30. MEZINÁRODNÍ KONFERENCE

HISTORIE MATEMATIKY

Jevíčko, 21. 8. – 25. 8. 2009

Praha **2009**

Památce

Jaroslava Šedivého

(1934–1988)

zakladatele konferencí Historie matematiky

ISBN 978-80-7378-092-0

AKO RÝCHLO VIEME A MÔŽEME NÁSOBIŤ

ŠTEFAN PORUBSKÝ

Abstract: In the paper we shall review some methods used for the multiplication in the past, compare them with the usual algorithm, and show their influence on the analysis of complexity of arithmetic operations.

1 Z histórie pojmu a používania násobenia

Násobenie je jedna zo základných aritmetických operácií, medzi ktoré dnes počítame sčítanie, odčítanie, násobenie, delenie a umocňovanie. Presný počet základných aritmetických operácií bol rôzny v rôznych dobách a u rôznych autorov. Ako operácie s číslami sa v priebehu vývoja najčastejšie udávalo týchto 5 operácií: numerácia[1], sčítanie, odčítanie, násobenie a delenie. Sacrobosco (asi 1195 – asi 1256) vo svojom diele *Algorismus* (zvanom tiež *Algorismus de integris* alebo *Algorismus vulgaris*[2]) rozoznáva dokonca 9 aritmetických operácií: numerácia, sčítanie, odčítanie, pólenie, zdvojovanie, násobenie, delenie, sčítanie aritmetických postupností (operácia zvaná progressio), druhú a tretiu odmocninu.[3] Táto kniha bola úvodom do elementárnej aritmetiky a prakticky prvou univerzitnou učebnicou zavádzajúcou indicko-arabské číslice a počítanie a hojne sa používala v stredoveku (dielo malo niekoľko vydaní medzi rokmi 1488 a 1582).

Latinské slovo *multiplicatio* vzniklo zložením slov *multus* (mnohý, početný) a *plicare* (zložiť). Ide o latinskú formu gréckych slov πολνπασιάζειυ alebo πολλαπλασιάζειυ. Prvé z nich používal Euklid a Diofant, druhé Herón, ale napr. Pappus používal obidva výrazy. V latinských textoch je násobenie avizované pomocou *ducere in* (vtiahnuť do) a v taliančine pomocou *moltiplicare via* [G, zv. II, str. 216]. Tieto výrazy sa postupom času zredukovali na *in* alebo *via*. Napríklad F.Viète zapisuje súčin A a B pomocou „A *in* B“. Podľa [16] *násobení v mathematice jest základní úkon početní, kterým hledáme součet dvou n. několika čísel stejné velikosti*. Z etymologického hľadiska pod slovom *násobit* nájdeme v [20], že *násob* je staročeské *krát*, a že *násobeno* vzniklo z pôvodního *na sobě*, a tak *trojnásobný je vlastně trojí na sobě*. Podľa [15] toto slovo *vyjádřuje vzájemný poměr mezi aspoň dvěma předměty, jako by ležely „na sobě“, ve stejné podobě ve 2, 3 at. exemplářích*.

V tzv. trevízskej aritmetike[4] *Arte dell'Abbaco* je násobenie definované takto: *pochopiť ho [tj. násobenie] je nutné vedieť, že násobiť jedno číslo samo sebou, alebo iným číslom,*

---

[1] Napr. v renesancii operácia numerácie zahrnovala aj proces učenia sa číselných symbolov, čo bolo typické pre obdobie zavádzania indicko-arabského spôsobu zapisovania čísiel a počítania, viď tiež [13].

[2] Sacrobosco odôvodňuje názov diela nasledovne: Hanc igitur scientiam numeraci compendiosam eidam philosophus edidit nomine ALGUS, unde et Algoritmus nunciatur, vel ars numeraci, vel ars inductia in numerum interpretatur (tu ALGUS znamená Al Chvárizmí).

