Kitajski izrek o ostankih

Tina Mozetič, Lucija Pinterić, Ana Knap
Mentorica: Živa Urbančič

Matematični raziskovalni tabor
20. avgust 2016

Povzetek

V članku si bomo pogledali, kako rešujemo sisteme kongruenčnih enačb. Najprej bomo spoznali Bezoutovo identiteto in kongruenco ter nato pridobljeno znanje navezali na Kitajski izrek o ostankih, ki ga bomo uporabili za pomoč pozabljivi veverički Jasni.

1 Uvod

Veverička Jasna je lansko jesen skrila lešnike v različna skrivališča, a se ne spomni, koliko jih je bilo. Boji se, da je izpraznila vso ozimnico. Ker ima obsesivo kompulzivno motnjo, zagotovo ve, da jih je razporedila tako, da jih je v vsakem skrivališču skrila enako število. Najprej jih je razporedila v kupčke po 3, vendar ji je eden ostal sam. Prav tako ji je en lešnik ostal, ko jih je razporedila v kupčke po 5. V tretje ji je končno uspelo lešnike urediti v kupčke po 13. Ali lahko povemo, koliko lešnikov je skrila?

2 Bezoutova indentiteta

Bezoutova indentiteta je eden od osnovnih izrekov teorije števil. Zato ni presenetljivo, da je v veliko pomoč pri dokazu Kitajskega izreka o ostankih.

Izrek 1. ***Bezoutova identiteta.*** *Naj bosta x in y neničelni celi števili in naj bo D njun največji skupni delitelj. Potem obstajata taki celi števili a in b, da D lahko zapišemo kot*

$$D = ax + by.$$

Števili a in b imenujemo ***Bezoutova koeficienta****.*

Bezuotova identiteta torej pomeni, da lahko največji skupni delitelj dveh števil zapišemo kot vsoto njunih večkratnikov. Bezoutova koeficienta nista enolično določena.

Pri iskanju Bezoutovih koeficientov si bomo pomagali z razširjenim Evklidovim algoritmom. To bomo demonstrirali na primeru, ko je $x = 21$ in $y = 8$. Najprej izvedemo Evklidov algoritem, da dobimo največji skupni delitelj, ki je v tem primeru $D = 1$, in iz vsake vrstice izrazimo ostanek. S simboli to zapišemo kot

$$\begin{aligned}
21 = 2 \cdot 8 + 5 \quad &\Rightarrow \quad 5 = 21 - 2 \cdot 8 \\
8 = 1 \cdot 5 + 3 \quad &\Rightarrow \quad 3 = 8 - 1 \cdot 5 \\
5 = 1 \cdot 3 + 2 \quad &\Rightarrow \quad 2 = 5 - 1 \cdot 3 \\
3 = 1 \cdot 2 + 1 \quad &\Rightarrow \quad 1 = 3 - 1 \cdot 2
\end{aligned}$$

Nato jih od spodaj navzgor vstavljamo v zadnjo enačbo, v kateri izrazimo D. Ko postopek končamo, je največji skupni delitelj izražen v željeni obliki.

$$\begin{aligned}
1 &= 3 - 2 \cdot 1 \\
1 &= 3 - (5 - 1 \cdot 3) \\
1 &= 2 \cdot 3 - 5 \\
1 &= 2 \cdot (8 - 1 \cdot 5) - 5 \\
1 &= 2 \cdot 8 - 3 \cdot 5 \\
1 &= 2 \cdot 8 - 3 \cdot (21 - 2 \cdot 8) \\
1 &= 2 \cdot 8 - 3 \cdot 21 + 6 \cdot 8
\end{aligned}$$

$$1 = \underbrace{8}_{b} \cdot \underbrace{8}_{y} + \underbrace{(-3)}_{a} \cdot \underbrace{21}_{x}$$

3 Kongruenca

Kongruenca je matematičen pojem, ki nam pomaga pri raziskovanju ostankov pri celoštevilskem deljenju. Včasih želimo elemente, ki dajo pri deljenju z nekim pozitivnim celim številom enak ostanek, obravnavati kot ekvivalentne. Zato definiramo:

Definicija 1. *Če imata celi števili x in y pri deljenju z $n \in \mathbb{N}$ isti ostanek, pravimo, da sta si* ***kongruentni po modulu n****, in pišemo:*

$$x \equiv y \,(\mathrm{mod}\, n).$$

Opomba. *Vsako celo število je kongruentno po modulu n nekemu x, ki leži med 0 in n, torej $0 \leq x < n$.*

