PŘEDMLUVA

Ach, drahá Ofélie!
Nevyznám se v básnění;
nedovedu počítat [své vzdechy].

— HAMLET (Jednání II, obraz 2, řádek 120). Překlad František Nevrla

ALGORITMY probírané v této knize pracují přímo s čísly; přesto se domnívám, že je správné označit je jako *seminumerické*, protože se nacházejí na hranici mezi numerickými (číselnými) a symbolickými výpočty. Každý z těchto algoritmů nejenže vypočte požadovanou odpověď na daný numerický problém, ale také by měl být v souladu s vnitřními mechanismy digitálního počítače. V mnoha případech nedokážou lidé ocenit úplnou krásu takového algoritmu, dokud sami neznají alespoň trochu strojový jazyk počítače; efektivita příslušného počítačového programu je důležitým faktorem, který nemůžeme od samotného algoritmu odloučit. Problém tedy zní: najít nejlepší způsoby zpracování čísel v počítači. K tomu budeme potřebovat taktické i numerické úvahy. Téma tohoto svazku knihy je proto nepochybně součástí jak informatiky, tak i numerické matematiky.

Někteří lidé, kteří pracují ve „vyšší úrovni“ numerické analýzy, budou zde probíraná témata považovat spíše za záležitost systémových programátorů. Jiní lidé, kteří se pohybují naopak ve „vyšší úrovni“ systémového programování, je budou zařazovat do numerické analýzy. Věřím ale, že existuje také malá, přesto významná množina lidí, pro něž bude detailní studium těchto základních metod zajímavé. Uvedené metody operují sice na poměrně nízké úrovni, jsou ale základem všech „vznešenějších“ aplikací počítačů na numerické problémy, a proto je důležité je znát. Zde se tedy pohybujeme na pomezí mezi numerickou matematikou a programováním počítačů, a právě díky kombinaci obou typů dovedností je toto téma tak zajímavé.

Vzhledem k povaze probíraných témat najdete v tomto svazku celé série významně vyšší podíl matematické látky než v ostatních. Ve většině případů odvozujeme potřebná matematická témata téměř od základů (nebo od výsledků dokázaných ve svazku 1), avšak v několika snadno patrných částech předpokládáme znalosti diferenciálního a integrálního počtu.

Tento svazek obsahuje kapitoly 3 a 4 z celé série. Kapitola 3 se zabývá „náhodnými čísly“: studuje nejen různé způsoby generování náhodných posloupností, ale také vyšetřuje statistické testy náhodnosti a transformace rovnoměrně rozdělených náhodných čísel do jiných typů náhodných veličin – tak si ukážeme aplikaci

náhodných čísel v praxi. Do textu jsem zahrnul také zvláštní část o samotné povaze náhodnosti. V kapitole 4 se pokouším vyprávět fascinující příběh objevování procesů aritmetiky, který se odehrává již dlouhá staletí. Rozebereme zde různé systémy reprezentace čísel a jejich vzájemné převody; budeme se zabývat aritmetickými operacemi nad čísly s pohyblivou řádovou čárkou, nad celými čísly ve vysoké přesnosti, nad racionálními zlomky, polynomy a mocninnými řadami, včetně otázek rozkladu na prvočinitele a hledání největších společných dělitelů.

Jednu i druhou kapitolu (3 a 4) je možné vzít za základ jednosemestrálního vysokoškolského kursu bakalářského nebo magisterského studia. Kursy „náhodných čísel“ a „aritmetiky“ dnes sice v mnoha studijních programech chybí, podle mého názoru nicméně čtenář sám přijde na to, že se text velmi dobře hodí k jednotnému výkladu témat a že má skutečnou vzdělávací hodnotu. Podle mých vlastních zkušeností jsou tyto kursy dobrým prostředkem pro zavedení elementární teorie pravděpodobnosti a teorie čísel. Téměř všechna témata, která se obvykle v takovýchto úvodních kursech probírají, jsou uváděna jako aplikovaná a právě zařazení jejich aplikací může být pro řadu studentů významnou motivací ke studiu a pochopení celé teorie. Navíc, v každé z kapitol najdete několik námětů k pokročilejším tématům, jež mohou u studentů podnítit zájem o další studium matematiky.

Celá tato kniha je z velké části nezávislá, kromě některých částí výkladu, kde se hovoří o počítači `MIX` probíraném ve svazku 1. Příloha B obsahuje přehled použitých matematických notací, z nichž některé se mírně liší od tvaru používaného v klasické matematické literatuře.

