IZDAJA DRUŠTVO MATEMATIKOV, FIZIKOV IN ASTRONOMOV SLOVENIJE

ISSN 0473-7466

2010
Letnik 57
5

OBZORNIK ZA MATEMATIKO IN FIZIKO

OBZORNIK ZA MATEMATIKO IN FIZIKO

Glasilo Društva matematikov, fizikov in astronomov Slovenije
Ljubljana, SEPTEMBER 2010, letnik 57, številka 5, strani 157–196

Naslov uredništva: DMFA–založništvo, Jadranska ulica 19, p. p. 2964, 1001 Ljubljana **Telefon:** (01) 4766 553, 4232 460 **Telefaks:** (01) 4232 460, 2517 281 **Elektronska pošta:** zaloznistvo@dmfa.si **Internet:** http://www.obzornik.si/ **Transakcijski račun:** 03100–1000018787 **Mednarodna nakazila:** SKB banka d.d., Ajdovščina 4, 1513 Ljubljana **SWIFT (BIC):** SKBASI2X **IBAN:** SI56 0310 0100 0018 787

Natisnila tiskarna COLLEGIUM GRAPHICUM v nakladi 1250 izvodov.

Člani društva prejemajo Obzornik brezplačno. Celoletna članarina znaša 21 EUR, za druge družinske člane in študente pa 10,50 EUR. Naročnina za ustanove je 35 EUR, za tujino 40 EUR. Posamezna številka za člane stane 3,19 EUR, stare številke 1,99 EUR.

DMFA je včlanjeno v Evropsko matematično društvo (EMS), v Mednarodno matematično unijo (IMU), v Evropsko fizikalno društvo (EPS) in v Mednarodno združenje za čisto in uporabno fiziko (IUPAP). DMFA ima pogodbo o recipročnosti z Ameriškim matematičnim društvom (AMS).

Revija izhaja praviloma vsak drugi mesec. Sofinancirata jo Javna agencija za knjigo Republike Slovenije ter Ministrstvo za šolstvo in šport.

Poštnina plačana pri pošti 1102 Ljubljana

NAVODILA SODELAVCEM OBZORNIKA ZA ODDAJO PRISPEVKOV

Revija Obzornik za matematiko in fiziko objavlja izvirne znanstvene in strokovne članke iz matematike, fizike in astronomije, včasih tudi kak prevod. Poleg člankov objavlja prikaze novih knjig s teh področij, poročila o dejavnosti Društva matematikov, fizikov in astronomov Slovenije ter vesti o drugih pomembnih dogodkih v okviru omenjenih znanstvenih ved. Prispevki naj bodo zanimivi in razumljivi širšemu krogu bralcev, diplomantov iz omenjenih strok.

Članek naj vsebuje naslov, ime avtorja (oz. avtorjev), sedež institucije, kjer avtor(ji) dela(jo), izvleček v slovenskem jeziku, naslov in izvleček v angleškem jeziku, klasifikacijo (MSC oziroma PACS) in citirano literaturo. Slike in tabele, ki naj bodo oštevilčene, morajo imeti dovolj izčrpen opis, da jih lahko večinoma razumemo tudi ločeno od besedila. Avtorji člankov, ki želijo objaviti slike iz drugih virov, si morajo za to sami priskrbeti dovoljenje (copyright). Prispevki so lahko oddani v računalniški datoteki PDF ali pa natisnjeni enostransko na belem papirju formata A4. Zaželena velikost črk je 12 pt, razmik med vrsticami pa vsaj 18 pt.

Prispevke pošljite odgovornemu uredniku ali uredniku za matematiko oziroma fiziko na zgoraj napisani naslov uredništva. Vsak članek se praviloma pošlje dvema anonimnima recenzentoma, ki morata predvsem natančno oceniti, kako je obravnavana tema predstavljena, manj pomembna pa je originalnost (in pri matematičnih člankih splošnost) rezultatov. Če je prispevek sprejet v objavo, potem urednik prosi avtorja še za izvorne računalniške datoteke. Le-te naj bodo praviloma napisane v eni od standardnih različic urejevalnikov TEX oziroma LATEX, kar bo olajšalo uredniški postopek.

Avtor se z oddajo članka strinja tudi z njegovo kasnejšo objavo v elektronski obliki na internetu.

ARITMETIKA DVOJIŠKIH KONČNIH OBSEGOV

JERNEJ TONEJC

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Math. Subj. Class. (2010): 11T{06, 22, 55, 71}, 12E{05, 20, 30}, 68R05

V članku predstavimo končne obsege in aritmetiko v končnih obsegih karakteristike 2. Ti imajo pomembno vlogo v implementaciji številnih kriptosistemov in kod za odpravljanje napak. Opišemo učinkovite algoritme za računanje v polinomskih bazah končnih obsegov, ki se pogosto uporabljajo v kriptografskih aplikacijah.

ARITHMETIC OF BINARY FINITE FIELDS

We introduce finite fields and arithmetic in finite fields of characteristic 2 which play an important role in implementation of many cryptosystems and error-correcting codes. We describe efficient arithmetic algorithms in polynomial bases for finite fields which are often used in cryptographic applications.

Uvod

S končnimi obsegi so se ukvarjali ugledni matematiki, kot so Fermat, Euler, Lagrange in Legendre, ki so prispevali k razvoju teorije praštevilskih obsegov $\mathbb{Z}_p$. Splošno teorijo končnih obsegov sta začela graditi Gauss in Galois. Vendar pa se je le-ta uveljavila v uporabni matematiki šele s prihodom računalnikov, kjer ne gre brez diskretnih matematičnih struktur. Spomnimo se, da je obseg najpreprostejša algebraična struktura, v kateri lahko izvajamo vse elementarne aritmetične operacije, tj. seštevamo, odštevamo, množimo in delimo (v resnici množimo z multiplikativnim inverzom). Z razvojem teorije kodiranja, kriptografije in številnih kriptosistemov, ki uporabljajo končne obsege, se je pokazala potreba po izboljšavi algoritmov za aritmetiko nad končnimi obsegi. Pri izvajanju kriptografskih aplikacij se osnovne aritmetične operacije v obsegih izvršijo zelo velikokrat, zato je hitrost ključnega pomena. Seštevanje elementov je običajno hitro, zato pa sta množenje in še posebej računanje inverza časovno zahtevnejši operaciji.

Računalniki skoraj vedno računajo s števili, predstavljenimi v dvojiškem sistemu. Naravno število $k \in [2^n, 2^{n+1})$, kjer je $n \in \mathbb{N}$, lahko zapišemo kot

$$k = 2^n k_n + 2^{n-1} k_{n-1} + \cdots + 2k_1 + k_0\,, \quad \text{kjer je } k_i \in \mathbb{Z}_2 \ \text{ in } \ k_n \neq 0\,. \quad (1)$$

Slika 1. Če bi nam bankomat odvrnil, da po njegovem izračunu morda le ni gotovo, da smo pravi lastnik bančne kartice, bi bili najbrž nejevoljni. Pričakujemo natančen odgovor DA oziroma NE.

V računalniku shranimo le $(n+1)$-terico $k_n k_{n-1} \ldots k_1 k_0$. Če je $\mathbf{s} = s_{n+1} s_n \ldots s_1 s_0$ vsota števil $\mathbf{a} = a_n a_{n-1} \ldots a_1 a_0$ in $\mathbf{b} = b_n b_{n-1} \ldots b_1 b_0$, manjših od 2^{n+1}, potem za $i \in \{0, 1, \ldots, n\}$ velja

$$d_i = a_i + b_i + c_{i-1}\,, \quad s_i = d_i \bmod 2\,, \quad c_i = d_i \operatorname{div} 2 \quad \text{in} \quad s_{n+1} = c_n\,. \tag{2}$$

Z div smo označili celoštevilsko deljenje, c_i pa je seveda prenos pri seštevanju. Pri tem privzamemo $c_{-1} = 0$ in opomnimo, da je število s_{n+1} lahko tudi enako 0.

Tudi polinom $p(x)$ stopnje n s koeficienti iz $\mathbb{Z}_2$ je primeren za hranjenje v računalniškem pomnilniku, saj za

$$p(x) = \sum_{i=0}^{n} p_i x^i, \qquad \text{kjer } p_i \in \mathbb{Z}_2 \ \text{ in } \ p_n \neq 0\,, \tag{3}$$

spet shranimo samo $(n+1)$-terico $p_n p_{n-1} \ldots p_1 p_0$. Če predstavlja $s_n s_{n-1} \ldots s_1 s_0$ vsoto polinomov stopnje kvečjemu n, predstavljenih z $a_n a_{n-1} \ldots a_1 a_0$ in $b_n b_{n-1} \ldots b_1 b_0$, za vsak $i \in \{0, 1, \ldots, n\}$ velja

$$s_i = a_i + b_i \bmod 2\,. \tag{4}$$

Med zapisoma (1) in (3) na prvi pogled ni velike razlike, le število „2“ zamenjamo s spremenljivko „x“. Vendar pa računalniško vezje za seštevanje, ki ga predstavlja enačba (4), sestavlja en sam „ekskluzivni ali“ (XOR), za

izračun izrazov v (2) pa potrebujemo zaradi morebitnega prenosa dvakrat toliko vezja. V namenskih tiskanih vezjih se tako namesto praštevilskih obsegov večinoma uporabljajo razširitve dvojiškega obsega. Drugi razlog za njihovo uporabo izhaja iz vprašanja:

Ali je lahko kvadriranje bistveno hitrejše od množenja?

Naslednja identiteta

$$a \cdot b = \frac{(a+b)^2 - (a-b)^2}{4}$$

nakazuje, da je odgovor najbrž NE. Kajti če bi znali „zelo“ hitro kvadrirati, potem bi kvečjemu dvakrat počasneje lahko izračunali tudi produkt. Ta enačba seveda velja le, če karakteristika obsega ni enaka 2. V razširitvah dvojiških obsegov pa je nekoliko drugače. V tem primeru namreč obstajajo t. i. normalne baze, v katerih je kvadriranje povsem enostavno. Izvedemo ga le s cikličnim zamikom, množenje pa ostane težko (kvadratne zahtevnosti glede na dolžino zapisa). Zato se bomo osredotočili na aritmetiko dvojiških obsegov, na katere bodo vezani tudi vsi naši primeri.

V nadaljevanju najprej predstavimo osnove končnih obsegov, nato pa se posvetimo aritmetiki v razširitvah dvojiškega obsega. Seštevanje je običajno relativno hitra operacija (linearna glede na dolžino zapisa podatkov), kar potem ne velja za množenje. Obstaja pa tudi takšna predstavitev elementov, da je množenje hitro in seštevanje počasno, kot bomo videli v naslednjem razdelku. Nato vpeljemo polinomske baze in opišemo metode množenja, kvadriranja in redukcije v njih. Posebej obravnavamo deljenje, ki ga izvajamo s pomočjo razširjenega Evklidovega algoritma. Opišemo tudi elegantno Berlekampovo izvedbo razširjenega Evklidovega algoritma, ki je še posebej uporabna za računalnike z zelo malo pomnilnika. Na koncu predstavimo vlogo končnih obsegov v kriptografiji, kjer je učinkovita aritmetika pogosto ključnega pomena pri reševanju računsko zahtevnih problemov.

Končni obsegi

Spomnimo se, da je obseg tak kolobar z enoto za množenje, v katerem je vsak neničeln element obrnljiv. Podobseg pa je podmnožica obsega, ki je za isti operaciji tudi obseg. Za vsak končen obseg obstaja tako najmanjše naravno število p, za katero velja $a+a+\cdots+a = p \cdot a = 0$, kjer je a poljuben element danega obsega. Tako število p imenujemo *karakteristika* končnega

obsega in mora biti zaradi minimalnosti praštevilo. Množica ostankov pri deljenju s praštevilom p, skupaj z običajnim seštevanjem in množenjem po modulu p, tvori obseg $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, ki mu pravimo *praobseg* in ga spoznamo že pri študiju deljivosti naravnih števil. Le-ta nima prav nobenega netrivialnega podobsega!

Izrek 1. *Moč poljubnega končnega obsega je enaka p^n, kjer je p neko praštevilo in n neko naravno število.*

Skica dokaza. Naj bo $\mathbb{F}$ poljuben končen obseg in p njegova karakteristika. V tem obsegu enota za množenje generira podobseg, ki je izomorfen praobsegu $\mathbb{Z}_p$. Obseg $\mathbb{F}$ je vektorski prostor nad tem podobsegom $\mathbb{Z}_p$, saj je za seštevanje komutativna grupa, skalarno množenje vektorjev pa je kar običajno množenje v $\mathbb{F}$. Ker je obseg končen, ima kot vektorski prostor tudi končno razsežnost. Označimo jo z n. Število elementov tega obsega je torej enako p^n. ∎

V nadaljevanju bomo videli, kako konstruiramo končni obseg s p^n elementi za poljubno praštevilo p in poljubno naravno število n. Krajši uvod v grupe in končne obsege najdemo v [6], bolj obširen pa v [12]. Končni obsegi so podrobno predstavljeni v [8], s kriptografskega stališča pa v [9] in [10].

Pišimo $q = p^n$. Ker so vsi končni obsegi z enakim številom elementov med seboj izomorfni, bomo obseg s q elementi označili z $\mathrm{GF}(q)$, kjer je GF okrajšava za Galoisov obseg (angl. *Galois field*), in ga obravnavali kot vektorski prostor nad obsegom $\mathbb{Z}_p$. Če so elementi $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ baza prostora $\mathrm{GF}(q)$ nad obsegom $\mathbb{Z}_p$, lahko vsak element obsega $\mathrm{GF}(q)$ zapišemo v obliki vsote

$$\sum_{i=0}^{n-1} a_i \alpha_i, \quad \text{kjer} \quad a_i \in \mathbb{Z}_p \,,$$

ali krajše kot vektor $(a_{n-1}, a_{n-2}, \ldots, a_1, a_0)$.

Množica neničelnih elementov obsega $\mathrm{GF}(q)$ tvori za množenje grupo moči $q-1$, ki jo označimo z $\mathrm{GF}(q)^*$ in imenujemo *multiplikativna grupa* končnega obsega. Lagrangeev izrek nam pove, da red poljubnega elementa končne grupe deli moč te grupe (glej npr. [12, str. 57]), od koder takoj sledi, da vsak element grupe $\mathrm{GF}(q)^*$ reši enačbo

$$x^{q-1} = 1 \,. \tag{5}$$

Izrek 2. *Multiplikativna grupa* $\mathrm{GF}(q)^*$ *končnega obsega* $\mathrm{GF}(q)$ *je ciklična.*

Kot je bralec verjetno že uganil, bo enačba (5) v dokazu izreka imela ključno vlogo. Preden se lotimo dokaza izreka, potrebujemo še dve lemi.

