MATEMAGIČAR

Petar Mladinić, Zagreb

GAUSSOV RAČUN OSTATAKA

Jedan od najvećih matemagičara **K. F. Gauss** osmislio je jednostavan račun nazvan *modularna aritmetika* ili *aritmetika skupova ostataka.*

* * *

Račun ostataka vidimo u svakodnevnoj uporabi. On se službeno ne uči u temeljnom matematičkom kurikulu pa ga većina ljudi niti ne koristi jer ga ne poznaje. Ljudi se muče na najobičnijim problemima svakodnevnih izračuna koje bi vrlo lako proveli kad bi znali Gaussovu ideju računanja s ostatcima koji se dobiju pri dijeljenju brojeva. U ovom ćemo tekstu naznačiti tu Gaussovu ideju.

* * *

a) Uvod

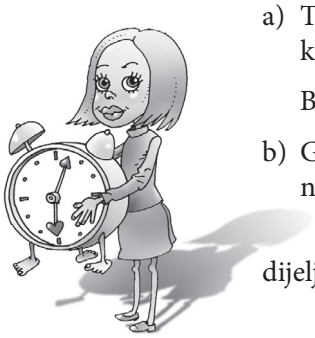
Evo nekoliko mogućih svakodnevnih primjera.

Primjer 1. Danas je četvrtak 31. prosinca 2020. godine.

a) Koji će dan u tjednu biti za 23 dana, a koji za 370 dana?

b) Koji će mjesec u godini biti za 5 mjeseci, a koji za 23 mjeseca?

Rješenje. Razmotrit ćemo ove brojeve i ostatak koji se dobije nakon dijeljenja.



a) Tjedan ima 7 dana. Broj 23 podijelimo brojem 7 i dobijemo ostatak 2. Dakle, dva dana nakon četvrtka je subota.

Broj 370 nakon dijeljenja brojem 7 daje ostatak 6, pa je odgovor srijeda.

b) Godina dana ima 12 mjeseci. Prosinac je 12. mjesec. Dakle, 12 + 5 = 17 daje nakon dijeljenja brojem 12 ostatak 5, pa je odgovor: bit će svibanj.

U slučaju od 23 mjeseca nakon prosinca dobiva se 12 + 23 = 35. Nakon dijeljenja brojem 12 dobivamo ostatak 11, pa je odgovor: studeni.

Primjer 2. U ovom trenutku pogledam na klasičnu ručnu uru koja ima označene satove od 1 do 12 (odnosno 0). Ura pokazuje 10 sati. Imam sastanak za 7 sati. Gdje će se tada nalaziti mala kazaljka?

Odgovor. Kazaljka će se nalaziti na 5 sati.

Napomena. Slično se računa ako imamo uru koja pokazuje vrijeme od 1 do 24 sata.

b) Aritmetika 12-satne ure

Vizualizirajmo ovu aritmetiku ure.

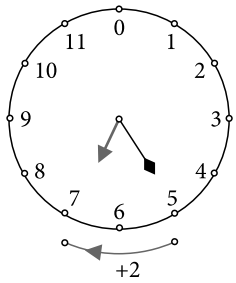
Primjer 3. Nađimo sljedeće zbrojeve u 12-satnoj aritmetici:

a) 5 + 2,

b) 8 + 9,

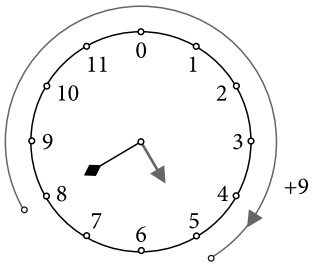
Rješenje. Na uri kazaljkom naznačimo prvi pribrojnik, a zatim zarotirajmo kazaljku za vrijednost drugog pribrojnika u smjeru kretanja kazaljke na uri. Taj smjer naziva se *pozitivnim*.

a) Imamo 5 + 2 = 7.



Slika 1.

b) U ovom slučaju imamo 8 + 9 = 5.



Slika 2.

Vidimo da 12-satna ura ima samo sljedeće vrijednosti:

$$\{0,1,2,3,4,5,6,7,8,9,10,11\}.$$

Evo tablice zbrajanja 12-satne ure.

1	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

Vrijedi primjerice

$$5 + 9 = 9 + 5 = 2,$$

a ostala računanja može se provjeriti u tablici.

Dakle, ova je operacija **komutativna**, tj. vrijedi $a + b = b + a$. Vrijedi primjerice

$$(4 + 5) + 9 = 9 + 9 = 6$$

kao i

$$4 + (5 + 9) = 4 + 2 = 6.$$

Dakle, ova je operacija **asocijativna**, tj. vrijedi $(a + b) + c = a + (b + c)$. Broj 0 je **neutralan** za zbrajanje jer je $a + 0 = 0 + a = a$.

