KITAJSKI IZREK O OSTANKIH, 1. del

V tem sestavku bomo predstavili starodavni *kitajski izrek o ostankih*, v drugem delu pa še nekaj konkretnih zgledov uporabe, ki kažejo na to, da je izrek aktualen še danes. Videli bomo, kako lahko iz obrobnih informacij sestavimo celotno sliko, podobno kot če bi iz tlorisa, narisa in stranskega risa (torej posameznih projekcij) ugotovili, za kakšno telo gre.[1]

V daljni Kitajski je Sun Tsu Suan-Ching v četrtem stoletju postavil naslednje vprašanje:

> *Poišči število, katero da pri deljenju s* 3 *ostanek* 2,
> *pri deljenju s* 5 *ostanek* 3 *in pri deljenju s* 7 *ostanek* 2.

Odgovor na to vprašanje iščite najprej sami in šele nato nadaljujte z branjem. Že kukate? Pa vam dam namig: na list napišite nekaj začetnih števil, ki dajejo ostanek 2 pri deljenju s 3: $2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, \ldots$ Ste se že utrudili? Pa saj ni tako težko, prvo število je že sam ostanek, potem pa samo še prištevate 3. Preostali množici pa poiščite sami in premislite, kaj bi počeli z njimi prebrisami presekovci.

Ste že nazaj! Koliko rešitev ste pa našli? Eno? Dve? Gotovo jih lahko najdete več!

Poglejmo, kako smo nalogo ugnali mi. Če iskano število n pomanjšamo za 2, potem je deljivo tako s 3 kot tudi s 7. Če upoštevamo še, da sta si ti števili tuji, lahko zapišemo

$$n = 21\,m + 2 \qquad \text{za neko celo število } m.$$

Po drugi strani pa $5 \,|\, (21\,m + 2) - 3 = 21\,m - 1$, oziroma če odštejemo večkratnik števila pet, $5 \,|\, 21\,m - 1 - 5 \times 4\,m = m - 1$. Zaključimo $m - 1 = 5\,\ell$ za neko celo število ℓ oziroma

$$m = 5\,\ell + 1 \qquad \text{in zato} \qquad n = 21\,(5\,\ell + 1) + 2 = 105\,\ell + 23.$$

Število n, ki je oblike $n = 105\,\ell + 23$, oziroma

$$n = 3\,(35\,\ell + 7) + 2 = 5\,(21\,\ell + 4) + 3 = 7\,(15\,\ell + 3) + 2,$$

očitno zadovoljuje vse tri začetne pogoje, kar pomeni, da je rešitev neskončno:

$$\ldots, \quad -82 \text{ (za } \ell = -1), \quad 23 \text{ (za } \ell = 0), \quad 128 \text{ (za } \ell = 1), \quad \ldots$$

[1] Taka lastnost je res nekaj izjemnega, saj v ravnini recimo sploh ne ločimo sence kroga in kvadrata - v obeh primerih gre za daljico. Morda pa bralca bolj zanima geometrija kakor algebra, o kateri bomo govorili v nadaljevanju. V tem primeru je zate naloga, ki jo je avtor tega sestavka reševal v osmem razredu osnovne šole na šolskem tekmovanju. Poišči ključ, katerega omenjene tri projekcije so krog, kvadrat ter enakostranični trikotnik.

Morda pa vas pritegne tudi nekoliko mlajša, a po drugi strani še bolj zanimiva zgodba iz Brahma-Sphuta-Siddhanta, ki jo je pripovedoval Brahmagupta (rojen konec 6. stoletja):[2]

