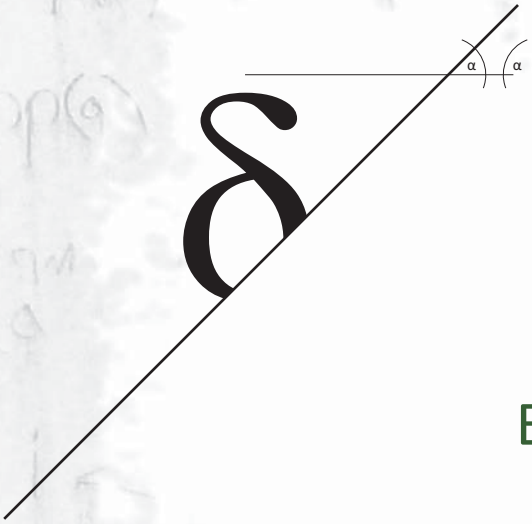

Evklidov algoritem

Euclidean Algorithm

Marjan Jerman
Univerza v Ljubljani,
Fakulteta za matematiko
in fiziko

Σ Povzetek

V prispevku je na kratko opisana zgodovina Evklidovega algoritma. Navedene so nekatere njegove klasične uporabe v teoriji števil: Bezoutova identiteta, reševanje linearnih diofantskih enačb, uporaba pri kitajskem izreku o ostankih, aproksimacija korenov naravnih števil z verižnimi ulomki in reševanje Pellove enačbe. Prispevek se konča s posplošitvijo na evklidske kolobarje, kjer so omenjeni kolobarji polinomov v eni spremenljivki s koeficienti iz obsega, Gaussova števila in Eisensteinova števila.

Ključne besede: zgodovina matematike, Evklidov algoritem, Bezoutova identiteta, linearne diofantske enačbe, kitajski izrek o ostankih, verižni ulomki, Pellova enačba, evklidski kolobar

Σ Abstract

The article briefly describes the history of Euclidean algorithm. Described within are some classical methods of its use in the theory of numbers: Bézout's identity, solving linear Diophantine equations, its application on the Chinese remainder theorem, approximation of the roots of natural numbers with help of continued fractions, and solving Pell's equation. The article concludes with a generalization based on Euclidean domains, mentioning the domains of polynomials in one variable with coefficients from a division ring, Gaussian integers and Eisenstein integers.

Keywords: *history of mathematics, Euclidean algorithm, Bézout's identity, linear Diophantine equations, Chinese remainder theorem, continued fractions, Pell's equation, Euclidean domain*

α Uvod

Evklidov algoritem je prvič omenjen v Evklidovih Elementih[1], vendar so ga poznali že dosti prej. Pitagorejci[2] so verjetno z njegovo pomočjo računali zelo natančne približke korenov naravnih števil. V sedmi knjigi Elementov je zelo strnjeno zapisana različica algoritma za cela števila, ki nam izračuna največji skupni delitelj dveh naravnih števil:

Zaporedoma odštevaj manjše število od večjega, dokler manjše število ne postane delitelj večjega. Takrat je manjše od števil največji skupni delitelj začetnih števil.

V deseti knjigi Elementov je opisana geometrijska različica Evklidovega algoritma, s pomočjo katere lahko Evklidov algoritem do neke mere posplošimo na realna števila. Za dani daljici pravimo, da sta *soizmerljivi*, če obstaja takšna (krajša) daljica, imenovana *skupna mera daljic*, da je vsaka od danih daljic enaka celemu številu kopij krajše daljice. Tudi v geometrijskem primeru poteka Evklidov algoritem skoraj enako kot prej:

Zaporedoma odštevaj krajšo daljico od večje. Če po nekaj korakih dobiš enaki daljici, si s tem dobil največjo skupno mero začetnih daljic. Če se postopek v končnem številu korakov ne konča z enakima daljicama, začetni daljici nista soizmerljivi.

V modernem matematičnem jeziku bi lahko rekli, da sta realni števili soizmerljivi, če je njun kvocient racionalno število.

V srednji šoli običajno povemo Evklidov algoritem za naravni števili kot eno od možnosti za iskanje največjega skupnega delitelja teh dveh števil. V nadaljevanju prispevka bodo opisane še nekatere druge pomembne uporabe algoritma, ki so zaradi elementarnosti velikokrat dostopne tudi srednješolcem, ki želijo poglobiti svoje znanje matematike.

