Aritmetika včera a dnes

L'ubomíra Balková

lubomira.balkova@fjfi.cvut.cz

Máme-li úkol vynásobit dvě přirozená čísla a k dispozici tužku a papír, většina z nás použije algoritmus, který jsme se učili už na základní škole:

		4	7
		5	3
	1	4	1
2	3	5	
2	4	9	1

Přesto ale algoritmů pro násobení existuje velké množství. Egyptské a ruské násobení jsou založené na binárním rozvoji násobitele. Cauchyovo komplementární násobení využívá zápis čísel pomocí záporných cifer. Kromě algoritmů, které urychlují násobení zpaměti a na papíře, si také ukážeme efektivní algoritmy pro počítačové násobení. Při násobení velkých čísel se vyplatí vyjádřit čísla v tzv. redundantní binární soustavě, kde připustíme kromě cifer 0 a 1 i cifru -1. Moderní éru v násobení velkých čísel odstartovaly ale zejména Karacubův algoritmus a modulární násobení.

Kromě násobení budeme studovat i další aritmetické operace. Například nás budou zajímat paralelní algoritmy, které existují pro sčítání. Při klasickém sčítání se objevuje přenos, který znemožňuje provádět sčítání na každé pozici nezávisle na předchozích. Vysvětlíme si algoritmus paralelního sčítání, který roku 1961 vymyslel litevský matematik A. Avizienis.

Práce bude mít několik cílů:

1. Programy pro násobení pomocí nejrůznějších algoritmů.
2. Porovnání rychlosti a paměťové náročnosti jednotlivých algoritmů.
3. Tvorba www stránky, kde budou vysvětleny jednotlivé algoritmy, popsána jejich historie a budou na ní k dispozici programy.
4. Programy pro výpočet i dalších základních aritmetických operací (sčítání, odčítání, dělení, umocňování, druhá a třetí odmocnina) pomocí co nejširší škály algoritmů.