Harjoitukset 2 **Lukuteoria**
tiistai 27.9.2011 16.00-17.30 MaD-302 **HUOMAA AIKA**

1. *Etsi Eratostheneen seulalla lukua* 200 *pienemmät alkuluvut. (Tai ohjelmoi tietokoneesi etsimään paljon lisää.)*

2. *Olkoon* $p \neq 3$ *alkuluku. Näytä, että* p *on muotoa*

$$p = 3k + 1 \quad \textit{tai} \quad p = 3k - 1 \quad \textit{jollain } k \in \mathbb{N}.$$

3. *Todista: jos* p *on alkuluku ja* $a \in \mathbb{Z}$*, niin joko* $p \mid a$ *tai* $(a, p) = 1$*.*

4. *Näytä, että jos* n *ja* a *ovat luonnollisia lukuja ja* $\sqrt[n]{a} \in \mathbb{Q}$*, niin* $\sqrt[n]{a} \in \mathbb{N}$ *ja siis esimerkiksi* $\sqrt[3]{10}$ *ei ole rationaaliluku.*

5. *Eukleideen klassisessa todistuksessa löydetään alkulukujoukon* $\{p_1, p_2, \ldots, p_n\}$ *ulkopuolella oleva alkuluku* p_{n+1} *tutkimalla luvun*

$$N_n = p_1 p_2 \cdots p_n + 1$$

alkutekijöitä.

Etsi tällä menetelmällä alkulukuja aloittaen joukoista $\{2\}$*, sitten joukosta* $\{2, p_2\}$*, missä* p_2 *on ensimmäisestä vaiheesta saatu alkuluku, itse asiassa* $N_2 = 2+1 = 3$*, joten* p_2 *on 3, koska* N_2 *sattuu itse olemaan alkuluku. Jatka, kunnes tapahtuu jompikumpi seuraavista:*

(1) *olet löytänyt 5 paritonta alkulukua. (Saat kyllä jatkaakin, jos haluat.)*
(2) N_p *ei ole alkuluku, vaan* $p_n \neq N_n$*.*

Mitä ajatuksia tai kysymyksiä herää?

6. *a) Luvut* $3, 5$ *ja* 7 *ovat muotoa* $p, p+2, p+4$ *oleva alkulukukolmikko. Miksi ei voi olla luonnollista lukua* $p > 3$*, jolle luvut* p*,* $p+2$ *ja* $p+4$ *ovat alkulukuja?*

b) Olkoot $a, b \in \mathbb{N}$ *ja* $(a, b) \geq 2$*. Osoita, että joukossa* $A = \{an+b \mid n = 0, 1, 2, \ldots\}$ *on korkeintaan yksi alkuluku.*

7. *Osoita, että on olemassa sellainen vakio* $C \in \mathbb{R}$*, että kaikilla* $k \geq 2$ *pätee epäyhtälö*

$$\sum_{p \leq k, p \in \mathbb{P}} \frac{1}{p} \geq \log\log k + C, \tag{1}$$

joten sarja $\sum_{p \in \mathbb{P}} \frac{1}{p}$ *hajaantuu. Voit lähteä siitä luennolla jo todistetusta tiedosta, että*

$$\prod_{p \leq k, p \in \mathbb{P}} \frac{1}{1 - p^{-1}} \geq \sum_{n} \frac{1}{n} \geq \log k. \tag{2}$$

Ota puolittain logaritmit. Vasemman puolen logaritmin laskemiseksi muista hiukan logaritmin laskusääntöjä ja ota huomioon, että

(1) $-\log\left(1 - \frac{1}{p}\right) \leq \frac{1}{p} + \frac{1}{p^2}$*, mitä ei tarvitse todistaa* **lukuteorian** *kurssilla, mutta kyllä nähdään helposti sarjakehitelmästä tai toteamalla, että funktio* $f(x) = \log(1+x) - x + x^2$ *on vähenevä välillä* $[-\frac{1}{2}, 0]$
(2) *sarja* $\sum_p p^{-2}$ *suppenee.*

KÄÄNNÄ

8. *Laske konvoluutiot (,jos osaat - en ole itse ehtinyt kokeilla kaikkia. Jos ei onnistu yleisesti, laske ainakin arvo kohdassa 1. :-)*

(1) $E_0 * E_0$
(2) $E * E_0$
(3) $E_0 * \Omega$
(4) $E * N_\alpha$
(5) $E * \sigma_{\frac{1}{2}}$
(6) $\mu * E * E_0$.

