

Περί αναγωγισιμότητας πολυωνύμων.

Θάνος Μάγκος

Περίληψη

Στο παρόν άρθρο θα εξετάσουμε την έννοια της αναγωγισιμότητας πολυωνύμων. Όπως θα φανεί, η περίπτωση που παρουσιάζει μεγαλύτερο ενδιαφέρον είναι εκείνη, κατά την οποία οι συντελεστές του πολυωνύμου είναι ακέραιοι. Στη συνέχεια θα παραθέσουμε ορισμένα κριτήρια αναγωγισιμότητας, μερικά εκ των οποίων δεν είναι ευρέως γνωστά, καθώς και εφαρμογές τους. Στο τέλος παρατίθενται πέντε προβλήματα σχετικά με ανάγωγα πολυώνυμα.

Περιεχόμενα

1	Εισαγωγή	1
2	Αναγωγισιμότητα στα $\mathbb{Z}[x], \mathbb{Q}[x]$.	2
3	Το κριτήριο των Schönemann-Eisenstein	3
4	Το σώμα $\mathbb{Z}_p$.	5
5	Πολυώνυμα με έναν κυρίαρχο συντελεστή.	6
6	Πρώτοι αριθμοί και ανάγωγα πολυώνυμα.	8
7	Ανάγωγα τριώνυμα	10
8	Μερικά προβλήματα σχετικά με ανάγωγα πολυώνυμα	11

1 Εισαγωγή

Ας είναι $\mathbb{K}$ κάποιο από τα σύνολα $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Με $\mathbb{K}[x]$ συμβολίζουμε το σύνολο των πολυωνύμων με συντελεστές από το $\mathbb{K}$. Έτσι, με $\mathbb{Z}[x]$ συμβολίζουμε τον δακτύλιο των πολυωνύμων με ακέραιους συντελεστές κ.ο.κ.

ΟΡΙΣΜΟΣ: Έστω

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

πολυώνυμο με συντελεστές στο $\mathbb{K}$. Το $P(x)$ ονομάζεται ανάγωγο στο $\mathbb{K}[x]$, αν δεν μπορεί να γραφεί ως το γινόμενο δύο πολυωνύμων θετικού βαθμού, με συντελεστές από το $\mathbb{K}$.

Από τον παραπάνω ορισμό γίνεται φανερό ότι τα ανάγωγα πολυώνυμα αποτελούν ένα ανάλογο των πρώτων αριθμών. Όπως ακριβώς οι πρώτοι αριθμοί δεν μπορούν να

γραφούν ως το γινόμενο δύο ακεραίων μεγαλύτερων της μονάδας, έτσι και τα ανάγωγα πολυώνυμα δεν αναλύονται σε γινόμενο πολυωνύμων θετικού βαθμού. Μάλιστα, όπως ακριβώς ένας θετικός ακέραιος αναλύεται κατά μοναδικό τρόπο σε γινόμενο πρώτων παραγόντων, έτσι και κάθε πολυώνυμο αναλύεται μονοσήμαντα σε γινόμενο ανάγωγων πολυωνύμων (αν δεν ληφθεί υπόψη η σειρά ή οι μεγιστοβάθμιοι συντελεστές).

Ας θεωρήσουμε για παράδειγμα το πολυώνυμο

$$f(x) = x^4 + 1.$$

Στο $\mathbb{C}[x]$ έχουμε την παραγοντοποίηση

$$f(x) = (x - \theta_0)(x - \theta_1)(x - \theta_2)(x - \theta_3),$$

όπου

$$\theta_j = \cos \frac{2j+1}{4}\pi + i \sin \frac{2j+1}{4}\pi$$

οι τέταρτες ρίζες του -1 . Δηλαδή το $f(x)$ δεν είναι ανάγωγο στο $\mathbb{C}[x]$. Επίσης παρατηρούμε ότι είναι

$$x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2 = (x^2 + 1)^2 - (x\sqrt{2})^2$$

άρα

$$f(x) = (x^2 - x\sqrt{2} + 1)(x^2 + x\sqrt{2} + 1)$$

οπότε το $f(x)$ δεν είναι ανάγωγο στο $\mathbb{R}[x]$.

Εξετάζουμε τώρα αν το $f(x)$ είναι ανάγωγο στο $\mathbb{Z}[x]$. Καθώς είναι τετάρτου βαθμού, αν δεν είναι ανάγωγο, θα γράφεται ως το γινόμενο ενός πρωτοβάθμιου και ενός τριτοβάθμιου ή ως το γινόμενο δύο δευτεροβάθμιων. Η πρώτη περίπτωση αποκλείεται, αφού τότε το $f(x)$ θα είχε ακέραια ρίζα. Στη δεύτερη περίπτωση θα είχαμε την ανάλυση

$$f(x) = (x^2 + ax + b)(x^2 + cx + d), a, b, c, d \in \mathbb{Z},$$

οπότε θα καταλήγαμε στο σύστημα

$$a + c = ad + bc = b + d + ac = 0, bd = 1.$$

Αυτό όμως είναι αδύνατο στους ακέραιους. Άρα το $f(x)$ είναι ανάγωγο στο $\mathbb{Z}[x]$.

Φαίνεται λοιπόν, ότι η έννοια του ανάγωγου πολυωνύμου συνδέεται στενά με το σύνολο $\mathbb{K}[x]$ ως προς το οποίο την εξετάζουμε.

Καταρχάς, ως παρατηρήσουμε ότι το Θεμελιώδες Θεώρημα της Άλγεβρας εξασφαλίζει πως τα μόνα ανάγωγα πολυώνυμα στο $\mathbb{C}[x]$ είναι τα πρωτοβάθμια, αφού κάθε πολυώνυμο $P(x)$ βαθμού $n > 0$ έχει n ακριβώς ρίζες στο $\mathbb{C}$ και επομένως μπορεί να γραφεί ως

$$P(x) = c \prod_{j=1}^n (x - r_j).$$

Ως εκ τούτου, η έννοια της αναγωγιμότητας στο $\mathbb{C}[x]$ δεν παρουσιάζει ενδιαφέρον.

Εξετάζουμε στη συνέχεια την αναγωγιμότητα στο $\mathbb{R}[x]$. Ας θεωρήσουμε ένα πολυώνυμο $P(x) \in \mathbb{R}[x]$. Είναι εύκολο να δούμε ότι αυτό γράφεται ως το γινόμενο πολυωνύμων με πραγματικούς συντελεστές και με βαθμούς 1 ή 2. Αυτό προκύπτει από την παραγοντοποίηση που αναφέρθηκε προηγουμένως, σε συνδυασμό με το γεγονός ότι οι μη πραγματικές ρίζες ενός πολυωνύμου $P(x) \in \mathbb{R}[x]$ εμφανίζονται σε ζεύγη συζυγών. Διαπιστώνουμε λοιπόν, ότι τα μόνα ανάγωγα πολυώνυμα με πραγματικούς συντελεστές είναι τα πρωτοβάθμια, καθώς και τα δευτεροβάθμια με αρνητική διακρίνουσα.

Από τα προηγούμενα γίνεται φανερό ότι το αν ένα πολυώνυμο είναι ανάγωγο στο $\mathbb{R}[x]$ ή στο $\mathbb{C}[x]$ είναι τετριμμένο. Ωστόσο, η κατάσταση είναι τελείως διαφορετική αν αναφερόμαστε σε αναγωγιμότητα στο $\mathbb{Z}[x]$ ή στο $\mathbb{Q}[x]$. Στα επόμενα θα ασχοληθούμε αποκλειστικά με πολυώνυμα που έχουν ακέραιους συντελεστές και η έννοια της αναγωγιμότητας θα περιοριστεί στην αναγωγιμότητα στα $\mathbb{Z}[x], \mathbb{Q}[x]$. Αυτή η περίπτωση είναι και η πιο ενδιαφέρουσα.

2 Αναγωγιμότητα στα $\mathbb{Z}[x], \mathbb{Q}[x]$.

Αν

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

είναι πολυώνυμο με ακέραιους συντελεστές, ονομάζουμε περιεχόμενο (content) του $P(x)$ τον μέγιστο κοινό διαιρέτη των συντελεστών $a_n, a_{n-1}, \dots, a_1, a_0$ και τον συμβολίζουμε με $\text{cont}(P(x))$. Επίσης, ένα πολυώνυμο $P(x) \in \mathbb{Z}[x]$, για το οποίο ισχύει $\text{cont}(P(x)) = 1$, ονομάζεται πρωταρχικό. Είναι φανερό ότι κάθε πολυώνυμο $P(x) \in \mathbb{Z}[x]$ μπορεί να γραφεί στη μορφή $P(x) = dR(x)$, όπου d το περιεχόμενό του και $R(x)$ πρωταρχικό πολυώνυμο.

Θα χρειαστούμε το ακόλουθο

ΘΕΩΡΗΜΑ 1. Το γινόμενο πρωταρχικών πολυωνύμων είναι πρωταρχικό πολυώνυμο

ΑΠΟΔΕΙΞΗ. Ας είναι

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

$$Q(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0,$$

δύο πρωταρχικά πολυώνυμα. Ας είναι

$$d = \text{cont}(P(x)Q(x)).$$

Υποθέτουμε ότι ισχύει $d > 1$ και ας είναι p ένας πρώτος διαιρέτης του d . Ας είναι ακόμα $j \geq 0$ ο μικρότερος δείκτης για τον οποίο ισχύει $p \nmid a_j$ και $k \geq 0$ ο μικρότερος δείκτης για τον οποίο ισχύει $p \nmid b_k$.

