1. Dokaži sledeče trditve.

(a) $\lfloor x \rfloor \neq \lceil x - 1 \rceil \Rightarrow x = \lfloor x \rfloor = \lceil x \rceil$

(b) $x, y \geq 0 \Rightarrow \lfloor x \rfloor \cdot \lfloor y \rfloor \leq \lfloor xy \rfloor \leq xy$

(c) $x, y > 0 \wedge \lfloor x \rfloor \cdot \lfloor y \rfloor = \lfloor xy \rfloor \Rightarrow x, y \in \mathbb{N}$

2. Z Evklidovim algoritmom izračunaj največji skupni delitelj števil 190 in 968. Kolikšen je njun najmanjši skupni večkratnik?

3. Z razširjenim Evklidovim algoritmom izračunaj največji skupni delitelj števil 709 in 655.

4. Izračunaj najmanjše tako naravno število x, da velja $204 \cdot x \equiv 1 \pmod{785}$.

5. Izračunaj $5^{2014} \bmod 11$.

6. Tabeliraj vrednosti Eulerjeve funkcije ϕ za števila od 1 do 20.

7. Za kriptosistem RSA izberemo praštevili $p = 67$ in $q = 89$. Izračunaj javni modul n ter izberi javni eksponent e in tajni eksponent d, da bo e čimmanjši. Z dobljenimi parametri zašifriraj sporočilo $m = 75$ ter preveri, da se pravilno odšifrira.