

Teorie čísel a úvod do šifrování

RNDr. Zbyněk Šír, MFF UK

V tomto kurzu se seznámíme s řadou vlastností celých čísel a jejich bohatými aplikacemi. Naučíme se pracovat se zbytky po dělení a dokážeme si malou Fermatovu větu. Budeme pak umět jednoduše řešit úlohy typu

Je $2010^{2010} + 1$ dělitelné číslem 13?

Dále si ukážeme základní vlastnosti prvočísel a předvedeme si, jak se testuje, jestli je dané (velmi velké) číslo prvočíslem.

Na závěr se seznámíme se slavným RSA šifrovacím algoritmem, který je založen na velké složitosti výpočtu prvočíselného rozkladu. U tohoto algoritmu (užívaného i pro šifrování v rámci internetu) není možno zprávu rozluštit, i když víme, jak byla zašifrována.