Lema 3. *Označimo s* φ *Eulerjevo funkcijo, tj.* $\varphi(n)$ *je število naravnih števil, manjših od* n*, ki so si tuja z* n*. Potem za vsako naravno število* m *velja*

$$\sum_{d|m} \varphi(d) = m\,. \tag{6}$$

Dokaz. Oglejmo si množice $A(d) = \big\{k \in \{1,\ldots,m\}\colon \mathrm{D}(k,m) = d\big\}$. Očitno velja $A(d) = \emptyset$, če $d \nmid m$ in $A(d_1) \cap A(d_2) = \emptyset$, če $d_1 \neq d_2$. Ker za vsako naravno število $k \leqslant m$ obstaja d, za katerega je $\mathrm{D}(k,m) = d$, velja

$$\{1,\ldots,m\} = \bigcup_{d|m} A(d)\,,$$

kjer vzamemo unijo po vseh deliteljih števila m. Koliko elementov pa ima $A(d)$? Vsak $k \in A(d)$ je večkratnik števila d, torej velja $A(d) \subseteq \big\{d, 2d, \ldots, \frac{m}{d}d\big\}$. Ker velja še

$$\mathrm{D}(\ell d, m) = d \quad\Longleftrightarrow\quad \mathrm{D}\left(\ell d, \frac{m}{d}d\right) = d \quad\Longleftrightarrow\quad \mathrm{D}\left(\ell, \frac{m}{d}\right) = 1\,,$$

je moč množice $A(d)$ natanko $\varphi\left(\frac{m}{d}\right)$. Če upoštevamo, da so množice $A(d)$ med seboj disjunktne, vidimo, da smo dokazali naslednje:

$$\sum_{d|m} \varphi\left(\frac{m}{d}\right) = m\,.$$

Ko d preteče vse delitelje števila m, tudi $\frac{m}{d}$ preteče vse delitelje (v obratnem vrstnem redu), torej lahko zgornjo enakost zapišemo kot

$$\sum_{d|m} \varphi(d) = m\,,$$

kar smo želeli dokazati. ∎

Lema 4. *Naj bo $\mathbb{F}$ poljuben komutativen obseg in m poljubno naravno število. Če ima enačba*

$$x^m = 1 \tag{7}$$

v $\mathbb{F}$ natanko m rešitev, potem obstaja taka rešitev $g \in \mathbb{F}$, da velja $g^k \neq 1$ za vsa naravna števila $k < m$.

Dokaz. Preprosto je videti, da je množica vseh rešitev te enačbe v $\mathbb{F}$ grupa za množenje, saj je po predpostavki $\mathbb{F}$ komutativen. Naj bo $a \in \mathbb{F}$ poljubna rešitev enačbe (7). Potem obstaja najmanjše naravno število $d \leqslant m$, da velja $a^d = 1$, imenujmo ga *minimalna stopnja* elementa a. Očitno d deli m, sicer pridemo v protislovje z minimalnostjo. Elementi $a^0, a^1, a^2, \ldots, a^{d-1}$ so zaradi minimalnosti d med seboj različni, rešijo enačbo (7), hkrati pa zadoščajo enačbi $x^d = 1$, saj za $k \in \mathbb{Z}$ velja

$$(a^k)^m = a^{km} = (a^m)^k = 1^k = 1\,, \qquad (a^k)^d = a^{kd} = (a^d)^k = 1^k = 1\,.$$

Ker ima enačba $x^d = 1$ kvečjemu d rešitev, so to natanko vse možne rešitve. Torej je poljuben element z minimalno stopnjo d v množici $\{a, a^2, \ldots, a^{d-1}\}$. Zanimajo nas torej tisti elementi a^k, $1 \leqslant k \leqslant d-1$, katerih minimalna stopnja je prav tako d. To se zgodi takrat, ko je k tuj proti d. Takih je natanko $\varphi(d)$.

Za vsako rešitev enačbe (7) obstaja neki delitelj števila m, ki je minimalna stopnja te rešitve. Za poljubna različna delitelja d_1, d_2 števila m sta množici rešitev z minimalnima stopnjama d_1 in d_2 disjunktni. Pravkar smo videli, da imamo natanko $\varphi(d)$ rešitev z minimalno stopnjo d, kakor hitro imamo vsaj eno. Torej imamo natanko

$$\sum \varphi(d) \tag{8}$$

rešitev, kjer seštevamo po vseh tistih deliteljih števila m, za katere obstaja vsaj ena rešitev z minimalno stopnjo d. Primerjajmo ta izraz z lemo 3. Ker smo predpostavili, da ima enačba (7) m rešitev, hkrati pa velja (6), moramo v vsoti (8) seštevati po vseh deliteljih števila m. Torej je v njej tudi člen $\varphi(m)$, kar pomeni, da obstaja vsaj en element $g \in \mathbb{F}$, ki reši enačbo (7), katerega minimalna stopnja je m, kar je ravno to, kar smo želeli dokazati.∎

Element g iz leme imenujemo *primitivni m-ti koren enote* v obsegu $\mathbb{F}$. Sedaj imamo vse, kar potrebujemo za dokaz izreka.

Dokaz izreka 2. Wedderburnov izrek [12, str. 288] nam pove, da je vsak končen obseg komutativen, torej lahko za $\mathrm{GF}(q)$ uporabimo rezultat, ki smo ga pravkar dokazali. Videli smo, da ima enačba (5) natanko $q-1$ rešitev v $\mathrm{GF}(q)$, zato v $\mathrm{GF}(q)$ obstaja primitivni $(q-1)$-vi koren enote. To pa je ravno generator $\mathrm{GF}(q)^*$, torej je multiplikativna grupa končnega obsega res ciklična. ∎

Obseg $\mathrm{GF}(q)$ torej sestavljajo elementi $0, z, z^2, \ldots, z^{q-1}$, kjer je z primitivni $(q-1)$-vi koren enote. Pri takem načinu predstavitve elementov obsega je množenje hitro, saj v pomnilnik namesto elementa z^k zapišemo le eksponent k. Ker velja $z^{k_1} \cdot z^{k_2} = z^{k_1+k_2}$, produkta ni težko izračunati. Vendar v tej predstavitvi ne znamo hitro in enostavno izračunati vsote. Za $k_1 \leqslant k_2$ je $z^{k_1} + z^{k_2} = z^{k_1}(1 + z^{k_2-k_1})$, zato zadošča, da za vsak $k \in \mathbb{Z}_q$ poznamo eksponent $\ell \in \mathbb{Z}_q$, za katerega velja $z^\ell = z^k + 1$. Tabela vseh takih parov je poznana pod imenom ZechLog tabela. Medtem ko za majhne q taka tabela poenostavi računanje, pa za velike končne obsege izračun vseh parov (k, ℓ) ni enostaven, njihovo hranjene pa zavzame tudi veliko računalniškega pomnilnika. Za primer navedimo, da bi že za $\mathrm{GF}(2^{40})$ bila potrebna količina pomnilnika za hranjenje tabele kar 5 terabajtov, medtem ko se v praksi uporabljajo končni obsegi velikosti vsaj 2^{160}.

Najbolj znana konstrukcija razširitev končnih obsegov sloni na nerazcepnih polinomih. Iskanje nerazcepnega polinoma stopnje m iz kolobarja $\mathrm{GF}(q)[x]$ v splošnem ni tako enostavno, saj ne obstaja dokazano deterministično algoritem s polinomsko časovno zahtevnostjo (tj. število operacij v $\mathrm{GF}(q)$, ki jih algoritem opravi, je omejeno z nekim polinomom v m in n, kjer je $q = p^n$). Trenutno znani dokazi namreč temeljijo na veljavnosti posplošene Riemannove hipoteze. Da problem kljub vsemu ni brezupen, nas prepriča dejstvo, da obstajajo precej učinkoviti verjetnostni algoritmi. Konkretne konstrukcije nerazcepnih polinomov lahko bralec najde v [10, pogl. 3].

Izrek 5. *Naj bo $m \in \mathbb{N}$ in $\mathrm{GF}(q^m)$ končen obseg, ki vsebuje podobseg $\mathrm{GF}(q)$. Potem v kolobarju polinomov $\mathrm{GF}(q)[x]$ obstaja nerazcepen polinom $f(x)$ sto-*

pnje m, za katerega je

$$\mathrm{GF}(q^m) \cong \mathrm{GF}(q)[x]/(f(x))\,,$$

kjer je $\mathrm{GF}(q)[x]/(f(x))$ *obseg polinomov nad* $\mathrm{GF}(q)$*, reduciranih po modulu polinoma* $f(x)$*. Velja še* $\mathrm{GF}(q^m) \cong \mathrm{GF}(q)(\alpha)$*, kjer je* α *ničla polinoma* $f(x)$*.*

Skica dokaza. Ker je $f(x)$ nerazcepen, je $\mathrm{GF}(q)[x]/(f(x))$ obseg z natanko q^m elementi. Že prej smo videli, da vsak neničeln element $a \in \mathrm{GF}(q^m)$ reši enačbo $x^{q^m-1} = 1$. Če to enačbo pomnožimo z x, potem je njena rešitev tudi 0, od koder takoj sledi, da je vsak obseg s q^m elementi razpadni obseg polinoma $x^{q^m} - x$. Ker so vsi razpadni obsegi istega polinoma med seboj izomorfni, velja $\mathrm{GF}(q)[x]/(f(x)) \cong \mathrm{GF}(q^m)$. Dokazati moramo torej obstoj nerazcepnega polinoma $f(x) \in \mathrm{GF}(q)[x]$ stopnje m. Označimo z N_q število nerazcepnih polinomov v $\mathrm{GF}(q)[x]$ stopnje m z vodilnim koeficientom 1, ki delijo $x^{q^m} - x$. Velja ocena

$$\frac{1}{2m} \leqslant \frac{N_q}{q^m} \leqslant \frac{1}{m}\,,$$

od koder sledi, da nerazcepen polinom $f(x) \in \mathrm{GF}(q)[x]$ stopnje m mora obstajati. Za dokaz zadnje trditve v izreku si oglejmo naravno projekcijo

$$\pi\colon \mathrm{GF}(q)[x] \to \mathrm{GF}(q)[x]/(f(x))\,, \qquad \pi\colon g(x) \mapsto g(x) \bmod f(x)\,.$$

Enostavno je videti, da je $\pi(x)$ ničla polinoma $f(x)$, od koder trditev takoj sledi. ∎

Elementi obsega $\mathrm{GF}(q^m)$ tako ustrezajo polinomom nad $\mathrm{GF}(q)$ stopnje manj kot m. Seštevanje polinomov iz kolobarja $\mathrm{GF}(q)[x]$ stopnje manj kot m se enostavno prevede v kvečjemu m seštevanj elementov obsega $\mathrm{GF}(q)$, kot smo videli že v uvodu. Pri množenju pa ne gre tako zlahka, saj lahko stopnja produkta dveh polinomov doseže oz. preseže stopnjo nerazcepnega polinoma $f(x)$ in je zato potrebna redukcija po modulu polinoma $f(x)$.

Primer 1. Konstruirajmo obseg $\mathrm{GF}(2^3)$. Najprej moramo najti nerazcepen polinom stopnje 3 nad $\mathbb{Z}_2$. Najbolj preprosto bi bilo poskusiti kar z binomom. Vendar pa za polinom $f(x)$ s sodo mnogo neničelnimi členi nad $\mathbb{Z}_2$ velja $f(1) = 0$, kar pomeni, da je $f(x)$ razcepen. Zato mora imeti nerazcepen polinom iz kolobarja $\mathbb{Z}_2[x]$ liho število neničelnih členov. Njegov

konstantni člen je neničeln, sicer bi bil polinom deljiv z x. Tako sta edina kandidata $f_1(x) = x^3 + x + 1$ in $f_2(x) = x^3 + x^2 + 1$. Oba sta nerazcepna nad $\mathbb{Z}_2$, saj 0 in 1 nista ničli nobenega izmed njiju. Naj bo μ ničla polinoma $f_1(x)$. Potem je $\mu^3 = \mu + 1$ in elementi obsega $\mathrm{GF}(2^3)$ so

$$0\,,\mu\,,\mu^2\,,\mu^3 = \mu + 1\,,\mu^4 = \mu^2 + \mu\,,\mu^5 = \mu^2 + \mu + 1\,,\mu^6 = \mu^2 + 1\,,\mu^7 = 1\,.$$

Za ničlo ν polinoma $f_2(x)$ pa velja $\nu^3 = \nu^2 + 1$ in dobimo naslednjo upodobitev:

$$0\,,\nu\,,\nu^2\,,\nu^3 = \nu^2 + 1\,,\nu^4 = \nu^2 + \nu + 1\,,\nu^5 = \nu + 1\,,\nu^6 = \nu^2 + \nu\,,\nu^7 = 1\,.$$

V obeh primerih lahko to zapišemo kot trojice $a_2a_1a_0$, kjer $a_i \in \mathbb{Z}_2$ ustreza koeficientu pri μ^i oz. ν^i na desni strani enačaja. V primeru ν tako dobimo

$$000, 010, 100, 101, 111, 011, 110, 001\,. \quad \diamond$$

Polinomske baze

Naj bo $f(x)$ nerazcepen polinom stopnje m iz kolobarja $\mathrm{GF}(q)[x]$ in naj bo α njegova ničla. *Minimalni polinom* elementa α je tak polinom $r(x)$, za katerega velja $r(\alpha) = 0$, ima vodilni koeficient enak 1 in ima med vsemi polinomi s pravkar omenjenima lastnostma najmanjšo stopnjo. Vsak polinom $g(x) \in \mathrm{GF}(q)[x]$, ki ima element α za ničlo, je zato deljiv z minimalnim polinomom $r(x)$ elementa α. Ker pa je polinom $f(x)$ nerazcepen, mora biti kar enak skalarnemu večkratniku minimalnega polinoma $r(x)$. Zato element α ni ničla nobenega neničelnega polinoma iz kolobarja $\mathrm{GF}(q)[x]$ stopnje manjše od m. Sledi, da morajo biti elementi $1, \alpha, \ldots, \alpha^{m-1}$ linearno neodvisni nad $\mathrm{GF}(q)$ in zato sestavljajo bazo. Imenujemo jo *polinomska baza* vektorskega prostora $\mathrm{GF}(q^m)$ nad obsegom $\mathrm{GF}(q)$. Torej vsaka ničla nerazcepnega polinoma stopnje m iz kolobarja $\mathrm{GF}(q)[x]$ določa polinomsko bazo v $\mathrm{GF}(q^m)$. Pri zapisu elementov končnega obsega $\mathrm{GF}(2^m)$ v polinomski bazi pogosto namesto ničle α polinoma $f(x)$ pišemo kar x. Za različne nerazcepne polinome dobimo različne baze istega vektorskega prostora.

