Κεφάλαιο 6: Απομόνωση και προσέγγιση πραγματικών ριζών πολυωνυμικών εξισώσεων

Μέθοδοι για την εύρεση των πραγματικών ριζών — ή για την επίλυση — πολυωνυμικών εξισώσεων, οποιουδήποτε βαθμού, στον δακτύλιο $\mathbb{Z}[x]$ περιγράφονται στα βιβλία Αριθμητικής Ανάλυσης και Θεωρίας Εξισώσεων. Η παρουσίασή μας του θέματος αυτού διαφέρει σε τρία σημαντικά σημεία:

- Ακολουθώντας την "Γαλλική μαθηματική σχολή" κάνουμε διάκριση ανάμεσα στην **απομόνωση** και **προσέγγιση** των ριζών. Αντίθετα, στο μεγαλύτερο μέρος της βιβλιογραφίας ακολουθείται η "Αγγλική μαθηματική σχολή" όπου η προσέγγιση των ριζών ισοδυναμεί με την λύση των εξισώσεων.

- Διατυπώνουμε με ακρίβεια τα θεωρήματα των Budan (1807) και Fourier (1820) που δίνουν ένα **πάνω φράγμα** (upper bound) στον αριθμό των πραγματικών ριζών που έχει μία πολυωνυμική εξίσωση σε τυχαίο ανοικτό διάστημα (ℓ, r). Βλέπε και το Figure 6.1. Τονίζουμε πως η διατύπωση του θεωρήματος του Budan δύσκολα βρίσκεται στην βιβλιογραφία διότι αντ' αυτής υπάρχει η διατύπωση του θεωρήματος του Fourier. Το τελευταίο μάλιστα συχνά ονομάζεται θεώρημα του Budan ή και θεώρημα των Budan-Fourier.

- Παρουσιάζουμε το θεώρημα του A.J.H. Vincent του 1836, με την βοήθεια του οποίου αναπτύσσονται δύο μέθοδοι απομόνωσης των πραγματικών ριζών πολυωνυμικών εξισώσεων με συνεχή κλάσματα. Η πρώτη μέθοδος ανήκει στον Vincent (1836) αλλά έχει εκθετικό χρόνο υπολογισμού. Η δεύτερη μέθοδος ανήκει στον γράφοντα — αναπτύχθηκε το 1978 και βελτιώθηκε με τον Strzebonski το 1994 — και όχι μόνο έχει πολυωνυμικό χρόνο υπολογισμού αλλά είναι και η **ταχύτερη μέθοδος απομόνωσης που υπάρχει**. Το θεώρημα του Vincent είχε τόσο πολύ ξεχαστεί ώστε ακόμα και η *Enzyclopaedie der mathematischen Wissenschaften* το αγνοεί.

Τονίζουμε πως και ο ίδιος ο Vincent είχε τόσο ξεχαστεί ώστε το μικρό του όνομα αρχικά αποδόθηκε σαν M., επειδή το Γαλλικό μαθηματικό περιοδικό στο οποίο δημοσιεύθηκε η εργασία του τον ανέφερε σαν M. Vincent. Πολύ αργότερα και ύστερα από υπόδειξη κατάλαβε ο γράφων ότι το M. ήταν για την

Γαλλική λέξη "κύριος" ενώ στην πραγματικότητα ο Vincent είχε τρία μικρά ονόματα Alexandre Joseph Hidulf ???.

Στην συνέχεια θα εξετάσουμε λεπτομερώς τις δύο κλασσικές μεθόδους για την απομόνωση των πραγματικών ριζών πολυωνυμικών εξισώσεων με ακέραιους συντελεστές, δηλαδή την μέθοδο της ***διχοτόμησης***, Sturm (1829), και την μέθοδο των ***συνεχών κλασμάτων* (σ.κ.)**, Vincent - Akritas - Strzebonski (1836, 1978, 1994).

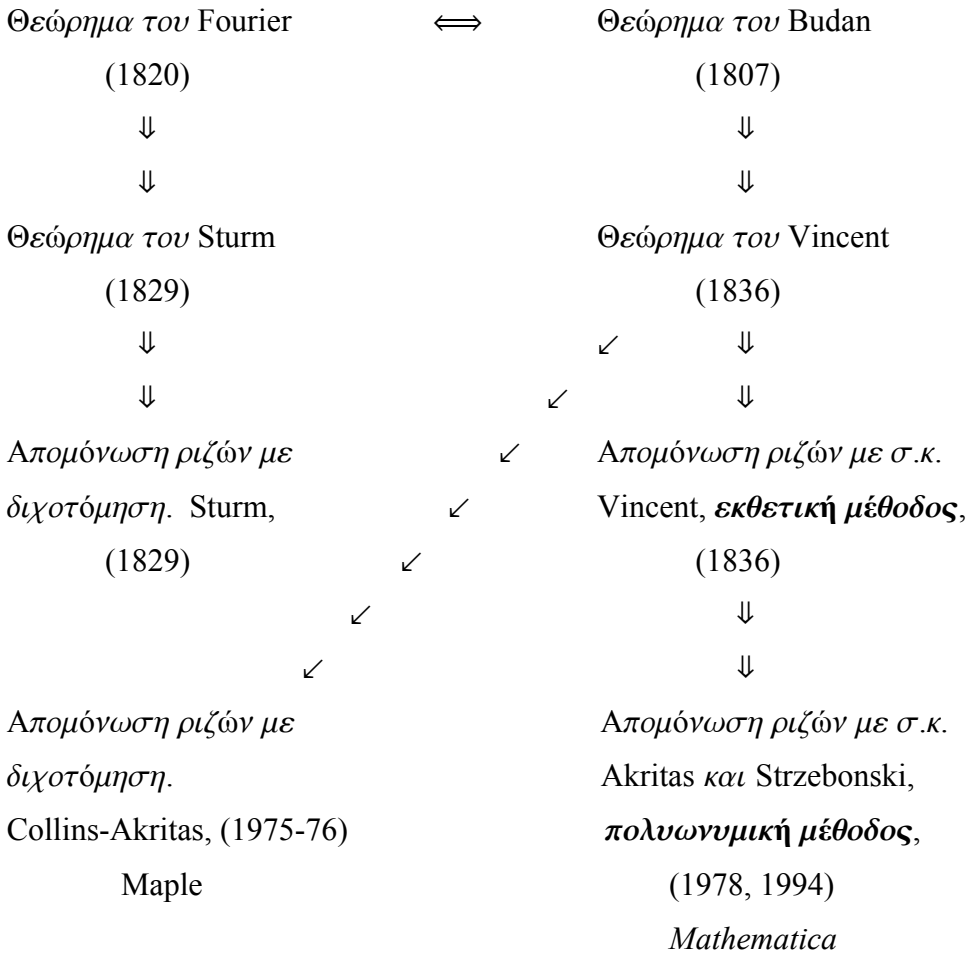


Figure 6.1. Τα θεωρήματα των Budan και Fourier και οι δύο κλασσικές μέθοδοι απομόνωσης των πραγματικών ριζών πολυωνυμικών εξισώσεων. Η μέθοδος των Collins-Akritas βασίζεται σε μία ολική τροποποίηση του θεωρήματος του Vincent, δεν θεωρείται κλασσική και δεν καλύπτεται στο βιβλίο αυτό.

6.1 Ιστορική ανασκόπηση και βασικές έννοιες

Τα αρχαιότερα δείγματα αλγεβρικών εξισώσεων εμφανίζονται το 1700 ή 1650 π.Χ. στον πάπυρο Rhind, στον οποίο ο Αιγύπτιος Ahmes περιέλαβε και παλαιότερες εργασίες. Βρίσκουμε για παράδειγμα το εξής πρόβλημα: "Μία ποσότητα μαζί με το έβδομό της κάνουν 19. Ποια είναι η ποσότητα;" Προφανώς, το πρόβλημα είναι να λύσουμε την εξίσωση $x + (\frac{1}{7})x = 19$, όπως θα λέγαμε σήμερα. Λόγω έλλειψης κατάλληλου αλγεβρικού συμβολισμού οι Αιγύπτιοι έλυναν παρόμοιες εξισώσεις με έναν πολύπλοκο τρόπο που αργότερα έγινε γνωστός σαν μέθοδος της "λάθους θέσης."

Αν και μερικοί υποστηρίζουν πως οι Έλληνες έλυσαν εξισώσεις δευτέρου βαθμού, εν γένει ούτε οι Αιγύπτιοι ούτε οι Έλληνες δεν έκαναν καμία σημαντική πρόοδο. Οι Άραβες πέτυχαν περισσότερα, αλλά μόνο την εποχή της Αναγέννησης σημειώθηκε αξιοσημείωτη πρόοδος, όταν οι Ιταλοί μαθηματικοί του δέκατου πέμπτου και δέκατου έκτου αιώνα (Tartaglia, Cardano και Ferrari) πέτυχαν να λύσουν με ριζικά τις γενικές εξισώσεις ***τρίτου*** και ***τετάρτου*** βαθμού. Στο ***βιβλίο του* Dunham** περιγράφεται με ενδιαφέρον η διαμάχη, μεταξύ των Tartaglia και Cardano, για την προτεραιότητα της ανακάλυψης.

Τον δέκατο έβδομο και δέκατο όγδοο αιώνα έγιναν πολλές προσπάθειες για την επίλυση της γενικής εξίσωσης ***πέμπτου*** βαθμού. Με τις προσπάθειες αυτές αποκτήθηκε μια βαθύτερη κατανόηση της "φύσης" των ριζών των αλγεβρικών εξισώσεων (ειδικά με την εργασία των Cardano και Descartes), αλλά παρ' όλα αυτά κανένας δεν μπόρεσε να λύσει με ριζικά την εξίσωση πέμπτου βαθμού.

Επόμενο ήταν να αναρωτηθούν οι μαθηματικοί αν είναι δυνατή μια τέτοια λύση. Η απάντηση δόθηκε το 1804 από τον Paolo Ruffini, ο οποίος απέδειξε πως είναι αδύνατο να λυθεί η γενική εξίσωση πέμπτου βαθμού με ριζικά. Αργότερα, το 1826, ο Abel απέδειξε πως είναι αδύνατο να λυθούν με ριζικά γενικές αλγεβρικές εξισώσεις βαθμού μεγαλύτερου του 4.

Στις αρχές του δέκατου ένατου αιώνα η προσοχή των μαθηματικών είχε ήδη στραφεί στις ***αριθμητικές μεθόδους*** για την επίλυση πολυωνυμικών εξισώσεων με ακέραιους συντελεστές. Αυτή την περίοδο ο Fourier συνέλαβε

την ιδέα να "σπάσει" το πρόβλημα σε **δύο υποπροβλήματα:** δηλαδή πρώτα να **απομονώσει** τις ρίζες και έπειτα να τις **προσεγγίσει** με όση ακρίβεια επιθυμείται.

Απομόνωση (isolation) των πραγματικών ριζών μιας πολυωνυμικής εξίσωσης είναι η διαδικασία εύρεσης πραγματικών διαστημάτων, μη τεμνομένων μεταξύ τους, έτσι ώστε κάθε διάστημα περιέχει ακριβώς μία πραγματική ρίζα, και κάθε πραγματική ρίζα περιέχεται σε κάποιο διάστημα. Από την άλλη μεριά, **προσέγγιση** (approximation) είναι η διαδικασία σμίκρυνσης των διαστημάτων απομόνωσης τόσο, όσο να προσεγγισθούν οι ρίζες στον επιθυμητό βαθμό ακρίβειας.

Το πρόβλημα της απομόνωσης των ριζών ήταν το σημαντικότερο και τράβηξε την προσοχή των μαθηματικών. Με ξεκάθαρο τον σκοπό, ήρθε τώρα και η επιτυχία. Στις αρχές του δέκατου ένατου αιώνα ο F.D. Budan και ο J.B.J. Fourier παρουσίασαν δύο διαφορετικά (αλλά ισοδύναμα) θεωρήματα που μας επιτρέπουν να υπολογίσουμε τον **μέγιστο** δυνατό αριθμό πραγματικών ριζών που έχει μία εξίσωση με πραγματικούς συντελεστές μέσα σε ένα δεδομένο διάστημα.

Το θεώρημα του Budan δημοσιεύτηκε το 1807 στην εργασία "Nouvelle méthode pour la résolution des équations numériques", ενώ το θεώρημα του Fourier πρωτοδημοσιεύθηκε το 1820 στο "Le bulletin des sciences par la société philomatique de Paris." Εξ αιτίας της σημασίας των δύο αυτών θεωρημάτων δημιουργήθηκε μεγάλη έριδα σχετικά με την προτεραιότητα ανακάλυψης. Όπως μας πληροφορεί ο F. Arago στο βιβλίο του *Biographies of distinguished scientific men* (p. 383) ο Fourier "εθεώρησε απαραίτητο να λάβει βεβαιώσεις από τέως φοιτητές της Πολυτεχνικής Σχολής ή από καθηγητές του Πανεπιστημίου" για να αποδείξει ότι είχε διδάξει το θεώρημά του το 1796, 1797 και 1803.