β Bezoutova identiteta

Naj bosta m in n naravni števili z največjim skupnim deliteljem D in $n \geq m$. Evklidov algoritem poteka takole:

$$n = k_1 m + r_1; 0 < r_1 < m$$
$$m = k_2 r_1 + r_2; 0 < r_2 < r_1$$
$$r_1 = k_3 r_2 + r_3; 0 < r_3 < r_2$$
$$\vdots$$
$$r_{s-1} = k_{s+1} r_s + r_{s+1}; 0 < r_{s+1} < r_s$$
$$r_s = k_{s+2} r_{s+1} + D; 0 < D < r_{s+1}$$
$$r_{s+1} = k_{s+3} D$$

Preberimo Evklidov algoritem v obratnem vrstnem redu:

Iz predzadnje enačbe lahko izrazimo D kot

$$D = r_s - k_{s+2} r_{s+1}.$$

Na enak način preberemo

$$r_{s+1} = r_{s-1} - k_{s+1} r_s,$$

zato velja tudi

$$D = r_s - k_{s+2}(r_{s-1} - k_{s+1} r_s).$$

V vsakem naslednjem koraku s pomočjo višje ležečih vrstic v Evklidovem algoritmu vsak ostanek zamenjamo s celoštevilsko kombinacijo ostankov r_{t-1} in r_{t-2}. Skupni delitelj D tako vsakič napišemo kot celoštevilsko kombinacijo ostankov z nižjima indeksoma.

Prva vrstica nam pove Bezoutovo identiteto[3]

1 *Evklidovi Elementi so zbirka 13 knjig iz tretjega stoletja pr. Kr., ki povzemajo najpomembnejše starogrško znanje matematike.*

2 *Pitagora (570-500 pr. Kr.). Na jugu Italije, ki je bil tedaj del antične Grčije, je ustanovil versko-filozofsko bratovščino, ki se je ukvarjala s teoretično matematiko, glasbo in astronomijo.*

3 *Étienne Bézout (1730-1783), francoski matematik*

$D = mx + ny$

za primerni celi števili x in y.

Poglejmo si jo za par naravnih števil 67 in 120.

Najprej izvedimo Evklidov algoritem:

$120 = 1 \cdot 67 + 53$
$67 = 1 \cdot 53 + 14$
$53 = 3 \cdot 14 + 11$
$14 = 1 \cdot 11 + 3$
$11 = 3 \cdot 3 + 2$
$3 = 2 \cdot 1 + 1$

Največji skupni delitelj 1 lahko sedaj napišemo kot celoštevilsko kombinacijo števil 67 in 120:

$1 = 3 - 2 = 3 - (11 - 3 \cdot 3) = 4 \cdot 3 - 11 =$
$= 4 \cdot (14 - 11) - 11 = 4 \cdot 14 - 5 \cdot 11 =$
$= 4 \cdot 14 - 5 \cdot (53 - 3 \cdot 14) = 19 \cdot 14 - 5 \cdot 53 =$
$= 19 \cdot (67 - 53) - 5 \cdot 53 = 19 \cdot 67 - 24 \cdot 53 =$
$= 19 \cdot 67 - 24 \cdot (120 - 67) = 43 \cdot 67 - 24 \cdot 120$

Razcep ni enoličen. Na primer, velja tudi:

$1 = (43 + 120) \cdot 67 - (24 + 67) \cdot 120$

δ Linearne diofantske enačbe

Naj bosta m in n naravni števili z največjim skupnim deliteljem D. Če je rešljiva linearna diofantska enačba

$$mx + ny = c,$$

je jasno, da mora D deliti tudi c, $c = Dc'$.

Bezoutova identiteta nam pove, da velja tudi obratno. Če D deli c, lahko najdemo celi števili x' in y', za kateri velja

$$D = mx' + ny'$$

in tako dobimo eno od rešitev diofantske enačbe:

$$c = Dc' = m(x'c') + n(y'c').$$

Če je $m = Dm'$ in $n = Dn'$, lahko D v diofantski enačbi pokrajšamo. S tem dosežemo, da sta števili m' in n' tuji. Lahko je videti[4], da so vse rešitve enačbe

$$m'x + n'y = 1$$

oblike $x = x' + kn'$, $y = y' - km'$. Rešitve enačbe

$$m'x + n'y = c'$$

pa so le ustrezno pomnožene, $x = c'x' + kn'$, $y = c'y' - km'$.