[3] Na Sacroboscov Algorismus úzko naväzuje napr. aj najstarší zachovalý čisto matematický rukopis českého pôvodu *Algorismus prosaycus* [13], ktorý obsahuje aritmetické výklady Křišťana z Prachatic jedného z najvýznamnějších profesorov pražskej univerzity konca 14. a prvej polovice 15. stor.

[4] Asi najstaršia známa tlačená kniha „kupeckých počtov“, ktorá propaguje indicko-arabský spôsob počítania. Vyšla v r. 1478 a je napísaná v benátskom dialekte.

znamená nájsť z dvoch daných čísel tretie, ktoré obsahuje jedno z týchto čísiel toľkokrát, koľko je v tom druhom jednotiek.

Znak $\times$ pre násobenie sa po prvýkrát[5] objavuje v r. 1631 v diele *Clavis mathematicae* od Williama Oughtreda (1574–1660). Bodka ako znak pre násobenie sa objavuje v liste Leibniza Johannovi Bernoullimu zo dňa 29.7.1698, ale používala sa príležitostne už aj predtým, napr. Th. Harriot v *Artis analyticae praxis* z r. 1631 píše $aaa - 3 \cdot bba = +2 \cdot ccc$.

2 Niektoré historické formy násobenia

2.1 Egyptské násobenie

Písmo sa objavilo asi 4000 rokov pr.n.l. v Mezopotámii a asi 3200 rokov pr. n. l. v Egypte [24]. Najjednoduchší systém na zapisovanie čísiel je unárny systém. V tomto systéme je každé prirodzené číslo reprezentované odpovedajúcim počtom istých symbolov, napr. | . Systém tohto typu je vhodný len pre zaznamenávanie malých čísiel. Pre zaznamenanie väčších hodnôt sa potom používajú zvláštne symboly pre isté hodnoty a konkrétne hodnoty sa potom zaznamenajú aditívne pomocou zoskupovania takýchto symbolov[6]. Typickým predstaviteľom takéhoto tzv. *aditívneho systému* je systém používaný v starom Egypte. Aditívny systém zápisu čísiel je vhodný najmä pre operácie sčítania a odčítania. Násobenie, ktoré je vo svojej podstate skrátená forma opakovaného sčítania, je možné v jeho najprimitívnejšej forme realizovať tak, že symboly reprezentujúce násobenca[7] zopakujeme v počte odpovedajúcom násobiteľovi, a vo vzniknutom zoskupení znakov potom zoskupíme a v prípade potreby ich preskupíme postupne do vyšších rádov. V násobení, ktoré demonštrujú egyptskí pisári je použitý skrátený spôsob, v ktorom počet odpovedajúci násobiteľovi sa získava pomocou zdvojovania, alebo dokonca pomocou päť- alebo desaťnásobku (pre detaily viď. napr. [1], str. 41.

Prirodzená otázka je, ako bolo možné takýto spôsob násobenia objaviť. Jedna veľmi prirodzená teória dáva toto násobenie do súvisu s vážením na rovnoramenných váhach [11]. Takéto váhy sú známe už z predhistorických dôb a môžeme ich nájsť aj na staroegyptských reliéfoch ako nástroj na váženie duší po smrti. Najjednoduchším spôsob ako dostať závažie hodnoty $a2^{n-1}$ je nasledujúci: položíme do jednej misky závažie váhy a v druhej ho vyvážime do rovnováhy. Preložíme závažie do druhej misky a po vyvážení na druhej strane máme váhu $2a$. Opakovaním postupu dostaneme postupne závažia $a, 2a, 4a, 8a, \ldots, 2^{n-1}a$. V tomto štádiu odvážime akúkoľvek váhu ab, kde b má n (binárnych) cifier výberom patričnej kombinácie závaží zo skupiny $a, 2a, 4a, 8a, \ldots, 2^{n-1}a$, ktorá dáva v súčte b. Od tejto praktickej skúsenosti k egyptskému násobeniu je len krôčik.