Primer 2. Že v prejšnjem primeru smo se prepričali, da je polinom $f(x) = x^3 + x^2 + 1$ nerazcepen nad $\mathbb{Z}_2$. Torej je $\mathrm{GF}(2^3) \cong \mathbb{Z}_2[x]/(f(x)) \cong \mathbb{Z}_2(\nu)$, kjer

je ν ničla polinoma $f(x)$, množica $\{\nu^2, \nu, 1\}$ pa je polinomska baza obsega $\mathrm{GF}(2^3)$. Vsak element zapišemo kot $a_2\nu^2+a_1\nu+a_0$, kar tako kot v prejšnjem primeru okrajšamo v trojico $a_2a_1a_0$. Tabela 1 prikazuje produkte elementov v $\mathrm{GF}(2^3)$.

·	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	101	111	001	011
011	000	011	110	101	001	010	111	100
100	000	100	101	001	111	011	010	110
101	000	101	111	010	011	110	100	001
110	000	110	001	111	010	100	011	101
111	000	111	011	100	110	001	101	010

Tabela 1. Množenje v obsegu $\mathrm{GF}(2^3)$.

Za zgled zmnožimo npr. elementa $\nu + 1$ in $\nu^2 + \nu$:

$$(\nu + 1)(\nu^2 + \nu) = \nu^3 + \nu^2 + \nu^2 + \nu = \nu^3 + \nu = (\nu^2 + 1) + \nu = \nu^2 + \nu + 1\,.\diamond$$

Preprosta metoda množenja elementov obsega $\mathrm{GF}(2^m)$, predstavljenih v polinomski bazi $\{x^{m-1}, x^{m-2}, \ldots, x, 1\}$ z nerazcepnim polinomom $f(x)$ stopnje m, temelji na zvezi

$$a(x) \cdot b(x) = a_0\, b(x) + a_1\, xb(x) + \cdots + a_{m-1}\, x^{m-1}b(x)\,.$$

Po vrsti rekurzivno računamo $x^i b(x) \pmod{f(x)}$ za $i \in \{1, 2, \ldots, m - 1\}$ in prištevamo tiste člene, pri katerih je a_i enak 1. Produkt $x \cdot b(x) \pmod{f(x)}$ izračunamo z zamikom koordinat vektorja $b(x)$. Spravimo ga kar v $b(x)$ ter mu na vsakem koraku prištejemo polinom $f(x)$, če je pred zamikom b_{m-1} enak 1. Tak pristop se dobro obnese v strojni opremi, kjer delamo na bitnem nivoju in lahko izvedemo zamik vektorja v enem ciklu. V programski implementaciji pa elemente običajno shranjujemo kot vektorje w-bitnih besed $A = (A[t - 1], \ldots, A[1], A[0])$, kjer je $t = \lceil m/w \rceil$, zato pri takem pristopu potrebujemo $m - 1$ zamikov besed. Množenje lahko izvedemo hitreje, če najprej zmnožimo elemente brez sprotnega reduciranja (kot običajno množimo polinome) in na koncu napravimo redukcijo

po modulu nerazcepnega polinoma $f(x)$. Pri tem izračunanemu $x^k b(x)$ za $k \in \{0, 1, \ldots, w-1\}$ dodamo na konec j ničelnih besed in dobimo element $x^{wj+k} b(x)$. Tako za množenje porabimo samo $w-1$ vektorskih zamikov (množenj z x). Podrobnejši opis algoritma za množenje in njegovih izboljšav je v [4, pogl. 2].

Posebej omenimo kvadriranje polinomov v obsegih karakteristike 2, ki je mnogo hitrejše od množenja dveh različnih polinomov. Kvadriranje dvojiških polinomov je linearna operacija, kvadrat polinoma $a(x) = \sum_{i=0}^{m-1} a_i x^i$ je namreč kar $a(x)^2 = \sum_{i=0}^{m-1} a_i x^{2i}$. Kvadrat elementa dobimo z vstavitvijo ničelnih bitov med bite elementa $a(x)$:

$$(a_{m-1}, a_{m-2}, \ldots, a_1, a_0) \longmapsto (a_{m-1}, 0, a_{m-2}, 0, \ldots, 0, a_1, 0, a_0)\,.$$

Računanje v polinomskih bazah je bolj učinkovito, če je nerazcepni polinom $f(x)$ iz izreka 5 enostavnejši. V praksi izberemo take $f(x)$, ki imajo malo neničelnih koeficientov, saj to poenostavi modularno redukcijo s polinomom $f(x)$. Polinome s tremi neničelnimi členi imenujemo *trinomi*. Le-ti omogočajo hitrejšo implementacijo aritmetike končnih obsegov. V tabeli 2 so našteti nerazcepni trinomi nad obsegom $\mathbb{Z}_2$ stopnje $m \in (150, 500)$, ki se pogosto uporabljajo v kriptosistemih z eliptičnimi krivuljami. V tabeli je zapisano število m, za katero nerazcepen trinom obstaja, ter najmanjše število k, za katero je polinom $x^m + x^k + 1$ nerazcepen nad $\mathbb{Z}_2$.

Tako pri množenju kot tudi pri kvadriranju polinomov lahko stopnja produkta $c(x)$ doseže ali preseže stopnjo m izbranega nerazcepnega polinoma $f(x)$. Stopnja produkta je lahko največ $2m-2$, zmanjšamo pa jo z redukcijo po modulu nerazcepnega polinoma $f(x)$. Vzemimo vektor w-bitnih besed $C = (C[n], C[n-1], \ldots, C[1], C[0])$ in opišimo algoritem, ki temelji na dejstvu, da za $i \geq m$ velja $x^i = x^{i-m} f_1(x) \pmod{f(x)}$, kjer je $f_1(x) = f(x) - x^m$.

Če je $f(x)$ trinom, potem je $x^m = x^k + 1$ in je redukcija učinkovitejša, saj moramo pri reduciranju člena x^i za $i \geq m$ popraviti vektor C le na dveh mestih: pri $x^{i-(m-k)}$ in x^{i-m}. Ob redukciji naslednjega člena x^{i-1} popravljamo sosednje bite prej omenjenih mest. Zato lahko redukcijo izvajamo nad besedami namesto nad biti in s tem pohitrimo algoritem.

m	k	m	k	m	k	m	k	m	k	m	k	m	k
151	3	153	1	154	15	155	62	156	9	159	31	161	18
162	27	166	37	167	6	169	34	170	11	172	1	174	13
175	6	177	8	178	31	180	3	182	81	183	56	185	24
186	11	191	9	193	15	196	3	198	9	199	34	201	14
202	55	204	27	207	43	209	6	210	7	212	105	214	73
215	23	217	45	218	11	220	7	223	33	225	32	228	113
231	26	233	74	234	31	236	5	238	73	239	36	241	70
242	95	244	111	247	82	249	35	250	103	252	15	253	46
255	52	257	12	258	71	260	15	263	93	265	42	266	47
268	25	270	53	271	58	273	23	274	67	276	63	278	5
279	5	281	93	282	35	284	53	286	69	287	71	289	21
292	37	294	33	295	48	297	5	300	5	302	41	303	1
305	102	308	15	310	93	313	79	314	15	316	63	318	45
319	36	321	31	322	67	324	51	327	34	329	50	330	99
332	89	333	2	337	55	340	45	342	125	343	75	345	22
346	63	348	103	350	53	351	34	353	69	354	99	358	57
359	68	362	63	364	9	366	29	367	21	369	91	370	139
372	111	375	16	377	41	378	43	380	47	382	81	383	90
385	6	386	83	388	159	390	9	391	28	393	7	394	135
396	25	399	26	401	152	402	171	404	65	406	141	407	71
409	87	412	147	414	13	415	102	417	107	418	199	420	7
422	149	423	25	425	12	426	63	428	105	431	120	433	33
436	165	438	65	439	49	441	7	444	81	446	105	447	73
449	134	450	47	455	38	457	16	458	203	460	19	462	73
463	93	465	31	468	27	470	9	471	1	473	200	474	191
476	9	478	121	479	104	481	138	484	105	486	81	487	94
489	83	490	219	492	7	494	17	495	76	497	78	498	155

Tabela 2. Nerazcepni trinomi nad $\mathbb{Z}_2$. Do te tabele lahko pridemo na požrešen način (podobno kot npr. pri Eratostenovem rešetu) tako, da najprej zmnožimo vse nerazcepne linearne polinome, tj. x in $x+1$. Njihovi produkti x^2, x^2+x, x^2+1 očitno ne „pokrijejo“ vseh (štirih) polinomov stopnje 2. Zato je polinom x^2+x+1 nerazcepen. Sedaj množimo x in $x+1$ s polinomi stopnje 2 in ugotovimo, da pri stopnji 3 tudi ne „pokrijemo“ vseh polinomov. Z nadaljevanjem tega postopka lahko poiščemo vse nerazcepne polinome želene stopnje. Kadar za neki m ne obstaja nerazcepen trinom, iščemo nerazcepen pentanom ali heptanom. Za vse $m \leqslant 10\,000$ obstaja vsaj nerazcepen pentanom, kolikor ni že nerazcepnega trinoma stopnje m, glej [11].

Invertiranje in razširjeni Evklidov algoritem

Za invertiranje elementov obsega $\mathrm{GF}(2^m)$ lahko uporabimo razširjeni Evklidov algoritem [1, razdelek 2.1], ki ga bomo podrobneje opisali v nadaljevanju.

Slika 2. Evklid

Morda je sicer na prvi pogled bolj naravna metoda potenciranja, saj za vsak $\alpha \in \mathrm{GF}(2^m)$ velja $\alpha^{2^m} = \alpha$, od koder za $\alpha \neq 0$ sledi $\alpha^{-1} = \alpha^{2^m-2}$. Tak pristop se dobro obnese v teoriji, vendar pa se razširjeni Evklidov algoritem v praksi izkaže za dosti hitrejšega. Za $m = 173$ pri računanju inverza s potenciranjem porabimo 10 množenj, medtem ko lahko z razširjenim Evklidovim algoritmom inverzni element dobimo s 3–4 množenji.

Za dani polinom $a(x) \in \mathbb{Z}_2[x]$ stopnje manj od m iščemo tak polinom $p(x) \in \mathbb{Z}_2[x]$ stopnje manj od m, da velja $a(x)p(x) \equiv 1 \pmod{f(x)}$. To pomeni, da obstaja tak polinom $q(x)$, da v kolobarju polinomov $\mathbb{Z}_2[x]$ velja

$$a(x)\,p(x) + q(x)\,f(x) = 1\,. \tag{9}$$

Ker je polinom $f(x)$ nerazcepen, je največji skupni delitelj polinomov $f(x)$ in $a(x)$ enak 1. V splošnem je enačbo (9) težko rešiti, zato si pomagamo z enostavnejšimi primeri. Poznamo namreč rešitev enačbe (9), kadar na desni strani stoji bodisi $f(x)$ ali $a(x)$. V prvem primeru je rešitev kar $p(x) = 0$ in $q(x) = 1$. V drugem primeru, ko je na desni $a(x)$, pa enačbo reši par $p(x) = 1$ in $q(x) = 0$. Zdaj lahko z iterativno metodo poiščemo zaporedji polinomov p_i in q_i, za kateri velja $ap_i + fq_i = r_i$. Upoštevamo omenjena posebna primera in začnemo z $r_{-2} = f$, $r_{-1} = a$, $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$ in $q_{-1} = 0$. Na vsakem koraku iščemo taka polinoma s_i in r_i, da velja

$$r_{i-2} = s_i r_{i-1} + r_i\,,$$

pri čemer je stopnja polinoma r_i manjša od stopnje polinoma r_{i-1}. Postavimo še

$$q_i = s_i q_{i-1} + q_{i-2} \quad \text{in} \quad p_i = s_i p_{i-1} + p_{i-2}$$

ter ponavljamo postopek, dokler na nekem koraku ne dobimo $r_k = 0$. Iskana rešitev je potem $q(x) = q_{k-1}$ in $p(x) = p_{k-1}$, kjer je stopnja q manjša od stopnje a, stopnja p pa manjša od stopnje f. Potrebujemo le polinom $p(x)$, zato zaporedja q_i sploh ne računamo. Za lažjo predstavo si oglejmo primer.

Primer 3. Naj bo $a(x) = x^4+x+1$ in $f(x) = x^5+x^2+1$. Poiščimo inverz polinoma $a(x)$.

$$\begin{aligned} r_{-2} = x^5+x^2+1 &= x(x^4+x+1)+x+1 \\ r_{-1} = x^4+x+1 &= (x^3+x^2+x)\cdot(x+1)+1 \\ r_0 = x+1 &= (x+1)\cdot 1+0 \end{aligned}$$

$$\begin{aligned} x\cdot 1+0 &= x = p_0(x) \\ (x^3+x^2+x)\cdot x+1 &= x^4+x^3+x^2+1 = p_1(x) \\ (x+1)\cdot(x^4+x^3+x^2+1)+x &= x^5+x^2+1 = p_2(x)\,. \end{aligned}$$

V zadnji vrstici postane ostanek r_2 enak 0, zato je inverz polinoma $a(x)$ enak $p_1(x)$. Podrobneje si oglejmo ta postopek z vidika računalnikov. Računalnik polinome deli postopoma, tako da množi polinom nižje stopnje z ustrezno potenco elementa x. To pomeni, da izvaja ciklični zamik, vse dokler nimata oba polinoma enake stopnje. Nato zamenja polinom, ki je na začetku višje stopnje, z njuno razliko. Postopek ponavlja, vse dokler se stopnja tistega polinoma, ki ima višjo ali enako stopnjo, ne zmanjša pod stopnjo drugega polinoma. Tako se po delih izračuna vsak polinom s_i. Oglejmo si pravkar opisani postopek na našem primeru. Za $i = 0$ se v prvem koraku r_{-1} najprej pomnoži z elementom x. Razlika med r_{-2} in $x \cdot r_{-1}$ je linearni polinom $r_0 = x+1$ in takoj se lahko izračuna $p_0 = s_0 \cdot p_{-1}+p_{-2} = x\cdot 1+0 = x$. Nato se za $i = 1$ (pri deljenju polinoma r_{-1} z r_0) ostanek iz prejšnjega koraka r_0 najprej množi z ustrezno potenco elementa x, kar predstavlja prvi sumand v s_1, recimo mu s_{11}:

$$r_{-1} = x^4 + x + 1 = x^3 \cdot (x + 1) + x^3 + x + 1\,.$$

Razlika med r_{-1} in $x^3 \cdot r_0$ je polinom $x^3 + x + 1$, ki je višje stopnje od r_0. Zato se polinoma zamenja in postopek se ponovi. Pri tem se spet množi

z ustrezno potenco elementa x, ki zdaj predstavlja drugi del polinoma s_1, tj. s_{12}:

$$x^3 + x + 1 = x^2 \cdot (x + 1) + x^2 + x + 1\,.$$

Ker je razlika med $x^3 + x + 1$ in $x^2 \cdot r_0$ še vedno višje stopnje od r_0, se ju spet zamenja in množi r_0 z elementom x, kar ustreza tretjemu sumandu polinoma s_1, tj. s_{13}:

$$x^2 + x + 1 = x \cdot (x + 1) + 1\,.$$

Sedaj je ostanek enak 1 in je nižje stopnje od linearnega polinoma r_0. Tako se po delih izračuna $s_1 = s_{11} + s_{12} + s_{13}$. Ob tem se vzporedno računa polinom $p_1 = s_1 p_0 + p_{-1}$ kot

$$((s_{11}p_0 + p_{-1}) + s_{12}p_0) + s_{13}p_0 = ((x^3 \cdot x + 1) + x^2 \cdot x) + x \cdot x = x^4 + x^3 + x^2 + 1\,.$$

