

PRESEK

List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652

Letnik 30 (2002/2003)

Številka 4

Strani 226-231

Aleksandar Jurišić:

RAČUNALA NOVE DOBE, 1. del

Ključne besede: matematika, algebra, grupa, obseg, seštevanje, množenje.

Elektronska verzija: <http://www.presek.si/30/1522-Juriscic.pdf>

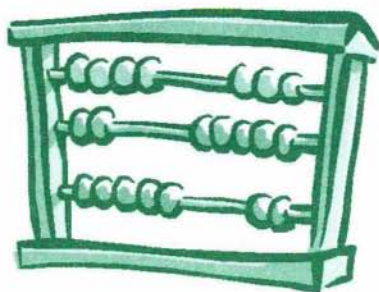
© 2003 Društvo matematikov, fizikov in astronomov Slovenije

© 2010 DMFA - založništvo

Vse pravice pridržane. Razmnoževanje ali reproduciranje celote ali posameznih delov brez poprejšnjega dovoljenja založnika ni dovoljeno.

RAČUNALA NOVE DOBE, 1. del

Ste že kdaj razmišljali, na kakšen način računajo računalniki ter ostale digitalne naprave, ki nas obkrožajo v času informacijske revolucije? V tem sestavku se bomo poskusili s pomočjo osnovnošolskega računanja približati računalom, ki jih preko številnih naprav, kot so osebni računalniki in pametne kartice, uporabljamo v vsakdanji praksi.



Vsi poznamo tabele za seštevanje in množenje (tabela 1).

+	1	2	3	4	5	6	7	8	9	10	...
1	2	3	4	5	6	7	8	9	10	11	...
2	3	4	5	6	7	8	9	10	11	12	...
3	4	5	6	7	8	9	10	11	12	13	...
4	5	6	7	8	9	10	11	12	13	14	...
5	6	7	8	9	10	11	12	13	14	15	...
6	7	8	9	10	11	12	13	14	15	16	...
7	8	9	10	11	12	13	14	15	16	17	...
8	9	10	11	12	13	14	15	16	17	18	...
9	10	11	12	13	14	15	16	17	18	19	...
10	11	12	13	14	15	16	17	18	19	20	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

(a)

*	1	2	3	4	5	6	7	8	9	10	...
1	1	2	3	4	5	6	7	8	9	10	...
2	2	4	6	8	10	12	14	16	18	20	...
3	3	6	9	12	15	18	21	24	27	30	...
4	4	8	12	16	20	24	28	32	36	40	...
5	5	10	15	20	25	30	35	40	45	50	...
6	6	12	18	24	30	36	42	48	54	60	...
7	7	14	21	28	35	42	49	56	63	70	...
8	8	16	24	32	40	48	56	64	72	80	...
9	9	18	27	36	45	54	63	72	81	90	...
10	10	20	30	40	50	60	70	80	90	100	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

(b)

Tabela 1. (a) tabela za seštevanje, (b) tabela za množenje.

Drugi tabeli pravimo *poštevanka* in se jo morajo drugošolci od nekdaj učiti na pamet ter si jo zapomniti za vse življenje. Seveda si ni potrebno zapomniti vseh 100 zmnožkov; večkratniki števil 1 in 10 so otročje lahki, množenje z 2 ni nič težje kot seštevanje, vrstni red pri množenju ni prav nič pomemben (*zakon o zamenjavi* ali *komutativnost*) (tabela 2).

1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22
23	24	25	26	27	28	29	30	31	32	33
34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55

(a)

1	6	11	16	21	26	31	36	41	46	51
2	7	12	17	22	27	32	37	42	47	52
3	8	13	18	23	28	33	38	43	48	53
4	9	14	19	24	29	34	39	44	49	54
5	10	15	20	25	30	35	40	45	50	55

(b)

Tabela 2. Ploščina pravokotnika s stranicama a in b je enaka tako ab kakor tudi ba . Enkrat štejejo kvadratke po vrsticah, drugi pa po stolpcih.

Tabela za poštevanke je simetrična glede na diagonalo, torej si je potrebno zapomniti le približno tretjino zmnožkov. Omenimo še dve bližnjici.

