Lukuteoria 1 2023

Harjoitus 3: ratkaisuja

1. Olkoon $n \in \mathbb{Z}$. osoita, että $6 \mid n(n+1)(n+2)$ ja $24 \mid n(n+1)(n+2)(n+3)$.

Ratkaisu. Yksi kolmesta peräkkäisestä luvusta on jaollinen luvulla 3. Lisäksi ainakin yksi luvuista on parillinen. Ensimmäinen väite seuraa Lemmasta 2.14(1), koska $\mathrm{syt}(2,3) = 1$.

Yksi neljästä peräkkäisestä luvusta on jaollinen luvulla 4 ja jokin toinen on lisäksi jaollinen luvulla 2. Siis $8 \mid n(n+1)(n+2)(n+3)$. Lisäksi ainakin yksi luvuista on jaollinen kolmella, joten $3 \mid n(n+1)(n+2)(n+3)$. Jälkimmäinen väite seuraa Lemmasta 2.14(1), koska $\mathrm{syt}(3,8) = 1$.

2. Olkoot $a, b, c \in \mathbb{Z} - \{0\}$ siten, että $\mathrm{syt}(a,c) = 1$. Osoita, että $\mathrm{syt}(a,b) = \mathrm{syt}(a,bc)$.

Ratkaisu. Todistus perustuu kahteen havaintoon jaollisuudesta:

(1) Koska $\mathrm{syt}(a,b)$ jakaa luvun b, niin se jakaa myös luvun bc. Siis $\mathrm{syt}(a,b)$ on lukujen a ja bc yhteinen tekijä. Seurauksen 2.6 nojalla $\mathrm{syt}(a,b) \mid \mathrm{syt}(a,bc)$.[1]

(2) Määritelmän nojalla $\mathrm{syt}(a,bc) \mid bc$. Huomaamme, että $\mathrm{syt}(\mathrm{syt}(a,bc),c) = 1$, sillä $\mathrm{syt}(a,bc) \mid a$. Gaussin lemman nojalla $\mathrm{syt}(a,bc) \mid b$, joten $\mathrm{syt}(a,bc)$ on lukujen a ja b yhteinen tekijä. Seurauksen 2.6 nojalla $\mathrm{syt}(a,bc) \mid \mathrm{syt}(a,b)$.

Kohtien (1) ja (2) ja Lauseen 1.3(10) nojalla $\mathrm{syt}(a,b) = \mathrm{syt}(a,bc)$, koska $\mathrm{syt}(a,b)$ ja $\mathrm{syt}(a,bc)$ ovat luonnollisia lukuja.

3. Laske $\mathrm{syt}(234, 1026)$ Eukleideen algoritmilla. Etsi luvut $x, y \in \mathbb{Z}$, joille

$$\mathrm{syt}(234, 1026) = 234x + 1026y\,.$$

Ratkaisu. Eukleideen algoritmi antaa

$$\begin{aligned}
1026 &= 4 \cdot 234 + 90 \\
234 &= 2 \cdot 90 + 54 \\
90 &= 1 \cdot 54 + 36 \\
54 &= 1 \cdot 36 + 18 \\
36 &= 2 \cdot 18\,.
\end{aligned}$$

Siis $\mathrm{syt}(234, 1026) = 18$. Peruuttamalla saadaan

$$\begin{aligned}
\mathrm{syt}(234, 1026) &= 18 = 54 - 36 = 54 - (90 - 54) = 2 \cdot 54 - 90 = 2(234 - 2 \cdot 90) - 90 \\
&= 2 \cdot 234 - 5 \cdot 90 = 2 \cdot 234 - 5(1026) - 4 \cdot 234) = 22 \cdot 234 - 5 \cdot 1026\,,
\end{aligned}$$

joten $x = 22$ ja $y = -5$.

4. Etsi lineaarisen Diofantoksen yhtälön $654x - 9876y = 42$ ratkaisu.

[1] Tämä päätelmä ei käytä oletusta, että a ja c ovat suhteellisia alkulukuja.

Ratkaisu. Eukleideen algoritmi antaa

$$\begin{aligned}
9876 &= 654 \cdot 15 + 66 \\
654 &= 66 \cdot 9 + 60 \\
66 &= 60 \cdot 1 + 6 \\
60 &= 6 \cdot 10.
\end{aligned}$$

Siis $\mathrm{syt}(9876, 654) = 6$. Peruuttamalla saadaan

$$\begin{aligned}
6 &= 66 - 60 = 66 - (654 - 66 \cdot 9) = 9876 - 654 \cdot 15 - (654 - (9876 - 654 \cdot 15) \cdot 9) \\
&= -151 \cdot 654 + 10 \cdot 9876\,,
\end{aligned}$$

joten

$$42 = 7 \cdot 6 = -1057 \cdot 654 + 70 \cdot 9876\,.$$

Siis $x = -1057$ ja $y = -70$.

5. Etsi lineaarisen Diofantoksen yhtälön $12345x + 54321y = 9$ ratkaisu.

Ratkaisu. Eukleideen algoritmi antaa

$$\begin{aligned}
54321 &= 12345 \cdot 4 + 4941 \\
12345 &= 4941 \cdot 2 + 2463 \\
4941 &= 2463 \cdot 2 + 15 \\
2463 &= 15 \cdot 164 + 3 \\
15 &= 3 \cdot 5.
\end{aligned}$$

Siis $\mathrm{syt}(54321, 12345) = 3$. Täten saadaan

$$\begin{aligned}
9 &= 3 \cdot 3 = 3\big(2463 - (15 \cdot 164)\big) = 3\big(2463 - (4941 - 2463 \cdot 2)164\big) \\
&= 3\big((12345 - 4941 \cdot 2) - (4941 - (12345 - 4941 \cdot 2)2)164\big) \\
&= 3\Big(\big(12345 - (54321 - 12345 \cdot 4)2\big) \\
&\qquad - \big(54321 - 12345 \cdot 4 - (12345 - (54321 - 12345 \cdot 4)2)2\big)164\Big) \\
&= 10851 \cdot 12345 - 2466 \cdot 54321
\end{aligned}$$

joten $x = 10851$ ja $y = -2466$.

6. Tee Eratostheneen seula luvuille $1 - 100$.

Ratkaisu.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

7. Tee Eratostheneen seula luvuille 101 – 200.

Ratkaisu.

101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	157	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	~~169~~	~~170~~
~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~

8. Todista Lemma 3.9(2).

Ratkaisu. Väite pätee Lemman 3.9(1) nojalla, kun $n = 2$, tällöin valitaan $a = a_1$ ja $b = a_2$. Oletetaan, että väite pätee luvulla n. Olkoot $a_i \in \mathbb{Z}$ kaikilla $2 \leqslant i \leqslant n$ ja oletetaan, että $p \mid (a_1 \cdots a_n)$. Jos $p \mid a_n$, niin $p \mid a_i$ jollain $1 \leqslant i \leqslant n$. Jos $p \nmid a_n$, niin Lemman 3.9(1) nojalla $p \mid (a_1 \cdots a_{n-1})$. Induktio-oletuksen nojalla $p \mid a_i$ jollain $1 \leqslant i \leqslant n-1$. Siis $p \mid a_i$ jollain $1 \leqslant i \leqslant n$. Väite seuraa induktioperiaatteen nojalla.