Algoritmikus problémamegoldás a matematikában

Nagy Gábor Péter

Szegedi Tudományegyetem
Bolyai Intézet

Lemma Tábor népszerűsítő előadás
2025. július 14.

Tagolás

1. Algoritmusok az általános iskolában: geometria és a négy alapművelet
2. Egyenletek megoldása
3. Algoritmusok prímszámokkal

Tartalomjegyzék

Mi az, hogy algoritmus?

Definíció (Perplexity AI)

Az algoritmus olyan, pontosan meghatározott lépésekből álló utasítássorozat, amely egy adott probléma megoldására vagy feladat elvégzésére szolgál. Ezek a lépések mindig meghatározott sorrendben követik egymást, és végrehajtásuk eredményeként eljutunk a kívánt célhoz vagy eredményhez.

Az algoritmusok jellemzői:

1. **Világosak:** minden lépés egyértelműen meghatározott.
2. **Végesek:** véges számú lépésből állnak.
3. **Általánosak:** bármilyen, jól definiált probléma megoldására alkalmazhatók, legyen az matematikai, informatikai vagy akár hétköznapi feladat (pl. recept, útvonaltervezés, mosogatás)

Geometria: szerkesztés körzővel és vonalzóval

- Szakaszfelező merőleges
- Háromszög körülírt köre
- Szabályos n-szög szerkesztése
- Szögfelezés
- Szögharmadolás

Gondoljuk meg:

- *Világosak??*
- *Végesek??*
- *Általánosak??*

Megjegyzés. A gyakorlati alkalmazás teljesen más sztori...

A modern számfogalom

A geometria sokezer éves:

A modern számfogalom pár száz éves:

- Természetes és pozitív racionális számok: **OK**
- Hindu-arab számok, műveletek: **9-12. század**
- Pozitív valós számok: **16-17. század**
- Negatív számok: **17-18. század**

A négy alapművelet

- A számábrázolás
  1. tízes számrendszerben;
  2. 2-es számrendszerben;
  3. tetszőleges b alapú számrendszerben.
- A műveletek
  - összeadás, kivonás, szorzás;
  - osztás egyjegyűvel vagy többjegyűvel;
  - maradékos osztás vagy "adott tizedesjegyig".
- A lépésszám a számok **"hosszától"** függ, és nem az értékétől.
- A lépésekhez tudni kell a **"szorzótáblát".**

Tartalomjegyzék

Gyökvonás

Tétel

$\sqrt{2} \notin \mathbb{Q}$.

Négyzetgyökvonás algoritmus

Input: $x > 0$ valós szám. **Output:** $\sqrt{x}$ közelítő értéke.

Kezdő lépés: Legyen $a_1 = 1$.

Kellően sok n-re számítsuk ki:

$$a_{n+1} = \frac{a_n + \frac{x}{a_n}}{2}$$

Példa: $x = 10$.

$$1 = 1.000000000000$$

$$\frac{11}{2} = 5.500000000000$$

$$\frac{161}{44} = 3.659090909090909$$

$$\frac{45281}{14168} = 3.196005081874647$$

$$\frac{4057691201}{1283082416} = 3.16245562280389$$

$$\frac{32927862745156792961}{10412704459122043232} = 3.162277665175675$$

$$\frac{216848828649408547815429723518738920576 1}{685736206471705483022831680917430579904} = 3.16227766016838,$$

$$\frac{940468289732410986733926616197149991979558973594628248469509131993563568208 1281}{297402186271756606367853773680033489315339907993280826802387932325812841525 3888} = 3.16227766016838$$

Megoldóképletek

- Másodfokú egyenlet megoldóképlete:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

- Harmadfokú $X^3 + pX + q = 0$ egyenlet megoldóképlete:
  - Scipione del Ferro (1465–1526)
  - Niccolò Tartaglia (1499–1557)
  - Girolamo Cardano (1501–1576)

$$\sqrt{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

- Negyedfokú: Lodovico Ferrari dolgozta ki a 16. században

Abel–Ruffini-tétel (19. század eleje)

Az ötöd- és magasabb fokú egyenletnek nincs megoldóképlete.

Közelítő megoldások

- Newton-módszer, gyorsan konvergál!
- A pontatlanság **matematikai kezelése** komoly kihívás
- A pontatlan számolás **gyakorlati alkalmazása** fontos!!

Tartalomjegyzék

Nagy számok

- **Hány másodperces a világ?**

$$\begin{aligned} & 13{,}8 \text{ milliárd év} \times 356 \text{ nap} \times 24 \text{ óra} \times 60 \text{ perc} \times 60 \text{ másodperc} \\ = \quad & 13.8 \cdot 10^9 \cdot 365 \cdot 24 \cdot 60 \cdot 60 \\ = \quad & 4.35197 \cdot 10^{17} \\ \approx \quad & 2^{59}. \end{aligned}$$

- A **leggyorsabb szuperszámítógép** (El Capitan) másodpercenként

$$2\,746 \text{ exaFLOPS} = 2.764 \cdot 10^{18} \approx 2^{61}$$

  műveletet tud elvégezni.
- Az **univerzum atomjainak** becsült száma $10^{80} \approx 2^{265}$.

