PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **24** (1996/1997)
Številka 5
Strani 290–295

Primož Potočnik:

NENAVADNA ARITMETIKA ALI NE POSKUŠAJTE TEGA V ŠOLI!

Ključne besede: matematika.

Elektronska verzija: http://www.presek.si/24/1306-Potocnik.pdf

NENAVADNA ARITMETIKA ALI NE POSKUŠAJTE TEGA V ŠOLI!

Gotovo ne bi poželi prevelikih simpatij svojih učiteljic oziroma učiteljev matematike, če bi pri kontrolnih nalogah pisali enakosti

$$1+1=0, \quad 1+3=2, \quad 2+3=1, \quad 2\cdot 3=5, \quad 3\cdot 7=9\,.$$

Bojim se, da vas iz kaše ne bi izvlekel niti pričujoči prispevek, zato vam toplo priporočam, da (ne)znanja, ki ga boste pridobili s prebiranjem naslednjih vrstic, ne uporabite v šoli.

Za kaj gre? Vzemimo dve naravni števili a in b ter ju zapišimo dvojiško. Naj tu povem, da bomo v nadaljevanju število 0 vseskozi prištevali k množici naravnih števil.

$$a = a_o + a_1\cdot 2 + a_2\cdot 2^2 + \ldots + a_n\cdot 2^n = a_n a_{n-1}\ldots a_{o(2)}; \quad a_i \in \{0,1\}$$
$$b = b_o + b_1\cdot 2 + b_2\cdot 2^2 + \ldots + b_m\cdot 2^m = b_m b_{m-1}\ldots b_{o(2)}; \quad b_i \in \{0,1\}\,.$$

Definirajmo vsoto števil a in b na običajen način, le da pri seštevanju *v kupčku* ne prenašamo *viška* v naslednji stolpec. Da ne bo prihajalo do zmede, bomo takšno seštevanje označevali s $\oplus$, navadno pa s $+$. Velja torej

$$c = a\oplus b, \quad \text{kjer } c = c_s c_{s-1}\ldots c_{o(2)}, \quad s=\max\{m,n\}$$
$$\text{in } c_k = a_k + b_k (\mathrm{mod}\ 2)\,.$$

Oglejmo si zgled. $1 = 1_{(2)}$, $3 = 11_{(2)}$,

$$\begin{array}{r} 1_{(2)} \\ 11_{(2)} \\ \hline 10_{(2)}\,. \end{array}$$

Ko smo v desnem stolpcu sešteli $1+1$, smo dobili $2 = 10_{(2)}$, kar je po modulu 2 enako 0.[1] Desni stolpec rezultata je zato enak 0. Pri običajnem seštevanju bi enico prenesli v levi stolpec, tu pa tega nismo storili.

---

[1] Da je neko število a po modulu m enako številu b, pomeni, da je število $a-b$ deljivo s številom m, oziroma, da dasta števili a in b pri deljenju s številom m enaka ostanka.

Tako definirano seštevanje ima vse lepe lastnosti navadnega seštevanja. Z lahkoto se namreč lahko prepričamo, da velja:

$$(a \oplus b) \oplus c = a \oplus (b \oplus c), \tag{1}$$

$$a \oplus b = b \oplus a\,, \tag{2}$$

$$0 \oplus a = a \oplus 0 = a\,. \tag{3}$$

Poleg teh običajnih lastnosti pa velja še mnogo manj običajna:

$$a \oplus a = 0\,. \tag{4}$$

To pa lahko preberemo tudi drugače:

Za vsako naravno število a obstaja tako naravno število b, da velja $a \oplus b = b \oplus a = 0$.

Takšnemu številu, ki je v našem primeru kar enako številu a samemu, rečemo običajno k a nasprotno število. Ugotovili smo torej, da ima v množici naravnih števil vsako število svoje nasprotno število glede na operacijo $\oplus$. To pa je že lastnost, ki je navadno seštevanje ne premore. Tu bi bilo naravnemu številu a obratno število število $-a$, ki pa ni več naravno, saj je negativno, če je le $a \neq 0$. Gimnazijci bodo ugotovili:

Množica naravnih števil tvori skupaj z operacijo $\oplus$ komutativno (Abelovo) grupo.