Ο συντελεστής του x^{j+k} είναι ο

$$c_{j+k} = a_j b_k + a_{j+1} b_{k-1} + \dots + a_{j+k} b_0.$$

Επειδή ο p διαιρεί όλους τους συντελεστές $b_0, b_1, \dots, b_{k-1}$ αλλά και τον c_{j+k} , προκύπτει ότι $p \mid a_j b_k$, που είναι αδύνατο. Άρα $d = 1$ και το $P(x)Q(x)$ είναι πρωταρχικό.

Είμαστε τώρα έτοιμοι να αποδείξουμε το

ΛΗΜΜΑ. (Gauss) Έστω πρωταρχικό πολυώνυμο $P(x) \in \mathbb{Z}[x]$. Το $P(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$ αν και μόνο αν είναι ανάγωγο στο $\mathbb{Z}[x]$.

ΑΠΟΔΕΙΞΗ. Το ευθύ είναι προφανές. Θα αποδείξουμε ότι αν ένα πολυώνυμο είναι ανάγωγο στο $\mathbb{Z}[x]$, τότε είναι ανάγωγο και στο $\mathbb{Q}[x]$. Υποθέτουμε λοιπόν ότι ισχύει

$$P(x) = R(x)T(x),$$

με τα πολυώνυμα $R(x), T(x)$ να είναι μη σταθερά και με ρητούς συντελεστές. Κάνοντας τα κλάσματα ομώνυμα και βγάζοντας όποιους κοινούς παράγοντες είναι δυνατόν, το γινόμενο $R(x)T(x)$ μπορεί να λάβει τη μορφή

$$\frac{m}{n} f(x)g(x),$$

όπου m, n είναι ακέραιοι, πρώτοι μεταξύ τους και τα πολυώνυμα $f(x), g(x)$ έχουν ακέραιους συντελεστές και είναι πρωταρχικά. Είναι δηλαδή

$$nP(x) = mf(x)g(x).$$

Από το προηγούμενο λήμμα, το γινόμενο $f(x)g(x)$ είναι πρωταρχικό πολυώνυμο και επομένως έχουμε

$$n = \text{cont}(nP(x)) = \text{cont}(mf(x)g(x)) = m.$$

Άρα

$$P(x) = f(x)g(x), f(x), g(x) \in \mathbb{Z}[x],$$

το οποίο αντίκειται στην υπόθεση ότι το πολυώνυμο είναι ανάγωγο στο $\mathbb{Z}[x]$. Δηλαδή, το πολυώνυμο $P(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

Γίνεται λοιπόν φανερό ότι, ουσιαστικά, οι έννοιες της αναγωγισιμότητας στο $\mathbb{Z}[x]$ και της αναγωγισιμότητας στο $\mathbb{Q}[x]$ ταυτίζονται. Έτσι, στα επόμενα, θα γράφουμε απλώς ανάγωγο πολυώνυμο, χωρίς άλλη διευκρίνιση.

Φτάνουμε λοιπόν στο καίριο ερώτημα της έννοιας της αναγωγισιμότητας. Αν δοθεί ένα πολυώνυμο $P(x) \in \mathbb{Z}[x]$ πώς μπορούμε να διαπιστώσουμε ότι αυτό είναι ανάγωγο; Η απάντηση σε αυτή την ερώτηση δεν είναι, εν γένει, καθόλου απλή. Υπάρχουν όμως διάφορα κριτήρια που εγγυώνται ότι ένα πολυώνυμο είναι ανάγωγο. Αυτό είναι το αντικείμενο των επόμενων ενοτήτων.

3 Το κριτήριο των Schönemann-Eisenstein

Πρόκειται για το γνωστότερο κριτήριο αναγωγισιμότητας πολυωνύμων με ακέραιους συντελεστές. Αποδείχθηκε ανεξάρτητα από τους γερμανούς Theodor Schönemann (1846) και Gotthold Eisenstein (1850). Συνήθως, στη βιβλιογραφία, αναφέρεται σαν κριτήριο του Eisenstein. Στο παρόν άρθρο θα τηρηθεί αυτή η πρακτική, αν και προηγείται η ανακάλυψή του από τον Schönemann. Ο αναγνώστης που ενδιαφέρεται να εξερευνήσει την ιστορία σχετικά με το θέμα αυτό, παραπέμπεται στο [3].

ΘΕΩΡΗΜΑ 2. (1ο Κριτήριο Eisenstein) Έστω πολυώνυμο

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

με ακέραιους συντελεστές και p ένας πρώτος, για τον οποίο ισχύει

$$p|a_0, p|a_1, \dots, p|a_{n-1}, p \nmid a_n, p^2 \nmid a_0.$$

Τότε, το $P(x)$ είναι ανάγωγο.

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι το $P(x)$ δεν είναι ανάγωγο, οπότε θα υπάρχουν μη σταθερά πολυώνυμα $B(x), C(x)$ (τα οποία μπορούμε, λόγω του λήμματος του Gauss, να υποθέσουμε ότι έχουν ακέραιους συντελεστές), ώστε

$$P(x) = B(x)C(x).$$

Ας είναι

$$B(x) = b_r x^r + \dots + b_1 x + b_0,$$

$$C(x) = c_s x^s + \dots + c_1 x + c_0.$$

Φανερά ισχύει $a_0 = b_0 c_0$. Από την σχέση $p|a_0$ προκύπτει ότι $p|b_0$ ή $p|c_0$. Υποθέτουμε χωρίς βλάβη της γενικότητας ότι $p|b_0$. Τότε, από την $p^2 \nmid a_0$, έχουμε $p \nmid c_0$. Ας είναι $k < n$ ο μικρότερος δείκτης για τον οποίο ισχύει $p \nmid b_k$. Αυτός σίγουρα υπάρχει, αφού διαφορετικά θα είχαμε $p|a_j$ για όλα τα $j = 0, 1, \dots$, που είναι άτοπο. Ισχύει

$$\alpha_k = c_0 b_k + c_1 b_{k-1} + \dots + c_k b_0.$$

Από την σχέση αυτή προκύπτει τότε $p|c_0 b_k$, άτοπο. Άρα το $P(x)$ είναι ανάγωγο.

ΠΑΡΑΔΕΙΓΜΑ 1. Το πολυώνυμο

$$P(x) = 4x^7 - 6x^5 + 9x^2 + 27x - 3$$

είναι ανάγωγο, λόγω του κριτηρίου Eisenstein για τον πρώτο $p = 3$.

Επίσης το κριτήριο Eisenstein μας επιτρέπει να κατασκευάσουμε ανάγωγα πολυώνυμα οποιουδήποτε βαθμού.

ΠΑΡΑΔΕΙΓΜΑ 2. Το πολυώνυμο

$$f(x) = x^n - p, n > 1$$

και p πρώτος, είναι ανάγωγο.

ΠΑΡΑΔΕΙΓΜΑ 3. Ας εξετάσουμε τώρα το πολυώνυμο

$$P(x) = x^4 + 1.$$

Είναι προφανές ότι το κριτήριο Eisenstein δεν μπορεί να εφαρμοστεί, αφού δεν υπάρχει πρώτος διαιρέτης του 1. Τη δυσκολία αυτή θα την προσπεράσουμε βασιζόμενοι στην προφανή παρατήρηση ότι ένα πολυώνυμο $P(x)$ είναι ανάγωγο αν, και μόνο αν, το $P(x + \lambda)$, $\lambda \in \mathbb{Z}$ είναι ανάγωγο. Στην περίπτωσή μας έχουμε

$$P(x - 1) = (x - 1)^4 + 1 =$$

$$x^4 - 4x^3 + 6x^2 - 4x + 2,$$

και είναι φανερό ότι στο $P(x - 1)$ εφαρμόζεται το κριτήριο Eisenstein για $p = 2$.

Ας τονίσουμε όμως ότι γενικά δεν υπάρχει τρόπος να γνωρίζουμε εκ των προτέρων ποιος είναι ο αριθμός λ που μας εξυπηρετεί. Μάλιστα, υπάρχει περίπτωση να μην υπάρχει καν τέτοιος αριθμός. Ας θεωρήσουμε π.χ. το

$$P(x) = x^3 + x + 1.$$

Αυτό είναι ανάγωγο, γιατί προφανώς δεν έχει ακέραια ρίζα. Ωστόσο, το κριτήριο Eisenstein αποτυγχάνει, όποιος αριθμός και αν επιλεγεί ως λ . Πράγματι, είναι

$$P(x + \lambda) = x^3 + 3\lambda x^2 + (3\lambda^2 + 1)x + \lambda^3 + \lambda + 1$$

οπότε είναι φανερό ότι δεν υπάρχει πρώτος που να διαιρεί τους συντελεστές των x, x^2 . Ίσως το κλασικότερο παράδειγμα αυτού του είδους να αποτελεί η απόδειξη της αναγωγιμότητας του κυκλοτομικού πολυωνύμου $\Phi_p(x)$ όταν p πρώτος.

ΠΑΡΑΔΕΙΓΜΑ 4. Το πολυώνυμο

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 \text{ } p \text{ πρώτος,}$$

είναι ανάγωγο.

Πράγματι, παρατηρούμε ότι

$$\Phi_p(x) = \frac{x^p - 1}{x - 1},$$

οπότε

$$\Phi_p(x + 1) = \frac{(x + 1)^p - 1}{x} =$$

$$x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \dots + \binom{p}{p-2}x + p.$$

Είναι γνωστό ότι αν p πρώτος, οι διωνυμικοί συντελεστές $\binom{p}{k}, 1 \leq k \leq p-1$ διαιρούνται με το p . Άρα το $\Phi_p(x + 1)$ είναι ανάγωγο, από το κριτήριο του Eisenstein για τον πρώτο p .