Naj velja $a \equiv a' \,(\mathrm{mod}\, n)$ in $b \equiv b' \,(\mathrm{mod}\, n)$, medtem ko naj bo k poljubno celo število. Za kongruenco veljajo sledeče lastnosti:

- Kongruentnost po modulu n je ekvivalenčna relacija,
- $a + b \equiv a' + b' \,(\mathrm{mod}\, n)$ in $a - b \equiv a' - b' \,(\mathrm{mod}\, n)$,
- $a \cdot b \equiv a' \cdot b' \,(\mathrm{mod}\, n)$,
- $k \cdot a \equiv k \cdot a' \,(\mathrm{mod}\, n)$,
- $a^k \equiv a'^{\,k} \,(\mathrm{mod}\, n)$.

Sedaj, ko poznamo pojem kongruence, lahko problem veverice Jasne predstavimo drugače. Iščemo rešitev sistema

$$x \equiv 1 \,(\mathrm{mod}\, 3)$$
$$x \equiv 1 \,(\mathrm{mod}\, 5)$$
$$x \equiv 0 \,(\mathrm{mod}\, 13).$$

4 Formulacija izreka

Obstoj rešitve zgornjemu podobnih sistemov nam zagotavlja Kitajski izrek o ostankih. Najstarejša omemba tega izreka sega v 3. stoletje, ko ga je kitajski matematik Sun Či formuliral v svoji knjigi Sun Čijeva klasična matematika. V zapisu izreka ni dokazal in prav tako ni v celoti podal algoritma za iskanje rešitve. Čeprav so delne dokaze poznali že prej, je bila najbolj splošna oblika izreka dokazana šele v 13. stoletju.

Izrek 2. ***Kitajski izrek o ostankih.*** *Naj bodo $n_1, \ldots, n_k$ paroma tuja si cela števila in $n_i > 1$ za vsak $i \in \{1, 2, \ldots, k\}$. Z N označimo produkt teh števil ($N = n_1 \cdot \ldots \cdot n_k$). Naj bodo $a_1, \ldots, a_k$ taka cela števila,*

da za vsak $i \in \{1, \ldots, k\}$ velja $0 \leq a_i < n_i$. Potem obstaja celo število x, ki zadošča sistemu:

$$x \equiv a_1 \pmod{n_1}$$
$$\vdots$$
$$x \equiv a_k \pmod{n_k}.$$

Vsaki dve števili, ki zgornjemu sistemu zadoščata, sta si kongruentni po modulu N.

Dokaz izreka bomo razdelili na dva dela. V prvem bomo dokazali, da je rešitev (če le obstaja) enolična do modula N natančno, v drugem pa, da prav res tudi obstaja.

Dokaz.

1. Najprej dokažimo enoličnost. Predpostavimo, da obstajata 2 rešitvi. Označimo ju z x in y. Oglejmo si le ostanke pri deljenju z n_1:

   $$x \equiv a_1 \pmod{n_1}$$
   $$y \equiv a_1 \pmod{n_1}$$

   Iz tega lahko sklepamo, da je $x \equiv y \pmod{n_1}$. Podoben sklep lahko naredimo za vsak indeks in dobimo $x \equiv y \bmod n_i$.
   Zgornjo ugovitev lahko ekvivalentno zapišemo kot:

   $$n_i \mid x - y \quad \forall i \in 1, 2, \ldots, k$$

   Ker je N večkratnik vsakega n_i, vemo, da velja $N \mid x - y$. To pomeni, da je x kongruenten y po modulu N, torej

   $$x \equiv y \pmod{N}.$$

   S tem smo dokazali, da je rešitev enolična do modula N natančno.

2. Sedaj dokažimo še obstoj. Naj bosta n_1 in n_2 tuji si celi števili. Iščemo x, ki ustreza sistemu

   $$x \equiv a_1 \pmod{n_1}$$
   $$x \equiv a_2 \pmod{n_2}.$$

   Pokažimo, da je eno od števil, ki rešijo zgornji sistem oblike

   $$x = a_2 \cdot m_1 \cdot n_1 + a_1 \cdot m_2 \cdot n_2.$$

Iz Bezoutove indentitete izrazimo $m_1 \cdot n_1$ kot $1 - m_2 \cdot n_2$ in vstavimo v izraz za x:

$$x = a_2 \cdot (1 - m_2 \cdot n_2) + a_1 \cdot m_2 \cdot n_2$$

$$x = a_2 - m_2 \cdot n_2 \cdot (a_2 - a_1)$$

Iz tega je razvidno, da je x res kongruenten a_2 po modulu n_2, saj je $m_2 \cdot n_2 \cdot (a_2 - a_1)$ večkratnik n_2. Iz Bezoutove identitete lahko izrazimo tudi $m_2 \cdot n_2$ in po enakem postopku pokažemo, da je $x \equiv a_1 \pmod{n_1}$.

