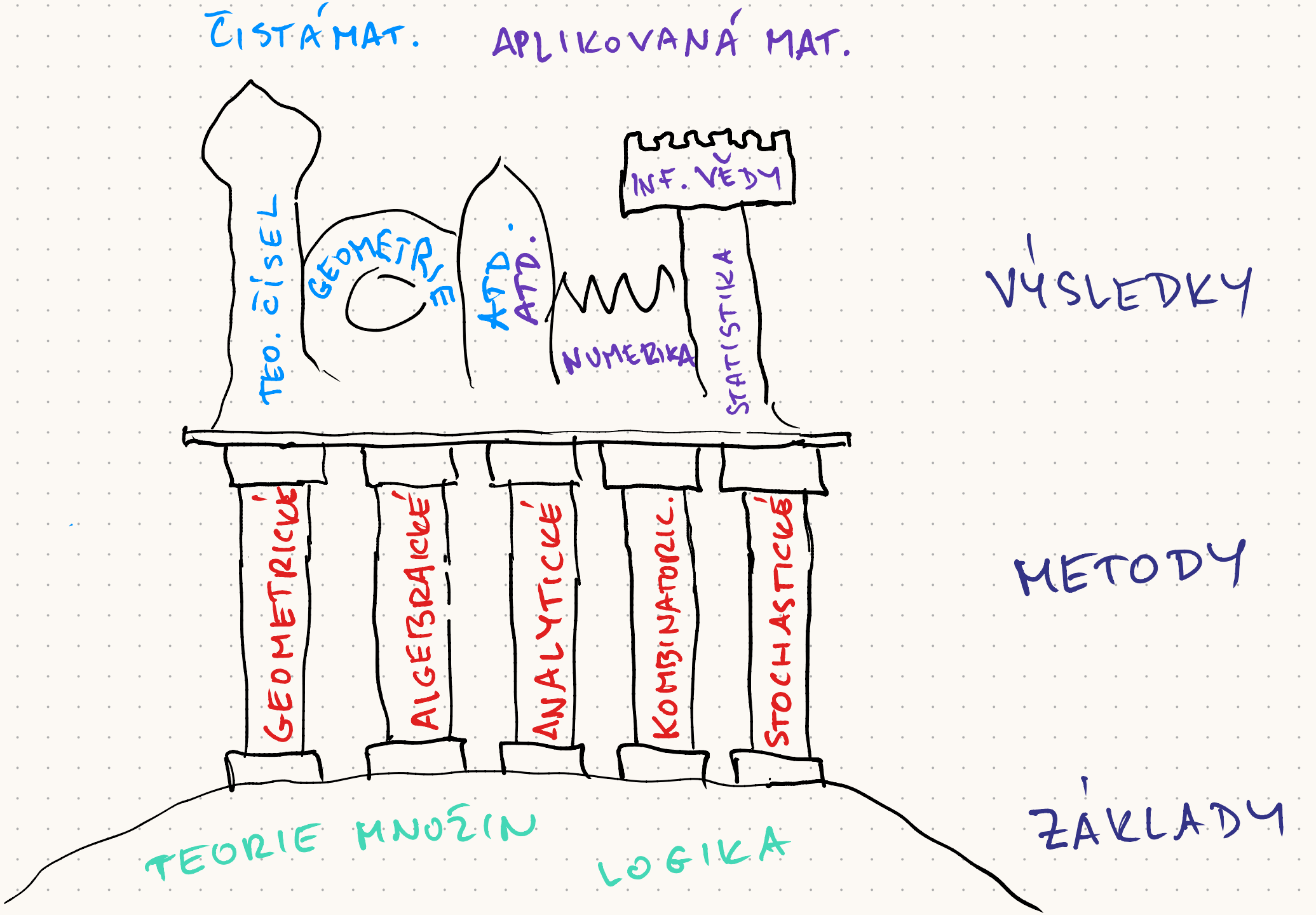


ALGEBRA na matfyzu v 2. ročníku

- úvod do metod obecné (nelineární) algebry
- ukázky použití – v čisté mat.
  - ↳ základní věta algebry
  - ↳ Řešení diofantických rovnic
  - ↳ Kombin. počítání se symetriemi
  - ↳ (Ne)řešitelnost úloh prav./kruž.
  - ↳ (Ne)řešitelnost polynom. rovnic
- v aplikované mat.
  - ↳ Konečná tělesa a triky s přenosem informace
  - ↳ šifry

CHCETE VÍC?

