

תורת המספרים - תרגיל 1

1. נסמן:

$$d_1 = \gcd(a, l), \quad d_2 = \gcd(l, a), \quad d_3 = \gcd(|a|, |l|), \quad d_4 = \gcd(a, l + na)$$

$d_2 a, \quad d_2 l \Rightarrow d_1 d_2$
$d_3 a , \quad d_3 l \xRightarrow{\frac{ x }{y} = \pm \frac{x}{y}} d_3 a, \quad d_3 l \Rightarrow d_2 d_3$
$d_4 a, \quad d_4 l + na \xRightarrow{\text{divides a linear combination}} d_4 a, \quad d_4 1 \cdot (l + na) - n(a) = l$ $\xRightarrow{\frac{ x }{y} = \pm \frac{x}{y}} d_4 a , \quad d_4 l \Rightarrow d_3 d_4$
$d_1 a, \quad d_1 l \xRightarrow{\text{divides a linear combination}} d_1 a, \quad d_1 1 \cdot l + n \cdot a = l + na \Rightarrow d_4 d_1$

וקיבלנו בסה"כ ש $d_1|d_2|d_3|d_4|d_1$, ולכן $d_1 = d_2 = d_3 = d_4$

2. יהי

$$a = \prod_{i=0}^n p_i^{a_i}, \quad l = \prod_{i=0}^m p_i^{l_i}, \quad d = \gcd(a, l) = \prod_{i=0}^k P_i^{d_i}, \quad s = \min\{n, m\}$$

הפירוק של d, a, l לגורמים ראשוניים.

אזי, מהיות d מחלק משותף, $d_i \leq l_i, a_i$ לכל $0 \leq i \leq s$.

מהיות d מקסימלי, $d_i = \min\{l_i, a_i\}$ לכל $0 \leq i \leq s$.

לכל $i > s$, מתקיים $d_i = 0$, $l_i = 0 \vee a_i = 0$ (מהיות d מחלק משותף), $d_i = 0$ ולכן

$$d = \gcd(a, l) = \prod_{i=0}^{\min\{m, n\}} P_i^{\min\{l_i, a_i\}}$$

3. מסתיים אחרי זמן סופי - נשים לב שלכל n מתקיים $a_n, l_n \in \mathbb{N}_0$. ההוכחה באינדוקציה. (עבור הבסיס $n = 0$ נשתמש בנתון. נניח והטענה נכונה עבור n . a_{n+1}, l_{n+1} עפ"י הגדרתם הם מספרים טבעיים.)

לכל n נסמן $S_n = a_n + l_n$. נקבל שלכל $n > 1$ מתקיים:

$$S_n = a_n + l_n = l_{n-1} + r_{n-1} < a_{n-1} + l_{n-1} = S_{n-1}$$

ולכן $S_0 > S_1 > S_2 > \dots$ אך לכל n מתקיים $S_n \geq 0$ ולכן האלגוריתם לא ירוץ יותר מ S_0 איטרציות.

נכונות - נוכיח ש $(a, l) = (a_n, l_n)$ באינדוקציה על n

בסיס: $n = 0$. טריוואלי משאלה 1. $(a, l) = (|a|, |l|)$.

הנחה: הטענה נכונה עבור n .

$$(a_{n+1}, l_{n+1}) = (l_n, r_n) = (l_n, a_n + q_n l_n) \xRightarrow{\text{שאלה 1}} (l_n, a_n) \xRightarrow{\text{הנחת האינדוקציה}} (a, l) \text{ צעד } (a, l)$$

4.

$$(455, 1235) = (1235, 455) = (2 \cdot 455 + 325, 455) = (455, 325) = (1 \cdot 325 + 130, 325) \\ = (325, 130) = (2 \cdot 130 + 65, 130) = (130, 65) \xRightarrow{\text{65|130}} 65$$

5. נניח בשלילה שקיים איבר בסדרה, a , ומספר שלם t כך ש $a = t^2$. ולכן בפרט $a \equiv t^2 \pmod{4}$

אבל

$$0^2 \equiv 0 \pmod{4}, \quad 1^2 \equiv 1 \pmod{4}, \quad 2^2 \equiv 0 \pmod{4}, \quad 3^2 \equiv 1 \pmod{4}$$

ולכן

$$t^2 \equiv 0, 1 \pmod{4}$$

אך

$$a = 1 \dots 11 \equiv_{4|100} 11 \equiv 3 \not\equiv 0, 1 \equiv t^2 \pmod{4}$$

סתירה! מסקנה -אף איבר בסדרה אינו ריבוע של מספר שלם.