Ženica gre na trg prodajat jajca. Ravno, ko zloži jajca na stojnico, podivja konj in podre stojnico. Jajca se strejo in ženica je vsa obupana. Jezdec galantno ponudi poravnavo, a ženica ne zna povedati, koliko jajc je bilo na stojnici. Potarna, da je šlo s temi jajci od samega začetka vse narobe. Spomni se, da je pri zbiranju jajc prosila hčer, da zleze v kurnik in ji podaja jajca. Dajala je po dve jajci naenkrat in na koncu ji je dala še eno samo jajce. Ko je sama zlagala jajca v škatlo, je prijela po tri in tudi njej je na koncu ostalo ravno eno jajce. Škatlo je razmočil dež in jajca je bilo potrebno preložiti. Tokrat je hči z vsako roko prijela po dve jajci in jih z obema rokama hkrati podajala materi, na koncu pa ji je dala eno samo jajce. Ko je oče kuhal jajca, je v posodo dal po pet jajc naenkrat in tudi on je na koncu moral seči po eno samo jajce. Ta nesrečna nedeljivost se je nadaljevala, saj so jajca zložili v škatle po šest in za zadnjo škatlo imeli eno samo jajce. Tedaj pa se oglasi njen sin in pove, da je pri barvanju jajca postavil v vrsto po sedem in se je ravno izšlo ter da se gotovo da izračunati, koliko jajc je potrebno plačati. Nekemu možu se ženica zasmili in ji prišepne, naj zahteva od jezdeca plačilo za 721 *jajc. Število* 721 *res daje ostanek* 1 *pri deljenju z* 2, 3, 4, 5, 6 *in je deljivo s* 7*, vendar pa se je zdelo jezdecu vseeno malo preveč denarja in premalo strtih jajc.*

Pomagajte jezdecu in ugotovite, če je mu je res potrebno plačati toliko jajc.

[2] Zgodbo smo za naše potrebe nekoliko priredili, glejte pa tudi V. Batagelj, Bistrovidec: Razbita jajca, *Presek* **11**/2, str. 130.

Ste že našli pravi odgovor? Tule je naša rešitev, ki je kar nekoliko podobna prejšnji. Očitno je dovolj iskati število n, ki daje pri deljenju s $60 = 3 \times 4 \times 5$ ostanek 1 (saj sta bila podatka o deljivosti z 2 in 6 pravzaprav popolnoma odveč - po drugi strani pa si lahko mislimo, da je možnosti, da si je ženica vse skupaj izmislila, nekoliko manj), hkrati pa je deljivo s 7, tj.

$$n = 60\,m + 1 \qquad \text{za } m \in \mathbb{Z} \qquad \text{in} \qquad 7 \,|\, 60\,m + 1.$$

Zopet se spomnimo, da lahko slednjo relacijo še nekoliko preoblikujemo, saj lahko po mili volji dodajamo ali odvzemamo večkratnike števila sedem:

$$7 \,|\, (60 - 7 \times 8)\,m + 1 + 7 = 4\,m + 8 = 4\,(m + 2).$$

Od tod zaključimo $7 \,|\, m + 2$, tj.

$$m = 7\,\ell - 2 \;\; \text{za } \ell \in \mathbb{Z} \qquad \text{in končno} \qquad n = 60\,(7\,\ell - 2) + 1 = 420\,\ell - 119.$$

Torej lahko jezdec plača tudi le $1 \times 420 - 119 = 301$ jajce (namesto prvotno predlaganih $2 \times 420 - 119 = 721$ jajc), navkljub vsesplošni naklonjenosti ženici.

Precej logično je, da smo število $60\,m$ nadomestili s $4\,m$, saj daje število 60 ostanek 4 pri deljenju s 7. Nato pa smo samo še prišteli eno sedmico in že smo lahko izpostavili 4.

Če želimo ugnati vsako nalogo takega tipa, se moramo vprašati, ali nam uspe končno izpostavljanje v vsakem primeru ali pa gre samo za naključje - začetniško srečo? Recimo, da bi prišli do relacije $7 \mid a\,m + b$, kjer sta a in b ostanka pri deljenju s 7. Sedaj je potrebno prišteti x sedmic, da bo $a \mid b + 7\,x$, oziroma za dani števili a in b v celih številih rešiti enačbo $b = a\,y - 7\,x$. Grški filozof Diophantus iz tretjega stoletja je napisal številne knjige o problemih, ki iščejo celoštevilske rešitve. Po njemu imenujemo take enačbe *diofantske*. Se da torej vedno rešiti pravkar dobljeno diofantsko enačbo? Tablica za množenje po modulu 7, glej tabelo 1(b), ima to lastnost, da v stolpcu večkratnikov števila a (ali pa kateremkoli drugem stolpcu) nastopajo prav vsi od nič različni ostanki pri deljenju s sedem, torej tudi število b. Le-to pa ustreza ravno večkratniku $a\,y$. Glej A. Jurišić, Računala nove dobe, *Presek* **30** (2002-03), str. 226–231 (1. del) in 291–296 (2. del).