Večkratniki števila 9. Koliko je 9×7 ? Uporabimo metodo računanja s prsti. Ne vzamemo v roke žepnega računalca, temveč potegnemo iz žepov deset prstov. Ker gre za sedemkratnik števila devet, pripognemo sedmi prst z leve in odčitamo: šest (6) prstov na levi ter trije (3) na desni in že vemo, da je pravilni odgovor 63.

Večkratniki števila 11. Koliko je 11×13 ? Zelo enostavno! Enico in trojko razmaknemo, med njiju pa zapišemo njuno vsoto in že dobimo iskani produkt 143.

Ko končno obvladamo tabelo množenja, ni več težko zmnožiti poljubnih števil (zapisanih v desetiškem zapisu), saj množimo le posamezne številke in nato samo še seštevamo (tabela 3).

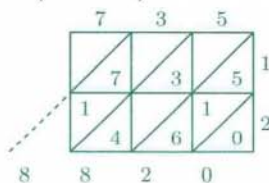


Tabela 3. France Križanič v svoji knjigi *Križem po matematiki* predstavi indijski način množenja s pomočjo pravokotne mreže, razdeljene v kvadrate. Vsaki številki prvega faktorja pripada po en stolpec, vsaki številki drugega faktorja pa ena vrsta kvadratkov. V vsak kvadratoček zapišemo produkt obeh števil, ki pripadata stolpcu in vrsti, v kateri je kvadratoček. Desetice tako dobljenega produkta zapišemo v levi zgornji kot, enice pa v spodnji desni kot. Ko so vpisani vsi produkti, je potrebno le še sešteti števila v smeri diagonal in že dobimo produkt.

Če pa bi računali v petiškem zapisu ali celo dvojiškem, bi bila matematika v drugem razredu veliko lažja (tabela 4).

*	1_5	2_5	3_5	4_5	10_5	...
1_5	1_5	2_5	3_5	4_5	10_5	...
2_5	2_5	4_5	11_5	13_5	20_5	...
3_5	3_5	11_5	14_5	22_5	30_5	...
4_5	4_5	13_5	22_5	31_5	40_5	...
10_5	10_5	20_5	30_5	40_5	100_5	...
\vdots		\vdots	\vdots	\vdots	\vdots	\ddots

(a)

*	1_2	10_2	...
1_2	1_2	10_2	...
10_2	10_2	100_2	...
\vdots	\vdots	\vdots	\ddots

(b)

+	0_2	1_2	...
0_2	0_2	1_2	...
1_2	1_2	10_2	...
\vdots	\vdots	\vdots	\ddots

(c)

Tabela 4. (a) tabela za množenje v petiškem sistemu, (b) tabela za množenje v dvojiškem sistemu, (c) tabela za seštevanje v dvojiškem sistemu.

V prvem primeru bi si bilo potrebno zapomniti le 6 zmnožkov, v drugem pa pravzaprav nobenega. Prav zato običajno računalniki računajo račune v dvojiškem sistemu. Pred njimi pa so tako računali že Indijanci. Ko so npr. želeli izračunati 15×13 , so enega izmed faktorjev zapisali kot vsoto potenc števila 2, npr. $13 = 1 + 4 + 8$, t.j. v dvojiškem sistemu 1101_2 , in nato drugega le množili z dve in seštevili (tabela 5a). Če je tudi drugo število zapisano v dvojiškem sistemu, t.j. $15 = 1 + 2 + 4 + 8 = 1111_2$, potem je množenje z dve doseženo na prav enostaven način: na koncu števila je potrebno pripisati ničlo (tabela 5b) in že dobimo $11000011_2 = 128 + 64 + 2 + 1 = 195$.

$$\begin{array}{r}
 15 \times 1 = 15 \\
 30 \times 0 = 0 \\
 60 \times 1 = 60 \\
 120 \times 1 = 120 \\
 \hline
 195
 \end{array}$$

(a)

$$\begin{array}{r}
 1111_2 \times 1 = 1111_2 \\
 11110_2 \times 0 = 0_2 \\
 111100_2 \times 1 = 111100_2 \\
 1111000_2 \times 1 = 1111000_2 \\
 \hline
 11000011_2
 \end{array}$$

(b)

Tabela 5.

