**Lukuteoria I**

Harjoituksia 2009

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

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

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

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

3. Määrää sellaiset luvut $n \in \mathbb{N}$, että

   (a) $n^2 + 1 \in \mathbb{P}$,

   (b) $n^3 + 1 \in \mathbb{P}$,

   (c) $n^4 + 1 \in \mathbb{P}$.

4. Kertaa ryhmän, renkaan, kokonaisalueen, kunnan sekä karakteristikan määritelmät.

5. Olkoot $a, b \in \mathbb{Z}^+$ annettu. Näytä, että on olemassa yksikäsitteiset $q, r \in \mathbb{Z}$ siten, että
$$a = bq + r, \quad -b/2 < r \leq b/2.$$

6. Olkoon $x \in \mathbb{R}_{\geq 1}$ 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) Laske $\omega_d(1000)$, kun
$$d = 5, 25, 125, 625.$$

   (c) Määrää 7. jaolliset kokonaisluvut väliltä [1000, 10000].

7. Osoita, että
$$2 \nmid \lfloor (2 + \sqrt{3})^n \rfloor \quad \forall\ n \in \mathbb{Z}^+.$$

8. Olkoot $p, p + 2, p + 4 \in \mathbb{P}$. Näytä, että $p = 3$.

9. Olkoot $a, b \in \mathbb{Z}^+$. Osoita, että
$$ab = \mathrm{syt}(a, b)\mathrm{pyj}(a, b).$$

10. (a) Olkoon

$$Q_k = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}.$$

Määrää $\det Q_k$ ja $Q_k^{-1}$.

(b) Osoita, että

$$\mathrm{syt}(a, b) = s_n a + t_n b.$$

11. Olkoon $p \in \mathbb{P}_{\geq 5}$. Määrää

(a) $\bar{3}^{-1}$,

(b) $\bar{4}^{-1}$. ryhmässä $\mathbb{Z}_p^*$.

12. Määrää ryhmän $\mathbb{Z}_n^*$ kertaluku, kun

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

(b) $n = 24$,

(c) $n = 13!$.

13. (a) Todista Wilsonin lause:

Jos $p$ on alkuluku, niin $(p-1)! \equiv -1 (\mathrm{mod}\ p)$.

(b) Jos $n$ ei ole alkuluku, niin $(n-1)! \not\equiv -1 \pmod{n}$.

14. (a) Olkoot $p, q \in \mathbb{P}$ ja $p \neq q$. Näytä, että yhtälöistä

$$\begin{cases} a \equiv b \pmod{p} \\ a \equiv b \pmod{q} \end{cases}$$

seuraa

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

(b) Olkoot $m_i \in \mathbb{Z}$ ja $m_i \perp m_j$ kaikilla $i \neq j$. Näytä, että yhtälöistä

$$a \equiv b \pmod{m_i} \quad \forall \quad i = 1, ..., r$$

seuraa

$$a \equiv b \pmod{m_1 \cdots m_r}.$$

15. Ratkaise yhtälöryhmä

$$\begin{aligned} 3x &\equiv 2 \quad &&(\mathrm{mod}\ 5) \\ 4x &\equiv -2 \quad &&(\mathrm{mod}\ 7) \\ 2x &\equiv 4 \quad &&(\mathrm{mod}\ 9). \end{aligned}$$

16. Näytä, että

(a) $\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r}$,

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

17. Osoita, että

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

18. Osoita, että

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

19. Osoita, että

 (a) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.
 (b) $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$ kun $n \geq 1$.

20. (a) Osoita induktiolla, 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) $A^n - B^n = (A-B)(A^{n-1} + A^{n-2}B + \cdots + AB^{n-2} + B^{n-1})$.

21. Johda ja todista kaava

$$\sum_{k=0}^{m} k \cdot k! = (m+1)! - 1.$$

22. Todista, että

$$n^4 + 4^n \in \mathbb{P} \Rightarrow n = 1.$$

23. 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?