6. נניח בשלילה ש $p \neq 3$. אזי $p \not\equiv 3 \pmod{3}$ (כי p ראשוני). ולכן $p \equiv 1, 2 \pmod{3}$

$$\begin{cases} p \equiv 1 \pmod{3} \\ p \equiv 2 \pmod{3} \end{cases} \Rightarrow \begin{cases} p^2 + 2 \equiv 1^2 + 2 \equiv 3 \equiv 0 \pmod{3} \\ p^2 + 2 \equiv 2^2 + 2 \equiv 6 \equiv 0 \pmod{3} \end{cases}$$

$$\Rightarrow 3 | p^2 + 2 \quad \Rightarrow \quad p^2 + 2 = 3 \Rightarrow p = 1$$

because p^2+1 is prime

וקיבלנו סתירה! מסקנה $p = 3$.

7. הטענה נכונה לכל מספר טבעי. יהי n מספר טבעי גדול מ-1 כלשהו.

[עבור $(0,0) = 0$ נקבל $(0,0) = 0$ כדרוש]

נסמן $d = (a, l)$. אזי בפרט $d | a, l$ ולכן $n^d - 1 | n^a - 1, n^l - 1$

$$n^a - 1 = n^{kd} - 1 = (n^d)^k - 1 \equiv 1^k - 1 = 1 - 1 = 0 \pmod{n^d - 1}$$

[כ"ל לגבי $n^l - 1$]

$$n^{(a,l)} - 1 = (n^d - 1) | (n^a - 1, n^l - 1)$$

בכיוון השני -

אם $a = l$ נקבל ש $(n^a - 1, n^l - 1) = n^a - 1$

אם הם שונים, נניח $a > l$ נקבל ש

$$(n^a - 1, n^l - 1) \equiv_{\text{משאלה 1}} (n^a - 1 - (n^l - 1), n^l - 1) = (n^a - n^l, n^l - 1)$$

$$= (n^l(n^{a-l} - 1), n^l - 1)$$

אבל $\gcd(n^l - 1, n^l) = 1$ [כי הם מספרים עוקבים] ולכן

$$(n^a - 1, n^l - 1) = (n^l(n^{a-l} - 1), n^l - 1) = (n^{a-l} - 1, n^l - 1)$$

כמו כן $a > l$ ולכן גם $a - l \in \mathbb{N}$.

קעת נסמן $a_1 = a, l_1 = l$ ולכל m טבעי,

$$(n^{a_m} - 1, n^{l_m} - 1) = n^{a_m} - 1$$

אחרת נסמן $a_{m+1} = |a_m - a_l| > 0, l_{m+1} = \min\{a_m, a_l\}$ ונקבל (מהכתוב במסגרת) ש $(n^{a_m} - 1, n^{l_m} - 1) = (n^{a_{m+1}} - 1, n^{l_{m+1}} - 1)$

נשים לב שלכל m מתקיים $a_m, l_m \in \mathbb{N}$. ההוכחה באינדוקציה. (עבור הבסיס $m = 1$ נשתמש בנתון. נניח והטענה נכונה עבור m . עפ"י הגדרתם הם מספרים טבעיים.)

אם נסמן $S_m = a_m + l_m$, קל לראות ש $S_1 > S_2 > S_3 > \dots$, (כי לכל m טבעי מתקיים $[S_{m+1} = a_{m+1} + l_{m+1} = |a_m - a_l| + \min\{a_m, a_l\} = \max\{a_m, a_l\} < a_m + a_l = S_m$)

אך לכל $m > 0$ $S_m > 0$ [כי הוא סכום של שני מספרים טבעיים] ולכן קיים m' טבעי כך ש $a_{m'} = l_{m'}$ והאלגוריתם ייפסק.

