אלגברה ב' - פתרון גליון 1

♠ [H] תרגיל 1.3.10: בשלילה, נניח שקיים $n \geq m_0, n \in \mathbb{N}$ כך שהטענה $P(n)$ איננה מתקיימת. אזי הקבוצה $A = \{m \in \mathbb{N} \,|\, m \geq m_0 \quad and \quad \neg P(m)\}$ - קבוצת כל הטבעיים $m \geq m_0$ שאינם מקיימים את הטענה P - איננה ריקה.
יהא n_0 איבר מינימלי בקבוצה A, ואז בוודאי:
$n_0 > m_0 \Rightarrow n_0 - 1 \geq m_0 \quad and \quad n_0 - 1 \notin A \Rightarrow P(n_0 - 1),$
ולפי הנחת האינדוקציה (הנחה 2 בנתון), נקבל כי הטענה $P(n_0)$ נכונה, בסתירה להיות $n_0 \in A$.
הוכחת סעיף ב' דומה, ואתם מתבקשים לשחזר אותה מן ההוכחה של סעיף א'. ■

♠ [H] תרגיל 1.3.11: על-מנת להראות שפעולות החיבור והכפל ב-J_n מוגדרות היטב, נוכיח כי:
$[a] = [b],\, [c] = [d] \Rightarrow [a + c] = [b + d], [ac] = [bd].$
דהיינו, אם $a - b \in n\mathbb{Z}$ וגם $c - d \in n\mathbb{Z}$, אזי עלינו להראות כי $(a + c) - (b + d), ac - bd \in n\mathbb{Z}$.
נזכירכם כי $n\mathbb{Z}$ מהווה סימון לקבוצת כל הכפולות השלמות של n.
לפי ההנחה, קיימים שלמים x, y כך ש-$a - b = xn,\, c - d = yn$, ואז:
$(a + c) - (b + d) = (a - b) + (c - d) = xn + yn = (x + y)n \Rightarrow [a + c] = [b + d];$
$ac - bd = ac - cb + cb - bd = c(a - b) + b(c - d) = cxn + byn = (cx + by)n \Rightarrow [ac] = [bd],$
כנדרש. ■

♠ [H] תרגיל 1.3.12: מרגע שהוכחנו כי הפעולות ב-J_n מוגדרות היטב, נוכל לרשום -

(1) $[i] + [j] = [i + j] = [j + i] = [j] + [i];$
(2) $[i][j] = [ij] = [ji] = [j][i];$
(3) $([i] + [j]) + [k] = [i + j] + [k] = [(i + j) + k] = [i + (j + k)] = [i] + [j + k] = [i] + ([j] + [k]);$
(4) $([i][j])[k] = [ij][k] = [(ij)k] = [i(jk)] = [i][jk] = [i]([j][k]);$
(5) $[i]([j] + [k]) = [i][j + k] = [i(j + k)] = [ij + ik] = [ij] + [ik] = [i][j] + [i][k];$
(6) $[0] + [i] = [0 + i] = [i];$
(7) $[1][i] = [1 \cdot i] = [i].$

♠ [H] תרגיל 1.3.14: בלי הגבלת הכלליות, a הוא שלם חיובי: ברור שהטענה נכונה עבור $a = 0$, ואם a שלילי, נבחין בין שני מקרים:

- p איזוגי: במקרה זה $a^p = -(-a)^p \equiv -(-a) \bmod p = a \bmod p$;
- $p = 2$: כאן $a \equiv (-a) \bmod p$ לכל a שלם, ואין הבחנה בין ערכים שליליים לערכים חיוביים.

ובכן, נותר להוכיח את הטענה עבור $a \in \mathbb{N}$, וברור שהיא נכונה בהצבת $a = 1$.
נראה כעת כי אם $a^p \equiv a \bmod p$, אזי גם $(a + 1)^p \equiv (a + 1) \bmod p$. נחשב:

$$(a + 1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = a^p + 1 + \sum_{k=1}^{p-1} \underbrace{\frac{p!}{k! \cdot (p - k)!}}_{\text{תמיד שלם!}} \cdot a^k$$

אם נראה כי כל המחוברים בתוך הסכום האחרון מתחלקים בראשוני p, נוכיח בכך את שלב המעבר האינדוקטיבי:
p הוא מספר ראשוני, ולכן הוא זר לכל מספר טבעי הקטן ממנו - בפרט p זר לכל מכפלה של טבעיים הקטנים ממנו. מכאן נובע, שעבור $0 < k < p$ מתקיים:

$$\underbrace{(k!(p-k)!)\,\big|p!\,,\ p\big|p!}_{\text{מחלקים זרים של p!}} \Rightarrow (p\cdot k!(p-k)!)\,\big|p! \Rightarrow p\left|\frac{p!}{k!\cdot(p-k)!}\right..$$

נסכם: הוכחנו כי $(a+1)^p \equiv a^p+1\, mod\, p$. נפעיל את הנחת האינדוקציה על-מנת לקבל
$a^p+1 \equiv a+1\, mod\, p,$

ובכך סיימנו את ההוכחה. ■