ΠΑΡΑΔΕΙΓΜΑ 5. Δίνεται το πολυώνυμο $P(x) = x^2 + 10x + n$. Υπάρχουν άπειρες τιμές του ακεραίου n , για τις οποίες το $P(x)$ δεν είναι ανάγωγο, καθώς και άπειρες τιμές του ακεραίου n , για τις οποίες το $P(x)$ είναι ανάγωγο.

Πράγματι, αν θέσουμε

$$n = 25 - m^2, m \in \mathbb{Z}$$

είναι

$$P(x) = (x + 5 - m)(x + 5 + m),$$

ενώ αν θέσουμε

$$n = 4m + 2, m \in \mathbb{Z},$$

το $P(x)$ είναι ανάγωγο από το κριτήριο του Eisenstein για $p = 2$.

ΠΑΡΑΔΕΙΓΜΑ 6. Το πολυώνυμο

$$P(x) = 6x^5 + 9x^3 + 12x^2 + 4,$$

δεν ικανοποιεί το κριτήριο Eisenstein. Ωστόσο, το ικανοποιεί το αντίστροφό του, δηλαδή το πολυώνυμο

$$P^*(x) = 4x^5 + 12x^3 + 9x^2 + 6$$

για τον πρώτο $p = 3$.

Γενικότερα είναι εύκολο να αποδειχθεί ότι:

ΠΡΟΤΑΣΗ 1. Το πολυώνυμο

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

είναι ανάγωγο, αν και μόνο αν το πολυώνυμο

$$a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$

είναι ανάγωγο.

Η απόδειξη είναι απλή και αφήνεται στον αναγνώστη. Κλείνουμε την ενότητα με το

ΘΕΩΡΗΜΑ 3. (Γενικευμένο κριτήριο Eisenstein) Έστω πολυώνυμο

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

με ακέραιους συντελεστές, p πρώτος και $k \in \{0, 1, 2, \dots, n-1\}$.

Αν ισχύει

$$p | a_0, p | a_1, \dots, p | a_k, p \nmid a_{k+1}, p^2 \nmid a_0$$

τότε το $P(x)$ έχει ανάγωγο παράγοντα με βαθμό μεγαλύτερο του k .

ΑΠΟΔΕΙΞΗ. Είναι ουσιαστικά ίδια με την απόδειξη του κριτηρίου του Eisenstein.

Είναι φανερό ότι το κριτήριο του Eisenstein είναι ειδική περίπτωση του παραπάνω όταν $k = n - 1$. Μια κλασική εφαρμογή του γενικευμένου κριτηρίου αποτελεί το 1^ο θέμα της Διεθνούς Μαθηματικής Ολυμπιάδας του 1993.

ΠΑΡΑΔΕΙΓΜΑ 7. Αν $n > 1$ ακέραιος, να αποδείξετε ότι είναι ανάγωγο το πολυώνυμο

$$f(x) = x^n + 5x^{n-1} + 3.$$

Πράγματι, η εφαρμογή του γενικευμένου κριτηρίου για τον πρώτο $p = 3$, μας λέει ότι το $f(x)$ έχει ανάγωγο παράγοντα με βαθμό μεγαλύτερο ή ίσο του $n - 1$. Αν ο ανάγωγος παράγοντας είχε βαθμό $n - 1$, το $f(x)$ θα είχε πρωτοβάθμιο παράγοντα και συνεπώς ακέραια ρίζα. Όμως είναι φανερό ότι το $f(x)$ δεν έχει ρίζα κανέναν από τους $-1, -3, 1, 3$ (Θεώρημα Ακεραίων Ριζών). Άρα το $f(x)$ είναι όντως ανάγωγο. Αργότερα θα συναντήσουμε ακόμα δύο αποδείξεις για την αναγωγιμότητα του $f(x)$.

4 Το σώμα $\mathbb{Z}_p$.

Ας είναι p πρώτος και

$$\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$$

το πεπερασμένο σώμα με p στοιχεία. Ως συνήθως, με $\mathbb{Z}_p[x]$ θα συμβολίζουμε το σύνολο των πολυωνύμων με συντελεστές από το $\mathbb{Z}_p$. Θα αποδείξουμε το ακόλουθο:

ΘΕΩΡΗΜΑ 4. Ας είναι

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

μη σταθερό πολυώνυμο με ακέραιους συντελεστές. Ας είναι ακόμα $\bar{P}(x)$ το πολυώνυμο που προκύπτει από το $P(x)$ μετά από την αναγωγή όλων των συντελεστών του modulo p , όπου p πρώτος που δεν διαιρεί τον a_n . Αν το $\bar{P}(x)$ είναι ανάγωγο στο $\mathbb{Z}_p[x]$, τότε το $P(x)$ είναι ανάγωγο.

ΑΠΟΔΕΙΞΗ. Υποθέτουμε ότι το $P(x)$ δεν είναι ανάγωγο, οπότε θα υπάρχουν πολυώνυμα $B(x), C(x)$ ώστε

$$P(x) = B(x)C(x).$$

Από το λήμμα του Gauss τα $B(x), C(x)$ υποθέτουμε ότι έχουν ακέραιους συντελεστές. Ας είναι

$$B(x) = b_k x^k + \dots + b_1 x + b_0, C(x) = c_l x^l + \dots + c_1 x + c_0.$$

Είναι φανερό τότε ότι ισχύει $\bar{P}(x) = \bar{B}(x)\bar{C}(x)$ με $\bar{B}(x), \bar{C}(x) \in \mathbb{Z}_p[x]$. Επειδή $p \nmid a_n$ και ισχύει προφανώς $a_n = b_k c_l$, έχουμε $p \nmid b_k, p \nmid c_l$. Επομένως ισχύει $\bar{b}_k \neq 0$ και $\bar{c}_l \neq 0$, δηλαδή

$$\deg \bar{B}(x) = k, \deg \bar{C}(x) = l.$$

Άρα το $\bar{P}(x)$ δεν είναι ανάγωγο στο $\mathbb{Z}_p[x]$. Άτοπο. Άρα το $P(x)$ είναι ανάγωγο και η απόδειξη ολοκληρώθηκε.

ΠΑΡΑΤΗΡΗΣΕΙΣ ΣΤΟ ΘΕΩΡΗΜΑ 4.

α) Η συνθήκη ο p να μην διαιρεί τον a_n είναι ουσιώδης στο θεώρημα και δεν μπορεί να παραληφθεί. Για παράδειγμα, αν

$$P(x) = 2x^3 + 3x^2 + 3x + 1,$$

στο $\mathbb{Z}_2[x]$ είναι

$$\bar{P}(x) = x^2 + x + \bar{1},$$

το οποίο είναι ανάγωγο στο $\mathbb{Z}_2[x]$, αφού

$$\bar{P}(\bar{0}) = \bar{P}(\bar{1}) = \bar{1} \neq \bar{0}.$$

Όμως το $P(x)$ δεν είναι ανάγωγο, αφού

$$P(x) = (2x+1)(x^2+x+1).$$

β) Το αντίστροφο του θεωρήματος δεν ισχύει. Ακόμα περισσότερο, μπορεί ένα πολυώνυμο $P(x)$ να είναι ανάγωγο, αλλά να μην υπάρχει κανένας πρώτος p , ώστε το $\bar{P}(x)$ να είναι ανάγωγο στο $\mathbb{Z}_p[x]$. Ένα τέτοιο παράδειγμα είναι το πολυώνυμο

$$P(x) = x^4 - 10x^2 + 1.$$

Ας αποδείξουμε αρχικά ότι είναι ανάγωγο. Από το θεώρημα των ρητών ριζών, βλέπουμε ότι δεν έχει ρητή ρίζα, άρα δεν έχει πρωτοβάθμιο παράγοντα. Αναζητούμε τώρα ανάλυση του $P(x)$ υπό τη μορφή

$$P(x) = (x^2 + ax + b)(x^2 + cx + d), a, b, c, d \in \mathbb{Z}.$$

Από την εξίσωση των αντίστοιχων συντελεστών προκύπτει

$$a + c = 0, ac + b + d = -10,$$

$$ad + bc = 0,$$

$$bd = 1.$$

Από την τελευταία εξίσωση βρίσκουμε $b = d = 1$ ή $b = d = -1$, οπότε η δεύτερη εξίσωση γίνεται $ac = -12$ ή $ac = -8$. Λόγω της πρώτης εξίσωσης, έχουμε τότε $a^2 = 12$ ή $a^2 = 8$ που είναι αδύνατες στο $\mathbb{Z}$. Άρα το $P(x)$ είναι ανάγωγο.

