Lukuteoria 1 2023

Harjoitus 5: ratkaisuja

1. Onko $46^{78} + 89^{67}$ jaollinen luvulla 5?

Ratkaisu. Huomaamme, että $46 \equiv 1 \mod 5$ ja $89 \equiv -1 \mod 5$. Lauseen 5.4(3) nojalla $46^{78} \equiv 1^{78} = 1$ ja $89^{67} \equiv (-1)^{67} = -1$, joten Lauseen 5.4(1) nojalla $46^{78} + 89^{67} \equiv 1 - 1 = 0 \mod 5$. Siis $5 \mid 46^{78} + 89^{67}$.

2. Osoita yhtälöiden $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$ avulla, että $2^{32} \equiv -1 \pmod{641}$.

Ratkaisu. Yhtälöiden mukaan $5^4 \equiv -2^4 \pmod{641}$ ja $5 \cdot 2^7 \equiv -1 \pmod{641}$. Nostamalla jälkimmäinen yhtälö neljänteen potenssiin saadaan Lauseen 5.4 perusteella $5^4 2^{28} \equiv 1 \pmod{641}$ ja yhdistämällä tämä ensimmäisen yhtälön kanssa saadaan $1 \equiv -2^4 2^{28} = -2^{32}$, kuten haluttiin näyttää.

3. Todista Lemma 5.7.

Ratkaisu. Oletuksen nojalla on $q \in \mathbb{Z}$, jolle $b = a + qn$. Olkoon $d \in \mathbb{N}$ siten, että $d \mid a$ ja $d \mid n$. Tällöin $d \mid qn$, joten $d \mid b = a + qn$. Suurin yhteinen tekijä on tekijä, joten $\operatorname{syt}(a, n) \mid b$. Siis $\operatorname{syt}(a, n) \mid \operatorname{syt}(b, n)$. Vastaavasti nähdään, että lukujen b ja n yhteiset tekijät ovat luvun a tekijöitä, joten $\operatorname{syt}(b, n) \mid \operatorname{syt}(a, n)$.

4. Olkoon p alkuluku. Osoita, että $(x + y)^p \equiv x^p + y^p \pmod{p}$ kaikille $x, y \in \mathbb{Z}$.

Ratkaisu. Olkoon $1 \leqslant k \leqslant p - 1$. Tällöin $\binom{p}{k} = \frac{p!}{k!\,(p-k)!} \in \mathbb{N} - \{0\}$. Siis $p \mid \binom{p}{k} k!(p-k)!$. Koska $k, p - k < p$, niin Eukleideen lemman nojalla $p \nmid k!$ ja $p \nmid (p-k)!$. Siis $p \mid \binom{p}{k}$ eli $\binom{p}{k} \equiv 0 \mod p$. Binomikaavan, Lauseen 5.4 ja Seurauksen 5.5 nojalla

$$(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-1-k} \equiv x^p + y^p \mod p\,.$$

Toinen tapa: Fermat'n pienen lauseen nojalla $x^p \equiv x \mod p$ ja $y^p \equiv y \mod p$. Siis $x + y \equiv x^p + y^p \mod p$. Samoin Fermat'n pienen lauseen nojalla $(x + y)^p \equiv x + y \mod p$. Väite seuraa yhdistämällä nämä havainnot:

$$(x + y)^p \equiv x + y \equiv x^p + y^p \mod p\,.$$

5. Miksi Harjoitustehtävässä 4 ei väitetä, että $(x+y)^n \equiv x^n + y^n \pmod{n}$ kaikille $x, y \in \mathbb{Z}$ ja kaikille $n \in \mathbb{N} - \{0, 1\}$?

Ratkaisu. Esimerkiksi $(1+1)^4 = 2^4 \equiv 0 \not\equiv 2 = 1^4 + 1^4 \mod 4$.

6. Olkoot $a, b \in \mathbb{Z}$ parittomia lukuja. Osoita, että $a^2 + b^2 \neq c^2$ kaikilla $c \in \mathbb{Z}$.[1]

Ratkaisu. Koska a ja b ovat parittomia, niiden neliöille pätee $a^2 \equiv b^2 \equiv 1 \mod 4$, joten $a^2 + b^2 \equiv 2 \mod 4$. Mutta $c^2 \equiv 0 \mod 4$ tai $c^2 \equiv 1 \mod 4$, joten yhtälö $a^2 + b^2 = c^2$ on mahdoton.

7. Olkoot $a, b \in \mathbb{Z}$, $a \not\equiv 0 \mod 3$ ja $b \not\equiv 0 \mod 3$. Osoita, että $a^2 + b^2 \neq c^2$ kaikilla $c \in \mathbb{Z}$.

Ratkaisu. $a^2 \equiv 1 \mod 3$ ja $b^2 \equiv 1 \mod 3$, joten $a^2 + b^2 \equiv 2 \mod 3$. Mutta $c^2 \equiv 0 \pmod 3$ tai $c^2 \equiv 1 \pmod 3$.

8. Määritä neliönjäännökset mod 10.[2]

Ratkaisu. Jos $x \equiv y \mod 10$, niin $x^2 \equiv y^2 \mod 10$, joten luvuilla x ja y on sama neliönjäännös. Siksi riittää määrittää lukujen $0 \leqslant x \leqslant 9$ neliönjäännökset mod 10. Lasku osoittaa, että $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16 \equiv 6 \mod 10$, $5^2 = 25 \equiv 5 \mod 10$, $6^2 = 36 \equiv 6 \mod 10$, $7^2 = (-3)^2 = 9$, $8^2 = (-2)^2 = 4$ ja $9^2 = (-1)^2 = 1$. Neliönjäännökset mod 10 ovat siis 0, 1, 4, 5, 6 ja 9.

[1] Tarkastele kysymystä mod 4.

[2] Jos $x, y \in \mathbb{Z}$, $x \equiv y \pmod n$, niin Lauseen 5.4 nojalla $x^2 \equiv y^2 \mod n$.