Lukuteoria 1
Harjoitus 4, 7.2.2018, ratkaisuehdotuksia

Näissä harjoituksissa käytetään seuraavia merkintöjä: Kaikkien alkulukujen joukko on $\{p_1, p_2, p_3, ...\}$, missä alkuluvut on numeroitu suuruusjärjestyksessä pienimmästä alkaen. Siis näissä harjoituksissa $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ jne. (Huom! Tämä ei ole universaali merkintätapa lukuteoriassa, joten tämä merkintätapa pitää aina erikseen kertoa kun sitä haluaa käyttää. Monesti kirjaimilla $p_1, p_2, ...$ merkitään vain joitakin mielivaltaisia alkulukuja, kuten olemme luennoillakin nähneet.)

1. Osoita, että luku 107 on alkuluku.

Ratkaisu. Koska $\sqrt{107} < 11$ ja pätee $2 \nmid 107$, $3 \nmid 107$, $5 \nmid 107$ ja $7 \nmid 107$, Lemman 3.1.8 nojalla 107 on alkuluku.

2. Määritellään $a_1 = p_1 + 1$, $a_2 = p_1p_2 + 1$, yleisesti $a_j = p_1p_2 \cdots p_j + 1$. Mitkä luvuista a_1, a_2, a_3, a_4 ovat alkulukuja?

Ratkaisu. $a_1 = 2 + 1 = 3$ (alkuluku) ja $a_2 = 2 \cdot 3 + 1 = 7$ (alkuluku). $a_3 = 2 \cdot 3 \cdot 5 + 1 = 31$. Koska $\sqrt{31} < 6$ ja on $2 \nmid 31$, $3 \nmid 31$ ja $5 \nmid 31$, luku 31 on alkuluku. $a_4 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$. Koska $\sqrt{211} < 15$ ja on $2 \nmid 211$, $3 \nmid 211$, $5 \nmid 211$, $7 \nmid 211$, $11 \nmid 211$ ja $13 \nmid 211$, myös luku 211 on alkuluku.
Siis kaikki luvut a_1, a_2, a_3, a_4 ovat alkulukuja.

Huomautus: Kuitenkin $a_6 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$.

3. Etsi luvuille 63 ja 78 alkutekijäesitykset, ja selvitä niiden avulla $\text{syt}(63, 78)$.

Ratkaisu. Alkutekijäesitykset ovat $63 = 3^2 \cdot 7$ ja $78 = 2 \cdot 3 \cdot 13$. Kirjoittamalla

$$63 = 2^0 \cdot 3^2 \cdot 7 \cdot 13^0, \quad 78 = 2 \cdot 3 \cdot 7^0 \cdot 13,$$

saadaan Lauseen 3.1.10 nojalla

$$\text{syt}(63, 78) = 2^0 \cdot 3 \cdot 7^0 \cdot 13^0 = 3.$$

4. Osoita, että jos a on yhdistetty luku, niin $a \nmid [(a-1)! + 1]$.

Ratkaisu. Koska a on yhdistetty luku, sillä on tekijänä alkuluku p jolle pätee $2 \leq p \leq a - 1$. Siis $p \mid (a-1)!$. Tehdään vastaoletus, että $a \mid [(a-1)! + 1]$. Koska $p \mid a$, Proposition 2.1.4 kohdan 1 nojalla on $p \mid [(a-1)! + 1]$, joten Proposition 2.1.4 kohdan 2 nojalla p jakaa luvun

$$[(a-1)! + 1] - (a-1)! = 1.$$

Tämä on ristiriita, sillä $p \geq 2$. Siis vastaoletus on väärä, joten on $a \nmid [(a-1)! + 1]$.

5. Esimerkissä 3.2.2 saatiin osoitettua, että äärettömän moni alkuluku on muotoa $4n+3$ jollakin $n \in \mathbb{N}$. Yritä samalla idealla osoittaa, että äärettömän moni alkuluku on muotoa $4l + 1$ jollakin $l \in \mathbb{Z}$. Missä kohdassa todistusyrityksesi jää jumiin?

Ratkaisu. Yritetään näyttää Esimerkkiä 3.2.2 seuraamalla, että muotoa

$$4n+1, \quad N \in \mathbb{N} \setminus \{0\},$$

olevia alkulukuja on äärettömän monta. Olkoot $p_1, \ldots, p_k$ muotoa $4n+1$ olevia alkulukuja. Määritellään

$$N = 4p_1 \cdots p_k + 1.$$

Luku N on muotoa $4n+1$. Se ei ole jaollinen millään luvuista p_i, $i = 1, \ldots, k$, eikä luvuilla $2, 3$.

Jos N on alkuluku, olemme löytäneet lukujen $p_1, ..., p_k$ ulkopuolelta muotoa $4n+1$ olevan alkuluvun. Jos N on yhdistetty luku, sillä on esitys $N = q_1 \cdots q_s$, missä luvut q_i ovat alkulukuja. (Itse asiassa myös tapaus N on alkuluku solahtaisi tähän, silloin vain $N = q_1$.) Yritetään näyttää, että jokin luvun N alkutekijöistä q_i on muotoa $4n+1$.

