Lukuteorian perusteet

Exercises/Harjoituksia 2018

1. (a) Show by induction/Osoita induktiolla, that/että

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

Osoita, että

(b) $a^n + 1 = (a+1)(a^{n-1} - a^{n-2} + \cdots - a + 1)$ jos $2 \nmid n$.

(c) $A^n - B^n = (A-B)(A^{n-1} + A^{n-2}B + \cdots + AB^{n-2} + B^{n-1})$.

(d) $a^3 + 1 = (a+1)(a^2 - a + 1)$.

(e) $a^4 + 4 = (a^2 - 2a + 2)(a^2 + 2a + 2)$.

2. Osoita, että

(a) $\lceil x \rceil = -\lfloor -x \rfloor \quad \forall x \in \mathbb{R}$,

(b) $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \quad \forall x \in \mathbb{R}$,

(c) $\lfloor x + k \rfloor = \lfloor x \rfloor + k \quad \forall x \in \mathbb{R}, \forall k \in \mathbb{Z}$,

(d) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \quad \forall x, y \in \mathbb{R}$,

(e) $\lfloor x \rfloor \lfloor y \rfloor \leq \lfloor xy \rfloor \quad \forall x, y \in \mathbb{R}_{\geq 0}$.

3. Let/Olkoon $x \in \mathbb{R}_{\geq 1}$ be given/annettu ja $\omega_d(x) = \#\{k \in \mathbb{Z} | 1 \leq k \leq x, d|k\}$.

(a) Näytä, että $\omega_d(x) = \lfloor x/d \rfloor$.

(b) Compute/Laske $\omega_d(1000)$, kun

$$d = 5, 25, 125, 625.$$

(c) Määrää/Determine välillä/in the interval [1000, 10000] olevien 7. jaollisten kokonaislukujen lukumäärä/ number of integers divisible by 7.

4. Olkoot $a, b, q, r \in \mathbb{Z}$ ja $a = qb + r,\ 0 \leq r < |b|$. Näytä, että

$$q = \left\lfloor \frac{a}{b} \right\rfloor, \quad r = a - b\left\lfloor \frac{a}{b} \right\rfloor$$

jos $b \in \mathbb{Z}^+$.

5. Olkoot $a, b \in \mathbb{Z}^+$ annettu. Show that there exist unigue/Näytä, että on olemassa yksikäsitteiset $q, r \in \mathbb{Z}$ such/siten, that/että

$$a = bq + r, \quad -b/2 < r \leq b/2.$$

6. Investigate/Tutki for which/millä numbers/luvuilla $n \in \mathbb{Z}_{\geq 1}$ holds/pätee
   (a) $n^2 + 1 \in \mathbb{P}$,
   (b) $n^3 + 1 \in \mathbb{P}$,
   (c) $n^4 + 1 \in \mathbb{P}$.
7. Olkoot/let $p, p+2, p+4 \in \mathbb{P}$. Show that/Näytä, että $p = 3$.
8. Olkoot $a \in \mathbb{Z},\ a \geq 2,\ m \in \mathbb{Z}^+$. Osoita, että
   (a) jos $a^m + 1 \in \mathbb{P},$ niin $2|a$ ja $m = 2^n,\ n \in \mathbb{N}$.
   (b) jos $a^m - 1 \in \mathbb{P}, m \geq 2,$ niin $a = 2$ ja $m = p \in \mathbb{P}$.
9. Olkoot $a \in \mathbb{Z},\ a \geq 2$. Osoita, että
$$\text{syt}(a^n - 1,\ a^m - 1) = a^{\text{syt}(n,m)} - 1 \quad \forall\ m, n \in \mathbb{Z}^+.$$
10. Olkoot $a, b, q, r \in \mathbb{Z}^+$. Osoita, että
    (a)
$$ab = \text{syt}(a, b)\text{pyj}(a, b).$$
    (b)
$$\text{pyj}(a, b) = ab \quad \Leftrightarrow \quad a \perp b.$$
    (c)
$$a \perp b \quad \Rightarrow \quad (a + b, a^2 + b^2)|2.$$
    (d)
$$a = qb + r \quad \Rightarrow \quad (a, b) = (b, r).$$
11. Osoita, että
$$2 \nmid \lfloor (2 + \sqrt{3})^n \rfloor \quad \forall\ n \in \mathbb{Z}^+.$$
12. Prove that/Todista, että
$$n^4 + 4^n \in \mathbb{P} \Rightarrow n = 1.$$
13. (a) Olkoon
$$Q_k = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}.$$
    Määrää/Determine detQ_k ja Q_k^{-1}.
    (b) Todista palautuskaavat/prove the recurrences (3.47).
    (c) Todista (3.48).
    (d) Osoita, että
$$\text{syt}(a, b) = s_n a + t_n b.$$
    (e) Olkoot $a = 909$ ja $b = 309$. Etsi/Find s_n ja t_n käyttämällä palautuskaavoja/by using the recurrences.
14. Kertaa ryhmän, renkaan, kokonaisalueen, kunnan sekä karakteristikan määritelmät.