Předmluva ke třetímu vydání

Druhé vydání této knihy bylo dokončeno v roce 1980 a představovalo v té době první velkou zkoušku pro prototyp systému elektronického publikování nazývaný TEX a METAFONT. Nyní mohu s potěšením vzdát hold dovršenému vývoji těchto systémů: vracím se ke knize, která podnítila jejich vznik a formovala je. Přinejmenším jsem tak schopen dovést všechny svazky *Umění programování* do konzistentního formátu, jejž bude možné snadno přizpůsobit budoucím změnám v technologiích zobrazování a tisku. Díky novému uspořádání jsem do textu mohl začlenit tisíce zlepšení, na která jsem už dlouho čekal.

V tomto novém vydání jsem znovu prošel celý text slovo za slovem, pokusil jsem se zachovat mladickou nevázanost původních vět, a zároveň do nich vnést kousek úsudku zralého muže. Přidal jsem desítky nových cvičení a k desítkám jiných jsem doplnil nové a rozšířené odpovědi. Změny se zkrátka objevují všude, ale nejvýznamnější jsou v částech 3.5 (o teoretických zárukách náhodnosti), 3.6 (o přenositelných generátorech náhodných čísel), 4.5.2 (o binárním algoritmu největšího společného dělitele) a 4.7 (o vytváření a iteracích mocninných řad).

Kniha *Umění programování* je však stále ve vývoji. Výzkum seminumerických algoritmů se nadále řítí neuvěřitelnou rychlostí. V některých částech

uvidíte proto symbol „ve výstavbě“, kterým se omlouvám, že daný materiál není zcela aktuální. Mám plné šuplíky důležitého materiálu, který chci začlenit do posledního, nejslavnějšího, čtvrtého vydání Svazku 2, asi za 16 roků ode dnešního dne, ale nejprve musím dokončit svazky 4 a 5 a jejich vydání nechci odkládat více, než kolik je absolutně nezbytné.

Jsem neobyčejně vděčný stovkám lidí, kteří mi během posledních 35 roků pomohli sesbírat a vytříbit tento materiál. Většinu náročných prací na přípravě nového vydání zajistil Silvio Levy, jenž zodpovědně upravil elektronický text, a Jeffrey Oldham, který převedl téměř všechny původní ilustrace do formátu METAPOST. Opravil jsem veškeré chyby, na které mne upozornili čtenáři (a také několik chyb, jichž si kupodivu nevšiml nikdo), a s novým materiálem jsem se pokoušel nezanést chyby nové. Přesto vím, že v knize nějaké závady být můžou, a každou z nich chci opravit co nejdříve. Za každou odbornou, typografickou nebo historickou chybu proto s radostí vyplatím 2,56 dolaru tomu, kdo ji nalezne jako první. Webová stránka citovaná na stránce iv obsahuje aktuální seznam všech dosud oznámených chyb.

Stanford, California D. E. K.
červenec 1997

Jestliže příprava knihy trvala osm roků,
musel bych poděkovat příliš mnoha kolegům, písařkám,
studentům, učitelům a přátelům.
Kromě toho, nemám v úmyslu jako obvykle zbavit tyto osoby
odpovědnosti za chyby, které v tisku zůstaly.
Měli mi je opravit!
A někdy jsou dokonce odpovědní za myšlenky,
které se po dlouhé době ukážou být nesprávnými.
Přes to všechno ale svým spolubojovníkům děkuji.

— EDWARD F. CAMPBELL, JR. (1975)

‘Defendit numerus’, [v počtu je bezpečí]
je zásadou hlupáků;
‘Deperdit numerus’, [v počtu je zkáza]
zásadou moudrých.

— C. C. COLTON (1820)

POZNÁMKY KE CVIČENÍM

Cvičení v celé této sérii knih jsou vhodná k samostatnému studiu i pro výuku. Naučit se nějaké téma jen s tím, že si něco přečteme, ale nepokusíme se aplikovat poznatky na konkrétní problémy, je velmi obtížné, ne-li nemožné, protože teprve při cvičení plně pochopíme, co všechno jsme se naučili. Navíc, nejlépe se naučíme to, na co přijdeme sami. Proto tvoří cvičení velkou část tohoto díla; pokoušel jsem se v nich ale zachovat co nejvíce informativní hodnoty a současně volit takové problémy, které jsou zajímavé a poučné.

V mnoha knihách jsou lehká cvičení zamíchána přímo mezi ta nejobtížnější. To bývá někdy nešťastné, protože čtenáři rádi dopředu vědí, kolik jim řešení problému asi zabere – jinak mohou všechny problémy nakonec přeskočit. Klasickým příkladem této situace je kniha *Dynamic Programming*, kterou napsal Richard Bellman; je to důležité, průkopnické dílo, v němž jsou ovšem problémy na konci některých kapitol sepsány pod jednotný nadpis „Exercises and Research Problems“, tedy „Cvičení a výzkumné problémy“; až krajně triviální otázky jsou zde zařazeny přímo doprostřed složitých a dosud nevyřešených problémů. Říká se, že se prý jednou někdo Dr. Bellmana zeptal, jak pozná běžné cvičení od výzkumného problému, a on tehdy odpověděl: „Pokud dokážete otázku vyřešit, znamená to, že je to cvičení; jinak je to výzkumný problém.“