Egyptská forma násobenia je pravdepodobne veľmi stará a násobenie pripisované Egypťanom, sa u mnohých autorov nazýva *etiópskym násobením*, pretože s týmto spôsobom

---

[5] Všeslovanké spojenie *-krát* je odvodené od praslovanského slova *kert*, ktoré pôvodne označovalo *sekať*, a používalo sa aj v zmysle *vrub*, pomocou ktorého sa v minulosti zaznamenával počet [7], [20].

[6] Nie je bez zajímavosti poznamenať, že 5 nezapisovali v tvare ||||| ale ||| || alebo $\begin{matrix}|||\\||\end{matrix}$.

[7] V latinských dielach sa činitele nazývali: *numerus multiplicandus*, *numerus multiplicans* a výsledok *numerus productus*. Pozdejšie sa slovo numerus z týchto väzieb vytratilo.

násobenia oboznámili Egypťanov údajne tzv. etiópske kmene (o roli Ethiopians viď napr. [9]). Operáciu zdvojovania a pólenia uvádza ako samostatné operácie aj Al Chvárizmí vo svojom diele *Algoritmi de numero Indorum*[8]. Ján (Juan) zo Sevilly (Johannes Hispalensis alebo Johannes Hispaniensis), ktorý žil v 12. stor. (zomrel asi r. 1153 [6]) poukazuje na to, že zdvojovanie je druh násobenia a pólenie je druh delenia, ale ich uvedenie ako samostatných operácií je zdôvodniteľné skutočnosťou, že výpočet druhej odmocniny vyžaduje zdvojovanie a pólenie [3], [10].

Trošku sofistikovanejšie je tzv. *ruské (sedliacke) násobenie*[9]. V tomto prípade nie je nutné hľadať riadky, ktorých mocniny dvojky v prvom dávajú násobiteľa, ale postup je zautomatizovaný pomocou tzv. pólenia, tj. delenia dvomi, pričom v prípade delenia nepárneho čísla sa výsledok berie len podiel a zvyšok 1 sa neberie do úvahy, a sčítajú sa dvojnásobky odpovedajúce riadkom s neúplným delením. Napr. [18], pri výpočte súčinu 13×15 postup vyzerá nasledovne[10]

egyptský spôsob			ruský spôsob		
\	1	15	\	13	15
	2	30		6	30
\	4	60	\	3	60
\	8	120	\	1	120
		195			195

Aj keď sa tento spôsob násobenia sa zdá jednoduchší, než ten čo používame v súčasnosti v bežnom živote my, je matematická zložitosť obidvoch metód rovnaká [11].

2.2 Indicko-arabské násobenie

Masové rozšírenie papieru približne od 12. stor. sa prejavilo aj v spôsobe prevádzania výpočtov. Písaná forma umožňujúca zachovať pred očami celý postup výpočtu a tým i jeho kontrolu, prispela, aj keď veľmi pomaly, k presadeniu sa pozičného zápisu pomocou arabských číslic. V počiatočných etapách narážali indicko-arabské číslice, akože pochádzajúce od muslimov a židov[11], najmä na odpor cirkvi, aj keď aj tu existovali výnimky. Napr. pápež Silvester II[12] (946–1003) presadzoval arabskú vzdelanosť a vedomosti, aj keď nie s veľkým úspechom.

Propagácia indického pozičného zápisu a výpočtu (tzv. *modus Indorum*) čísel v Európe je obyčajne spojovaná s Fibonacciho *Liber Abbaci*. Ovšem jeden z prvých

---

[8] Toto dielo Al Chvárizmího sa zachovalo len v latinskom preklade a nemá názov. Názov *Algoritmi de numero Indorum* mu dal Baldassarre Boncompagni v r. 1857.

[9] Ruské preto, lebo po rozšírení vzdelanosti a indicko-arabského spôsobu násobenia, ktoré sa dnes učíme v škole, západná časť Európy na tento spôsob násobenia zabudla, a s „velkým“ prekvapením ho znovu objavila v 19. stor. v Rusku, kde ho bežne používali mužíci. Uvedomme si, že toto násobenia nevyžaduje znalosť malej násobilky, ktorú nás naučila povinná školská dochádzka.

