- 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: $c \equiv g^{a \cdot b} \cdot m \pmod n$.