Izbrana poglavja iz matematike

Vincenc Petruna

12. november 2007

Kazalo

1 Boolova algebra

V četverici $(\mathcal{B}, +, \cdot, -)$, ki jo sestavlja množica $(\mathcal{B})$ z dvočlenima operacijama $+$ in $\cdot$ ter enočlena operacija negacija $-$ naj veljajo naslednji računski zakoni:

1. $(\mathcal{B}, +)$ je *Abelova polgrupa*, saj veljajo za operacijo $+$ naslednji zakoni:
   - $(a + b) + c = a + (b + c)$ - asociativni zakon,
   - $a + 0 = a$ - enota za disjunkcijo,
   - $a + b = b + a$ - komutativni zakon.
2. $(\mathcal{B}, \cdot)$ je *Abelova polgrupa*, saj veljajo za konjunkcijo naslednji zakoni:
   - $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ -asociativni zakon,
   - $a \wedge 0 = a$ - enota za konjunkcijo,
   - $a \wedge b = b \wedge a$ - komutativni zakon.
3. Disjunkcijo in konjunkcijo vežeta distributivna zakona:
   - $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$,
   - a$\vee b \wedge c = (a \vee b) \wedge (a \vee c)$.
4. Negacija je definirana z naslednjima enačbama

$$a \vee \overline{a} = 1,$$

$$a \wedge \overline{a} = 0.$$

O veljavnosti zgornjih zakonov se lahko lahko prepričamo npr. s primerjavo pravilnostnih tabel levih in desnih strani (naredi to vsaj za nekaj primerov).

Struktura $(\mathcal{B}, \vee, \wedge,)$, za katero veljajo zgornje lastnosti, se po Georgu Booleu imenuje *Boolova algebra*. Izjave so glede na omenjene operacije torej Boolova algebra. V srednji šoli spoznamo še dve Boolovi algebri: algebro množic in algebro dogodkov pri verjetnostnem računu.

Opazimo, da so zgoraj navedeni zakoni simetrični na zamenjavo $\wedge$ in $\vee$ ter 0 in 1. To pomeni, za iz veljavnega izreka o izjavah z omenjeno zamenjavo spet dobimo veljaven izrek.

1.1 Izreki

Vstavimo v prvi distributivni zakon $c = \overline{b}$. Dobimo

$$a \wedge (b \vee \overline{b}) = (a \wedge b) \vee (a \wedge \overline{b}).$$

Leva stran je enaka (pojasni, zakaj)

$$a \wedge (b \vee \overline{b}) = a \wedge 1 = a,$$

tako da je

$$(a \wedge b) \vee (a \wedge \overline{b}) = a.$$

1.1.1 Idempotentnost

V zgornji zvezi postavimo še $b = a$. Leva stran postane (spet pojasni vsak korak)

$$(a \wedge a) \vee (a \wedge \overline{a}) = (a \wedge a) \vee (1) = a \wedge a,$$

tako da dobimo zvezo

$$a \wedge a = a.$$

Pravimo, da je vsak element a *idempotenten* za konjunkcijo. Velja tudi

$$a \vee a = a,$$

kar pomeni, da je vsak element idempotenten tudi za disjunkcijo (to zvezo na podoben način dokaži sam, izhajaj iz 2. distributivnega zakona.)

V Boolovi algebri so torej vsi elementi idempotentni tako glede na disjunkcijo kot na konjunkcijo.

Vprašanji: Ali v množici celih števil obstaja kak idempotenten element glede na seštevanje? Kaj pa glede na množenje?

1.1.2 Absorbcijski zakon

Koliko je $a \vee 1$ in koliko $a \wedge 0$?

Prvo zvezo izpeljimo iz zakonov takole

$$a \vee 1 = a \vee (a \vee \overline{a}) = (a \vee a) \vee \overline{a} = a \vee \overline{a} = 1.$$

Torej

$$a \vee 1 = 1.$$

To zvezo imenujemo *absorbcijski zakon.* Utemelji posamezne korake. podobno izpelji tudi

$$a \wedge 0 = 0.$$

1.1.3 De Morganova izreka

Glasita se takole

$$\overline{a \vee b} = \overline{a} \wedge \overline{b},$$
$$\overline{a \wedge b} = \overline{a} \vee \overline{b}.$$

Dokaz: Dokazali bomo samo prvega. Po definiciji negacije moramo torej dokazati dvoje:

1. $$a \vee b \vee \overline{a} \wedge \overline{b} = 1,$$
2. $$a \vee b \wedge \overline{a} \wedge \overline{b} = 0.$$

Pa poglejmo, če je res:

1. $$a \vee b \vee \overline{a} \wedge \overline{b} = (a \vee \overline{a}) \wedge (a \vee \overline{b}) \vee b = a \vee \overline{b} \vee b = a \vee 1 = 1,$$
2. $$a \vee b \wedge \overline{a} \wedge \overline{b} = 0 \vee 0 = 0.$$

Dokaz drugega De Morganovega izreka je prepuščen bralcu.

Naloga: Pokaži na dva načina, da je

$$\overline{(a \vee b) \wedge (a \vee \overline{b}) \wedge (\overline{a} \vee b) \wedge (\overline{a} \vee \overline{b})} = 1$$

Preveri De Morganova izreka tudi s pravilnostno tabelo.

1.2 Implikacija in identiteta

Definicija: Implikacija $a \Rightarrow b$, je nepravilna le, če je a pravilna in hkrati b nepravilna. V vseh ostalih primerih je to pravilna izjava.

Definicija: Ekvivalenca ali identiteta $a \Longleftrightarrow b$ je pravilna tedaj, ko sta izjavi istega tipa, sicer je nepravilna. Tvorimo jo z besedami a natanko tedaj, kot b ⁄ Dve izjavi sta ekvivalentni ali identični, če imata isti prostor pravilnosti.

