Lukuteoria 1 2023

Harjoitus 6: ratkaisuja

1. Osoita, että $4 \mid (a_s a_{s-1} \dots a_1 a_0)_{10}$, jos ja vain jos $4 \mid (2a_1 + a_0)$.

Ratkaisu. Koska $10 \equiv 2 \mod 4$ ja $10^k \equiv 2^k \equiv 0 \mod 4$ kaikilla $k \geqslant 2$, niin

$$a_s 10^s + \dots + a_1 10 + a_0 \equiv 0 + \dots + 0 + (a_1 2 + a_0) \mod 4,$$

eli $(a_s a_{s-1} \dots a_1 a_0)_{10} \equiv 2a_1 + a_0 \mod 4$.

2. Olkoon p alkuluku, joka ei ole 2 eikä 5. Osoita, että
(1) p jakaa äärettömän monta luvuista $9, 99, 999, 9999, 99999, \dots$.
(2) p jakaa äärettömän monta luvuista $11, 111, 1111, 11111, \dots$.

Ratkaisu. (1) Jos alkuluku p ei ole 2 eikä 5, niin $p \nmid 10$. Täten Fermat'n pienen lauseen ja Lauseen 5.4 nojalla $(10^{p-1})^n \equiv 1 \mod p$ kaikilla $n \in \mathbb{N}$. Täten $10^{n(p-1)} - 1 \equiv 0 \mod p$ eli p jakaa äärettömän monta luvuista $9, 99, 999, 9999, 9999, \dots$.

(2) Huomataan, että $999 \dots 999 = 111 \dots 111 \cdot 3^2$. Täten kohdan (1) perusteella alkuluku p, joka ei ole 2, 3 eikä 5 jakaa äärettömän monta luvuista $11, 111, 1111, 11111, \dots$. Luku 3 jakaa n-numeroisen luvun $111 \dots 111$ jos $3 \mid n$. Koska kolmella jaollisia lukuja n on äärettömästi, 3 jakaa äärettömän monta luvuista $11, 111, 1111, 11111, \dots$.

3. Osoita, että 91 on valealkuluku kannassa 3.

Ratkaisu. $91 = 7 \cdot 13$. Huomaamme, että $3^3 = 27 \equiv -1 \mod 7$ ja $3^3 \equiv 1 \mod 13$. Siis $3^{90} = (3^3)^{30} \equiv (-1)^{30} \mod 7$ ja $3^{90} = (3^3)^{30} \equiv (1)^{30} \mod 13$. Seurauksen 5.13 nojalla $3^{90} \equiv 1 \mod 91$.

4. Osoita, että 2821 on Carmichaelin luku.

Ratkaisu. Kokeilemalla huomamme, että luvun 2821 alkutekijäesitys on $2821 = 7 \cdot 13 \cdot 31$. Lisäksi $2820 = 2^2 3 \cdot 5 \cdot 47$, joten luvut $6 = 7 - 1$, $12 = 13 - 1$ ja $30 = 31 - 1$ ovat luvun $2820 = 2821 - 1$ tekijöitä. Olkoon $a \in \mathbb{Z}$ siten, että $\mathrm{syt}(a, 2821) = 1$. Tällöin $7 \nmid a$, $13 \nmid a$ ja $31 \nmid a$. Fermat'n pienen lauseen nojalla $a^6 \equiv 1 \mod 7$, $a^{12} \equiv 1 \mod 13$ ja $a^{30} \equiv 1 \mod 31$. Siis

$$\begin{aligned} a^{2820} &= (a^6)^{470} \equiv 1^{470} = 1 \mod 7 \\ a^{2820} &= (a^{12})^{235} \equiv 1^{235} = 1 \mod 13 \\ a^{2820} &= (a^{30})^{94} \equiv 1^{94} = 1 \mod 31\,. \end{aligned}$$

Seurauksen 5.13 nojalla $a^{2820} \equiv 1$ kaikilla $a \in \mathbb{Z}$, joille $\mathrm{syt}(a, 2821) = 1$. Siis 2821 on Carmichaelin luku.

5. Olkoon $n \in \mathbb{Z}$. Osoita, että $42 \mid n^7 - n$.

Ratkaisu. Fermat'n pienen lauseen nojalla $n^7 \equiv n \mod 7$ kaikilla $n \in \mathbb{Z}$. Täten $7 \mid n^7 - n$. Huomataan nyt, että

$$n^7 - n = n(n^6 - 1) = n(n^3 - 1)(n^3 + 1)\,.$$

Jos $2 \mid n$, niin $2 \mid n(n^6 - 1) = n^7 - n$. Jos $n \equiv 1 \mod 2$, niin $n^6 - 1 \equiv 1 - 1 = 0 \mod 2$. Jos $3 \mid n$, niin $3 \mid n^7 - n$. Jos $n \equiv 1 \mod 3$, niin $n^3 - 1 \equiv 1 - 1 = 0 \mod 3$, joten $3 \mid n^7 - n$. Jos $n \equiv -1 \mod 3$, niin $n^3 + 1 \equiv -1 + 1 = 0 \mod 3$, joten $3 \mid n^7 - n$.

Seurauksen 5.13 nojalla $42 = 2 \cdot 3 \cdot 7 \mid n^7 - n$.

6. Ratkaise lineaariset kongruenssiyhtälöt

(a) $5x \equiv 2 \pmod 7$,

(b) $4x \equiv 5 \pmod 6$.

Ratkaisu. (a) Kokeilemalla huomaamme, että $5 \cdot 6 = 30 \equiv 2 \mod 7$. Lauseen 6.4 nojalla tämä on ainoa ratkaisu $\mod 7$.

(b) $\mathrm{syt}(4, 6) = 2 \nmid 5$, joten Lauseen 6.4 nojalla yhtälöllä ei ole ratkaisua.

7. Ratkaise lineaarinen kongruenssiyhtälö $12x \equiv 9 \pmod{15}$.

Ratkaisu. Yhtälöllä on $3 = \mathrm{syt}(12, 15)$ ratkaisua $\mod 15$. Helposti nähdään, että $12 \cdot 2 = 24 \equiv 9 \mod 15$. Lauseen 6.4 nojalla kaikki ratkaisut ovat 2, 7 ja $12 \mod 15$.

8. Ratkaise lineaarinen kongruenssiyhtälö $240x \equiv 21 \pmod{561}$.

Ratkaisu. Eukleideen algoritmin antaa

$$\begin{aligned} 561 &= 2 \cdot 240 + 81 \\ 240 &= 2 \cdot 81 + 78 \\ 81 &= 78 + 3\,, \end{aligned}$$

ja tähän voi lopettaa, koska $3 \mid 78$. Siis $\mathrm{syt}(240, 561) = 3$. Koska $3 \mid 21$, yhtälöllä on 3 ratkaisua Lauseen 6.4 nojalla. Peruuttamalla saamme

$$\begin{aligned} 3 &= 81 - 78 \\ &= 81 - (240 - 2 \cdot 81) = 3 \cdot 81 - 240 \\ &= 3(561 - 2 \cdot 240) - 240 = 3 \cdot 561 - 7 \cdot 240\,. \end{aligned}$$

Täten

$$21 = 7 \cdot 3 \equiv 7 \cdot (-7) \cdot 240 = -49 \cdot 240\,.$$

Koska $\frac{561}{3} = 187$, kaikki ratkaisut ovat $-49 \equiv 512$, 138 ja $325 \mod 561$.