9. *Laske alla oleva esimerkki uudelleen laajennetulla Eukleideeen algoritmilla. (Ratkaisu on jo mukana! Ei käydä tarkasti läpi demoissa. Ohjelmointitaitoisille tiedoksi!)*

Aluksi esimerkki muistin virkistämiseksi: Eukleideen algoritmi luvuille 126 ja 35:

$$\begin{aligned} 126 &= 3 \cdot 35 + 21, \\ 35 &= 1 \cdot 21 + 14, \\ 21 &= 1 \cdot 14 + 7, \\ 14 &= 2 \cdot 7. \end{aligned}$$

Kertoimet s ja t löydetään "takaperin laskemalla":

$$\begin{aligned} (126, 35) = 7 &= 21 - 1 \cdot 14, \\ &= 21 - (35 - 1 \cdot 21), \\ &= (126 - 3 \cdot 35) - (35 - (126 - 3 \cdot 35)), \\ &= 2 \cdot 126 - 7 \cdot 35. \end{aligned}$$

Tämä menetelmä kertoimien määräämiseksi ei ole kovin käyttökelpoinen tietokoneella laskettaessa. Eukleideen algoritmista saatavat välivaiheet pitäisi tallettaa muistiin, jotta niitä voitaisiin käyttää kertoimien s ja t määräämiseen edellisen esimerkin mukaisesti. **Kertoimet s ja t voidaan kuitenkin määrätä suoraan käyttämällä ns. laajennettua Eukleideen algoritmia.**

1.1. Laajennettu Eukleideen algoritmi. *Olkoot luvut ℓ, q_i ja r_i kuten Eukleideen algoritmissa. Pyritään etsimään luvut s_i ja t_i siten, että $s_i r_0 + t_i r_1 = r_i$ kaikille $0 \leq i \leq \ell$. Oletetaan aluksi, että tällaiset luvut ovat olemassa. Kun tätä oletusta sovelletaan indekseihin $i-1$, i ja $i+1$, saadaan Eukleideen algoritmin avulla*

$$\begin{aligned} r_{i+1} = r_{i-1} - q_i r_i &= (s_{i-1} r_0 + t_{i-1} r_1) - q_i (s_i r_0 + t_i r_1) \\ &= (s_{i-1} - q_i s_i) r_0 + (t_{i-1} - q_i t_i) r_1. \end{aligned} \tag{3}$$

Toisaalta $r_{i+1} = s_{i+1} r_0 + t_{i+1} r_1$. Valitaan kertoimet seuraavan palautuskaavan mukaisesti

$$\begin{aligned} s_{i+1} &= s_{i-1} - q_i s_i, \\ t_{i+1} &= t_{i-1} - q_i t_i. \end{aligned} \tag{4}$$

Tällöin yhtälöstä (3) seuraa, että jos $s_k r_0 + t_k r_1 = r_k$ arvoilla $k = i-1$ ja $k = i$ ja kertoimet s_k ja t_k on määrätty palautuskaavojen (4) avulla, niin yhtälö $s_k r_0 + t_k r_1 = r_k$ on voimassa myös, kun $k = i+1$. Riittää siis löytää sopivat aloitusarvot. Tällaiset ovat

$$s_0 = 1, \quad t_0 = 0, \quad s_1 = 0, \quad t_1 = 1.$$

Laajennetussa Eukleideen algoritmissa määrätään luvut ℓ, q_i, $r_i \in \mathbb{N}$, s_i, $t_i \in \mathbb{Z}$, $1 \leq i \leq \ell$, *siten, että* $0 \leq r_{i-1} < r_i$, *kun* $1 \leq i \leq \ell$, *ja*

$$\begin{cases} s_0 = 1, \quad t_0 = 0 \\ s_1 = 0, \quad t_1 = 1 \\ r_{i-1} = q_i r_i + r_{i+1} \\ s_{i-1} = q_i s_i + s_{i+1} \\ t_{i-1} = q_i t_i + t_{i+1} \end{cases} \tag{5}$$

Tällöin $s_i r_0 + t_i r_1 = r_i$ *kaikille* $0 \leq i \leq \ell$ *ja* $r_\ell = (r_0, r_1)$.
Lisätietoa laajennetusta Eukleideen algoritmista löytyy kirjoista [**?**, §3.2], [**?**, §4.5.2].

Esimerkki. *Käydään läpi edellisen esimerkin lasku laajennetulla Eukleideen algoritmilla.*

i	r_i	s_i	t_i
0	126	1	0
1	35	0	1
2	21	1	−3
3	14	−1	4
4	7	2	−7
5	0	−5	18

Riviltä $i = 4$ *saadaan*
$r_\ell = (r_0, r_1) = s_\ell r_0 + t_\ell r_1$, *eli*
$7 = (126, 35) = 2 \cdot 126 - 7 \cdot 35$.