

Počítačová algebra: Cvičení 2

14. října 2021

1. Napište příkaz, který vynásobí dvě čísla v $\mathbb{Z}$ a v $\mathbb{Z}_{32}$ a vypíše výsledek.
2. Napište funkci, která spočítá mocninu a^b pomocí binárního mocnění. Jakou má tento algoritmus časovou složitost?
3. Napište dvě funkce, které pro $a, b \in \mathbb{Z}$ spočítají $NSD(a, b)$ pomocí Eukleidova algoritmu – jedna s pomocí rekurze, druhá bez ní. Porovnejte jejich rychlost navzájem a oproti zabudované funkci *gcd*.
(K porovnávání se mohou hodit funkce *timeit*, *ZZ.random_element*.)
4. Modifikací algoritmu z předchozí úlohy napište funkci, která kromě $NSD(a, b)$ vrátí i koeficienty u, v takové, že $NSD(a, b) = ua + vb$.
5. Reprezentujme číslo $n = \sum_{i=0}^n a_i B^i$ v bázi B pomocí seznamu (*list*) $[a_0, a_1, \dots, a_n]$. Pro takto reprezentovaná čísla, napište funkce sčítání, odčítání a násobení konstantou.
6. Pro reprezentaci čísel z úlohy 5 napište funkci na převod čísel mezi bázemi.
(Nápověda: prvek *ZZ* má metodu *digits*. Opačným směrem funguje *ZZ(list, B)*)
7. Pro reprezentaci čísel z úlohy 5 napište funkci násobení pomocí klasické školské metody.
8. Pro reprezentaci čísel z úlohy 5 implementujte metodu násobení pomocí Karacubova triku. Porovnejte rychlost s klasickým školním násobením.
9. Napište funkce *gcd_list*(*[list of integers]*, *function f*), *lcm_list*(*...*), které pro seznam celých čísel a libovolnou funkci $f(a, b) = NSD(a, b)$ spočtou jejich největšího společného dělitele a nejmenší společný násobek. Zkuste ji následně použít, jak se zabudovanou funkcí *gcd*, tak s funkcí z úlohy 3.