Podobno v tretjem koraku ($i = 2$) iz $r_0 = x + 1 = (x + 1) \cdot 1 + 0$ sledi, da je $s_2 = x + 1$, $r_1 = 1$ in $r_2 = 0$. Potem pa polinoma p_2 sploh ni treba računati, saj je inverz elementa a enak polinomu p_1. $\diamond$

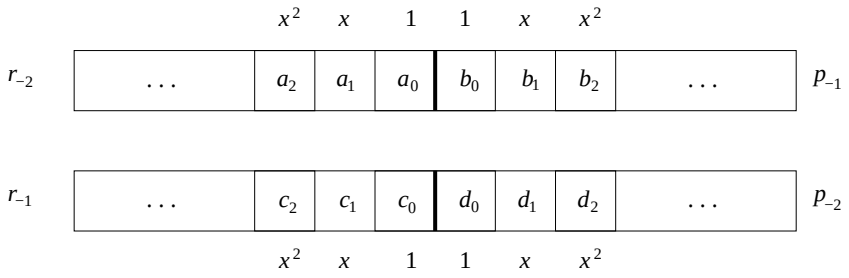
Berlekampov algoritem

Predstavimo Berlekampovo realizacijo razširjenega Evklidovega algoritma [1, razdelek 2.3], ki je posebej prilagojena za računalnike z zelo malo pomnilnika, kot so na primer pametne kartice. Potrebujemo namreč le dva

Slika 3. Elwyn Ralph Berlekamp

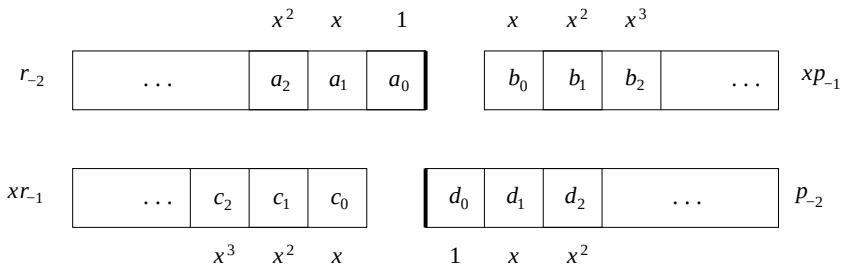
registra z $m+2$ biti, kjer je m stopnja nerazcepnega polinoma, opravimo pa najmanjše možno število logičnih operacij. Ideja je v zamikanju parov polinomov.

Koeficiente polinomov r in p postavimo skupaj tako, da najbolj levi bit predstavlja vodilni koeficient polinoma r, najbolj desni bit pa vodilni koeficient polinoma p. Na začetku so v zgornjem registru koeficienti polinoma r_{-2}, katerim sledi enica, ki predstavlja p_{-1}. V spodnji register pa na začetek zložimo koeficiente polinoma r_{-1}, katerim sledi p_{-2}. Takšen zapis je najprimernejši, saj polinomom r_i stopnja pada, polinomom p_i pa se veča. Začetno stanje prikazuje slika 4.



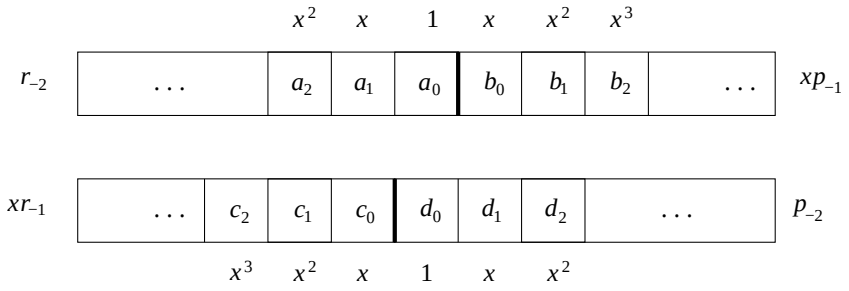
Slika 4. Začetno stanje registrov.

Če množimo polinom r_{-1} z elementom x, zaradi povezave med enačbama $r_{-2} = s_0 r_{-1} + r_0$ in $p_0 = s_0 p_{-1} + p_{-2}$ hkrati množimo tudi p_{-1} z elementom x. Pri tem se levi del spodnjega registra, v katerem so zapisani koeficienti polinoma r_{-1}, zamakne za eno mesto v levo. Desni del zgornjega registra pa se zaradi množenja p_{-1} z x zamakne za eno mesto v desno. Zamika sta prikazana na sliki 5.



Slika 5. Zamik registrov pri množenju z x.

Ta dva zamika pa sta ekvivalentna temu, da le zgornji register zamaknemo za eno mesto v desno, kot prikazuje slika 6. Potem seveda ne moremo med seboj primerjati bitov, ki ležijo med obema odebeljenima črtama. Lahko pa primerjamo tiste, ki ležijo na levi strani bolj leve odebeljene črte, saj le-ti ustrezajo enakim potencam elementa x. Podobno lahko med seboj primerjamo bite, ki ležijo na desni strani bolj desne odebeljene črte in ustrezajo naraščajočim potencam elementa x.



Slika 6. Kompaktna oblika registrov.

Algoritem je sestavljen le iz zamikov in seštevanj. Skupno število zamikov (Z) je $2m + 1$. Ker vsakemu seštevanju (S) sledi zamik, ne more biti več kot $2m$ seštevanj in celoten algoritem ne zahteva več kot $4m + 1$ operacij. Oglejmo si postopek na primeru iz prejšnjega razdelka. Z rimskimi številkami so označene skupine operacij, ki ustrezajo posameznim vrsticam v primeru, vejica pa ima enako vlogo kot odebeljena črta na slikah.

Primer 4.

$$\textbf{I.} \quad \begin{pmatrix} 1\,0\,0\,1\,0\,1, & 1 \\ 0\,1\,0\,0\,1\,1, & 0 \end{pmatrix} = \begin{pmatrix} r_{-2}, & p_{-1} \\ r_{-1}, & p_{-2} \end{pmatrix} = \begin{pmatrix} f(x), 1 \\ a(x), 0 \end{pmatrix}$$

$$\text{Z}: \quad \begin{pmatrix} 1\,0\,0\,1\,0\,1, & 1 \\ 1\,0\,0\,1\,1, & 0\,0 \end{pmatrix} = \begin{pmatrix} r_{-2}, & xp_{-1} \\ xr_{-1}, & p_{-2} \end{pmatrix}$$

$$\text{S}: \quad \begin{pmatrix} 0\,0\,0\,0\,1\,1, & 1 \\ 1\,0\,0\,1\,1, & 0\,1 \end{pmatrix} = \begin{pmatrix} r_{-2} + xr_{-1}, & xp_{-1} \\ xr_{-1}, & p_{-2} + xp_{-1} \end{pmatrix}$$

$$\textbf{II}.\ \ \mathrm{Z}: \quad \begin{pmatrix} 0\,0\,0\,1\,1,\ 1\,0 \\ 1\,0\,0\,1\,1,\ 0\,1 \end{pmatrix} = \begin{pmatrix} r_0,\ p_{-1} \\ r_{-1},\ p_0 \end{pmatrix}$$

$$3\times\mathrm{Z}: \begin{pmatrix} 1\,1,\ 1\,0\,0\,0\,0 \\ 1\,0\,0\,1\,1,\ 0\,1 \end{pmatrix} = \begin{pmatrix} x^3r_0,\ p_{-1} \\ r_{-1},\ x^3p_0 \end{pmatrix}$$

$$\mathrm{S}: \quad \begin{pmatrix} 1\,1,\ 1\,0\,0\,0\,1 \\ 0\,1\,0\,1\,1,\ 0\,1 \end{pmatrix} = \begin{pmatrix} x^3r_0,\ p_{-1}+x^3p_0 \\ r_{-1}+x^3r_0,\ x^3p_0 \end{pmatrix}$$

$$\mathrm{Z}: \quad \begin{pmatrix} 1\,1,\ 1\,0\,0\,0\,1 \\ 1\,0\,1\,1,\ 0\,1\,0 \end{pmatrix} = \begin{pmatrix} x^2r_0,\ p_{-1}+x^3p_0 \\ r_{-1}+x^3r_0,\ x^2p_0 \end{pmatrix}$$

$$\mathrm{S}: \quad \begin{pmatrix} 1\,1,\ 1\,0\,0\,1\,1 \\ 0\,1\,1,\ 0\,1\,0 \end{pmatrix} = \begin{pmatrix} x^2r_0,\ p_{-1}+(x^3+x^2)p_0 \\ r_{-1}+(x^3+x^2)r_0,\ x^2p_0 \end{pmatrix}$$

$$\mathrm{Z}: \quad \begin{pmatrix} 1\,1,\ 1\,0\,0\,1\,1 \\ 1\,1,\ 0\,1\,0\,0 \end{pmatrix} = \begin{pmatrix} xr_0,\ p_{-1}+(x^3+x^2)p_0 \\ r_{-1}+(x^3+x^2)r_0,\ xp_0 \end{pmatrix}$$

$$\mathrm{S}: \quad \begin{pmatrix} 1\,1,\ 1\,0\,1\,1\,1 \\ 0\,0\,1,\ 0\,1\,0\,0 \end{pmatrix} = \begin{pmatrix} xr_0,\ p_{-1}+(x^3+x^2+x)p_0 \\ r_{-1}+(x^3+x^2+x)r_0,\ xp_0 \end{pmatrix}$$

$$\textbf{III}.\ \ \mathrm{Z}: \quad \begin{pmatrix} 1\,1,\ 1\,0\,1\,1\,1 \\ 0\,1,\ 0\,1\,0\,0\,0 \end{pmatrix} = \begin{pmatrix} r_0,\ p_1 \\ r_1,\ p_0 \end{pmatrix}$$

$$\mathrm{Z}: \quad \begin{pmatrix} 1\,1,\ 1\,0\,1\,1\,1 \\ 1,\ 0\,1\,0\,0\,0\,0 \end{pmatrix} = \begin{pmatrix} r_0,\ xp_1 \\ xr_1,\ p_0 \end{pmatrix}$$

◇

Končni obsegi v kriptografiji

Področje končnih obsegov je polno raziskovalnih problemov, tako teoretičnih, kakor tudi tistih, ki so povezani z njihovo uporabo. Mnogo slednjih izvira iz kriptografije in teorije kodiranja, kjer je aritmetika končnih obsegov velikokrat bistvenega pomena. V algoritmih pogosto uporabljamo razširitve dvojiških obsegov ali praštevilske obsege. Prednost prvih je v prilagodljivosti dvojiškemu zapisu v računalnikih, prednost drugih pa v že vgrajeni aritmetiki v sodobnih procesorjih. Primeri kriptografskih shem, ki temeljijo na končnih obsegih, so

- klasični Diffie-Hellmanov protokol za dogovor o ključu [2], [5],
- ElGamalove sheme za digitalni podpis [3] ter

- kriptosistemi z javnimi ključi, ki uporabljajo eliptične krivulje [7].

Učinkovitost teh računsko zahtevnih shem je odvisna od hitrosti izvajanja aritmetičnih operacij, zahtevnost teh pa je odvisna od izbire baze. Idealno bi bilo, če bi lahko vsako operacijo opravili v tisti bazi, v kateri jo znamo najbolj učinkovito izvesti, saj bi potem lahko kombinirali najboljše iz različnih svetov. V praksi je izbor baze odvisen od tega, katere operacije z elementi najpogosteje izvajamo. V kriptografiji so najbolj uveljavljene polinomske in normalne baze in videli smo, da imajo polinomske baze pomembno vlogo že pri vpeljavi končnih obsegov. Njihova praktična prednost se pokaže predvsem v učinkovitem invertiranju, ki ga izvajamo z razširjenim Evklidovim algoritmom. Normalne baze pa so zanimive tako s stališča matematične teorije kot tudi zaradi praktične uporabe, zato si zaslužijo posebno obravnavo.

LITERATURA

[1] E. Berlekamp, *Algebraic Coding Theory*, Aegean Park Press; Revised edition, 1984.

[2] W. Diffie in M. E. Hellman, *New directions in Cryptography*, IEEE Transactions on Information Theory **IT-22**, (1976) 6, str. 644–654.

[3] ElGamal, *A public-key cryptosystem and signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory **IT-21**, (1985) 4, str. 469–472.

[4] D. Hankerson, A. Menezes in S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2004.

[5] A. Jurišić, *Diffie-Hellmanov dogovor o ključu*, Presek **34**, (2006/2007) 1, str. 25–30.

[6] A. Jurišić, *Računala nove dobe*, Presek **30**, (2002/2003) 4 in 5, str. 226–231 in 290–296 .

[7] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation **48**, (1987), str. 203–209 .

[8] R. Lidl in H. Niederreiter, *Encyclopedia of Mathematics and Its Applications: Finite Fields*, Cambridge University Press, 1987.

[9] A. J. Menezes, P. van Oorschot in S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[10] A. J. Menezes, I. F. Blake, S. Gao, R. C. Mullin, S. A. Vanstone in T. Yaghoobian, *Applications of Finite Fields*, Kluwer Academic Publishers, 1993.

[11] G. Seroussi, *Table of Low-Weight Binary Irreducible Polynomials*, Hewlett-Packard Laboratories Technical Report, HPL-98-135, 1998.

[12] I. Vidav, *Algebra*, DMFA–založništvo, 2003.