A prímtényezős felbontás

Az **RSA titkosírási eljárás** biztonsága az alábbi problémán nyugszik:

A feladat

- **Input:** 10-es számrendszerben n jeggyel leírható pozitív egész N szám
- **Output:** $n = p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}$ prímtényezős felbontás

A **nyerserő (brute-force)** algoritmus:

- Keressük N osztóit 3-tól $\sqrt{N}$-ig próbálgatással.
- Rossz esetben a lépésszám kb.

$$\frac{1}{2}\sqrt{N} \approx 2^{1.66\,n}.$$

- **Reménytelen,** ha a számjegyek n száma több ezer.
- **Trükkök százaival** jelenleg kb. $n = 70$ számjegyű számokat tudunk hatékonyan szorzatra bontani.

Prímtesztelés

Az RSA gyakorlati **megvalósítása** szempontjából fontosak a nagy prímszámok:

Feladat

- **Input:** 10-es számrendszerben n jeggyel leírható pozitív egész N szám
- **Output:** Igaz-e, hogy N prímszám.

- **FIGYELEM!** Nem feladat N-et tényezőkre bontani.
- Nehezebb, mint a prímtényezős felbontás.
- *Pontosabban:* **visszavezethető** a prímtényezős felbontásra.
- A nyerserő-algoritmus lépésszáma kb. $2^{1.66\,n}$; nem használható nagy n-re.
- **Miller–Rabin-teszt** (1980) NEM VILÁGOS (probabilisztikus) algoritmus.
- **Agrawal-Kayal-Saxena (AKS) teszt** (2002) lépésszáma kb. n^{12}.

Tanúk keresése

Kis Fermat-tétel (nem nagyon nehéz)

Ha p prím, akkor minden a pozitív egészre $a^p - a$ osztható p-el.

Pl. $3^5 - 3 = 243 - 3 = 240 = 5 \cdot 48$.

A tanú fogalma

Adott a N pozitív egész. Azt mondjuk, hogy az a szám tanúskodik N összetettségére, ha $a^N - a$ nem osztható N-el.

Pl. $2^6 - 2 = 62$ nem osztható 6-al. Az $a = 2$ tanúsítja, hogy $N = 6$ összetett szám (nem prím).

Carmichael-számok ("álprímek")

Azt az N összetett számot nevezzük Carmichael-számnak, aminek nincs tanúja.

- A legkisebb Carmichael-szám az $561 = 3 \cdot 11 \cdot 17$.
- Nem tudjuk, hogy végtelen sok van-e belőlük.

Probabilisztikus algoritmusok

- Miller tanúja jobb: minden összetett N számnak van tanúja.
- Be lehet bizonyítani, hogy az 1 és N közé eső számok kb. fele tanú.
- **Ötlet:**
  - Válasszunk 100 számot véletlenül 1 és N között.
  - Ha találunk köztük tanút, akkor N biztosan összetett.
  - Ha nem találunk, akkor N prímszám

$$1 - \frac{1}{2^{100}} \approx 99.9999999999999999999999999997\%$$

  valószínűséggel.
- Ezek az *"ipari prímek"*.

A legnagyobb közös osztó

A feladat

- **Input:** 10-es számrendszerben n jeggyel leírható pozitív egész N és M számok
- **Output:** lnko(N, M)

- A iskolában tanult módszer a **prímtényezős felbontást** használja, amire nem ismert *hatékony algoritmus*.
- 2000 éve ismert az **Euklideszi algoritmus:**

Észrevétel

Ha a d szám közös osztója N-nek és M-nek, akkor osztója $N + M$-nek és $N - M$-nek is.

- **Következmény:** lnko(N, M) = lnko$(N, N - M)$.

Feladat

Határozzuk meg $N = 235\,757$ és $M = 74\,939$ lnko-ját.

Az Euklideszi algoritmus páratlan számokra

Feladat

Határozzuk meg $N = 235\,757$ és $M = 74\,939$ legnagyobb közös osztóját.

	N	M	
Kivonás	235 757	74 939	160 818
Osztás 2-vel	160 818	74 939	80 409
Kivonás	80 409	74 939	5 470
Osztás 2-vel	5 470	74 939	2 735
Kivonás	74 939	2 735	72 204
Osztás 2-vel	72 204	2 735	36 102
Osztás 2-vel	36 102	2 735	18 051
Kivonás	18 051	2 735	15 316
Osztás 2-vel	15 316	2 735	7 658
Osztás 2-vel	7 658	2 735	3 829
Kivonás	3 829	2 735	1 094
Osztás 2-vel	1 094	2 735	547
Kivonás	2 735	547	2 188
Osztás 2-vel	2 188	547	1 094
Osztás 2-vel	1 094	547	547
Kivonás	547	547	0