Όπως θα δούμε στην ενότητα 6.2, βασιζόμενος στο θεώρημα του Fourier, ο C. Sturm παρουσίασε το 1829 ένα βελτιωμένο θεώρημα που μας επιτρέπει να υπολογίσουμε — με **διχοτόμηση** — τον **ακριβή** αριθμό των πραγματικών ριζών που έχει μία εξίσωση με ακέραιους συντελεστές μέσα σε ένα δεδομένο διάστημα. Έτσι ο Sturm είναι ο πρώτος που **έλυσε** το πρόβλημα της

απομόνωσης των πραγματικών ριζών και δικαιολογημένα έγινε παγκόσμια διάσημος.

Έτσι, *από το* 1830 *μέχρι το* 1978 *η μέθοδος του* Sturm *ήταν η μόνη ευρέως γνωστή και χρησιμοποιούμενη, με συνέπεια το θεώρημα του* Budan *να ξεχασθεί παντελώς — και μαζί του και το θεώρημα του* Vincent *που απορρέει από αυτό*. Απ' *ότι ξέρουμε, η διατύπωση του θεωρήματος του* Budan *μπορεί να βρεθεί μόνο στο άρθρο του* Vincent, 1836, *και στις εργασίες του συγγραφέα αυτού του μονογράμματος ενώ, σε αντίθεση, το θεώρημα του* Fourier *βρίσκεται σε όλα τα βιβλία τα σχετικά με την θεωρία των εξισώσεων*.

Στην *ενότητα* 6.3, *παρουσιάζουμε το θεώρημα του* Budan, *στο οποίο στηρίζεται το θεώρημα του* Vincent *του* 1836. Το *τελευταίο είναι η βάση της μεθόδου των* ***συνεχών κλασμάτων*** (Vincent-Akritas-Strzebonski) *για την απομόνωση των πραγματικών ριζών πολυωνυμικών εξισώσεων με ακέραιους συντελεστές, μιας μεθόδου κατά πολύ καλλίτερης της μεθόδου του* Sturm. Η *μέθοδος των συνεχών κλασμάτων είναι η πιο γρήγορη στον κόσμο και χρησιμοποιείται στο Mathematica*. Σε *αντίθεση η μέθοδος του* Sturm *δεν χρησιμοποιείται πουθενά πλέον*.

Το *θεώρημα του* Vincent *είχε τόσο πολύ ξεχαστεί ώστε προ του* 1978 *δεν αναφέρεται από κανέναν συγγραφέα με εξαίρεση τον* **Obreschkoff** (1963) *και* **Uspensky** (1948). Ο *γράφων ανακάλυψε το θεώρημα του* Vincent *στο βιβλίο του* Uspensky *το* 1975-76 *και στο θέμα αυτό έγραψε την διδακτορική του διατριβή* (1978).

Σημειώνουμε *παρενθετικά πως υπάρχει και η μέθοδος των* Collins-Akritas *για την απομόνωση των πραγματικών ριζών πολυωνυμικών εξισώσεων με* ***διχοτόμηση***. Η *μέθοδος αυτή αναπτύχθηκε το* 1975-76, *στηρίζεται σε μία ολική τροποποίηση του θεωρήματος του* Vincent *και χρησιμοποιείται στο* Maple.

Για *την ιστορία αναφέρουμε πως υπάρχει μια αναφορά του* Uspensky — *στην εισαγωγή του βιβλίου του* — *ότι ο ίδιος ανεκάλυψε την μέθοδο απομόνωσης πραγματικών ριζών με συνεχή κλάσματα*. Έτσι *λοιπόν, αρχικά, η μέθοδος του* Vincent *εσφαλμένα ονομαζόταν* "***μέθοδος του* Uspensky**" *ενώ η μέθοδος των* Collins-Akritas *ονομαζόταν* "***τροποποιημένη μέθοδος του* Uspensky**". Όμως

όπως τόνισε ο γράφων, ο Uspensky δεν είχε υπ' όψη του το θεώρημα του Budan και το μόνο που έκανε ήταν να διπλασιάσει τον χρόνο υπολογισμού της μεθόδου του Vincent. Λεπτομέρειες θα δούμε στην ενότητα 6.3.

6.2 Το *θεώρημα του* Fourier *και η μέθοδος του* Sturm *για την απομόνωση πραγματικών ριζών με διχοτόμηση*

Στην ενότητα αυτή θα γνωρίσουμε το θεώρημα του Fourier, το οποίο μας δίνει τον ***μέγιστο δυνατό*** πραγματικών ριζών που έχει μία εξίσωση με ακέραιους συντελεστές μέσα σε ένα διάστημα. Στην συνέχεια θα δούμε πως ο Sturm τροποποίησε το θεώρημα του Fourier ώστε να παίρνουμε τον ***ακριβή*** αριθμό των πραγματικών ριζών μέσα στο υπό εξέταση διάστημα.

■ 6.2.1 Το *θεώρημα του* Fourier

Το *θεώρημα του* Fourier *βασίζεται στην εργασία των* Cardano *και* Descartes *την οποία πρώτα παρουσιάζουμε*. Χρειαζόμαστε τον ακόλουθο ορισμό:

Ορισμός:
Έστω μία πεπερασμένη ή άπειρη ακολουθία πραγματικών αριθμών $c_1, c_2, c_3, \ldots$ Λέμε ότι ανάμεσα στους αριθμούς c_ℓ και c_r ($\ell < r$) υπάρχει μία ***μεταβολή προσήμου*** (sign variation) ή απλά ***μεταβολή*** όταν ισχύουν τα ακόλουθα:

i. Αν $r = \ell + 1$, οι αριθμοί c_ℓ και c_r έχουν αντίθετα πρόσημα.
ii. Αν $r \geq \ell + 2$, οι αριθμοί $c_{\ell+1}, \ldots, c_{r-1}$ είναι όλοι μηδέν και οι c_ℓ και c_r έχουν αντίθετα πρόσημα.

Ακολουθεί ένα πρόγραμμα στο *Mathematica* για τον υπολογισμό των μεταβολών προσήμου τόσο μιας αριθμητικής ακολουθίας όσο και ενός πολυωνύμου μιας μεταβλητής.

```
variations[s_] := Module[{lis, l, i, v = 0},
   If[PolynomialQ[s, Variables[s]],
    lis = Select[CoefficientList[s, Variables[s]], # ≠ 0 &],
    lis = Select[s, # ≠ 0 &]];
   l = Length[lis];
   If[l > 1,
    Do[If[Not[Equal[Sign[lis[[i]]], Sign[ lis[[i + 1]]]]], v++],
     {i, l - 1}]];
   v] /; ListQ[s] || Which[Length[Variables[s]] == 0,
    AtomQ[Variables[s]], Length[Variables[s]] == 1,
    AtomQ[First[Variables[s]]]]
```

Παράδειγμα:
Έστω το πολυώνυμο $p(x) = x^3 - 7x + 7$, οι συντελεστές του οποίου σχηματίζουν την πεπερασμένη ακολουθία $\{1, 0, -7, 7\}$. Στην ακολουθία αυτή υπάρχουν 2 μεταβολές προσήμου. Πράγματι,

```
variations[x^3 - 7 x + 7]
2
```

Ο Gerolamo Cardano (1501-1576) είναι ο πρώτος στην ιστορία των μαθηματικών που σύνδεσε τον **αριθμό ρ_+ των θετικών ριζών** ενός πολυωνύμου $p(x)$ με τον **αριθμό ν των μεταβολών προσήμου** στην ακολουθία των συντελεστών του $p(x)$.

Συγκεκριμένα ο Cardano ήξερε τις εξής δύο περιπτώσεις:

- αν στους συντελεστές ενός πολυωνύμου δεν υπάρχει **καμία** μεταβολή προσήμου, δηλαδή $\nu = 0$, τότε δεν υπάρχει **καμία** θετική ρίζα, δηλαδή $\rho_+ = 0$, και
- αν στους συντελεστές ενός πολυωνύμου υπάρχει **μία** μεταβολή προσήμου, δηλαδή $\nu = 1$, τότε υπάρχει **μία** θετική ρίζα, δηλαδή $\rho_+ = 1$.

Οι περιπτώσεις αυτές όσο και αν φαίνονται απλές χρησιμοποιούνται — όπως θα δούμε στην ενότητα 6.3 — σαν κριτήριο τερματισμού στην πιο γρήγορη μέθοδο απομόνωσης πραγματικών ριζών — αυτή με συνεχή κλάσματα. Επίσης χρησιμοποιούνται και σαν κριτήριο τερματισμού στην μέθοδο των Collins-Akritas.

Παράδειγμα:
Έτσι για παράδειγμα το πολυώνυμο $p(x) = x^3 + 7x + 7$, δεν έχει καμία θετική ρίζα, ενώ το πολυώνυμο $p(x) = x^3 - 7x - 7$, έχει μία θετική ρίζα.

Αυτό που έκανε ο René Descartes (1596-1650) ήταν να γενικεύσει το "θεώρημα" του Cardano. Συγκεκριμένα, στον Descartes οφείλουμε την σχέση $\nu = \rho_+ + 2\lambda$, όπου $\lambda \in \mathbb{Z}_{\geq 0}$, την οποία θα αποδείξουμε πιο κάτω με την βοήθεια του θεωρήματος του Fourier.

Όπως *αναφέραμε στην προηγούμενη ενότητα, το θεώρημα του* Fourier *δημοσιεύθηκε το* 1820 *και βρίσκεται σε όλα τα βιβλία τα σχετικά με την θεωρία των εξισώσεων είτε με το όνομα* Budan - Fourier *είτε μόνο με το όνομα* Budan. *Προτού το διατυπώσουμε θα παρουσιάσουμε δύο βοηθητικά λήμματα. Αν και ενδιαφερόμαστε μόνο για πολυώνυμα με ακέραιους συντελεστές θα αποδείξουμε τα λήμματα αυτά στην γενικότερη περίπτωση με πραγματικούς συντελεστές.*

Λήμμα 6.2.1:
Έστω ότι $p(x) = 0$ *είναι μία πολυωνυμική εξίσωση βαθμού* $n > 0$ *με πραγματικούς συντελεστές και έστω ότι έχει μία πραγματική ρίζα* α *πολλαπλότητας* m. *Τότε για* $\epsilon > 0$ *τα πολυώνυμα* $p(x)$ *και* $p^{(1)}(x)$ — *όπου εν γένει* $p^{(i)}(x)$ *είναι η* i*-στή παράγωγος του* $p(x)$ — *έχουν* ***αντίθετα*** *πρόσημα στο διάστημα* $(\alpha - \epsilon, \alpha)$ *και* ***ίδια*** *πρόσημα στο διάστημα* $(\alpha, \alpha + \epsilon)$.

Απόδειξη:
Εφαρμόζουμε το ανάπτυγμα κατά Taylor, *δηλαδή*

$$p(\alpha \pm x) = \sum_{i=0}^{n} \frac{p^{(i)}(\alpha)}{i!}\, x^i.$$

Τότε λόγω της πολλαπλότητας m *της ρίζας* α, *έχουμε*

$$p(\alpha \pm \epsilon) = \sum_{i=m}^{n} \frac{p^{(i)}(\alpha)}{i!}\, (\pm\epsilon)^i = \frac{p^{(m)}(\alpha)}{m!}\, (\pm\epsilon)^m + \cdots + \frac{p^{(n)}(\alpha)}{n!}\, (\pm\epsilon)^n$$

και

$$p^{(1)}(\alpha \pm \epsilon) = \sum_{i=m}^{n} \frac{p^{(i)}(\alpha)}{(i-1)!}\, (\pm\epsilon)^{i-1} = \frac{p^{(m)}(\alpha)}{(m-1)!}\, (\pm\epsilon)^{m-1} + \cdots + \frac{p^{(n)}(\alpha)}{(n-1)!}\, (\pm\epsilon)^{n-1}$$

Βλέπουμε όμως πως για ϵ *αρκετά μικρό τα πρόσημα στις δύο τελευταίες εξισώσεις εξαρτώνται μόνο από το πρόσημο του όρου* $p^{(m)}(\alpha)$ — *του πρώτου όρου που δεν έχει ρίζα το* α — *και συνεπώς είναι αντίθετα στο διάστημα* $(\alpha - \epsilon, \alpha)$ *και ίδια στο διάστημα* $(\alpha, \alpha + \epsilon)$.//

Παράδειγμα:
Έστω $p(x)$ *το ακόλουθο πολυώνυμο που έχει την ρίζα* $\alpha = 2$, *πολλαπλότητας* 4.

```
p[x_] := (x^3 - 7 x + 7) (x - 2)^4 // Expand
```

