דף נוסחאות – תורת המספרים

מוסכמה: כל המספרים הם שלמים אלא אם כן צוין אחרת

1. **קבוצות מספרים:**
   הטבעיים (natural numbers): $\mathbb{N} = \{0,1,2,\dots\}$.
   השלמים (integers): $\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$
   השלמים החיוביים: $\mathbb{Z}^+ = \{1,2,3,\dots\}$
   הרציונליים (rationals): $\mathbb{Q} = \{p/q \ : \ p,q \in \mathbb{Z},\ q \neq 0\}$
   הממשיים (real numbers): $\mathbb{R}$.
   הממשיים החיוביים: $\mathbb{R}^+$
   המרוכבים (complex numbers): $\mathbb{C} = \{a+bi \ : \ a,b \in \mathbb{R}\}$

2. **עיקרון הסדר הטוב (well-ordering principle):** כל תת-קבוצה לא ריקה של $\mathbb{N}$ מכילה מספר מינימלי.

3. **הגדרה:** נאמר ש-a **מחלק** את b, ומסמנים $a \mid b$, אם קיים c כך ש- $ac = b$.

4. **משפט החילוק (division algorithm):** אם a,b הם מספרים כאשר $b \neq 0$, אזי קיים זוג מספרים **ייחודי** q,r כך ש- $a = qb + r$ וכך ש- $0 \le r < |b|$. למספר r קוראים **שארית**, ומסמנים $r = a \bmod b$.

5. **הגדרה:** אם $x \in \mathbb{R}$ אזי $\lfloor x \rfloor$ מסמן את המספר השלם הכי גדול שלא גדול מ-x.

6. **טענה:** אם $x \in \mathbb{R}^+$ ו- $d \in \mathbb{Z}^+$ אזי קיימים בדיוק $\lfloor x/d \rfloor$ מספרים שלמים חיוביים לא גדולים מ-x שמתחלקים ב-d.

7. **הגדרה:** קבוצת המחלקים של n: $D(n) = \{m : m \mid n\}$.

8. **הגדרה: המחלק המשותף המקסימלי (greatest common divisor)** של a,b, שמסומן (a,b) או $\gcd(a,b)$, נתון ע"י:

$$\gcd(a,b) = \max(D(a) \cap D(b))$$

9. **הגדרה:** אם $\gcd(a,b) = 1$ אזי נאמר ש- a,b הם **זרים (relatively prime)**.

10. **הגדרה:** מספר $n > 1$ נקרא **ראשוני (prime)** אם אין לו מחלקים חיוביים חוץ מ-1 ו-n. אחרת הוא נקרא **פריק (composite)**.

11. **למה:** $\gcd(a,b) = \gcd(a - kb, b)$

12. **משפט ה- gcd המורחב (extended gcd theorem):** יהיו a,b מספרים, ונסמן $d = \gcd(a,b)$. אזי קיימים מספרים x,y כך ש- $d = ax + by$.

13. **למה:** כל מחלק משותף של a,b מחלק את $\gcd(a,b)$.

14. **למה:** אם a,b הם זרים וכל אחד מהם מחלק את c, אזי גם ab מחלק את c.

15. **למה:** $\gcd(ac,bc) = c\gcd(a,b)$

16. **למה:** יהיו a,b מספרים, ונסמן $d = \gcd(a,b)$. אזי $a/d,\ b/d$ הם זרים.

17. **למה של אוקלידס (Euclid's lemma):** אם a,b הם זרים ו- $a \mid bc$, אזי $a \mid c$.

18. **הגדרה: הכפולה המשותפת המינימלית (least common multiple)** של a,b, שמסומנת $\mathrm{lcm}(a,b)$, נתונה ע"י

$$\mathrm{lcm}(a,b) = \min\{m \in \mathbb{Z}^+ : a \mid m, b \mid m\}$$

19. **למה:** $ab = \mathrm{lcm}(a,b) \cdot \gcd(a,b)$

20. **למה:** כל כפולה משותפת של a,b היא כפולה של $\mathrm{lcm}(a,b)$.

21. **למה:** תהי $ax + by = c$ משוואה כאשר a,b,c הם מספרים נתונים ו- x,y הם נעלמים. אזי למשוואה יש פתרון אם ורק אם c היא כפולה של $d = \gcd(a,b)$. במקרה כזה, אם $(x = x_0,\ y = y_0)$ הוא פתרון מסוים למשוואה, אזי כל פתרון למשוואה הוא מהצורה

$$\left(x = x_0 + \frac{b}{d}t,\ \ y = y_0 - \frac{a}{d}t\right)$$

22. **משפט (אינדוקציה – induction):** תהי $S(n)$ טענה התלויה במספר $n \in \mathbb{N}$. נניח ש-
- $S(0)$ היא נכונה,
- לכל $n \in \mathbb{N}$, אם $S(n)$ היא נכונה, אז גם $S(n+1)$ היא נכונה.