Pravilnostni tabeli za obe izjavi sta:

a	b	$a \Rightarrow b$	$a \Leftrightarrow b$
p	p	p	p
p	n	n	n
n	p	p	n
n	n	p	p

Medtem ko so konjunkcija, disjunkcija in negacija osnovne izjave, lahko implikacijo in identiteto zapišemo z osnovnimi izjavami.

a $\Rightarrow b$ a$\vee\overline{b}$

$\overline{\overline{a} \wedge b}$

$\overline{b} \Rightarrow \overline{a}$

2 Izjave in Boolova algebra

V množici izjav ($\mathcal{B}$) z operacijami disjunkcija, konjunkcija in negacija veljajo naslednji računski zakoni:

1. $(\mathcal{B}, \vee)$ je *Abelova polgrupa*, saj veljajo za disjunkcijo naslednji zakoni:
   - $(a \vee b) \vee c = a \vee (b \vee c)$ - asociativni zakon,
   - $a \vee 1 = a$ - enota za disjunkcijo,
   - $a \vee b = b \vee a$ - komutativni zakon.
2. $(\mathcal{B}, \wedge)$ je *Abelova polgrupa*, saj veljajo za konjunkcijo naslednji zakoni:
   - $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ -asociativni zakon,
   - $a \wedge 0 = a$ - enota za konjunkcijo,
   - $a \wedge b = b \wedge a$ - komutativni zakon.
3. Disjunkcijo in konjunkcijo vežeta distributivna zakona:
   - $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$,
   - a$\vee b \wedge c = (a \vee b) \wedge (a \vee c)$.
4. Negacija je definirana z naslednjima enačbama
$$a \vee \overline{a} = 1,$$
$$a \wedge \overline{a} = 0.$$

O veljavnosti zgornjih zakonov se lahko lahko prepričamo npr. s primerjavo pravilnostnih tabel levih in desnih strani (naredi to vsaj za nekaj primerov).

Struktura $(\mathcal{B}, \vee, \wedge,)$, za katero veljajo zgornje lastnosti, se po Georgu Booleu imenuje *Boolova algebra*. Izjave so glede na omenjene operacije torej Boolova algebra. V srednji šoli spoznamo še dve Boolovi algebri: algebro množic in algebro dogodkov pri verjetnostnem računu.

Opazimo, da so zgoraj navedeni zakoni simetrični na zamenjavo $\wedge$ in $\vee$ ter 0 in 1. To pomeni, za iz veljavnega izreka o izjavah z omenjeno zamenjavo spet dobimo veljaven izrek.

2.1 Izreki

Vstavimo v prvi distributivni zakon $c = \overline{b}$. Dobimo

$$a \wedge (b \vee \overline{b}) = (a \wedge b) \vee (a \wedge \overline{b}).$$

Leva stran je enaka (pojasni, zakaj)

$$a \wedge (b \vee \overline{b}) = a \wedge 1 = a,$$

tako da je

$$(a \wedge b) \vee (a \wedge \overline{b}) = a.$$

2.1.1 Idempotentnost

V zgornji zvezi postavimo še $b = a$. Leva stran postane (spet pojasni vsak korak)

$$(a \wedge a) \vee (a \wedge \overline{a}) = (a \wedge a) \vee (1) = a \wedge a,$$

tako da dobimo zvezo

$$a \wedge a = a.$$

Pravimo, da je vsak element a *idempotenten* za konjunkcijo. Velja tudi

$$a \vee a = a,$$

kar pomeni, da je vsak element idempotenten tudi za disjunkcijo (to zvezo na podoben način dokaži sam, izhajaj iz 2. distributivnega zakona.)

V Boolovi algebri so torej vsi elementi idempotentni tako glede na disjunkcijo kot na konjunkcijo.

Vprašanji: Ali v množici celih števil obstaja kak idempotenten element glede na seštevanje? Kaj pa glede na množenje?

2.1.2 Absorbcijski zakon

Koliko je $a \vee 1$ in koliko $a \wedge 0$?

Prvo zvezo izpeljimo iz zakonov takole

$$a \vee 1 = a \vee (a \vee \overline{a}) = (a \vee a) \vee \overline{a} = a \vee \overline{a} = 1.$$

Torej

$$a \vee 1 = 1.$$

To zvezo imenujemo *absorbcijski zakon.* Utemelji posamezne korake. podobno izpelji tudi

$$a \wedge 0 = 0.$$

2.1.3 De Morganova izreka

Glasita se takole

$$\overline{a \vee b} = \overline{a} \wedge \overline{b},$$
$$\overline{a \wedge b} = \overline{a} \vee \overline{b}.$$

Dokaz: Dokazali bomo samo prvega. Po definiciji negacije moramo torej dokazati dvoje:

1. $$a \vee b \vee \overline{a} \wedge \overline{b} = 1,$$
2. $$a \vee b \wedge \overline{a} \wedge \overline{b} = 0.$$

Pa poglejmo, če je res:

1. $$a \vee b \vee \overline{a} \wedge \overline{b} = (a \vee \overline{a}) \wedge (a \vee \overline{b}) \vee b = a \vee \overline{b} \vee b = a \vee 1 = 1,$$
2. $$a \vee b \wedge \overline{a} \wedge \overline{b} = 0 \vee 0 = 0.$$

Dokaz drugega De Morganovega izreka je prepuščen bralcu.

Naloga: Pokaži na dva načina, da je

$$\overline{(a \vee b) \wedge (a \vee \overline{b}) \wedge (\overline{a} \vee b) \wedge (\overline{a} \vee \overline{b})} = 1$$

Preveri De Morganova izreka tudi s pravilnostno tabelo.

2.2 Implikacija in identiteta

Definicija: Implikacija $a \Rightarrow b$, je nepravilna le, če je a pravilna in hkrati b nepravilna. V vseh ostalih primerih je to pravilna izjava.