PRESNETI ČAJ

JANEZ STRNAD

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

PACS: 47.55.Ca, 47.55.dr

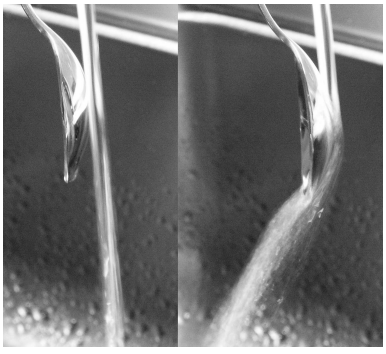
Marsikdo godrnja, ko pri nalivanju čaja iz čajnika zgreši skodelico. Podrobnejša opazovanja pojava pripeljejo do zanimivih spoznanj o toku tekočine.

THE TEAPOT EFFECT

It is annoying when pouring tea from a teapot the liquid misses the cup. Detailed observations of the phenomenon lead to interesting insight concerning the flow of fluids.

Opis pojava

Pogosto pri natakanju počasen curek čaja spolzi ob nosu čajnika in zgreši skodelico. Huje bi bilo, če bi se to pripetilo pri pretakanju kisline. Zato priporočajo, da med steklenico in posodo, v katero natakamo, postavimo stekleno palčko. Nezaželena vlaga se nabira na dnu okna, polzi po okviru navzdol in kvari les. Tok vode po spodnjem delu okvira v notranjost preprečimo z navpično zarezo na spodnji strani okvira. Plamen ob požaru lahko po oviri doseže mesto, na katerem povzroči še več škode. Pri opisanih pojavih tok tekočine, na primer vode ali zraka, sledi oviri, če ni preveč ukrivljena (slika 1).



Slika 1. Curek vode steče ob žlici. (Foto: Aleš Mohorič)

Vlogo ovire lahko prevzame tudi drug tekočinski tok. Pojav je že dolgo znan. O njem je leta 1800 poročal Thomas Young: „Tlak, ki sili plamen sveče k zračnemu toku iz meha, je verjetno natančno podoben tlaku, ki povzroči, da se zračni tok ob oviri ukrivi. Zaznamujte jamico, ki jo na vodni gladini povzroči tanek zračni curek. Z izbočenim telesom se s strani približajte curku in jamica bo takoj pokazala, da se je curek odklonil proti telesu.“ [1] Pogosto pojav imenujejo po čajniku teapot effect.

Pojav je pri večji hitrosti zraka od leta 1910 raziskoval Henri-Marie Coandă.[1] Zato govorijo o *Coandovem pojavu*. Nekateri povežejo pojav v počasnem toku s čajem, pojav v hitrem toku pa s Coando.

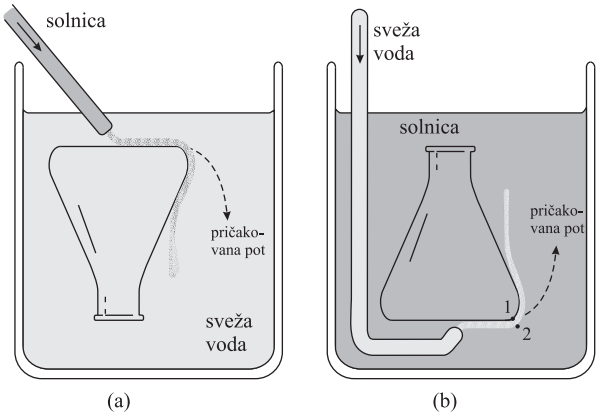
Okvirno pojasnimo pojav. Mislimo na tokovno cev v stacionarnem toku in Newtonov zakon $dF = dm\,a$ za del tekočine predelajmo v $-S dp = S\rho ds \cdot a$ in $dp = -\rho a ds$. Pri tem je a pospešek, $dm = S\rho ds$ masa dela tekočine v tokovni cevi z dolžino ds in presekom S ter dp razlika tlakov. Minus opozarja, da sila deluje od večjega tlaka k manjšemu. Za tangentni pospešek vstavimo $a = dv/dt$ in upoštevamo hitrost $v = ds/dt$. Enačba $dp = -\rho v dv$ pove, da v tangentni smeri hitrost narašča s pojemajočim tlakom. Sklep poznamo iz Bernoullijeve enačbe.

Manj znano enačbo dobimo za ukrivljeno tokovno cev v radialni smeri. Za radialni pospešek vstavimo $a = -v^2/r$ z razdaljo od krivinskega središča tokovnic r. Minus opozarja, da pospešek kaže proti krivinskemu središču. Enačba $dp = \rho dr \cdot v^2/r$ pove, da tlak v ukrivljeni tokovni cevi narašča prečno na tokovnice v smeri od krivinskega središča. Zadnjo enačbo uporabimo za curek tekočine v laminarnem toku ob oviri. Na kraju, na katerem bi se ločil od ovire, curek nekaj mirujoče okolne tekočine potegne za seboj in tokovnice se ukrivijo. V točki bliže oviri (točka 1 na sliki 2b) je zato tlak manjši kot v točki dalj od ovire (točka 2 na sliki). Razlika tlakov potegne curek proti oviri. Lahko bi rekli, da ob ločitvi curka od ovire nastanejo vrtinci, ki silijo curek proti oviri. Kako daleč curek sledi oviri, je odvisno od hitrosti in lastnosti tekočine ter od ukrivljenosti ovire.

Markus Reiner je skrbno obdelal pojav, ne da bi poznal Coandovo delo [2]. V čisto vodo so postavili steklenico z ravnim dnom in trikotniškim presekom. Najprej je bila obrnjena z vratom navzdol. Na vodoravno dno so

[1] Henri-Marie Coandă (1886–1972) je bil romunski častnik, letalec in aerodinamik, ki je deloval tudi v Franciji in Angliji. Pojav je opazil ob ponesrečenem poizkusu z reakcijskim letalom. Po njem se imenuje mednarodno letališče v Bukarešti.

s cevko poševno usmerili curek goste solne raztopine. Tok so zaznamovali z zrncem živilskega barvila. Curek goste raztopine je polzel ob stranski steni, preden se je obrnil navpično navzdol (slika 2a).



Slika 2. Curek slane vode v čisti vodi (a) in curek čiste vode v slani vodi (b). V curku vode se tokovnice ukrivijo, tako da je tlak v bližnji točki 1 manjši kot v bolj oddaljeni točki 2, in razlika tlakov potisne curek proti oviri [2, 5].

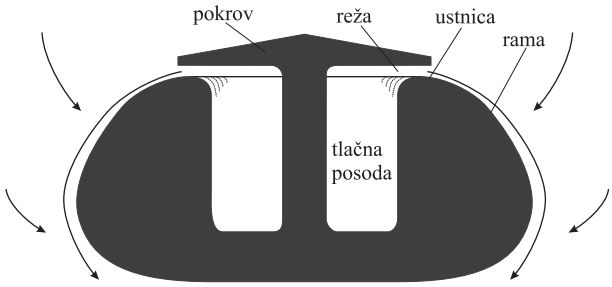
Nato so v nasičeno raztopino soli postavili steklenico z vratom navzgor in na vodoravno dno s cevko dovajali curek čiste vode. Zdaj je curek polzel ob vodoravnem dnu in nato ob stranski steni, preden se je obrnil navpično navzgor (slika 2b). Pri prvem poskusu je steklo privlačilo curek goste raztopine, pri drugem pa curek čiste vode. Po tem so sklepali, da pri pojavu nista pomembna površinska napetost ali adhezija, to je sila trdnega telesa na tekočino. Na izid poskusa ni vplivalo, če so nos čajnika prevlekli s tanko plastjo voska ali parafina, ki ga voda ne omoči. Namesto stekla so uporabili druge snovi in spreminjali okoliščine. Vselej je tekočina vsaj na kratki razdalji sledila oviri.

Pojav je leta 1957 z matematične strani obdelal Joseph Keller [3]. V dveh razsežnostih so rešili enačbe za gibanje neviskozne nestislijive tekočine. Pri tem so nos čajnika opisali z vzporednima poltrakoma. Dobili so štiri rešitve. Dve so poznali. Pri prvi je tekočina tvorila omejen curek s konstantno hitrostjo po preseku med poltrakoma in njunima podaljškoma, pri drugi pa neomejen tok po vsej ravnini. Preostalih dveh rešitev še niso poznali. Pri prvi se je tok obrnil in se vračal po zunanji strani zgornjega poltraka, pri drugi pa po zunanji strani spodnjega poltraka. Če so vključili težo, je rešitev, pri kateri se je tekočina vračala ob zgornjem poltraku, postala

nestabilna. Rešitev, pri kateri se je tekočina vračala ob spodnjem poltraku, pa je ostala stabilna. Ta rešitev je ustrezala pojavu, značilnemu za čajnik. Viskoznost in površinska napetost nista vplivali na naravo rešitev.

Uporaba

Pojav so poskušali izkoristiti. Coandă je poganjal zrak skozi ozko režo ter za ploskev z osno simetrijo dosegel, da je curek sledil površju telesa in spremenil smer za 180°. Pri tem je curek iz okolice posrkal dvajsetkratni masni tok okolnega zraka. Tlak ob površju telesa je bil na vrhnji strani telesa manjši od zračnega tlaka. Zmanjšani tlak je dodatno pospeševal curek, ki je izhajal iz reže in povzročal dinamični vzgon. Običajno dinamični vzgon nastane zaradi gibanja krila po zraku. Opisani vzgon pa nastane zaradi curka zraka, ne da bi se telo gibalo (slika 3).



Slika 3. H. Coandă in I. Reba sta delala poskuse z osno simetričnim telesom. Iz šobe je izhajal curek zraka in zajel veliko okolnega zraka. Zmanjšani tlak ob vrhnji ploskvi je povzročil dinamični vzgon [4].

Coandă je izdelal model vozila na zračno blazino. Za vzgon je poskrbel zmanjšani tlak na vrhnji ploskvi, medtem ko pri običajnih vozilih te vrste za vzgon poskrbi povečan tlak na spodnji ploskvi. Nenavadni predlog je naletel na nasprotovanje, še posebej, ker je imel model obliko letečega krožnika. Poskusi bi zatonili v pozabo, če v zasedenem Parizu med drugo svetovno vojno Nemci Coande ne bi vpregli v raketna raziskovanja. To je po vojni pritegnilo pozornost zaveznikov, ki so se namenili zadevo preiskati. Poskuse je najprej povzel eden od vodilnih aerodinamikov Theodore von Kármán leta 1949, pozneje pa se jih je lotil tudi Imants Reba na Brooklynskem tehnološkem inštitutu in v njegovem Laboratoriju za raketni pogon [4].

Reba je leta 1961 nadaljeval poskuse z vozilom na zračni blazini na razi-

skovalnem inštitutu, povezanem z vojsko. Model vozila s premerom 60 cm je imel stožčasto vrhnjo ploskev. Skozi režo v obliki ozkega obroča s premerom 15 cm je izhajal curek zraka z zvočno hitrostjo. Curek je ob površju vozila zajel zrak iz okolice, presegel zvočno hitrost in se zvrtinčil. Raziskali so več kot trideset različnih oblik telesa in z migoticami opazovali tok. Ugotovili so, da vzgon poveča stopnička tik pod šobo v obliki reže. Pomembni so bili še premer in širina reže, hitrost toka ter višina stopnice. Vendar niso mogli doseči želenega vzgona. Leta 1963 je Coandă ob obisku predložil vodoravno pregrado in rep. Potem se je vozilo celo za več centimetrov dvignilo od tal. Delali so tudi poskuse s čolnom na zračni blazini. Vrtinčenje so izkoristili pri gorilniku za popolno zgorevanje plina. Na ta način so želeli narediti gorilnik za sežiganje težkih olj.

Izdelali so dva prototipa letal VZ-9 Avrocar, ki sta se dvignila in spustila navpično. Nato so poskuse opustili. Pojav pa so uspešno uporabili pri vrsti letal, med njimi pri ameriških Boeingu YC-14 in C-17 Globemasterju III ter posebej pri ruskem Antonovu An-72 [1]. S curki zraka, ki jih pihajo ob zgornjih ploskvah kril, povečajo vzgon, kar je zaželeno pri majhni hitrosti letala ob vzletu in pristanku. Pojav izkoriščajo tudi pri odstranjevanju smeti in rib iz vode v dovodih k turbinam ter za brisalce brez metlic na šipah avtomobilov. Pojav so obdelali v obliki, v kateri ga je mogoče opisati pri pouku v srednjih šolah [6].

Model za hitri tok

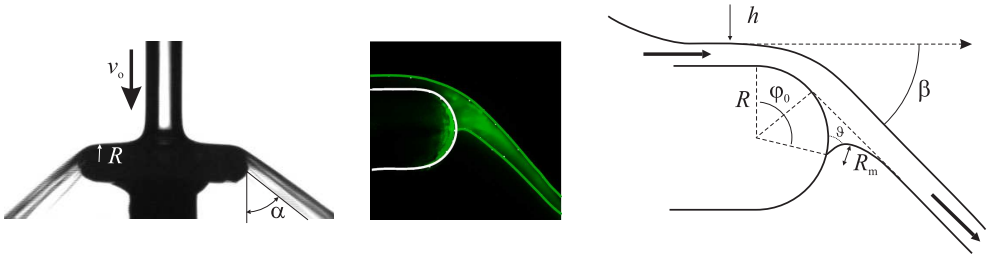
Francoska raziskovalna skupina je izvedla podrobne poskuse s poenostavljenim modelom v različnih okoliščinah [7]. Na vodoravno krožno ploščico s polmerom $r = 15$ mm so navpično navzdol usmerili curek vode s polmerom $r_0 = 4$ mm in hitrostjo v_0 od 1 do 5 m/s. Na ploščici se je curek nadaljeval kot tanka plast z debelino h. Voda je tekla radialno navzven in se na robu ploščice odklonila poševno navzdol. Merili so odklon α proti navpičnici, v odvisnosti od hitrosti v_0.

Pri prvem nizu poskusov so merili s ploščicami, katerih površje so na različne načine obdelali, da se je spremenil mejni kot ϑ. Pri drugem nizu poskusov so merili s ploščicami z različnimi debelinami $2R$ s krivinskim polmerom R na robu osnega preseka. V tretjem nizu so merili z vodo ter z mešanico glicerina in vode z dvakrat večjo viskoznostjo. Pokazalo se je, da to ni vplivalo na izide. Tok je bil precej hiter. Reynoldsovo število v

navpičnem curku $Re = 2r_0\rho v/\eta$ je merilo od 4 000 do 20 000, v plasti pa je bilo $Re = h\rho v/\eta$ desetkrat manjše. Teže ni bilo treba upoštevati. Izidi pa so bili odvisni od mejnega kota in od površinske napetosti. S superhidrofobno snovjo z mejnim kotom blizu 180° na ploščici so preprečili pojav (slika 4).