אזי $S(n)$ נכונה לכל $n \in \mathbb{N}$.

23. **המשפט היסודי של האריתמטיקה (fundamental theorem of arithmetic):** כל מספר חיובי ניתן להיכתב כמכפלה של מספרים ראשוניים באופן **ייחודי** (עד כדי סדר הגורמים).

24. **למה:** אם n אינו ראשוני, אזי יש לו גורם ראשוני קטן-שווה ל- $\sqrt{n}$.

25. **למה:** יהי $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ הפירוק לראשוניים של שני מספרים a, b. אז:

$$\gcd(a,b) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \cdots p_n^{\min\{a_n,b_n\}},$$

$$\operatorname{lcm}(a,b) = p_1^{\max\{a_1,b_1\}} p_2^{\max\{a_2,b_2\}} \cdots p_n^{\max\{a_n,b_n\}}$$

26. **הגדרה:** המספרים a, b נקראים **שקולים (congruent)** מודולו m, ומסמנים $a \equiv b \pmod{m}$, אם $m \mid (b-a)$.

27. **למה:** $a \equiv b \pmod{m}$ אם ורק אם $a \bmod m = b \bmod m$.

28. **למה:** היחס מודולו m הוא יחס שקילות, כלומר הוא מקיים את התכונות הבאות:
- $a \equiv a \pmod{m}$.
- אם $a \equiv b \pmod{m}$ אז גם $b \equiv a \pmod{m}$.
- אם $a \equiv b \pmod{m}$ וגם $b \equiv c \pmod{m}$ אז גם $a \equiv c \pmod{m}$.

29. **למה:** נניח ש- $a \equiv b \pmod{m}$ וגם $c \equiv d \pmod{m}$. אזי:
1. $a \pm c \equiv b \pm d \pmod{m}$
2. $ac \equiv bd \pmod{m}$
3. $a^k \equiv b^k \pmod{m}$

30. **מסקנה:** יהי $p(x)$ פולינום בעל מקדמים שלמים. אם $a \equiv b \pmod{m}$ אזי $p(a) \equiv p(b) \pmod{m}$.

31. **למה:** נניח ש- $ac \equiv bc \pmod{m}$, ונסמן $d = \gcd(c,m)$. אזי $a \equiv b \pmod{m/d}$.

32. **למה:** אם $a \equiv b \pmod{m_1}$ וגם $a \equiv b \pmod{m_2}$, אזי $a \equiv b \pmod{\operatorname{lcm}(m_1,m_2)}$.

33. **למה:** תהי $ax \equiv b \pmod{m}$ משוואה כאשר a, b, m הם מספרים נתונים ו-x הוא נעלם. נסמן $d = \gcd(a,m)$. אזי:
- אם $d \nmid b$ אזי למשוואה אין פתרון.
- אחרת, למשוואה יש d פתרונות לא שקולים מודולו m.

34. **הגדרה:** יהיו a, m מספרים זרים. אזי **ההופכי** של a מודולו m **(modular inverse)** הוא הפתרון x למשוואה $ax \equiv 1 \pmod{m}$.

35. **למה:** יהיו a, b, c, d, r, s, m מספרים נתונים, כאשר m זר ל- $(ad - bc)$. אזי למערכת

$$\begin{aligned} ax + by &\equiv r \pmod{m} \\ cx + dy &\equiv s \pmod{m} \end{aligned}$$

יש פתרון יחיד מודולו m.

36. **למה:** יהי $p > 2$ מספר ראשוני, ויהי a מספר שאינו מתחלק ב-p. אזי a הוא ההופכי של עצמו מודולו p^k אם ורק אם $a \equiv \pm 1 \pmod{p^k}$.

37. **למה:** נתבונן במשוואה $x^2 \equiv 1 \pmod{2^k}$.
- אם $k = 1$ אזי הפתרון היחיד הוא $x \equiv 1$.
- אם $k = 2$ אזי יש שני פתרונות: $x \equiv \pm 1$.
- אם $k \geq 3$ אזי יש ארבעה פתרונות: $x \equiv \pm 1$, $x \equiv 2^{k-1} \pm 1$.

38. **משפט השאריות הסיני (Chinese remainder theorem):** יהיו $m_1, m_2, \dots, m_k$ מספרים זרים אחד לשני, ויהיו $a_1, a_2, \dots, a_k$ מספרים כלשהם. אז למערכת

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

יש פתרון יחיד מודולו $M = m_1 m_2 \dots m_k$: נסמן $M_i = M/m_i$ עבור $1 \leq i \leq k$, ויהי y_i ההופכי של M_i מודולו m_i. אז הפתרון היחיד הוא $x = \sum_{i=1}^{k} a_i M_i y_i$.