[כי כל פעם S_m קטן ב 1 לפחות ולכן האלגוריתם לא יכיל יותר מ S_1 איטרציות.]

ולכן $(n^a - 1, n^l - 1) = n^{a_{m'}} - 1$ נסמן

$a_{m'} = x$ ובפרט $(n^a - 1), (n^l - 1) | (n^x - 1)$.

טענה: $x | a, l$. עפ"י משפט החלוקה קיימים $q, r \in \mathbb{Z}$ כך ש $a = qx + r, \quad 0 \leq r < x$

ולכן

$$n^a = n^{qx+r} = (n^x)^q \cdot n^r$$

ולכן

$$1 \equiv n^a = (n^x)^q \cdot n^r \equiv 1^q \cdot n^r = n^r \pmod{(n^x - 1)}$$

ולכן $n^x - 1 | n^r - 1$ אבל ממשפט החלוקה $r < x$ ולכן $n^x - 1 > n^r - 1$ ולכן בהכרח

$n^r - 1 = 0$ ולכן $n^r = 1$ ולכן $r = 0$ (כי $n > 1$) וקיבלנו ש $x | a$.

בצורה דומה נקבל ש $x | l$ ולכן $x | (a, l)$ ולכן $(n^a - 1, n^l - 1) = (n^x - 1) | (n^{(a,l)} - 1)$ מ.ש.ל.

8. לכל n טבעי נסמן ב l_n את מספר הספרות ב a_n . ולכן $l_1 = l_2 = 1, l_3 = 2, l_4 = 3$ ובמקרה הכללי $l_{n+2} = l_{n+1} + l_n$ [מבניית הסדרה]

טענה 1: לא קיימים בסדרה 2 איברים a_n, a_{n+1} כך ש l_n, l_{n+1} שניהם זוגיים. הוכחה: אם קיימים כאלו, נבחר את n המינימלי עבורו זה מתקיים. ($n > 1$). נשים לב ש $l_{n-1} = l_{n+1} - l_n$ ולכן גם l_{n-1} זוגי ו $n - 1$ גם מקיים את הטענה. סתירה למינימליות של n !

טענה 2: $2 | l_n \Leftrightarrow 3 | n$

הוכחה: באינדוקציה.

בסיס: $n = 1, 2$. $3 \nmid n$ וגם $2 \nmid l_1 = l_2 = 1$

הנחה: הטענה נכונה עבור $1, 2, \dots, n - 1$.

צעד: $l_n = l_{n-1} + l_{n-2}$. היות ו $n - 2, n - 1, n$ הינם מספרים עוקבים בדיוק אחד מהם מתחלק ב 3. ולכן

$$3 | n \Leftrightarrow 3 \nmid (n - 1), (n - 2) \Leftrightarrow 2 \nmid l_{n-1}, l_{n-2} \Leftrightarrow 2 | l_n$$

מההנחה

מטענה 1

והטענה הוכחה באינדוקציה.

מבניית הסדרה

$$a_{n+2} = a_n + 10^{l_n} \cdot a_{n+1} \equiv a_n + (-1)^{l_n} \cdot a_{n+1} \pmod{11}$$

ולכן (מטענה 2)

$$a_{n+2} \equiv \begin{cases} a_n + a_{n+1} & n \equiv 0 \pmod{3} \\ a_n - a_{n+1} & n \not\equiv 0 \pmod{3} \end{cases}$$

ולכן

$$a_3 \equiv a_1 - a_2 = 0 - 1 = -1 \pmod{11}, \quad a_4 \equiv a_2 - a_3 \equiv 1 + 1 = 2 \pmod{11}$$

$$a_5 \equiv a_3 + a_4 \equiv -1 + 2 = 1 \pmod{11}, \quad a_6 \equiv a_4 - a_5 \equiv 2 - 1 = 1 \pmod{11}$$

ובסה"כ $a_1 \equiv 0 \pmod{11}$, $a_2, a_3, a_4, a_5, a_6 \not\equiv 0 \pmod{11}$. נבדוק למה a_{n+6} שקול