Θα αποδείξουμε τώρα ότι το $\bar{P}(x)$ δεν είναι ανάγωγο στο $\mathbb{Z}_p[x]$ για οποιονδήποτε πρώτο p . Διακρίνουμε τρεις περιπτώσεις:

1^η περίπτωση: Αν το 2 είναι τετράγωνο modulo p , δηλαδή υπάρχει a ώστε να ισχύει $a^2 = \bar{2}$, βλέπουμε ότι ισχύει

$$x^4 - \bar{10}x^2 + \bar{1} = (x^2 - \bar{2}ax - \bar{1})(x^2 + \bar{2}ax - \bar{1}).$$

2^η περίπτωση: Αν το 3 είναι τετράγωνο modulo p , δηλαδή αν υπάρχει b ώστε να ισχύει $b^2 = \bar{3}$, βλέπουμε ότι ισχύει

$$x^4 - \bar{10}x^2 + \bar{1} = (x^2 - \bar{2}bx + \bar{1})(x^2 + \bar{2}bx + \bar{1}).$$

3^η περίπτωση: Αν δεν ισχύει τίποτα από τα προηγούμενα, το 6 είναι τετράγωνο modulo p , δηλαδή αν υπάρχει c ώστε να ισχύει $c^2 = \bar{6}$ και τότε ισχύει

$$x^4 - \bar{10}x^2 + \bar{1} = (x^2 - (\bar{5} + 2\bar{c}))(x^2 + (\bar{5} - 2\bar{c})).$$

Ας δούμε μερικά παραδείγματα εφαρμογής του θεωρήματος.

ΠΑΡΑΔΕΙΓΜΑ 8. Το πολυώνυμο

$$P(x) = x^3 - 8x^2 + 7x + 2019,$$

στο $\mathbb{Z}_2[x]$ γίνεται

$$\overline{P}(x) = x^3 + x + \overline{1}.$$

Ισχύει

$$\overline{P}(\overline{0}) = \overline{P}(\overline{1}) = \overline{1} \neq \overline{0},$$

δηλαδή δεν έχει ρίζες στο $\mathbb{Z}_2$. Άρα το $\overline{P}(x)$ είναι ανάγωγο στο $\mathbb{Z}_2[x]$ και επομένως το $P(x)$ είναι ανάγωγο στο $\mathbb{Z}[x]$.

ΠΑΡΑΔΕΙΓΜΑ 9. Το πολυώνυμο

$$P(x) = x^3 + (3m-1)x + 3n+1, \quad m, n \in \mathbb{Z},$$

είναι ανάγωγο, αφού στο $\mathbb{Z}_3[x]$ γίνεται

$$\overline{P}(x) = x^3 - x + \overline{1}$$

και αυτό είναι ανάγωγο στο $\mathbb{Z}_3[x]$. Πράγματι, είναι

$$\overline{P}(\overline{0}) = \overline{P}(\overline{1}) = \overline{1} \neq \overline{0}.$$

5 Πολυώνυμα με έναν κυρίαρχο συντελεστή.

Θα αναφέρουμε δύο κριτήρια που αφορούν πολυώνυμα στα οποία υπάρχει ένας κυρίαρχος μεταξύ των συντελεστών. Το πρώτο έχει μάλλον απλή απόδειξη. Οφείλεται στον Osada [10, σελ.58]

ΘΕΩΡΗΜΑ 5. Ας είναι

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + p$$

μη σταθερό πολυώνυμο με ακέραιους συντελεστές, όπου p πρώτος.

α) Αν $p > |a_1| + |a_2| + \dots + |a_{n-1}| + |a_n|$, τότε το $P(x)$ είναι ανάγωγο.

β) Αν $p \geq |a_1| + |a_2| + \dots + |a_{n-1}| + |a_n|$ και καμία από τις ρίζες του $P(x)$ δεν είναι ρίζα της μονάδας, τότε το $P(x)$ είναι ανάγωγο.

ΑΠΟΔΕΙΞΗ. α) Ας είναι $a \in \mathbb{C}$ μια ρίζα του $P(x)$. Αποδεικνύουμε ότι $|a| > 1$. Πράγματι, αν υποθέσουμε ότι ισχύει $|a| \leq 1$, έχουμε

$$\begin{aligned} p &= |a_n a^n + a_{n-1} a^{n-1} + \dots + a_1 a| \\ &\leq |a_n| + |a_{n-1}| + \dots + |a_1|, \end{aligned}$$

που αντίκειται στην υπόθεση. Ας είναι τώρα

$$P(x) = f(x)g(x),$$

όπου $f(x), g(x)$ πολυώνυμα θετικού βαθμού με ακέραιους συντελεστές. Είναι

$$P(0) = f(0)g(0),$$

άρα

$$|f(0)||g(0)| = p.$$

Επειδή ο p είναι πρώτος, υποθέτουμε χωρίς βλάβη της γενικότητας ότι $|f(0)| = 1$. Ας είναι ακόμα λ ο συντελεστής του μεγιστοβαθμίου όρου του $f(x)$. Από τους τύπους Vieta έχουμε ότι για τις ρίζες $\xi_1, \xi_2, \dots, \xi_k$ του $f(x)$ ισχύει

$$|\xi_1 \xi_2 \dots \xi_k| = \frac{1}{|\lambda|} \leq 1,$$

αφού $\lambda \in \mathbb{Z}$. Όμως οι ρίζες $\xi_1, \xi_2, \dots, \xi_k$ είναι και ρίζες του $P(x)$, άρα, όπως είδαμε προηγουμένως, $|\xi_i| > 1$ για κάθε $i = 1, 2, \dots, k$. Το άτοπο αυτό αποδεικνύει ότι το $P(x)$ είναι ανάγωγο υπεράνω του $\mathbb{Z}$.

β) Προφανής!

Το παραπάνω θεώρημα, αν και αποδεικνύεται εύκολα, έχει μάλλον αρκετά περιοριστικές προϋποθέσεις. Εκτός από το ότι απαιτείται ο σταθερός όρος να είναι κατά απόλυτη τιμή μεγαλύτερος από το άθροισμα των υπολοίπων, πρέπει να είναι και πρώτος. Στο επόμενο θεώρημα δεν απαιτείται κανένας συντελεστής να είναι πρώτος, αλλά τώρα ο κυρίαρχος συντελεστής είναι ο συντελεστής του x^{n-1} . Ερχόμαστε λοιπόν στο επόμενο κριτήριο, το οποίο οφείλεται στον Oskar Perron. Ο συντομότερος τρόπος να αποδειχθεί είναι με χρήση του θεωρήματος Rouché, από τη μιγαδική ανάλυση. Αυτή την απόδειξη μπορεί να την αναζητήσει ο αναγνώστης στο κλασικό βιβλίο του Victor Prasolov *Polynomials* ([10], σελ. 56). Εδώ θα παραθέσουμε μια στοιχειώδη απόδειξη, η οποία οφείλεται στον Ρουμάνο μαθηματικό Laurențiu Panaitopol [8].

ΘΕΩΡΗΜΑ 6. (Κριτήριο του Perron) Έστω μονικό πολυώνυμο με ακέραιους συντελεστές

$$P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0, a_0 \neq 0.$$

Αν ισχύει $|a_{n-1}| > 1 + |a_{n-2}| + \dots + |a_1| + |a_0|$, το $P(x)$ είναι ανάγωγο.

Το κρίσιμο σημείο της απόδειξης του θεωρήματος (είτε με χρήση του θεωρήματος Rouché, είτε με στοιχειώδη μέσα) είναι η απόδειξη του παρακάτω λήμματος:

ΛΗΜΜΑ. Το πολυώνυμο της εκφώνησης του θεωρήματος Perron έχει ακριβώς μια ρίζα με μέτρο > 1 και οι υπόλοιπες $n-1$ ρίζες βρίσκονται στο εσωτερικό του δίσκου $|z| < 1$.

ΑΠΟΔΕΙΞΗ ΤΟΥ ΛΗΜΜΑΤΟΣ: Αρχικά αποδεικνύουμε ότι το πολυώνυμο δεν έχει ρίζα w με $|w| = 1$. Πράγματι, αν ίσχυε αυτό θα είχαμε

$$-a_{n-1}w^{n-1} = w^n + a_{n-2}w^{n-2} + \dots + a_1w + a_0$$

οπότε

$$\begin{aligned} |a_{n-1}| &= |-a_{n-1}w^{n-1}| = \\ |w^n + a_{n-2}w^{n-2} + \dots + a_1w + a_0| &\leq \\ \leq |w^n| + |a_{n-2}w^{n-2}| + \dots + |a_1w| + |a_0| &= \\ 1 + |a_{n-2}| + \dots + |a_1| + |a_0|, \end{aligned}$$

που αντιβαίνει στην υπόθεση.