[10] Toto násobenie nájdeme aj v spomínanom rukopise *Algorismus prosaycusi.*

[11] Pomenovanie *arabské číslice* podľa Sartona [21], zv. 2, str. 618, bolo odvodené od Sacroboscovej poznámky v *Algoritme*: Sinistrorsum autem scribimus in hac arte arabico sive iudaico, huius scientiae inventorum. (Píšeme tu doľava podľa spôsou Arabov alebo Židov objaviteľov tejto vedy).

[12] Mimochodom prvý pápež francúzskeho pôvodu. Študoval v Španielsku v Barcelone a u arabských učiteľov v Cordobe a Seville. Napísal niekoľko vedeckých traktátov a údajne vynašiel kyvadlové hodiny.

popisov indického pozičného systému v Európe je v knihe *Liber algorismi* od Jána zo Sevilly[13] [3]. Popis ako násobili starí Indovia nájdeme v [23].

Nie je možné na tomto mieste uviesť všetky formy násobenia, ktoré sa v minulosti používali. Napr. Luca Pacioli (1445–1517) vo svojej *Summa de Arithmetica, Geometria, Proportioni e Proportionalita* (vyšla 1494 a 1523) uvádza 8 spôsobov násobenia pomocou indicko-arabských cifier, a Pietro Antonio Cataldi (1548–1626) v diele *Prima Parte della Pratica Aritmetica* z r. 1602 uvádza ďalšie tri spôsoby.

2.3 Cauchyho komplementárne násobenie

Podľa Cauchyho je možné súčin dvoch čísiel xy vypočítať najpohodlnejšie pomocou tzv. *komplementárneho násobenia* [4]: najprv vytvorme súčet $x+y$ a tento rozložme iným spôsobom na súčet dvoch čísiel $x+y=x'+y'$. Potom $xy=x'y'+(x-x')(y-x')$ a tiež $xy=x'y'+(x-y')(y-y')$. S využitím týchto vzťahov napr. súčin 23×67 môžeme spočítať takto: $23+67=30+60$ a tento rozklad vedie na postup $23\times67=30\times60+(23-30)(67-30)=1800-7\times37=1800-259=1541$ (skúste rozklad $23+67=40+50$).

Špeciálnym prípadom komplementárneho násobenia je nasledujúca forma: Napíšme $x=z+a$, $y=z+b$ a zvoľme v predchádzajúcom postupe $x'=2z$, $y'=a+b$, čím dostaneme $x\times y=2z(a+b)+(z-a)(z-b)$.

V prípade voľby $z-5$ dostaneme pravidlo zvané *regula ignavi*, t.j. vzorec $(5+a)(5+b)=10(a+b)+(5-a)(5-b)$, ktoré nám umožňuje redukovať malú násobilku 10×10 na znalosť „menšej“ násobilky 5×5. V interpretácii pomocou počítania na prstoch dostaneme tzv. cigánske násobenie, napr. $7\times8=10(2+3)+(5-2)(5-3)$.

2.4 Kulikovo dvojciferné násobenie

Ak zvolíme $z=100$ v predchádzajúcej forme násobenia, potom pre súčiny do velikosti 200×200 nám stačí mať k dispozícii tabuľky súčinov do 100×100. Je okamžite jasné, že pokiaľ by sme vedeli naspamäť namiesto malej násobilky, „veľkú“ násobilku 100×100 budeme schopní analogickým spôsobom k tomu, čo používame na násobenie násobiť ľubovoľne veľké čísla tak, že budeme násobiť po dvojiciach s využitím sady tabuliek umiestnených na 13 stranách, ktoré vydal J. Ph. Kulik knižne [14][14]. Princíp použitia je v tom, že namiesto toho aby sme vynásobili dve 2-miestne čísla (čo vyžaduje 4 násobenia a 3 sčítania) vezmeme výsledok z tabuliek. Napr. ak chceme vynásobiť 1743×37 môžeme postupovať takto (každý medzivýsledok v riadku je vzatý z tabuliek):

