Razdoblja u razvitku pojedinca
Razvoj teorije brojeva
O nastanku računara

N. Ikodinović

ikodinovic@matf.bg.ac.rs

November 28, 2018

Pregled predavanja

1. Istorijske epohe i obrazovni ciklusi
2. Razvoj teorije brojeva
3. O nastanku računara

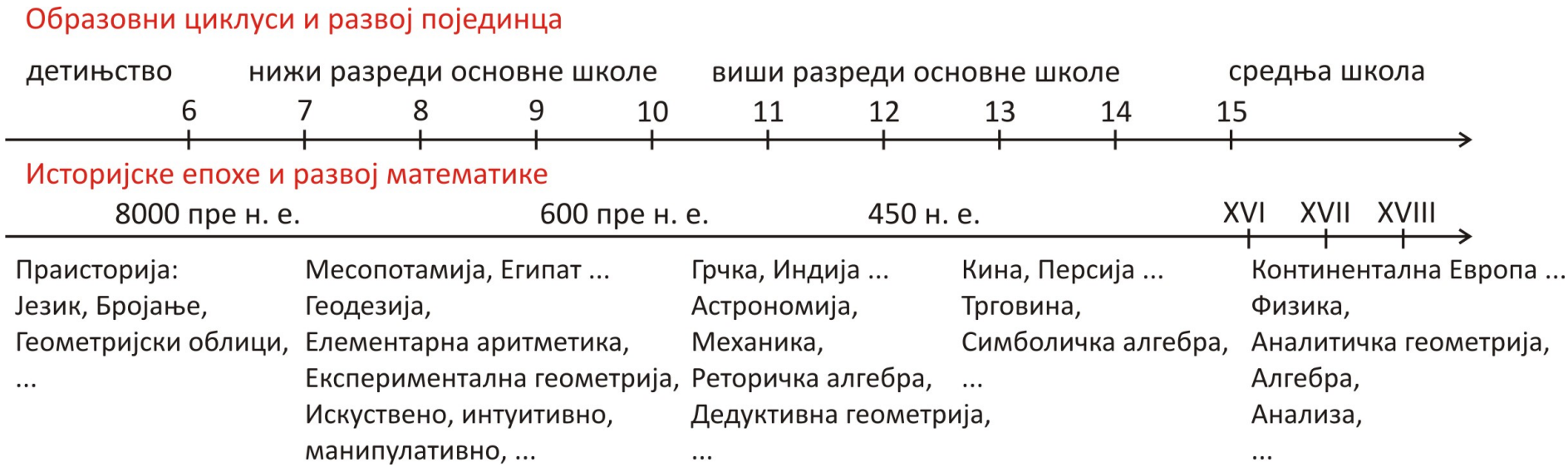
Pregled predavanja

Historia magistra vitae est

> *Zoolozi tvrde da embrionalni razvoj životinje sumira za vrlo kratko vreme istoriju njenih predaka iz raznih geoloških epoha. Čini se da isto važi i za razvoj uma. Zadatak predavača je da provuče kroz dečiji um ono što je prolazio kroz umove predaka, ubrzanim koracima, ali bez izostavljanja bilo kog koraka. U ovom smislu, istorija nauke treba da bude naš vodič.*

H. Poincaré, *Logika i intuicija u matematici i nastavi matematike*, L'Enseignement Mathématique, 1899

Historia magistra vitae est



Branford Benchara, *A study of mathematical education*, Oxford University Press, 1924 (1908)

Pregled predavanja

(Dedekind-)Peanova aritmetika

$0 \in \mathbb{N} \xrightarrow{'} \mathbb{N}$

(P1) Za svako $n \in \mathbb{N}$, $n' \neq 0$ (0 nije sledbenik nijednog broja).

(P2) Za sve $m, n \in \mathbb{N}$, iz $m' = n'$ sledi $m = n$ (sledbenik je 1-1 funkcija).

(P3) Ako je $S \subseteq \mathbb{N}$ i važi:

(BI) $0 \in S$,

(IK) ako $x \in S$, onda $x' \in S$,

onda je $S = \mathbb{N}$.

