ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Ἐαρινὸ Ἑξάμηνο 2019

Καθηγητὴς Ν. Γ. Τζανάκης

Λύσεις ἀσκήσεων ἐπιλεγμένων ἀπὸ τὴν ἐξέταση τῆς Προόδου

Ἡ ἀρίθμησή τους δὲν συμπίπτει μὲ αὐτὴ τῶν θεμάτων τῆς ἐξέτασης

1. *Ἂν $(a, b) = 1$ καὶ $d|a + b$, ἀποδεῖξτε ὅτι $(a, d^2) = 1$.*

   Λύση. Ἔστω ὅτι $(a, d^2) > 1$. Τότε ὑπάρχει πρώτος p ποὺ διαιρεῖ τὸν a καὶ τὸν d^2. Ἐπειδὴ ὁ p εἶναι πρῶτος, ἡ σχέση $p \mid d^2$ συνεπάγεται ὅτι $p \mid d$. Ἀλλὰ $d \mid a + b$ ἄρα $p \mid a + b$. Ὅμως $p \mid a$, ἄρα $p \mid (a + b) - a$, δηλαδή, $p \mid b$. Ἔτσι ὁδηγηθήκαμε στὸ συμπέρασμα ὅτι $p \mid a$ καὶ $p \mid b$, ποὺ ἔρχεται σὲ ἀντίφαση μὲ τὴν ὑπόθεση $(a, b) = 1$.

2. *Ἂν $(a, b) = 1$ καὶ $d|a^2 + b$, ἀποδεῖξτε ὅτι $(b, d) = 1$.*

   Λύση. Ἔστω ὅτι $(b, d) > 1$. Τότε ὑπάρχει πρώτος p ποὺ διαιρεῖ τὸν b καὶ τὸν d. Ἀλλὰ $d \mid a^2 + b$ ἄρα $p \mid a^2 + b$. Ὅμως $p \mid b$, ἄρα $p \mid (a^2 + b) - b$, δηλαδή, $p \mid a^2$. Ἐπειδὴ ὁ p εἶναι πρῶτος, ἡ σχέση $p \mid a^2$ συνεπάγεται ὅτι $p \mid a$. Ἔτσι ὁδηγηθήκαμε στὸ συμπέρασμα ὅτι $p \mid a$ καὶ $p \mid b$, ποὺ ἔρχεται σὲ ἀντίφαση μὲ τὴν ὑπόθεση $(a, b) = 1$.

3. *Ἂν ὁ p εἶναι πρῶτος καὶ ὁ a εἶναι ὁποιοσδήποτε ἀκέραιος ἀποδεῖξτε ὅτι ὁ p διαιρεῖ τὸν $a^{k(p-1)+1} - a$ γιὰ κάθε $k \geq 0$. Βάσει αὐτοῦ ἀποδεῖξτε ὅτι ὁ $1365 = 3 \cdot 5 \cdot 7 \cdot 13$ διαιρεῖ τὸν ἀριθμὸ $a^{13} - a$, ὁποιοσδήποτε κι ἂν εἶναι ὁ ἀκέραιος a.*

   Λύση. Ὁ p εἶναι πρῶτος, ἄρα ἢ $p \mid a$ ἢ $(p, a) = 1$. Στὴν πρώτη περίπτωση, προφανῶς ὁ p διαιρεῖ τὸν $a^{k(p-1)+1} - a = a\,(a^{k(p-1)} - 1)$. Στὴ δεύτερη περίπτωση ἰσχύει τὸ θεώρημα τοῦ Fermat $a^{p-1} \equiv 1 \pmod p$ καὶ ὑψώνοντας στὴ δύναμη k ἔχομε $a^{k(p-1)} \equiv 1 \pmod p$, ἄρα ὁ p διαιρεῖ τὸν $a^{k(p-1)} - 1$ καί, συνεπῶς, διαιρεῖ καὶ τὸν $a\,(a^{k(p-1)} - 1) = a^{k(p-1)+1} - a$.
   Ἐφαρμογή. Τὸ 13 εἶναι τῆς μορφῆς $k(p - 1) + 1$ γιὰ $p \in \{3, 5, 7, 13\}$ διότι $13 = 6(3 - 1) + 1$, $13 = 3(5 - 1) + 1$, $13 = 2(7 - 1) + 1$, $13 = 1(13 - 1) + 1$. Ἄρα, βάσει αὐτοῦ ποὺ ἀποδείξαμε προηγουμένως, καθένας ἀπὸ τοὺς πρώτους 3,5,7,13 διαιρεῖ τὸν $a^{13} - a$ γιὰ κάθε ἀκέραιο a. Τότε ὅμως, ἀπὸ γνωστὴ ἰδιότητα, καὶ τὸ γινόμενο αὐτῶν τῶν πρώτων διαιρεῖ τὸν $a^{13} - a$.

