לינארית 2 הרצאה מספר 10

מבוא לתורת המספרים

הגדרה: מספר טבעי $p \geq 2$ נקרא מספר ראשוני, אם יש לו בדיוק שני מחלקים טבעיים: p ו- 1.

הערה: 1 לא נחשב מספר ראשוני.

המספרים הראשוניים הם: $2,3,5,7,11,13,17,19,23,29,\dots$

משפט היסודי של אריתמטיקה: יהי $2 \leq n \in \mathbb{N}$. אזי קיימים מספרים ראשוניים $p_1, p_2, \dots, p_k$ ומספרים טבעיים $\alpha_1, \alpha_2, \dots, \alpha_k$ כך ש- $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ והצגה זו היא ההצגה היחידה עד כדי סדר האגפים במכפלה.

דוגמה:

$$540 = \frac{540 \quad 270 \quad 135 \quad 45 \quad 15 \quad 5 \quad 1}{2 \quad 2 \quad 3 \quad 3 \quad 3 \quad 5} = 2^2 \cdot 3^3 \cdot 5^1$$

הגדרה: יהיו $m,n \in \mathbb{N}$. המספר הטבעי הגדול ביותר d שמחלק גם את m וגם את n נקרא המחלק המשותף המקסימלי של m ו- n. סימון $d = gcd(m,n)$

המספר הטבעי הקטן ביותר L נקרא הכפולה המשותפת המינימלית של m ו- n אם L המספר המינימלי שמתחלק גם ב- m וגם ב- n. סימון: $L = Lcm(m,n)$

למשל: $m = 24$, $n = 60$.

$$gcd(24,60) = 12 \qquad Lcm(24,60) = 120$$

$$\left.\begin{aligned} 24 &= 2^3 \cdot 3 \\ 60 &= 2^2 \cdot 3 \cdot 5 \end{aligned}\right\} \begin{aligned} gcd(24,60) &= 2^2 \cdot 3^1 = 4 \cdot 3 = 12 \\ Lcm(24,60) &= 2^3 \cdot 3^1 \cdot 5^1 = 8 \cdot 3 \cdot 5 = 120 \end{aligned}$$

טענה: עבור $m,n \in \mathbb{N}$ מתקיים: $gcd(m,n) \cdot Lcm(m,n) = m \cdot n$

הוכחה: נסמן: $m = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} \cdot r$ ונסמן: $n = p_1^{\beta_1} \cdot \dots \cdot p_k^{\beta_k} \cdot s$ כאשר $p_1, \dots, p_k$ המחלקים הראשוניים המשותפים, כאשר $\alpha_1 \dots \alpha_k, \beta_1 \dots \beta_k$ טבעיים. כאשר אין חלק משותף בין r ל- s כלומר $gcd(r,s) = 1$

בסימונים האלה:

$$gcd(m,n) = p_1^{\min(\alpha_1,\beta_1)} \cdot \dots \cdot p_k^{\min(\alpha_k,\beta_1)}$$

$$Lcm(m,n) = p_1^{\max(\alpha_1,\beta_1)} \cdot \dots \cdot p_k^{\max(\alpha_k,\beta_1)} \cdot r \cdot s$$

$$\Downarrow$$

$$gcd(m,n) \cdot Lcm(m,n) = \prod_{j=1}^{k} p_j^{\min(\alpha_j,\beta_j)} \cdot \prod_{i=1}^{k} p_i^{\max(\alpha_i,\alpha_j)} \cdot r \cdot s$$

$$p^{\min(\alpha,\beta)} \cdot p^{\max(\alpha,\beta)} = p^{\alpha+\beta}$$

$$= \prod_{j=1}^{k} p_j^{\alpha_j+\beta_i} \cdot r \cdot s = \underbrace{\prod_{j=1}^{k} p_j^{\alpha_j} \cdot r}_{m} \cdot \underbrace{\prod_{j=1}^{k} p_j^{\beta_j} \cdot s}_{n} = m \cdot n$$

טענה: יהיו $m,n\in\mathbb{N}$ ויהי $d=\gcd(m,n)$, אז קיימים $\alpha,\beta\in\mathbb{Z}$ כך ש- $d=\underbrace{\alpha m+\beta n}_{\text{צירוף לינארי}}$ - להוכיח בכל

הוכחה: נתבונן בקבוצה: $S=\{\alpha n+\beta n \mid \alpha,\beta\in\mathbb{Z}\}$

נסמן ב- d_0 את המספר החיובי הקטן ביותר ב- S.

