Računala nove dobe, 1. del

18. dec., 2002

Ste že kdaj razmišljali o aritmetiki, ki jo uporabljamo v vsakdanjem življenju? Večina ljudi jo zamenjuje kar za celotno matematiko. Na kakšen način računajo računalniki ter ostale digitalne naprave (digit je angl. beseda za število), ki nas obkrožajo v času informacijske revolucije? Nekateri se sicer skušajo prilagajati našemu načinu računanja, vse več pa je takih, ki so jim časovna in prostorska učinkovitost ter preciznost ključnega pomena. Take naprave računajo na malce drugačen način. V tem sestavku se bomo poskusili s pomočjo osnovnošolskega računanja približati računalom, ki jih preko številnih naprav, kot so osebni računalniki, diskmani in pametne kartice, uporabljamo v vsakdanji praksi.

Vsi poznamo tablici za seštevanje in množenje, glej tabelo 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) tablica za seštevanje, (b) tablica za množenje.

Na prvo tablico se privadimo kot prvošolci, ne da bi to sploh opazili, drugi pa pravimo *poštevanka* in so se jo morali drugošolci od nekdaj naučiti na pamet in si jo zapomniti za celo življenje. Seveda si ni potrebno zapomniti vseh 100 produktov iz zgornje tablice. Večkratniki števil 1 in 10 so otročje lahki. Množenje z 2 ni nič težje kot seštevanje. Pa še nekaj opazimo. Vrstni red pri množenju ni prav nič pomemben (temu se učeno pravi *zakon o zamenjavi* ali *komutativnost*), glej tabelo 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 štejemo kvadratke po vrsticah, drugič pa po stolpcih.

Zato je tablica za poštevanko simetrična glede na diagonalo. Torej si je potrebno zapomniti le približno tretjino produktov. Omenimo še dve bližnjici.

Večkratniki števila 9: *Koliko je* 9×7*? Uporabimo metodo računanja s prsti! Predse ne postavimo žepnega računalnika, temveč iz žepov potegnemo deset prstov. Ker gre za sedemkratnik števila devet, pripognemo sedmi prst in odčitamo: šest (6) prstov na levi ter trije (3) na desni in že vemo, da je pravilen 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 tablico množenja, ni več težko zmnožiti poljubni števili (zapisani v desetiškem zapisu), saj množimo le posamezne števke in nato samo še seštevamo, glej tabelo 3.

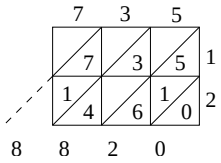

Tabela 3: F. Križanič v svoji knjigi *Križem po matematiki* predstavi indijski način množenja s pomočjo pravokotne mreže, razdeljene v kvadrate. Vsaki števki prvega faktorja pripada po en stolpec, vsaki števki drugega faktorja pa ena vrsta kvadratkov. V vsak kvadratek zapišemo produkt obeh števil, ki pripadata stolpcu in vrsti, v kateri je kvadratek. 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 smo dobili produkt.

Če pa bi računali v petiškem zapisu ali celo dvojiškem, bi bila matematika v drugem razredu veliko lažja, glej tabelo 4.

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

(a)

$*$	1_2	10_2	$\dots$
1_2	1_2	10_2	$\dots$
10_2	10_2	100_2	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$

(b)

$+$	0_2	1_2	$\dots$
0_2	0_2	1_2	$\dots$
1_2	1_2	10_2	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$

(c)

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

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

$$\begin{aligned} 15 &\times 1 = 15 \\ 30 &\times 0 = 0 \\ 60 &\times 1 = 60 \\ 120 &\times 1 = 120 \\ \hline & \quad 195 \end{aligned}$$

(a)

$$\begin{aligned} 1111_2 &\times 1 = 1111_2 \\ 11110_2 &\times 0 = 0_2 \\ 111100_2 &\times 1 = 111100_2 \\ 1111000_2 &\times 1 = 1111000_2 \\ \hline & \quad 1100011_2 \end{aligned}$$

(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 $a \geq b$, potem se lahko vprašamo

$$b \text{ plus koliko je } a.$$

Se pravi, da pogledamo v vrstico, ki ustreza številu b, iskano razliko pa najdemo na vrhu stolpca, ki ustreza številu a iz te vrstice. Na primer 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 $\mathbb{Z}$.

Z deljenjem pa nismo tako srečne roke. 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 se da deliti s poljubnim od nič različnim številom, a potem nastanejo drugi problemi. Lahko namreč najdemo 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 problemov tudi delili, po možnosti na enak način kot znamo odštevati. Da bi bilo to mogoče, se morajo v vsaki vrstici tablice 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*, tj. da je rezultat, ki ga dobimo po opravljeni operaciji med dvema številoma, zopet v množici, iz katere smo izbrali števili. Množica naravnih števil je zaprta za seštevanje in množenje, saj v tablicah 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, kateremu prištejemo 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 $a = b = 1$, tj. 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 neki množici G z binarno operacijo $\circ$, tj. operacijo, ki vsakemu urejenemu paru elementov iz G priredi natanko določen element, veljajo naslednja pravila:

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

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

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

(G4) za vse $a, b, c \in G$ 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 enica ima inverzni element za množenje).

Morda bo kdo pomislil, da je prišla definicija grupe iz glave enega samega matematika, pa temu sploh ni tako. Matematiki so potrebovali več kot 100 let trdega dela na teoriji grup, 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 (tj. 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". Proces poudarka na strukturi se je nadaljeval vse do leta 1854, ko je *Arthur Cayley* (1821-1895) pokazal, da se da grupa 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 običajno seštevanje in množenje), velja

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

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

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

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:

(1) Najdi 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 katerem drugem sistemu.

(2) 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. Ena 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 na množicah?

(3) 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?

(4) 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 zgoščenk ter prenašanju slik z oddaljenih planetov kot je Mars pa boste spoznali v članku NAPAKE NISO ZA VEDNO.

Aleksandar Jurišić