Slika 4. S superhidrofobno snovjo so premazali nos čajnika (levo) in s tem preprečili pojav (desno) [7].

Približno so ugotovili, kako je odklon odvisen od mejnega kota in debeline ploščice. Privzeli so, da je masni tok v navpičnem curku $\phi_{m0} = \rho v_0 \pi r_0^2$ enak radialnemu masnemu toku v plasti $\phi = \rho v \cdot 2\pi r h$ in da se ohrani tudi tok gibalne količine $v_0\phi_{m0} = v\phi_m$. Iz tega sta sledili zvezi $v = v_0$ in $h = \frac{1}{2}r_0^2/r$. Na robu ploščice pri razdalji r od osi se je curek odlepil in se od vodoravnice odklonil za kot $\beta = \frac{1}{2}\pi - \alpha$ (slika 5).

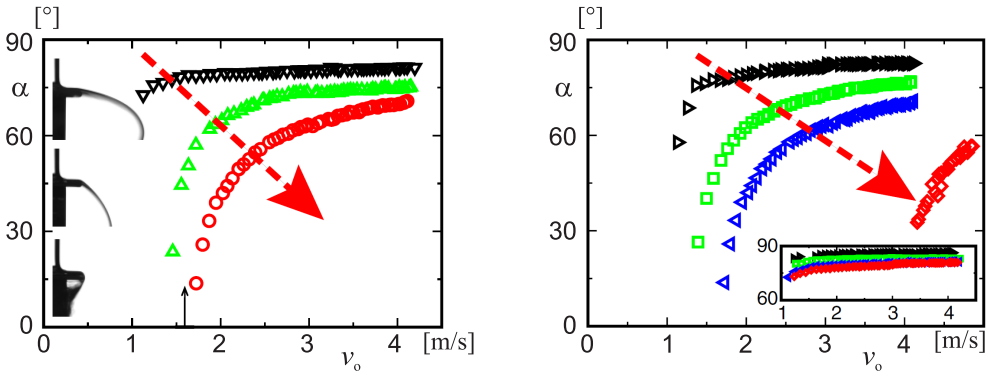


Slika 5. Slika poskusne naprave (levo) in slika plasti, ko se odlepi od ploščice (desno). Po [7].

Po več približnih korakih so dobili zvezo:

$$\beta \propto \sqrt{1 + \cos\vartheta}/v_0\,.$$

Merjenja so pokazala, da kot $\alpha = \frac{1}{2}\pi - \beta$ zares narašča z naraščajočo hitrostjo in z naraščajočim mejnim kotom (slika 6).



Slika 6. Odvisnost kota α od hitrosti v_0 za tri vrednosti mejnega kota ϑ (levo, puščica kaže od mejnega kota 175° preko 115° do 10°) in tri vrednosti krivinskega polmera R (desno, puščica kaže od polmera 0,03 mm preko 0,5 mm do 1,2 mm). V računih se pojavita kot φ, ki določa omočeno področje, in krivinski polmer meniska R_m. Po [7]. Zahvaljujem se profesorju Lydericu Bocquetu z univerze Lyon 1, ki je ljubeznivo dovolil objavo te in prejšnje slike.

Opisana raziskovanja so pritegnila precej pozornosti.

LITERATURA

[1] Coanda effect, `http://en.wikipedia.org/wiki/Coand%83_effect`.

[2] M. Reiner, *The teapot effect ... a problem*, Phys. Today **9** (1956) 16–20 (9); *Teapot means Coanda*, ibid. **20** (1967) 5, 15.

[3] J. B. Keller, *Teapot effect*, J. Appl. Phys. **28** (1957) 859–864.

[4] I. Reba, *Applications of the Coanda effect*, Scientific American **214** (1966) 6, 84–91.

[5] J. Walker, *The troublesome teapot effect, or why a poured liquid clings to the container*, Scientific American **251**, (1984) 4, 140–144.

[6] T. López-Arias, L. M. Gratton, S. Bon in S. Oss, *„Back of the spoon“ outlook of Coanda effect*, Phys. Teacher, **47** (2009) 508–512.

[7] C. Duez, C. Ybert, C. Clanet in L. Bocquet, *Wetting controls separation of inertial flows from solid surfaces*, Phys. Rev. Lett. **104** (2010) 084503 1–4.

ZGODOVINA REŠEVANJA POLINOMSKIH ENAČB

MARJAN JERMAN

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Math. Subj. Class. (2010): 12D10, 97H30

V članku je kratek oris zgodovine reševanja polinomskih enačb.

HISTORY OF SOLVING POLYNOMIAL EQUATIONS

The article outlines a short history of solving polynomial equations.

Uvod

Ko skušamo predstaviti nova poglavja iz matematike, večinoma posežemo po najkrajših in najbolj elegantnih poteh. Takšen način je po navadi najbolj pregleden in estetsko všečen. Do cilja pridemo sorazmerno hitro, poslušalca pa na poti obremenimo z najmanjšo možno količino potrebnih vmesnih rezultatov. Večina ljubiteljev matematike nas je nad takim načinom navdušenih, le redko pa se zavemo, da zelo prečiščena rešitev problema pogosto zakrije motivacijo za njegovo postavitev in intuicijo, ki je privedla do rešitve. Tako velikokrat zamudimo priložnost pokazati, kako iz različnih zornih kotov pogledati na problem in kako ga napasti z različnimi sredstvi.

Za večino dijakov je reševanje linearne enačbe žal le enostaven postopek premetavanja členov, reševanje kvadratne enačbe pa je enakovredno pomnjenju sorazmerno zapletenega obrazca. Prav tako nekateri študenti matematike o kubičnih enačbah vedo le, da se dajo rešiti z zelo zoprnimi in težko izračunljivimi formulami. V članku bi rad pokazal, kako lahko z zgodovinskim pogledom na reševanje enačb vsaj nekatere dijake in študente navdušimo za matematiko in jim predstavimo, koliko iskrivih in globokih idej je skritih za na videz suhoparnimi rezultati.

Ukvarjali se bomo z reševanjem polinomske enačbe

$$a_n x^n + \cdots + a_1 x + a_0 = 0. \tag{1}$$

Zgodovina in matematika se prepleteta že pri postavitvi problema:

(i) Kaj sploh pomeni simbolni zapis (1)?

(ii) Kateri številski množici pripadajo koeficienti polinoma a_i? V kateri množici iščemo rešitev x?

(iii) Ali je možna in kako poteka osnovna aritmetika (seštevanje, odštevanje, množenje in deljenje) s temi števili?

(iv) Ali je obstoj rešitev in ali so metode reševanja problema podobne za vse izbire številskih množic?

Na videz odvečna vprašanja skrivajo globoke ideje, ki so se rojevale vsaj 5000 let. Za ilustracijo bom navedel le nekaj zelo pomanjkljivih odgovorov, s katerimi želim osvetliti njihov pomen:

(i) Simbola + in − je uvedel Johannes Widman (1462–1500), simbol za enakost = Robert Recorde (1510–1558), simbol za koren pa Christoff Rudolff (1499–1545). Približno v istem času so začeli simbolno zapisovati tudi potence. Pred tem so bile enačbe opisane z dolgim in težko preglednim tekstom, ki ni omogočal danes na videz enostavnih algebrajskih manipulacij.

(ii) Pitagora (570–500 pr. Kr.) je trdil, da vsaki stvari ustreza ali naravno število ali kvocient dveh naravnih števil. Ničlo so po dolgih stoletjih težav z mestnim zapisom odkrili Babilonci, verjetno pa so jo zares razumeli šele dosti kasneje v Indiji. Negativnih števil v zahodni civilizaciji niso znali uporabljati skoraj do konca renesanse.

(iii) V Egiptu so za zapis števil uporabljali sistem, v katerem se da sorazmerno lahko seštevati in odštevati, množenje in deljenje pa sta zelo zapleteni operaciji. Šele Eudoxusu (405–355 pr. Kr.) je na precej zapleten način uspelo definirati množenje pozitivnih realnih števil. Še danes je recimo zelo težko na srednješolskem nivoju odgovoriti, kaj sploh pomeni zapis $2^{\sqrt{3}}$.

(iv) Če zahtevamo, da so koeficienti in rešitve v enačbi (1) realna števila, je iskanje ničel polinoma bistveno različno od reševanja starogrških diofantskih enačb, kjer so koeficienti in rešitve cela števila. Še bolj zapleteni so nekateri problemi iz teoretičnega računalništva, kjer so koeficienti polinoma celoštevilski ostanki pri deljenju s praštevilom.

Članek ni sistematičen pregled zgodovine reševanja polinomskih enačb. V nadaljevanju bom navedel le nekatere pomembne utrinke iz zgodovine matematike, ki so povezani z njihovim reševanjem.

Koeficienti naših polinomov bodo realni, rešitve pa večinoma realne, včasih tudi kompleksne.

Linearne enačbe

Skoraj vso egiptovsko matematiko poznamo iz Rhindovega in Moskovskega papirusa, ki izvirata približno iz let 1850 pr. Kr. in sta se skoraj neverjetno ohranila zaradi zelo suhega podnebja.

Rhindov papirus[1] je dobrih 30 centimetrov širok in šest metrov dolg zvitek, ki vsebuje 87 nalog. Štiriindvajseta naloga pravi:

Če neki količini dodamo njeno četrtino, dobimo 15*. Kolikšna je ta količina?*

Danes bi se naloge lotili z reševanjem enačbe

$$x + \frac{x}{4} = 15.$$

Pred skoraj 4000 leti pa so se problema lotili drugače, z metodo napačne predpostavke. To metodo so uporabljali do renesančnih časov.

Da bi si poenostavil računanje, pisar Ahmes najprej poskuša z rešitvijo $x = 4$. Ko izračuna vrednost izraza $x + \frac{x}{4} = 5$, ugotovi, da je rešitev za trikrat premajhna. Zato je prava rešitev $x = 4 \cdot 3 = 12$.

Nekateri zgodovinarji Ahmesovo rešitev interpretirajo drugače. Najprej Ahmes neznano količino razdeli na štiri enake dele, nato pa ugotovi, da je vsak del vreden tri enote.

Bralci naj sami premislijo, pri katerih polinomih lahko za iskanje ničel uporabimo Ahmesovo metodo.

Iz približno istega časa izvira babilonska[2] glinena tablica številka 8389, ki jo hranijo v Muzeju antičnega Bližnjega vzhoda v Berlinu. Prva naloga se v razširjenem prevodu glasi nekako takole:

[1] Alexander Henry Rhind (1833–1863) je bil škotski egiptolog, ki je leta 1858 na tržnici v Luxorju kupil papirus, odnesen iz Ramzesovega templja. Papirus je napisal pisar Ahmes približno 1850 let pr. Kr. Papirus je od leta 1863 v Britanskem muzeju.

[2] Babilonci so živeli v Mezopotamiji, med rekama Evfrat in Tigris. Na tem območju se je razvila sumerska civilizacija že pred letom 3500 pr. Kr. Med leti 2300 in 2100 pr. Kr. so območje zasedli Akadijci, leta 2100 pr. Kr. pa so Sumerce premagali Babilonci. Različne kulture so se v dosežkih zelo plodno medsebojno dopolnjevale.

Prvo polje da 4 *kur/bur pšenice,*[3] *drugo pa* 3 *kur/bur. Prvi pridelek presega drugega za* 500 *sil. Skupna površina obeh polj je* 1800 *sar. Koliko pridelka je zraslo na posameznem polju?*

Z današnjimi sredstvi bi nalogo zapisali kot sistem dveh linearnih enačb:

$$\begin{aligned} x + y &= 1800 \\ \frac{1200}{1800}x - \frac{900}{1800}y &= 500 \end{aligned}$$

Rešitev na tablici pa je napisana kot zaporedje računov, brez kakršnekoli razlage. Če jo razložimo in opišemo z današnjim matematičnim jezikom, gre nekako takole:

Najprej so izračunali $\frac{x+y}{2} = 900$. Nato so na videz uvedli novo spremenljivko $z = \frac{x-y}{2}$, ki je z iskanima količinama enostavno povezana: $x = 900+z$, $y = 900 - z$. Hkrati ustreza linearni enačbi z le eno neznanko:

$$\frac{2}{3}(900 + z) - \frac{1}{2}(900 - z) = 500.$$

Od tod so dobili: $z = 300$, $x = 1200$ in $y = 600$.

Kvadratne enačbe

Babilonska tablica številka 13 901, ki izvira približno iz leta 1600 pr. Kr. in je shranjena v Britanskem muzeju, vsebuje 24 nalog. Ker je napisana v retoričnem slogu, je bila verjetno namenjena poučevanju matematike. Prva naloga na tablici pravi:

Če ploščini kvadrata prištejemo stranico, dobimo $\frac{3}{4}$*. Poišči stranico kvadrata.*

Danes bi nalogo prevedli v kvadratno enačbo:

$$x^2 + x = \frac{3}{4}.$$

Na tablici pa rešitev poteka takole: Vzemi 1 in jo deli z 2, dobiš $\frac{1}{2}$. Če to polovico pomnožiš samo s sabo, dobiš $\frac{1}{4}$. Seštevek $\frac{1}{4}$ in $\frac{3}{4}$ je enak 1, to je kvadrat števila 1. Na koncu od 1 odštej število, ki si ga prej množil s sabo (to je $\frac{1}{2}$). Stranica kvadrata je torej $\frac{1}{2}$.

[3] Približno velja: bur = 1800 sar, 1 sar = 36 m^2, kur = 300 sil, 1 sila = 1 liter

Na videz nerazumljiv tekst skupaj s podobnimi babilonskimi nalogami razkriva, da so že takrat znali rešiti kvadratno enačbo

$$x^2 + ax = b \tag{2}$$

s formulo

$$x = \sqrt{\left(\frac{a}{2}\right)^2 + b} - \frac{a}{2}.$$

In kje se skriva druga rešitev kvadratne enačbe? Enačba (2) je zapisana tako, da so njeni koeficienti pozitivna števila. Tudi stranica, ki jo iščemo, je pozitivno število, zato je pred korenom smiseln le pozitivni predznak.

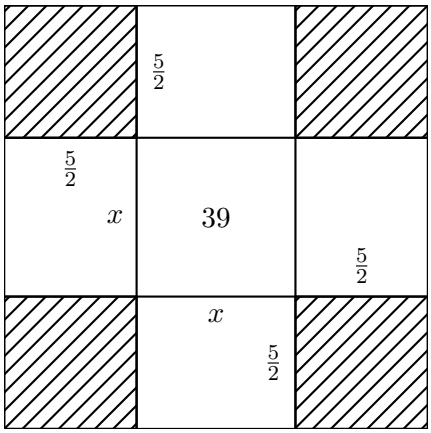
Še bolj nazorno so se precej kasneje kvadratnih enačb lotili Arabci.