נוכיח כי $d=d_0$

מתקיים: $\begin{cases} d \text{ מחלק את } m \\ d \text{ מחלק את } n \end{cases} \Leftarrow d$ מחלק את $\alpha m+\beta n$ לכל α,β ולכן $d\mid d_0$ (d מחלק את d_0)

נראה כי d_0 מחלק את d (כלומר $d_0\mid d$).

לפי עקרון החילוק עם שארית מתקיים: $m=d_0\cdot q+r$ כאשר שארית r היא $0<r<d_0$.

מכאן: $r=\underbrace{m}_{\in S}-\underbrace{d_0\cdot q}_{\in S}\in S$

לכן $r=0$ כי אחרת נקבל סותר את העובדה ש- d_0 הוא המינימום הקטן ביותר ב- S.

קיבלנו:

$$0=m-d_0\cdot q$$
$$m=d_0\cdot q$$
$$d_0\mid m$$

באופן דומה אפשר גם להראות כי $d_0\mid n$. כלומר יש לנו מספר $d_0\mid m$ וגם $d_0\mid n$

קיבלנו כי d_0 מחלק משותף של m ו- n.

לכן $d\geq d_0\geq d$

$d_0\mid d$ ושניהם חיוביים.

ומכאן $d=d_0$, שזה מוכיח את הטענה.

הגדרה: שני מספרים טבעיים m,n נקראים זרים, אם $\gcd(m,n)=1$.

למשל: $24,35$ - זרים כי $\gcd(24,35)=1$

מהטענה הקודמת נובע שאם m,n זרים אז קיימים $\alpha,\beta\in\mathbb{Z}$ כך ש- $\alpha m+\beta n=1$

גם להיפך נכון, אם עבור $m,n\in\mathbb{N}$ מסוימים קיימים $\alpha,\beta\in\mathbb{Z}$ כך ש- $\alpha m+\beta n=1$ אז m,n זרים.

ואכן, אם נניח כי קיים $1<d=\gcd(m,n)$ נקבל כי d הזה מחלק גם את $\alpha m+\beta n$ לכל $\alpha,\beta\in\mathbb{Z}$.

אבל קיבלנו כי $d\mid 1$ (וזו סתירה כי לקחנו מספר שגדול מ- 1 וקיבלנו שהוא מחלק את 1)

לסיכום $m,n\in\mathbb{N}$ אמ"מ קיימים $\alpha,\beta\in\mathbb{Z}$ כך ש- $\alpha m+\beta n=1$.

אלגוריתם אוקלידס למציאת $\gcd(m,n)$

נתבונן בתהליך הבא:

$$m=n\cdot q_0+r_1 \qquad 0\leq r_1<n$$
$$n=r_1\cdot q_1+r_2 \qquad 0\leq r_2<r_1$$
$$r_1=r_2\cdot q_2+r_3 \qquad 0\leq r_3<r_2$$
$$\vdots$$
$$r_{k-3}=r_{k-2}q_{k-2}+r_{k-1}$$
$$r_{k-2}=r_{k-1}q_{k-1}+r_k \qquad 0\leq r_k<r_{k-1}$$
$$r_{k-1}=r_k\cdot q_k$$

m/r_1

$23=1\cdot 20+3$

הסדרה של השאריות: $r_1>r_2>r_3>\dots$ היא סדרה של מספרים לא שליליים שיורדת ממש. אז בשלב מסוים נקבל 0.

טענה: $\gcd(m,n)=r_k$

הוכחה:

$r_k \mid r_{k-1} \Rightarrow r_k \mid r_{k-2} \Rightarrow r_k \mid r_{k-3} \Rightarrow \dots \Rightarrow r_k \mid n \Rightarrow r_k \mid m$.

מכאן r_k מחלק משותף של m ו- n ולכן $r_k \le \overbrace{\gcd(m,n)}^{d}$

מצד שני $d \mid r_1 \Rightarrow d \mid r_2 \Rightarrow \dots \Rightarrow d \mid r_k$, כלומר $d \le r_k$.

מצד אחד $r_k \le d$ ומצד שני $d \le r_k$ ולכן $d = r_k$.