4. *Ἂν ὁ p εἶναι πρῶτος καὶ ὁ n εἶναι ὁποιοσδήποτε ἀκέραιος ἀποδεῖξτε ὅτι ὁ p διαιρεῖ τὸν $n^{k(p-1)+1} - n$ γιὰ κάθε $k \geq 0$. Βάσει αὐτοῦ ἀποδεῖξτε ὅτι ὁ $14105 = 5 \cdot 7 \cdot 13 \cdot 31$ διαιρεῖ τὸν ἀριθμὸ $n^{61} - n$, ὁποιοσδήποτε κι ἂν εἶναι ὁ ἀκέραιος n.*

   Λύση. Ὁ πρῶτος ἰσχυρισμὸς εἶναι ἀκριβῶς ὁ ἴδιος μὲ αὐτὸν τῆς 3. Ἡ ἐφαρμογὴ εἶναι ἐντελῶς ἀνάλογη. Τώρα παρατηροῦμε ὅτι τὸ 61 εἶναι τῆς μορφῆς $k(p - 1) + 1$ γιὰ $p \in \{5, 7, 13, 31\}$ διότι $61 = 15(5 - 1) + 1$, $61 = 10(7 - 1) + 1$, $61 = 5(13 - 1) + 1$, $61 = 2(31 - 1) + 1$.

5. *Ἔστω ὅτι οἱ a, b εἶναι ἀκέραιοι > 1, πρῶτοι μεταξύ τους καὶ $a^2 b^3 = 3^6 \cdot 5^4 \cdot 7^3$.*
   (α΄) Ἀποδεῖξτε ὅτι ὁ a δὲν εἶναι διαιρετὸς διὰ 7.
   (β΄) Ὑπολογῖστε ὅλα τὰ δυνατὰ ζεύγη ἀκεραίων a, b, ποὺ πληροῦν τὶς παραπάνω συνθῆκες.

   Λύση. Κατ' ἀρχὰς παρατηροῦμε τὰ ἑξῆς: (1) Ἀφοῦ οἱ a, b εἶναι > 1, καθένας ἔχει ἕνα τουλάχιστον πρώτο ποὺ τὸν διαιρεῖ. Οἱ πρῶτοι ποὺ ἐμφανίζονται στὴν ἀνάλυση τοῦ a καὶ τοῦ b εἶναι κάποιοι ἀπὸ τοὺς $3, 5, 7$. (2) Ἀφοῦ $(a, b) = 1$, ἀποκλείεται νὰ ὑπάρχει πρῶτος ποὺ νὰ διαιρεῖ συγχρόνως τὸν a καὶ τὸν b. (3) Καθένας ἀπὸ τοὺς 3,5,7 πρέπει νὰ ἐμφανίζεται στὴν ἀνάλυση τοῦ a ἢ τοῦ b, ἀλλὰ ὄχι στὴν ἀνάλυση καὶ τῶν δύο, καθὼς εἴπαμε παραπάνω στὸ (2).