Definicija: Ekvivalenca ali identiteta $a \Longleftrightarrow b$ je pravilna tedaj, ko sta izjavi istega tipa, sicer je nepravilna. Tvorimo jo z besedami a natanko tedaj, kot b ; Dve izjavi sta ekvivalentni ali identični, če imata isti prostor pravilnosti.

Pravilnostni tabeli za obe izjavi sta:

a	b	$a \Rightarrow b$	$a \Leftrightarrow b$
p	p	p	p
p	n	n	n
n	p	p	n
n	n	p	p

Medtem ko so konjunkcija, disjunkcija in negacija osnovne izjave, lahko implikacijo in identiteto zapišemo z osnovnimi izjavami.

a $\Rightarrow b$ a$\vee\overline{b}$

$\overline{\overline{a} \wedge b}$

$\overline{b} \Rightarrow \overline{a}$

2.3 Tavtologija

3 Popolna (matematična) indukcija

Indukcija je način sklepanja iz enote na množino, ki se uporablja v znanosti. Običajna indukcija kot način dokazovanja v matematiki ni uporabna, ker lahko pridemo do napačnih sklepov. Poglejmo si to na primeru Fermatovih števil:

Primer: Pierre de Fermat je leta 1640 domneval, da so vsa števila oblike

$$F(n) = 2^{2^n} + 1, n \in \mathcal{N} \cup \{\mathcal{O}\}$$

praštevila, saj so taka $F(0)$, $F(1)$, $F(2)$, $F(3)$ in $F(4)$. A leta 1732 je Leonard Euler pokazal, da je $F(5)$ deljivo z 641 (preveri s kalkulatorjem).

Zato se v matematiki se kot metoda dokazovanja uporablja strožja oblika indukcije - tako imenovana **popolna ali matematična indukcija.** Vpeljal jo je leta 1838 Augustus De Morgan.

Izrek: Imejmo števno neskončno množico A in lastnost L, ki je smiselna za elemente te množice. Naj velja naslednje:

1. Naj za prvi element a_1 množice A lastnost L velja, torej $n = 1 \rightarrow L(a_1)$,
2. Naj velja implikacija: če velja lastnost L za element z indeksom $n-1$, velja lastnost tudi za element z indeksom n, torej $L(a_{n-1}) \rightarrow L(a_n)$,

Potem velja lastnost L za vse elemente množice A.
Dokaz je preprost. Najprej uporabimo 1). L velja torej za $n = 1$. Naprej ves čas uporabljamo 2. Ker velja L za $n = 1$, velja tudi za $n = 2$. Ker velja za $n = 2$, velja tudi za $n = 3$, itd.
Najtežji del dokazovanja z indukcijo je uporaba predpostavke implikacije: predpostavimo, da L velja za $n - 1$, uporabiti moramo to predpostavko v izpeljavi, da L velja tudi za n.
Sicer pa je matematična indukcija zelo močno orodje za dokazovanje. Poglejmo primere:

1. **Dokaži, da je vsota prvih n naravnih števil** $1 + 2 + 3 + ... + n$ **enaka**
$$S_n = \frac{n(n+1)}{2}.$$

   Rešitev: Za $n = 1$ dobimo $S_1 = 1$, obrazec očito velja. Predpostavimo sedaj, da obrazec velja tudi za $n - 1$, torej
$$S_{n-1} = 1 + 2 + 3 + ... + n - 1 = \frac{(n-1)n}{2}.$$
   Pokažimo, da ob tej predpostavki velja obrazec tudi za n. Potem, ko uporabimo predpostavko, je vsota n členov enaka
$$S_n = 1+2+3+...+(n-1)+n = S_{n-1}+n = \frac{(n-1)n}{2}+n = \frac{n^2-n+2n}{2} = \\ = \frac{n(n+1)}{2},$$
   kar je bilo treba dokazati.
2.
3.
4.
5.

4 Pitagorejska trojica

Števila $a, b, c \, \epsilon \mathcal{N}$ so *Pitagorejska trojica*, če zadoščajo enačbi
$$a^2 + b^2 = c^2.$$

Najmanjša in najbolj znana Pitagorejska trojica je $(3, 4, 5)$. Pitagorejska trojica je *primitivna*, če sta a in b tuji si števili. Obravnavamo samo pritimitivne pitagorejske trojice, saj ostale lahko dobimo z množenjem števil z istim faktorjem.

Velja naslednje: eno od števil a, b je vedno liho in drugo vedno sodo, c pa je vedno liho število.
Pitagora in Babilonci so nam zapustili naslednjo formulo za določanje Pitagorejskih trojic

$$(2m, m^2 - 1, m, m^2 + 1),$$

pri čemer je $m > 1 \epsilon \mathcal{N}$. Metoda nam da nekatere primitivne in nekatere neprimitivne Pitagorejske trojice. Stari Grki (Diofant 3.stol. našega štetja) pa so iznašli obrazec

$$(v^2 - u^2, 2uv, u^2 + v^2),$$

kjer sta $u, v, u < v$ tuji si števili nasprotne parnosti. Formula nam da samo primitivne Pitagorejske trojice.

V Pitagorejski trojici je produkt obeh katet vedno deljiv z 12 in produkt vseh treh števil vedno deljiv s 60. Ni znano, ali obstajata dve različni Pitagorejski trojici, ki imata enak produkt. Nekaj primitivnih pitagorejskih trojic je zbranih v naslednji tabeli:

begintable[h]

a	3	5	8	7	20		12	9	28	11	16		33	48	13	36	39
b	4	12	15	24	21		35	40	45	60	60		56	55	84	77	80
c	5	13	17	25	29		37	41	53	61	65		65	73	85	85	89

a	65	20	60	15	44		88	17	24	51	85		119	52
b	72	99	91	112	117		105	144	143	140	132		120	165
c	97	101	109	113	125		137	145	145	149	157		169	173

5 Pitagorejska četverica

Množica naravnih števil $\{a, b, c, d\}$ je *Pitagorejska četverica,* če zadošča enačbi

$$a^2 + b^2 + c^2 = d^2.$$

Če sta a, b lihi števili, potem ne obstajata ustrezna c, d, sicer pa taki števili vedno obstajata.