24. Olkoot $a \in Z,\ a \geq 2,\ m \in \mathbb{Z}^+$. 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 $m = p \in \mathbb{P}$.

25. Olkoot $a \in \mathbb{Z},\ a \geq 2$. Osoita, että

$$\text{s.y.t.}(a^n - 1,\ a^m - 1) = a^{\text{s.y.t.}(n,m)} - 1 \ \forall\ m, n \in \mathbb{Z}^+.$$

26. Määrää luvun

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

alkutekijähajoitelma.

27. Todista binomikaava.

28. 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 $p = 11, 13$.

29. Olkoon $p \in \mathbb{P}_{\geq 5}$ ja

$$\prod_{k=1}^{p-1}(x-k) = \sum_{i=0}^{p-1}(-1)^i W_i x^i.$$

   (a) Määrää kertoimen $W_{p-3}$ eksplisiittinen lauseke ja osoita, että $p \big| W_{p-3}$.

   (b) Määrää kertoimien $W_i$ palautuskaava.

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

31. Näytä, että

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

32. Määrää sellainen $k \in \mathbb{Z}$, että

$$\overline{4/5}^{-1} = \bar{k} \pmod{11}.$$

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

34. Määrää

   $\binom{31}{11} \pmod{p}$, kun

   $p = 7, 11$.

35. Johda summakaavat

   (a) $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

   (b) $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

   (c) $\sum k^3 = \frac{n^2(n+1)^2}{4}$

36. Näytä, että

   (a) $\lim_{n\to\infty} \frac{f_{n+1}}{f_n} = \frac{1+\sqrt{5}}{2} = \alpha$.

(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) $f_{2n} = \sum\limits_{k=0}^{n} \binom{n}{k} f_k$

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

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

37. Osoita, että

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

38. Johda generoivasta sarjasta

$$L(z) = \sum_{k=0}^{\infty} l_k z^k$$

Binet'n esitys Lucasin luvuille $l_k$.

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

40. Olkoon $p \in \mathbb{P}_{\geq 3}$. Näytä, että

$$\binom{p+1}{j} \equiv 0 \pmod{p}$$

aina, kun $2 \leq j \leq p - 1$.

41. Näytä, että

$$2^{n-1} f_n \equiv n \pmod{5}.$$

42. Johda teleskooppiperiaatteella summan

$$\sum_{k=1}^{m} f_k$$

arvo.

43. Osoita, että formaalille eksponenttisarjalle $e^T = \mathrm{EXP}(T)$ pätee

(a) $e^{0\cdot T} = 1$.

(b) $e^{-T} = \frac{1}{e^T}$.

(c) $e^{nT} = (e^T)^n \ \forall n \in \mathbb{Z}$.

(d) $e^{iT} = \cos T + i \sin T \ ; \ i^2 = -1$.

44. Määrää 10 ensimmäistä Bernoullin lukua.

45. Osoita generoivan sarjan avulla tehtävän 36 kohtien e) ja f) tulokset.

46. Olkoot $A(T), B(T) \in \mathbb{R}[[T]]$ ja $A(T)B(T) = 1$.
Näytä, että $\mathrm{ord} A(T) = \mathrm{ord} B(T) = 0$.

47. Määrää sellainen $A(T) \in \mathbb{Z}[[T]]$, että

$$(1 - T - T^2)A(T) = P(T),$$

missä

(a) $P(T) = T$.

(b) $P(T) = 2 + T$.

48. Osoita, että

$$\mathrm{BIN}_{1/2}(T)^2 = 1 + T.$$

49. Määrää summat

$$S_m(n) = 1^m + 2^m + \cdots + n^m,$$

kun $m = 1, \cdots, 5$.

50. Määrää Bernoullin polynomit $B_n(x)$, kun $n = 0, 1, \cdots, 5$.

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

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

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

(a) Osoita valuaation $v_p$ ominaisuudet 1-4.