$43\times37=$ 1591
$17\times37=$ 629
630591

[13] Dielo je rozšíreným spracovaním Al Chvárizmího *Algoritmi de numero Indorum*. Rozšírenie je možno skoršieho dáta. Podľa [5] v Erfurte existuje rovnaký rukopis, kde ako prekladatel je uvedený Gerhard z Cremony (Gherardo da Cremona alebo Gerard Cremonensis, žil 1114–1187) [10].

[14] Knižočka sa predávala za tretinu toliara a zisk z predaja šiel na podporu obyvateľov Krakova poškodených požiarom 18. a 19. júla 1850.

Kulik samozrejme udáva aj postup, ako môžeme pomocou týchto tabuliek deliť. „Energetická“ úspora pri počítaní je „akumulovaná“ v pripravených tabuľkách. Tabuľky tohto druhu sa potom na prelome 19. a 20. stor. objavili v podstatne väčšom rozsahu.

2.5 Tabuľky štvrťkvadrátov

Už starí Babylóňania poznali tieto algebraické vzorce $ab = \frac{1}{2}((a+b)^2 - a^2 - b^2)$ a $ab = \frac{1}{4}((a+b)^2 - (a-b)^2)$. Ich moderný matematický význam z hľadiska analýzy zložitosti násobenia ukazuje, že zložitosť násobenia sa rovná zložitosti umocňovania na druhú. To znamená, že keby sme boli schopný rýchle umocňovať, môžeme aj rýchle násobiť (a samozrejme aj naopak). J. Ph. Kulik v druhej časti knihy [14] zostavil tabuľky, o ktorých v úvode píše: *Usporiadanie druhej tabuľky je založené na doposiaľ nepoužitom šikovnom nápade, pomocou ktorého sa súčin dvoch čísiel prevedie na rozdiel dvoch čísiel získaných z tabuľky. .... K tomu, aby sme pre dva dané čísla pomocou tabuľky našli ich súčin, musíme ich najprv sčítať a jedno od druhého odpočítať. Dostaneme dve nové čísla, na ktoré použijeme tabuľku, a preto ich nazveme argumenty tabuľky. ....* (Pre nedostatok miesta odkazujeme čitateľa buď na [14] alebo na [19] pre ďalšie podrobnosti.)

Kulik tvrdí, že jeho nápad je nový a doposiaľ nepoužitý. V úvode píše, že o nápade, na ktorom sú tabuľky založené po prvýkrát informoval už v r. 1833. Je síce možné, že o tom naozaj nevedel, ale skutočnosť je pre neho krutá. Podľa úvodu v [2] *Aj keď Ludolf už v r. 1680 vo svojej Tetragonometrii a po ňom C. Séguin v Paríži v r. 1801 dávajú návod, ako využiť tabuľky štvorcov pre účely násobenia, trvalo to ďalších 15 rokov kým inžinier Anton Voisin v Nismes vydal v r. 1816 prvé multiplikačné tabuľky tohto druhu.*[15]

3 Efektívnejšie formy násobenia

História a každodenná skúsenosť ukazujú, že násobenie je náročná operácia, či už na počet úkonov, ktoré si vyžaduje, ale aj na „priestor“ ktorý zaberá. Okrem toho vyžaduje prípravné vedomosti, napr. znalosť násobenia dvomi, alebo malú násobilku, a pod. Preto sa ľudia snažili v celej histórii nájsť jeho čo najjednoduchšiu formu. V nasledujúcich riadkoch si uvedieme len zlomok z takýchto nápadov. Prirodzená otázka, ktorá pritom vyvstane znie, je historický vývoj aj cestou k väčšej efektivite? Inými slovami je tá forma násobenia, ktorá sa presadí voči staršej „menej namáhavá“? Jedným z veľmi zaujímavých poučení, ktoré nám priniesol rozvoj výpočtových metód je poznatok, že efektívnosť foriem základných algoritmov, ktoré používame (a učíme) pre takú základnú operáciu ako násobenie, je veľmi malá. V jazyku modernej matematiky má školské násobenie[16] dvoch n-miestnych čísiel zložitosť $O(n^2)$. V nasledujúcich riadkoch naznačíme myšlienky, ktoré otvorili cestu k metódam, pomocou ktorých dnes vieme vynásobiť dva takéto čísla so zložitosťou $O(n(\log n)(\log\log n))$. Podrobnejšiu analýzu rôznych foriem násobenia nájde čitateľ napr. v [12].