Grupe in obsegi

Poleg seštevanja in množenja pa se v prvih razredih osnovne šole naučimo tudi odštevati in deliti. Seveda začnemo najprej odštevati manjša števila od večjih. Pri tem si lahko pomagamo s tabelo 1a. Če želimo izračunati $a - b$ in je $a \geq b$, se lahko vprašamo:

b plus koliko je a ?

To pomeni, da pogledamo v vrstico, ki ustreza številu b , iskano razliko pa najdemo na vrhu stolpca, ki ustreza številu a iz te vrstice. Za razliko $5 - 3$ poiščemo v tretji vrstici število 5. Najdemo ga na drugem mestu in zato vemo, da je razlika enaka 2. Šele nekoliko kasneje se naučimo, da moramo v primeru, ko želimo odšteti večje število od manjšega, števili najprej zamenjati, na koncu pa dobljeni razliki spremeniti predznak. Zaradi tega smo povečali množico naravnih števil \mathbb{N} do množice celih števil \mathbb{Z} .

Deljenje ni tako preprosto. Če želimo a deliti z b , se lahko prav tako kot prej vprašamo: " b krat koliko je a ?" Vendar ni gotovo, da bomo v vrstici, ki ustreza številu b , našli število a . Pogosto se namreč zgodi, da število a ni deljivo s številom b . Množico števil lahko sicer povečamo do množice ulomkov \mathbb{Q} , kjer lahko delimo s poljubnim od nič različnim številom, a potem nastopijo druge težave. Najdemo lahko različne ulomke, ki so si poljubno blizu, tudi tako blizu, da jih računalnik ne more več ločiti. Ker pa si želimo, da bi se računalniki čim manj motili, se vprašajmo po množicah, v katerih bi lahko brez težav tudi delili, po možnosti na enak način kot znamo odštevati. Da bi bilo to mogoče, se morajo v vsaki vrstici tabele pojaviti vsa od nič različna števila. Pravzaprav se je potrebno vprašati, na katera pravila se želimo pri računanju opreti. Naštejmo jih nekaj.

1. Običajno je prvo pravilo *zaprtost*, rezultat, ki ga dobimo po opravljeni operaciji med dvema številoma, je tudi v množici, iz katere smo izbrali števili. Množica naravnih števil je zaprta za seštevanje in množenje, saj v tabelah 1a in 1b nastopajo samo naravna števila. Ni pa množica naravnih števil zaprta za odštevanje. To lastnost ima na primer množica celih števil.

2. V množici celih števil igra pomembno vlogo število 0; pa ne samo zato, ker loči pozitivna števila od negativnih, pač pa tudi zato, ker se nobeno število s prištevanjem števila 0, ne spremeni. Tudi pri množenju najdemo nekaj podobnega. Če pomnožimo katerokoli od nič različno število z 1, dobimo zopet isto število. Takemu številu pravimo *nevtralni element* ali pa tudi *enota* za ustrezno operacijo.

3. V množici celih števil sta poljubni števili $-a$ in a povezani z enoto za seštevanje na naslednji način: $a + (-a) = 0$. Pravimo, da je $-a$ nasprotni element števila a . Celo število b je *obratni element* celega števila a , če je $ab = 1$. Od tod sledi $a = b = 1$ ali $a = b = -1$, t.j. v množici celih števil imata le števili 1 in -1 obratni element.

4. Če si izberemo poljubna števila a , b in c , potem velja $a + (b + c) = (a + b) + c$ in $a(bc) = (ab)c$. O drugi enakosti se lahko prepričamo z računanjem prostornine kvadra s stranicami a , b in c . Tem lastnostim pravimo *zakon o združevanju* za seštevanje oziroma za množenje (ali tudi *asociativnost*). Le-ta nam pove, da je vseeno, ali začnemo računati z leve ali z desne. To seveda ne drži za odštevanje ali deljenje.