Rešimo na primer diofantsko enačbo

$$67x + 120y = 3.$$

V prejšnjem razdelku smo dobili razcep

$$1 = 43 \cdot 67 - 24 \cdot 120$$

Zato so vse rešitve enačbe $67x+120y=1$ oblike

$$x = 43 + 120k,\ y = -24 - 67k$$

rešitve enačbe $67x + 120y = 3$ pa oblike

$x = 3 \cdot 43 + 120k$, $y = -3 \cdot 24 - 67k$,
$x = 9 + 120l$, $y = -5 - 67l$

V teoriji kodiranja je zelo pomembno iskanje multiplikativnih inverzov iz obsega ostankov po praštevilskem modulu $\boldsymbol{Z}_p$, kjer je p praštevilo. Če je $m \in \boldsymbol{Z}_p \setminus \{0\}$, dobimo $m^{-1} \in \boldsymbol{Z}_p \setminus \{0\}$ kot rešitev diofantske enačbe

$$mx = 1 + py$$

Ker je p praštevilo, sta si števili m in p tuji in enačba je rešljiva s samo eno rešitvijo $x \in \{1,2, \ldots p - 1\}$.

Tako recimo inverz elementa 14 v obsegu $\boldsymbol{Z}_{23}$ dobimo z reševanjem diofantske enačbe

$$14x - 23k = 1$$

4 *To je verjetno prvi uvidel indijski matematik Brahmagupta (598-670).*

Iz Evklidovega algoritma za 14 in 23

$23 = 14 + 9$

$12 = 9 + 5$

$9 = 5 + 4$

$5 = 4 + 1$

dobimo:

$$1 = 5 - 4 = 5 - (9 - 5) = 2 \cdot 5 - 9 = 2 \cdot (14 - 9) - 9 =$$
$$= 2 \cdot 14 - 3 \cdot 9 = 2 \cdot 14 - 3 \cdot (23 - 14) = 5 \cdot 14 - 3 \cdot 23$$

Zato je 5 multiplikativni inverz elementa 14 v obsegu $\boldsymbol{Z}_{23}$. Res je $5 \cdot 14 = 70 = 1$.

ε Kitajski izrek o ostankih

V slavni klasični kitajski matematični knjigi *Devet poglavij matematičnih spretnosti* iz drugega stoletja, v kateri je zbrano kitajsko znanje matematike od 10. stoletja pr. Kr. naprej, je zapisana naslednja naloga:

> Skupina prijateljev prispeva za skupen nakup. Če vsak plača po 8 kovancev, zberejo tri kovance preveč. Če pa vsak da po 7 kovancev, zmanjkajo štirje. Poišči število prijateljev in znesek nakupa.

Z vidika stroge moderne matematike manjka še dodatna zahteva, da iščemo najmanjše možno število prijateljev v skupini. Rešitev sicer ni enolična.

Iščemo torej najmanjše naravno število, ki da pri delitvi z 8 ostanek 3, pri delitvi s 7 pa ostanek -4.

V knjigi je še več podobnih nalog, vse pa lahko posplošimo na reševanje sistema kongruenc:

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$\vdots$

$x \equiv a_k \pmod{m_k}$

Kitajski izrek o ostankih pove, da je ta sistem zagotovo rešljiv, če so moduli paroma tuji. Prvi algoritem za reševanje sistema je zapisal indijski matematik Aryabhata[5]. Zvito je ugotovil, da je treba rešitev x iskati v obliki

$x = x_1 m_2 m_3 \cdots m_k + x_2 m_1 m_3 m_4 + m_k + \cdots$
$+ x_k m_1 m_2 \cdots m_{k-1}$.

Vsak od seštevancev je deljiv z vsemi moduli, razen z enim, zato lahko problem prevedemo na reševanje več lažjih in manjših problemov oblike

$x_t m_1 \cdots m_{t-1} m_{t+1} \cdots m_k \equiv a_t \pmod{m_t}$, $1 \le t \le k$,

vsak od njih pa je ekvivalenten reševanju ustrezne linearne diofantske enačbe, ki jo lahko rešimo s pomočjo Evklidovega algoritma.