Proseminář z algebry

PÁ 13:10

1. ELEMENTÁRNÍ TEORIE ČÍSEL

2. ZÁKLADNÍ ALGEBRAICKÉ OBJEKTY
   - abstraktní struktury
   - polynomy, číselné obory

3. TEORIE DĚLITELNOSTI
   - ireducibilní rozklady, NSD, ... pro různé typy oborů

4. POLYNOMY
   - modulární aritmetika, konstrukce konečných těles
   - kořeny polynomů, Vietovy vztahy, zákl. věta algebry

5. GRUPY
   - metoda jak pracovat se symetriemi, Burnsideova věta
   - cyklické gwpy a krypto

6. TĚLESOVÁ ROZŠÍŘENÍ
   - rozšíření těles jako vektorové prostory
   - Galoisova teorie

ELEMENTÁRNÍ TEORIE ČÍSEL

dělení se zbytkem
výpočet NSD
Bézoutova rovnost:

$NSD(a,b) = ua + vb$

prvočísla
základní věta aritmetiky

$\forall a \; \exists! \; p_i, k_i \; t.ž. \; a = p_1^{k_1} \cdots p_n^{k_n}$

modulární aritmetika

$a \equiv b \pmod m$

a její vlastnosti

Eulerova věta

$NSD(a,m) = 1 \Rightarrow$

$a^{\varphi(m)} \equiv 1 \pmod m$

a kryptosystém RSA

Čínská věta o zbytcích

$\exists! \; x \in \{0 \dots M-1\} \; t.ž.$

$x \equiv a_1 \pmod{m_1}$

$\vdots$

$x \equiv a_n \pmod{m_n}$

(m_i nesoud., $M = \prod m_i$)

a vzorec na Eulerovu funkci

$\varphi(n) = p_1^{k_1-1}(p_1-1) \cdots p_n^{k_n-1}(p_n-1)$

$a \equiv b \pmod m \overset{\text{def}}{\iff} m \mid a-b$

$\iff a \bmod m = b \bmod m$

Ma $\mathbb{Z}$, $m \neq 0$

- je to ekvivalence

  $a \equiv a \pmod m$

  $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$

  $a \equiv b,\ b \equiv c \Rightarrow a \equiv c \pmod m$

- je to invariantní vůči $+, -, \cdot$

  $a \equiv b \pmod m$, $c \equiv d \pmod m$ $\Rightarrow$

  $a + c \equiv b + d \pmod m$

  $a - c \equiv b - d \pmod m$

  $a \cdot c \equiv b \cdot d \pmod m$

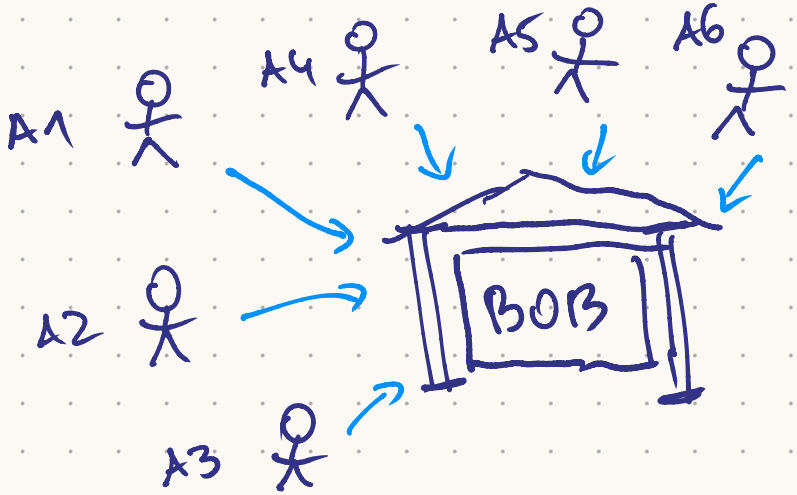
  $a^k \equiv b^k \pmod m \quad \forall k$

- krácení:

  $a \equiv b \pmod m \iff ca \equiv cb \pmod{cm}$

  $a \equiv b \pmod m \iff ca \equiv cb \pmod m$ pokud jsou c, m nesoudělná

KRYPTOSYSTÉM RSA (Rivest, Shamir, Adleman 1977)



Alice K: veřejný klíč (na psaní)
Bob: soukromý klíč (na čtení)

SETUP:

Bob zvolí $N = pq$
(čili $\varphi(N) = (p-1)(q-1)$)
zvolí náhodné e nesoudělné s $\varphi(N)$
spočte d t.ž. $d \cdot e \equiv 1 \pmod{\varphi(N)}$

⇒ VEŘEJNÝ OF: N, e
TAJNÝ OF: d
(tajné jsou $p, q, \varphi(N)$)

ŠIFROVÁNÍ:

zpráva $x \in \{0, \dots, N-1\}$
nesoudělná s N

zašifrování: $y = x^e \bmod N$

dešifrování: $x = y^d \bmod N$