($\mathcal{P}$3) Ako je $\mathcal{S}$ neko svojstvo (prirodnih brojeva) i važi:

(BI) 0 ima svojstvo $\mathcal{S}$, $[\mathcal{S}(0)]$

(IK) ako x ima svojstvo $\mathcal{S}$, onda x' ima svojstvo $\mathcal{S}$; $[\forall x(\mathcal{S}(x) \Rightarrow \mathcal{S}(x'))]$

onda svaki prirodan broj ima svojstvo $\mathcal{S}$. $[\forall x \mathcal{S}(x)]$

Princip rekurzije

TEOREMA. [**Princip rekurzije**] Neka je X bilo koji skup, $a \in X$ i $h : X \to X$. Tada postoji jedinstvena funkcija $f : \mathbb{N} \to X$ takva da je

$$(\text{Rec}) \left| \begin{array}{l} f(0) = a, \\ f(n') = h(f(n)),\ n \in \mathbb{N}. \end{array} \right.$$

Osnovne operacije i relacije

$$\left| \begin{array}{l} m + 0 = m \\ m + n' = (m + n)' \end{array} \right. \qquad \left| \begin{array}{l} m \cdot 0 = m \\ m \cdot n' = (m \cdot n) + m \end{array} \right.$$

$$m \leqslant n \overset{\text{def}}{\Leftrightarrow} (\exists k \in \mathbb{N})(m + k = n)$$

$$m \mid n \overset{\text{def}}{\Leftrightarrow} (\exists k \in \mathbb{N})(m \cdot k = n)$$

PPI vs. PNE

Teorema.

[**Princip potpune indukcije** (PPI)] Neka je $S \subseteq \mathbb{N}$. Ako važi

$$(\forall n \in \mathbb{N})((\forall k < n)\, k \in S \Rightarrow n \in S),$$

onda je $S = \mathbb{N}$.

Teorema.

[**Princip najmanjeg elementa** (PNE)] Svaki neprazan podskup od $\mathbb{N}$ ima najmanji element, tj. $\mathbb{N}$ je dobro uredjen.

PPI vs. PNE

$S \subseteq \mathbb{N},\ S^{\complement} = \mathbb{N} \setminus S$

$$\boxed{(\forall n \in \mathbb{N})((\forall k < n)\, k \in S \Rightarrow n \in S) \Rightarrow (\forall n \in \mathbb{N})\, n \in S}$$

$$(\forall n \in \mathbb{N})((\forall k < n)\, k \in S^{\complement} \Rightarrow n \in S^{\complement}) \Rightarrow (\forall n \in \mathbb{N})\, n \in S^{\complement}$$

$$(\forall n \in \mathbb{N})((\forall k < n)\, \neg k \in S \Rightarrow n \in \neg S) \Rightarrow (\forall n \in \mathbb{N})\, \neg n \in S$$

$$[(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)]$$

$$\neg(\forall n \in \mathbb{N})\, \neg n \in S \Rightarrow \neg(\forall n \in \mathbb{N})((\forall k < n)\, \neg k \in S \Rightarrow \neg n \in S)$$

$$[\neg(\forall n \in \mathbb{N}) \cdots \Leftrightarrow (\exists n \in \mathbb{N}) \neg \cdots ; \quad \neg(p \Rightarrow q) \Leftrightarrow (p \wedge \neg p); \quad \neg\neg p \Leftrightarrow p]$$

$$\boxed{(\exists n \in \mathbb{N})\, n \in S \Rightarrow (\exists n \in \mathbb{N})((\forall k < n)\, \neg k \in S \wedge n \in S)}$$

Nekoliko zadataka

Fermaov beskonačni spust

Jedino rešenje jednačine $x^2 + y^2 + z^2 = 2xyz$ u skupu $\mathbb{N}$ jeste $x = y = z = 0$. Dokazati.