Če v množici G z binarno operacijo \circ , t.j. operacijo, ki vsakemu urejenemu paru elementov iz G priredi natanko določen element, veljajo naslednja pravila:

$$(G1) \text{ za vsaka } a, b \in G \text{ je } \boxed{a \circ b \in G},$$

$$(G2) \text{ obstaja tak element } e \in G, \text{ da za vsak } g \in G \text{ velja } \boxed{e \circ g = g \circ e = g},$$

$$(G3) \text{ za vsak element } g \in G \text{ obstaja tak } f \in G, \text{ da je } \boxed{g \circ f = f \circ g = e},$$

$$(G4) \text{ za vse } a, b, c \in G \text{ velja } \boxed{(a \circ b) \circ c = a \circ (b \circ c)},$$

potem pravimo, da je par (G, \circ) **grupa**. Elementu e pravimo **enota** grupe, elementu f pa **inverz** elementa g . Množica celih števil je grupa za seštevanje, ni pa grupa za množenje, saj ni izpolnjeno pravilo (3) (le 1 in -1 imata inverzni element za množenje).

Matematiki so potrebovali več kot sto let trdega dela, da so končno (eksplicitno) zapisali zgornja pravila (*aksiome*). *Joseph Louis Lagrange* (1736–1813) je leta 1771 postavil prvi pomembnejši izrek. *Augustin Louis Cauchy* (1789–1857) je študiral grupe permutacij, medtem ko je *Niels Henrik Abel* (1802–1829) s teorijo grup pokazal, da enačba 5. stopnje ni rešljiva z radikali (t.j. rešitve ne znamo zapisati s formulami kot v primeru enačb nižjih stopenj). Pravi pionir abstraktnega pristopa pa je bil *Evariste Galois* (1811–1832), ki je leta 1823 prvi uporabil besedo "grupa". Leta 1854 je *Arthur Cayley* (1821–1895) pokazal, da je grupo moč definirati ne glede na konkretno naravo njenih elementov.

Galois je vpeljal tudi naslednji pojem. Če za neko množico \mathcal{O} z binarnima operacijama, ki ju bomo označili s $+$ in $*$ (četudi ne predstavljata nujno običajnega seštevanja in množenja), velja

(O1) par $(\mathcal{O}, +)$ je grupa z enoto 0,

(O2) par $(\mathcal{O} \setminus \{0\}, *)$ je grupa z enoto 1,

(O3) za vse $a, b, c \in \mathcal{O}$ je $a * (b + c) = a * b + a * c$ in $(b + c) * a = b * a + c * a$,

potem imenujemo trojico $(\mathcal{O}, +, *)$ **obseg**. Množica ulomkov z običajnim seštevanjem in množenjem je primer obsega. O lastnosti (O3), ki jo imenujemo *zakon o razčlenjevanju* oziroma *distributivnost*, se lahko prepričamo z računanjem površine pravokotnika s stranicama a in $b + c$.

Za konec zastavimo še nekaj nalog:

- Poišči še kakšno zanimivo pravilo za množenje (kot sta bili pravili za računanje večkratnikov števil 9 in 11). Če ne gre v desetiškem sistemu, pa poskusi v kakšnem drugem sistemu.
- Poznamo še veliko grup, ki ne izhajajo iz množice števil s seštevanjem ali pa množenjem. Poišči še kakšne množice z binarnimi operacijami in preveri, katera izmed pravil (G1) – (G4) veljajo zanje. Zanimiva množica so simetrije določenega geometrijskega objekta, npr. enakostraničnega trikotnika ali pa kocke. Kakšno binarno operacijo bi vpeljali med simetrije, da bi dobili grupo? Spet druga zanimiva množica so funkcije. Kaj pa lahko rečemo o preseku in uniji množic?
- Dokaži, da je v poljubni grupi G za vsaka $a, b \in G$ rešljiva enačba $a \circ x = b$. Poišči nekaj najmanjših grup (glede na število elementov). Kako jih lahko najlažje predstaviš?
- Poišči najmanjši obseg.

V drugem delu si bomo za cilj postavili iskanje obsega s končno mnogo elementi, v katerem bo računanje v nekem smislu še udobnejše kot v obsegih, ki jih srečamo v osnovni ali srednji šoli (racionalna števila \mathbb{Q} , realna števila \mathbb{R} ali celo kompleksna števila \mathbb{C}). Več o uporabi končnih obsegov pri nemotenemu branju zgoščenek ter prenašanju slik z oddaljenih planetov kot je Mars pa boste spoznali v članku *Napake niso za vedno*.