Για $\epsilon = 0.025$, από τα γραφήματα των $p(x)$ και $p^{(1)}(x)$, βλέπουμε πως τα πρόσημα είναι αντίθετα στο διάστημα $(2 - \epsilon, 2)$ και ίδια στο διάστημα $(2, 2 + \epsilon)$. (Το γράφημα της $p^{(1)}(x)$ είναι με **διακεκομμένη γραμμή**.)

```
ϵ = 0.025;
plot0 = Plot[{p[x]}, {x, 2 - ϵ, 2 + ϵ},
   AxesOrigin → {2, 0}, DisplayFunction :→ Identity];

plot1 = Plot[{p'[x]}, {x, 2 - ϵ, 2 + ϵ}, AxesOrigin → {2, 0},
  PlotStyle → {Dashing[{0.05,0.05}]}, DisplayFunction :→ Identity];

Show[{plot0, plot1}, DisplayFunction :→ $DisplayFunction];
```

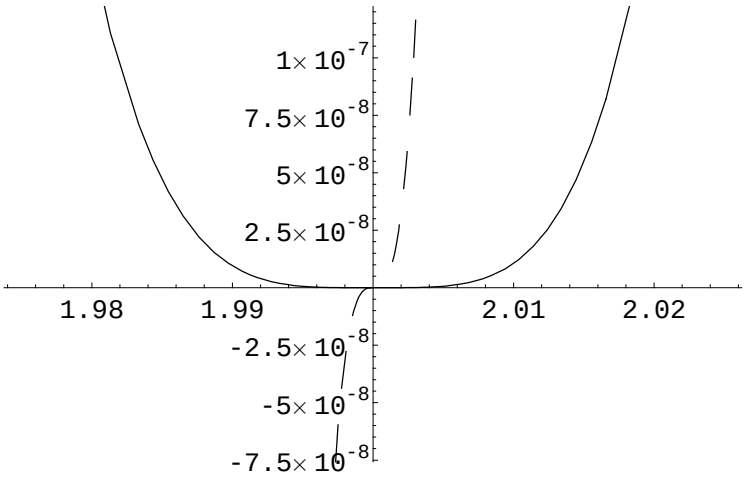


Figure 6.2. Τα γραφήματα της $p(x)$ και της παραγώγου της $p^{(1)}(x)$ (με διακεκομμένη γραμμή). Στο διάστημα $(2 - \epsilon, 2)$ τα πρόσημα των $p(x)$ και $p^{(1)}(x)$ είναι αντίθετα ενώ στο διάστημα $(2, 2 + \epsilon)$ τα πρόσημα είναι ίδια.

Λήμμα 6.2.2:

Έστω πάλι ότι $p(x) = 0$ *είναι μία πολυωνυμική εξίσωση βαθμού* $n > 0$ *με πραγματικούς συντελεστές και έστω ότι έχει μία πραγματική ρίζα* α *πολλαπλότητας* $m > 1$. *Θεωρούμε τα* m *πολυώνυμα* $p(x)$, $p^{(1)}(x)$, …, $p^{(m-1)}(x)$ *όπου και πάλι το* $p^{(i)}(x)$ *συμβολίζει την i-στή παράγωγο του* $p(x)$. *Τότε για* $\epsilon > 0$, *αν στα m πολυώνυμα αντικαταστήσουμε την μεταβλητή x με τιμές από το διάστημα* $(\alpha - \epsilon, \alpha)$ *τα πρόσημα της αριθμητικής ακολουθίας που προκύπτει είναι* ***εναλασσόμενα***, *ενώ αν αντικαταστήσουμε την μεταβλητή x με τιμές από το διάστημα* $(\alpha, \alpha + \epsilon)$ *τα πρόσημα της αριθμητικής ακολουθίας που προκύπτει* ***συμπίπτουν*** *με το πρόσημο του* $p^{(m)}(\alpha)$, *όπου* $p^{(m)}(x)$ *είναι η πρώτη συνάρτηση για την οποία το α δεν είναι ρίζα*.

Απόδειξη:

Εφαρμόζουμε επαναληπτικά το Λήμμα 6.2.1.//

Παράδειγμα (συνέχεια):

Συνεχίζουμε με τα γραφήματα των επόμενων μερικών παραγώγων του $p(x)$. *Κάθε ένα γράφημα το συγκρίνουμε με το γράφημα της προήγουμενης παραγώγου και βλέπουμε πως στο διάστημα* $(\alpha - \epsilon, \alpha)$ *τα πρόσημα είναι αντίθετα, ενώ στο διάστημα* $(\alpha, \alpha + \epsilon)$ *τα πρόσημα είναι ίδια*. *Τα γραφήματα της* ***πρώτης*** *και* ***τρίτης*** *παραγώγου είναι με* ***διακεκομμένες γραμμές***.

```
plot2 = Plot[p''[x], {x, 2 - ϵ, 2 + ϵ},
   AxesOrigin → {2, 0}, DisplayFunction :→ Identity ];

Show[{plot1, plot2}, DisplayFunction :→ $DisplayFunction];
```

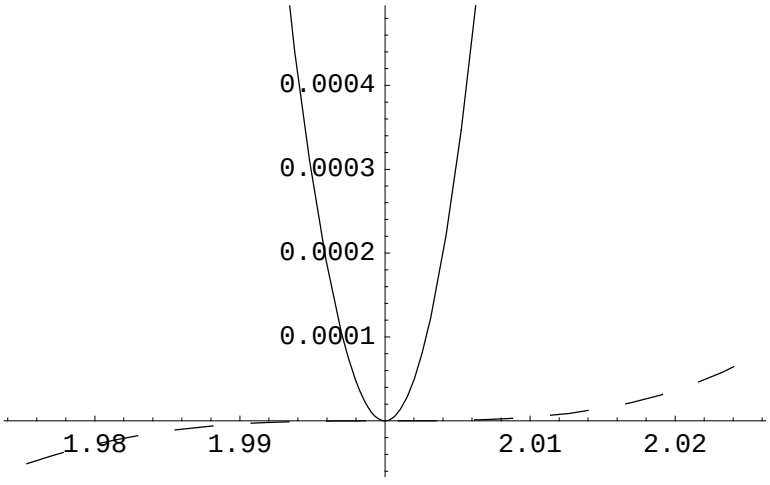


Figure 6.3. Τα γραφήματα της $p^{(1)}(x)$ (με διακεκομμένη γραμμή) και της παραγώγου της $p^{(2)}(x)$.

```
plot3 = Plot[{p'''[x]}, {x, 2 - ϵ, 2 + ϵ}, AxesOrigin → {2, 0},
  PlotStyle → {Dashing[{0.05,0.05}]}, DisplayFunction :→ Identity];

Show[{plot2, plot3}, DisplayFunction :→ $DisplayFunction];
```

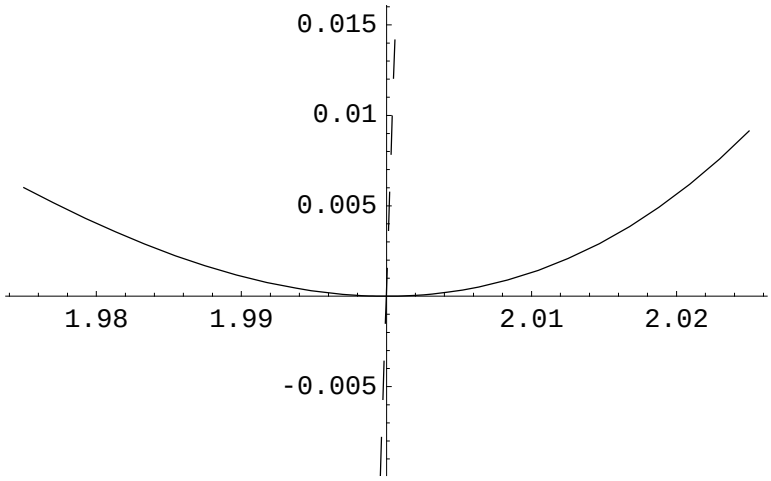


Figure 6.4. Τα γραφήματα της $p^{(2)}(x)$ και της παραγώγου της $p^{(3)}(x)$ (με διακεκομμένη γραμμή).

```
plot4 = Plot[p''''[x], {x, 2 - ϵ, 2 + ϵ},
   AxesOrigin → {2, 0}, DisplayFunction :→ Identity];

Show[{plot3, plot4}, DisplayFunction :→ $DisplayFunction];
```

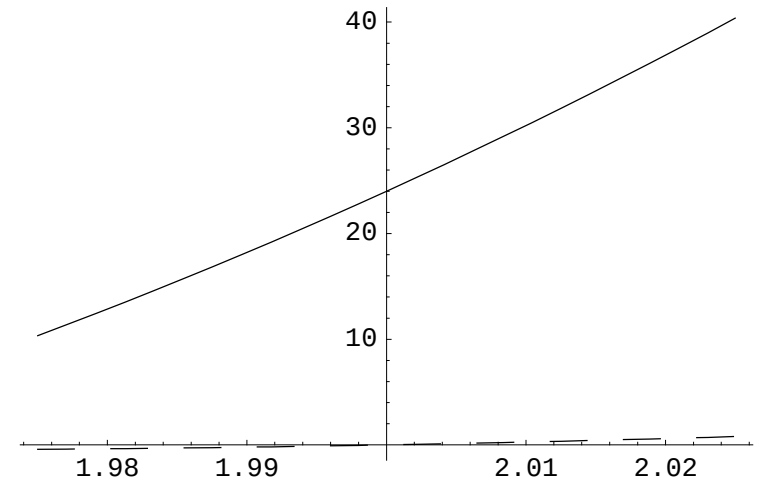


Figure 6.5. Τα γραφήματα του $p^{(3)}(x)$ (με διακεκομμένη γραμμή) και της παραγώγου της $p^{(4)}(x)$.

Οι παράγωγοι $p^{(3)}(x)$ και $p^{(4)}(x)$ είναι οι τελευταίες για τις οποίες ισχύει ότι στο διάστημα $(2 - \epsilon, 2)$ τα πρόσημά τους είναι αντίθετα ενώ στο διάστημα $(2, 2$

+ ϵ) *είναι ίδια*. Στο Figure 6.6 *συγκρίνουμε τις* $p^{(4)}(x)$ *και* $p^{(5)}(x)$ *και βλέπουμε ότι τα πρόσημα είναι τα ίδια στο διάστημα* (2 - ϵ, 2 + ϵ).

```
plot5 = Plot[{p'''''[x]}, {x, 2 - ϵ, 2 + ϵ}, AxesOrigin → {2, 0},
  PlotStyle → {Dashing[{0.05,0.05}]}, DisplayFunction :→ Identity];

Show[{plot4, plot5}, DisplayFunction :→ $DisplayFunction];
```

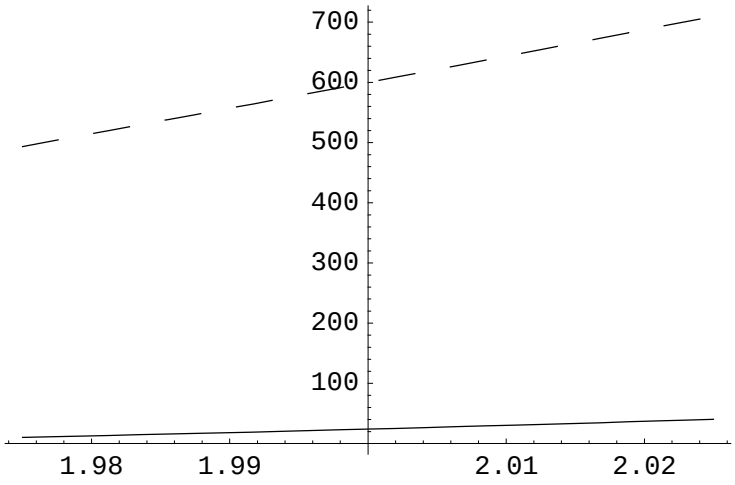


Figure 6.6. Τ*α γραφήματα της* $p^{(4)}(x)$ *και της παραγώγου της* $p^{(5)}(x)$ (*με διακεκομμένη γραμμή*).

Ορισμός:

Έστω $p(x) = 0$ *είναι μία πολυωνυμική εξίσωση βαθμού* $n > 0$ *με πραγματικούς συντελεστές*. Ονομάζουμε ***ακολουθία*** **Fourier** *την ακολουθία των* $n + 1$ *συναρτήσεων*

$$F_{\text{seq}}(x) = \{p(x), p^{(1)}(x), p^{(2)}(x), \ldots, p^{(n)}(x)\}$$

όπου $p^{(i)}(x)$ *είναι η i-στή παράγωγος του* $p(x)$

Παράδειγμα:

Έστω *πάλι το πολυώνυμο* $p(x) = x^3 - 7x + 7$. Η *ακολουθία* Fourier *είναι*

$$F_{\text{seq}}(x) = \{x^3 - 7x + 7, 3x^2 - 7, 6x, 6\}$$

Θεώρημα του Fourier (1820): (Υπολογισμός *ενός πάνω φράγματος στον αριθμό των πραγματικών ριζών που έχει μία εξίσωση σε ένα ανοιχτό διάστημα*.)

