ia}{p}\right)$$

to jest $\alpha_{k+i} = \alpha_k + \alpha_i$ a je-li $\alpha_k + \alpha_i > p$

$$\alpha_{k+i} = Z\left(\frac{\alpha_k + \alpha_i}{p}\right)$$

neb obecněji

$$Z\left(\frac{\alpha_{k+i}}{p}\right) = Z\left(\frac{\alpha_k}{p}\right) + Z\left(\frac{\alpha_i}{p}\right). \qquad (1)$$

*) Viz Dr. *Studničky:* „Nauka o číslech“ pag. 88. —

Z tohoto vzorce si odvodíme jiný, který nám k rychlému vyčíslení jakéhokoli α_n poslouží, při čemž třeba jen α_1 znáti které snadno odvodíme.

Položme $i = (n-1)\,k$, kde $n < \frac{p}{k}$ pak

$$\alpha_{nk} = \alpha_k + \alpha_{(n-1)k}$$

a je-li

$$\alpha_k + \alpha_{(n-1)k} > p, \quad \alpha_{nk} = Z\left(\frac{\alpha_k + \alpha_{(n-1)k}}{p}\right)$$

obecněji

$$Z\left(\frac{\alpha_{nk}}{p}\right) = Z\left(\frac{\alpha_k}{p}\right) + Z\left(\frac{\alpha_{(n-1)k}}{p}\right)$$

obdobně

$$Z\left(\frac{\alpha_{(n-1)k}}{p}\right) = Z\left(\frac{\alpha_k}{p}\right) + Z\left(\frac{\alpha_{(n-2)k}}{p}\right)$$

$$Z\left(\frac{\alpha_{(n-2)k}}{p}\right) = Z\left(\frac{\alpha_k}{p}\right) + Z\left(\frac{\alpha_{(n-3)k}}{p}\right)$$

$$\vdots$$

$$Z\left(\frac{\alpha_{2k}}{p}\right) = Z\left(\frac{\alpha_k}{p}\right) + Z\left(\frac{\alpha_k}{p}\right)$$

$$Z\left(\frac{\alpha_k}{p}\right) = Z\left(\frac{\alpha_k}{p}\right).$$

Sečtením na obou stranách povstane pak

$$Z\left(\frac{\alpha_{nk}}{p}\right) = nZ\left(\frac{\alpha_k}{p}\right) = Z\left(\frac{n\alpha_k}{p}\right). \qquad (2)$$

Znamená-li α_{nk}, zbytek absolutně menší než p, pak jest

$$\alpha_{nk} = Z\left(\frac{n\alpha_k}{p}\right)$$

je-li $n\alpha_k > p$.

Je-li konečně $k = 1$, plyne z toho

$$\alpha_n = Z\left(\frac{n\alpha_1}{p}\right), \text{ kde } \alpha_n < p \text{ a } n\alpha_1 > p$$

Tento vzorec má praktickou cenu v případech, kde je a velké, α_1 pak poměrně malé.

Je-li $a < p$, pak postrádá vzorec ceny, když nejmenší zbytek $\alpha_1 = a$.