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

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

53. 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 $v_p(A/p^2) \geq 0$.

54. Olkoot $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Osoita, että

(a) $a(a^m - 1)B_m \in \mathbb{Z}$.

(b) $a^m(a^m - 1)B_m/m \in \mathbb{Z}$.

55. Määrää summa

$$\sum_{k=1}^{n} \binom{k+r}{r+1}.$$

56. Määrää sarjojen

(a) $\sinh(T)$,

(b) $\cosh(T)$,

(c) $\coth(T)$,

(d) $\tanh(T)$,

(e) $\cot(T)$,

(f) $\tan(T)$,

(g) $1/\cosh(T)$,

(h) $1/\sinh(T)$,

(i) $1/\cos(T)$,

(j) $1/\sin(T)$

kertoimet.

57. Todista Bernoullin polynomien ominaisuudet

(a) $B_n(0) = (-1)^n B_n(1) = B_n$.

(b) $\frac{d}{dx} B_n(x) = nB_{n-1}(x)$.

(c) $B_n(x+1) - B_n(x) = nx^{n-1}$.

(d) $B_n(1-x) = (-1)^n B_n(x)$.

(e) $B_n(1/2) = (2^{1-n} - 1)B_n$.

58. Osoita, että

$$1^m + 2^m + \cdots + n^m = \frac{B_{m+1}(n+1) - B_{m+1}}{m+1}.$$

59. Olkoon $p \in \mathbb{P}$, näytä, että

$$pB_2 \equiv 1^2 + 2^2 + \cdots + (p-1)^2 \pmod{p}.$$

60. (a) Olkoon $p \in \mathbb{P}, p \equiv 1(\text{mod } 3)$. Näytä, että

$$B_{2p} = \frac{1}{6} + A_{2p},$$

missä $A_{2p} \in \mathbb{Z}$.

(b) Tarkastele lukujen $B_{2k}$ nimittäjiä $D_{2k}$, kun $k = 0, 1, \cdots, 13, 19$.

(c) Osoita, että alkuluvut 5, 7, 11, 13, 17 ovat säännöllisiä.
$B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_4 = -1/30, B_6 = 1/42, B_8 = -1/30,$
$B_{10} = 5/66, B_{12} = -691/2730, B_{14} = 7/6.$

61. Asetetaan $a_1 = 1$ ja

$$a_{n+1} = \frac{1}{n}(1 + a_1^2 + \cdots + a_n^2), n \in \mathbb{Z}^+.$$

Tutki väitettä

$$a_n \in \mathbb{Z} \quad \forall\ n \in \mathbb{Z}^+.$$

62. Näytä, että

$$E_{2k} = -\frac{4^{2k+1}}{2k+1} B_{2k+1}\left(\frac{1}{4}\right).$$

63. Osoita, että

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

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

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

65. Näytä, että

(a) $E_n \in \mathbb{Z}\ \forall n \in \mathbb{N},$

(b) $s_1(n,k) \in \mathbb{Z}\ \forall n \in \mathbb{N}, 0 \leq k \leq n,$

(c) $S_2(n,k) \in \mathbb{Z}\ \forall n \in \mathbb{N}, 0 \leq k \leq n.$

66. Näytä, että

(a) $s_1(n,0) = \delta_{n,0}, s_1(n,n) = 1,$

(b) $s_1(n,1) = (-1)^{n-1}(n-1)!,$

(c) $s_1(n,2) = (-1)^n(n-1)!H_{n-1},$

(d) $s_1(n,n-1) = -\binom{n}{2}.$

67. Näytä, että

(a) $S_2(n,m) = S_2(n-1,m-1) + mS_2(n-1,m),$

(b) $S_2(n,m) = \frac{1}{m!}\sum_{i=0}^{m}(-1)^i\binom{m}{i}(m-i)^n$

aina, kun $n \in \mathbb{Z}^+, 0 \le m \le n$.