15. Määrää

    (a) $\bar{3}^{-1}$ ryhmässä/in the group $\mathbb{Z}_p^*,\ p \in \mathbb{P}_{\geq 5}$.

    (b) $\bar{4}^{-1}$ ryhmässä $\mathbb{Z}_p^*,\ p \in \mathbb{P}_{\geq 5}$.

    (c) $\overline{13}^{-1}$ ryhmässä $\mathbb{Z}_{1001}^*$.

    (d) $\overline{17}^{-1}$ ryhmässä $\mathbb{Z}_{1001}^*$.

16. Määrää ryhmän $\mathbb{Z}_n^*$ kertaluku/order, kun

    (a) $n = p \in \mathbb{P}$,

    (b) $n = 24$,

    (c) $n = 13!$.

17. Muodosta Pascalin kolmio (mod p) riville $n = 12$ asti, kun $p = 2, 3, 5$.

18. Olkoot $n, m \in \mathbb{Z}^+$ ja $a, b, c, d \in \mathbb{Z}$.

    (a) Todista, että jos

    $$a \equiv b \pmod{n},\ c \equiv d \pmod{n},$$

    niin

    $$ac \equiv bd \pmod{n}.$$

    (b) Todista, että jos

    $$a \equiv b \pmod{mn},$$

    niin

    $$a \equiv b \pmod{n}.$$

19. Ratkaise yhtälöryhmä

$$\begin{cases} 3x \equiv 2 & \pmod{5} \\ 4x \equiv -2 & \pmod{7} \\ 2x \equiv 4 & \pmod{9}. \end{cases}$$

20. Olkoot $k, n, r \in \mathbb{N}$. Näytä, että

    (a)

    $$\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r};$$

    (b)

    $$\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}.$$

21. Olkoot $n, r \in \mathbb{N}$. Osoita, että

(a)
$$\binom{n}{r} < \binom{n}{r+1} \Leftrightarrow 0 \leq r < \frac{1}{2}(n-1).$$

(b)
$$\binom{n}{r} = \binom{n}{r+1} \Leftrightarrow 2 \nmid n, \quad r = \frac{1}{2}(n-1).$$

22. Osoita, että

(a)
$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

(b)
$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0, \quad n \geq 1.$$

23. Osoita, että
$$\sum_{k=0}^{n} \frac{(-1)^k}{k+1} \binom{n}{k} = \frac{1}{n+1}.$$

24. Olkoon $r \in \mathbb{N}$. Määrää summa
$$\sum_{k=1}^{n} \binom{k+r}{r+1}.$$

25. Olkoon $p \in \mathbb{P}$ ja
$$n = \sum n_i p^i, \quad 0 \leq n_i \leq p-1$$
luvun $n \in \mathbb{Z}^+$ p-kantaesitys sekä asetetaan
$$s_p(n) = \sum n_i.$$
Osoita, että
$$v_p(n!) = \frac{n - s_p(n)}{p-1}.$$

26. (a) Todista Wilsonin lause: Jos p on alkuluku, niin
$$(p-1)! \equiv -1 \pmod{p}.$$

(b) Jos $n \in \mathbb{Z}^+$ ei ole alkuluku, niin määrää
$$(n-1)! \pmod{n}.$$

27. Olkoot $a/b \in \mathbb{Q}, a \perp b, n \in \mathbb{Z}_{\geq 2}$ ja $n \big| a/b$. Näytä, että $n \perp b$.

28. (a) Onko luku
$$\frac{1}{13} - \frac{2}{5},$$
jaollinen luvulla n, kun $n = 2, 3, 4, 5, 6, 7$.