Pri naši kitajski nalogi torej rešujemo sistem kongruenc

$x \equiv -3 \pmod{8}$,

$x \equiv 4 \pmod{7}$.

Modula 8 in 7 sta si tuja, zato je sistem rešljiv. Rešitev iščemo z nastavkom

$x = 8x_1 + 7x_2$

pri čemer morata x_1 in x_2 ustrezati diofantskima enačbama

$8x_1 = 7k + 4$

$7x_2 = 8l - 3$.

Na enak način kot prej lahko najdemo rešitve teh diofantskih enačb:

$x_1 = 4 + 7m$, $k = 4 + 8m$,

$x_2 = 3 + 8n$, $l = 3 + 7n$,

zato je

$$x = 8(4 + 7m) + 7(3 + 8n) = 53 + 56(m + n).$$

5 *Aryabhata (476-550), indijski matematik*

Najmanjše naravno število, ki ustreza zgornji zahtevi, je $x = 53$. Če 7 prijateljev prispeva po 8 kovancev, je zbranih 56 kovancev za 3 preveč, če pa prispevajo po 7 kovancev, je zbranih 49 za 4 premalo.

γ Verižni ulomki

Evklidov algoritem za realna števila je na prvi pogled zelo nenavaden, je pa že Pitagorejcem služil za iskanje izjemno dobrih približkov korenov naravnih števil.

Poglejmo si, kako lahko najdemo zaporedne približke za $\sqrt{2}$.

Evklidov algoritem za $\sqrt{2}$ in 1 se sicer zaradi iracionalnosti števila $\sqrt{2}$ nikoli ne konča, a med računanjem opazimo zelo jasen vzorec:

$\sqrt{2} = 1 \cdot 1 + (\sqrt{2} - 1)$
$1 = 2 \cdot (\sqrt{2} - 1) + (3 - 2\sqrt{2})$
$\sqrt{2} - 1 = 2 \cdot (3 - 2\sqrt{2}) + (5\sqrt{2} - 7)$
$3 - 2\sqrt{2} = 2 \cdot (5\sqrt{2} - 7) + (17 - 12\sqrt{2})$
⋮

Sorazmernostne dvojke se v vseh naslednjih korakih ponavljajo. Posamezne korake algoritma bi lahko zapisali tudi drugače:

$$\sqrt{2} = 1 + \frac{1}{\frac{1}{\sqrt{2}-1}} = 1 + \frac{1}{2 + \frac{3-2\sqrt{2}}{\sqrt{2}-1}} =$$

$$= 1 + \frac{1}{2 + \frac{1}{2 + \frac{5\sqrt{2}-7}{3-2\sqrt{2}}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{17-12\sqrt{2}}{5\sqrt{2}-7}}}}} = \cdots$$

Običajno na kratko napišemo, da številu $\sqrt{2}$ ustreza periodičen neskončni *verižni ulomek*

$\sqrt{2} = [1; 2, 2, 2, \ldots] = [1; \overline{2}]$.

Ker se ostanki z vsakim korakom Evklidovega algoritma manjšajo, dobivamo čedalje boljše približke za $\sqrt{2}$:

$$\sqrt{2} \cong 1, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \cdots$$

Izkaže se, da se da vsak koren naravnega števila, ki ni popoln kvadrat, zapisati s periodičnim verižnim ulomkom, ki pa je lahko veliko bolj zapleten, recimo

$\sqrt{61} = [7; \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$.

Približki za korene z verižnimi ulomki so v vseh primerih zelo dobri. Zaporedna racionalna aproksimacija $\frac{a}{b}$ se od prave vrednosti korena razlikuje za manj kot $\frac{1}{b^2}$. Na primer:

$$\left|\sqrt{2} - \frac{17}{12}\right| < \frac{1}{12^2}$$

Z neskončnimi verižnimi ulomki se da napisati celo transcendentna števila, na primer
$\pi = [3; 7,15,1,292,1,1,1,2,1,3,1,14,2,1,1,2,2,2,2,...]$,

ki pa seveda nimajo periode. Presenetljivo lahko najdemo vzorec v verižnem ulomku za osnovo naravnega logaritma e:
$e = [2; 1,2,1,1,4,1,1,6,1,1,8,1,1,10,1,1,12,1,1,\ldots]$.

