Αριστοτελειο Πανεπιστημιο Θεσσαλονικης
Τμημα Μαθηματικων

Εισαγωγή στην Άλγεβρα
Τελική Εξέταση Σεπτεμβρίου 2016
Λύσεις

Ομάδα Θεμάτων Α

1. Να χρησιμοποιήσετε Μαθηματική Επαγωγή, για να αποδείξετε ότι

$$\sum_{i=1}^{n}(i+1)(i+2) = \frac{(n+1)(n+2)(n+3)}{3} - 2.$$

Απάντηση Στην απάντηση πρέπει να υπάρχουν ξεκάθαρα τα τρια στάδια της μεθόδου.

Βασικό Βήμα. Ελέγχουμε αν η πρόταση είναι αληθής για $n = 1$. Το άθροισμα έχει έναν μόνο όρο, για $n = 1$. Έτσι $(1+1)(1+2) = 2 \cdot 3$ ενώ $(2 \cdot 3 \cdot 4)/3 - 2 = 8 - 2 = 6$, άρα η πρόταση ισχύει για $n = 1$.

Επαγωγική Υπόθεση για $n = k$. Υποθέτουμε ότι η πρόταση είναι αληθής για $n = k$ (όπου $k \geq 1$). Δηλαδή δεχόμαστε ότι

$$\sum_{i=1}^{k}(i+1)(i+2) = \frac{(k+1)(k+2)(k+3)}{3} - 2. \ (*)$$

Επαγωγικό Βήμα (Απόδειξη για $n = k+1$). Πρέπει να αποδείξουμε ότι

$$\sum_{i=1}^{k+1}(i+1)(i+2) = \frac{(k+2)(k+3)(k+4)}{3} - 2.$$

Προσοχή: ΔΕΝ ξεκινάμε από την ισότητα που θέλουμε να αποδείξουμε, γιατί αυτό πολλές φορές οδηγεί σε πρωθύστερα. Ξεκινάμε από το άθροισμα και εντοπίζουμε πως μπορούμε να χρησιμοποιήσουμε την υπόθεση της επαγωγής.

$$\sum_{i=1}^{k+1}(i+1)(i+2) = \sum_{i=1}^{k}(i+1)(i+2) + (k+2)(k+3).$$

Χρησιμοποιώντας την επαγωγική υπόθεση (βλ. (*)), συμπεραίνουμε ότι το αρχικό άθροισμα είναι ίσο με

$$\left(\frac{(k+1)(k+2)(k+3)}{3} - 2\right) + (k+2)(k+3).$$

Κάνοντας τις πράξεις και βγάζοντας κοινό παράγοντα το $(k+2)(k+3)$, συμπεραίνουμε ότι το αρχικό άθροισμα ισούται με

$$\left(\frac{(k+1)(k+2)(k+3)}{3} + (k+2)(k+3)\right) - 2 = \frac{(k+1)(k+2)(k+3) + 3(k+2)(k+3)}{3} - 2$$

$$= \frac{(k+2)(k+3)((k+1)+3)}{3} - 2 = \frac{(k+2)(k+3)(k+4)}{3} - 2$$

και το ζητούμενο αποδείχθηκε για $n = k+1$. Επομένως, σύμφωνα με την Μαθηματική Επαγωγή, η Πρόταση ισχύει για όλα τα $n \geq 1$.

Το αντίστοιχο θέμα της ομάδας **Β** ζητούσε την απόδειξη της ισότητας

$$\prod_{i=1}^{n}\left(1-\frac{1}{(i+1)^2}\right)=\frac{(n+2)}{2(n+1)}.$$

Επαγωγικό βήμα. Το γινόμενο έχει μόνο έναν όρο, για $n=1$ και $1-1/(1+1)^2=3/4$ ενώ $(1+2)/2(1+1)=3/4$, άρα η πρόταση ισχύει για $n=1$.

