

Pozvánka na výběrovou přednášku  
**Aritmetika a algoritmy, 1/1 Zk**

Přednáška je zamýšlena jako seznámení s nezákladnějšími pojmy z teoretické informatiky (*polynomiální algoritmus*) a z algebry (*grupa a okruh*) a na interakci mezi těmito obory. Některá matematická znalost někdy pomůže sestavit užitečný algoritmus, ale může se i stát, že zamýšlení nad určitým algoritmem dá nějaký matematický poznatek.

Zváni jsou studenti všech oborů, avšak těm, kteří již mají za sebou první ročník oboru logika nebo první ročník MFF, přednáška mnoho dát nemůže. Jedním z cílů totiž je oslovit zájemce, kteří se s matematikou rozloučili někdy okolo maturity. Protože se budeme (také) zabývat dokazováním důsledků z nějakých předpokladů, přednášku lze též chápat jako kurs logiky (skoro) bez logické teorie.

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 dost neužitečná zábava. Ale v posledních desetiletích se ukázalo, že některé velmi staré objevy související s prvočíslly (*Eukleidův algoritmus* a *čínská zbytková věta*) nacházejí uplatnění v *kryptografii*, takže je, většinou nevědomky, všichni používáme doslova každý den. Jedna z kryptografických metod, metoda RSA, bude v přednášce probrána. Filosofické, metodologické či historické otázky předmětem přednášky nejsou, ale nějaké světlo na ně také padne.

Koná se ve **Čt 13:20–14:50 v učebně 352 v Celetné 20, začínáme 20.2.2025**. Další informace je v SISu (ALG110008) a (později) na <http://www.cuni.cz/~svejdar/?s=aa>. Přístup do učebny 352 je z Celetné po schodech do prvního patra, a pak *zadním* schodištěm do třetího patra.

Vítězslav Švejdar, Katedra logiky FF UK