(b) Millä luvuilla $n = 2, 3, 4, 5, 6, 7$ pätee
$$\frac{1}{13} \equiv \frac{2}{5} \pmod{n}.$$

(c) Määrää sellainen luku $k \in \{0, 1, 2, ..., n-1\}$, että
$$\frac{21}{65} \equiv k \pmod{n},$$
kun $n = 2, 3, 4, 5, 6, 7$.

29. Määrää
$$\binom{1/2}{5} \pmod{7}.$$

30. Näytä, että
$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \equiv \frac{25}{7} \pmod{5^3}.$$

31. Määrää lukujen

(a) $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$

(b) $1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2}$

osoittajien alkutekijähajoitelmat, kun $p = 7, 11, 13$. Mitä huomaat?

32. Suoraan laskemalla näytä, että
$$2^{p-1} \equiv 1 + p\left(1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2}\right) \pmod{p^2},$$
kun $p = 11, 13$.

33. (a) Määrää sellainen $k \in \mathbb{Z}$, $0 \leq k \leq 10$, että
$$\frac{5}{4} \equiv k \pmod{11}.$$

(b) Määrää sellainen $h \in \mathbb{Z}$, että
$$\overline{4/5}^{\,-1} = \bar{h} \pmod{11}.$$

34. Olkoon $p \in \mathbb{P}_{\geq 5}, p \equiv 1 \pmod 3$ ja $m = (2p-2)/3$. Osoita, että
$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{m} \equiv 0 \pmod{p}.$$
Tarkat perustelut.

35. (a) Osoita kaavojen (5.131) ja (5.132) yhtäpitävyys.
    (b) Todista (5.137).
    (c) Todista (5.139).

36. Määrää

    (a)
    $$\binom{31}{11} \pmod 7;$$

    (b)
    $$\binom{3333}{110} \pmod{11};$$

    (c)
    $$\binom{p^{1000}+p^{101}-1}{p^{100}+1} \pmod p, \quad p \in \mathbb{P}.$$

37. Olkoon $p \in \mathbb{P}_{\geq 3}$. Näytä, että
    $$\binom{p+1}{j} \equiv 0 \pmod p$$
    aina, kun $2 \leq j \leq p-1$.

38. Johda ja todista kaava
    $$\sum_{k=0}^{m} k \cdot k! = (m+1)! - 1.$$

39. Johda summakaavat
    (a) $\sum\limits_{k=1}^{n} k = \frac{n(n+1)}{2}$
    (b) $\sum\limits_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$
    (c) $\sum k^3 = \frac{n^2(n+1)^2}{4}$

40. Näytä, että
    (a) $\lim\limits_{n\to\infty} \frac{f_{n+1}}{f_n} = \frac{1+\sqrt{5}}{2} = \alpha.$
    (b) $f_{n+2} > \alpha^n \ \forall\ n \geq 2.$
    (c) $f_{n+1}^2 - f_{n-1}^2 = f_{2n}.$

    (d) $f_{2k} = \lfloor \frac{\alpha^{2k}}{\sqrt{5}} \rfloor$; $f_{2k+1} = \lceil \frac{\alpha^{2k+1}}{\sqrt{5}} \rceil \ \forall\ k \in \mathbb{N}$
    (e) $f_{n+1} = \sum\limits_{k\geq 0} \binom{n-k}{k}$

(f) $f_{2n} = \sum_{k=0}^{n} \binom{n}{k} f_k$

(g) $2f_{n+m} = f_n l_m + f_m l_n$

(h) $2l_{n+m} = l_n l_m + 5 f_n f_m$

41. Osoita, että
$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} \quad \forall\, n \in \mathbb{Z}^-.$$

42. Johda generoivasta sarjasta
$$L(z) = \sum_{k=0}^{\infty} l_k z^k$$
Binet'n esitys Lucasin luvuille l_k.

43. Olkoot $d, n, M, N \in \mathbb{Z}$. Osoita

(a) $d|n \Leftrightarrow f_d | f_n$.

