LUKUTEORIAN ALKEET

6. LASKUHARJOITUKSET

(1) Kuinka monta primitiivistä juurta on modulossa 13? Määritä lisäksi primitiiviset juuret modulo 13.
(2) Esitä koko redusoitu jäännössysteemi jonkin valitsemasi primitiivisen juuren avulla.
(3) Ratkaise yhtälö $x^2 \equiv 12 \pmod{13}$. (Vihje: esitä 12 primitiivisen juuren avulla, järkeile, miksi saat ottaa neliöjuuret yhtälöstä, ja viimeistele ratkaisu Lagrangen lauseella.)
(4) Olkoon $n = 47 \cdot 53$. Valitse jokin e RSA:n julkisen avaimen osaksi (ei, ei lukua 1, koska silloin salaus ei varsinaisesti salaisi), ja määritä loput RSA:n käytössä vaadittavat parametrit. Havainnollista lopulta järjestelmää kryptaamalla luku 28 ja sen jälkeen purkamalla kryptaus.
(5) Olkoon $n = 16637$. Määritä sen alkutekijät p ja q.
(6) Olkoon RSA:n julkinen avain $(n, e) = (16637, 11)$ määritä loput parametrit, eli murra systeemi.