Ας είναι τώρα $x_1, x_2, \dots, x_n$ οι ρίζες του $P(x)$. Από τους τύπους Vieta ισχύει

$$|x_1x_2\cdots x_n| = |a_0| \geq 1$$

και επειδή καμία ρίζα δεν έχει μοναδιαίο μέτρο, υπάρχει ρίζα, έστω η x_1 , ώστε $|x_1| > 1$. Ας είναι

$$Q(x) = x^{n-1} + b_{n-2}x^{n-2} + \dots + b_1x + b_0$$

το μονικό πολυώνυμο με ρίζες τις $x_2, x_3, \dots, x_n$. Είναι τότε

$$P(x) = (x - x_1)Q(x) =$$

$$\begin{aligned} x^n + (b_{n-2} - x_1)x^{n-1} + (b_{n-3} - b_{n-2}x_1)x^{n-2} + \dots + \\ + (b_0 - b_1x_1)x - b_0x_1. \end{aligned}$$

Επομένως έχουμε

$$a_{n-1} = b_{n-2} - x_1,$$

$$a_{n-2} = b_{n-3} - b_{n-2}x_1,$$

$$\dots,$$

$$a_1 = b_0 - b_1x_1, a_0 = -b_0x_1$$

και από τη συνθήκη του θεωρήματος προκύπτει

$$|b_{n-2} - x_1| > 1 + |b_{n-3} - b_{n-2}x_1| + \dots + |b_0 - b_1x_1| + |b_0x_1| \geq$$

$$\begin{aligned} 1 + |b_{n-2}||x_1| - |b_{n-3}| + |b_{n-3}||x_1| - |b_{n-4}| + \dots + \\ + |b_1||x_1| - |b_0| + |b_0||x_1| = \end{aligned}$$

$$1 + |b_{n-2}| + (|x_1| - 1)(|b_{n-2}| + |b_{n-3}| + \dots + |b_0|).$$

Επομένως λαμβάνουμε

$$|b_{n-2}| + |x_1| > 1 + |b_{n-2}| + (|x_1| - 1) \sum_{k=0}^{n-2} |b_k|$$

δηλαδή

$$\sum_{k=0}^{n-2} |b_k| < 1.$$

Ας είναι τώρα $w \in \mathbb{C}$ με $|w| \geq 1$. Έχουμε

$$|Q(w)| = |w^{n-1} + b_{n-2}w^{n-2} + \dots + b_1w + b_0| \geq$$

$$\geq |w|^{n-1} - |b_{n-2}||w|^{n-2} - |b_1||w| - |b_0| \geq$$

$$\geq |w|^{n-1} - |w|^{n-1}(|b_{n-2}| + |b_{n-3}| + \dots + |b_0|) =$$

$$|w|^{n-1} \left(1 - \sum_{k=0}^{n-2} |b_k| \right) > 0.$$

Επομένως το $Q(x)$ δεν έχει ρίζα με μέτρο μεγαλύτερο ή ίσο του 1. Άρα όλες οι ρίζες του βρίσκονται στο εσωτερικό του δίσκου $|z| < 1$ και η απόδειξη του λήμματος ολοκληρώθηκε. Πλέον, η απόδειξη του κριτηρίου του Perron είναι απλή.

ΑΠΟΔΕΙΞΗ ΘΕΩΡΗΜΑΤΟΣ 6 Υποθέτουμε ότι υπάρχουν μη σταθερά πολυώνυμα $A(x), B(x)$ με ακέραιους συντελεστές, ώστε

$$P(x) = A(x)B(x).$$

Από το λήμμα, το $P(x)$ έχει ακριβώς μια ρίζα με μέτρο > 1 , άρα ένα από τα $A(x), B(x)$ έχει όλες τις ρίζες του με μέτρο μικρότερο του 1. Ας πούμε ότι αυτό είναι το $A(x)$ και οι ρίζες του είναι οι $r_1, \dots, r_k$. Είναι τότε

$$|A(0)| = |r_1r_2\cdots r_k| < 1,$$

άτοπο, αφού $A(0) \in \mathbb{Z}^*$. Συνεπώς, το $P(x)$ είναι ανάγωγο.

ΕΦΑΡΜΟΓΕΣ

α) Το πολυώνυμο του παραδείγματος 7 είναι ανάγωγο, αφού ικανοποιεί τις προϋποθέσεις του κριτηρίου Perron.

β) Αν a θετικός ακέραιος, το πολυώνυμο

$$P(x) = x^n + (a+3)x^{n-1} + x + a,$$

είναι ανάγωγο.

6 Πρώτοι αριθμοί και ανάγωγα πολυώνυμα.

Η 6^η Βαλκανική Μαθηματική Ολυμπιάδα (B.M.O.) έλαβε χώρα στις αρχές του Μάη του 1989 στο Σπλιτ της τότε Γιουγκοσλαβίας. Ένα από τα τέσσερα θέματα του διαγωνισμού ήταν το ακόλουθο:

2^ο Πρόβλημα της 6^{ης} B.M.O:

Ας είναι

$$\overline{a_n a_{n-1} \dots a_1 a_0} = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0$$

η δεκαδική αναπαράσταση ενός πρώτου αριθμού και ας είναι $n > 1, a_n > 1$. Να αποδείξετε ότι το πολυώνυμο $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ δεν μπορεί να γραφεί ως το γινόμενο δύο μη σταθερών πολυωνύμων με ακέραιους συντελεστές.

Το πρόβλημα αυτό δεν ήταν καινούριο. Υπάρχει στο κλασικό βιβλίο των Pólya-Szegő *Problems and Theorems in Analysis II. Theory of Functions. Zeros. Polynomials. Determinants. Number Theory. Geometry.* [9]. Εκεί αποδίδεται το πρόβλημα αυτό στον A. Cohn. Μάλιστα, στην αρχική του μορφή, το πρόβλημα είναι λίγο γενικότερο, καθώς δεν έχει τον περιορισμό $a_n > 1$. Προφανώς, στην B.M.O. δόθηκε αυτή η συνθήκη, ώστε να διευκολυνθούν οι διαγωνιζόμενοι.

Ας δούμε αρχικά μια λύση του παραπάνω προβλήματος. ΑΠΟΔΕΙΞΗ. Υποθέτουμε ότι υπάρχουν πολυώνυμα $Q(x), R(x) \in \mathbb{Z}[x]$ τέτοια, ώστε να ισχύει

$$P(x) = Q(x) R(x).$$

Τότε

$$P(10) = Q(10) R(10),$$

οπότε ο αριθμός $Q(10) R(10)$ είναι πρώτος. Επομένως ισχύει $|Q(10)| = 1$ ή $|R(10)| = 1$. Ας υποθέσουμε ότι $|Q(10)| = 1$. Ας είναι $x_1, x_2, \dots, x_r \in \mathbb{C}$ οι ρίζες του $Q(x)$ (οι οποίες προφανώς είναι και ρίζες του $P(x)$). Τότε ισχύει

$$|c| |10 - x_1| |10 - x_2| \dots |10 - x_r| = 1 \quad (*)$$

Όμως, για τις ρίζες x_i ισχύει

$$|x_i| \leq 1 + \max \left\{ \left| \frac{a_k}{a_n} \right|, k = 0, 1, 2, \dots, n-1 \right\} \leq 1 + \frac{9}{2} = \frac{11}{2}.$$

Επομένως είναι

$$|10 - x_i| \geq 10 - |x_i| \geq 10 - \frac{11}{2} = \frac{9}{2}.$$

Τότε, λόγω της (*) καταλήγουμε σε άτοπο. Άρα το $P(x)$ είναι ανάγωγο.

Αποδεικνύουμε το θεώρημα για τα φράγματα των ριζών, το οποίο χρησιμοποιήθηκε παραπάνω.

ΘΕΩΡΗΜΑ 7. Έστω πολυώνυμο

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, a_n \neq 0$$

με $a_i \in \mathbb{C}, i = 0, 1, 2, \dots$. Αν z ρίζα του $f(x)$, ισχύει $|z| \leq 1 + M$, όπου

$$M = \max \left\{ \left| \frac{a_k}{a_n} \right|, k = 0, 1, 2, \dots, n-1 \right\}.$$

ΑΠΟΔΕΙΞΗ. Αρκεί να αποδειχθεί το θεώρημα για τις ρίζες για τις οποίες ισχύει $|z| > 1$. Ισχύει

$$-a_n z^n = a_{n-1} z^{n-1} + \dots + a_1 z + a_0,$$

επομένως

$$|a_n| |z|^n \leq |a_{n-1}| |z|^{n-1} + \dots + |a_1| |z| + |a_0|$$

άρα

$$\begin{aligned} |z|^n &\leq \left| \frac{a_{n-1}}{a_n} \right| |z|^{n-1} + \dots + \left| \frac{a_0}{a_n} \right| \leq \\ M (|z|^{n-1} + \dots + |z| + 1) &= \\ M \frac{|z|^n - 1}{|z| - 1}. \end{aligned}$$

Επομένως ισχύει

$$\begin{aligned} M &\geq \frac{|z| - 1}{|z|^n - 1} |z|^n = \frac{|z|^{n+1} - 1}{|z|^n - 1} - 1 \Rightarrow \\ M + 1 &\geq \frac{|z|^{n+1} - 1}{|z|^n - 1}. \end{aligned}$$

Επειδή προφανώς είναι

$$\frac{|z|^{n+1} - 1}{|z|^n - 1} \geq |z|$$

η απόδειξη ολοκληρώνεται.

Καταρχάς, ας παρατηρήσουμε ότι το παραπάνω πρόβλημα μας λέει ότι από κάθε πρώτο αριθμό (που δεν έχει ως πρώτο ψηφίο τη μονάδα) μπορούμε να κατασκευάσουμε ένα ανάγωγο πολυώνυμο. Για παράδειγμα, ο 6427 είναι πρώτος, οπότε το $6x^3 + 4x^2 + 2x + 7$ είναι ανάγωγο. Ομοίως, το $2x^4 + x^3 + 3x^2 + 4x + 7$ είναι ανάγωγο, γιατί ο 21347 είναι πρώτος. Όπως όμως αναφέραμε προηγουμένως η συνθήκη $a_n > 1$ είναι περιττή και μπορεί να παραληφθεί. Θα αποδείξουμε τώρα το κριτήριο του Cohn στη γενικότερη μορφή του.

ΘΕΩΡΗΜΑ 8. (Κριτήριο του Cohn) Ας είναι

$$\overline{a_n a_{n-1} \dots a_1 a_0} = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0$$

η δεκαδική αναπαράσταση ενός πρώτου αριθμού και ας είναι $n > 1$. Τότε το πολυώνυμο

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

είναι ανάγωγο.

