Pozvánka na výběrovou přednášku

Aritmetika a algoritmy, 1/1 Zk, v LS

Přednáška je zamýšlena jako úvod do matematického myšlení pro zájemce, kteří s matematikou zkušenost nemají, avšak nezaujali k ní negativní postoj. Lze ji též chápat jako kurs logiky (skoro) bez logické teorie. Budeme se zabývat některými důležitými pojmy z teoretické informatiky (např. *polynomiální algoritmus*) a z algebry (*grupa* a *okruh*) a jejich interakcí. V tomto školním roce se nepředpokládá účast studentů logiky.

Jak lze ověřit, že číslo 193 707 721 je prvočíslo? A pomůže k tomu počítač? Zájem matematiků o velká prvočísla se po staletí jevil jako naprosto nepraktická zábava. Až v posledních desetiletích se ukázalo, že velká prvočísla, podobně jako některé velmi staré objevy (*Eukleidův algoritmus* a *čínská zbytková věta*) nacházejí uplatnění v *kryptografii*, takže je, možná nevědomky, všichni používáme doslova každý den. Jedna z kryptografických metod, metoda RSA, bude v přednášce také probrána.

Matematickým myšlením se rozumí, že formulujeme tvrzení a definice a tvrzení dokazujeme z předpokladů a s využitím oněch definic. Matematikové rádi zdůrazňují, že matematika není počítání, ale dokazování. Dokazováním z předpokladů se v přednášce budeme vydatně zabývat. Avšak, náhodou nebo spíš vzhledem k oněm souvislostem s teoretickou informatikou, na počítání také často dojde. Filozofické, metodologické či historické otázky sice předmětem přednášky v podstatě nejsou, ale jsou v pozadí všeho výkladu a nějaké světlo na ně padne.

Koná se v **Út 10:50–12:20 v učebně 137 v Celetné 20**, začínáme **19.2.2019**. Další informace je v ISu a (postupně bude) na http://www.cuni.cz/~svejdar/?s=aa.

doc RNDr Vítězslav Švejdar CSc
Katedra logiky FF UK