אפשרות א: $n \equiv 0 \pmod{3}$

$$a_{n+6} \equiv a_{n+4} - a_{n+5} \equiv a_{n+4} - (a_{n+4} + a_{n+3}) \equiv -a_{n+3} \pmod{11}$$

ולכן גם $a_{n+3} \equiv -a_n \pmod{11}$ ובסה"כ $a_{n+6} \equiv a_n \pmod{11}$

אפשרות ב: $n \equiv 1 \pmod{3}$

$$a_{n+6} \equiv a_{n+4} - a_{n+5} \equiv a_{n+4} - (a_{n+3} - a_{n+4}) \equiv 2a_{n+4} - a_{n+3} \equiv$$

$$2(a_{n+2} + a_{n+3}) - a_{n+3} = 2a_{n+2} + a_{n+3} \equiv 2a_{n+2} + (a_{n+1} - a_{n+2}) = a_{n+1} + a_{n+2} \equiv$$

$$a_{n+1} + (a_n - a_{n+1}) = a_n \pmod{11}$$

ובסה"כ $a_{n+6} \equiv a_n \pmod{11}$

אפשרות ג: $n \equiv 2 \pmod{3}$

$$a_{n+6} \equiv a_{n+4} + a_{n+5} \equiv a_{n+4} + (a_{n+3} - a_{n+4}) \equiv a_{n+3}$$

ולכן גם $a_{n+3} \equiv a_n \pmod{11}$ ובסה"כ $a_{n+6} \equiv a_n \pmod{11}$

וקיבלנו שלכל n טבעי מתקיים $a_{n+6} \equiv a_n \pmod{11}$.

כעת נעבור להוכחת הטענה $n \equiv 1 \pmod{6} \Leftrightarrow a_n \equiv 0 \pmod{11}$. נוכיחה באינדוקציה על n .

בסיס: $n = 1, 2, 3, 4, 5, 6$ הראינו שהטענה מתקיימת.

הנחה: הטענה נכונה עבור $n - 1, 1, 2, 3, 4, 5, 6, \dots$

צעד:

$$a_n \equiv 0 \pmod{11} \Leftrightarrow_{a_n \equiv a_{n-6}} a_{n-6} \equiv 0 \pmod{11} \Leftrightarrow_{\text{מההנחה}} n - 6 \equiv 1 \pmod{6} \Leftrightarrow$$

$$n \equiv 1 \pmod{6}$$

מ.ש.ל

9. $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right)$ אבל $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$ נחשב כעת את $\left(\frac{3}{p}\right)$ עפ"י הלמה של גאוס
 כאשר n הינו מספר האיברים בקבוצה $\left(\frac{3}{p}\right) = (-1)^n$

$$\left\{3, 6, 9, \dots, 3 \left(\frac{1}{2}(p-1)\right)\right\}$$

אשר חלוקתם ב p משאירה שארית הגדולה מ $\frac{p}{2}$. אלו בדיוק האיברים $3t$ המקיימים

$$\frac{p}{2} < 3t < p \Leftrightarrow \frac{p}{6} < t < \frac{p}{3} \Leftrightarrow \left\lfloor \frac{p}{6} \right\rfloor + 1 \leq t \leq \left\lfloor \frac{p}{3} \right\rfloor$$

$$[3t \leq \frac{3}{2}(p-1) < \frac{3}{2}p \text{ אלו היחידים היות }]$$

$$\text{ולכן } n = \left\lfloor \frac{p}{3} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor \text{ ולכן}$$

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{1}{2}(p-1) + \left\lfloor \frac{p}{3} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor}$$

$$= \begin{cases} p = 6k + 1 \Rightarrow (-1)^{\frac{1}{2}(6k+1-1) + \left\lfloor \frac{6k+1}{3} \right\rfloor - \left\lfloor \frac{6k+1}{6} \right\rfloor} = (-1)^{3k+2k-k} = (-1)^{4k} = 1 \\ p = 6k + 5 \Rightarrow (-1)^{\frac{1}{2}(6k+5-1) + \left\lfloor \frac{6k+5}{3} \right\rfloor - \left\lfloor \frac{6k+5}{6} \right\rfloor} = (-1)^{3k+2+2k+1-k} = (-1)^{4k+3} = -1 \end{cases}$$

ובסה"כ קיבלנו

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{6} \\ -1 & p \equiv 5 \pmod{6} \end{cases}$$

[נשים לב שהיות ו p ראשוני, אלו האפשרויות היחידות שלו, אחרת הוא יתחלק ב 2 או ב 3.]