Θα χρειαστούμε το ακόλουθο

ΛΗΜΜΑ. Αν $w \in \mathbb{C}$ ρίζα του $P(x)$, ισχύει

$$\Re(w) < \frac{1 + \sqrt{1 + 4M}}{2}$$

όπου

$$M = \max \left\{ \left| \frac{a_k}{a_n} \right|, k = 0, 1, 2, \dots, n-1 \right\}.$$

ΑΠΟΔΕΙΞΗ ΤΟΥ ΛΗΜΜΑΤΟΣ.

Ας υποθέσουμε ότι η w είναι ρίζα του $P(x)$ με

$$\Re(w) \geq \frac{1 + \sqrt{1 + 4M}}{2}.$$

Τότε έχουμε

$$|w| \geq \Re(w) \geq \frac{1 + \sqrt{1 + 4M}}{2}.$$

Από την $P(w) = 0$ προκύπτει

$$a_n w^n + a_{n-1} w^{n-1} = -(a_{n-2} w^{n-2} + \dots + a_1 w + a_0)$$

οπότε

$$w + \frac{a_{n-1}}{a_n} = - \left(\frac{a_{n-2}}{a_n} \cdot \frac{1}{w} + \frac{a_{n-3}}{a_n} \cdot \frac{1}{w^2} + \dots + \frac{a_0}{a_n} \cdot \frac{1}{w^{n-1}} \right).$$

Επομένως

$$\left| w + \frac{a_{n-1}}{a_n} \right| \leq M \left(\frac{1}{|w|} + \frac{1}{|w|^2} + \dots + \frac{1}{|w|^{n-1}} \right) <$$

$$\frac{M}{|w| - 1} \leq \frac{2M}{\sqrt{1 + 4M} - 1}.$$

Όμως είναι και

$$\left| w + \frac{a_{n-1}}{a_n} \right| \geq \Re \left(w + \frac{a_{n-1}}{a_n} \right) = \Re(w) + \frac{a_{n-1}}{a_n} \geq$$

$$\Re(w) \geq \frac{1 + \sqrt{1 + 4M}}{2}.$$

Αυτό είναι αδύνατο, αφού

$$\frac{2M}{\sqrt{1 + 4M} - 1} = \frac{1 + \sqrt{1 + 4M}}{2}.$$

Μπορούμε τώρα να αποδείξουμε το κριτήριο του Cohn.

ΑΠΟΔΕΙΞΗ ΤΟΥ ΘΕΩΡΗΜΑΤΟΣ 8.

Καταρχάς είναι εύκολο να αποδειχθεί ότι ισχύει

$$\Re(w) < \frac{19}{2} \Leftrightarrow |10 - w| > |9 - w|.$$

Ας υποθέσουμε λοιπόν ότι υπάρχουν μη σταθερά πολυώνυμα $Q(x), R(x)$ με ακέραιους συντελεστές, ώστε

$$P(x) = Q(x) R(x).$$

Τότε

$$P(10) = Q(10) R(10),$$

οπότε ο αριθμός $Q(10) R(10)$ είναι πρώτος. Επομένως ισχύει

$$|Q(10)| = 1 \text{ ή } |R(10)| = 1.$$

Ας υποθέσουμε ότι $|Q(10)| = 1$.

Ας είναι $x_1, x_2, \dots, x_r \in \mathbb{C}$ οι ρίζες του $Q(x)$ (οι οποίες προφανώς είναι και ρίζες του $P(x)$). Τότε ισχύει

$$|c| |10 - x_1| |10 - x_2| \dots |10 - x_r| = 1$$

Από το λήμμα προκύπτει ότι

$$\Re(x_i) < \frac{1 + \sqrt{37}}{2} < \frac{19}{2},$$

άρα $|10 - x_i| > |9 - x_i|$ για κάθε i . Επομένως λαμβάνουμε

$$1 = |c| |10 - x_1| |10 - x_2| \dots |10 - x_r| >$$

$$|c| |9 - x_1| |9 - x_2| \dots |9 - x_r|$$

δηλαδή $1 > |Q(9)|$. Αυτό όμως είναι αδύνατο, αφού φανερά το $|Q(9)|$ είναι θετικός ακέραιος. Άρα το $P(x)$ είναι ανάγωγο.

Το 1981 οι Brillhart, Filaseta και Odlyzko ([1]) απέδειξαν το εξής γενικότερο:

ΘΕΩΡΗΜΑ 9. (Γενικευμένο Κριτήριο Cohn) Έστω p πρώτος και $b \geq 2$ ένας ακέραιος. Αν $\overline{p_n p_{n-1} \dots p_1 p_0}$ είναι η αναπαράσταση του p στη βάση b και $p_n \neq 0$, τότε το πολυώνυμο

$$f(x) = p_n x^n + p_{n-1} x^{n-1} + \dots + p_1 x + p_0$$

είναι ανάγωγο.

Οι συγγραφείς αναφέρουν ως παράδειγμα τον πρώτο αριθμό 397. Σύμφωνα με το παραπάνω θεώρημα, γράφοντας τον αριθμό αυτόν σε διάφορες αναπαραστάσεις, λαμβάνουμε ανάγωγα πολυώνυμα.

p	Ανάγωγο Πολυώνυμο
$(110001101)_2$	$x^8 + x^7 + x^3 + x^2 + 1$
$(112201)_3$	$x^5 + x^4 + 2x^3 + 2x^2 + 1$
$(12031)_4$	$x^4 + 2x^3 + 3x + 1$
$(3042)_5$	$3x^3 + 4x + 2$
$(1501)_6$	$x^3 + 5x^2 + 1$
$(1105)_7$	$x^3 + x^2 + 5$
$(615)_8$	$6x^2 + x + 5$

Ο M. Ram Murty στο [7] έδωσε μια απλοποιημένη απόδειξη του γενικευμένου κριτηρίου του Cohn. Η απόδειξη αυτή μοιάζει με την απόδειξη του θεωρήματος 6.

7 Ανάγωγα τριώνυμα

Ακόμα και αν περιοριστούμε στην περίπτωση τριωνύμου, και μάλιστα ειδικής μορφής, το να αποφανθούμε αν είναι ή όχι ανάγωγο δεν είναι απλή υπόθεση. Ένα αποτέλεσμα προς αυτή τη κατεύθυνση είναι το

Θεώρημα 9^ο : Αν m, n φυσικοί αριθμοί με $m > n$ και $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$, τα πολυώνυμα

$$f(x) = x^m + \varepsilon_1 x^n + 4\varepsilon_2$$

είναι ανάγωγα, εκτός από τις παρακάτω περιπτώσεις:

$$\bullet x^{3t} + \varepsilon_1 x^{2t} + 4\varepsilon_1 =$$

$$(x^t + 2\varepsilon_1)(x^{2t} - \varepsilon_1 x^t + 2)$$

$$\bullet x^{5t} + \varepsilon_1 x^{2t} - 4\varepsilon_1 =$$

$$(x^{3t} + \varepsilon_1 x^{2t} - x^t - 2\varepsilon_1)(x^{2t} - \varepsilon_1 x^t + 2)$$

$$\bullet x^{11t} + \varepsilon_1 x^{4t} + 4\varepsilon_1 =$$

$$(x^{5t} - x^{3t} - \varepsilon_1 x^{2t} + 2\varepsilon_1)(x^{6t} + x^{4t} + \varepsilon_1 x^{3t} + x^{2t} + 2)$$

Οι παράγοντες στις παραπάνω περιπτώσεις είναι ανάγωγα πολυώνυμα.

Το θεώρημα αυτό οφείλεται στον Arne Jonassen. Η απόδειξη βρίσκεται στο [4].

Ένα ακόμα σχετικό αποτέλεσμα, το οποίο οφείλουμε στον Ernst Selmer [11] είναι το εξής:

Θεώρημα 10^ο :

α) Το πολυώνυμο $P(x) = x^n - x - 1$ είναι ανάγωγο για όλες τις τιμές του $n \geq 2$.

β) Το πολυώνυμο $Q(x) = x^n + x + 1$ είναι ανάγωγο όταν $n \not\equiv 2 \pmod{3}$, αλλά έχει παράγοντα το $x^2 + x + 1$ όταν $n \equiv 2 \pmod{3}$. Στην περίπτωση αυτή, ο άλλος παράγοντας είναι ανάγωγο πολυώνυμο.