Jakoyhtälön perusteella kaikilla $i = 1, \ldots, s$ on $n_i, r_i \in \mathbb{Z}$, joille

$$q_i = 4n_i + r_i \text{ ja } 0 \leq r_i \leq 3.$$

Koska N ei ole jaollinen luvulla 2, niin r_i ei voi olla 0 eikä 2. Jos kaikki luvut q_i ovat muotoa $4n+3$, luku N on joko muotoa $4n+1$ tai $4N+3$, ja *tähän todistusyritys jää jumiin.* On nimittäin

$$(4n_1+3)(4n_2+3) = 4(4n_1n_2 + 3n_1 + 3n_2 + 2) + 1.$$

Siis, jos lukuja q_i on parillinen määrä (eli s on parillinen) ja kaikki luvut q_i ovat muotoa $4n+3$, N on muotoa $4n+1$, joten emme pysty toteamaan tätä tilannetta mahdottomaksi emmekä siis pääse eteenpäin.

Huomautus: On kuitenkin totta, että muotoa $4n+1$ olevia alkulukuja on äärettömän paljon. Yleisemmin ottaen, Dirichlet todisti vuonna 1837, että jos $a, b \in \mathbb{N} \setminus \{0\}$ ja $\text{syt}(a, b) = 1$, niin äärettömän moni alkuluku on muotoa

$$p = an + b, \quad n \in \mathbb{N} \setminus \{0\}.$$

Todistus on vaikea.

6. Olkoon $p > 3$ alkuluku. Osoita, että $p^2 = 12k + 1$ jollakin $k \in \mathbb{N}$.

Vihje: On yhtäpitävää osoittaa, että luku $(p+1)(p-1)$ on jaollinen luvulla 12.

Ratkaisu. Luku $(p+1)(p-1)$ on yhdistetty luku, sillä $p+1$ on parillinen luku. Olkoon

$$(p+1)(p-1) = 2^{d_1}3^{d_2}p_3^{d_3} \cdots p_k^{d_k},$$

missä $d_i \geq 0$ kaikilla $i \in \{1, 2, ..., k\}$. Riittää osoittaa, että $d_1 \geq 2$ ja $d_2 \geq 1$ (eli että alkutekijäesityksessä luku 2 esiintyy vähintään kahdesti ja 3 vähintään kerran). Koska luvut $(p+1)$ ja $(p-1)$ ovat molemmat parillisia, on $4 \mid (p+1)(p-1)$. Siis $d_1 \geq 2$. Toisaalta, koska $p > 3$ on alkuluku, on oltava $p = 3k+1$ jollakin $k \geq 1$ (jolloin $3 \mid (p-1)$) tai $p = 3k+2$ jollakin $k \geq 1$ (jolloin $3 \mid (p+1)$). Siis $3 \mid (p+1)(p-1)$, joten $d_2 \geq 1$. Siis $(p+1)(p-1)$ on jaollinen luvulla 12.

Toinen tapa: Tehtävän voi tehdä myös huomaamalla, että luvun p on kolmosta suurempana alkulukuna oltava jotain seuraavista tyypeistä: $p = 12k+1$, $p = 12k+5$, $p = 12k+7$ tai $p = 12k+11$ jollakin $k \in \mathbb{N}$. Suorilla laskuilla nähdään, että jokaisen tyypin neliö on muotoa $12l+1$ jollakin $l \in \mathbb{N}$.

7. Matemaatikko Mauno Matikka on lueskellut luentomonistetta ja löytänyt kaamean virheen: Lause 3.2.4 ja Seuraus 3.2.3 ovat ristiriidassa keskenään! Maunon argumentti käyttää näiden harjoitusten merkintöjä $p_1, p_2, ...$ ja on seuraavanlainen: Lauseen 3.2.4 nojalla mielivaltaisen suurelle luvulle $m \in \mathbb{N}$ löytyy sellainen $n \in \mathbb{N}$, että $p_{n+1} - p_n > m$. Koska m on mielivaltaisen suuri, voidaan olettaa että $m > 2^{2^n}$. Mutta tällöin

$$p_{n+1} > p_n + m > m > 2^{2^n},$$

mikä on ristiriidassa Seurauksen 3.2.3 kanssa.

Miksi Maunon päättely on väärin?

Ratkaisu. Olkoon $m \in \mathbb{N}$. Tällöin todella on sellainen $n \in \mathbb{N}$, että $p_{n+1} - p_n > m$. *Luku n valitaan sen mukaan, mikä luku m on, eli luvun n valinta riippuu luvusta m.* On siis mieletöntä sanoa, että m olisi jokin luvusta n riippuva luku. Siis virke "Koska m on mielivaltaisen suuri, voidaan olettaa että $m > 2^{2^n}$ "on absurdi.