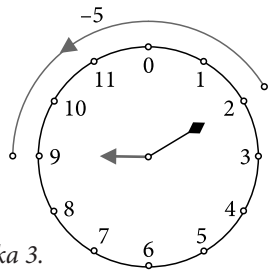
U slučaju oduzimanja brojeva rotiramo kazaljku u suprotnom smjeru od uobičajenog rotiranja kazaljke. Taj smjer naziva se *negativnim*.

Primjer 4. Izračunajmo:

a) 2 – 5,

b) 7 – 14.

Rješenje. Na uri naznačimo kazaljkom prvi pribrojnik, a zatim zarotirajmo kazaljku za vrijednost drugog pribrojnika u suprotnome smjeru od uobičajenog kretanja kazaljke na uri.



Slika 3.

a) Imamo 2 – 5 = 9.

Također vrijedi 2 – 5 = 9 jer je 9 + 5 = 2.

b) Imamo 7 – 14 = 5 jer je 5 + 14 = 19 = 7.

Broj –5 je suprotan broju 5, tj. vrijedi da je $-a$ suprotan od a. Zato i rotiramo kazaljku ure u suprotnom/negativnom smjeru.

Vrijedi

$$a + (-a) = (-a) + a = 0.$$

Evo tablice suprotnih brojeva 12-satne ure.

a	0	1	2	3	4	5	6	7	8	9	10	11
$-a$	0	11	10	9	8	7	6	5	4	3	2	1

Napomena. Vrijedi $a - b = a + (-b)$.

Razmotrimo množenje brojeva.

Primjer 5. Izračunajmo umnožak:

a) $5 \cdot 4$, b) $6 \cdot 9$,

c) $6 \cdot 0$, d) $0 \cdot 8$.

Rješenje. Umnožak brojeva je zapis zbrajanja.

a) $5 \cdot 4 = 4 + 4 + 4 + 4 + 4 = 8$,

b) $6 \cdot 9 = 9 + 9 + 9 + 9 + 9 + 9 = 6$,

c) $6 \cdot 0 = 0 + 0 + 0 + 0 + 0 + 0 = 0$,

d) $0 \cdot 8 = 0$.

Primjer 6. Napišimo tablicu množenja za 4-satnu aritmetiku.

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	1	2
3	0	3	2	1

Rješenje. Skup brojeva za 4-satnu aritmetiku je {0, 1, 2, 3}.

Evo tablice množenja u 4-satnoj aritmetici (desno).

Napomena. Jednakovrijedne su sljedeće tvrdnje koje nam pomažu u računanju:

a) $a - b = d$ i $b + d = a$,
b) $a : b = q$ i $b \cdot q = a$.

Zadatci. Za vježbu riješite sljedeće zadatke.

1. Napišite tablice zbrajanja i množenja u 5-satnoj aritmetici.
2. Izračunajte u 12-satnoj aritmetici:
   a) 8 – 3, b) 4 – 9, c) 3 · 4.
3. Izračunajte u 5-satnoj aritmetici:
   a) 1 : 3, b) 3 : 1, c) 2 : 3.

Uputa. U tablici u zadatku 1. nađite koja dva broja pomnožena daju treći broj.

b) Gaussov račun ostataka

Gauss je vidio da se u svim ovim računima s konačnim brojem elemenata, nazvanim **konačnim matematičkim sustavima**, radi o ostatcima nakon dijeljenja prirodnih brojeva.

Radi se o tzv. **modularnim sustavima**.

Primjer 7. Izračunajmo ostatke dijeljenja broja a brojem b:

a) $a = 14, b = 12$, b) $a = 26, b = 12$,
c) $a = 35, b = 5$, d) $a = 26, b = 7$.

Rješenje.

a) Dijeljenjem broja 14 brojem 12 dobivamo količnik 1 i ostatak 2, tj. $14 = 1 \cdot 12 + 2$.

Gauss bi ovaj račun zapisao kao

$$14 \equiv 2 (\mathrm{mod}\, 12) \text{ jer je } 14 = 1 \cdot 12 + 2.$$

b) $26 \equiv 2 (\mathrm{mod}\, 12)$ jer je $26 = 2 \cdot 12 + 2$.
c) $35 \equiv 0 (\mathrm{mod}\, 5)$ jer je $35 = 7 \cdot 5 + 0$.
d) $26 \equiv 5 (\mathrm{mod}\, 7)$ jer je $26 = 3 \cdot 7 + 5$.

Cijeli brojevi a i b su **kongruentni po modulu m**, gdje je m prirodan broj veći od 1 i nazvan **modul** ako i samo ako je razlika $a - b$ djeljiva brojem m, tj. ako je

$$a - b = k \cdot m, k \in Z.$$

To zapisujemo ovako:

$$a \equiv b (\mathrm{mod}\, m).$$

Zadatak 4. Je li istinita tvrdnja da je $27 \equiv 9 (\mathrm{mod}\, 6)$?

Zadatak 5. Izračunaj:

a) $(9 + 4) (\mathrm{mod}\, 3)$, b) $(27 - 5) (\mathrm{mod}\, 6)$,
c) $(50 + 34) (\mathrm{mod}\, 7)$, d) $(8 \cdot 9) (\mathrm{mod}\, 10)$,
e) $(12 \cdot 10) (\mathrm{mod}\, 5)$.

