Kevad 2018

Vihjeid 15. praktikumiks

1. Näide 9.3.

2. Näide 9.7.

3. Näide 9.8.

4. Tegurdada moodul n ehk leida $\varphi(n)$. Näide 9.8.

5. Näited 9.8 ja 9.9.

6. Astendada kongruentsi $2^{2^n} \equiv -1 \pmod{F_n}$ sobiva kahe astmega.

7. Korselti kriteerium. Paaritud algarvud kujul $2^k + 1$ on alati Fermat' algarvud (vihje: $2^l + 1 \mid 2^k + 1$, kui $k = lm$ ja m on paaritu). Fermat' arvud ei jaga üksteist (vihje: kui $n > m$, siis $F_n \equiv 2 \pmod{F_m}$, kasutades sama võtet, mis 6. ülesandes).

8. Üldisust kitsendamata $(c, n) = (c', n) = 1$ (miks?). Leida s kujul $s^{ue-ve'}$, $u, v \in \mathbb{N}$. Eukleidese algoritm ja astendamine mooduli järgi on "kiired".