Έστω $p(x) = 0$ μία πολυωνυμική εξίσωση βαθμού $n > 0$ με πραγματικούς συντελεστές. και έστω ότι έχει μία πραγματική ρίζα α πολλαπλότητας $m > 1$. Αν στην ακολουθία Fourier $F_{\text{seq}}(x) = \{p(x), p^{(1)}(x), p^{(2)}(x), \ldots, p^{(n)}(x)\}$ αντικαταστήσουμε το x με τυχαίους πραγματικούς αριθμούς ℓ, r ($\ell < r$), τότε προκύπτουν οι αριθμητικές ακολουθίες $F_{\text{seq}}(\ell)$ και $F_{\text{seq}}(r)$ με v_ℓ και v_r μεταβολές προσήμου αντίστοιχα. Ισχύουν τα ακόλουθα:

i. Η ακολουθία $F_{\text{seq}}(\ell)$ δεν μπορεί να έχει λιγότερες μεταβολές προσήμου από την ακολουθία $F_{\text{seq}}(r)$. Δηλαδή, $v_\ell \geq v_r$.
ii. Ο αριθμός ρ των πραγματικών ριζών της εξίσωσης $p(x) = 0$ που βρίσκονται στο διάστημα (ℓ, r) ποτέ δεν μπορεί να είναι μεγαλύτερος από τον αριθμό των μεταβολών προσήμου που χάνονται στην $F_{\text{seq}}(x)$ κατά την μετάβασή μας από την αντικατάσταση $x \leftarrow \ell$ στην αντικατάσταση $x \leftarrow r$. Δηλαδή, $\rho \leq v_\ell - v_r$.
iii. Όταν ο αριθμός ρ των πραγματικών ριζών της εξίσωσης $p(x) = 0$ που βρίσκονται στο διάστημα (ℓ, r) είναι γνήσια μικρότερος από τον αριθμό των μεταβολών προσήμου που χάνονται στην $F_{\text{seq}}(x)$ κατά την μετάβασή μας από την αντικατάσταση $x \leftarrow \ell$ στην αντικατάσταση $x \leftarrow r$, τότε η διαφορά είναι άρτιος αριθμός. Δηλαδή, $\rho = v_\ell - v_r - 2\lambda$, όπου $\lambda \in \mathbb{Z}_{>0}$.

Απόδειξη:
Όταν το x μεταβάλλεται στο διάστημα (ℓ, r) ο αριθμός των μεταβολών προσήμου στην ακολουθία Fourier, $F_{\text{seq}}(x)$, αλλάζει **μόνο** όταν το x είναι ρίζα του $p(x)$ ή μιας των παραγώγων του. Εξετάζουμε τις δύο αυτές περιπτώσεις:

Περίπτωση 1η. Έστω ότι α είναι ρίζα του $p(x)$ πολλαπλότητας m. Από το Λήμμα 6.2.2 προκύπτει πως όταν το x μεταβάλλεται στο διάστημα $(\alpha - \epsilon, \alpha + \epsilon)$, για αρκετά μικρό $\epsilon > 0$, υπάρχουν m μεταβολές προσήμου στην ακολουθία Fourier αμέσως πριν το πέρασμα από την ρίζα α, και δεν υπάρχει καμία μεταβολή προσήμου στην ακολουθία Fourier αμέσως μετά το πέρασμα από την ρίζα α. Συνεπώς, στην ακολουθία Fourier, $F_{\text{seq}}(x)$, χάνονται m μεταβολές προσήμου.

Περίπτωση 2η. Έστω ότι το α είναι τώρα ρίζα μιας παραγώγου, πολλαπλότητας m. Δηλαδή, για κάποιο i, $0 < i < n$, έχουμε $p^{(i-1)}(\alpha) \neq 0$ και $p^{(i)}(\alpha) = 0$. Θεωρούμε την ακολουθία

$$D_{\text{seq}}(x) = \{p^{(i-1)}(x),\ p^{(i)}(x),\ p^{(i+1)}(x),\ \ldots,\ p^{(i+m)}(x)\}$$

που είναι ***υποακολουθία*** *της* $F_{\text{seq}}(x)$, *και όπου* $p^{(i+m)}(x)$ *είναι το πρώτο πολυώνυμο για το οποίο* α *δεν είναι ρίζα.* Προσέξτε πως *όταν το* x *μεταβάλλεται στο διάστημα* $(\alpha - \epsilon,\ \alpha + \epsilon)$, *για αρκετά μικρό* $\epsilon > 0$, *τα πρόσημα των* $p^{(i-1)}(x)$ *και* $p^{(i+m)}(x)$ *δεν αλλάζουν επειδή τα πολυώνυμα αυτά δεν μηδενίζονται.* Με *την βοήθεια του* Λήμματος 6.2.2, *και λαμβάνοντας υπ' όψη την τιμή της* m (*άρτια ή περιττή*) *καθώς επίσης και το αν τα πρόσημα των* $p^{(i-1)}(x)$ *και* $p^{(i+m)}(x)$ *είναι ίδια ή αντίθετα, προκύπτει πως στην ακολουθία* $D_{\text{seq}}(x)$ *χάνεται* ***άρτιος*** *αριθμός προσήμων όταν το* x *μεταβάλλεται στο διάστημα* $(\alpha - \epsilon,\ \alpha + \epsilon)$, *για αρκετά μικρό* $\epsilon > 0$. (Βλέπε *και το παράδειγμα που ακολουθεί.*)

Συνεπώς, *όταν το* x *μεταβάλλεται σε τυχαίο διάστημα* $(\ell,\ r)$, *ο αριθμός των μεταβολών προσήμου που χάνονται στην ακολουθία* $F_{\text{seq}}(x)$ ***είτε*** *είναι ίσος με τον αριθμό* ρ *των πραγματικών ριζών του* $p(x)$ *στο διάστημα αυτό* ***είτε*** *ξεπερνάει τον* ρ *κατά άρτιο αριθμό.*//

Προσοχή:
Όταν το x *μεταβάλλεται σε τυχαίο διάστημα* $(\ell,\ r)$ *με την ακολουθία* $F_{\text{seq}}(x)$ *μπορούμε να βρούμε τον ακριβή αριθμό των ριζών μόνο στις εξής* ***δύο*** *περιπτώσεις*: **(*α*)** *αν δεν χάνεται καμία μεταβολή προσήμου τότε δεν υπάρχει καμία ρίζα στο* $(\ell,\ r)$, *και* **(*β*)** *αν χάνεται μία μεταβολή προσήμου τότε υπάρχει μία πραγματική ρίζα στο* $(\ell,\ r)$. **Τα *αντίστροφα των* (*α*) *και* (*β*) *δεν ισχύουν***!

Παράδειγμα: (*της* **2*ης περίπτωσης*** *του θεωρήματος του* Fourier)
Έστω το πολυώνυμο $p(x) = x^4 - 8x^3 + 24x^2$. Το $\alpha = 2$ *δεν είναι ρίζα του, αλλά είναι ρίζα πολλαπλότητας* $m = 2$ *της παραγώγου του* $p^{(2)}(x)$ — *δηλαδή χρησιμοποιώντας τον συμβολισμό του παραπάνω θεωρήματος,* $i = 2$ *στην ακολουθία* $D_{\text{seq}}(x)$.

```
p[x_] = x^4 - 8 x^3 + 24 x^2;
{p[2], p'[2], p''[2], p'''[2], p''''[2]}
```

```
{48, 32, 0, 0, 24}
```

Έτσι στο παράδειγμα αυτό έχουμε $D_{\text{seq}}(x) = \{p^{(1)}(x),\ p^{(2)}(x),\ p^{(3)}(x),\ p^{(4)}(x)\}$.

```
Dseq[x_] := {p'[x], p''[x], p'''[x], p''''[x]}
```

Θα δούμε πως όταν το x μεταβάλλεται σε τυχαίο διάστημα $(2 - \epsilon, 2 + \epsilon)$, ο αριθμός των μεταβολών προσήμου που χάνονται στην ακολουθία $D_{seq}(x)$ είναι άρτιος. Πράγματι, στο διάστημα $(2 - \epsilon, 2)$ έχουμε 2 μεταβολές προσήμου,

```
Dseq[1.98]
```

```
{32., 0.0048, -0.48, 24}
```

```
variations[Dseq[1.98]]
```

```
2
```

ενώ στο διάστημα $(2, 2 + \epsilon)$ — με βάση το Λήμμα 6.2.2 — τα πολυώνυμα $p^{(2)}(x)$ και $p^{(3)}(x)$ παίρνουν το πρόσημο του $p^{(4)}(x)$ και έτσι δεν έχουμε μεταβολές προσήμου.

```
Dseq[2.02]
```

```
{32., 0.0048, 0.48, 24}
```

```
variations[Dseq[2.02]]
```

```
0
```

Συνεπώς χάθηκαν 2 μεταβολές προσήμου. Προσέξτε πως τα πρόσημα των $p^{(1)}(x)$ και $p^{(4)}(x)$ είναι ίδια και δεν αλλάζουν επειδή τα πολυώνυμα αυτά δεν μηδενίζονται στο $\alpha = 2$.

Παράδειγμα: (υπολογισμός ενός πάνω φράγματος στον αριθμό των πραγματικών ριζών μέσα σε ένα διάστημα με την βοήθεια του θεωρήματος του Fourier)

Έστω το πολυώνυμο $p(x) = x^3 - 7x + 7$. Για να βρούμε ένα πάνω φράγμα στον αριθμό των πραγματικών ριζών που έχει το πολυώνυμο αυτό στο διάστημα $(0, 2)$ με το θεώρημα του Fourier υπολογίζουμε την ακολουθία Fourier, $F_{seq}(x)$, του πολυωνύμου αυτού

```
p[x_] = x^3 - 7 x + 7;
Fseq[x_] := {p[x], p'[x], p''[x], p'''[x]}
Fseq[x]
```

```
{7 - 7 x + x^3, -7 + 3 x^2, 6 x, 6}
```

και κατόπιν υπολογίζουμε τον αριθμό των μεταβολών προσήμου που χάνονται στην $F_{\text{seq}}(x)$ *κατά την μετάβαση του x από το* 0 *στο* 2. *Συγκεκριμένα έχουμε*

```
Fseq[0]
```

```
{7, -7, 0, 6}
```

```
variations[Fseq[0]]
```

```
2
```

και

```
Fseq[2]
```

```
{1, 5, 12, 6}
```

```
variations[Fseq[2]]
```

```
0
```

Δηλαδή χάνονται δύο μεταβολές προσήμου, και αυτό σημαίνει πως στο διάστημα (0, 2) *το πολυώνυμο είτε έχει δύο πραγματικές ρίζες* ή *καμία, κάτι που πρέπει να διερευνηθεί. Στο Mathematica ένα πρόγραμμα που υπολογίζει την ακολουθία* Fourier *είναι το εξής*:

```
createFourierSequence[p_] :=
 Module[{Fseq = {}, q = p, r, v = First[Variables[p]]},
   r = D[p, v]; AppendTo[Fseq, {q, r}];
While[Exponent[r, v] > 0, r = D[r, v]; AppendTo[Fseq, r]
   ]; Fseq // Flatten
  ] /; AtomQ[First[Variables[p]]]
```

και για το τελευταίο παράδειγμα έχουμε:

```
p[x_] = x^3 - 7 x + 7;
Fseq[x_] = createFourierSequence[p[x]];
variations[Fseq[0]] - variations[Fseq[2]]
```

```
2
```

Το *θεώρημα του* Fourier *μπορεί να χρησιμοποιηθεί για την απόδειξη του ακόλουθου θεωρήματος*.

Θεώρημα των Cardano-Descartes: (Υ*πολογισμός ενός πάνω φράγματος στον αριθμό των θετικών ριζών που έχει μία εξίσωση.*)

Έστω $p(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ *μία πολυωνυμική εξίσωση βαθμού* $n > 0$ *με πραγματικούς συντελεστές.* Αν ν *είναι ο αριθμός των μεταβολών προσήμου στην ακολουθία των συντελεστών* $\{c_n, c_{n-1}, \ldots, c_1, c_0\}$ — *όπου οι μηδενικοί συντελεστές έχουν παραληφθεί — και* ρ_+ *είναι ο αριθμός των θετικών ριζών της* $p(x) = 0$, *τότε* $\boldsymbol{\nu = \rho_+ + 2\lambda}$, *όπου* $\lambda \in \mathbb{Z}_{\geq 0}$.