Nekatere Pitagorejske četverice generirajo naslednji obrazci:

$$a = 2mp \quad (1)$$
$$b = 2np \quad (2)$$
$$c = p^2 - (m^2 + n^2) \quad (3)$$
$$d = p^2 + (m^2 + n^2) \quad (4)$$

6 Kriteriji deljivosti

Zanimajo nas pravila za deljivost s praštevili, ki so tuja osnovi 10. Število a je v desetiškem sestavu zapisano kot

$$a = \overline{a_n ... a_1 a_o} = 10k_o + a_o,$$

pri tem pa je k_o število desetic, ali, zapisano z desetiško številko

$$k_o = \overline{a_n ... a_2 a_1}.$$

6.1 Pravilo za deljivost s 7

Izrek: Število a deljivo s 7, če je deljivo s 7 število $k_o + 5a_o$.
Dokaz: Namesto

$$5a = 50k_o + 5a_o$$

pišemo

$$5a = 49k_o + (k_o + 5a_o)$$

Prvi člen na desni, je deljiv s 7, zato je deljivost števila $5a$ odvisna od tega, ali je s 7 deljiv oklepaj. Če je, je s 7 deljivo število $5a$. Ker sta 5 in 7 tuji si števili, mora biti s 7 deljiv a.

Preverjanje deljivosti spravimo v naslednjo tabelo:

6.2 Pravilo za deljivost z 13

Izrek: Število a je deljivo s 13, če je s 13 deljivo število $k_o + 4a_o$.
Dokaz: Namesto

$$4a = 40k_o + 4a_o$$

pišemo

$$4a = 39k_o + (k_o + 4a_o)$$

Prvi člen na desni, je deljiv s 13, zato je deljivost števila $4a$ odvisna od tega, ali je s 13 deljiv oklepaj. Če je, je s 13 deljivo število $4a$. Ker sta 4 in 13 tuji si števili, mora biti s 13 deljiv a.

Naloge in vaje: 1. Dokaži izreke:

(a) Število a je deljivo s 17, če je s 17 deljivo število $k_o - 5a_o$.
(b) Število a je deljivo s 19, če je s 19 deljivo število $k_o + 2a_o$.
(c) Število a je deljivo s 23, če je s 23 deljivo število $k_o + 7a_o$.
(d) Število a je deljivo s 29, če je s 29 deljivo število $k_o - 3a_o$.
(e) Število a je deljivo s 49, če je s 49 deljivo število $k_o + 5a_o$.

2. Med navedenimi števili določi tista, ki so deljiva s 13: a)3151512

Primer: Naj bo $a = 2322,\ b = 654$. Izvedemo algoritem

$$\begin{array}{rcrcrcr} 2322 & = & 3 & \text{x} & 654 & + & 360 \\ 654 & = & 1 & \text{x} & 360 & + & 294 \\ 360 & = & 1 & \text{x} & 294 & + & 66 \\ 294 & = & 4 & \text{x} & 66 & + & 30 \\ 66 & = & 2 & \text{x} & 30 & + & 6 \\ 30 & = & 5 & \text{x} & 6 & + & 0 \end{array}$$

Zadnji od 0 različen ostanek je 6, kar je največji skupni delitelj teh števil.

Izrek: Za vsak par celih števil $a,\ b$ obstajata taki celi števili $x,\ y$, da je $ax + by = D(a, b)$.

Dokaz: Najprej označimo z $E(a, b)$ število vrstic v Evklidovem algoritmu. Tako lahko vidimo iz prejšnjega primera, da je $E(654, 2322) = 6$, medtem ko je $E(3, 6) = 1$. Dokaz po potekal z indukcijo:

1. $E(a, b) = 1$ pomeni, da $a|b$, torej je $b = ka$ in je $D(a, b) = a$. Iz zapisa
$$ax + by = a$$
razberemo, da je $x = k + 1$ in $y = -1$. Za $E(a, b) = 1$ torej izrek velja.
2. Naj bo $E(a, b) = n$ in predpostavimo sedaj, da izrek velja za $E(u, r) = n - 1$. To pomeni, da je $a = bu + r$. po predpostavki obstajata taki števili x in y, da velja enačba
$$bx + ry = D(b, r) = D(a, b)$$
Izrazimo r kot $r = a - bu$. Dobimo
$$b(x - uy) + ay = D(a, b)$$
Iskani števili smo torej našli. Poglej tudi Pigeonhole principle=Dirichletov princip

8 Razširjeni Evklidov algoritem

Pokazali smo, da za vsak par celih števil $a,\ b$ obstajata taki celi števili $x,\ y$, da je $ax + by = D(a, b)$. A običajni Evklidov algoritem ne daje števil $x,\ y$, ki ta rešitvi zgornje Diofantske enačbe. Zato uporabljamo *razširjen Evklidov algoritem.*

Po prejšnjem izreku je

$$D(a, b) = ax + by$$

linearna kombinacija števil a in b. POrebej sta tudi števili a in b trivialni linerni kombinaciji teh števil, namreč

$$a = a \cdot 1 + b \cdot 0$$

in

$$b = a \cdot 0 + b \cdot 1.$$

Prepišimo obe vrstici, nato pa uporabimo osnovni izrek o deljenju $a = kb + o$.