39. **משפט וילסון (Wilson's theorem):**
p הוא ראשוני אם ורק אם $(p-1)! \equiv -1 \pmod{p}$.

40. **המשפט הקטן של פרמה (Fermat's little theorem):**
אם p ראשוני ו-a זר ל-p, אזי $a^{p-1} \equiv 1 \pmod{p}$.

41. **מסקנה:** אם p ראשוני, אזי $a^p \equiv a \pmod{p}$.

42. **הגדרה:** מספר פריק n ייקרא **פסאודו-ראשוני (pseudoprime)** לבסיס a, אם n זר ל-a וגם $a^{n-1} \equiv 1 \pmod{n}$.

43. **הגדרה:** אם n פריק, ומתקיים $a^{n-1} \equiv 1 \pmod{n}$ לכל a שזר ל-n, אזי n נקרא **מספר קרמייקל (Carmichael number)**.

44. **משפט:** מספר פריק n הוא מספר קרמייקל אם ורק אם $n = p_1 p_2 \dots p_k$ כאשר $p_1, p_2, \dots, p_k$ שונים אחד מהשני, ו- $(p_i - 1) \mid (n-1)$ לכל $1 \le i \le k$.

45. **הגדרה (פונקצית אוילר – Euler's totient function):** $\varphi(n)$ הוא מספר המספרים בין 1 ל-n שזרים ל-n: $\varphi(n) = |\{1 \le i \le n : \gcd(i,n) = 1\}|$

46. **משפט (אוילר – Euler's theorem):** אם a זר ל-n אזי $a^{\varphi(n)} \equiv 1 \pmod{n}$.

47. **מסקנה:** אם a זר ל-n אזי ההופכי של a מודולו n הוא $a^{\varphi(n)-1}$.

48. **למה:** אם p ראשוני, אזי $\varphi(p) = p - 1$, ובאופן יותר כללי, $\varphi(p^k) = p^{k-1}(p-1)$.

49. **למה:** אם m, n זרים, אזי $\varphi(mn) = \varphi(m)\varphi(n)$.

50. **מסקנה:** יהי $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ הפירוק של n לראשוניים. אזי:

$$\begin{aligned}\varphi(n) &= p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1)\cdots p_k^{a_k-1}(p_k-1)\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\end{aligned}$$

51. **למה:** $\varphi(n)$ זוגי לכל $n > 2$.

52. **למה:** אם ל-n יש k מחלקים ראשוניים אי-זוגיים שונים, אזי $2^k \mid \varphi(n)$.

53. **משפט:** $n = \sum_{d \mid n} \varphi(d)$

54. **למה:** אם $p > 2$ ראשוני ו-a זר ל-p, אזי למשוואה $x^2 \equiv a \pmod{p}$ יש או 0 או 2 פתרונות מודולו p.

55. **הגדרה:** יהי $p > 2$ ראשוני ו-a זר ל-p. אם קיים x כך ש- $x^2 \equiv a \pmod{p}$ אזי a נקרא **שארית ריבועית (quadratic residue)** מודולו p. אחרת, a נקרא **אי-שארית ריבועית (quadratic nonresidue)** מודולו p.

56. **למה:** יהי $p > 2$ ראשוני. אזי יש בדיוק $(p-1)/2$ שאריות ריבועיות ובדיוק $(p-1)/2$ אי-שאריות ריבועיות מודולו p.

57. **הגדרה (סימן לז'נדר – Legendre symbol):** יהי $p > 2$ ראשוני ו-a זר ל-p. אזי $\left(\frac{a}{p}\right) = +1$ אם a היא שארית ריבועית מודולו p, ו- $\left(\frac{a}{p}\right) = -1$ אחרת.

58. **משפט (מבחן אוילר – Euler's criterion):** יהי $p > 2$ ראשוני ו-a זר ל-p. אזי $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

59. **למה:** יהי $p > 2$ ראשוני ויהיו a, b זרים ל-p. אזי: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

60. **למה (גאוס – Gauss' lemma):** יהי $p > 2$ ראשוני ו-a זר ל-p. יהי k מספר השאריות מבין

$$a \bmod p, \quad 2a \bmod p, \quad \ldots, \quad \left(\frac{p-1}{2} \cdot a\right) \bmod p$$

שגדולות מ- $p/2$. אזי $\left(\frac{a}{p}\right) \equiv (-1)^k \pmod{p}$.

61. **למה:** יהי $p > 2$ ראשוני. אזי:

- $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv 3 \pmod{4} \end{cases}$
- $\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv 1, 7 \pmod{8} \\ -1, & p \equiv 3, 5 \pmod{8} \end{cases}$
- $\left(\frac{-2}{p}\right) = \begin{cases} 1, & p \equiv 1, 3 \pmod{8} \\ -1, & p \equiv 5, 7 \pmod{8} \end{cases}$