Απόδειξη:

Αυτό *που ζητάμε είναι ένα πάνω φράγμα στον αριθμό των πραγματικών ριζών της* $p(x) = 0$ *μέσα στο διάστημα* $(0, \infty)$. Η *ακολουθία* Fourier *στην περίπτωσή μας είναι* $F_{\text{seq}}(x) = \{p(x), p^{(1)}(x), p^{(2)}(x), \ldots, p^{(n)}(x)\}$, *όπου*

$$\begin{aligned} p(x) &= c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0, \\ p^{(1)}(x) &= n c_n x^{n-1} + \cdots + c_1, \\ p^{(2)}(x) &= n(n-1) c_n x^{n-2} + \cdots + (2!)c_2, \\ &\vdots \\ p^{(n)}(x) &= (n!)c_n. \end{aligned}$$

Με *βάση το θεώρημα του* Fourier *υπολογίζουμε πρώτα την ακολουθία*

$$F_{\text{seq}}(0) = \{ c_0, c_1, (2!)c_2, \ldots, (n!)c_n\}$$

που έχει ν μεταβολές προσήμου, και έπειτα την ακολουθία $F_{\text{seq}}(\infty)$ *που δεν έχει μεταβολή προσήμου — επειδή όλοι οι όροι έχουν το πρόσημο του* c_n. Συνεπώς *από το θεώρημα του* Fourier *έχουμε*

$$\nu = \rho_+ + 2\lambda,$$

όπου $\lambda \in \mathbb{Z}_{\geq 0}$.//

Προσέξτε πως το θεώρημα των Cardano-Descartes μας δίνει τον ***ακριβή*** αριθμό των θετικών ριζών ***μόνο*** στις περιπτώσεις που $\nu = 0$ ή $\nu = 1$ — οπότε κατ' ανάγκη $\lambda = 0$.

- **6.2.2 Το *θεώρημα του* Sturm**

Από ιστορική άποψη αξίζει να αναφέρουμε πως τα δύο βασικά θέματα μελέτης στην ζωή του Fourier ήταν η θεωρία της θερμότητας και η θεωρία αριθμητικής επίλυσης εξισώσεων. Και τα δύο αυτά θέματα συνεχίστηκαν αργότερα από τον Sturm, ο οποίος είχε προσωπικές και επιστημονικές σχέσεις με τον Fourier. Το 1829 οι χειρόγραφες εργασίες του Fourier σχετικά με την αριθμητική επίλυση εξισώσεων είχαν διαδοθεί σε αρκετούς ειδικούς επί του θέματος, ανάμεσα στους οποίους ήταν και ο Sturm — ο οποίος αναφέρει ξεκάθαρα πόσο πολύ επηρεάστηκε από τις εργασίες του Fourier.

Αυτό που έκανε ο Sturm στην θεωρία αριθμητικής επίλυσης εξισώσεων ήταν να αντικαταστήσει την ακολουθία Fourier με την ακολουθία

$$S_{\text{seq}}(x) = \{p(x),\, p^{(1)}(x),\, r_1(x),\, \ldots,\, r_k(x)\},$$

η οποία αποκαλείται ***ακολουθία* Sturm**. Η ακολουθία αυτή προκύπτει με εφαρμογή του Ευκλείδειου αλγόριθμου στα πολυώνυμα $p(x)$ και $p^{(1)}(x)$, ορίζοντας τα $r_i(x)$, $1 \leq i \leq k$, σαν τα ***αρνητικά*** των υπολοίπων που προκύπτουν. Δηλαδή η ακολουθία Sturm ορίζεται από τις ακόλουθες σχέσεις:

$$\begin{aligned}
p(x) &= p^{(1)}(x)\, q_1(x) - r_1(x),\\
p^{(1)}(x) &= r_1(x) q_2(x) - r_2(x),\\
r_1(x) &= r_2(x) q_3(x) - r_3(x),\\
&\vdots\\
r_{k-2}(x) &= r_{k-1}(x) q_k(x) - r_k(x),
\end{aligned}$$

Το πλεονέκτημα της ακολουθίας Sturm είναι ότι μπορούμε τώρα να αποκτήσουμε τον ***ακριβή*** αριθμό των πραγματικών ριζών που έχει η εξίσωση $p(x) = 0$ μέσα σε ένα δεδομένο διάστημα. Προσέξτε πως αν ο βαθμός του πολυωνύμου $p(x)$ είναι n τότε, συνήθως, η ακολουθία Sturm αποτελείται

συνολικά από $n + 1$ συναρτήσεις — δεδομένου ότι στην διαδικασία εύρεσης ενός μέγιστου κοινού διαίρέτη (μ.κ.δ.) των $p(x)$ και $p^{(1)}$, ο βαθμός κάθε υπολοίπου είναι συνήθως κατά μονάδα μικρότερος από τον βαθμό του προηγουμένου υπολοίπου. Επιπλέον, αν δεν υπάρχουν πολλαπλές ρίζες το $r_k(x)$ είναι σταθερά. (Λεπτομέρειες για την εύρεση ενός μ.κ.δ. δύο πολυωνύμων θα δούμε σε ένα από τα επόμενα κεφάλαια. Η μετατροπή ενός πολυωνύμου με πολλαπλές ρίζες σε ένα με απλές θα συζητηθεί σε άλλη ενότητα αυτού του κεφαλαίου.)

Παράδειγμα:

Η ακολουθία Sturm για το πολυώνυμο $p(x) = x^3 - 7x + 7$ είναι $S_{seq}(x) = \{p(x), p^{(1)}(x), r_1(x), r_2(x)\}$, όπου $p^{(1)}(x)$ είναι η πρώτη παράγωγος του $p(x)$ και τα υπόλοιπα υπολογίζονται ως εξής: Το $r_1(x)$ είναι

```
p[x_] = x^3 - 7 x + 7; pp[x_] = D[p[x], x];
r1 = -PolynomialMod[p[x], pp[x]]
```

$$-7 + \frac{14\,x}{3}$$

ή ισοδύναμα $r_1(x) = 2x - 3$. Προσέξτε πως αν υπολογίσουμε και το πηλίκο $q_1(x)$,

```
q1 = PolynomialQuotient[p[x], pp[x], x]
```

$$\frac{x}{3}$$

τότε ισχύει η προαναφερθείσα σχέση $p(x) = p^{(1)}(x)\, q_1(x) - r_1(x)$:

```
p[x] == Evaluate[(pp[x] q1 - r1) // Expand]
```

```
True
```

Αντίστοιχα το $r_2(x)$ υπολογίζεται

```
r2 = -PolynomialMod[pp[x], r1]
```

$$\frac{1}{4}$$

ή ισοδύναμα $r_2(x) = 1$. Αν δε υπολογίσουμε και το πηλίκο $q_2(x)$,

```
q2 = PolynomialQuotient[pp[x], r1, x]
```

$$\frac{27}{28} + \frac{9\,x}{14}$$

τότε ισχύει η δεύτερη (*και τελευταία για το παράδειγμα αυτό*) *προαναφερθείσα σχέση* $p^{(1)}(x) = r_1(x)q_2(x) - r_2(x)$:

```
pp[x] == Evaluate[(r1 q2 - r2) // Expand]
```

```
True
```

Άρα *η ακολουθία* Sturm *για το πολυώνυμο* $p(x) = x^3 - 7x + 7$ *είναι* $S_{\text{seq}}(x) = \{x^3 - 7x + 7,\ 3x^2 - 7,\ 2x - 3,\ 1\}$. Στο *Mathematica ένα πρόγραμμα που υπολογίζει την ακολουθία* Sturm *είναι το εξής*:

```
createSturmSequence[p_] :=
 Module[{Sseq = {}, q = p, r, v = First[Variables[p]]},
   r = D[p, v]; AppendTo[Sseq, {q, r}];
While[Exponent[r, v] > 0, temp = -PolynomialMod[q, r];
    AppendTo[Sseq, temp]; q = r; r = temp
   ]; Sseq // Flatten
  ] /; AtomQ[First[Variables[p]]]
```

Οι *συντελεστές των μελών της ακολουθίας που υπολογίζονται είναι όμως είναι ρητοί και όχι ακέραιοι*.

```
Sseq[x_] = createSturmSequence[x^3 - 7 x + 7]
```

$$\left\{7 - 7\,x + x^3,\ -7 + 3\,x^2,\ -7 + \frac{14\,x}{3},\ \frac{1}{4}\right\}$$

Όπως *θα δούμε σε επόμενο κεφάλαιο, ο απλούστερος — αλλά όχι ο πιο αποτελεσματικός — τρόπος για να πάρουμε ακέραιους συντελεστές στα υπόλοιπα είναι ο εξής*: **1*ον***. *πριν την διαίρεση πολλαπλασιάζουμε τον διαιρετέο με τον κύριο συντελεστή του διαιρέτη υψωμένο στην δύναμη* $m - n + 1$, *όπου* m *είναι ο βαθμός του διαιρετέου και* n *είναι ο βαθμός του διαιρετη, και* **2*ον***. *μετά την διαίρεση διαιρούμε τους συντελεστές του υπολοίπου με τον μέγιστο κοινό διαιρέτη τους*. Έτσι *τώρα το πρόγραμμα γίνεται*

```
createSturmSequenceIC[p_] := Module[
   {cl, gcd, lc, m, n, q = p, r, Sseq = {}, v = First[Variables[p]]},
   r = D[p, v]; AppendTo[Sseq, {q, r}];
   m = Exponent[q, v]; n = Exponent[r, v];
While[n > 0,
    lc = Last[CoefficientList[r, v]];
    temp = -PolynomialMod[lc^(m-n+1) q, r];
    cl = CoefficientList[temp, v];
    gcd = GCD[Apply[Sequence, cl]];
    cl = cl/gcd;
    temp = Fold[ v #1 + #2 &, 0, Reverse[cl]] // Expand;
    AppendTo[Sseq, temp]; q = r; r = temp; m = n;
    n = Exponent[r, v]
   ]; Sseq // Flatten
  ] /; AtomQ[First[Variables[p]]]
```

και η ακολουθία Sturm *είναι*:

```
Sseq[x_] = createSturmSequenceIC[x^3 - 7 x + 7]
```

```
{7 - 7 x + x^3, -7 + 3 x^2, -3 + 2 x, 1}
```

Οι 4 *χαρακτηριστικές ιδιότητες των μελών της ακολουθίας* Sturm:

Έστω $p(x) = 0$ *μία εξίσωση με ρητούς συντελεστές και χωρίς πολλαπλές ρίζες*. Για *τις συναρτήσεις της ακολουθίας* Sturm, $S_{\text{seq}}(x) = \{p(x), p^{(1)}(x), r_1(x), \ldots, r_k(x)\}$, *ισχύουν τα εξής*:

ι. Αν α *είναι μία ρίζα του πολυωνύμου* $p(x)$ *τότε για αρκετά μικρό* $\epsilon > 0$ *τα πολυώνυμα* $p(x)$ *και* $p^{(1)}(x)$ *έχουν αντίθετα πρόσημα στο διάστημα* $(\alpha - \epsilon, \alpha)$ *και ίδια πρόσημα στο διάστημα* $(\alpha, \alpha + \epsilon)$.

Απόδειξη:

Αυτό *είναι το* Λήμμα 6.2.1.

ιι. Δύο *διαδοχικά μέλη της ακολουθίας* Sturm *δεν μπορούν να μηδενίζονται ταυτόχρονα*.

Απόδειξη:

Υποθέτουμε *το αντίθετο*. Δηλαδή έστω ότι $r_i(x) = 0$ *και* $r_{i+1}(x) = 0$. Τότε από *τις σχέσεις ορισμού των υπολοίπων έχουμε*: $r_i(x) = r_{i+1}(x)q_{i+2}(x) - r_{i+2}(x) = 0$,

που συνεπάγεται $r_{i+2}(x) = 0$. *Συνεπώς,* $r_{i+3}(x) = 0\ldots$, $r_k(x) = 0$. *Αυτή είναι όμως και η αντίφαση, διότι* $r_k(x)$ *είναι σταθερά. Προφανώς, το ίδιο ισχύει και για τα πολυώνυμα* $p(x)$ *και* $p^{(1)}(x)$.//

ιιι. *Αν για τυχαίο* i, $i \neq k$, *η συνάρτηση* $r_i(x)$ *της ακολουθίας* Sturm *μηδενίζεται για κάποια τιμή* x_0, *τότε οι γειτονικές της συναρτήσεις στην ακολουθία, εκτιμώμενες στην ίδια τιμή, έχουν αντίθετα πρόσημα.*

Απόδειξη:
Πράγματι, έστω ότι $r_i(x_0) = 0$. *Τότε από την σχέση ορισμού των υπολοίπων έχουμε:* $r_{i-1}(x_0) = r_i(x_0)q_{i+1}(x_0) - r_{i+1}(x_0)$ *απ' όπου προκύπτει* $r_{i-1}(x_0) = - r_{i+1}(x_0)$. *Προφανώς, το ίδιο ισχύει και για το πολυώνυμο* $p^{(1)}(x)$.//

ιν. *Η τελευταία συνάρτηση* $r_k(x)$ *δεν μηδενίζεται και συνεπώς δεν αλλάζει πρόσημο.*

Απόδειξη:
Προφανής διότι το πολυώνυμο $p(x)$ *δεν έχει πολλαπλές ρίζες.*//

Έχοντας αποδείξει τις χαρακτηριστικές αυτές ιδιότητες των μελών της ακολουθίας Sturm *είμαστε έτοιμοι για το ακόλουθο:*

Θεώρημα του Sturm (1829):
Έστω η πολυωνυμική εξίσωση $p(x) = 0$ *με ακέραιους συντελεστές και χωρίς πολλαπλές ρίζες. Τότε, για τον αριθμό* ρ *των πραγματικών ριζών της στο διάστημα* (ℓ, r) *ισχύει η ισότητα*

$$\boldsymbol{\rho = \nu_\ell - \nu_r},$$

όπου ν_ℓ, ν_r *είναι οι μεταβολές προσήμου των αριθμητικών ακολουθιών* $S_{\text{seq}}(\ell)$ *και* $S_{\text{seq}}(r)$ *αντίστοιχα.*

Απόδειξη:

Αυτό που πρέπει να δείξουμε είναι πως όταν το x μεταβάλλεται από το ℓ στο r, η ακολουθία Sturm ***χάνει*** μία μεταβολή προσήμου όταν το x περνάει από μία ρίζα α της $p(x) = 0$ και, σε αντίθεση από την ακολουθία Fourier, ***δεν χάνει*** καμία μεταβολή προσήμου όταν το x περνάει από μία ρίζα ενός άλλου μέλους της ακολουθίας.

