Lukuteoria 1 2023

Harjoitus 7: ratkaisuja

1. Ratkaise lineaarinen Diofantoksen yhtälö $6x + 21y = 15$. Etsi kaikki ratkaisut.

Ratkaisu. Kokeilemalla huomataan, että $6\cdot(-1)+21\cdot 1 = 15$. Nyt seurauksen 6.7 nojalla Diofantoksen yhtälön ratkaisut ovat $x = -1 + 7i$ ja $y = 1 - 2i$ kaikilla $i \in \mathbb{Z}$.

2. Ratkaise lineaarinen kongruenssiyhtälöpari

$$\begin{cases} x \equiv 3 \mod 7, \\ x \equiv 5 \mod 9 \end{cases}$$

Ratkaisu. Käytetään Kiinalaisen jäännöslauseen todistuksen merkintöjä. Tällöin $c_1 = 9$ ja $c_2 = 7$. Yhtälöllä $2x \equiv 9x \equiv 1 \mod 7$ on ratkaisu $d_1 \equiv 4 \mod 7$ ja yhtälöllä $7x \equiv 1 \mod 9$ on ratkaisu $d_2 \equiv 4 \mod 9$. Siis yhtälöparin ratkaisu on $3\cdot 9\cdot 4+5\cdot 7\cdot 4 = 108+140 = 248 \equiv 59 \mod 63$.

Toinen ratkaisu: Ensimmäisen yhtälön ratkaisut ovat $x = 3 + 7k$. Sijoittamalla tämä toiseen yhtälöön saadaan $3 + 7k \equiv 5 \mod 9$ eli $7k \equiv 2 \mod 9$, jonka ratkaisut ovat $k = -1 + 9\ell$. Siis $x = 3 + 7(9\ell - 1) = -4 + 63\ell$. Siis ratkaisu on $x \equiv -4 \equiv 59 \mod 63$.

3. Ratkaise lineaarinen kongruenssiyhtälöryhmä

$$\begin{cases} x \equiv 0 \mod 3, \\ x \equiv 1 \mod 4 \\ x \equiv 5 \mod 7 \end{cases}$$

Ratkaisu. Ensimmäisen yhtälön ratkaisut ovat muotoa $x = 3k$, $k \in \mathbb{Z}$. Sijoitetaan tämä toiseen yhtälöön, jolloin päädytään yhtälöön $3k \equiv 1 \mod 4$. Tällä yhtälöllä on yksi ratkaisu $\mod 4$, $k = 3 + 4j$, joten $x = 9 + 12j$, $j \in \mathbb{Z}$. Sijoitetaan tämä viimeiseen yhtälöön ja päädytään ratkaisemaan yhtälö $9 + 12j \equiv 5 \mod 7$ eli $5j \equiv 12j \equiv -4 \equiv 3 \mod 7$. Tämän yhtälön ratkaisu on $j \equiv 2 \mod 7$, joten $x = 9 + 12(2 + 7\ell) \equiv 33 \mod 84$.

4. Ratkaise lineaarinen kongruenssiyhtälöryhmä

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 2 \mod 17 \\ x \equiv 7 \mod 25 \end{cases}$$

Ratkaisu. Modulit 3, 17 ja 25 ovat suhteellisia alkulukuja, joten Kiinalaisen jäännöslauseen nojalla yhtälöparilla on yksikäsitteinen ratkaisu $\mod 1275 = 3 \cdot 17 \cdot 25$. Ensimmäisen yhtälön ratkaisut ovat muotoa $x = 2+3k$, $k \in \mathbb{Z}$. Sijoitetaan tämä toiseen yhtälöön, jolloin päädytään yhtälöön $3k \equiv 0 \mod 17$. Siis $x = 2+17\ell$. Sijoitetaan tämä kolmanteen yhtälöön ja päädytään yhtälöön $2 + 17\ell \equiv 7 \mod 25$ eli $17\ell \equiv 2 \mod 25$. Ratkaistaan vastaava lineaarinen Diofantoksen yhtälö $17\ell + 25m = 5$: Eukleideen algoritmi antaa

$$25 = 1 \cdot 17 + 8$$
$$17 = 2 \cdot 8 + 1\,.$$

Peruuttamalla saadaan

$$1 = 17 - 2 \cdot 8 = 17 - 2(25 - 17) = 3 \cdot 17 - 2 \cdot 25\,.$$

Siis $3 \cdot 17 \equiv 1 \mod 25$, joten $\ell = 5 \cdot 3 = 15 \mod 25$. Tästä saadaan ratkaisuksi

$$x = 2 + 17 \cdot 15 = 257 \mod 1275\,.$$

5. Todista Lemma 6.14.

Ratkaisu. Koska p on alkuluku, $\mathrm{syt}(p, n) \neq 1$, jos ja vain jos $p \mid n$. Välillä $1 \leqslant n \leqslant p^k$ tämä pätee luvuille kp, kun $1 \leqslant n \leqslant p^{k-1}$. Siis

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)\,.$$

6. Määritä $\phi(1000)$ ja $\phi(2343)$.

Ratkaisu. Multiplikatiivisuuden, alkutekijäesityksen ja Lemman 6.14 nojalla

$$\phi(1000) = \phi(2^3 5^3) = \phi(2^3)\phi(5^3) = 2^2 5^2 4 = 400\,.$$

Jaollisuussääntöjen opastamana löydämme alkutekijäesityksen

$$2343 = 3 \cdot 781 = 3 \cdot 11 \cdot 71\,,$$

joten

$$\phi(2343) = \phi(3)\phi(11)\phi(71) = 2 \cdot 10 \cdot 70 = 1400\,.$$

7. Määritä $\phi(75141)$.

Ratkaisu. (a) Numerosumma $7 + 5 + 1 + 4 + 1 = 18$ on jaollinen luvulla 9, joten $9 \mid 75141$. Lasku antaa $75141 = 9 \cdot 8349$. Luvun 8349 numerosumma $8 + 3 + 4 + 9 = 24$ on jaollinen luvulla 3, joten $3 \mid 8349$. Lasku antaa $8349 = 3 \cdot 2783$. Luvun 2783 vuorotteleva numerosumma on 0, joten $11 \mid 2783$. Itse asiassa $2783 = 11 \cdot 253$. Luvun 253 vuorotteleva numerosumma on 0, joten $11 \mid 253$. Itse asiassa $253 = 11 \cdot 23$ ja 23 on alkuluku. Siis $71541 = 3^3 \cdot 11^2 \cdot 23$.
(b) Lauseen 6.13 ja (a)-kohdan nojalla

$$\phi(75141) = 3^3 \cdot 11^2 \cdot 23(1 - \frac{1}{3})(1 - \frac{1}{11})(1 - \frac{1}{23}) = 43560\,.$$

8. Mitkä ovat luvun 3^{400} desimaaliesityksen kaksi viimeistä numeroa?

Ratkaisu. $3^{400} = 3^{10\phi(100)} = \left(3^{\phi(100)}\right)^{10} \equiv 1^{10} = 1 \pmod{100}$, joten viimeiset numerot ovat 01.