(α′) Ἂν $7 \mid a$, τότε ἡ ἀνάλυση τοῦ a σὲ πρώτους περιέχει τὸ 7, σὲ κάποια δύναμη, ἔστω ν, ἐνῶ ἡ ἀνάλυση τοῦ b δὲν περιέχει τὸ 7. Ἡ ἀνάλυση τοῦ a^2 σὲ πρώτους περιέχει τὸ 7 στὴ δύναμη 2ν. Ὅμως στὴ σχέση $a^2b^3 = 3^6 \cdot 5^4 \cdot 7^3$ τὸ 7 ἐμφανίζεται μὲ ἐκθέτη 3 στὸ δεξιὸ μέλος, ἄρα πρέπει νὰ ἐμφανίζεται μὲ ἐκθέτη 3 καὶ στὸ ἀριστερὸ μέλος, δηλαδή, $2\nu = 3$, ἄτοπο. Ἐναλλακτικά, μὲ χρήση ἐκθετῶν: Ἂν $7 \mid a$, τότε $v_7(a) > 1$ καὶ $v_7(b) = 0$. Ἐφαρμόζοντας τὴ συνάρτηση v_7 στὴ σχέση $a^2b^3 = 3^6 \cdot 5^4 \cdot 7^3$ παίρνομε $2v_7(a) + 3v_7(b) = 3$, ἄρα $2v_7(a) = 3$, ἄτοπο.
(β′) Ἀφοῦ τὸ 7 δὲν ἐμφανίζεται στὴν ἀνάλυση τοῦ a, πρέπει νὰ ἐμφανίζεται στὴν ἀνάλυση τοῦ b.
Ἐντελῶς ἀνάλογα, τὸ 5 δὲν διαιρεῖ τὸ b, διότι, ἂν τὸ 5 διαιροῦσε τὸν b, ὁ ἐκθέτης τοῦ 5 στὸ ἀριστερὸ μέλος θὰ ἦταν πολλαπλάσιο τοῦ 3, ἐνῶ ὁ ἐκθέτης τοῦ 5 στὸ δεξιὸ μέλος ἰσοῦται μὲ 4. Ἀφοῦ τὸ 5 δὲν ἐμφανίζεται στὴν ἀνάλυση τοῦ b, θὰ ἐμφανίζεται στὴν ἀνάλυση τοῦ a.
Μένει ὁ πρῶτος 3. Πρώτη περίπτωση: Ἂν ἐμφανίζεται στὴν ἀνάλυση τοῦ a, τότε δὲν ἐμφανίζεται στὴν ἀνάλυση τοῦ b, ἄρα $a = 3^3 \cdot 5^2$ καὶ $b = 7$. Ὁ ἐκθέτης ποὺ βάλαμε σὲ κάθε πρῶτο εἶναι τέτοιος ὥστε στὸν a^2b^2 νὰ ἐμφανιστεῖ ἐκθέτης 6 στὸν 3, ἐκθέτης 4 στὸν 5 καὶ ἐκθέτης 3 στὸν 7. Δεύτερη περίπτωση: Ἂν ἐμφανίζεται στὴν ἀνάλυση τοῦ b, τότε δὲν ἐμφανίζεται στὴν ἀνάλυση τοῦ a, ἄρα $a = 5^2$ καὶ $b = 3^2 \cdot 7$. Καὶ πάλι ἐπιλέξαμε τοὺς ἐκθέτες τῶν πρώτων ἔτσι ὥστε a^2b^3 νὰ ἐμφανιστεῖ ἐκθέτης 6 στὸν 3, ἐκθέτης 4 στὸν 5 καὶ ἐκθέτης 3 στὸν 7.