Πράγματι, από την πρώτη ιδιότητα (***ι***) — ή το Λήμμα 6.2.1 — συμπεραίνουμε πως όταν το x περνάει από μία ρίζα α της $p(x) = 0$ χάνεται ακριβώς μία μεταβολή προσήμου.

Έτσι ας υποθέσουμε πως το x περνάει από μία (**όχι κατ' ανάγκη απλή**) ρίζα α_i της $r_i(x) = 0$. Από τις ιδιότητες (***ιι***) και (***ιιι***) έπεται πως $r_{i-1}(\alpha_i)$ και $r_{i+1}(\alpha_i)$ είναι μή μηδενικά και έχουν αντίθετα πρόσημα. Διαλέγουμε τότε ένα μικρό διάστημα $(\alpha_i - \epsilon, \alpha_i + \epsilon)$, $\epsilon > 0$, όπου οι δύο αυτές συναρτήσεις δεν μηδενίζονται, που σημαίνει πως δεν αλλάζουν πρόσημα και δημιουργούμε τον ακόλουθο πίνακα (Figure 6.7):

x	r_{i-1}	r_i	r_{i+1}	r_{i-1}	r_i	r_{i+1}
$\alpha_i - \epsilon$	+	±	-	-	±	+
α_i	+	0	-	-	0	+
$\alpha_i + \epsilon$	+	∓(±)	-	-	∓(±)	+

Figure 6.7. Στις δύο στήλες της συνάρτησης r_i, τα πρόσημα (±) δηλώνουν ρίζα με πολλαπλότητα.

Από τον πίνακα του σχήματος 6.7 βλέπουμε πως όταν το x περνάει από μία (όχι κατ' ανάγκη απλή) ρίζα α_i της $r_i(x) = 0$ ***δεν χάνεται μεταβολή προσήμου***, και αυτό σημπληρώνει την απόδειξή μας.//

Παράδειγμα:

Έστω πάλι το πολυώνυμο $p(x) = x^3 - 7x + 7$ η ακολουθία Sturm του οποίου, όπως είδαμε, είναι $S_{seq}(x) = \{x^3 - 7x + 7, 3x^2 - 7, 2x - 3, 1\}$. Με βάση το θεώρημα του Sturm ο ακριβής αριθμός των πραγματικών ριζών που έχει το $p(x)$ στο διάστημα $(0, 2)$ είναι $v_0 - v_2$, όπου v_0, v_2 είναι οι μεταβολές προσήμου των αριθμητικών

ακολουθιών $S_{seq}(0)$ *και* $S_{seq}(2)$ *αντίστοιχα*. *Στο συγκεκριμένο παράδειγμα* $S_{seq}(0) = \{7, -7, -3, 1\}$ *με* 2 *μεταβολές προσήμου*, $v_0 = 2$, *και* $S_{seq}(2) = \{1, 5, 1, 1\}$ *με καμία μεταβολή προσήμου*, $v_2 = 0$. *Συνεπώς υπάρχουν* $v_0 - v_2 = 2$ *πραγματικές ρίζες στο διάστημα* (0, 2). *Το αποτέλεσμα αυτό επιβεβαιώνεται και με το Mathematica*:

```
Sseq[x_] = createSturmSequenceIC[x^3 - 7 x + 7];
variations[Sseq[0]] - variations[Sseq[2]]
```

```
2
```

Ο *ίδιος ο* Sturm *ανέφερε πως το θεώρημα αυτό του* 1829 *ήταν παράπλευρο αποτέλεσμα των εκτεταμένων ερευνών του στην περιοχή των εξισώσεων διαφορών δευτέρας τάξης*. *Το αίτημα να μην έχει η εξίσωση* $p(x) = 0$ *πολλαπλές ρίζες δεν είναι περιορισμός της γενικότητας*, *διότι στην αντίθετη περίπτωση* — *όπως θα δούμε στην επόμενη ενότητα* — *τις* "*βγάζουμε*" *με μία εύκολη* "*παραγοντοποίηση*" (squarefree factorization) *και ύστερα εφαρμόζουμε το θεώρημα του* Sturm.

Το 1835 ο Sturm *τροποποίησε το θεώρημά του έτσι ώστε να μπορεί να προσδιορίζει τον αριθμό των ζευγών μιγαδικών ριζών που έχει η εξίσωση* $p(x) = 0$, *στην περίπτωση που η ακολουθία* Sturm *έχει* $n + 1$ *μέλη*, *όπου* $n = \deg(p(x))$.

Θεώρημα του Sturm (1835):
Έστω η πολυωνυμική εξίσωση $p(x) = 0$ *βαθμού* n, *με ακέραιους συντελεστές και χωρίς πολλαπλές ρίζες*. *Τότε*, *ο αριθμός των* ***ζευγών μιγαδικών ριζών*** *του* $p(x)$ *ισούται με τον αριθμό των μεταβολών προσήμου στην ακολουθία των πρώτων όρων των* n *συναρτήσεων* $\{p^{(1)}(x), r_1(x), \ldots, r_k(x)\}$ *της ακολουθίας* Sturm $S_{seq}(x)$.

Απόδειξη:
Η *αλήθεια αυτού του κανόνα βασίζεται στο γεγονός ότι η μία από τυχαίες δύο γειτονικές συναρτήσεις της ακολουθίας* Sturm *έχει βαθμό άρτιο και η άλλη περιττό*. *Επομένως*, *αν οι δύο αυτές συναρτήσεις έχουν το ίδιο πρόσημο για* $x = +\infty$, *θα έχουν αντίθετα πρόσημα για* $x = -\infty$, *και αντίστροφα*. *Έτσι αν εκτιμήσουμε την ακολουθία* Sturm, $S_{seq}(x)$, *στα σημεία* $x = +\infty$ *και* $x = -\infty$ *κάθε* ***μεταβολή προσήμου*** *σε μία ακολουθία αντιστοιχεί σε* ***σταθερότητα***

προσήμου *στην άλλη* (*βλέπε και το παράδειγμα που ακολουθεί*). *Δηλαδή ο αριθμός σταθερότητων προσήμου στην ακολουθία* Sturm *εκτιμημένης στο σημείο* $x = -\infty$ *ισούται με τον αριθμό μεταβολών προσήμου στην ακολουθία* Sturm *εκτιμημένης στο σημείο* $x = +\infty$.

Έστω ότι i *είναι ο αριθμός των μεταβολών προσήμου στην ακολουθία* $S_{seq}(+\infty)$. *Οι μεταβολές αυτές προέρχονται από τα πρόσημα των συντελεστών των υψηλότερων βαθμών ως προς* x (*των πρώτων όρων*), *στις* n *συναρτήσεις* $\{p^{(1)}(x), r_1(x), \ldots, r_k(x)\}$ *της ακολουθίας* Sturm $S_{seq}(x)$ — *όπου οι πρώτοι όροι των* $p(x)$ *και* $p^{(1)}(x)$ *θεωρούνται θετικοί*.

Μόλις *είδαμε όμως ότι στην ακολουθία* $S_{seq}(-\infty)$ *ο αριθμός σταθερότητων προσήμου θα είναι* i, *ή ισοδύναμα η ακολουθία* $S_{seq}(-\infty)$ *θα έχει* $n - i$ *μεταβολές προσήμου*. (*Εδώ θεωρούμε δεδομένο ότι στην ακολουθία* Sturm *υπάρχουν* $n + 1$ *συναρτήσεις και ότι στην* $S_{seq}(x)$ *ο αριθμός των μεταβολών προσήμου συν τον αριθμό των σταθερότητων προσήμου ισούται με* n.)

Από *το θεώρημα όμως του* Sturm *του* 1829 *ξέρουμε πως ο αριθμός των πραγματικών ριζών της* $p(x) = 0$ *που βρίσκονται στο διάστημα* $(-\infty, +\infty)$ *ισούται με* $\mathbf{v_{-\infty} - v_{\infty}}$, *όπου* $v_{-\infty}$, v_{∞} *είναι οι μεταβολές προσήμου των αριθμητικών ακολουθιών* $S_{seq}(-\infty)$ *και* $S_{seq}(\infty)$ *αντίστοιχα*. *Στην προκειμένη περίπτωση το* $p(x)$ *έχει* $n - 2i$ *πραγματικές ρίζες, που σημαίνει πως έχει* $2i$ *μιγαδικές ρίζες που εμφανίζονται σε ζευγάρια*. *Επομένως έχει* i *ζευγάρια μιγαδικών ριζών*.//

Παράδειγμα:
Έστω το πολυώνυμο $p(x) = x^5 - 3x^3 + 7x^2 - 28x + 28$ *και η αντίστοιχη ακολουθία* Sturm, $S_{seq}(x)$

```
p[x_] = (x - 2 i) (x + 2 i) (x^3 - 7 x + 7) // Expand;
Sseq[x_] = createSturmSequenceIC[p[x]]
```

```
{28 - 28 x + 7 x^2 - 3 x^3 + x^5, -28 + 14 x - 9 x^2 + 5 x^4,
 -140 + 112 x - 21 x^2 + 6 x^3, -4564 + 2352 x + 493 x^2, 520304 - 350941 x, -1}
```

Προσέξτε τις μεταβολές και σταθερότητες προσήμου στις ακολουθίες $S_{seq}(-\infty)$ *και* $S_{seq}(+\infty)$.

```
Limit[Sseq[x], x → -∞]
```

```
{-∞, ∞, -∞, ∞, ∞, -1}
```

```
Limit[Sseq[x], x → ∞]
```

```
{∞, ∞, ∞, ∞, -∞, -1}
```

Το *πολυώνυμό μας έχει ένα ζευγάρι μιγαδικών ριζών και αυτό φαίνεται από το γεγονός ότι η ακολουθία* $S_{\text{seq}}(+\infty)$ *έχει μία μεταβολή προσήμου*. *Πράγματι*, *είτε έχουμε*

```
variations[Limit[Sseq[x], x → ∞]]
```

```
1
```

είτε

```
variations[Map[Last[CoefficientList[#, x]] &, Drop[Sseq[x], 1]]]
```

```
1
```

όπου η παραπάνω αριθμητική ακολουθία αποτελείται από τους συντελεστές των πρώτων όρων των 5 *τελευταίων συναρτήσεων της ακολουθίας* Sturm

```
Map[Last[CoefficientList[#, x]] &, Drop[Sseq[x], 1]]
```

```
{5, 6, 493, -350941, -1}
```

■ 6.2.3 Η *κλασσική μέθοδος διχοτόμησης του* Sturm *για την απομόνωση των πραγματικών ριζών ενός πολυωνύμου*

Το *θεώρημα του* Sturm *μπορεί να χρησιμοποιηθεί για την απομόνωση των πραγματικών ριζών πολυωνυμικών εξισώσεων με ακέραιους συντελεστές και χωρίς πολλαπλές ρίζες*. *Στην ενότητα αυτή περιγράφουμε την κλασσική μέθοδο διχοτόμησης του* Sturm, *ενώ στην επόμενη ενότητα*, 6.2.4, *θα μελετήσουμε έναν αλγόριθμο για την διάσπαση ενός πολυωνύμου σε παράγοντες χωρίς πολλαπλές ρίζες*.

Σύμφωνα *με την αρχική*, *κλασσική*, *πρόταση του* Sturm, *ο πιο αποτελεσματικός τρόπος για την απομόνωση των πραγματικών ριζών του πολυωνύμου* $p(x)$ *είναι*

να απομονώσουμε ***πρώτα τις θετικές ρίζες*** *του* $p(x)$ *και* ***ύστερα τις αρνητικές*** *— αφού πρώτα τις κάνουμε θετικές με την αντικατάσταση* $x \leftarrow -x$.

Το *πρώτο και άμεσο πλεονέκτημα της πρότασης του* Sturm *είναι ότι για τα συμμετρικά πολυώνυμα — δηλαδή εκείνα για τα οποία ισχύει* $p(x) = p(-x)$ *ή με άλλα λόγια εκείνα για τα οποία οι θετικές τους ρίζες ισούνται (σε απόλυτες τιμές) με τις αρνητικές τους — η απομόνωση των αρνητικών ριζών καθίσταται περιττή*!

