Povinná zkoušková zadání z předmětu 11MA pro studenty kombinované formy studia v ZS 2010/2011

Jan Přikryl

22. ledna 2011

Ze zadání na následujících stránkách si prosím vyberte tři, která vypracujete a nahrajete na server obdobným způsobem, jako domácí úkoly.

Zadání K1

Připomeňme si, že pro Eulerovu funkci totient $\phi(n)$ platí, mimo jiné, že pro prvočíslo p je

$$\phi(p) = p - 1,$$

pro dvě různá prvočísla p a q, $p \neq q$, je

$$\phi(pq) = (p-1)(q-1),$$

pro složené číslo $n = p_1^{e_1} \cdot p_2^{e_2} \dots p_N^{e_N} = \prod_{i=1}^{N} p_i^{e_i}$ je

$$\phi(n) = \prod_{i=1}^{N} p_i^{e_i - 1}(p_i - 1).$$

Eulerova věta přitom říká, že nesoudělná a a n platí

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Úkoly:

1. Doplňte tabulku funkčních hodnot:

n	1	2	3	4	5	6	7	8	9	10
$\phi(n)$										

n	11	12	13	14	15	16	17	18	19	20
$\phi(n)$										

2. Dokažte, pro které hodnoty je $\phi(n)$ liché číslo.
3. Dokažte, pro které hodnoty je $\phi(n) = 2$.
4. Dokažte, že platí $1001^4 \equiv 1 \pmod{10}$ pomocí
   a) přímého výpočtu mocniny,
   b) Eulerovy věty.
5. Zajímavé zjištění je, že i když pro většinu čísel n je $m = \phi(n)$ nejnižší hodnota, splňující kongurenci $a^m \equiv 1 \pmod{n}$, není tomu tak vždy. Již pro celkem pět různých n z intervalu $1, 2, \dots, 20$ uvedeného v bodě 1 lze nalézt $m < \phi(n)$, pro nějž tato kongruence stále platí. Nalezněte alespoň dvě taková m.

Zadání K2

Podle Malé Fermatovy věty platí pro každé prvočíslo p a $a \in \mathbb{Z}$, $p \nmid a$ kongruence

$$a^{p-1} \equiv 1 \pmod{p}.$$

Tohoto tvrzení lze s výhodou využít při hledání zbytků po dělení vysokých mocnin čísel. Například zbytek po dělení čísla 6^{52} prvočíslem 11 je 3 – platí totiž, že $6^{52} = 6^{50} \cdot 6^2 = (6^{10})^5 \cdot 6^2 \equiv (1)^5 \cdot 36 \pmod{11} \equiv 3 \pmod{p}$.

Úkoly:

1. Nalezněte zbytek při dělení $3^{82} : 17$.
2. Nalezněte zbytek při dělení $2^{17} : 19$.
3. Nalezněte zbytek při dělení $2^{p-2} : p$, kde $p \neq 2$ je prvočíslo.
4. Nalezněte hodnotu $n \in \mathbb{N}$ splňující rovnici

$$133^5 + 110^5 + 84^5 + 27^5 = n^5.$$

Zadání K3

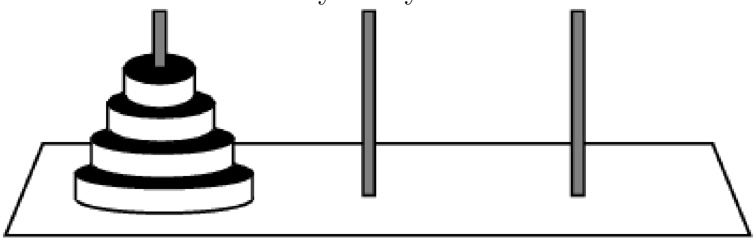
Kvalitu algoritmů můžeme posuzovat podle rychlosti konvergence a podle počtu iteračních kroků.

Úkoly:

1. Ukaže, že algoritmus aritmeticko-geometrického průměru čísel x a y, definovaný jako
$$a_{n+1} = \frac{a_n + g_n}{2},$$
$$g_{n+1} = \sqrt{a_n \cdot g_n}$$
s počátečními hodnotami $a_0 = x$ a $b_0 = y$ konverguje pro
$$\epsilon_n = \frac{a_n - g_n}{a_n}$$
kvadraticky.

2. Ukažte, že Euklidův algoritmus pro výpočet nějvyššího společného dělitele dvou čísel a a b má pro $a < b$ nejvýše $2\log_2 a+1$ iterací.

3. Nalezněte počet iteračních kroků algoritmu pro úlohu „Hanojské věže“. V této úloze máme přemístit věž skládající se ze 4 disků z levého sloupce do pravého tak, že přemístit můžeme vždy jen jeden disk a přemisťování probíhá s podmínkou, že v každém kroku musí být vždy menší disk na větším.



4. Nalezněte počet iteračních kroků pro Hanojskou věž skládající se z n disků.

Zadání K4

Trojici a, b, c kladných přirozených čísel budeme říkat pythagorejská, pokud je splněna rovnost

$$a^2 + b^2 = c^2. \tag{1}$$

Každou pythagorejskou trojici a, b, c si můžeme představit jako délky stran pravoúhlého trojúhelníka, pro které je rovnost (1) Pythagorovou větou. Asi nejznámější pythagorejskou trojicí je trojice $a = 3, b = 4, c = 5$.