Επαγωγική Υπόθεση για $n=k$. Υποθέτουμε ότι για $n=k$ (όπου $k\geq 1$) η πρόταση είναι αληθής, δηλ. ισχύει ότι

$$\prod_{i=1}^{k}\left(1-\frac{1}{(i+1)^2}\right)=\frac{(k+2)}{2(k+1)}. \ (**)$$

Απόδειξη για $n=k+1$. Πρέπει να αποδείξουμε ότι

$$\prod_{i=1}^{k+1}\left(1-\frac{1}{(i+1)^2}\right)=\frac{(k+3)}{2(k+2)}.$$

Πράγματι:

$$\prod_{i=1}^{k+1}\left(1-\frac{1}{(i+1)^2}\right)=\prod_{i=1}^{k}\left(1-\frac{1}{(i+1)^2}\right)\left(1-\frac{1}{(k+2)^2}\right).$$

Χρησιμοποιώντας την επαγωγική υπόθεση (βλ. (**)), συμπεραίνουμε ότι το αρχικό γινόμενο είναι ίσο με

$$\frac{(k+2)}{2(k+1)}\left(\frac{(k+2)^2-1}{(k+2)^2}\right)=\frac{1}{2(k+1)}\,\frac{(k^2+4k+3)}{(k+2)}=$$
$$\frac{1}{2(k+1)}\,\frac{(k+1)(k+3)}{(k+2)}=\frac{(k+3)}{2(k+2)}.$$

Συνεπώς, η πρόταση είναι αληθής, για $n=k+1$. Σύμφωνα με την Μαθηματική Επαγωγή, η πρόταση ισχύει για όλα τα $n\geq 1$.

2. Έστω $\mathcal{R}$ η παρακάτω σχέση στο σύνολο $\mathbb{Z}\times\mathbb{Z}_{20}$:

$$(m,\bar{n})\mathcal{R}(a,\bar{b})\Leftrightarrow n\equiv b \text{ mod } 5.$$

Να αποδείξετε ότι η $\mathcal{R}$ είναι καλά ορισμένη.

Απάντηση Ο τρόπος που γράφουμε τα στοιχεία του $\mathbb{Z}\times\mathbb{Z}_{20}$ δεν είναι μοναδικός:

$$(m,\bar{n})=(m,\bar{n}') \text{ αν και μόνο αν } n\equiv n' \text{ mod } 20.$$

Θέλουμε, λοιπόν, να δείξουμε ότι η σχέση $\mathcal{R}$ είναι ανεξάρτητη της επιλογής του αντιπροσώπου. Πρώτα θα δείξουμε ότι αν $(m,\bar{n})=(m,\bar{n}')$ και $(m,\bar{n})\mathcal{R}(a,\bar{b})$, τότε $(m,\bar{n}')\mathcal{R}(a,\bar{b})$ (δηλ. $n'\equiv a$ mod 5). Πράγματι

$$n\equiv n' \text{ mod } 20\Rightarrow n=n'+20k \text{ και } n\equiv a \text{ mod } 5\Rightarrow n=a+5t.$$

Τότε, όμως,

$$n'=n-20k=(a+5t)-20k=a+5(t-4k)\Rightarrow n'\equiv a \text{ mod } 5\Rightarrow (m,\bar{n}')\mathcal{R}(a,\bar{b}).$$

Ομοίως, αν $(a,\bar{b})=(a,\bar{b}')$ και $(m,\bar{n})\mathcal{R}(a,\bar{b})$, προκύπτει ότι $(m,\bar{n})\mathcal{R}(a,\bar{b}')$, αφού

$$b=b'+20f, n=b+5g\Rightarrow n=b'+5(4f+g)\Rightarrow (m,\bar{n})\mathcal{R}(a,\bar{b}').$$

Άρα η $\mathcal{R}$ είναι ανεξάρτητη της επιλογής αντιπροσώπων και είναι καλά ορισμένη.

3. Έστω $\mathcal{R}$ η σχέση του προηγούμενου ερωτήματος. Να αποδείξετε ότι η $\mathcal{R}$ είναι σχέση ισοδυναμίας, να βρείτε πόσες κλάσεις ισοδυναμίας υπάρχουν και να γράψετε από δύο αντιπροσώπους για κάθε κλάση ισοδυναμίας.

