Lukuteoria 1 (MATA151)
Kurssitentti, 11.4.2018
Malliratkaisut

1. (a) Määritä lukujen 75 ja 27 suurin yhteinen tekijä $\text{syt}(75, 27)$.

(b) Kuinka monta kokonaislukuratkaisua Diofantoksen yhtälöllä

$$75x + 27y = 1$$

on? Perustele.

Ratkaisu.
(a) Koska $75 = 3 \cdot 5^2$ ja $27 = 3^3$, saadaan $\text{syt}(75, 27) = 3^1 \cdot 5^0 = 3$. (Voi toki käyttää myös Eukleideen algoritmia.)

(b) Edellisen kohdan perusteella $3 \mid (75x+27y)$ kaikilla kokonaisluvuilla x, y, kun taas $3 \nmid 1$. Siis kyseisellä Diofantoksen yhtälöllä ei ole kokonaislukuratkaisuja.

2. (a) Mikä on alkuluvun määritelmä?

(b) Muotoile tarkasti Aritmetiikan peruslause. (Ei todistusta.)

(c) Mikä on luvun 130 alkutekijäesitys?

Ratkaisu.
(a) Luonnollinen luku $a \geq 2$ on alkuluku, jos sen ainoat positiiviset tekijät ovat 1 ja a.

(b) Aritmetiikan peruslause sanoo, että jokainen luonnollinen luku $a \geq 2$ on joko alkuluku tai voidaan esittää alkulukujen tulona, ja tämä esitys on tekijöiden järjestystä vaille yksikäsitteinen.

(c) $130 = 2 \cdot 5 \cdot 13$.

3. (a) Oletetaan, että p on alkuluku. Osoita, että $\sqrt{p}$ ei ole kokonaisluku.

(b) Oletetaan, että a on yhdistetty luku. Osoita, että $a \nmid [(a-1)! + 1]$.

Ratkaisu.
(a) Tehdään vastaoletus, että $\sqrt{p} = a \in \mathbb{Z}$. Koska $p \geq 2$, on oltava $1 < a < p$. Korottamalla puolittain toiseen potenssiin saadaan $p = a^2$, mistä seuraa että $a \mid p$. Tämä on ristiriidassa alkuluvun määritelmän kanssa. Siis $\sqrt{p}$ ei ole kokonaisluku.

(b) 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 $p \mid a$, pätee $p \mid [(a-1)! + 1]$, joten p jakaa luvun

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

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

4. (a) Etsi lineaarisen kongruenssiyhtälön $2x \equiv 4 \pmod 6$ kaikki kokonaisluku-ratkaisut.

(b) Osoita, että $9^{43} \equiv 2 \pmod 7$.

Ratkaisu.

(a) Huomataan, että yhtälö pätee kun $x \in \{2, 5\}$, ja yhtälö ei päde kun $x \in \{0, 1, 3, 4\}$. Siis kaikki ratkaisut muodostuvat kongruenssiluokista $[2]_6$ ja $[5]_6$.

(b) Koska luku 7 on alkuluku, Fermat'n pienen lauseen nojalla saadaan

$$9^{43} \equiv (9^6)^7 \cdot 9 \equiv 9^6 \cdot 9 = 9^7 \equiv 9 \equiv 2 \pmod 7.$$

5. (a) Osoita, että

$$\sum_{k=1}^{100} k \equiv 0 \pmod 5.$$

(b) Osoita, että

$$\sum_{k=1}^{2018} k^3 \equiv 1 \pmod 5.$$

Ratkaisu.

(a)

$$\begin{aligned}\left[\sum_{k=1}^{100} k\right]_5 &= 20\left([1]_5 + [2]_5 + [3]_5 + [4]_5 + [0]_5\right) \\ &= 20[0 + 1 + 2 + 3 + 4]_5 = 20[0]_5 \\ &= [0]_5,\end{aligned}$$

josta väite seuraa.

(b)

$$\begin{aligned}\left[\sum_{k=1}^{2018} k^3\right]_5 &= 403\left([1]_5^3 + [2]_5^3 + [3]_5^3 + [4]_5^3 + [0]_5^3\right) + [1]_5^3 + [2]_5^3 + [3]_5^3 \\ &= 403\left([1]_5 + [3]_5 + [2]_5 + [4]_5 + [0]_5\right) + [1]_5 + [3]_5 + [2]_5 \\ &= 403[0]_5 + [1]_5 \\ &= [1]_5,\end{aligned}$$

josta väite seuraa.