Torej

$$a = a \cdot 1 + b \cdot 0$$

$$b = a \cdot 0 + b \cdot 1$$

$$o = a \cdot 1 + (-k) \cdot b.$$

Tako nadaljujemo, doker ne pridemo do največjega skupnega delitelja obeh števil. Na levi strani teče običajni Evklidov algoritem, na desni strani pa so trenutni koeficienti A in B te količnik k. Če vseskupaj spravimo v tabelo, vsakič množimo vsa števila levo od trenutnega k s k nato pa jih odštejemo od istoležnih števil v zgornji vrstici in zapišemo. Več naj pove primer.

Primer : Rešimo enačbo

$$2322x + 654y = 6.$$

E.a	A	B	k
2322	1	0	
654	0	1	3
360	1	-3	1
294	-1	4	1
66	2	-7	4
30	-9	32	2
6	20	-71	5
0			

Tabela kaže potek razširjenega Evklidovega algoritma za števili $a = 2322$ in $b = 654$. Iskana x in y pridelamo v zadnji vrstici, in sicer $x = 20$ in $y = -71$.

9 Kongruence

Kongruence je so nenavadno uporabno orodje, ki ga je leta 1801 odkril K.F. Gauss.

Definicija: Celi števili sta kongruentni po modulu m, če dasta pri deljenju z m isti ostanek.

Z drugimi besedami: Števili a in b sta kongruentni, če je $m|(a-b)$. Po modulu m kongruentni števili označimo kot

$$a = b(m).$$

Tako je $10 = 4(4)$, $5 = 0(5)$, $16 = 6(10)$, $12 \neq 2(6)$.

Izrek: Kongruenca je ekvivalenčna relacija, saj velja:

1. povratnost ali refleksivnost, $a = a(m)$,
2. vzajemnost ali simetričnost $a = b(m) \Rightarrow b = a(m)$,
3. prehodnost ali tranzitivnost $a = b(m) \& b = c(m) \Rightarrow a = c(m)$.

Dokaz : 1. $a - a = 0 = km \Rightarrow a = a(m)$.

2. $a = b(m) \Rightarrow a - b = km \Rightarrow b - a = (-k)m \Rightarrow b = a(m)$.
3. $(a = b(m) \wedge b = c(m)) \Rightarrow (a - b = k_1 m \wedge b - c = k_2 m) \Rightarrow a - c = a - b + b - c = (k_1 + k_2)m \Rightarrow a = c(m)$.

Posledica: Kongruenca po modulu m razdeli množico celih števil $\mathcal{Z}$ na m podmnožic kongruenčne razrede. V istem kongruenčnem razredu so tista števila, ki dajo pri deljenju z m enak ostanek.

Primer: Naj bo denimo $m = 5$. množica $\mathcal{Z}$ razpade na naslednje kongruenčne razrede:

$$[0] = \{..., -5, 0, 5, 10, 15, ...\},$$
$$[1] = \{..., -4, 1, 6, 11, 16, ...\},$$
$$[2] = \{..., -3, 2, 7, 12, 17, ...\},$$
$$[3] = \{..., -2, 3, 8, 13, 18, ...\},$$
$$[4] = \{..., -1, 4, 9, 14, 19, ...\}.$$

9.1 Lastnosti kongruenc

Med računanjem s kongruencami in enačbami je precej podobnosti in nekaj razlik. Oglejmo si jih.

Izrek 1: Kongruenca se ne spremeni, če na obeh straneh prištejemo ali odštejemo število.

$$a = c(m) \Rightarrow a + c = b + c(m).$$

Dokaz: $a + c = b + c(m) \Rightarrow a + c - (b + c) = km \Rightarrow a - b = km \Rightarrow a = c(m)$.

Izrek 2: Kongruenca se ne spremeni, če obe strani pomnožimo z istim številom.

$$a = c(m) \Rightarrow a \cdot c = b \cdot c(m).$$

Dokaz: $a = c(m) \Rightarrow a - b = km \Rightarrow ac - bc = (ck)m \Rightarrow a \cdot c = b \cdot c(m)$.

Izrek 3: Naj bosta a in m tuji si števili. Potem obstaja tako celo število $k \in \mathcal{Z}$, da velja

$$ak = 1(m).$$

Dokaz: Po izreku ua dve tuji števili a in m vedno obstajata taki celi števili e in k, da velja

$$ak + em = 1.$$

Od tod pa sledi $ak = 1(m)$.

9.2 Modularna aritmetika

S kongruenčnimi razredi lahko računamo. Seštevanje definiramo med konguenčnima razredoma tako, da je vsota dveh kongruenčnih razredov razred, v katerem so vsote predstavnikov razredov. Podobno definiramo tudi množenje. Torej

$$[a] + [b] = [a + b]$$

in

$$[a] \cdot [b] = [a + b]\,.$$

Primer: Če imamo aritmetiko po modulu $m = 5$ velja $[2] + [3] = [0]$ in $[2] \cdot [3] = [1]\,$, v aritmetiki po modulu $m = 11$ pa velja $[8] + [9] = [6]$ in $[8] \cdot [9] = [6]\,$.

Izkaže se, da so množice kongruenčnih razredov s tako definiranima operacijama izredno bogata struktura. Struktura $(\mathcal{Z}_{\Updownarrow}, +, \cdot)$ je *kolobar*, struktura $(\mathcal{Z}_{\surd}, +, \cdot)$, kjer je p praštevilo, pa celo *obseg*.

Primeri: Tabela za seštevanje po modulu 9:

	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

Tabela za množenje po modulu 9:

	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

V tej tabeli opazimo elemente, ki sami niso 0, a njihov produkt je 0. Taki elementi se imenujejo *delitelji niča.*

Pa še tabeli za računanje z praštevilskim modulom $p = 11$.