3.1 České násobenie

Trošku nepovšimnuté zostalo násobenie navrhnuté Svobodom a Valachom [22] a Kolmogorovom pomenované ako *české* [11]. Neskoršie bolo nezávisle objavené

[15] Žiaľ, je tu aj odkaz, že Kulikove tabuľky obsahujú 30 chýb.
[16] T.j. ten známy spôsob násobenia, ktorý sa učíme v školách

Garnerom v r. 1959 (viď [12]). Jedná sa formu násobenia, ktorú dnes nazývame *modulárnym násobením*. Činitele sa zredukujú modulo vhodne zvolených modulov, získané hodnoty sa vynásobia a pomocou čínskej zvyškovej vety sa získaný súčin „zdvihne“ do hodnoty skutočného súčinu. Aj keď sa táto myšlienka zdá komplikovaná, v celkovom hodnotení jej zložitosti je výhodnejšia než štandardne používané násobenie. Pre detaily čitateľa odporúčame na [11], [12], [22].

3.2 Karacubovo násobenie

Na jeseň r. 1960 na seminári na moskovskej univerzite zopakoval Kolmogorov svoju hypotézu, že zložitosť násobenia je $O(n^2)$. V priebehu 1 týždňa mladý poslucháč A. A. Karacuba s použitím veľmi jednoduchej myšlienky našiel spôsob násobenia, ktorého zložitost bola $O(n^{\log_2 3})$. Keďže $\log_2 3 = 1{,}5849\ldots < 2$, Kolmogorova hypotéza bola vyvrátená [11]. Myšlienka dôkazu bola extrémne jednoduchá. Súčin dvoch $2n$-miestnych binárnych čísiel vynásobme nasledovne: $(2^n a_1 + a_2)(2^n b_1 + b_2) = (2^{2n} + 2^n)a_1 b_1 + 2^n (a_1 - a_2)(b_2 - b_1) + (2^n + 1)a_2 b_2$. To znamená, že potrebujeme vynásobiť len tri namiesto štyroch n-miestnych čísiel!!! Objav odštartoval novú éru v analýze efektívnosti základných aritmetických operácií a v metódach používaných na násobenie veľkých čísiel.

Literatura

[1] Bečvář J., Bečvářová M., Vymazalová H.: *Matematika ve starověku. Egypt a Mezopotámie*. Dějiny matematiky, zv. 23, Prometheus, Praha, 2003.

[2] Blater J.: *Tafel der Viertel-Quadrate aller ganzen Zahlen von 1 bis 200 000 welche die Ausführung von multiplikationen, Quadrirungen und das Ausziehen der Quadratwurzel bedeutend erleichtert und durch vorzügliche Correctheit fehlerlose Resultate verbürgt*. Wien, 1887.

[3] Boncompagni B.: *Tratatti d'Aritmtica publicati da Baldassare Boncompagni. I. Algoritmi de numero indorum. II. Joanni Hispalensis liber algorismi de practica Arismetrice*. Roma, 1857.

[4] Cauchy A.-L.: *Sur les moyens d'éviter les erreurs dans les calculs numériques*. Comp. Rendus 11(1840), 431–442

http://mathdoc.emath.fr/cgi-bin/oetoc?id=OE_CAUCHY_1_5.