Paskalov trougao

Dokazati jednakost $\binom{n}{k} : \binom{n}{k+1} = \frac{k+1}{n-k}$

UPUTSTVO. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

Elementarna teorija brojeva

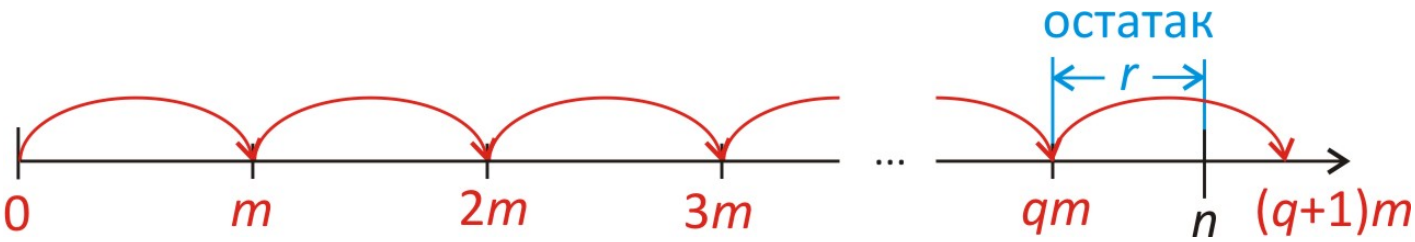
Teorema o ostatku

Za sve n i $m > 0$ postoje jedinstveni (količnik) q i (ostatak) r takvi da je $n = qm + r$, $0 \leqslant r < m$.

$$\left[\frac{n}{m}\right] \stackrel{\text{def}}{=} \text{količnik pri deljenju } n \text{ sa } m \quad (m > 0)$$

$$n \,\mathbf{mod}\, m \stackrel{\text{def}}{=} \text{ostatak pri deljenju } n \text{ sa } m \quad (m > 0)$$

Dokaz...



Brojevne baze

Teorema o brojevnoj bazi

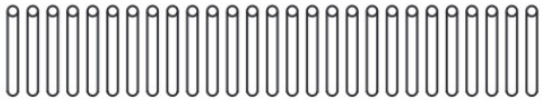
Neka je $b > 1$. Za svako $a > 0$ postoje jedinstveni prirodni brojevi q, k i r takvi da je

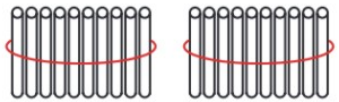
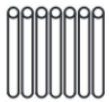
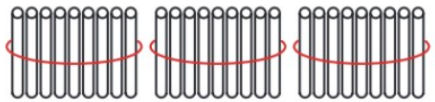
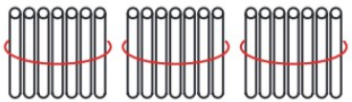
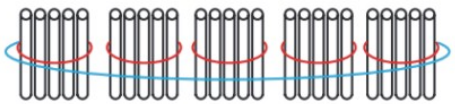
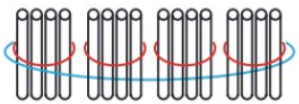
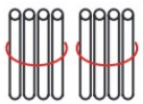
$$a = qb^k + r, 1 \leqslant q < b, 0 \leqslant r < b^k.$$

$$\begin{aligned}
n &= q_0 b + r_0, 0 \leqslant r_0 < b, \\
q_0 &= q_1 b + r_1, 1 \leqslant r_1 < b, (q_1 < q_0) \\
&\qquad n = (q_1 b + r_1)b + r_0 = q_1 b^2 + r_1 b + r_0 \\
q_1 &= q_2 b + r_2, 1 \leqslant r_2 < b, (q_2 < q_1) \\
&\qquad n = (q_2 b + r_2)b^2 + r_1 b + r_0 = q_2 b^3 + r_2 b^2 + r_1 b + r_0 \\
&\vdots \\
q_{k-1} &= 0b + r_k, 1 \leqslant r_k < b, (0 < q_{k-1}) \\
&\qquad n = r_k b^k + \cdots + r_2 b^2 + r_1 b + r_0
\end{aligned}$$

Reprezentacija broja n u bazi b jeste zapis $[r_k \cdots r_1 r_0]_b$.