Pomeni, da je operacija $\oplus$ v nekem smislu celo lepša kot $+$, saj navadno seštevanje v množici naravnih števil ne tvori grupe.

Podobno kot smo definirali operacijo $\oplus$, definirajmo še množenje $\odot$. Števili a in b, ki ju množimo, spet napišemo dvojiško in množimo *v kupčku* kot običajno, le da pri seštevanju po stolpcih ne prenašamo *viška* na naslednji stolpec. Zapisano s simboli

$$a_n a_{n-1} \ldots a_{o(2)} \odot b_m b_{m-1} \ldots b_{o(2)} = c_s c_{s-1} \ldots c_{o(2)}\,,$$

kjer

$$s = m + n \quad \text{in} \quad c_k = \Big(\sum_{i+j=k} a_i b_j\Big) (\mathrm{mod}\ 2)\,. \tag{M}$$

Spet si oglejmo zgled: $7 = 111_{(2)}$, $3 = 11_{(2)}$,

$$\begin{array}{l} \underline{111_{(2)} \odot 11_{(2)}} \\ 111 \\ \underline{\ 111} \\ 1001_{(2)} \end{array} \qquad = 9\,.$$

Brez težav se prepričamo, da velja

$$(a \odot b) \odot c = a \odot (b \odot c), \tag{5}$$

$$a \odot b = b \odot a, \tag{6}$$

$$1 \odot a = a \odot 1 = a \tag{7}$$

in da veže obe operaciji zakon distributivnosti

$$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)\,. \tag{8}$$

Dogovorimo se takoj, da bomo izraz $a \oplus (b \odot c)$ pisali poenostavljeno $a \oplus b \odot c$ in pri tem tiho privzeli, da ima množenje prednost pred seštevanjem.

Gimnazijec bo iz zakonov (5) – (8) zopet ugotovil, da množica naravnih števil skupaj z operacijama $\oplus$ in $\odot$ tvori kolobar (komutativen in z enoto 1), podobno kot ga tvori množica celih števil z operacijama običajnega seštevanja in množenja.[2]

Poleg tega, da operaciji $\oplus$ in $\odot$ prekašata navadni operaciji seštevanja in množenja v tem, da prelevita množico $\mathbb{N}$ v kolobar, pa velja še nekaj zanimivih lastnosti.

Spomnimo se, kolikokrat smo si želeli, da bi smeli kvadrirati dvočlenik kar po domače $(a + b)^2 = a^2 + b^2$, in se vedno znova spraševali, zakaj je svet tako grd, da moramo vrivati še mešani člen $2ab$. No, če bi namesto operacij $+$ in $\cdot$ uporabljali operaciji $\oplus$ in $\odot$, bi bilo vse lepše. Velja namreč

$$(a \oplus b)^2 = a^2 \oplus b^2\,.$$

Pri tem izraz a^2 pomeni seveda $a \odot a$ in ne $a \cdot a$.

---

[2] Vse zgornje in sledeče trditve bo bralec, ki je seznanjen z nekaj teorije algebre, najlaže dokazal, če bo opazil, da je kolobar $(\mathbb{N}, \oplus, \odot)$ izomorfen kolobarju polinomov nad obsegom ostankov po deljenju s številom 2, torej $\mathbb{Z}_2[X]$. Izomorfizem podaja preslikava $a_n \ldots a_{o(2)} \mapsto a_n x^n + \ldots + a_o$.