Naj bo n naravno število, ki ni popoln kvadrat. Diofantski enačbi

$x^2 - ny^2 = 1$

pravimo *Pellova enačba.*[6]

Enačbo lahko rešimo tako, da najprej z Evklidovim algoritmom poiščemo verižni ulomek za $\sqrt{n}$. Prvi od okrajšanih približkov $\frac{x}{y}$, ki jih dobimo z računanjem verižnega ulomka in ustreza Pellovi enačbi, je osnovna rešitev (x_1, y_1) enačbe. Vse druge rešitve (x_k, y_k) so z osnovno povezane z enačbo

6 *Enačbo je Euler pomotoma poimenoval po angleškem matematiku Johnu Pellu (1611-1685). Natančno je njene rešitve opisal William Brouncker (1620-1684), poznali pa so jih že indijski matematiki v 12. stoletju. V posebnih primerih so jo znali rešiti že Pitagorejci.*

$x_k + y_k\sqrt{n} = (x_1 + y_1\sqrt{n})^k$.

Na primer, pri reševanju enačbe
$x^2 - 7y^2 = 1$
si pomagamo z verižnim ulomkom
$\sqrt{7} = [2; \overline{1, 1, 1, 4}]$.

Med zaporednimi približki $\frac{2}{1}, \frac{3}{1}, \frac{5}{2}, \frac{8}{3}$, ... najdemo osnovno rešitev $x_1 = 8$, $y_1 = 3$. Ostale rešitve dobimo iz enakosti

$$x_k + y_k\sqrt{7} = (8 + 3\sqrt{7})^k.$$

η Posplošitve Evklidovega algoritma

Evklidov algoritem za naravni števili se vedno konča v končno korakih zato, ker se ostanki v vsakem naslednjem koraku algoritma strogo manjšajo. S to idejo lahko Evklidov algoritem izvajamo tudi v veliko bolj splošnih algebrskih strukturah.

Naj bo $\boldsymbol{N}$ množica naravnih števil in K komutativen kolobar. Kolobar K je e*vklidski kolobar*, če obstaja funkcija

$$\varphi: K\backslash\{0\} \to \boldsymbol{N} \cup \{0\}$$

z naslednjima lastnostma:

1. Če za $a, b \in K$ velja $ab \neq 0$, je $\varphi(a) \leq \varphi(ab)$.
2. Za $a, b \in K$, $b \neq 0$, obstajata elementa q, $r \in K$, tako da je $a = qb + r$. Pri tem je bodisi $r = 0$ bodisi $r \neq 0$ in $\varphi(r) < \varphi(b)$.

Druga lastnost nam zagotavlja, da lahko v kolobarju K izvajamo Evklidov algoritem, ki se konča po končno korakih.

Poglejmo si nekaj najpomembnejših primerov evklidskih kolobarjev.

Običajni Evklidov algoritem dobimo v primeru $K = \boldsymbol{Z}$ in $\varphi(x) = |x|$.

Zelo pomemben primer so polinomi v eni spremenljivki s koeficienti iz komutativnega obsega, na primer $\boldsymbol{R}[x]$. Za $\varphi(p)$ vzamemo stopnjo polinoma p.

Za ilustracijo z Evklidovim algoritmom poiščimo največji skupni delitelj polinomov $x^4 + x^3 + 2x^2 - 1$ in $x^2 + x - 1$:

$$x^4 + x^3 + 2x^2 - 1 = (x^2 + 3)(x^2 + x - 1) + (-3x + 2)$$

$$x^2 + x - 1 = \left(-\frac{1}{3}x + \frac{1}{9}\right)(-3x + 2) - \frac{11}{9}$$

$$-3x + 2 = \left(\frac{27}{11}x - \frac{18}{11}\right)\left(-\frac{11}{9}\right)$$

Njun največji skupni delitelj je konstanta, zato sta si polinoma tuja.

Na enak način kot v celih številih lahko s pomočjo Evklidovega algoritma rešujemo tudi polinomske linearne diofantske enačbe in si z njim pomagamo pri uporabi kitajskega izreka o ostankih. Algoritem nam pomaga tudi pri tvorbi *Sturmovega zaporedja*[7], ki nam prešteje realne ničle polinoma na danem intervalu.