$*_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(a)

$*_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(b)

Tabela 1: tablici za množenje po modulu 5 (a) oziroma 7 (b).

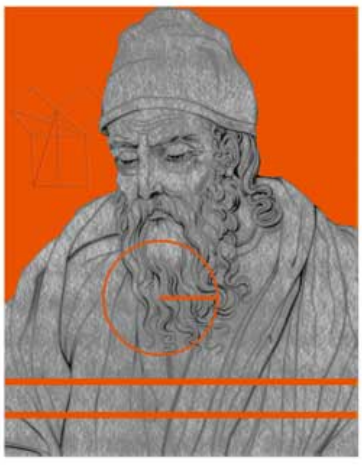
Če bi delali z veliko večjimi števili, bi bili hočeš nočeš prisiljeni uprabiti kaj bolj učinkovitega (kot sestavljanje tabele). V resnici iščemo v splošnem rešitev diofantske enačbe $a\,y - p\,x = b$, kjer smo število 7 nadomestili s p. Za obstoj rešitve je očitno potrebno, da je število b večkratnik največjega skupnega delitelja števil p in a, tj. $D(p, a) \mid b$. Ni pa to samo potreben temveč tudi zadosten pogoj za obstoj rešitve (glej M. Juvan, O Evklidovem algoritmu, *Presek* **21** (1993-94), str. 116–121). Če je torej p praštevilo, a pa ni njegov večkratnik, potem velja $D(p, a) = 1$ in je ta pogoj vedno izpolnjen. Za iskanje rešitve pa je najbolj primerno uporabiti ravno razširjen Evklidov algoritem iz že omenjenega Presekovega članka, ki je do današnjih dni ostal najbolj učinkovit.

Zgled: Evklidov algoritem (levo) in razširjeni Evklidov algoritem (desno). Rešujemo (linearno) difantsko enačbo $4864\,x + 3458\,y = 38$ in postavimo $p_0 = 0$ in $p_1 = 1$:

$$
\begin{aligned}
4864 &= \mathbf{1}{\cdot}3458{+}1406 & p_2 &:= p_1 - \mathbf{1} \cdot p_0 = 1 \\
3458 &= \mathbf{2}{\cdot}1406{+}646 & p_3 &:= p_2 - \mathbf{2} \cdot p_1 = -2 \\
1406 &= \mathbf{2}{\cdot}646{+}114 & p_4 &:= p_3 - \mathbf{2} \cdot p_2 = 5 \\
646 &= \mathbf{5}{\cdot}114{+}76 & p_5 &:= p_4 - \mathbf{5} \cdot p_3 = -27 \\
114 &= \mathbf{1}{\cdot}76{+}38 & p_6 &:= p_5 - \mathbf{1} \cdot p_4 = 32 \\
76 &= \mathbf{2}{\cdot}38{+}0 & p_7 &:= p_6 - \mathbf{2} \cdot p_5 = -91
\end{aligned}
$$

Ko pridemo do $x = p_7 = -91$, lahko dobimo $y = 128$ kot rešitev linearne enačbe. Končno imamo:

$$4864 \cdot (-91) + 3458 \cdot (128) = 38.$$



Zdi se, da smo zbrali vse začimbe, potrebne za okusno jed. Za konec izpopolnimo našo tehniko do te mere, da bo primerna za večkratno uporabo.