Dávat do knihy podobného druhu jak výzkumné problémy, tak i velmi snadná cvičení, je ovšem z řady důvodů rozumné; abych čtenáři ušetřil nepříjemné dilema, které otázky jsou které, označil jsem je *číselným hodnocením*, jež definuje úroveň obtížnosti. Číselné stupně mají následující obecný význam:

Hodnocení	*Význam*
00	Velice snadné cvičení, na které může čtenář, jenž dobře porozuměl probírané látce, odpovědět okamžitě; takovéto cvičení stačí prakticky vždy udělat jen „z hlavy“.
10	Jednoduchý problém, u něhož se musíte zamyslet nad přečtenou látkou, ale který ještě zdaleka není obtížný. Takovéto otázky byste měli zvládnout zhruba do jedné minuty a při řešení vám může pomoci tužka a papír.
20	Průměrně složitý problém, na kterém si vyzkoušíte základní porozumění probírané látce; k úplné odpovědi můžete ale potřebovat patnáct až dvacet minut.
30	Středně obtížný a/nebo složitý problém; k plně uspokojivé odpovědi se dopracujete i více než po dvou hodinách, případně po delší době, pokud u toho máte zapnutou televizi.

40 Dosti obtížný nebo rozsáhlý problém, který může být ve výuce vhodným námětem pro semestrální projekt. Student by měl být schopen problém vyřešit v rozumném čase, ale řešení není triviální.

50 Výzkumný problém, který dosud nebyl uspokojivě vyřešen (pokud bylo autorovi známo v době vzniku textu), i když se o jeho řešení mnozí pokoušeli. Pokud se vám podaří najít odpověď k takovémuto typu problému, rozhodně ji publikujte; také autora těchto stránek velice potěší, jestliže mu o řešení dáte co nejdříve vědět (za podmínky, že je řešení správné).

Interpolací této „logaritmické“ stupnice můžeme snadno vysvětlit i jiné číselné hodnocení. Výraz *17* bude například označovat cvičení, které je o něco více než průměrně jednoduché. Problémy s hodnocením *50*, které později nějaký čtenář vyřeší, mohou být v dalších vydáních knihy i v erratech na Internetu (viz strana iv) označeny číslem *45*.

Zbytek po dělení číselného hodnocení pěti vyjadřuje objem potřebné rutinní práce. Vyřešit cvičení označené číslem *24* může tedy trvat déle než cvičení s hodnocením *25*, ale ke cvičení s číslem *25* je potřeba více tvořivosti.

Autor se pokusil přiřadit číselné hodnocení jednotlivých cvičení co nejpřesněji, ale pro člověka, který nějaký problém vymyslí, je samozřejmě obtížné odhadnout, jak těžké bude hledat řešení pro někoho jiného; každý má navíc přirozené vlohy pro určité typy problémů, ale už ne pro jiné. Doufám, že je toto hodnocení dobrým odhadem obtížnosti; čísla berte ale jen jako rámcové vodítko, nikoli jako nějaký absolutní indikátor.

Knihu jsem psal pro čtenáře s různým stupněm matematického vzdělání a nadání; některá ze cvičení jsou proto určena jen pro matematicky zdatné studenty. Cvičení, k jehož řešení je potřeba více matematického myšlení či motivace, než kolik je běžné u lidí, kteří se zajímají jen o programování samotných algoritmů, má k hodnocení připojeno písmeno *M*. Pokud jsou ke cvičení nezbytné znalosti diferenciálního počtu nebo jiné vyšší matematiky, která není v této knize odvozena, je označeno písmeny „*VM*“. Samotné označení „*VM*“ ovšem *neznamená*, že by cvičení nutně muselo být obtížné.

Před některými cvičeními je uvedena šipka, „▸“; ta uvádí problémy, které jsou obzvláště názorné a jejichž řešení je možné čtenáři doporučit. Neočekávám samozřejmě, že každý čtenář či student vypracuje úplně *všechna* cvičení, a proto jsem takto označil ta nejcennější. (Tím vás ale nechci odradit od těch ostatních!) Každý čtenář by se ovšem měl přinejmenším pokusit o vyřešení všech problémů s hodnocením *10* a menším; podle šipek se může rozhodnout, kterým ze cvičení o vyšším hodnocení dá přednost.