Brojevne baze

Број: 

База b	b^2	b^1	b^0	Запис броја у датом систему
$b=10$				27
$b=9$				30
$b=7$				36
$b=5$				102
$b=4$				123

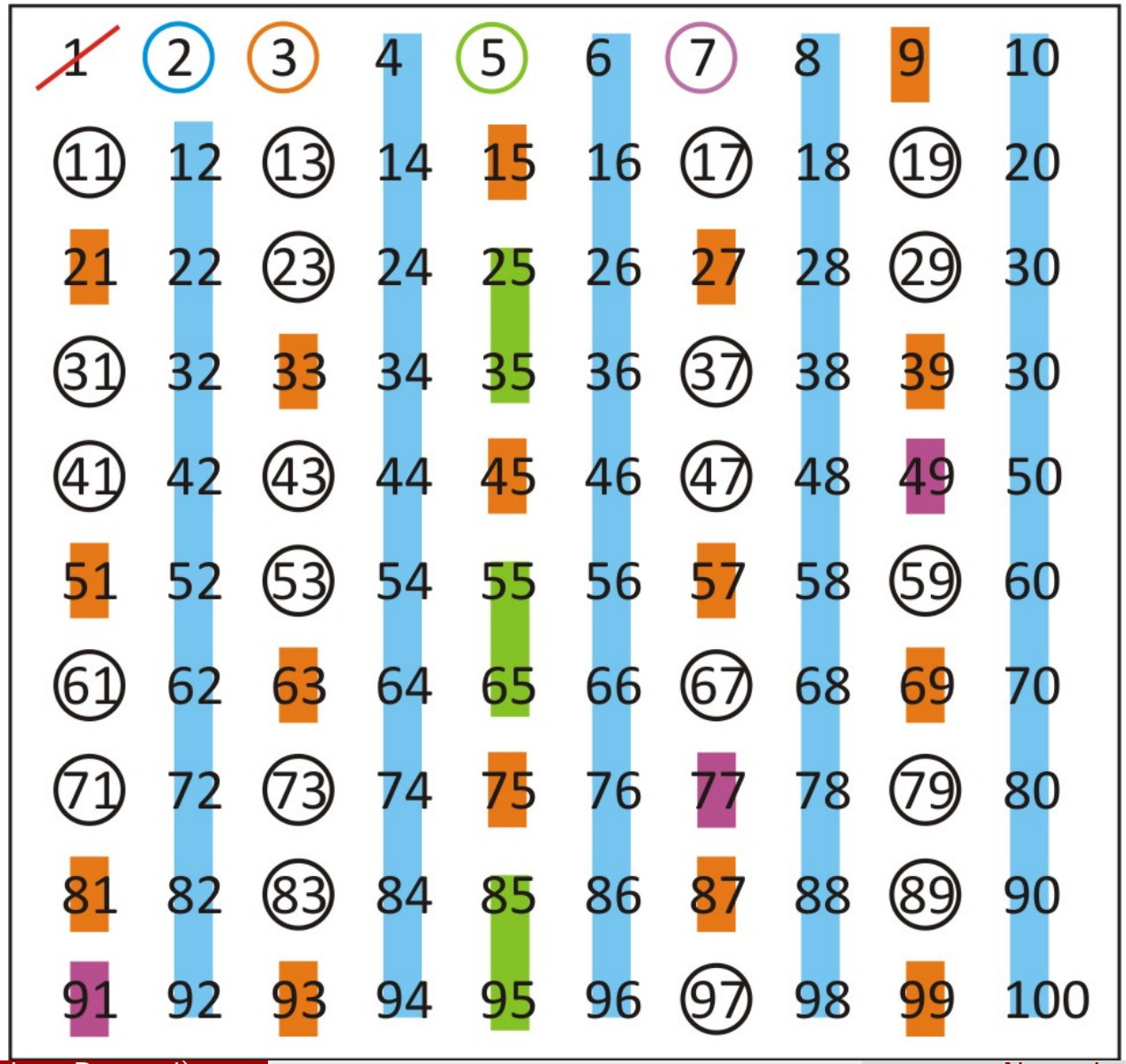
Tablica sabiranja i tablica množenja u bazi b

Npr. $b = 7$

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	10
2	2	3	4	5	6	10	11
3	3	4	5	6	10	11	12
4	4	5	6	10	11	12	13
5	5	6	10	11	12	13	14
6	6	10	11	12	13	14	15

$+$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	11	13	15
3	0	3	6	12	15	21	24
4	0	4	11	15	22	26	33
5	0	5	13	21	26	34	42
6	0	6	15	24	33	42	51

Prosti brojevi; Eratostenovo sito



Prosti brojevi; Eratostenovo sito

Teorema

Svaki prirodan broj veći od 1 ima delioca koji je prost broj.