Abu Jafar Muhammad ibn Musa Al-Khwarizmi (780–850) v svojem delu *Hisab al-jabr wal-muqabala* brez uporabe matematičnih simbolov najprej klasificira šest različnih tipov linearnih in kvadratnih enačb. Na videz pretirana razdelitev je potrebna, ker so takrat za koeficiente priznavali le pozitivna števila. Nato opiše operaciji *al-jabr* in *al-muqabala*, ki vsako linearno ali kvadratno enačbo prevedeta na enega od teh tipov. V današnjem jeziku operacija al-jabr poskrbi za odpravo negativnih členov (na obeh straneh enačbe prišteje nasprotno vrednost negativnih členov), operacija al-muqabala pa uravnoteži odvečne člene v enačbi (na obeh straneh odšteje manjšo od skupnih količin). Zato veliko zgodovinarjev matematike šteje Al-Khwarizmija za začetnika moderne algebre. Bralec lahko ugane, od kod prihaja beseda *algebra*, iz njegovega polatinjenega imena pa izvira tudi beseda *algoritem*.

V nadaljevanju pokaže, kako rešiti vsako od teh šestih enačb. Ker je reševanje v svojem bistvu geometrijsko, obstajajo špekulacije, da Al-Khwarizmijeve metode temeljijo na poznavanju prejšnjih del, morda Evklidovih *Elementov*[4] (300 pr. Kr.) ali pa židovskega dela *Mishnat ha Middot*[5] (pribl. 150 po Kr.).

[4] Evklid iz Aleksandrije (325–265 pr. Kr.) je v trinajstih knjigah zbral vse starogrško znanje matematike in ga postavil na aksiomatične temelje. *Elementi* so več kot 2000 let ostali najpomembnejše matematično delo zahodne civilizacije.

[5] *Mishnat ha Middot* (razprava o merah) je najstarejše židovsko delo o geometriji. Pisec rabin Nehemiah obravnava like in telesa, med drugim navede tudi Heronovo formulo za ploščino trikotnika. Razprava ima tudi teološko vrednost: rabin skuša na mehak način zaobiti v Bibliji navedeno dejstvo, da je $\pi = 3$. V jeruzalemskem templju naj bi stala ogromna posoda z okroglim robom, premerom 10 kubitov in obsegom 30 kubitov. Rabin pravi, da so premer merili z zunanje, obseg pa z notranje strani posode. Rob naj bi bil širok približno toliko, kot lahko razpremo dlan.



Slika 1. Reševanje enačbe $x^2 + 10x = 39$

Enačbo $x^2 + 10x = 39$ na primer reši takole (glej sliko 1): Vzemimo kvadrat s stranico x in mu nad vsako od stranic narišimo pravokotnik z osnovnico x in višino $\frac{5}{2}$. Skupna ploščina kvadrata in štirih pravokotnikov je $x^2 + 4 \cdot x \cdot \frac{5}{2}$. Ob ogliščih prvotnega kvadrata lahko med pravokotniki dorišemo štiri manjše kvadratke, ki skupaj s pravokotniki dopolnjujejo kvadrat s stranico x do večjega kvadrata s stranico $x + 2 \cdot \frac{5}{2}$. Večji kvadrat ima ploščino enako

$$x^2 + 4 \cdot x \cdot \frac{5}{2} + 4 \cdot \left(\frac{5}{2}\right)^2 = (x^2 + 10x) + 25 = 39 + 25 = 64,$$

zato je njegova stranica dolga 8, stranica x manjšega kvadrata pa meri $8 - 2 \cdot \frac{5}{2} = 3$.

Enako kot prej lahko vidimo, da druga rešitev geometrijsko ni smiselna. Morda je na tem mestu prav omeniti, da je šele Johann Carl Friedrich Gauss (1777–1855) leta 1849 dokazal, da ima polinom stopnje n z realnimi koeficienti natanko n kompleksnih ničel. Že leta 1799 je v svojem doktoratu pokazal, da se da vsak realni polinom razstaviti na nerazcepne linearne in kvadratne faktorje, vendar argumenti v njegovem topološkem dokazu ne zadoščajo današnjim matematičnim standardom. Leta 1816 je izdelal prvi popolnoma pravilen algebraičen dokaz.[6]

[6]Za dan polinom Gauss skonstruira nov polinom veliko višje lihe stopnje, ki ima ničle prek kvadratnih enačb povezane z ničlami prvotnega polinoma. Ker je novi polinom lihe stopnje, ima vsaj eno realno ničlo, zato ima prvotni polinom vsaj eno kompleksno ničlo.

Kubične enačbe

Prve kubične enačbe so se pojavile že pri Babiloncih kot praktični problemi pri izkopavanjih kleti. Na primer, enačbo $ax^3 + bx^2 = c$ so najprej prevedli v obliko $y^3 + y^2 = d$, nato pa so jo vsaj približno rešili s pomočjo obstoječih tabelic za vrednosti $n^3 + n^2$.

Znan je tudi grški mit o oraklu iz Delosa, ki je za končanje kuge svetoval prostorninsko podvojitev Apolonovega oltarja v obliki kocke.

Arhimed (287–212 pr. Kr.) se je v svojem delu *O sferi in valju* vprašal, kje je treba odrezati kroglo z ravnino tako, da bosta nastala kosa v volumskem razmerju 1 : 2. Bralec se lahko hitro prepriča, da sta tedaj polmer krogle r in višina odrezane kapice v povezana s kubično enačbo

$$v^3 - 3rv^2 + \frac{4}{3}r^3 = 0. \tag{3}$$

Zgodovinsko pomembno je tudi vprašanje, ali je možno samo s šestilom in ravnilom narisati pravilni sedemkotnik. Zelo lahko je videti, da se ga da narisati natanko takrat, ko se da narisati pravilni štirinajstkotnik. Če je r polmer štirinajstkotniku očrtanega kroga, a pa njegova stranica, se da na zvit način brez uporabe kotnih funkcij ugotoviti (slika 2), da ustrezata kubični enačbi

$$a^3 - ra^2 - 2r^2a + r^3 = 0.$$

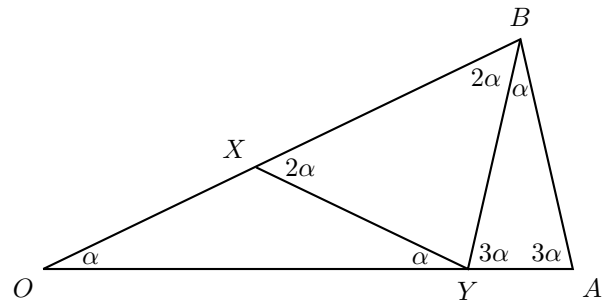
Ker je enačba za primerno izbiro polmera r nerazcepna nad racionalnimi števili,[7] je ta konstrukcija nemogoča.

Prav zadnja dva problema sta več kot tisoč let kasneje vzpodbudila arabske matematike, da so se intenzivno lotili reševanja kubičnih enačb. Omar Khayyam (1048–1122) je klasificiral 14 tipov kubičnih enačb (s pozitivnimi koeficienti), za vsakega od tipov preštel pozitivne rešitve in jih predstavil kot presek dveh krivulj drugega reda. Tako je recimo rešitev Arhimedove enačbe (3) abscisa preseka primerno izbrane parabole in hiperbole (slika 3)

$$y = x^2, \quad (x - 3r)y = -\frac{4}{3}r^3.$$

Seveda takrat še niso poznali matematičnega simbolizma in enačb krivulj v koordinatnem sistemu. Obe stožnici Khayyam opiše geometrijsko.

[7] V primeru $r = 1$ dobimo enačbo $p(a) = a^3 - a^2 - 2a + 1 = 0$. Če p ne bi bil minimalni polinom (nad $\mathbb{Q}$) za a, bi vseboval vsaj en linearen faktor, kar pomeni, da bi imel vsaj eno racionalno ničlo. Edina kandidata za racionalne ničle $a = \pm 1$ pa nista polinomovi ničli. Samo z ravnilom in šestilom se dajo narisati le nekatera števila, ki imajo minimalni polinom stopnje 2^m za primeren $m \in \mathbb{N} \cup \{0\}$.



Slika 2. Na sliki je enakokrak trikotnik $\triangle ABO$, ki ima kot ob vrhu enak $\alpha = \frac{1}{7} \cdot 180^\circ$, kota ob osnovnici pa merita 3α. Ta trikotnik je štirinajstina pravilnega štirinajstkotnika, iz katerega zlahka dobimo pravilni sedemkotnik. Evklid je zvito izbral točki X in Y na krakih tako, da je $\angle ABY = \alpha$ in $\angle BXY = 2\alpha$. Samo s pomočjo podobnosti lahko dobimo kubično zvezo med $OA = OB$ in AB (upoštevamo, da je $\triangle ABO \sim \triangle YAB$ in da sta višini trikotnikov $\triangle OYX$ in $\triangle OAB$ v razmerju $OX : OB$).

Dokončna rešitev kubične enačbe je prišla z renesanso in je povezana s hudimi spori o njenem avtorstvu. V tistih časih so matematiki velik delež svojih dohodkov pridobili na matematičnih tekmovanjih, ki so jih razpisali bogati pomembneži, zato je poznavanje rešitve kubične enačbe pomenilo veliko prednost pred tekmeci.

Kubično enačbo brez kvadratnih členov

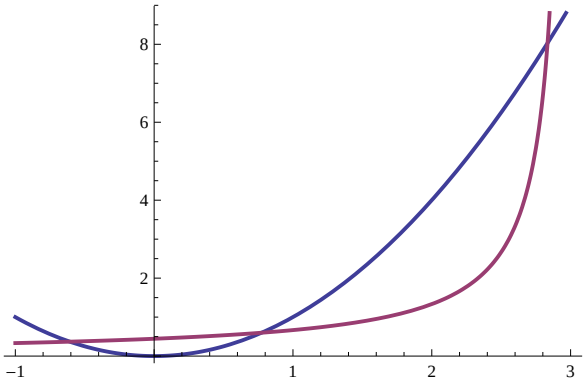
$$x^3 + px + q = 0 \tag{4}$$

je prvi rešil Scipione dal Ferro (1465–1526). Rešitev je napisal kot recept brez vsakršne razlage. Zaradi tedaj še zelo nerodne uporabe simbolov in nepoznavanja negativnih števil dal Ferro ni opazil, da je s tem v bistvu rešil poljubno kubično enačbo oblike

$$x^3 + ax^2 + bx + c = 0. \tag{5}$$

Translacija $y = x + \frac{a}{3}$ namreč poskrbi, da v enačbi (5) izginejo kvadratni členi in jo tako prevede na enačbo oblike (4).

Neodvisno od dal Ferra je rešitev poljubne kubične enačbe odkril Nicolo Tartaglia (1500–1557). Prav v tem času je Girolamo Cardano (1501–1576) skušal napisati knjigo *Ars Magna*, ki bi vsebovala tudi rešitev kubične enačbe. Po daljšem prepričevanju mu je s trikom uspelo prepričati Tartaglio, da mu je razkril rešitev. Pri tem mu je sveto obljubil, da rešitve nikomur



Slika 3. Rešitev Arhimedove kubične enačbe (3) v primeru $r = 1$ kot abscisa preseka parabole in hiperbole. Smiselna je le rešitev $0 < v < r$.

ne bo izdal. Ko je kasneje Cardano v Bologni našel dal Ferrove zapiske, je s tem delno spodbijal Tartaglievo prvo avtorstvo rešitve in se odločil, da lahko prelomi obljubo. Cardano je bil tudi sicer zelo problematična osebnost, a je njegova knjiga prinesla poleg sistematične rešitve še negotov pogled v nehote odkrita kompleksna števila.

Tartaglieva ideja za rešitev enačbe (4) temelji na dobro znani enakosti

$$(u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3.$$

Če jo prepišemo v obliko

$$(u+v)^3 - 3uv(u+v) - (u^3+v^3) = 0$$

in primerjamo z enačbo (4), opazimo, da bi morda lahko pomagala substitucija $x = u + v$, pri čemer bi veljalo

$$p = -3uv, \quad q = -(u^3+v^3). \tag{6}$$

Sedaj lahko uporabimo že znani babilonski trik, ki pove, da lahko s pomočjo vsote in razlike neznanih količin ti dve količini enostavno izračunamo. Velja namreč:

$$(u^3-v^3)^2 = (u^3+v^3)^2 - 4u^3v^3,$$

kar skupaj s povezavami (6) pomeni:

$$u^3+v^3 = -q, \quad u^3-v^3 = \pm\sqrt{q^2 + 4\left(\frac{p}{3}\right)^3}.$$

Tako je $x = u + v$, pri čemer je

$$\begin{aligned} u^3 &= -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}, \\ v^3 &= -\frac{q}{2} \mp \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}. \end{aligned}$$

Tretja korena za u in v izberemo tako,[8] da velja $p = -3uv$. Pričakovano se izkaže, da temu pogoju zadoščajo le tri kombinacije tretjih korenov, ki dajo vse ničle enačbe (4).

Ko je Cardano na ta način reševal enačbo $x^3 = 15x + 4$, je presenečen ugotovil, da ima enačba sicer zelo lepo rešitev $x = 4$, med reševanjem pa se ne more izogniti korenom negativnih števil:[9]

$$4 = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}.$$

Cardano ni vedel kaj storiti, za nasvet se je obrnil celo na Tartaglio, ki mu ni znal pomagati. Do intuitivne rešitve težav je prišel Rafael Bombelli (1526–1572), ki je nastavil enačbi

$$\sqrt[3]{2 \pm \sqrt{-121}} = 2 \pm t\sqrt{-1},$$

s tem nevede uvedel imaginarno enoto in po kubiranju dobil $t = 1$.[10] Pri tem je moral poleg običajnega pravila za računanje s koreni pozitivnih števil $\sqrt{x}\sqrt{y} = \sqrt{xy}$ uporabiti tudi novo pravilo $\sqrt{-x}\sqrt{-x} = -x$.

Enačbe četrte stopnje

Cardano je svojemu študentu Lodovicu Ferrariju (1522–1565) naročil, naj skuša rešiti sistem enačb

$$\begin{aligned} x_1 + x_2 + x_3 &= 10, \\ \frac{x_1}{x_2} &= \frac{x_2}{x_3}, \\ x_1 x_2 &= 6. \end{aligned}$$

[8] Naj bo $\zeta = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ primitivni tretji koren enote. Tedaj enačbama poleg u in v ustrezajo tudi $u\zeta$, $u\zeta^2$, $v\zeta$ in $v\zeta^2$. Seveda takrat kompleksnih števil še niso poznali.

[9] To se zgodi natanko takrat, ko so vsi trije koreni različni in realni.