Απάντηση

Αυτανακλασιστική Ιδιότητα: αφού $n \equiv n \bmod 5$, προκύπτει ότι $(m, \bar{n})\mathcal{R}(m, \bar{n})$.

Συμμετρική Ιδιότητα: Έστω ότι $(m, \bar{n})\mathcal{R}(a, \bar{b})$. Αφού $n \equiv b \bmod 5$ και άρα $b \equiv n \bmod 5$ προκύπτει ότι

Προσεταιριστική Ιδιότητα: Έστω ότι $(m, \bar{n})\mathcal{R}(a, \bar{b})$ και ότι $(a, \bar{b})\mathcal{R}(f, \bar{g})$. Τότε $n \equiv b \bmod 5$ και $b \equiv g \bmod 5$. Επομένως $n \equiv g \bmod 5$ και $(m, \bar{n})\mathcal{R}(f, \bar{g})$.

Αν $(m, \bar{n}) \in \mathbb{Z} \times \mathbb{Z}_{20}$, τότε η δεύτερη συντεταγμένη $\bar{n}$ ανήκει σε ένα από τα παρακάτω υποσύνολα του $\mathbb{Z}_{20}$:

$$A_1 = \{\overline{5n} : n \in \mathbb{Z}\} = \{\bar{0}, \bar{5}, \bar{10}, \bar{15}\},$$
$$A_2 = \{\overline{5n+1} : n \in \mathbb{Z}\} = \{\bar{1}, \bar{6}, \bar{11}, \bar{16}\},$$
$$A_3 = \{\overline{5n+2} : n \in \mathbb{Z}\} = \{\bar{2}, \bar{7}, \bar{12}, \bar{17}\}$$
$$A_4 = \{\overline{5n+3} : n \in \mathbb{Z}\} = \{\bar{3}, \bar{8}, \bar{13}, \bar{18}\},$$
$$A_5 = \{\overline{5n+4} : n \in \mathbb{Z}\} = \{\bar{4}, \bar{9}, \bar{14}, \bar{19}\}.$$

Οι κλάσεις ισοδυναμίας για τη σχέση $\mathcal{R}$ είναι οι:

$$[(0, \bar{0})] = [(1, \bar{5})] = \{(m, \overline{n}) : m \in \mathbb{Z}, \bar{n} \in A_1\}.$$
$$[(0, \bar{1})] = [(155, \bar{6})] = \{(m, \overline{n}) : m \in \mathbb{Z}, \bar{n} \in A_2\}.$$
$$[(0, \bar{2})] = [(-129, \bar{7})] = \{(m, \overline{n}) : m \in \mathbb{Z}, \bar{n} \in A_3\}.$$
$$[(0, \bar{3})] = [(1000, \bar{8})] = \{(m, \overline{n}) : m \in \mathbb{Z}, \bar{n} \in A_4\}.$$
$$[(0, \bar{4})] = [(0, \bar{9})] = \{(m, \overline{n}) : m \in \mathbb{Z}, \bar{n} \in A_5\}.$$

4. Να αποδείξετε ότι $\sqrt{18}$ είναι άρρητος.

Απάντηση Έστω ότι $\sqrt{18} = \dfrac{a}{b}$. Διαιρώντας τον αριθμητή a και παρανομαστή b του κλάσματος με τον μέγιστο κοινό διαιρέτη (a, b), μπορούμε να υποθέσουμε ότι $\sqrt{18} = \dfrac{m}{n}$, όπου $(m, n) = 1$. Έτσι $\sqrt{18}n = m$ και $18n^2 = m^2$. Όμως, $n \neq 1$ αφού $\sqrt{18} \notin \mathbb{Z}$. Άρα ο n έχει έναν πρώτο διαιρέτη p. Επομένως ο p διαιρεί τον m^2 και αφού ο pείναι πρώτος, συμπεραίνουμε ότι ο p διαιρεί τον m. Άρα $p|(m, n) = 1$ και αυτό μας οδηγεί σε άτοπο. Επομένως ο $\sqrt{18}$ είναι άρρητος.