Pro každou pythagorejskou trojici a, b, c platí

$$\gcd(a, b) = \gcd(b, c) = \gcd(a, c).$$

Řekneme, že pythagorejská trojice a, b, c je primitivní, když platí

$$\gcd(a, b) = \gcd(b, c) = \gcd(a, c) = 1.$$

Příkladem primitivní pythagorejské trojice je právě výše zmíněná trojice $a = 3$, $b = 4$, $c = 5$.

Úkoly:

1. Ukažte, že v primitivní pythagorejské trojici a, b, c musí být jedno z čísel a, b sudé a druhé liché.

2. Nechť jsou dána kladná čísla u, v, která nejsou obě lichá, a pro která platí $u > v$ a $\gcd(u, v) = 1$. Ukažte, že trojice čísel

$$\begin{aligned} a &= u^2 - v^2 \\ b &= 2uv \\ c &= u^2 + v^2 \end{aligned}$$

je primitivní pythagorejská trojice.

Zadání K5

Při výkladu o reprezentaci reálných čísel na počítači v pohyblivé řádové čárce jsme si říkali o tom, že vzhledem ke konečnému rozsahu reprezentace čísel dochází při numerických výpočtech k různým nepředpokládaným chybovým projevům.

Úkoly:

1. Vaším úkolem je vygenerovat $n+1$ bodů $x_0, x_1, \ldots, x_n$ rovnoměrně pokrývajících reálný interval hodnot $\langle a; b\rangle$ tak, že vzdálehost těchto bodů je $h = (b-a)/n$. První možností je počítat

$$x_0 = a, \quad x_k = x_{k-1} + h, \quad k = 1, 2, \ldots, n, \tag{2}$$

alternativně můžete použít předpis

$$x_k = a + k \cdot h, \quad k = 0, 1, \ldots, n. \tag{3}$$

Víte pouze, že budete počítat v pohyblivé řádové čárce, neznáte konkrétní hodnoty a, b a n.

   a) Přesto lze i takto obecně zadané varianty (2) a (3) posoudit z hlediska možných numerických chyb. Která z uvedených variant je při numerickém výpočtu přesnější a proč?

   b) Implementujte obě metody a na příkladu úlohy na intervalu $\langle 0; 1\rangle$ ukažte rozdíl mezi jejich výsledky.

2. Polynom

$$p(x) = (x-1)^6 \tag{4}$$

nabývá hodnoty nula v bodě $x = 1$ a hodnoty v ostatních x jsou vždy kladné. Pokud závorku roznásobíme, obdržíme rozšířenou formu

$$p(x) = x^6 - 6x^5 + 15x^4 - 20x^3 + 15x^2 - 6x + 1. \tag{5}$$

Ačkoliv jsou obě uvedené formy $p(x)$ matematicky ekvivalentní, při numerickém vyhodnocování nemusíme obdržet vždy ty samé výsledky. Vyneste do grafu 101 ekvidistantních hodnot $p(x)$ počítaných rovnicemi (4) a (5) pro $x \in \langle 0{,}995; 1{,}005\rangle$ (krok je tedy 0,0001). Měřítko grafu zvolte takové, aby v obou osách graf přesně pokrýval rozsah hodnot nezávisle a závisle proměnných. Vysvětlete důvod rozdílů, které pozorujete.

Zadání K6

Na přednášce jsme si ukazovali, jakými základními způsoby lze počítat kořeny nelineárních funkcí. V tmto zadání se blíže podíváme na dva zajímavé problémy, týkající se metody tečen a metody sečen.

Úkoly:

1. Mějme hladkou funkci $g : \mathbb{R} \to \mathbb{R}$ a pevný bod x^* této funkce takový, že $g(x^*) = x^*$.
   a) Formulujte všobecnou podmínku, za které iterační schéma $x_{k+1} = g(x_k)$ zkonverguje k x^* s kvadratickou rychlostí za předpokladu, že nástřel (počáteční odhad) x_0 je dostatečně blízko k x^*.
   b) Použijte tuto podmínku k důkazu tvrzení, že Newtonova metoda s kvadratickou rychlostí konverguje k jednoduché nule x^* hladké funkce $f : \mathbb{R} \to \mathbb{R}$ v okolí této nuly.
2. Ukažte, že iterativní metoda výpočtu

$$x_{k+1} = \frac{x_{k-1}f(x_k) - x_k f(x_{k-1})}{f(x_k) - f(x_{k-1})} \tag{6}$$

   je z matematického hlediska ekvivalentní metodě sečen, řešící skalární nelineární rovnici $f(x) = 0$.
3. Pokud použijete vztah (6) ke hledání kořene funkce $f(x)$, jaké budou jeho výhody či nevýhody oproti vzorci

$$x_{k+1} = x_k - f(x_k)\frac{x_k - x_{k-1}}{f(x_k) - f(x_{k-1})}? \tag{7}$$

4. Rekurentní výpočet dle (7) lze ještě poměrně jednoduchou úpravou zefektivnit. Jak?