Izrek o ostankih

V rubriki *Matematično razvedrilo* je kitajski izrek o ostankih omenil že E. Rusjan, Kako "uganeš" število, *Presek* **4**/4 (1976-77) , str. 237–239. Za tiste, ki jih je pričel zanimati ta izrek, je članek zelo primeren, saj govori pa o čarovniških sposobnostih (priporočam ogled še pred nadaljnjim branjem).[3]

Kitajski izrek o ostankih. *Naj bodo $a_1, a_2, ..., a_r$ cela števila, $m_1, m_2, ..., m_r$ pa naravna števila, ki so paroma tuja, tj. $D(m_i, m_j) = 1$ za $i \neq j$. Naj bo $M = m_1 \cdot m_2 \cdot \ldots \cdot m_r$ in število $x \in \{0, 1, \ldots, M-1\}$ tako, da ima pri deljenju z m_i ostanek a_i za $i \in \{1, 2, \ldots, r\}$, tj.*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, \quad x \equiv a_r \pmod{m_r}. \tag{1}$$

Potem je x natanko določeno število. Izračunamo ga na naslednji način:
za $M_j = M/m_j$ poiščemo $y_j = M_j^{-1} \bmod m_j$, za $j = 1, ..., r$ in nato sestavimo

$$x \quad = \quad a_1 \cdot M_1 \cdot y_1 + \cdots + a_r \cdot M_r \cdot y_r \mod M. \tag{2}$$

Zaradi angleškega imena Chinese Remainder Theorem se za ta izrek pogosto uporablja kratica CRT. Relacijam v (1) pravimo *kongruence* in jih preberemo na naslednji način: *x je kongruenten a_i po modulu m_i*, njihov pomen pa je, da imajo števila na obeh straneh relacije enak ostanek pri deljenju z ustreznim modulom. V zadnji enakosti pa *mod* na desni strani označuje ostanek dane vsote pri deljenju z modulom M. Sedaj pa pojasnimo še oznako M_j^{-1} oziroma $M_j^{-1} \bmod m_j$. Le-ta je rešitev kongruence $M_j \cdot y_j \equiv 1 \pmod{m_j}$ (tj. multiplikativni inverz števila M_j po modulu m_j) oziroma linearne diofantske enačbe $M_j \cdot y_j + m_j \cdot z_j = 1$.

Dokaz: Število M_i^{-1} oziroma y_i izračunamo s pomočjo razširjenega Evklidovega algoritma. To lahko storimo vedno, ker so si števila $m_1, m_2, ..., m_r$ paroma tuja in sta si zato tudi števili M_j in m_j tuji. Izraz (2) res zadovoljuje vse pogoje iz (1), saj je vsak njegov seštevanec, z izjemo i-tega: $a_i\, M_i\, y_i$, deljiv z m_i, v i-tem seštevancu pa sta števili M_i in y_i obratni po modulu m_i in zato res dobimo ostanek a_i.

Tudi dokaz enoličnosti rešitve ni dosti težji. Če obstajata dve rešitvi x in x' v množici $\{0, 1, \ldots, M-1\}$, potem velja $m_i \,|\, (x - x')$ za $i \in \{1, 2, \ldots, r\}$ in od tod (ker so števila $m_1, m_2, ..., m_r$ paroma tuja) tudi $M \,|\, (x - x')$ oziroma $x = x'$. □

Primer. Poiščimo tako naravno število x, ki daje ostanek 2 pri deljenju s 3, ostanek 3 pri deljenju s 4 in ostanek 1 pri deljenju s 5 in je manjše od $3 \cdot 4 \cdot 5 = 60$. Z uporabo razširjenega Evklidovega algoritma za

- $m_1 = 3$ in $M_1 = 4 \cdot 5 = 20$, pridemo do $20 \cdot 2 + 3 \cdot (-13) = 1$ in $M_1 \cdot y_1 = 40$;
- $m_2 = 4$ in $M_2 = 3 \cdot 5 = 15$, dobimo $15 \cdot 3 + 4 \cdot (-11) = 1$ in $M_2 \cdot y_2 = 45$;
- $m_3 = 5$ in $M_3 = 3 \cdot 4 = 12$, zaključimo še $+12 \cdot (-2) + 5 \cdot 5 = 1$ in $M_3 \cdot y_3 = -24$.