Podmnožici kompleksnih števil $\boldsymbol{Z}[\mathrm{i}] = \{a + bi;\ a, b \in \boldsymbol{Z}\backslash\}$, opremljeni z običajnima operacijama, pravimo *Gaussova števila*[8]. Za funkcijo φ vzamemo običajno razdaljo kompleksnega števila od izhodišča:

$$\varphi(a + bi) = a^2 + b^2 .$$

Zanimivo je, da se da s pomočjo obravnave kolobarja $\boldsymbol{Z}[\mathrm{i}]$ dobiti nekaj pomembnih lastnosti običajnih celih števil, ki bi jih bilo težko dokazati neposredno. Z Gaussovimi števili se da recimo zelo elegantno poiskati Pitagorejske trojice. Prav tako se da pokazati, da je možno praštevila, ki dajejo pri deljenju s 4 ostanek 1, napisati kot vsoto dveh celoštevilskih kvadratov.

7 *Jacques Charles François Sturm (1803-1855), francoski matematik*

8 *Carl Friedrich Gauss (1777-1855), nemški matematik, astronom in fizik*

V teoriji števil so pomembna tudi podobno skonstruirana *Eisensteinova števila*[9] oblike

$$z = a + b\omega, a, b \in \mathbf{Z}, \omega = \frac{1}{2}(-1 + i\sqrt{3})$$

z ustrezno funkcijo $\varphi(a + b\omega) = a^2 - ab + b^2$.

Vsako naravno število se da na le en način napisati kot produkt potenc praštevil (pravimo, da je $\boldsymbol{K}$ kolobar kolobar z *enolično faktorizacijo*). Prav tako drži zanimivo dejstvo, da za naravni števili in z največjim skupnim deliteljem D velja

$$\{am + bn; a, b \in \mathbf{Z}\} = \{cD; c \in \mathbf{Z}\}$$

(rečemo, da je kolobar $\boldsymbol{Z}$ *glavni*). V bolj splošnih algebrskih strukturah veljajo le inkluzije: vsak evklidski kolobar je glavni, vsak glavni kolobar pa je kolobar z enolično faktorizacijo.

φ Časovna zahtevnost Evklidovega algoritma

Zaradi široke uporabnosti Evklidovega algoritma v računalništvu je zelo pomembna tudi njegova časovna zahtevnost. Algoritem za naravni števili $n > m$ se konča prej kot v $5d$ korakih, kjer je d število števk števila m.[10] Zanimivo je, da algoritem poteka najpočasneje v primeru dveh zaporednih elementov Fibonaccijevega[11] zaporedja. Povprečno število korakov Evklidovih algoritmov za vse pare (m, n), $m < n$, je približno $0{,}843 \cdot \ln n$.

λ Zaključek

Evklidov algoritem je lep primer, kako pogosto za na videz standardno, rutinsko in ne preveč impresivno temo iz srednješolskega kurikuluma stoji navdušujoča zgodovina izjemnih idej, ki so jih skoraj istočasno zaradi praktičnih potreb neodvisno odkrivale različne civilizacije. Osnovne ideje ljudstev, ki abstrakcije niti niso znali zapisati v simboličnem zapisu, so postale temelji moderne matematike.

Zato upam, da bo pričujoči prispevek služil tudi kot ena od idej, kako matematiko na zanimiv način približati srednješolcem.

9 *Ferdinand Gotthold Max Eisenstein (18231852), nemški matematik*

10 *Gabriel Leon Jean Baptiste Lamé (1795-1870), francoski matematik*

11 *Leonardo Pisano Bigollo-Fibonacci (1170-1250), italijanski matematik. Fibonaccijevo zaporedje lahko definiramo z dvočleno rekurzivno zvezo* $F_{n+2} = F_{n+1} + F_n$ *in začetnima členoma* $F_1 = F_2 = 1$.

δ Viri in literatura:

1. W. S. Anglin, *Mathematics: a concise history and philosophy*, Undergraduate Texts in Mathematics, Readings in Mathematics, Springer-Verlag, New York, 1994.
2. T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1974.
3. J. J. Tattersall, *Elementary number theory in nine chapters*, Cambridge University Press, 1999.
4. I. Vidav, *Algebra*, 4. natis, DMFA, Ljubljana, 1989.
5. The Mac Tutor History of Mathematics archive, http://www-history.mcs.st-and.ac.uk/, citirano 11. 10. 2012.