- Eulerova funkce: $\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})...(p_k^{\alpha_k} - p_k^{\alpha_k - 1})$.
- Eulerova věta (také Fermatův test): $(a, m) = 1 \;\Rightarrow\; a^{\varphi(m)} \equiv 1 \pmod{m}$.
- Jacobiho symbol:
  - $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$, pro liché číslo b; přitom $b \equiv 1, 7 \pmod{8}$ dá $+1$, $b \equiv 3, 5 \pmod{8}$ dá -1,
  - $\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$, pro lichá čísla a, b; přitom vše dá $+1$, akorát $a, b \equiv 3 \pmod{4}$ dá -1,
  - Legendrův symbol: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$, pro p liché prvočíslo (také Eulerův-Jacobiho test).
- RSA: $n = p \cdot q$, $d \cdot e \equiv 1 \pmod{\varphi(n)}$, $c \equiv m^e \pmod{n}$, $m \equiv c^d \pmod{n}$.
- Rabin: $n = p \cdot q$, $c \equiv m^2 \pmod{n}$, $m \equiv \pm c^{\frac{p+1}{4}} \pmod{p}$, $m \equiv \pm c^{\frac{q+1}{4}} \pmod{q}$.
- ElGamal: $c \equiv m \cdot (g^a)^b \pmod{n}$.

- počet výběrů k objektů n druhů – kombinace: $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1}$
- počet výběrů k objektů n druhů – kombinace s opakováním: $\binom{n+k-1}{k}$
- počet pořadí $k = p_1 + \cdots + p_n$ objektů n druhů, pro p_1 objektů prvního druhu, ..., p_n objektů n-tého druhu – permutace s opakováním: $\frac{(p_1 + \cdots + p_n)!}{p_1! \cdots p_n!}$
- princip inkluze a exkluze: $|M \smallsetminus (A \cup B)| = |M| - |A| - |B| + |A \cap B|$
- princip inkluze a exkluze: $|M \smallsetminus (A \cup B \cup C)| = |M| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C|$
- součet n-prvkové **aritmetické** řady $x_1 + \cdots + x_n = n \cdot \frac{x_1 + x_n}{2}$

- rozvinutí některých vybraných funkcí:

$$\frac{1}{1-x} = \sum_{k \geq 0} x^k = 1 + x + x^2 + \cdots$$

$$\frac{1}{(1-x)^n} = \sum_{k \geq 0} \binom{k+n-1}{n-1} \cdot x^k$$

$$(1+x)^r = \sum_{k \geq 0} \binom{r}{k} \cdot x^k$$

$$\ln \frac{1}{1-x} = \sum_{k \geq 1} \frac{1}{k} \cdot x^k$$

$$e^x = \sum_{k \geq 0} \frac{1}{k!} \cdot x^k$$

kde v třetím vzorci $\binom{r}{k} = \frac{r(r-1)\cdots(r-k+1)}{k(k-1)\cdots 1}$