Uputa i rezultati: Zbrojite, oduzmite ili pomnožite brojeve u zagradi.

a) 2, b) 4, c) 0, d) 2, e) 0.

Modularni sustav (mod m) ima konačan skup brojeva

$$\{0, 1, 2, \ldots, m\text{-}1\}$$

Primjer 8. Riješimo sljedeće jednadžbe.

a) $x \equiv 5 (\mathrm{mod}\, 7)$,

b) $(3 + x) \equiv 5 (\mathrm{mod}\, 7)$,

c) $5 \cdot x \equiv 4 (\mathrm{mod}\, 9)$,

d) $6 \cdot x \equiv 3 (\mathrm{mod}\, 8)$.

Rješenje.

a) Lako je uočiti da vrijedi $5 \equiv 5 (\mathrm{mod}\, 7)$, pa je jedno rješenje $x = 5$. Odavde slijedi da je $x \in \{5, 12, 19...\}$.

b) Uočimo da je $(3 + 2) \equiv 5 (\mathrm{mod}\, 7)$, pa je jedno rješenje $x = 2$. Odavde slijedi da je $x \in \{2, 9, 16, 23...\}$.

c) Nađimo među brojevima iz skupa $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ onaj za koji je tvrdnja istinita. Dobivamo da vrijedi $5 \cdot 8 \equiv 4 (\mathrm{mod}\, 9)$, tj. $x = 8$ je jedno rješenje. Odavde se dobiva skup rješenja $x \in \{8, 17, 26...\}$.

d) Iz $6 \cdot x \equiv 3 (\mathrm{mod}\, 8)$ slijedi da je $6x - 3 = 8k, k \in Z$. Broj $6x - 3 = 3(2x - 1)$ je neparan broj, a broj $8k$ paran, pa zaključujemo da ova jednadžba nema rješenja.

Riješimo jedan konkretan primjer.

Primjer 9. Danica želi složiti svoju kolekciju CD-ova u skupine jednake veličine, ali nakon što ih je isprobala grupirati po 4, 5 i 6 diskova, otkrila je da joj uvijek ostaje 1 disk.

Pod pretpostavkom da Danica ima više od jednog CD-a, koliki je najmanji broj CD-a u njezinoj kolekciji?

Rješenje. Zapišimo podatke pomoću modula. Imamo

$$x \equiv 1 (\mathrm{mod}\ 4),$$
$$x \equiv 1 (\mathrm{mod}\ 5),$$
$$x \equiv 1 (\mathrm{mod}\ 6).$$

Skupovi pozitivnih brojeva x za svaku skupinu su

$$A = \{1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69...\},$$
$$B = \{1,6,11,16,21,26,31,36,41,46,51,56,61,66,71,76...\},$$
$$C = \{1,7,13,19,25,31,37,43,49,55,61...\}.$$

Dakle, u presjeku ovih skupova najmanji zajednički broj različit od 1 je broj 61.

Zadatci.

6. Koja je od sljedećih tvrdnji istinita, a koja je lažna:
   a) $5 \equiv 19 (\mathrm{mod}\ 3)$, b) $35 \equiv 8 (\mathrm{mod}\ 9)$,
   c) $5445 \equiv 0 (\mathrm{mod}\ 3)$, d) $7021 \equiv 4202 (\mathrm{mod}\ 6)$?

7. Koliko je:
   a) $(12 + 7) (\mathrm{mod}\ 4)$, b) $(62 + 95) (\mathrm{mod}\ 9)$,
   c) $(35 - 22) (\mathrm{mod}\ 5)$, d) $(82 - 45) (\mathrm{mod}\ 3)$,
   e) $(5 \cdot 8) (\mathrm{mod}\ 3)$, f) $(32 \cdot 21) (\mathrm{mod}\ 8)$,
   g) $(4 \cdot (13 + 6)) (\mathrm{mod}\ 11)$, h) $((10 + 7) \cdot (5 + 3)) (\mathrm{mod}\ 10)$?

8. Nađite pozitivna rješenja sljedećih jednadžbi:
   a) $x \equiv 3 (\mathrm{mod}\ 7)$, b) $(2 + x) \equiv 7 (\mathrm{mod}\ 3)$,
   c) $6x \equiv 2 (\mathrm{mod}\ 2)$, d) $(5x - 3) \equiv 7 (\mathrm{mod}\ 4)$.

9. Ako mi je ove godine rođendan bio u četvrtak, kojeg će mi dana biti sljedeće godine?

10. Koji će dan u tjednu biti 31. lipnja 2021. godine ako je 1. lipnja 2021. godine utorak?

11. Napišite tablice zbrajanja i množenja za dane u tjednu ako je NE = 0, PO = 1, UT = 2, SR = 3, ČE = 4, PE = 5 i SU = 6. (U nazivima dana u tjednu prepoznaju se ovi brojevi!) Napišite tablicu u kojoj se vidi koji je dan suprotan kojem danu.