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

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

Iz teh tablic lahko razberemo naslednje lastnosti:

1. Pri seštevanju dobimo naslednje vrstice z iz prve rotacijo vsebine vrstice.
2. Tablice za seštevanje in množenje so simetrične glede na glavno diagonalo (posledica katerega zakona je to?),
3. Pri množenju so števila v zadnji vrstici v nasprotnem vrstnem redu kot v prvi.
4.

9.2.1 Mali Fermatov izrek

Izrek: Za vsako praštevilo p in vsako celo število a velja

$$a^p = a(p).$$

Različica: Če je p poljubno praštevilo in a tuj p ($D(a,p) = 1$), je

$$a^p - 1 = 1(p).$$

Dokaz: Mali Fermatov izrek lahko uporabljamo kot praštevilski test za p. Na intervalu $[1, p)$ izbiramo a-je in preverjamo, ali velja mali Fermatov izrek. Pri velikih p-jih ne moremo preizkusiti vseh a-jev, zato jih izbiramo naključno. Če izrek vellja za veliko vrednosti števila a,

9.2.2 Wilsonov izrek

10 Diofantske enačbe

Diofantske enačbe so enačbe oblike $P(x, y) = 0$. Pri tem je $P(x, y) = 0$ polinom spremenjivk x in y s celimi koeficienti. Iščemo celoštevilske rešitve take enačbe. Delimo jih na več vrst: linearna Diofantska enačba, Pellova enačba, itd.

10.1 Linearna diofantska enačba

Je enačba oblike

$$ax + by = c$$

pri čemer so a, b in c cela števila. Imenuje se po Diofantu, ki jih je reševal v 3. stol. našega štetja. Iščemo cele rešitve.

Izrek: Diofantska enačba ax + by = c, za cele a, b in c je rešljiva v celih številih samo tedaj, če je največja skupna mera števil a in b delitelj števila c.

Izrek: Če poznamo eno od rešitev (x_1, y_1) enačbe $ax + by = c$, dobimo ostale rešitve kot

$$x = x_1 + bk,\ y = y_1 - ak,\ k \in \mathcal{Z}.$$

Dokaz: Naj velja

$$ax_1 + by_1 = c$$

in

$$ax + by = c.$$

Odštejemo, pa dobimo

$$a(x - x_1) + b(y - y_1) = 0.$$

Ker sta a in b tuji si števili, je $x - x_1 = bk$ in $y - y_1 = -ak$.

Na primeru

$$93x + 42y = 3$$

so prikazane tri metode za reševanje linearne diofantske enačbe:

Evklidov algoritem: Okrajšamo, dobimo $21x + 14y = 1$. Delimo večji koeficient z manjšim.

$$\begin{array}{rcl} 21 & = & 1{\cdot}14 \quad + \quad 7 \\ 14 & = & 2{\cdot}7 \end{array}$$

Splezamo še nazaj

$$\begin{array}{rcl} 9 & = & 93\text{-}2{\cdot}42 \\ 6 & = & 42\text{-}4{\cdot}9 = 42 - 4 \cdot (93 - 2 \cdot 9) = (-4) \cdot 93 + 9 \cdot 42 \\ 3 & = & 9\text{-}1{\cdot}6 = (93 - 2 \cdot 42) - ((-4) \cdot 93 + 9 \cdot 42) = 5 \cdot 93 + (-11) \cdot 42 \end{array}$$

Ena rešitev enačbe je torej $x_1 = 5$, $y_1 = -11$, splošna rešitev pa

$$x = 5 + 42k, \quad y = -11 - 93k, \quad k \in \mathcal{Z}.$$

Razširjeni Evklidov algoritem: Sestavimo tabelo tako, da zapišemo prvi dve vrstici in določimo prvi k, nato pa s tem k-jem množimo vsa števila levo od njega in dobljene produkte odštejemo od števil eno vrstico višje. Ponavljamo postopek.

E.a	A	B	k
93	1	0	
42	0	1	2
9	1	-2	4
6	-4	9	1
3	**5**	**-11**	2
0			

Spet smo dobili rešitev enačbe $x_1 = 5$, $y_1 = -11$, in splošno rešitev

$$x = 5 + 42k, \quad y = -11 - 93k, \quad k \in \mathcal{Z}.$$

S kongruencami : Enačbo

$$93x + 42y = 3$$

najprej okrajšamo, da dobimo

$$31x + 14y = 1,$$

nato pa jo zapišemo po modulu 14, torej

$$3x = 1(14)$$

. pomnožimo kongruenco s 5, da dobimo

$$x = 5(14)$$

. Od tod sledi $x = 5 + 14k$. Vstavimo to v enačbo, pa dobimo

$$155 + 70k + 14y = 1,$$

od tod pa $y = -11 - 5k$.

11 Verižni ulomki

Posplošeni verižni ulomek je izraz oblike

$$x = a_o + \frac{b_1}{a_1 + \frac{b_2}{a_3 + \frac{b_3}{a_4 + \ldots}}},$$

pri čemer so a_i in b_i naravna števila. Če so vsi $b_i = 1$, je verižni ulomek *enostaven*, torej

$$x = a_o + \frac{1}{a_1 + \frac{1}{a_3 + \frac{1}{a_4 + \ldots}}}.$$

Primer:

$$\frac{13}{10} = 1 + \frac{3}{10} =$$
$$= 1 + \frac{1}{3 + \frac{1}{3}} = [1; 3, 3].$$

11.1 Predstavitev realnih števil z verižnimi ulomki

Ima nekaj prednosti pred zapisom v desetiškem sistemu:

1. Predstavitev števila z verižnim ulomkom je končna natanko tedaj, ko je število racionalno. **Primer:**
$$\frac{22}{7} = 3 + \frac{1}{7} = [3 : 7].$$
22
2. Predstavitve običajnih racionalnih števil z verižnimi ulomki so kratke.
3. Predstavitev poljubnega racionalnega števila z verižnim ulomkom je ena sama, če na koncu predstavitve ni 1. Za vsako racionalno število, izraženo kot verižni ulomek $[N; a, ..., z]$ pri $z > 1$, obstaja zapis z 1 na koncu $[N; a, ..., z - 1, 1]$.

$$x = 1 + \frac{1}{1 + \frac{1}{2+x-1}}.$$

Rešitev te enačbe je $\sqrt{3}$.