דוגמה: נמצא את $\gcd(\overset{m}{315},\overset{n}{616})$ ע"י שימוש באלגוריתם אוקלידס:

$$
\begin{array}{r|l}
 & 1 \\ \hline
615 & 315 \\
-315 & \\ \hline
301 & \\
\end{array}
\qquad q_0 = 1,\ r_1 = 301
$$

$$
\begin{array}{r|l}
 & 1 \\ \hline
315 & 301 \\
-301 & \\ \hline
14 & \\
\end{array}
\qquad q_1 = 1,\ r_2 = 14
$$

$$
\begin{array}{r|l}
 & 21 \\ \hline
301 & 14 \\
-280 & \\ \hline
21 & \\
-14 & \\ \hline
7 & \\
\end{array}
\qquad q_2 = 21,\ r_3 = 7
$$

$$
\begin{array}{r|l}
 & 2 \\ \hline
14 & 7 \\
-14 & \\ \hline
0 & \\
\end{array}
$$

השארית האחרונה שונה מ- 0

$\gcd(315,616) = 7$

התהליך:

$$616 = 315 \cdot 1 + 301$$
$$315 = 301 \cdot 1 + 14$$
$$301 = 14 \cdot 21 + 7$$
$$14 = 7 \cdot 2$$

שאלה: מהם α, β כך ש- $\alpha \cdot 616 + \beta \cdot 315 = 7$?

הגדרה: יהי $n > 1$ מספר טבעי. אומרים כי שני מספרים $a,b \in \mathbb{Z}$ שווים מודולו n אם $n \mid (a-b)$.

סימון: $a \equiv b \pmod n$

למשל: $8 \pmod 5 = 3$, $4 \equiv 11 \pmod 7$, $12 \pmod 7 = 5$.

תכונות בסיסיות:

① $a \equiv b \pmod n \iff b \equiv (a \bmod n)$

② $\begin{cases} a_1 \equiv b_1 \pmod n \\ a_2 \equiv b_2 \pmod n \end{cases} \Rightarrow a_1 \pm a_2 = (b_1 \pm b_2) \pmod n$

③ $\begin{cases} a_1 \equiv b_1 \pmod n \\ a_2 \equiv b_2 \pmod n \end{cases} \Rightarrow a_1 a_2 = (b_1 b_2) \pmod n$

הגדרה: יהי $n>1$ מספר טבעי ויהי $a\in\mathbb{Z}$.

אומרים כי a הפיך מודולו n אם קיים $b\in\mathbb{Z}$ כך ש- $a\cdot b\equiv 1 \pmod n$.

b נקרא הופכי של a מודולו n. מסמנים $b=a^{-1} \pmod n$.

דוגמה: 5 הפיך מודולו 12 כי $5\cdot 5=1 \pmod{12}$ וההופכי של 5 זה 5 עצמו (5 הופכי לעצמו מודולו 12).

7 הפיך מודולו 12 כי $7\cdot 7=1 \pmod{12}$ וההופכי של 7 זה 7 עצמו.

8 לא הפיך מודולו 12, כי אם $8\cdot b=1 \pmod{12}$ אז:

$$8b-1=12k \quad , k\in\mathbb{Z}$$

$$\underbrace{8b-12k}_{\text{מתחלק ב-4}} = \underbrace{1}_{\text{לא מתחלק ב-4}}$$

אז לא קיים b כזה ולכן 8 לא הפיך מודולו 12.

יהי n מספר טבעי. נסמן ב- $\varphi(n)$ את מספר ההפיכים מודולו n בקטע בין 0 ל- $n-1$.

למשל: $\varphi(4)=2$

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\varphi(6)=2$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

טענה: יהי n מספר טבעי ויהי $a\in\mathbb{Z}$

a הפיך מודולו n, אמ"מ $\gcd(a,n)=1$.

הוכחה: $\gcd(a,n)=1$ אמ"מ קיימים $\alpha,\beta\in\mathbb{Z}$ כך ש: $\alpha a+\beta n=1$ וזה קורה אמ"מ $\alpha a-1=\beta n$ וזה קורה כאשר $\alpha a-1$ מתחלק ב- n וזה אמ"מ $\alpha a=1 \pmod n$ וזה אמ"מ a הפיך מודולו n.

כלומר: $\gcd(a,n)=1 \iff$ קיימים $\alpha,\beta\in\mathbb{Z}$ כך ש: $\alpha a+\beta n=1 \iff \alpha a-1=\beta n \iff \alpha a-1$ מתחלק ב- $n \iff \alpha a=1 \pmod n$

דוגמה: נחשב את $\varphi(24)$: $24=2^3\cdot 3$

המספרים הטבעיים בין 0 ל- 23 הזרים ל- 24 הם: $1,5,7,11,13,17,19,23$ כלומר $\varphi(24)=8$

נשים לב כי לכל מספר ראשוני p מתקיים: $\varphi(p)=p-1$.