Θα αποδείξουμε το α)

ΑΠΟΔΕΙΞΗ. Αρχικά αποδεικνύουμε ότι το πολυώνυμο δεν έχει ρίζα z με $|z| = 1$. Έστω λοιπόν

$$z = \cos t + i \sin t, \quad t \in [0, 2\pi),$$

ρίζα του $P(x)$. Τότε είναι $z^n = z + 1$ άρα $|z + 1| = 1$, οπότε

$$(1 + \cos t)^2 + \sin^2 t = 1 \Rightarrow \cos t = -\frac{1}{2},$$

άρα $t = \frac{2\pi}{3}$ ή $\frac{4\pi}{3}$. Τότε $z^3 = 1$, οπότε

• αν $n = 3k$, είναι

$$P(z) = z^{3k} - z - 1 = -z \neq 0.$$

• αν $n = 3k + 1$, είναι

$$P(z) = z^{3k+1} - z - 1 = -1 \neq 0$$

• αν $n = 3k + 2$, είναι

$$P(z) = z^{3k+2} - z - 1 = z^2 - z - 1 = 2z^2 \neq 0.$$

Υποθέτουμε τώρα ότι υπάρχουν πολυώνυμα $f(x)$, $g(x)$ του $\mathbb{Z}[x]$, ώστε

$$P(x) = f(x)g(x).$$

Ας είναι $z_1, z_2, \dots, z_s$ οι ρίζες του $f(x)$. Προφανώς αυτές είναι και ρίζες του $P(x)$ και μάλιστα απλές, αφού δεν ικανοποιούν το σύστημα $P(x) = P'(x) = 0$. Χρειαζόμαστε το ακόλουθο

ΛΗΜΜΑ. Κάθε ρίζα z του $P(x)$ ικανοποιεί τη σχέση

$$2\Re\left(z - \frac{1}{z}\right) > \frac{1}{|z|^2} - 1.$$

ΑΠΟΔΕΙΞΗ ΤΟΥ ΛΗΜΜΑΤΟΣ. Πράγματι, αν

$$z = r(\cos t + i \sin t),$$

είναι

$$\Re\left(z - \frac{1}{z}\right) = \frac{r^2 - 1}{r} \cos t,$$

οπότε έχουμε να αποδείξουμε ότι

$$2\frac{r^2 - 1}{r} \cos t > \frac{1}{r^2} - 1 \Leftrightarrow$$

$$(r^2 - 1)(1 + 2r \cos t) > 0. *$$

Είναι όμως

$$r^{2n} = |z|^{2n} = |z + 1|^2 = 1 + 2r \cos t + r^2,$$

άρα

$$1 + 2r \cos t = r^{2n} - r^2.$$

Τότε η (*) γίνεται

$$(r^2 - 1)(r^{2n} - r^2) > 0,$$

η οποία φανερά ισχύει. Τώρα, από το λήμμα έχουμε

$$2\Re \sum_{j=1}^s \left(z_j - \frac{1}{z_j}\right) = \sum_{j=1}^s 2\Re \left(z_j - \frac{1}{z_j}\right) >$$

$$\sum_{j=1}^s \left(\frac{1}{|z_j|^2} - 1 \right) = \frac{1}{|z_1|^2} + \dots + \frac{1}{|z_s|^2} - s \geq 0,$$

με την τελευταία ανισότητα να είναι συνέπεια της ανισότητας Αριθμητικού Μέσου-Γεωμετρικού Μέσου και του γεγονότος ότι $|z_1 z_2 \dots z_s| = 1$, λόγω των τύπων Vieta. Άρα

$$l := \Re \sum_{j=1}^s \left(z_j - \frac{1}{z_j} \right) > 0.$$

Όμως, το $f(x)$ είναι μονικό, και επομένως από τους τύπους Vieta ο αριθμός l είναι ακέραιος. Επομένως ισχύει $l \geq 1$. Κάνοντας την ίδια διαδικασία με τις ρίζες του $g(x)$, λαμβάνουμε

$$\Re \sum_{j=s+1}^n \left(z_j - \frac{1}{z_j} \right) \geq 1.$$

Επομένως είναι

$$\Re \sum_{j=1}^n \left(z_j - \frac{1}{z_j} \right) \geq 2.$$

Όμως είναι από τους τύπους Vieta

$$\Re \sum_{j=1}^n \left(z_j - \frac{1}{z_j} \right) = 1.$$

8 Μερικά προβλήματα σχετικά με ανάγωγα πολυώνυμα

1. Έστω $p > 2$ ένας πρώτος και το πολυώνυμο

$$f(x) = x^p - x + p.$$

1. Να αποδείξετε ότι όλες οι ρίζες του f έχουν μέτρο μικρότερο από $p^{\frac{1}{p-1}}$.

2. Να αποδείξετε ότι το πολυώνυμο είναι ανάγωγο.

ΑΠΟΔΕΙΞΗ. α) Έστω $a \in \mathbb{C}$ ρίζα του $f(x)$. Ισχύει

$$|a|^p - |a| \leq |a^p - a| = p.$$

Έστω $|a| \geq p^{\frac{1}{p-1}}$.

Τότε έχουμε

$$|a|^p - |a| \geq p^{\frac{p}{p-1}} - p^{\frac{1}{p-1}} = (p-1)p^{\frac{1}{p-1}},$$

αφού η συνάρτηση $x^p - x$ είναι γνησίως αύξουσα στο διάστημα $\left(\frac{1}{p^{1/(p-1)}}, +\infty \right)$. Επομένως έχουμε

$$|a|^p - |a| > p,$$

αφού

$$(p-1)p^{\frac{1}{p-1}} > p \Leftrightarrow$$

$$(p-1)^{p-1} > p^{p-2} \Rightarrow$$

$$g(p-1) > g(p),$$

όπου

$$g(x) = \frac{\ln x}{x-1}, \quad x > 1$$

και η g είναι γνησίως φθίνουσα συνάρτηση.

β) Υποθέτουμε ότι υπάρχουν πολυώνυμα $A(x), B(x)$ στο $\mathbb{Z}[x]$, ώστε να ισχύει

$$f(x) = A(x)B(x).$$

Ένα εκ των A, B έχει σταθερό όρο το p ή το $-p$. Ας θέσουμε

$$A(x) = a_k x^k + \dots + a_1 x \pm p.$$

Επειδή κάθε ρίζα r_j του $A(x)$ είναι και ρίζα του $f(x)$, Λόγω του ερωτήματος α) θα ισχύει

$$|r_j| \leq p^{\frac{1}{p-1}}.$$

Όμως από τους τύπους Vieta είναι

$$|r_1 r_2 \dots r_k| = p,$$

άρα προκύπτει

$$p = |r_1| |r_2| \dots |r_k| < p^{\frac{k}{p-1}} \Rightarrow$$

$$p-1 < k \Rightarrow$$

$$k \geq p.$$

Οδηγηθήκαμε σε άτοπο, άρα το πολυώνυμο $f(x)$ είναι ανάγωγο.

2. Έστω ακέραιος $n > 1$ και το πολυώνυμο

$$f(x) = x^n + 5x^{n-1} + 3.$$

Να δοθεί μια καινούρια απόδειξη ότι το πολυώνυμο είναι ανάγωγο υπεράνω του $\mathbb{Z}$.

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι υπάρχουν πολυώνυμα $g(x), h(x) \in \mathbb{Z}[x]$, ώστε να ισχύει

$$f(x) = g(x)h(x)$$

και $\deg g, \deg h \geq 1$. Είναι $g(0)h(0) = f(0) = 3$, οπότε, χωρίς βλάβη της γενικότητας, ας είναι $|g(0)| = 1$. Ας είναι ακόμα

$$g(x) = (x - r_1)(x - r_2) \dots (x - r_k),$$

οπότε

$$|r_1 r_2 \dots r_k| = |g(0)| = 1.$$

Επειδή κάθε ρίζα του g είναι και ρίζα του f , ισχύει

$$r_i^n + 5r_i^{n-1} = -3,$$

άρα

$$|r_i|^{n-1} |r_i + 5| = 3,$$

για κάθε $i = 1, 2, \dots, k$. Πολλαπλασιάζοντας τις k αυτές ισότητες προκύπτει

$$|(r_1 + 5)(r_2 + 5) \cdots (r_k + 5)| = 3^k,$$

άρα ισχύει $|g(-5)| = 3^k$.

Όμως:

$$f(-5) = g(-5)h(-5) \Rightarrow$$

$$|g(-5)||h(-5)| = 3 \Rightarrow$$

$$3^k |h(-5)| = 3.$$

Άρα $k = 1$, οπότε $\deg g(x) = 1$. Δηλαδή το $f(x)$ έχει πρωτοβάθμιο παράγοντα, άρα ακέραια ρίζα. Αυτό όμως δεν συμβαίνει. Άρα το $f(x)$ είναι ανάγωγο υπεράνω του $\mathbb{Z}$.

3. Να αποδείξετε ότι το πολυώνυμο

$$f(x) = (x^2 + 1^2)(x^2 + 2^2) \cdots (x^2 + n^2) + 1$$

είναι ανάγωγο υπεράνω του $\mathbb{Z}$.

ΑΠΟΔΕΙΞΗ. Το ζητούμενο φανερά ισχύει όταν $n = 1$. Ας είναι λοιπόν $n \geq 2$. Υποθέτουμε ότι

$$f(x) = g(x)h(x),$$

με $g(x), h(x) \in \mathbb{Z}[x]$. Θέτουμε

$$g(x) = a_l x^l + \dots + a_1 x + a_0$$

και

$$h(x) = b_l' x^{l'} + \dots + b_1 x + b_0.$$

Παρατηρούμε ότι

$$1 = f(mi) = g(mi)h(mi),$$

για κάθε $m = \pm 1, \pm 2, \dots, \pm n$. Επειδή $g(x) \in \mathbb{Z}[x]$, θα ισχύει $g(mi) = 1, -1, i, -i$. Επίσης είναι

$$g(mi) = (a_0 - a_2 m^2 + a_4 m^4 - \dots) +$$

$$m(a_1 - a_3 m^2 + a_5 m^4 - \dots)i,$$

επομένως $g(mi) = \pm 1$ για $m \neq \pm 1$. Άρα

$$g(mi) = h(mi) = \pm 1,$$

για $m \neq \pm 1$. Τότε είναι

$$g(x) - h(x) = (x^2 + 2^2)(x^2 + 3^2) \cdots (x^2 + n^2)Q(x),$$

όπου $Q(x) \in \mathbb{Z}[x]$ και $\deg Q(x) \leq 1$. Τότε είναι

$$2 \geq |g(i) - h(i)| = (-1 + 2^2)(-1 + 3^2) \cdots (-1 + n^2)|Q(i)|,$$

επομένως ισχύει $Q(i) = 0$. Επειδή $Q(x) \in \mathbb{Z}[x]$, προκύπτει $Q(x) = 0$, οπότε $g(x) = h(x)$ και άρα $f(x) = g^2(x)$. Τότε

$$g^2(0) = f(0) \Rightarrow a_0^2 = (n!)^2 + 1,$$

που είναι αδύνατο.