Ακολουθώντας *την πρόταση του* Sturm, *και υποθέτοντας πως* $p(x) \neq 0$ *— διότι αλλιώς αντκαθιστούμε το* $p(x)$ *με το* $\frac{p(x)}{x}$ *και επιστρέφουμε το διάστημα* $(0, 0)$ *— υπολογίζουμε* ***πρώτα*** *την ακολουθία* Sturm *για το* $p(x)$ *και ύστερα βρίσκουμε κάποιο διάστημα* $(0, b_+)$, $b_+ \in \mathbb{Q}$, *που περιέχει τις θετικές ρίζες. Στην ενότητα* 6.2.5 *θα μάθουμε να υπολογίζουμε ένα πάνω φράγμα στις τιμές των θετικών ριζών ενός πολυωνύμου. Αν* $p(b_+) = 0$, *επιστρέφουμε το διάστημα* (b_+, b_+).

Στην ***συνέχεια*** *η απομόνωση των θετικών ριζών του* $p(x)$ *προχωράει ως εξής*: *Με την βοήθεια της ακολουθίας* Sturm *υπολογίζουμε τον ακριβή αριθμό των θετικών ριζών* $\rho_+ = v_0 - v_{b_+}$ *στο διάστημα* $(0, b_+)$. *Αν* $\rho_+ = 0$, *το διάστημα* $(0, b_+)$ *δεν έχει θετικές ρίζες και δεν λαμβάνεται πλέον υπ' όψη. Αν* $\rho_+ = 1$, *τερματίζει η απομόνωση των θετικών ριζών και επιστρέφουμε το διάστημα* $(0, b_+)$. *Αν* $\rho_+ > 1$, *ελέγχουμε αρχικά αν το μεσαίο σημείο* $m_p = \frac{b_+}{2}$ *είναι ρίζα του* $p(x)$. *Αν το αποτέλεσμα του τεστ είναι θετικό, επιστρέφουμε το διάστημα* (m_p, m_p), *και εξετάζουμε τα υποδιαστήματα* $(0, m_p)$ *και* (m_p, b_+).

Σε κάθε ένα από τα δύο αυτά υποδιάστηματα υπολογίζεται ο ακριβής αριθμός ρ_{v_+} *των πραγματικών ριζών. Αν* $\rho_{v_+} = 0$ *για κάποιο από αυτά, το αντίστοιχο υποδιάστημα δεν λαμβάνεται πλέον υπ' όψη. Αν* $\rho_{v_+} \geq 1$, *ενεργούμε όπως και πριν*.

Αφού *απομονώσουμε τις θετικές ρίζες κάνουμε την αντικατάσταση* $x \leftarrow -x$, *οπότε οι αρνητικές ρίζες γίνονται θετικές, ύστερα βρίσκουμε κάποιο διάστημα* $(0, b_-)$, $b_- \in \mathbb{Q}$, *που περιέχει τις "τέως" αρνητικές — αλλά τώρα θετικές — ρίζες, και επαναλμβάνουμε την ίδια διαδικασία*.

Η *μέθοδος σταματάει όταν έχουμε απομονώσει όλες τις πραγματικές ρίζες*. Ο *αριθμός των υποδιαιρέσεων — και εν γένει ο θεωρητικός χρόνος για την απομόνωση των ριζών — εξαρτάται από το πόσο κοντά είναι οι ρίζες*. *Στην ενότητα* 6.2.6 *υπολογίζουμε ένα κάτω φράγμα στην απόσταση μεταξύ δύο τυχαίων ριζών ενός πολυωνύμου*.

Ακολουθώντας *την πρόταση του* Sturm *το αρχικό διάστημα* $(0, b_+)$ *που χρησιμοποιούμε πρώτα για τις θετικές ρίζες*, *είναι εντελώς διαφορετικό από το αντίστοιχο αρχικό διάστημα* $(0, b_-)$ *που χρησιμοποιούμε στη συνέχεια για τις αρνητικές ρίζες*. *Συνεπώς*, *με αυτόν τον τρόπο* ***περιορίζουμε στο ελάχιστο τις άσκοπες υποδιαιρέσεις διαστημάτων και τους ελέγχους για ύπαρξη ρίζών σε αυτά***.

Η *πρόταση αυτή του* Sturm *εφαρμόσθηκε από τους Γάλλους μαθηματικούς του* 19*ου αιώνα*, *αλλά μετά περιέπεσε σε λήθη*. *Επανήλθε στο "φως" από τον γράφοντα*, *το* 1978, *στην διδακτορική του διατριβή*.

Έτσι, *τον εικοστό αιώνα και μέχρι το* 1978, *σαν αρχικό διάστημα χρησιμοποιούταν το διάστημα* $(-b, b)$, *όπου* b *είναι ένα φράγμα στις* ***απόλυτες τιμές των ριζών*** *του* $p(x)$. *Στην σχετική βιβλιογραφία υπάρχουν διάφορα θεωρήματα για τον υπολογισμό διαφόρων τιμών αυτού του* b, *τα οποία δεν θα μελετήσουμε εδώ*.

Το *μειονέκτημα όμως*, *της στρατηγικής αυτής είναι ότι οι αρνητικές και οι θετικές ρίζες δεν είναι κατ' ανάγκη ομοιόμορφα κατανεμημένες*. *Έτσι*, *σε απόλυτες τιμές*, *μπορεί να συμβεί οι μεν αρνητικές να είναι πολύ μεγάλες οι δε θετικές πολύ μικρές* (*ή και αντίστροφα*). *Στην περίπτωση αυτή* ***άσκοπα*** *θα* ***υποδιαιρούμε*** *πολλά διαστήματα*, *τα οποία και θα* ***ελέγχουμε*** *για ρίζες που δεν έχουν*.

Ακολουθεί *η κλασσική μέθοδος της διχοτόμησης του* Sturm *για την απομόνωση των πραγματικών ριζών πολυωνυμικών εξισώσεων με ακέραιους συντελεστές και χωρίς πολλαπλές ρίζες*.

Αλγόριθμος: Ο *κλασσικός αλγόριθμος του* Sturm (1829) *για τις θετικές ρίζες*.

Είσοδος: $p(x) = 0$, μία πολυωνυμική εξίσωση με ακέραιους συντελεστές, χωρίς πολλαπλές ρίζες και $p(0) \neq 0$.
Έξοδος: Τα διαστήματα απομόνωσης των **θετικών** ριζών του $p(x)$ ή οι ακριβείς θετικές ρίζες σε μορφή διαστημάτων.

==========

1. Ορίζουμε την λίστα των διαστημάτων απομόνωσης των ριζών *rootIsolationIntervals* = {}, καθώς και την λίστα των διαστημάτων προς εξέταση *intervalsToBeProcessed* = {}. Αρχικά οι δύο αυτές λίστες είναι κενές. Υπολογίζουμε επίσης την ακολουθία Sturm του $p(x)$ με την βοήθεια της συνάρτησης createSturmSequenceIC[].

2. Με την συνάρτηση CauchyPositiveRootUpperBound[], που περιγράφεται στην ενότητα 6.2.5, υπολογίζουμε ένα πάνω φράγμα, $b_+ \in \mathbb{Q}$, στις τιμές των θετικών ριζών του $p(x)$. Το b_+ υπολογίζεται κατά τέτοιο τρόπο ώστε είναι **γνήσια** μεγαλύτερο από κάθε θετική ρίζα του $p(x)$. Επιπλέον ορίζουμε το αρχικό διάστημα $(\ell, r) = (0, b_+)$, και το επισυνάπτουμε στην λίστα *intervalsToBeProcessed*.

3. (* επεξεργασία διαστήματος *)
Μέχρις ότου η λίστα *intervalsToBeProcessed* = {}, δηλαδή μέχρι να "αδειάσει", **επαναλαμβάνουμε** την εξής διαδικασία: Παίρνουμε το πρώτο διαθέσιμο διάστημα (ℓ, r). Με την βοήθεια του θεωρήματος του Sturm (1829) και της συνάρτησης variations[] υπολογίζουμε τον αριθμό των θετικών ριζών $\rho_+ = v_\ell - v_r$ στο διάστημα (ℓ, r). Αν $\rho_+ = 0$, το διάστημα (ℓ, r) δεν έχει θετικές ρίζες και δεν λαμβάνεται πλέον υπ' όψη. Αν $\rho_+ = 1$, επισυνάπτουμε το διάστημα (ℓ, r) στην λίστα *rootIsolationIntervals*. Αν $\rho_+ > 1$, τότε **(α)** θέτουμε $m_p = \frac{\ell+r}{2}$, υποδιαιρούμε το διάστημα (ℓ, r) στα υποδιαστήματα (ℓ, m_p) και (m_p, r), τα οποία επισυνάπτουμε στην λίστα *intervalsToBeProcessed*, διαστημάτων προς εξέταση, και **(β)** στην περίπτωση που $p(m_p) = 0$ επισυνάπτουμε το διάστημα (m_p, m_p) στην λίστα *rootIsolationIntervals*.
==========

Για την απομόνωση των **αρνητικών ριζών** πρώτα εξετάζουμε αν $p(x) = p(-x)$. Αν ισχύει η ισότητα, αυτό σημαίνει πως οι αρνητικές ρίζες είναι συμμετρικές

με τις θετικές για τις οποίες έχουμε ήδη υπολογίσει τα διαστήματα απομόνωσής τους. Άρα στην περίπτωση αυτή τα διαστήματα απομόνωσης των αρνητικών ριζών βρίσκονται στοιχειωδώς. Αν $p(x) \neq p(-x)$ *τότε θέτουμε* $p(x) \leftarrow p(-x)$, *επαναλαμβάνουμε τον παραπάνω αλγόριθμο ακόμα μία φορά και στο τέλος απεικονίζουμε τα διαστήματα απομόνωσης των ριζών στον αρνητικό ημιάξονα.*

Όσον αφορά το 0, *εύκολα ελέγχουμε αν* $p(0) = 0$, *και στην περίπτωση αυτή θέτουμε* $p(x) = \frac{p(x)}{x}$.

Ακολουθεί *ο παραπάνω αλγόριθμος εφαρμοσμένος στο Mathematica. Για τον αλγόριθμο αυτό χρειάζεται να έχουν ενεργοποιηθεί οι συναρτήσεις* variations[], CauchyPositiveRootUpperBound[], *και* createSturmSequenceIC[].

```
SturmPositiveRootIsolation[p_] :=
 Module[{b, intervalsToBeProcessed, left, midPoint, posroots,
   right, rootIsolationIntervals, Sseq, v = First[Variables[p]]},

  (*  step 1, initialization  *)
  rootIsolationIntervals = {};
  intervalsToBeProcessed = {};
  Sseq = createSturmSequenceIC[p];

  (*  step 2, initialization continued  *)
  b = CauchyPositiveRootUpperBound[p];
  left = 0; right = b;
  AppendTo[intervalsToBeProcessed, {left, right}];

  (*  step 3, processing of intervals  *)
  While[intervalsToBeProcessed ≠ {},
   {left, right} = First[intervalsToBeProcessed];
   intervalsToBeProcessed = Rest[intervalsToBeProcessed];
   posroots =
    variations[Sseq /. v -> left] - variations[Sseq /. v -> right];
   Switch[posroots,
    0, Null,
    1,
    AppendTo[rootIsolationIntervals, {left, right}]; Continue[],
    _, midPoint = (left + right)/2; AppendTo[
     intervalsToBeProcessed, {left, midPoint}];
    AppendTo[intervalsToBeProcessed, {midPoint, right}];
    If[(p /. v -> midPoint) == 0,
     AppendTo[rootIsolationIntervals, {midPoint, midPoint}]]];
  Sort[rootIsolationIntervals]]
```

Έτσι βλέπουμε πως οι ***θετικές*** ρίζες του πολυωνύμου $p(x) = x^3 - 7x + 7$ βρίσκονται στα διαστήματα απομόνωσης $(0, \frac{3}{2})$ και $(\frac{3}{2}, 3)$:

```
p[x_] = x^3 - 7 x + 7; SturmPositiveRootIsolation[p[x]]
```

$$\left\{\left\{0, \frac{3}{2}\right\}, \left\{\frac{3}{2}, 3\right\}\right\}$$

ενώ η μοναδική ***αρνητική*** βρίσκεται στο διάστημα $(-4, 0)$.

```
SturmPositiveRootIsolation[p[-x]]
```

```
{{0, 4}}
```

Προφανώς *το* 0 *δεν είναι ρίζα του* $p(x)$.

```
p[0] == 0
```

```
False
```

Τελειώνουμε *την περιγραφή του αλγορίθμου αυτού τονίζοντας ότι η εφαρμογή του θα μπορούσε να βελτιωθεί στο εξής σημείο*: Έστω (ℓ, r) *ένα διάστημα*. Κατ' *αρχάς υπολογίζουμε τον αριθμό των μεταβολών προσήμου των ακολουθιών* Sseq(ℓ) *και* Sseq(r). Αν *χρειαστεί να υποδιαιρέσουμε το διάστημα στα υποδιαστήματα* (ℓ, midPoint), *και* (midPoint, r) *τότε υπολογίζουμε ξανά τον αριθμό των μεταβολών προσήμου των ακολουθιών* Sseq(ℓ) *και* Sseq(midPoint) ή / *και* Sseq(r) *και* Sseq(midPoint). Δηλαδή *υπολογίζουμε δύο φορές τον αριθμό των μεταβολών προσήμου των ακολουθιών* Sseq(ℓ) *και* Sseq(r). Αυτό *μπορεί να αποφευχθεί, αλλά χάνεται η απλότητα του αλγορίθμου — κάτι που μας ενδιαφέρει περισσότερο εδώ*.