Ἐναλλακτικὴ λύση μὲ χρήση ἐκθετῶν: Κατ' ἀρχάς, γιὰ κάθε πρῶτο p ἰσχύει ὅτι, δὲν μπορεῖ νὰ εἶναι $v_p(a) > 0$ καὶ $v_p(b) > 0$, διότι αὐτὸ θὰ σήμαινε ὅτι p εἶναι κοινὸς διαιρέτης τῶν a, b. Ἐφαρμόζοντας τὴ συνάρτηση v_p στὴ σχέση $a^2b^3 = 3^6 \cdot 5^4 \cdot 7^3$ γιὰ $p = 7, 5, 3$, διαδοχικά, ἔχομε τὰ ἑξῆς:
• $2v_7(a) + 3v_7(b) = 3$ καὶ ἕνας ἐκ τῶν $v_7(a), v_7(b)$ εἶναι, ὑποχρεωτικά, 0. Εἶναι φανερὸ ὅτι, αὐτὴ ἡ ἰσότητα μπορεῖ νὰ ἰσχύει μόνο ἂν $v_7(a) = 0$ καὶ $v_7(b) = 1$. Δηλαδή, τὸ 7 δὲν ἐμφανίζεται στὴν ἀνάλυση τοῦ a καὶ ἐμφανίζεται στὴν ἀνάλυση τοῦ b μὲ ἐκθέτη 1.
• $2v_5(a) + 3v_5(b) = 4$ καὶ ἕνας ἐκ τῶν $v_5(a), v_5(b)$ εἶναι, ὑποχρεωτικά, 0. Εἶναι φανερὸ ὅτι, αὐτὴ ἡ ἰσότητα μπορεῖ νὰ ἰσχύει μόνο ἂν $v_5(b) = 0$ καὶ $v_5(a) = 2$. Δηλαδή, τὸ 5 ἐμφανίζεται στὴν ἀνάλυση τοῦ a μὲ ἐκθέτη 2 καὶ δὲν ἐμφανίζεται στὴν ἀνάλυση τοῦ b.
• $2v_3(a) + 3v_3(b) = 6$ καὶ ἕνας ἐκ τῶν $v_3(a), v_3(b)$ εἶναι, ὑποχρεωτικά, 0. Ἄρα, ἢ $v_3(a) = 3$ καὶ $v_3(b) = 0$, ἢ $v_3(a) = 0$ καὶ $v_3(b) = 2$. Στὴν πρώτη περίπτωση τὸ 3 ἐμφανίζεται στὴν ἀνάλυση τοῦ a μὲ ἐκθέτη 3 καὶ δὲν ἐμφανίζεται στὴν ἀνάλυση τοῦ b, ἐνῶ στὴ δεύτερη περίπτωση τὸ 3 ἐμφανίζεται στὴν ἀνάλυση τοῦ b μὲ ἐκθέτη 2 καὶ δὲν ἐμφανίζεται στὴν ἀνάλυση τοῦ a.

Συνδυάζοντας τὶς τρεῖς • βλέπομε ὅτι ἔχομε δύο δυνατὲς λύσεις: $a = 3^3 \cdot 5^2$, $b = 7$ ἢ $a = 5^2$, $b = 3^2 \cdot 7$.

Σημείωση. (1) Οἱ δύο λύσεις τῆς ἄσκησης 5 εἶναι ἰδιαίτερα λεπτομερεῖς καὶ δὲν ἀπαιτῶ ἡ δική σας λύση νὰ εἶναι τέτοια.

Στὴν ὁμάδα Β ὑπῆρχε ἀνάλογη ἄσκηση, ἡ ἑξῆς:

6. *Ἔστω ὅτι οἱ a, b εἶναι ἀκέραιοι > 1, πρῶτοι μεταξύ τους καὶ $a^3b^4 = 3^4 \cdot 5^{12} \cdot 11^3$.*
   (α′) Ἀποδεῖξτε ὅτι ὁ b δὲν εἶναι διαιρετός διὰ 11.
   (β′) Ὑπολογῖστε ὅλα τὰ δυνατά ζεύγη ἀκεραίων a, b, ποὺ πληροῦν τὶς παραπάνω συνθῆκες.
   Λύση. Ἐντελῶς ἀνάλογη μὲ αὐτὴν τῆς 5. Οἱ δυνατὲς λύσεις εἶναι $a = 5^4 \cdot 11$, $b = 3$ ἢ $a = 11$, $b = 3 \cdot 5^3$.