[5] Eneström G.: *Über den Bearbeiter oder Übersetzer des von Boncompagni (1857) herausgegebenen ‹Liber algorismi de practica arismetrice›*. Bibliotheca mathematica, séria 3, zv. VI, 1905, str. 114.

[6] Gericke H.: *Mathematik in Antike und Orient*. Fourier Verlag GmbH, Wiesbaden, 2004.

[7] Holub J., Lyer S.: *Stručný etymologický slovník jazyka českého*. SPN, Praha, 1978.

[8] Al Chvárizmí: *Aritmetický a algebraický traktát*. Edícia Prameny evropské vzdělanosti, OPS, 2009.

[9] Jackson J. G.: *Ethiopia and the origin of civilization*. [cit. 7. 6. 2009] http://www.africawithin.com/jgjackson/jgjackson_ethiopia_and_the_origin.htm.

[10] Juškevič A. P., Rozenfeld B. A.: *Poznámky k aritmetickému traktátu* (rusky). In Muhammad ibn Musa al-Chorezmi, *Matematické traktáty*, Vydavateľstvo FAN Uzbeckej SSR, Taškent, 1983.

[11] Karacuba A. A.: *The complexity of computation*. Proc. Steklov Inst. Math. 211(1995), 169–183.

[12] Knuth D. E.: *The Art of Computer Programming volume 2: Seminumerical algorithms*. (3rd ed.) Addison-Wesley, Boston etc., 1998.

[13] Křišťan z Prachatic: *Základy aritmetiky*. Oikoymenh, Praha, 1999 (Edícia latinského textu *Algorismus prosaycus* s českým prekladom, českou a nemeckou úvodnou štúdiou a s poznámkami Z. Silagiovej).

[14] Kulik J. Ph.: *Neue Multiplikations-Tafeln*. Ein unentbehrliches Hülfstmittel für Jedermann, um schnell, sicher und ohne Ermüdung zu rechnen. Leipzig, 1851, XII + 56 stran.

[15] Machek, V.: *Etymologický slovník jazyka českého a slovenského*. Nakladatelství ČSAV, Praha, 1957.

[16] *Ottův slovník náučný*. Praha, 1900.

[17] Pope Sylvester II, Catholic Encyclopedia. http://www.newadvent.org/cathen/14371a.htm [cit. 8. 6. 2009]

[18] Porubský Š.: *Peasant Multiplication*. *Interactive Information Portal for Algorithmic Mathematics.* Institute of Computer Science of the Czech Academy of Sciences, Prague, Czech Republic, web-page http://www.cs.cas.cz/portal/AlgoMath/NumberTheory/Arithmetics/Multiplication/PeasantMultiplication.htm.

[19] Porubský Š.: *Jakob Phillip Kulik – ein vergessener Rechenkünstler*. In ALGORISMUS 43. *Tagung zur Geschichte der Mathematik* (Roloff H., Weidauer M. (eds.), Rauner, Augsburk, 2004, 307–328.

[20] Rejzek J.: *Český etymologický slovník*. Leda, 2008.

[21] Sarton G.: *Introduction to the History of Science*. Carnegie Institution, Washington, Baltimore, 1927–1948.

[22] Svoboda A., Valach M.: *Operátorové obvody*. Stroje na zpracování informací 3(1955), 247–295.

[23] Sýkorová, I.: *Násobení ve středověké Indii*. In Historie matematiky. 29. Mezinárodní konference, Velké Meziříčí, 22. – 26. 8. 2008, 161–165.

[24] Wikipedia (The free encyclopedia): *Writing* [online]. Posledná revízia 25. mája 2009 o 09:09 [cit. 5. 6. 2009]. http://en.wikipedia.org/wiki/Writing#cite_note-8.

Adresa

Prof. RNDr. Štefan Porubský, DrSc.
Ústav informatiky AV ČR, v.v.i.
Pod Vodárenskou věží 2
182 07 Praha 8 – Libeň
e-mail: *porubskys@cs.cas.cz*