Po zgornjem postopku rešujemo sisteme dveh enačb. Če pa imamo sistem z več enačbami, najprej poiščemo rešitev prvih dveh enačb in ju združimo v eno. Dobimo sistem s $k-1$ enačbami od prvotnih k enačb.

$$k-1 \begin{cases} x \equiv a_{1,2} \pmod{n_1 \cdot n_2} \\ x \equiv a_3 \pmod{n_3} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

Postopek nato ponavljamo, dokler prvotnega sistema ne skrčimo do sistema dveh enačb, ki ga že znamo rešiti.

□

5 Algoritem za reševanje sistemov s kongruenco

Reševanje sistemov s kongruenco ponazorimo na primeru veveričke Jasne, ki ga predstavimo s sistemom:

$$x \equiv 1 \pmod{3}$$

$$x \equiv 1 \pmod{5}$$

$$x \equiv 0 \pmod{13}.$$

Rešitev bomo poiskali po postopku, ki smo ga uporabili v drugem delu dokaza Kitajskega izreka o ostankih, to je v dokazu obstoja rešitve. Najprej obravnavamo prvi dve enačbi in izračunamo Bezoutovo identiteto za $n_1 = 3$ in $n_2 = 5$, torej

$$1 = m_1 \cdot n_1 + m_2 \cdot n_2 =$$

$$\mathbf{2} \cdot 3 + (\mathbf{-1}) \cdot 5 = 1.$$

V vlogi Bezuotovega koeficienta m_1 imamo število 2, v vlogi m_2 pa -1. Kakor v dokazu sedaj zapišemo $a_{1,2}$ kot

$$a_{1,2} = a_1 \cdot m_2 \cdot n_2 + a_2 \cdot m_1 \cdot n_1 = 1 \cdot (-1) \cdot 5 + 1 \cdot 2 \cdot 3 = 1.$$

Ker vemo, da je končna rešitev x kongruentna delni rešitvi $a_{1,2}$ po modulu produkta $n_1 \cdot n_2$, lahko prvi dve enačbi združimo v eno.

$$x \equiv a_{1,2} \pmod{3 \cdot 5} \quad \Rightarrow \quad x \equiv 1 \pmod{15}$$

Naš novi sistem je:

$$x \equiv 1 \pmod{15}$$

$$x \equiv 0 \pmod{13}.$$

Postopek ponovimo in zapišemo Bezoutovo identiteto za $n_1 = 15$ in $n_2 = 13$.

$$1 = m_1 \cdot n_1 + m_2 \cdot n_2 =$$

$$(\mathbf{-6}) \cdot 15 + \mathbf{7} \cdot 13 = 1$$

V vlogi m_1 nastopa število -6, v vlogi m_2 pa 7. Naša rešitev je torej:

$$x = a_1 \cdot m_2 \cdot n_2 + a_2 \cdot m_1 \cdot n_1 = 0 \cdot (-6) \cdot 15 + 1 \cdot 7 \cdot 13 = 91$$

Veverička Jasna je torej lansko leto skrila najmanj 91 lešnikov. Vemo pa, da jih je lahko skrila tudi $91 + k \cdot 13 \cdot 15$ za $k = 0, 1, 2, \ldots$, saj so si ta števila med seboj kongruentna po modulu 195.

6 Zaključek

Kitajski izrek o ostankih je zelo pomemben izrek teorije števil, ki je tudi zelo lahko razumljiv. Poznamo veliko dokazov, ki uporabijo sredstva različnih vej matematike. Z nekaterimi od njih podamo tudi algoritem, ki nam pomaga reševati probleme, tako v vsakdanjem življenju, kot v svetu matematike.

7 Literatura

- `https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity#History`
- `http://mathworld.wolfram.com/Congruence.html`
- `https://en.wikipedia.org/wiki/Chinese_remainder_theorem`