Matematiikan laitos
Teknillinen korkeakoulu

Turunen

Mat-1.3111 Lukuteoria

Tentti 6.2.2010 klo 10–14

Täytä selvästi *jokaiseen vastauspaperiin* kaikki otsaketiedot. Merkitse kurssikoodi-kohtaan opintojakson numero, nimi ja onko kyseessä tentti vai välikoe. Tutkinto-ohjelmakoodit ovat ARK, AUT, BIO, EST, ENE, GMA, INF, KEM, KTA, KON, MAR, MTE, PUU, RRT, TFM, TIK, TLT, TUO, YYT.

Kokeessa ei saa käyttää laskinta eikä muita apuvälineitä.

1. Määrittele
   a) käänteisalkio modulo m,
   b) Dirichlet-tulo $f \star g$,
   c) diskreetti Fourier-muunnos.

2. Olkoon $p = 29$ ja $q = 17$.
   a) Laske Eukleideen algoritmin avulla $\gcd(p, q)$ ja ratkaise sen avulla yhtälöt

$$\begin{cases} qx \equiv 1 \pmod{p}, \\ py \equiv 1 \pmod{q}. \end{cases}$$

   b) Ratkaise Kiinalaisen jäännöslauseen avulla

$$\begin{cases} z \equiv 5 \pmod{p} \\ z \equiv 4 \pmod{q} \end{cases}$$

3. NO-yhtiön pomo Jorma-Pekka epäilee alaisensa Bobin vuodattavan yrityssalaisuuksia. Bobin RSA-salakirjoituksen julkinen avain on

$$(e, n) = (11, 221).$$

   Jorma-Pekka saa käsiinsä Bobin taskusta tipahtaneen lapun, jossa lukee

$$\phi(n) = 192.$$

   a) Selitä, miten Bobille lähetetään RSA-salattu viesti ja miten Bob purkaa tämän salauksen.

   b) Etsi luvun $n = 221$ alkutekijät tiedon $\phi(n) = 192$ avulla.

   (Tässä leikimme, että n olisi **valtavan suuri** luku eli ratkaisulta edellytetään, että se soveltuisi yleiseen tapaukseen. Siten esimerkiksi kokeilemalla saatu ratkaisu ei kelpaa.)

4. Mitä Lagrangen lause polynomeista (modulo alkuluku) sanoo? Todista Lagrangen lause.