Z uporabo pravil (4), (6) in (8) se v zgornjo trditev prepričajmo.

$$\begin{aligned}(a \oplus b)^2 &= (a \oplus b) \odot (a \oplus b) = (a \oplus b) \odot a \oplus (a \oplus b) \odot b = \\ &= a \odot a \oplus b \odot a \oplus a \odot b \oplus b \odot b = \\ &= a^2 \oplus (a \odot b \oplus a \odot b) \oplus b^2 = a^2 \oplus b^2 \,.\end{aligned}$$

Za vajo izpeljimo formulo za $\oplus$-vsoto prvih n naravnih števil. Z nekaj poskušanja uganemo in na koncu z uporabo popolne indukcije dokažemo formulo

$$1 \oplus 2 \oplus \ldots \oplus n = \begin{cases} 1 & \text{za } 4|(n+3) \\ n+1 & \text{za } 4|(n+2) \\ 0 & \text{za } 4|(n+1) \\ n & \text{za } 4|n \end{cases} .$$

Bralec lahko sam izpelje še formuli za $\oplus$-vsoto prvih n sodih in prvih n lihih števil.

Zanimivo je opazovati praštevila v kolobarju $(\mathbb{N}, \oplus, \odot)$. Pojem praštevila je tu definiran enako kot pri običajnih operacijah – praštevilo v kolobarju $(\mathbb{N}, \oplus, \odot)$, recimo mu $\odot$-praštevilo, je takšno naravno število p, ki ga lahko napišemo kot produkt $p = a \odot b$ drugih dveh naravnih števil le, če je eno od števil a in b enako 1, drugo pa p. Dodatno predpišemo še, da število 1 ni praštevilo. Pisec članka je poiskal vsa $\odot$-praštevila, ki so manjša od 500.

2, 3, 7, 11, 13, 19, 25, 31, 37, 41, 47, 55, 59, 61, 67, 73, 87, 91, 97, 103, 109,
115, 117, 131, 137, 143, 145, 157, 167, 171, 185, 191, 193, 203, 211, 213, 229,
239, 241, 247, 253, 283, 285, 299, 301, 313, 319, 333, 351, 355, 357, 361, 369,
375, 379, 391, 395, 397, 415, 419, 425, 433, 445, 451, 463, 471, 477, 487, 499.

Vidimo, da je med njimi nekaj običajnih praštevil, ni pa vseh. Prav tako niso vsa $\odot$-praštevila običajna praštevila. Zanimivo je, da se tudi tu pojavljajo tako imenovani *dvojčki*, to so pari praštevil, ki se razlikujejo le za 2, npr.

$$(11, 13),\ (59, 61),\ (115, 117) \ldots$$

Postavimo si lahko vprašanje, ali je takšnih parov praštevil neskončno, a bojim se, da odgovoriti nanj ni enostavno. Pri običajnih praštevilih je enako vprašanje eno od najslavnejših odprtih problemov teorije števil.

Čeprav se zdijo vprašanja v zvezi s $\odot$-praštevili enako težka kot vprašanja o običajnih praštevilih, je avtorju le uspelo dokazati zanimiv izrek.

Izrek: Če je od 2 različno število p z dvojiškim zapisom $p_n \ldots p_{o(2)}$ $\odot$-praštevilo, je $\odot$-praštevilo tudi število $\bar{p} = p_o \ldots p_{n(2)}$.

Dokaz: Najprej opazimo, da je zadnja dvojiška cifra p_o števila p enaka 1, saj bi se drugače število p lahko zapisalo kot produkt $p = p_n \ldots p_{1(2)} \odot 10_{(2)}$, to pa je v protislovju z dejstvom, da je p od 2 različno $\odot$-praštevilo.

Z grško črko τ označimo funkcijo, ki naravnemu številu $a = a_n \ldots a_{o(2)}$ priredi število $\tau(a) = a_o \ldots a_{n(2)}$. Velja torej $\bar{p} = \tau(p)$. Ker se število p konča na cifro 1, očitno drži enakost $\tau(\tau(p)) = p$.