4. Έστω $f(x) \in \mathbb{Z}[x]$ ανάγωγο πολυώνυμο υπεράνω του $\mathbb{Z}$ και το $|f(0)|$ δεν είναι τετράγωνο ακέραιου. Αν το $f(x)$ είναι μονικό, να αποδείξετε ότι το πολυώνυμο $f(x^2)$ είναι ανάγωγο υπεράνω του $\mathbb{Z}$.

ΑΠΟΔΕΙΞΗ. Ας είναι $\deg f = n$. Ας υποθέσουμε ότι υπάρχουν πολυώνυμα $R_1(x), R_2(x) \in \mathbb{Z}[x]$ με $\deg R_1, \deg R_2 \leq 2n - 1$, ώστε

$$Q(x) = f(x^2) = R_1(x)R_2(x).$$

Τότε είναι

$$Q(-x) = f(x^2) = R_1(-x)R_2(-x),$$

οπότε $Q(-x) = Q(x)$ για κάθε x . Ας είναι

$$F(x) = \gcd(R_1(x), R_1(-x)).$$

Επειδή είναι $F(-x) = F(x)$, υπάρχει πολυώνυμο $G(x)$, ώστε $F(x) = G(x^2)$ και $\deg G \leq n - 1$. Επειδή ακόμα είναι $G(x^2) | f(x^2)$, ισχύει $G(x) | f(x)$. Όμως το $f(x)$ είναι ανάγωγο, επομένως το $G(x)$ είναι σταθερό πολυώνυμο. Για τον ίδιο λόγο, και το $\gcd(R_2(x), R_2(-x))$ είναι σταθερό πολυώνυμο. Επομένως ισχύει $R_1(-x) | R_2(x)$ και $R_2(x) | R_1(-x)$. Άρα ισχύει $\deg R_1 = \deg R_2 = n$ και $R_2(x) = cR_1(-x)$, οπότε $Q(x) = cR_1(x)R_1(-x)$. Επειδή το $f(x)$ είναι μονικό, είναι $c = (-1)^n$ και $Q(0) = (-1)^n R_1^2(0)$, δηλαδή το $|f(0)|$ είναι τετράγωνο ακέραιου. Άτοπο! Επομένως το $f(x^2)$ είναι ανάγωγο υπεράνω του $\mathbb{Z}$.

5. Να αποδείξετε ότι το πολυώνυμο

$$P(x) = (x^2 - 8x + 25)(x^2 - 16x + 100) \cdots$$

$$(x^2 - 8nx + 25n^2) + 1, n \in \mathbb{N}^*$$

είναι ανάγωγο υπεράνω του $\mathbb{Z}$.

ΑΠΟΔΕΙΞΗ. Υποθέτουμε ότι ισχύει

$$P(x) = Q(x)R(x),$$

όπου

$$Q(x) = a_k x^k + \dots + a_1 x + a_0$$

και

$$R(x) = b_l x^l + \dots + b_1 x + b_0$$

με

$$a_j, b_i \in \mathbb{Z}, j = 0, 1, 2, \dots, k, i = 0, 1, 2, \dots, l, a_k b_l \neq 0$$

και $1 \leq k < 2n, 1 \leq l < 2n, k + l = 2n$. Ονομάζουμε

$$x_{\pm m} = 4m \pm 3mi, m = 1, 2, \dots, n$$

και παρατηρούμε ότι

$$P(x_{\pm m}) = 1 \Leftrightarrow Q(x_{\pm m})R(x_{\pm m}) = 1$$

και επειδή $Q(x_{\pm m}), R(x_{\pm m}) \in \mathbb{Z}$ είναι

Βιβλιογραφία

$$Q(x_{\pm m}) = R(x_{\pm m}) = 1 \text{ ή}$$

$$Q(x_{\pm m}) = R(x_{\pm m}) = -1 \text{ ή}$$

$$Q(x_{\pm m}) = -R(x_{\pm m}) = i \text{ ή}$$

$$Q(x_{\pm m}) = -R(x_{\pm m}) = -i.$$

Επίσης παρατηρούμε ότι

$$Q(x_{\pm m}) = Q(4m \pm 3mi) = \sum_{j=0}^k a_j (4m \pm 3mi)^j,$$

επομένως το φανταστικό μέρος του $Q(x_{\pm m})$ είναι πολλαπλάσιο του $3m$, άρα $Q(x_{\pm m}) \neq \pm i$. Το ίδιο συμπέρασμα ισχύει και για το $R(x_{\pm m})$. Συνεπώς είναι

$$Q(x_{\pm m}) = R(x_{\pm m}) = 1 \text{ ή}$$

$$Q(x_{\pm m}) = R(x_{\pm m}) = -1.$$

Θεωρούμε το πολυώνυμο $f(x) = Q(x) - R(x)$. Από τα προηγούμενα προκύπτει ότι οι $2n$ αριθμοί

$$x_{\pm m} = 4m \pm 3mi, m = 1, 2, \dots, n$$

είναι ρίζες του $f(x)$. Όμως $\deg f(x) \leq 2n - 1$, άρα $f(x) = 0$, οπότε $Q(x) = R(x)$ και είναι τελικά

$$P(x) = Q^2(x).$$

Θέτοντας σε αυτήν $x = 0$ λαμβάνουμε $a_0^2 = (5^n n!)^2 + 1$, που είναι αδύνατο.

1. M. BECHEANU-B. ENESCU *Balkan Mathematical Olympiads 1984-2006*, GIL, 2007
2. BRILLHART ET AL. *On an irreducibility theorem of A. Cohn*. Can. J. Math., Vol. XXXIII, No. 5, 1981, pp. 1055-1059
3. D. COX *Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it*. Amer. Math. Monthly 118 (2011), p.p. 3-21
4. A. T. JONASSEN *On the irreducibility of the trinomials $x^m \pm x^n \pm 4$* . Math. Scand. 21, 1967, 177-189.
5. SERGE LANG *Algebra* Springer, 2005
6. W. LJUNGGREN *On the irreducibility of certain trinomials and quadrimomials*. Math. Scand. 8, 1960, 65-70.
7. RAM MURTY *Prime numbers and irreducible polynomials*. Amer. Math. Monthly, Vol. 109, no. 5, 2002, 452-458.
8. L. PANAITOPOL *Criteriul lui Perron de ireductibilitate a polinoamelor cu coeficienti intregi*. Gaz. Mat. vol. XCVIII no. 10, 1993, 339-340.
9. G. PÓLYA G. SZEGŐ *Problems and Theorems in Analysis II*. Springer, 1976
10. V. PRASOLOV *Polynomials* Springer, 2004
11. E. SELMER *On the irreducibility of certain trinomials* Math. Scandinavica 4, 1956, 287-302.

ΣΥΝΤΑΚΤΙΚΗ ΕΠΙΤΡΟΠΗ

ΙΩΑΝΝΗΣ ΘΩΜΑΪΔΗΣ, Δρ Μαθηματικών Παν. Θεσσαλονίκης, τ. Σχολικός Σύμβουλος Μαθηματικών
 ΑΘΑΝΑΣΙΟΣ ΜΑΓΚΟΣ, Δρ Μαθηματικών Παν. Θεσσαλονίκης, Πειραματικό Γυμνάσιο Πανεπιστημίου Μακεδονίας
 ΝΙΚΟΛΑΟΣ ΜΑΥΡΟΓΙΑΝΝΗΣ, Δρ Μαθηματικών Παν. Αθηνών, Σύμβουλος Α' στο Ινστιτούτο Εκπαιδευτικής Πολιτικής
 ΕΤΑΓΓΕΛΟΣ ΜΟΥΤΡΟΥΚΟΣ, Δρ Μαθηματικών Παν. Chicago, Μουσικό Σχολείο Αγρινίου
 ΣΙΛΟΥΑΝΟΣ ΜΠΡΑΖΙΤΙΚΟΣ, Δρ Μαθηματικών Μαθηματικών Παν. Αθηνών, Postdoctoral Fellow, University of Edinburgh
 ΜΙΧΑΗΛ ΠΑΠΑΔΗΜΗΤΡΑΚΗΣ, Δρ Μαθηματικών Παν. California, Los Angeles, Καθηγητής Τμήματος Μαθηματικών & Εφαρμοσμένων Μαθηματικών Παν. Κρήτης
 ΣΤΑΥΡΟΣ ΠΑΠΑΔΟΠΟΥΛΟΣ, Δρ Μαθηματικών Παν. Κρήτης, Ιδιωτική Εκπαίδευση, Χαλκίδα
 ΑΧΙΛΛΕΑΣ ΣΥΝΕΦΑΚΟΠΟΥΛΟΣ, Δρ Μαθηματικών Παν. Cornell, Εκπαιδευτήρια Ράππου, Λάρισα
 ΔΗΜΗΤΡΙΟΣ ΧΕΛΙΩΤΗΣ, Δρ Μαθηματικών Παν. Stanford, Αναπληρωτής Καθηγητής Τμήματος Μαθηματικών Παν. Αθηνών
 ΔΗΜΗΤΡΙΟΣ ΧΡΙΣΤΟΦΙΔΗΣ, Δρ Μαθηματικών Παν. Cambridge, Assistant Professor in Mathematics, UCLan Cyprus