Tako je rešitev $x = 2 \cdot 40 + 3 \cdot 45 + 1 \cdot (-24) = 191 \bmod 60 = 11$.

[3] Glej ga zlomka. Sprva je avtor mislil, da se o izreku o ostankih v Preseku še ni pisalo. Časa, da bi prelistal 30 letnikov in več, v vsakem v povprečju po 6 izvodov, torej čez 180 zvezkov po povprečno 60 strani, tj. skoraj 11.000 strani, pa ni bilo. Vendar pa je to danes, ko smo čez počitnice spravili vse Preseke v digitalno obliko, precej lažje preveriti. Da pa vam prihranimo pot v knjižnico, vas bomo lahko kmalu napotili kar na internet.

Ko enkrat izračunamo produkte $M_1 \cdot y_1, \ldots, M_r \cdot y_r$, lahko hitro postrezemo z odgovori za različne $a_1, \ldots, a_r$.

Predno zaključimo prvi del, naj omenimo bralcem, da smo o kongruencah v Preseku že pisali:

F. Forstnerič, O kongruencah, *Presek* **7**/3 (1979/80), str. 145–152;

B. Lavrič, Ogrejmo se za kongruence in D. Pagon, Kongruence in Eulerjev izrek, *Presek* **15**/4 (1987/88), str. 193 in str. 194–196.

Res je od tedaj minilo že veliko časa, a branje vseh zgornjih člankov vsekakor toplo priporočamo. Kot zanimivost omenimo še, da je ta prispevek spodbudila prva naloga za tretjo skupino na letošnjem tekmovanju iz računalništva (IJS), glej `http://rtk.ijs.si/2008/rtk2008.pdf`, str. 36, ki govori o varnosti pinov (to so tiste štirimesne številke, ki jih uporabljamo za zaščito telefonov, bančnih kartic in podobno) ter je povezana z generatorji psevdo-naključnih števil - LFSR (a to je že druga zgodba).

V drugem delu pa vabimo bralce, da spoznajo številne uporabe CRT v praksi.

Aleksandar Jurišić

Anekdota iz bogate človeške zgodovine. V antičnem jeziku Malayalam je Bhaskara komentiral antični tekst "Aryabhatiyam".

Aryabhata je živel okoli leta 500 v mestu Bihar, ki v tistem času ni bilo neko zakotno mesto pokrito s kravjimi iztrebki, temveč v resnici precej napredna civilizacija. Aryabhata je študiral na Nalanda univerzi (eni najstarejših na svetu) in je med prvimi predlagal splošno metodo za reševanje linearnih Diofantskih enačb.

V S. Balachandra Raovi Indijski matematiki in astronomiji lahko preberete, da so bile take enačbe preučevane v antičnem Vedic tekstu Shulvasutras, starejši deli pa morda segajo celo do 800 let pred našim štetjem. Aryabhataova metoda za reševanje takšnih problemov je imenovana *kuttaka* in jo je predstavil Bhaskara leta 621. Kuttaka pomeni deliti na manjše dele, metoda pa je vsebovala preoblikovanje originalnih faktorjev v manjša števila in je danes standardna metoda za reševanje Diofantskih enačb prvega reda.

Po Aryabhati je Brahmagupta leta 628 obravnaval bolj zapletene Diofantske enačbe. V svojem delu Samasabhavana je npr. predstavil algoritem za reševanje Diofantske enačbe oblike $61x^2 + 1 = y^2$. Te metode niso bile poznane na Zahodu, tako da je reševanje enačbe predlagal leta 1657 francoski matematik Pierre de Fermat. Rešitev pa je našel Euler šele 70 let kasneje. Vendar pa je rešitev te enačbe zabeležil že Bhaskara II leta 1150 z uporabo variante Brahmaguptove metode. Ker njegovo najmanjšo rešitev predstavlja par $(x, y) = (226153980, 1766319049)$, je bil problem očitno precej zahteven.