Εναλλακτικά, παρατηρούμε ότι $18n^2 = 2 \cdot 9n^2$ είναι άρτιος ακέραιος, δηλ. ο m^2 είναι άρτιος και επομένως ο m είναι άρτιος, άρα $m = 2k$ και $2 \cdot 9n^2 = 4k^2$. Επομένως, $9n^2 = 2k^2$, δηλ. ο n^2 και κατά συνέπεια ο n είναι άρτιος, άρα $2|(m, n) = 1$ και αυτό μας οδηγεί σε άτοπο.

Προσοχή: ΔΕΝ καταλήγουμε σε άτοπο και η απόδειξη δεν είναι ολοκληρωμένη, αν προσπαθήσουμε να επιχειρηματολογήσουμε χρησιμοποιώντας ότι αφού $3|18n^2$, το 3 πρέπει να διαιρεί και το m^2 (δοκιμάστε το).

Προσοχή: ΔΕΝ είναι σωστό να γράψουμε $18|m^2 \Rightarrow 18|m$. Για παράδειγμα $18|6^2$, όμως το 18 δεν διαιρεί το 6.

5. Να αποδείξετε ότι $15(a, b) = (15a, 15b)$, για $a, b \in \mathbb{N}$.

Απάντηση Έστω $d = (a, b)$ και $D = (15a, 15b)$. Θα αποδείξουμε ότι $15d = D$. Πράγματι, αφού $d|a$ και $d|b$, συμπεραίνουμε ότι $15d|15a$ και $15d|15b$. Άρα $d|(15a, 15b)$. Αντίστροφα,

από το Θεώρημα του Bezout γνωρίζουμε ότι υπάρχουν $x, y \in \mathbb{Z}$ τέτοια ώστε $ax + by = d$. Επομένως $15ax + 15by = 15d$ και αφού $D|15a$, $D|15b$, συμπεραίνουμε ότι $D|15d$. Αφού, λοιπόν, $15d|D$ και $D|15d$, συμπεραίνουμε ότι $15d = D$.

6. Να αποδείξετε ότι υπάρχει μοναδικό $q \in \mathbb{N}$, τέτοιο ώστε $8^{100} = 11q + 1$. Στη συνέχεια να ελέγξετε αν υπάρχει $p \in \mathbb{N}$, τέτοιο ώστε $8^{100} = 11p + 7$.

   Απάντηση Σύμφωνα με το Μικρό Θεώρημα του Fermat, για $p = 11$ (και αφού $(8, 11) = 1$), $8^{10} \equiv 1 \bmod 11$. Επομένως $8^{100} = (8^{10})^{10} \equiv 1 \bmod 11$. Άρα υπάρχει $q \in \mathbb{Z}$, τέτοιο ώστε $8^{100} = 1+11q$. Αφού $8^{100}-1 > 11$, είναι φανερό ότι $q \in \mathbb{N}$. Επομένως υπάρχει $q \in \mathbb{N}$, τέτοιο ώστε $8^{100} = 11q+1$. Το 1 είναι λοιπόν το υπόλοιπο της διαίρεσης του 8^{100} με το 11. Από τη μοναδικότητα του πηλίκου και υπολοίπου (Θεώρημα Διαίρεσης), συμπεραίνουμε ότι το q είναι μοναδικό και ότι δεν υπάρχει $p \in \mathbb{N}$, τέτοιο ώστε $8^{100} = 11p + 7$.

7. Να βρείτε όλες τις λύσεις της γραμμικής ισοδυναμίας $5x \equiv 8 \mod 12$.