7. Okrajšanje predstavitve števila x z verižnim ulomkom vodi do racionalnega približka za x, ki je v določenem smislu najboljši racionalni približek.

11.2 Neskončni verižni ulomki

Vsak neskončni verižni ulomek je iracionalno število. Za verižni ulomek so prvi štirje približki (oštevilčeni od 0 do 3):
Z drugimi besedami in vsako iracionalno število lahko zapišemo na natančno en način kot neskončni verižni ulomek.
Neskončni verižni ulomki iracionalnih števil pridejo prav, saj njihovi prvi členi nudijo odlične racionalne približke števila. Tem približkom rečemo tudi konvergenti verižnega ulomka. Sodi približki so manjši od števila, lihi pa večji.
Za verižni ulomek $[a_o; a_1, a_2, ...]$ so prvi štirje približki (oštevilčeni od 0 do 3):

$$\frac{a_o}{1}, \quad \frac{a_o a_1 + 1}{a_1}, \quad \frac{a_2(a_o a_1 + 1) + a_1}{a_2 a_1 + 1}$$

ali splošno

$$\frac{h_n}{k_n} = \frac{a_n h_{n-1} + h_{n-2}}{a_n k_{n-1} + k_{n-2}}$$

Števce in imenovalce približkov lahko podamo z rekurzivnimi formulami:

$$h_{-2} = 0, \quad (5)$$
$$k_{-2} = 1 \quad (6)$$
$$h_{-1} = 1 \quad (7)$$
$$k_{-1} = 0 \quad (8)$$
$$h_n = a_n h_{n-1} + h_{n-2} \quad (9)$$
$$k_n = a_n k_{n-1} + k_{n-2} \quad (10)$$

11.3 Izreki

Izrek 1: Za vsak pozitivni $x \epsilon \mathcal{R}$ velja

$$[a_0, a_1, a_2, ..., a_{n-1}, x] = \frac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}}.$$

Izrek 2: Približki $[a_0; a_1, a_2, ...]$ so dani z

$$[a_o; a_1, a_2, ..., a_n] = \frac{h_n}{k_n}.$$

Izrek 3: Za približek $\frac{h_n}{k_n}$ velja $k_n h_{n-1} - h_n k_{n-1} = (-1)^n$.

Izrek 3: Razlika med sosednjima zaporednima približkoma verižnega ulomka je enotski ulomek.

$$|\frac{h_n}{k_n} - \frac{h_{n-1}}{k_{n-1}}| = \frac{1}{k_n k_{n-1}}.$$

11.4 Primeri

Pokaži, da je

1. $0,84375 = [0; 1, 5, 2, 2]$,,
2. $\sqrt{2} = [1; \overline{2}]$
3. $\sqrt{3} = [1; \overline{1, 2}]$
4. $\sqrt{5} = [2; \overline{4}]$
5. $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$
6. $\sqrt{8} = [2, \overline{1, 4}]$
7. Število zlatega reza $\Phi = \frac{1+\sqrt{5}}{2} = [1, \overline{1}]$
8. $[2; 3, 1] = [2; 4]$,
9. $\sqrt{18} = [4; \overline{4, 8}]$
10. Ludolfovo število $\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, ...]$. Določi prvih 5 približkov števila π.
11. Eulerjevo število (osnova naravnih logaritmov) $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 1$
12.

11.5 Uporaba verižnih ulomkov

1. Računanje približkov realnih števil.
2. Dokazovanje iracionalnosti števil. S pomočjo verižnih ulomkov so dokazali iracionalnost Riemanove funkcije.
3. Algoritem praštevilskega razcepa SQFOF (SqFoF, Square Form factorisation)

12 Neenakosti

12.1 Trivialna neenakost

Tako se imenuje kvadratna neenačba

$$x^2 \geq 0,$$

pri čemer je $x \epsilon \mathcal{R}$ poljubno realno število. Je posledica dejstva, da je kvadrat realnega števila vedno nenegativen. Enačaj velja le v primeru, ko je $x = 0$. Trivialno neenakost velikokrat uporabljamo pri dokazovanju neenakosti.

12.2 Sredine

Za poljubni realni števili $a, b > 0$ lahko definiramo:

1. **Kvadratna sredina** - koren iz aritmetične sredine kvadratov

$$KS = \sqrt{\frac{a^2 + b^2}{2}},$$

2. **Aritmetična sredina** $AS = \frac{a+b}{2}$,
3. **Geometrična sredina** $GS = \sqrt{ab}$,
4. **Harmonična sredina** $HS = \frac{2ab}{a+b}$.