Teorema

Ako je p najmanji prost delilac složenog broja n, onda je $p^2 \leqslant n$.

Algoritam

Da li je n prost ili složen broj?

1. Odredi sve proste brojeve p takve da je $p^2 \leqslant n$.
2. Ako neki od prostih brojeva iz koraka 1) deli n, onda je n složen broj. Ako svi prosti brojevi iz koraka 1) ne dele n, onda je n prost broj.

PRIMER. 283 je prost, jer je $17^2 = 289 > 283$ i

$$2 \nmid 283,\ 3 \nmid 283,\ 5 \nmid 283,\ 7 \nmid 283,\ 11 \nmid 283,\ 13 \nmid 283,$$

Prosti brojevi; Eratostenovo sito

Teorema

Svaki prirodan broj veći od 1 ima delioca koji je prost broj.

Teorema

Prostih brojeva ima beskonačno mnogo.

Osnovna teorema aritmetike

Za svaki $n > 1$ postoje jedinstveni prosti brojevi $p_1, p_2, \ldots, p_k$, takvi da je $p_1 < p_2 < \cdots < p_k$, i jedinstveni prirodni brojevi $\alpha_1, \alpha_2, \ldots, \alpha_k$ tako da je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

ZADATAK. Dokazati navedene teoreme.

Euklidov algoritam

Euklidov algoritam je postupak za nalaženje najvećeg zajedničkog delioca dva broja.

Primer.

$\mathbf{NZD}(300, 252) = ?$

$300 = 1 \cdot 252 + 48$

$\mathbf{NZD}(300, 252) = \mathbf{NZD}(252, 48)$

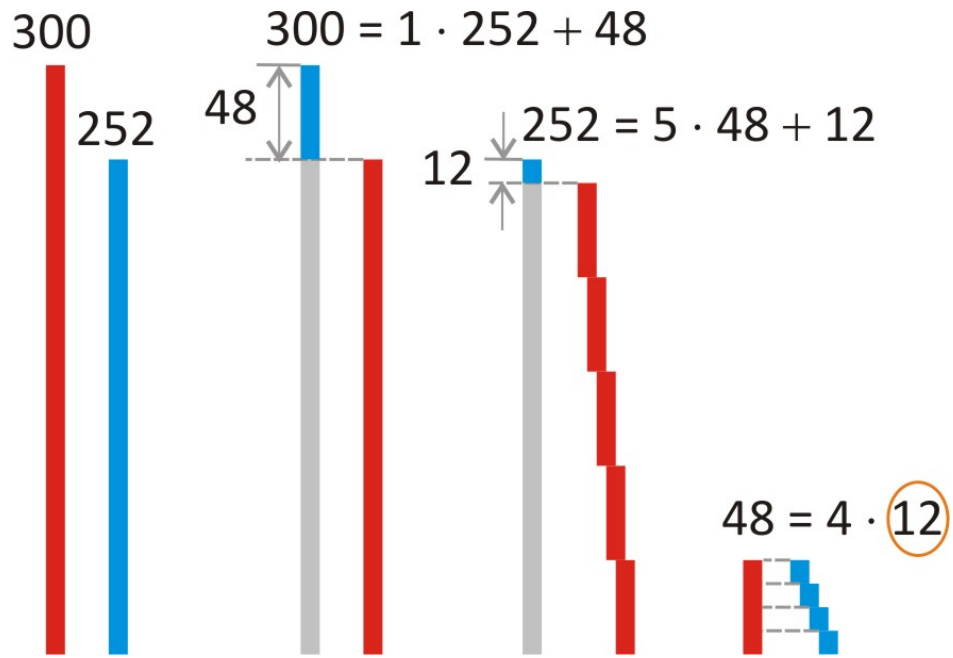
$252 = 5 \cdot 48 + 12$

$\mathbf{NZD}(252, 48) = \mathbf{NZD}(48, 12)$

$48 = 4 \cdot 12 + 0$

$\mathbf{NZD}(48, 12) = 12$

$$\boxed{\mathbf{NZD}(300, 252) = 12}$$



Euklidov algoritam

1. $\mathbf{NZD}(m,0) = m,\ m \geqslant 0$
2. $\mathbf{NZD}(m,n) = \mathbf{NZD}(n, m \bmod n),\ m,n > 0$