10. עפ"י הלמה של גאוס $\left(\frac{5}{p}\right) = (-1)^n$ כאשר n הינו מספר האיברים בקבוצה

$$\left\{5, 10, 15, \dots, 5 \left(\frac{1}{2}(p-1)\right)\right\}$$

אשר חלוקתם ב p משאירה שארית הגדולה מ $\frac{p}{2}$. אלו בדיוק האיברים $5k$ המקיימים

$$\frac{p}{2} < 5t < p \Leftrightarrow \frac{p}{10} < ts < \frac{p}{5} \Leftrightarrow \left\lfloor \frac{p}{10} \right\rfloor + 1 \leq t \leq \left\lfloor \frac{p}{5} \right\rfloor$$

או

$$p + \frac{p}{2} < 5t < p + p \Leftrightarrow \frac{3p}{10} < t < \frac{2p}{5} \Leftrightarrow \left\lfloor \frac{3p}{10} \right\rfloor + 1 \leq t \leq \left\lfloor \frac{2p}{5} \right\rfloor$$

$$[5t \leq \frac{5}{2}(p-1) < \frac{5}{2}p \text{ אלו היחידים היות }]$$

$$\text{ולכן } n = \left\lfloor \frac{p}{5} \right\rfloor - \left\lfloor \frac{p}{10} \right\rfloor + \left\lfloor \frac{2p}{5} \right\rfloor - \left\lfloor \frac{3p}{10} \right\rfloor \text{ ולכן}$$

$$\left(\frac{5}{p}\right) = (-1)^{\left\lfloor \frac{p}{5} \right\rfloor - \left\lfloor \frac{p}{10} \right\rfloor + \left\lfloor \frac{2p}{5} \right\rfloor - \left\lfloor \frac{3p}{10} \right\rfloor}$$

$$= \begin{cases} p = 10k + 1 \Rightarrow (-1)^{\left\lfloor \frac{10k+1}{5} \right\rfloor - \left\lfloor \frac{10k+1}{10} \right\rfloor + \left\lfloor \frac{2(10k+1)}{5} \right\rfloor - \left\lfloor \frac{3(10k+1)}{10} \right\rfloor} = (-1)^{2k-k+4k-3k} = (-1)^{2k} = 1 \\ p = 10k + 3 \Rightarrow (-1)^{\left\lfloor \frac{10k+3}{5} \right\rfloor - \left\lfloor \frac{10k+3}{10} \right\rfloor + \left\lfloor \frac{2(10k+3)}{5} \right\rfloor - \left\lfloor \frac{3(10k+3)}{10} \right\rfloor} = (-1)^{2k-k+4k+1-3k} = (-1)^{2k+1} = -1 \\ p = 10k + 7 \Rightarrow (-1)^{\left\lfloor \frac{10k+7}{5} \right\rfloor - \left\lfloor \frac{10k+7}{10} \right\rfloor + \left\lfloor \frac{2(10k+7)}{5} \right\rfloor - \left\lfloor \frac{3(10k+7)}{10} \right\rfloor} = (-1)^{2k+1-k+4k+2-3k-2} = (-1)^{2k+1} = -1 \\ p = 10k + 9 \Rightarrow (-1)^{\left\lfloor \frac{10k+9}{5} \right\rfloor - \left\lfloor \frac{10k+9}{10} \right\rfloor + \left\lfloor \frac{2(10k+9)}{5} \right\rfloor - \left\lfloor \frac{3(10k+9)}{10} \right\rfloor} = (-1)^{2k+1-k+4k+3-3k-2} = (-1)^{2k+2} = 1 \end{cases}$$

ובסה"כ קיבלנו

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{10} \\ -1 & p \equiv \pm 3 \pmod{10} \end{cases}$$

[נשים לב שהיות ו p ראשוני, אלו האפשרויות היחידות שלו, אחרת הוא יתחלק ב 2 או ב 5.]