Funkcija τ pa ima še eno zelo lepo lastnost – je multiplikativna:

$$\tau(a \odot b) = \tau(a) \odot \tau(b) .$$

V to se prepričamo s pomočjo definicije (M), ker pa je račun kar dolg in nič kaj težak, ga izpuščam.

Predpostavimo sedaj, da število $\bar{p}$ ni $\odot$-praštevilo. Tedaj obstajata od 1 in $\bar{p}$ različni naravni števili a in b, tako da velja $\bar{p} = a \odot b$. Vendar tedaj velja tudi

$$p = \tau(\tau(p)) = \tau(\bar{p}) = \tau(a \odot b) = \tau(a) \odot \tau(b) .$$

Ker je p $\odot$-praštevilo, je eno od števil $\tau(a)$ in $\tau(b)$, denimo $\tau(a)$, enako 1. Ker je $a \neq 1$, je število a oblike $10 \ldots 0_{(2)}$. To pa je nemogoče, saj bi bila tedaj zadnja števka produkta $\bar{p}$ tudi enaka 0, kar pa ni, saj je zadnja števka števila $\bar{p}$ hkrati prva števka števila p.

Predpostavka, da število $\bar{p}$ ni $\odot$-praštevilo, nas je pripeljala v protislovje, kar pomeni, da je bila napačna. S tem je izrek dokazan.

Za konec naj vas še prepričam, da operaciji $\oplus$ in $\odot$ nista povsem za lase privlečeni in da imata lahko tudi precejšnjo uporabno vrednost. Tisti bralci, ki berejo Presek že več let, se morda spomnijo zmagovalne strategije pri igri Nim, ki je bila opisana v 4. številki Preseka šolskega leta 1985-86. Naj na hitro ponovim.

Nim je igra, ki jo igrata dva igralca s pomočjo 15 vžigalic, ki jih na začetku razporedita v pet kupčkov po 1, 2, 3, 4 in 5 vžigalic. Igralca

izmenoma jemljeta vžigalice s kupčkov tako, da vsakič pobereta s poljubnega kupčka poljubno število vžigalic (vsaj eno in največ toliko, kot jih na izbranem kupčku je). Zmaga tisti, ki pobere zadnjo vžigalico.

Kako igrati, da bomo zmagali? Denimo, da je v trenutku, ko smo na potezi, v posameznih kupčkih $a_1, a_2, \ldots, a_5$ vžigalic. Seštejmo $s = a_1 \oplus a_2 \oplus \ldots \oplus a_5$. Če je vsota s enaka 0, smo izgubljeni. Če pa je $s \neq 0$, je gotovo (kot se izkaže) res $a_i \oplus s < a_i$ za vsaj en indeks $i \leq 5$. Ko poiščemo tak indeks, poberemo z i-tega kupčka toliko vžigalic, da jih bo ostalo še $a_i \oplus s$. Ker je $a_i \oplus s < a_i$, je to dovoljena poteza. Tedaj se bo naš nasprotnik znašel v situaciji $a_1, \ldots, a_i \oplus s, \ldots, a_5$ z vsoto

$$s = a_1 \oplus \ldots \oplus a_i \oplus s \oplus \ldots \oplus a_5 = s \oplus s = 0$$

in bo izgubljen, saj bo s svojo potezo vsoto 0 gotovo pokvaril. Od tod sledi, da našemu nasprotniku nikoli ne bo uspelo doseči situacije, ko bodo vsi kupčki prazni, saj je takrat vsota s enaka nič.

Na začetku je vsota $1 \oplus \ldots \oplus 5$ enaka 1, kot se to lepo vidi iz formule za vsoto prvih n naravnih števil, in zato tisti, ki je na potezi, dobi (denimo tako, da vzame osamljeno vžigalico s prvega kupčka). Naša formula nam pove tudi, da bi bila za prvega igralca igra izgubljena, če bi igrali z 28 vžigalicami in 7 kupčki, saj je vsota $1 \oplus \ldots \oplus 7$ enaka 0.

Primož Potočnik