Řešení většiny cvičení je uvedeno v sekci odpovědí. Ty, prosím, používejte s rozumem a na odpověď se nedívejte, pokud se nepokusíte problém poctivě vyřešit sami, nebo pokud na vyřešení tohoto konkrétního problému skutečně nemáte čas. Až *poté*, co přijdete na svoje vlastní řešení, nebo se o to alespoň pokusíte, může pro vás být vzorová odpověď poučením a návodem. Řešení uvedená v knize jsou často velmi stručná a detailní postupy jsou postaveny na předpokladu, že jste

se nejprve poctivě pokusili problém vyřešit vlastními silami. Někdy se z řešení dozvíte méně informací, než kolik bylo v otázce požadováno, jindy naopak více. Je také docela možné, že se vám podaří najít lepší odpověď než jaká je v knize uvedena; v tomto případě bude autor potěšen, pokud se s ním o řešení podělíte. V dalších vydáních knihy se pak podle možností objeví zdokonalené řešení spolu se jménem řešitele.

Při práci na cvičeních můžete obvykle využívat odpovědi na předchozí cvičení, pokud to není výslovně zakázáno. Také číselná hodnocení jsou definována s ohledem na toto pravidlo; je proto možné, že cvičení $n + 1$ bude mít nižší hodnocení než cvičení n, i když ve svém speciálním případě využívá výsledků cvičení n.

Shrnutí kódů:			
		00	Okamžitá odpověď
		10	Jednoduchá (do jedné minuty)
		20	Průměrná (čtvrt hodiny)
▶	Doporučené	*30*	Středně obtížná
M	Matematicky orientované	*40*	Semestrální projekt
VM	Vyžaduje „vyšší matematiku“	*50*	Výzkumný problém

CVIČENÍ

▶ **1.** [*00*] Co znamená hodnocení „*M20* “?

2. [*10*] Jakou hodnotu mohou mít cvičení v učebnici pro jejího čtenáře?

3. [*34*] Leonhard Euler vyslovil v roce 1772 hypotézu, že rovnice $w^4 + x^4 + y^4 = z^4$ nemá v oboru kladných celých čísel řešení, avšak Noam Elkies roku 1987 dokázal, že existuje nekonečně mnoho řešení [viz *Math. Comp.* **51** (1988), 825–835]. Najděte všechna celočíselná řešení taková, že $0 \le w \le x \le y < z < 10^6$.

4. [*M50*] Dokažte, že pokud je n celé číslo, $n > 4$, nemá rovnice $w^n + x^n + y^n = z^n$ žádné řešení, pro kladná celá čísla w, x, y, z.

Procvičování jest nejlepší cestou ke vzdělání.

— ROBERT RECORDE, *The Whetstone of Witte* (1557)

OBSAH

Kapitola 3 – Náhodná čísla 1

3.1. Úvod 1
3.2. Generování rovnoměrně rozdělených náhodných čísel 10
3.2.1. Lineární kongruenční metoda 10
3.2.1.1. Výběr modulu 12
3.2.1.2. Výběr násobitele 16
3.2.1.3. Potence 23
3.2.2. Jiné metody 26
3.3. Statistické testy 41
3.3.1. Obecné postupy testování při studiu náhodných veličin 42
3.3.2. Empirické testy 61
*3.3.3. Teoretické testy 80
3.3.4. Spektrální test 93
3.4. Ostatní typy náhodných veličin 119
3.4.1. Číselná rozdělení 119
3.4.2. Náhodné vzorkování a míchání 142
*3.5. Co je to náhodná posloupnost? 149
3.6. Shrnutí 184

Kapitola 4 – Aritmetika 194

4.1. Poziční číselné soustavy 195
4.2. Aritmetika čísel s pohyblivou řádovou čárkou 214
4.2.1. Výpočty v jednoduché přesnosti 214
4.2.2. Přesnost aritmetiky s pohyblivou řádovou čárkou 229
*4.2.3. Výpočty v dvojnásobné přesnosti 246
4.2.4. Statistické rozdělení čísel s pohyblivou řádovou čárkou 253
4.3. Aritmetika ve vícenásobné přesnosti 265
4.3.1. Klasické algoritmy 265
*4.3.2. Modulární aritmetika 284
*4.3.3. Jak rychle dokážeme násobit? 294
4.4. Převod základu číselné soustavy 319
4.5. Racionální aritmetika 330
4.5.1. Zlomky 330
4.5.2. Největší společný dělitel 333
*4.5.3. Analýza Euklidova algoritmu 356
4.5.4. Rozklad na prvočinitele 379

4.6. Aritmetika polynomů 418
4.6.1. Dělení polynomů 420
*4.6.2. Rozklad polynomů 439
4.6.3. Výpočty mocnin 461
4.6.4. Výpočty polynomů 485
*4.7. Manipulace s mocninnými řadami 525

Odpovědi na cvičení 538

Příloha A – Tabulky číselných veličin 726

1. Základní konstanty (desítkově) 726
2. Základní konstanty (osmičkově) 727
3. Harmonická čísla, Bernoulliho čísla, Fibonacciho čísla 728

Příloha B – Rejstřík notací 730

Rejstřík a slovníček pojmů 735