(b) jos $M \perp N$, niin $f_M f_N | f_{MN}$.

(c) $f_n \in \mathbb{P}_{\geq 5} \Rightarrow n \in \mathbb{P}$.

(d) $n \geq 4 \Rightarrow f_n + 1 \notin \mathbb{P}$.

44. Näytä, että
$$2^{n-1} f_n \equiv n \pmod 5.$$

45. Johda teleskooppiperiaatteella summan
$$\sum_{k=1}^{m} f_k$$
arvo.

46. Olkoon $D \in \mathbb{Z}$, $D \neq 1$, neliövapaa. Osoita, että $\sqrt{D} \notin \mathbb{Q}$.

47. (a) Näytä, että $\sqrt{6!} \notin \mathbb{Q}$.

(b) Päteekö $\sqrt{n!} \notin \mathbb{Q}$, aina kun $n \in \mathbb{Z}_{\geq 2}$?

48. Olkoot $n \in \mathbb{Z}_{\geq 3}$ ja $r \in \mathbb{Q}^+$. Osoita (Fermat'n suuren lauseen nojalla), että
$$\sqrt[n]{1 + r^n} \notin \mathbb{Q}.$$

49. (a) Osoita Neperin luvun e irrationaalisuus käyttäen luvun e^{-1} sarjaesitystä.

(b) Osoita, että ehdosta
$$ae^2 + be + c = 0, \quad a, b, c \in \mathbb{Z},$$
seuraa, että $a = b = c = 0$.

50. Olkoon $m \in 2\mathbb{Z}^+$. Osoita, että

$$2n+1 \underset{\mathbb{Q}[n]}{\mid} S_m(n).$$

51. Olkoon $p \in \mathbb{P}$.

    (a) Osoita valuaation v_p ominaisuudet 1-4.

    (b) Olkoon $A \in \mathbb{Q}$ ja $v_p(A) \geq 0 \ \forall p \in \mathbb{P}$. Näytä, että $A \in \mathbb{Z}$.

    (c) Osoita, että $\mathbb{Z}_{(p)}$ on rengas ja että sen yksikköryhmä $\mathbb{Z}^*_{(p)}$ on

$$\mathbb{Z}^*_{(p)} = \{A \in \mathbb{Q} |\ v_p(A) = 0\}.$$

52. Olkoot $p \in \mathbb{P}$, $k \in \mathbb{Z}^+$ ja $A = p^k/(k+1)$. Osoita, että

    (a) $v_p(A) \geq 0$.

    (b) jos $k \geq 2$, niin $v_p(A) \geq 1$.

    (c) jos $k \geq 3$ ja $p \geq 5$, niin $v_p(A/p^2) \geq 0$.

53. Määrää

    (a)

$$v_2\binom{1/2}{k}.$$

    (b) Määrää

$$v_p\binom{1/p}{k} \quad p \in \mathbb{P}.$$

54. Osoita, että

    (a) $n(n+1) \underset{\mathbb{Q}[n]}{\mid} S_m(n) \ \forall m \in \mathbb{Z}^+$,

    (b) $n^2(n+1)^2 \underset{Q[n]}{\mid} S_m(n) \ \forall m \in 2\mathbb{Z}^+ + 1$.

55. Olkoon $n \in \mathbb{Z}^+$. Osoita, että

    (a)

$$\binom{2n}{n} = 2^{2n}\frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots 2n}.$$

    (b)

$$\frac{(2n)!}{n!} = 2 \cdot 6 \cdot 10 \cdots (4n-2);$$

(c)
$$\frac{(2n)!}{2^n n!} = 1 \cdot 3 \cdot 5 \cdots (2n-1);$$

(d)
$$2^n n! \leq (2n)!.$$

56. Olkoot $n, r \in \mathbb{N}$. Osoita, että

(a)
$$\binom{2n}{r} < \binom{2n}{n} \quad \forall r \neq n, \quad 0 \leq r \leq 2n \geq 2.$$

(b)
$$2^n < \binom{2n}{n} < 2^{2n} \quad \forall n \geq 2.$$

(c)
$$\frac{2^{2n}}{2n} < \binom{2n}{n} < \frac{2^{2n}}{3} \quad \forall n \geq 3.$$