   Απάντηση Παρατηρούμε ότι x είναι λύση της γραμμικής ισοδυναμίας $5x \equiv 8 \mod 12$ αν και μόνο αν υπάρχει $k \in \mathbb{Z}$, τέτοιο ώστε $5x+12k = 8$. Όμως, $5 \cdot 4+12(-2) = 8$ και αν η δυάδα x, k ικανοποιεί την εξίσωση $5x + 12k = 8$, τότε το x ικανοποιεί την ισοδυναμία $x \equiv 4 \bmod 12$. Πράγματι

   $$5x + 12k = 8 = 5 \cdot 4 + 12(-2) \Rightarrow 5(x - 4) = 12(-2 - k) \Rightarrow 12|x - 4 \Rightarrow x \equiv 4 \bmod 12.$$

   Για την δεύτερη συνεπαγωγή παραπάνω, χρησιμοποιήσαμε το γεγονός ότι $(5, 12) = 1$. Αντίστροφα, αν $x = 4 + 12n$, για κάποιο $n \in \mathbb{N}$, τότε

   $$5x + 12(-2 - 5n) = 5(4 + 12n) + 12(-2 - 5n) = (5 \cdot 4 + 12(-2)) + 5 \cdot 12n - 12 \cdot 5n = 8.$$

   Άρα $x \equiv 4 \bmod 12$ δίνει όλες τις λύσεις της γραμμικής ισοδυναμίας $5x \equiv 8 \mod 12$.

   Σημείωση: στην προκειμένη περίπτωση, ήταν εύκολο να βρούμε μία συγκεκριμένη λύση της $5x + 12k = 8$. Γενικά, αν θέλουμε να βρούμε μία συγκεκριμένη λύση για την $ax + by = e$ (αν υπάρχει), πρώτα βρίσκουμε $x_1, x_2 \in \mathbb{Z}$ με την βοήθεια του Ευκλειδείου αλγορίκμου, τέτοια ώστε $(a, b) = ax_1 + bx_2$ και στη συνέχεια πολλαπλασιάζουμε τα x_1, x_2 με $e/(a, b)$:

   $$5 \cdot 5 + 12(-2) = 1 \Rightarrow 8 = 5 \cdot 40 + 12(-16).$$

   Εναλλακτικά, αφού $5 \cdot 5 \equiv 1 \mod 12$, συμπεραίνουμε ότι

   $$5x \equiv 8 \bmod 12 \Leftrightarrow 5 \cdot 5x \equiv 5 \cdot 8 \bmod 12 \Leftrightarrow x \equiv 40 \mod 12 \Leftrightarrow x \equiv 4 \bmod 12.$$

8. Να γράψετε τον φυσικό αριθμό 1 ως ακέραιο συνδυασμό των 55 και 116, χρησιμοποιώντας τον Ευκλείδειο Αλγόριθμο.

   Απάντηση $116 = 55 \cdot 2+6$, $55 = 6 \cdot 9+1$. Επομένως $1 = 55-6 \cdot 9 = 55-(116-55 \cdot 2)9 = 19 \cdot 55 - 116 \cdot 9$.

9. Να αποδείξετε ότι υπάρχουν άπειροι πρώτοι.

   Απάντηση Έστω ότι $\{p_1, p_2, \ldots, p_n\}$ είναι το σύνολο όλων των πρώτων. Τότε, αφού κάθε ακέραιος αναλύεται σε γινόμενο πρώτων (Θεμελιώδες Θεώρημα της Αριθμητικής), ο $m = p_1 \cdots p_n+1$ διαιρείται από τον p_i, για κάποιο $1 \leq i \leq n$. Άρα $p_i|m-p_1 \cdots p_n$ και άρα $p_i|m$. Καταλήξαμε σε άτοπο γιατί υποθέσαμε ότι το σύνολο των πρώτων είναι πεπερασμένο. Επομένως υπάρχουν άπειροι πρώτοι.

10. Να γράψετε τον αριθμό 123459 σε βάση 60.

    Απάντηση $123459 = 60 \cdot 2057 + 39$, $2057 = 60 \cdot 34 + 17$, $17 = 60 \cdot 0 + 17$, άρα $123459 = 60 \cdot (60 \cdot 34 + 17) + 39 = 60^2 \cdot 34 + 60 \cdot 17 + 39$ και $123459 = (34, 17, 39)_{60}$.