[10] Pri nastavku je imel Bombelli srečo. Izkaže se, da je najti ustrezni realni del enako težko kot rešiti osnovno kubično enačbo. Zato so tedanji matematiki tak primer imenovali *casus irreducibilis*.

Hitro lahko vidimo, da spremenljivka x_2 zadošča enačbi

$$x_2^4 + 6x_2^2 + 36 = 60x_2.$$

Med reševanjem tega problema je Ferrari odkril splošno metodo za reševanje enačbe

$$x^4 + ax^3 + bx^2 + cx + d = 0.$$

Enačbo je najprej nekoliko preoblikoval:

$$\left(x^2 + \frac{1}{2}ax\right)^2 = \left(\frac{1}{4}a^2 - b\right)x^2 - cx - d. \tag{7}$$

Ta enačba bi se bistveno poenostavila, če bi bila tudi njena desna stran popolni kvadrat. S tem bi reševanje enačbe četrte stopnje prevedli na reševanje dveh kvadratnih enačb. Žal diskriminanta kvadratne funkcije na desni strani enačbe (7) večinoma ni enaka 0. Ferrari je dobil genialno idejo in v levo stran enačbe uvedel nov parameter y, desno stran pa ustrezno prilagodil

$$\left(x^2 + \frac{1}{2}ax + y\right)^2 = \left(\frac{1}{4}a^2 - b + 2y\right)x^2 - (c - ay)x - d + y^2.$$

Da bo diskriminanta desne kvadratne funkcije enaka 0, mora veljati:

$$(c - ay)^2 - 4\left(\frac{1}{4}a^2 - b + 2y\right)(y^2 - d) = 0.$$

To pa je kubična enačba (imenujemo jo *kubična resolventa*) spremenljivke y z vsaj eno realno rešitvijo, ki jo znamo dobiti s pomočjo Cardanovih formul. Če je y ena od rešitev, smo tako enačbo (7) prevedli na reševanje dveh kvadratnih enačb:

$$x^2 + \frac{1}{2}ax + y = \pm\left(x\sqrt{\frac{1}{4}a^2 - b + 2y} + \sqrt{y^2 - d}\right).$$

Vsaka od enačb da po dve rešitvi.

Enačbe višjih stopenj

V prihodnjih stoletjih je veliko izjemnih matematikov, med njimi Ehrenfried Walter von Tschirnhaus (1651–1708), Leonhard Euler (1707–1783),

Étienne Bézout (1730–1783), Alexandre-Théophile Vandermonde (1735–1796), Edward Waring (1736–1798) in Joseph-Louis Lagrange (1736–1813) skušalo rešiti enačbo pete stopnje. Bolj natančno, skušali so najti formulo, ki bi rešitev enačbe pete stopnje opisala samo s pomočjo osnovnih računskih operacij in korenov (v takem primeru pravimo, da je enačba *rešljiva z radikali*).

Tschirnhaus je skušal najti substitucijo

$$y = x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0,$$

ki bi enačbo

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$

prevedla v obliko $y^n - c_0 = 0$. Njegova ideja temelji na pričakovanju, da je sistem $n-1$ enačb za vmesne koeficiente

$$c_{n-1} = \ldots = c_1 = 0$$

rešljiv, če le izberemo dovolj veliko število neznank $b_{m-1}, \ldots, b_0$.[11]

Splošno enačbo pete stopnje lahko s substitucijo $y = x^2 + b_1x + b_0$ prevedemo na enačbo oblike $y^5 + c_2y^2 + c_1y + c_0 = 0$. Pri tem je treba rešiti sistem dveh kvadratnih enačb z neznankama b_1 in b_0. Primerna kubična substitucija bi sicer odpravila tudi kvadratni člen, vendar bi bilo pri tem treba rešiti sistem treh enačb, ki je ekvivalenten reševanju polinomske enačbe šeste stopnje.[12] Erlandu Samuelu Bringu (1736–1798) in Georgeu Birchu Jerrardu (1804–1863) je neodvisno drug od drugega uspelo odpraviti tudi kvadratni člen tako, da sta uporabila substitucijo četrte stopnje. Gian Francesco Malfatti (1731–1807) je v primerih, ko je enačba $x^5+a_1x+a_0 = 0$ rešljiva z radikali, našel tudi njene rešitve, ki pa so odvisne od rešitev neke pripadajoče polinomske enačbe šeste stopnje.[13]

Leta 1799 je Paolo Ruffini (1765–1822) pokazal, da se rešitev enačb stopnje vsaj pet ne da zapisati na želen način. Med dokazovanjem je Ruffini

[11] Naj bo $K = \mathbb{Q}(a_0, ..., a_{n-1})$. Če je polinom $p \in K[x]$, ki mu želimo odpraviti vmesne člene, nerazcepen, lahko v jeziku moderne algebre rečemo, da Tschirnhausova transformacija $T\colon K[x] \to K[x]$ ohranja ustrezno razširitev polja, to je $K[x]/\langle p\rangle = K[x]/\langle T(p)\rangle$. Lomljeni oklepaji označujejo glavni ideal, ki ga generira ustrezni polinom. $T(p)$ si lahko predstavljamo tudi kot minimalni polinom enega od primitivnih elementov razširitve $K[x]/\langle p\rangle$.

[12] Kasneje se je izkazalo, da je poiskati substitucijo, ki bi odpravila vse vmesne člene v polinomu stopnje n, enako težko kot rešiti polinomsko enačbo stopnje $(n-1)!$. V primeru $n = 4$ imamo srečo, da ustrezna enačba šeste stopnje razpade na kvadratne faktorje.

[13] Leta 1991 je David S. Dummit [2] našel eksplicitne formule za ničle enačbe pete stopnje, ki je rešljiva z radikali.

uporabljal permutacije in razvil velik kos nove matematike, ki je kasneje postal del teorije grup. Dokaz je bil tako zapleten, da ga večina tedanjih matematikov ni razumela, zato rezultata niso popolnoma priznavali in šele Augustin Louis Cauchy (1789–1857) je leta 1821 potrdil, da Ruffinijevo delo dokazuje nerešljivost enačb stopnje vsaj pet z radikali. Kasneje se je izkazalo, da je Ruffinijev rezultat sicer pravilen, dokaz pa ima manjšo luknjo.

Niels Henrik Abel (1802–1829) ni poznal Ruffinijevega rezultata. Prepričan je bil, da mu je uspelo rešiti enačbo pete stopnje. Pred objavo odkritja so ga prosili, naj svojo metodo ilustrira na konkretnem primeru. Abel je med neuspešnim reševanjem primera našel napako v dokazu. Medtem pa je dobil tako dober vpogled v reševanje enačbe pete stopnje, da mu je uspelo izdelati prvi popolnoma pravilen dokaz o nerešljivosti enačb stopnje vsaj pet z radikali.

Navkljub rezultatom, ki sta jih dobila Ruffini in Abel, pa se dajo nekatere enačbe višjih stopenj vendarle rešiti na želeni način. Trivialen primer je recimo enačba $(x-1)^5 = 0$. Evariste Galois (1811–1832) je malo pred prezgodnjo smrtjo našel potrebne in zadostne pogoje, ki jih mora izpolnjevati polinom, da je enačba rešljiva z radikali. Permutacijska grupa polinomovih ničel, imenovana *Galoisova grupa*,[14] mora biti rešljiva kot grupa.[15] Polinom $x^5 - x - 1$ ima recimo Galoisovo grupo enako nerešljivi permutacijski grupi S_5, zato se njegovih ničel ne da zapisati samo z osnovnimi računskimi operacijami in koreni.

LITERATURA

[1] W. S. Anglin, *Mathematics: a concise history and philosophy*, Undergraduate Texts in Mathematics, Readings in Mathematics, Springer-Verlag, New York, 1994.

[2] D. S. Dummit, *Solving solvable quintics*, Math. Comp. **57** (1991), št. 195, 387–401.

[3] S. MacLane in G. Birkhoff, *Algebra*, 3. izdaja, AMS, Providence, RI, 1999.

[4] J. J. O'Connor in E. F. Robertson, *The MacTutor History of Mathematics archive*, http://www-history.mcs.st-and.ac.uk

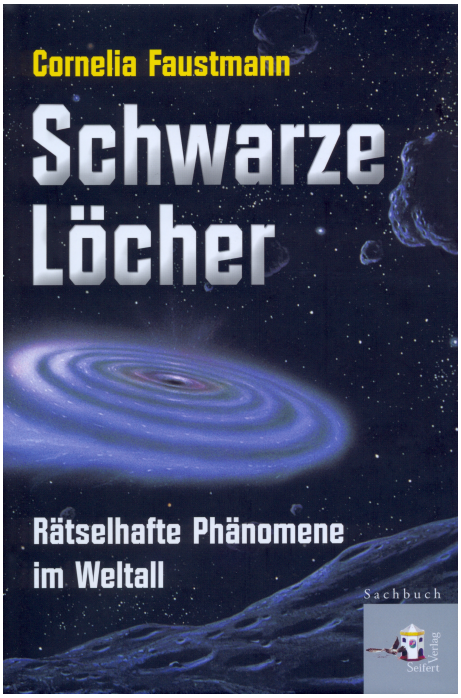
[5] J. Sesiano, *An introduction to the history of algebra. Solving equations from Mesopotamian times to the Renaissance*, iz francoščine prevedla Anna Pierrehumbert, Mathematical World **27**, AMS, Providence, RI, 2009.

[6] I. Vidav, *Algebra*, 4. natis, DMFA, Ljubljana, 1989.

[14] *Galoisovo grupo* tvorijo vse permutacije polinomovih ničel, ki ohranjajo veljavnost vseh algebrajskih enačb z racionalnimi koeficienti, ki jih ničle izpolnjujejo.

[15] Grupa G je *rešljiva*, če se zaporedje njenih komutatorskih podgrup $G, G', (G')', \ldots$ konča z enoto. *Komutatorska grupa* G' je najmanjša grupa, ki vsebuje vse produkte $xyx^{-1}y^{-1}$, $x, y \in G$.

Cornelia Faustmann, SCHWARZE LÖCHER – RÄTSELHAFTE PHÄNOMENE IM WELTALL, Seifert Verlag, Dunaj, 2008, 188 strani.



Črne luknje so nedvomno veličastni in obenem skrivnostni objekti v vesolju. Predstavljamo zanimivo, razmeroma enostavno napisano knjigo, ki bi morala pritegniti marsikaterega bralca že zaradi mladosti avtorice Cornelie Faustmann. Ta se je pogumno, brez zadržkov in samozavestno lotila študija črnih lukenj z upoštevanjem astronomskih opazovanj in računalniških simulacij, ki jih omogočata najsodobnejša vesoljska in računalniška tehnologija.

Poenostavljeno pravimo, da je črna luknja okrogel objekt, ki ima tako veliko maso, da z njega ne more ubežati niti svetloba. Zato črnih lukenj ne moremo videti in so dokazi o njihovem obstoju samo posredni. O njih sta že konec 18. stoletja razmišljala J. Mitchell in P. S. Laplace. Resneje so jih začeli študirati po letu 1916, ko je A. Einstein objavil *Osnove splošne teorije relativnosti*. Žal je druga svetovna vojna prekinila raziskovanja, povezana s črnimi luknjami, tako da so se jim resno posvetili šele leta 1967, ko je nastopila prava zlata doba za njihov študij.

Knjiga je smiselno razdeljena na tri glavne dele. Vsak del ima na začetku za uvod krajšo šaljivo, a vendar domiselno in poučno pripoved, ki ji sledi znanstvena razprava, bogato ilustrirana s fotografijami, skicami in razpredelnicami. Našteta je tudi cela vrsta znanstvenikov in njihovih razmišljanj v zvezi z dogajanjem v vesolju.

Prvi del knjige pripoveduje o nastajanju zvezd. Natančno opisuje dogajanje z zvezdo, v kateri potekajo zapleteni procesi zaradi gravitacije, ki zvezdo stiskajo, in silami, ki temu nasprotujejo. Spoznamo, kako nastanejo zvezde prvega niza, rdeče velikanke, supernove, bele pritlikavke, nevtronske zvezde, pulzarji in črne luknje.

Drugi del, pričenja ga pripoved o nenavadni sili in moči, ki stopita na prizorišče, obravnava glavno temo, črne luknje kot zagonetne objekte v vesolju. Najdemo veliko podatkov o tem, kako je potekalo raziskovanje, iskanje in odkrivanje črnih lukenj. Spoznamo tudi osnovne ugotovitve splošne teorije relativnosti, rentgensko sevanje in gravitacijske valove.

Pripoved o dogajanju pri padcu v črno luknjo uvaja tretji del knjige. Sledi razprava o znanstveni fantastiki, astronavtih in o nenavadnih pojavih v bližini črne luknje. Izvemo, kaj so črvine ali črvje luknje, potovanje skozi čas in bele luknje.

V dodatku knjige so slovarček osnovnih pojmov in glavni časovni mejniki od leta 1783 do leta 2008 v zvezi s črnimi luknjami, obsežen seznam zaporedno citiranih del, seznam uporabljene literature in spletnih virov, seznam slik, preglednica uporabljenih fizikalnih konstant in njihovih oznak, seznam v knjigi omenjenih oseb ter stvarno kazalo.

Avtorica Cornelia Faustmann se je rodila leta 1986 in se je že pri svojih desetih letih začela zanimati za črne luknje. Kot gimnazijka je napisala delo *Entstehung und Eigenschaften Schwarzer Löcher – Nastanek in lastnosti črnih lukenj*, za kar sta jo Avstrijsko fizikalno društvo in Avstrijsko društvo za astronomijo in astrofiziko tudi nagradili. Poimenovali so jo *čudežni otrok fizike*. Od leta 2004 študira astronomijo in latinščino na dunajski univerzi, kjer je od leta 2007 tudi tutorka za latinsko slovnico in kjer pripravlja doktorsko disertacijo. Leta 2007 je izšla knjižica *Einstein entformelt – Einstein brez formul* s podnaslovom *Wie ihm ein Teenager auf die Schliche kam – Kako ga je doumel najstnik*, ki sta jo napisala Cornelia Faustmann in človek, ki jo je odkril, znani avstrijski teoretični fizik Walter Thirring. Ta je tudi napisal tukaj predstavljeni knjigi lep in obširen predgovor.

Marko Razpet

OBZORNIK ZA MATEMATIKO IN FIZIKO
LJUBLJANA, SEPTEMBER 2010
Letnik 57, številka 5
ISSN 0473-7466, UDK 51 + 52 + 53

VSEBINA

CONTENTS

Na naslovnici je Coandov pojav: Ovira preusmeri plamen sveče (k članku Presneti čaj na strani 176) (Foto: Aleš Mohorič).