68. Olkoon $\delta = xD = x\frac{d}{dx}$ ja $f = f(x), g = g(x)$. Näytä, että

(a)
$$D^n fg = \sum_{k=0}^{n}\binom{n}{k}D^k f D^{n-k} g.$$

(b)
$$x^n D^n f = \sum_{k=0}^{n} s_1(n,k)\delta^k f.$$

(c)
$$\delta^n f = \sum_{k=0}^{n} S_2(n,k)x^k D^k f.$$

69. Osoita, että

$$B_m = \sum_{k=0}^{m}\frac{(-1)^k k!}{k+1}S_2(m,k).$$

70. Määrää Stirlingin kolmiot (mod $p$) 8. riville asti, kun $p = 2, 3, 5, 7$.

71. Olkoon $\alpha \in \mathbb{C}^*$. Osoita, että jonot

(a) $(\alpha^n),\ (n\alpha^n)$,

(b) $(\alpha^n), (n\alpha^n), (n^2\alpha^n)$

(c) $(1), (H_n)$,

(d) $(n!), (n!H_n)$.

ovat lineaarisesti vapaita $\mathbb{C}$:n yli.

72. Osoita differenssioperaattoreille

(a) $\triangle^n = (-1)^n\sum_{k=0}^{n}\binom{n}{k}(-E)^k$,

(b) $E^n = \sum_{k=0}^{n}\binom{n}{k}\triangle^k$ .

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

74. Olkoot $n \in \mathbb{Z}_{\ge 3}$ ja $r \in \mathbb{Q}^+$. Osoita (Fermat'n suuren lauseen nojalla), että

$$\sqrt[n]{1+r^n} \notin \mathbb{Q}.$$

75. (a) Ratkaise rekursio

$$a_{n+2} - (n+3)a_{n+1} + (n+1)a_n = 0.$$

(b) Olkoot $f_n = n!$ ja $e_n = n! \sum_{k=0}^{n} \frac{1}{k!}$. Osoita, että $\{(e_n), (f_n)\}$ on (a)-kohdan ratkaisukanta.

(c) Määrää rekursion

$$(n+2)b_{n+2} - (n+3)b_{n+1} + b_n = 0$$

ratkaisukanta.

(d) Ratkaise rekursio

$$a_{n+2} - (n+1)a_{n+1} - (n+1)a_n = 0.$$

(e) Olkoon $g_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$. Osoita, että $\{(f_n), (g_n)\}$ on (d)-kohdan ratkaisukanta.

76. Osoita rationaalilukujen ja -funktioiden supistamis- ja laventamissäännöt.

77. Osoita, että

(a) $\sum_{k=0}^{n} \binom{n}{k}\binom{m+k}{r}(-1)^k = (-1)^n \binom{m}{r-n}$.

(b) $\sum_{k=0}^{n} \binom{n}{k}\binom{k}{r}(-1)^k = (-1)^n \delta_{nr}$.

78. Olkoot $(a_n), (b_n) \subseteq \mathbb{C}$. Osoita identiteettien

$$a_n = \sum_{k=0}^{n} \binom{n}{k} b_k \quad \text{ja}$$

$$b_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} a_k$$

yhtäpitävyys.

79. Määrää

$$v_2 \binom{1/2}{k}, v_p \binom{1/p}{k} \quad p \in \mathbb{P}.$$

80. Olkoon $p \in \mathbb{P}$ ja

$$n = \sum n_i p^i, \quad 0 \le n_i \le p-1$$

luvun $n \in \mathbb{Z}^+$ $p$-kantaesitys sekä asetetaan

$$s_p(n) = \sum n_i.$$

Osoita, että

$$v_p(n!) = \frac{n - s_p(n)}{p - 1}.$$

81. (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 $a = b = c = 0$.