$[m \bmod n = \text{“ostatak pri deljenju } m \text{ sa } n\text{”}]$

PRIMER. $\mathbf{NZD}(252,300) = ?$

$\mathbf{NZD}(252,300) = \mathbf{NZD}(300, 252 \bmod 300)$ Pravilo 2.

$= \mathbf{NZD}(300,252)$ $[252 = 0 \cdot 300 + 252,\ 252 \bmod 300 = 252]$

$\mathbf{NZD}(300,252) = \mathbf{NZD}(252, 300 \bmod 252) = \mathbf{NZD}(252,48)$ Pravilo 2.

$\mathbf{NZD}(252,48) = \mathbf{NZD}(48, 252 \bmod 48) = \mathbf{NZD}(48,12)$ Pravilo 2.

$\mathbf{NZD}(48,12) = \mathbf{NZD}(12, 48 \bmod 12) = \mathbf{NZD}(12,0)$ Pravilo 2.

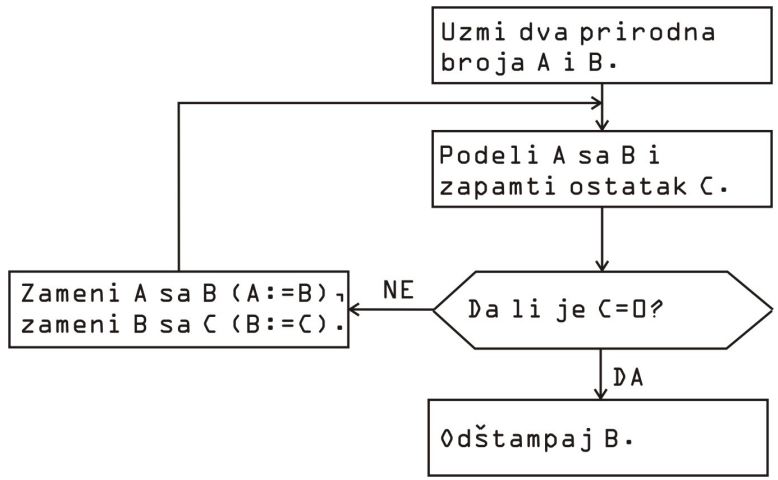
$\mathbf{NZD}(12,0) = 12$ Pravilo 1.

Euklidov algoritam

1. $\mathbf{NZD}(m,0) = m,\ m \geqslant 0$
2. $\mathbf{NZD}(m,n) = \mathbf{NZD}(n, m \bmod n),\ m \geqslant 0, n > 0$

E1 Podeli A sa B i zapamti ostatak C.

E2 Ako je $C = 0$, završi postupak i štampaj B; ako je $C > 0$, stavi da je $A := B$ i $B := C$ i idi na E1.



Knuth D., The Art of Computer programming, Addison Wesley, 1997

Pregled predavanja

Linearna Diofantova jednačina

ZADATAK. Odrediti cele brojeve x i y takve da je $300x + 252y = 6$.

$\text{NZD}(300, 252) = 12$;

$$300 = 1 \cdot 252 + 48$$
$$48 = 300 + (-1) \cdot 252$$
$$252 = 5 \cdot 48 + 12$$
$$12 = 252 + (-5) \cdot \underline{48} = 252 + (-5) \cdot (\underline{300 + (-1) \cdot 252}) = (-5) \cdot 300 + 6 \cdot 252$$

TEOREMA. Linearna Diofantova jednačina $ax + by = c$ ima rešenja u $\mathbb{Z}$ ako i samo ako $\text{NZD}(a, b) \mid c$.