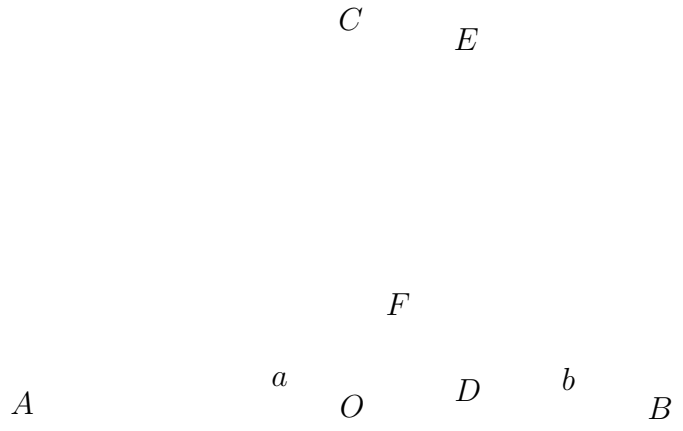
Izrek: Med sredinami veljajo naslednje neenakosti:

$$\min(a, b) \leq HS \leq GS \leq AS \leq KS \leq \max(a, b).$$

Dokazi: Po vrsti dokažemo vseh 5 sosednjih neenakosti takole:

1. Naj bo $\min(a,b) = a$. Potem je
$$\min(a,b) = a = \frac{2a^2}{a+a} = \frac{2}{\frac{1}{a}+\frac{1}{a}} \leq \frac{2}{\frac{1}{a}+\frac{1}{b}} = \frac{2ab}{a+b} = HS.$$
Ko smo namreč v zgornjem izrazu nadomestili a z b, smo imenovalec izraza zmanjšali, sam izraz pa povečali, od tod neenačaj. Ponovi dokaz, če je $\min(a,b) = b$.
2. Izhajamo iz trivialne neenakosti $(a-b)^2 \geq 0$. Od tod sledi
$$2ab \leq a^2 + b^2$$
in tudi
$$4ab \leq a^2 + 2ab + b^2.$$
Najprej delimo z desno stranjo (ki je gotovo pozitivna), nato pa neenačbo še pomnožimo z ab. Dobimo
$$\frac{4a^2b^2}{(a+b)^2} \leq ab.$$
Obe strani neenačbe še korenimo
$$HS = \frac{2ab}{a+b} \leq \sqrt{ab} = GS,$$
kar smo želeli dokazati.
3. Spet izhajamo iz trivialne neenakosti $0 \leq (a-b)^2$. Na obeh straneh neenačbe prištejemo $4ab$, nato pa obe strani korenimo in delimo z 2. Dobimo rezultat
$$GS = \sqrt{ab} \leq \frac{a+b}{2} = AS.$$
4. Še enkrat izhajamo iz trivialne neenakosti $0 \leq (a-b)^2$. Na obeh straneh neenačbe prištejemo $(a+b)^2$, nato pa obe strani delimo z 8, da dobimo
$$\frac{(a+b)^2}{4} \leq \frac{a^2+b^2}{2.}$$
Na obeh straneh še korenimo,pa imamo željeni rezultat
$$AS = \frac{a+b}{2} \leq \sqrt{\frac{a^2+b^2}{2}} = KS.$$
5. Naj bo $\max(a,b) = a$. Potem je
$$KS = \sqrt{\frac{a^2+b^2}{2}} \leq \sqrt{\frac{a^2+a^2}{2}} = a = \max(a,b),$$
, kar je bilo treba dokazati. Kje se dokaz spremeni,če je $\max(a,b) = b$, pa naj ugotovi bralec.

Kdaj velja v zgornji neenakosti enačaj?



Slika 1: Predstavitev sredin v pravokotnem trikotniku. Ugotovi, katera daljica ustreza posameznim sredinam, pa tudi, zakaj je tako.

12.3 Bernoullijeva neenakost

Po švicarskem matematiku Danielu Bernoulliju se imenuje naslednja neenakost

$$(1+a)^n \geq 1+na.$$

Neenakost velja za vsak $a > 0$ in vsak $n \epsilon \mathcal{N} \cup \{\prime\}$. Dokažemo jo tako, da v obliki binomskega izreka

$$(1+a)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$$

opustimo člene, v katerih je x na potenco 2 in več. Nekaj primerov:

- $n = 1, \quad 1 + a = 1 + a,$
- $n = 2, \quad (1+a)^2 > 1 + 2a,$
- $n = 3, \quad (1+a)^3 > 1 + 3a,$

12.4 Trikotniška neenakost

Za poljubna kompleksna števila $a, b, c \, \epsilon \mathcal{C}$ velja naslednja neenačba

$$|a+b| < |a| + |b|.$$

Ker so realna števila $\mathcal{R} \subseteq \mathcal{C}$,velja relacija tudi za realna števila. Ponazorimo jo lahko s stranicami trikotnika in vidimo, da neenakost izraža dejstvo, da je stranica trikotnika vedeno manjša od vsote drugih dveh stranic.

12.5 Cauchyjeva neenakost

Za poljubna vektorja $\vec{a}$ in $\vec{b}$ velja neenakost

$$\vec{a} \cdot \vec{b} \leq ab,$$

pri čemer sta a in b velikosti vektorjev.
Če sta vektorja zapisana v ortonormimrani bazi kot $\vec{a} = (a_1, a_2, a_3)$ in $\vec{b} = (b_1, b_2, b_3)$, potem lahko Cauchyjevo neenakost zapišemo tudi v obliki

$$a_1b_1 + a_2b_2 + a_3b_3 \leq \sqrt{(a_1^2 + a_2^2 + a_3^2)(b_1^2 + b_2^2 + b_3^2)}.$$

Ta neeenakost je posledica definicije skalarnega produkta vektorjev, torej enačbe

$$\vec{a} \cdot \vec{b} = ab \cos phi.$$

Neenakost velja, ker je $|\cos \phi| \leq 1$.

$$\vec{a} \cdot \vec{b} = ab \cos \alpha,$$

Pri čemer je α kot med obema vektorjema. Nenenakost sledi iz dejstva, da je v zgornjem izrazu $0 \leq \cos \alpha \leq 1$.

a	19	39	8	7	20		12	9	28	11	16		33	48	13	36	39
b	180	80	15	24	21		35	40	45	60	60		56	55	84	77	80
c	181	13	17	25	29		37	41	53	61	65		65	73	85	85	89

$$
\begin{array}{r}
1043 \\
15 \\
\hline
119 \\
45 \\
\hline
56 \\
30 \\
\hline
35
\end{array}
$$