ZADATAK. Da li jednačina $300x + 252y = 24$ ima rešenja u $\mathbb{Z}$?

DA: $\text{NZD}(300, 252) = 12 \mid 24$

ZADATAK. Da li jednačina $300x + 252y = 34$ ima rešenja u $\mathbb{Z}$?

NE: $\text{NZD}(300, 252) = 12 \nmid 34$

Diofantove jednačine

ZADATAK 1. Rešiti jednačinu $27x+59y=20$ u skupu $\mathbb{Z}$.

[Linearna Diofantova jednačina: $ax+by=c,\ a,b,c\in\mathbb{Z}$]

ZADATAK 2. Rešiti jednačinu $x^2-2y^2=1$ u skupu $\mathbb{Z}$.

[Pelova jednačina: $x^2-Dy^2=1$]

ZADATAK 3. Rešiti jednačinu $x^2+y^2=z^2$ u skupu $\mathbb{Z}$.

[Pitagorine trojke]

ZADATAK 4.* [Medjunarodna olimpijada, Luksemburg, 1980]
Rešiti jednačinu $x^3+x^2+xy^2+y^3=8(x^2+xy+y^2+1)$ u skupu $\mathbb{Z}$.

ZADATAK 5.* [MMO 1994]
Dokazati da jednačina $x^2+y^2+z^2=x^3+y^3+z^3$ ima beskonačno mnogo rešenja u skupu $\mathbb{Z}$.

ZADATAK 6.* [Balkanska olimpijada, Kipar 1998]
Dokazati da jednačina $y^2=x^5-4$ nema rešenja u skupu $\mathbb{Z}$.

II svetski kongres matematičara – 1900. godina, Pariz

Matematički problemi

⋮

10. *Ispitivanje rešivosti Diofantovih jednačina*

Za datu Diofantovu jednačinu sa bilo kojim brojem nepoznatih i celobrojnim koeficijentima, izmisliti postupak kojim se može odlučiti, koristeći konačan broj operacija, da li ta jednačina ima ili nema rešenja.

⋮

David Hilbert
(1862-1943)

Da li postoji algoritam DIOFANT?

Ako je $f(x_1, \ldots, x_n)$ polinom sa celobrojnim koeficijentima, da li jednačina $f(x_1, \ldots, x_n) = 0$ ima rešenja u skupu $\mathbb{Z}^n$?

ULAZ: $f(x_1, \ldots, x_n) = 0$
ALGORITAM:? DIOFANT
IZLAZ: DA/NE

ULAZ: $x_1^2 + x_2^2 - x_3^2 = 0$
ALGORITAM: DIOFANT
IZLAZ: DA

ULAZ: $x_1^5 - x_2^2 - 4 = 0$
ALGORITAM: DIOFANT
IZLAZ: NE

Ne sme da nas zavara 'polualgoritam'!

ZADATAK. Da li jednačina $x_1^3 + x_2^3 + x_3^3 = 29$ ima celobrojna rešenja?

$(0,0,0)$ – ne; $(0,0,1)$ – ne; $(0,1,0)$ – ne; $\ldots(1,1,1)$ – ne;e
$(0,0,-1)$ – ne; $\ldots(-1,-1,-1)$ – ne;
$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3,1,1)$ – DA

ZADATAK. Da li jednačina $x_1^3 + x_2^3 + x_3^3 = 30$ ima celobrojna rešenja?

DA: 'Najmanje' rešenje: $(-283059965, -2218888517, 2220422932)$

ZADATAK. Da li jednačina

$$x_1^{1729} x_2^{1093} x_3^{196884} - 163 x_1 x_2 x_3 x_4^{262537412640768000} = 561$$

ima celobrojna rešenja?

Važna pitanja

- Da li je opravdana sumnja da neki problemi nisu algoritamski rešivi?
- Kako dokazati da neki problem nije algoritamski rešiv?
- Šta je algoritam?

Al Horezmi

- Primeri algoritama su poznati praktično u svim oblastima matematike pri čemu neki potiču još iz antičkog doba.
- Reč *algoritam* dolazi od latinizovanog imena arapskog matematičara

  Abu Džafar Muhamed Ibn Musa **Al Horezmija**

  koji je u IX veku dao veliki doprinos matematici svojim delom

  Hisab **al džabr** *val mukabala*.
- Početkom XII veka jedna Al Horizmijeva knjiga je prevedena na latinski pod naslovom

  Algoritmi de numero indorum

  [prevod: *Al Horezmi o indijskoj veštini računanja*].

  Tada je u Evropu stigao savremeni pozicioni sistem zapisivanja brojeva (indijsko-arapske cifre).

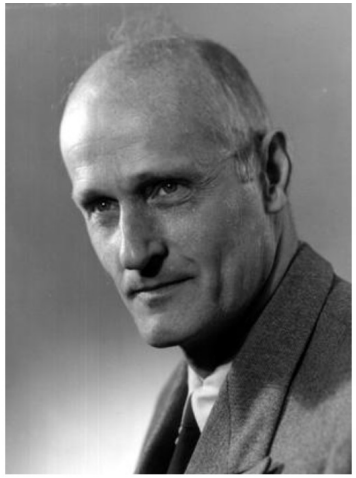
Šta je algoritam?

- Pojam *algoritma* ili *efektivne procedure* vekovima postoji u matematici bez precizne definicije. Neformalno, pod algoritmom se podrazumeva
  mehanički proces, definisan konačnim brojem instrukcija, koji se izvodi korak po korak nad konačnim skupom podataka, pri čemu je svaki korak nedvosmisleno definisan i realizuje se u konačnom vremenu i u ograničenom delu prostora.
- Iako navedena rečenica dosta dobro odgovara svakodnevnoj upotrebi ovog pojma, ona se ne može uzeti za (strogu) matematičku definiciju!
- Navedena 'definicija' nemoćna je pred problemima tipa: **pokazati da ne postoji algoritam za rešavanje nekog problema**.

30-te godine XX veka

Гедел
(1906-1978)

Черч
(1903-1995)



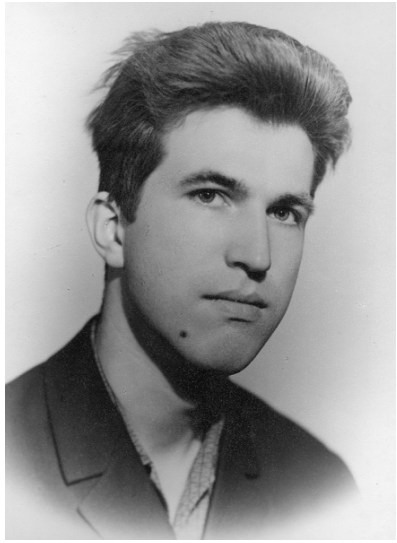
Клини
(1909-1994)

Тјуринг
(1912-1954)

30-te godine XX veka

- Kurt Gedel (1906–1978)
  1931 (Gedel ima 25 godine) Gedelove teoreme nepotpunosti; počinje da se nazire matematički pojam efektivne procedure;
  1934 Gedel uvodi pojam *uopštene rekurzivne funkcije* oslanjajući se na radove Erbrana i Akermana
- Alonso Čerč (1903–1995)
  1930 Čerč sa svojim studentima, medju kojima je najistaknutiji Klini (1909–1994), proučava λ-račun (Čerč ima 27 g., a Klini 21 g.);
  1936 Čerč formuliše čuvenu *Čerčovu tezu* i najavljuje da je Hilbertov Entscheidungsproblem nerešiv.
- Alan Tjuring (1912–1954)
  1936 Tjuring kao student (22. godine, 1935. godine) razmatra Entscheidungsproblem i svoje rešenje prikazuje svom profesoru . . . Ubrzo, Tjuringov rad priznaju Gedel, Čerč, Klini, a Tjuringov pristup smatraju genijalnim.
- Emil Post (1897–1954)
  1936 Definiše 'konačne kombinatorne procese' koji dosta podsećaju na Tjuringove mašine.

Još jedna teorema 'nemogućnosti'



Juri Matijasevič
(1947–)

Matijasevičeva teorema, 1970. godina

Ne postoji postupak o kojem Hilbert govori u svom X problemu.