Ανάλυση του χρόνου υπολογισμού της μεθόδου του Sturm:
Όπως *αναφέραμε, η μέθοδος του* Sturm *είναι μία μέθοδος απομόνωσης των πραγματικών ριζών ενός πολυωνύμου* $p(x)$ *με διχοτόμηση*. Ο *αριθμός των διχοτομήσεων εξαρτάται από το πόσο κοντά είναι οι ρίζες του* $p(x)$. Αν *το* $p(x)$ *έχει* k *διαφορτικές ρίζες*, $\alpha_1, \ldots, \alpha_k$, $k \geq 2$, *ορίζουμε την* ***ελάχιστη απόσταση των ριζών*** (minimum root separation) *του* $p(x)$ *ως*

$$\Delta = \min_{1 \leq i < j \leq k} |\alpha_i - \alpha_j| > 0.$$

Αν $k = 1$, *τότε* $\Delta = \infty$. Όπως *θα δούμε στην ενότητα* 6.2.6, *αν* $n \geq 2$ *είναι ο βαθμός του πολυωνύμου* $p(x)$, *τότε ένα κάτω φράγμα στο* Δ *δίνεται από τον τύπο*:

$$\Delta \geq \sqrt{3} \cdot n^{-(n+2)/2} \cdot | p(x) |_1^{-(n-1)}.$$

Αντιστρέφοντας *την παραπάνω ανισότητα και παίρνοντας λογαρίθμους έχουμε*

$$\log \Delta^{-1} \leq \log 3^{-1/2} + \tfrac{n+2}{2} \log n + (n - 1) \log | p(x) |_1$$

ή

$$\log \Delta^{-1} = O(n \log n + n \log | p(x) |_\infty),$$

όπου αντί του $| p(x) |_1$ χρησιμοποιούμε το $| p(x) |_\infty$ που είναι της ίδιας τάξης μεγέθους. Επιπλέον, λαμβάνοντας υπ' όψη ότι το β-μήκος του βαθμού των πολυωνύμων για τις περιπτώσεις που εξετάζουμε είναι $\lambda(n) = 1$, ή $\log n = 1$, προκύπτει

$$\log \Delta^{-1} = O(n \log | p(x) |_\infty).$$

Επειδή η τάξη μεγέθους των λογαρίθμων ως προς οποιανδήποτε βάση είναι η ίδια, έπεται πως ισχύει

$$\log_2 \Delta^{-1} = O(n \log | p(x) |_\infty),$$

που σημαίνει πως η παραπάνω έκφραση είναι ένα ***πάνω φράγμα στον αριθμό των διχοτομήσεων*** που γίνονται για την απομόνωση των ριζών του πολυωνύμου $p(x)$ με την ελάχιστη απόσταση. Δηλαδή, για την απομόνωση των δύο πλησιέστερων ριζών του $p(x)$, ***ο αριθμός των διχοτομήσεων*** είναι περίπου όσο το γινόμενο του βαθμού του $p(x)$ επί τον αριθμό των ψηφίων του μεγαλύτερου συντελεστή του.

Ας δούμε τώρα τον χρόνο υπολογισμού κάθε βήματος του αλγορίθμου. Στο ***πρώτο βήμα*** υπολογίζουμε την ακολουθία Sturm του $p(x)$, Sseq(x), το κόστος της οποίας — όπως θα δούμε στο κεφάλαιο 7 — είναι $O(n^5 \log^2 | p(x) |_\infty)$.

Στο ***δεύτερο βήμα*** υπολογίζουμε ένα πάνω φράγμα b στις τιμές των θετικών ριζών του $p(x)$, το κόστος του οποίου — όπως θα δούμε στην ενότητα 6.2.5 — είναι $O(n)$.

Στο ***τρίτο βήμα*** εκτιμούμε την ακολουθία Sturm του $p(x)$, Sseq(x), σε διάφορα ρητά σημεία — που είναι είτε ακραία είτε μεσαία σημεία διαστημάτων. Έστω $\frac{a}{d}$, $d > 0$, μη μηδενικός, ***θετικός*** ρητός αριθμός και $p(x) = \sum_{i=0}^{n} c_i x^i$ τυχαίο πολυώνυμο μέλος της ακολουθίας Sseq(x). Τότε το πρόσημο του $p(\frac{a}{d})$ είναι το ίδιο με το πρόσημο του $\sum_{i=0}^{n} c_i a^i d^{n-i}$, το οποίο υπολογίζεται μόνο με αριθμητική ακεραίων! Από την ενότητα 4.1 ξέρουμε πως το κόστος ενός τέτοιου υπολογισμού με την μέθοδο Ruffini-Horner είναι $O(n^2 \log^2 e \log | p(x) |_\infty)$, όπου $e = \max(a, d)$ και $\log e \le |\log \Delta^{-1}| = O(n \log | p(x) |_\infty)$.

Συνεπώς, *ο χρόνος υπολογισμού* ***κάθε μιας*** *από τις εκτιμήσεις των πολυωνύμων της ακολουθίας* Sturm *του* $p(x)$, *σε ρητό σημείο είναι*

$$O(n^4 \log^2 | p(x) |_\infty).$$

Αν *τώρα λάβουμε υπ' όψη ότι*: **1ον**, *η ακολουθία* Sturm *του* $p(x)$, Sseq(x), *έχει* $n + 1$ *πολυώνυμα*, **2ον**, *για τις δύο πλησιέστερες ρίζες θα γίνουν το πολύ* $O(n \log | p(x) |_\infty)$ *διχοτομήσεις*, *και* **3ον**, *στην χειρότερη περίπτωση οι ρίζες ανά δύο — δηλαδή σύνολικά* $\frac{n}{2}$ *ζεύγη — θα βρίσκονται σε απόσταση* Δ, *τότε έπεται πως ο χρόνος απομόνωσης των πραγματικών ριζών του* $p(x)$ *με την μέθοδο διχοτόμησης του* Sturm *είναι*

$$O(n^7 \log^3 | p(x) |_\infty).$$

- **6.2.4 Διάσπαση πολυωνύμου σε παράγοντες ελεύθερους από τετράγωνα**

Ένα *πολυώνυμο* $p(x)$ *ονομάζεται* ***ελεύθερο από τετράγωνα*** (squarefree) *αν δεν υπάρχει πολυώνυμο* $q(x)$ *θετικού βαθμού έτσι ώστε το* $q^2(x)$ *να διαιρεί το* $p(x)$. Εκτός *από την απομόνωση των ριζών*, *η διαδικασία διάσπασης ενός πολυωνύμου σε παράγοντες ελεύθερους από τετράγωνα εφαρμόζεται και στην ολοκλήρωση ρητών συναρτήσεων*. Προτού *παρουσιάσουμε τον αλγόριθμο χρειαζόμαστε λίγη θεωρία*.

Θεώρημα:

Έστω J *μια περιοχή μοναδικής παραγοντοποίησης χαρακτηριστικής μηδέν και έστω* $p(x) \in J[x]$ *ένα μη σταθερό και* ***αρχέγονο*** (primitive) *πολυώνυμο* (*οι συντελεστές του είναι πρώτοι μεταξύ τους*). Έστω *επί πλέον*

$$p(x) = p_1^{e_1}(x) p_2^{e_2}(x) \cdots p_n^{e_n}(x)$$

η μοναδική παραγοντοποίηση του $p(x)$ *σε γινόμενο* ***μη αναγώγιμων*** (irreducible) *παραγόντων* (*όπου* $p_i^{e_i}(x)$ *συμβολίζει τον παράγοντα* $p_i(x)$ *υψωμένο στην δύναμη* e_i), *και* $p'(x)$ *η πρώτη παράγωγός του*. Τότε

$$\gcd(p(x), p'(x)) = p_1^{e_1-1}(x)\, p_2^{e_2-1}(x) \cdots p_n^{e_n-1}(x).$$

Απόδειξη:

Έστω $q(x) = \prod_{i=2}^{n} p_i^{e_i}(x)$ και $r(x) = \gcd(p(x), p'(x))$. Τότε έχουμε $p(x) = p_1^{e_1}(x)q(x)$ και

$$p'(x) = p_1^{e_1}(x)q'(x) + e_1 p_1^{e_1-1}(x)p_1'(x)q(x)$$

από όπου συνεπάγεται πως το $p_1^{e_1-1}(x)$ ***διαιρεί*** το $r(x)$. Με την εις άτοπο απαγωγή θα δείξουμε πως το $p_1^{e_1}(x)$ ***δεν διαιρεί*** το $r(x)$. Έστω λοιπόν πως το $p_1^{e_1}(x)$ διαιρεί το $r(x)$. Τότε το $p_1^{e_1}(x)$ διαιρεί την παράγωγο $p'(x)$, απ' όπου συνεπάγεται πως το $p_1^{e_1}(x)$ διαιρεί την έκφραση $e_1 p_1^{e_1-1}(x)p_1'(x)q(x)$. Μετά από απαλοιφή όμως προκύπτει ότι το $p_1(x)$ διαιρεί την έκφραση $e_1 p_1'(x)q(x)$. Επί πλέον, επειδή τα πολυώνυμα $p_i(x)$ είναι πρώτα μεταξύ τους, ισχύει $\gcd(p_1(x), q(x)) = 1$ και συνεπώς πρέπει το $p_1(x)$ να διαιρεί την έκφραση $e_1 p_1'(x)$. Αυτό όμως είναι αδύνατο διότι $\deg(p_1(x) > \deg(p_1'(x)$. Άρα στο $r(x)$ ο βαθμός του $p_1(x)$ είναι $e_1 - 1$ και λόγω συμμετρίας ισχύει $r(x) = p_1^{e_1-1}(x)\ p_2^{e_2-1}(x) \cdots p_n^{e_n-1}(x)$, πράγμα που θέλαμε να δείξουμε.//

Από το παραπάνω θεώρημα συμπεραίνουμε πως αν $\gcd(p(x), p'(x)) = 1$, τότε το $p(x)$ ***δεν έχει πολλαπλές ρίζες***, και αντίστροφα. Ισχύουν επίσης τα εξής:

Λήμμα 1:

Οι απλές ρίζες ενός πολυωνύμου δεν είναι ρίζες της παραγώγου του.

Λήμμα 2:

Έστω J σώμα και $p(x) \in J[x]$ ένα ***μη αναγώγιμο*** πολυώνυμο που διαιρεί το $s(x) \in J[x]$. Τότε το $p^2(x)$ διαιρεί το $s(x)$ εάν και μόνο εάν το $p(x)$ διαιρεί το $s'(x)$.

Απόδειξη:

Επειδή το $p(x)$ διαιρεί το $s(x)$ μπορούμε να γράψουμε $s(x) = p(x)q(x)$, απ' όπου προκύπτει $s'(x) = p'(x)q(x) + p(x)q'(x)$. Συνεπώς, αν το $p^2(x)$ διαιρεί το $s(x)$ τότε το $p(x)$ διαιρεί το $q(x)$ και προφανώς το $p(x)$ διαιρεί το $s'(x)$. Αντιστόφως, αν το $p(x)$ διαιρεί το $s'(x)$ τότε το $p(x)$ διαιρεί την έκφραση $p'(x)q(x)$, που συνεπάγεται πως το $p(x)$ διαιρεί είτε το $p'(x)$ είτε το $q(x)$ (***βλέπε άσκηση ??***). Επειδή όμως $\deg(p(x) > \deg(p'(x)$ έπεται πως το $p(x)$ διαιρεί το $q(x)$, και συνεπώς το $p^2(x)$ διαιρεί το $s(x)$.//

Ας *δούμε τώρα τον αλγόριθμο διάσπασης ενός πολυωνύμου σε παράγοντες ελεύθερους από τετράγωνα*.

Έστω J *μια περιοχή μοναδικής παραγοντοποίησης χαρακτηριστικής μηδέν και έστω* $p(x) \in J[x]$, *ένα αρχέγονο πολυώνυμο μιας μεταβλητής και θετικού βαθμού. Υποθέτουμε επί πλέον πως* $p(x) = p_1^{e_1}(x)p_2^{e_2}(x) \cdots p_n^{e_n}(x)$ *είναι η μοναδική παραγοντοποίηση του* $p(x)$ *σε γινόμενο* ***μη αναγώγιμων*** *παραγόντων* $p_i(x)$, *κάθε ένας των οποίων έχει θετικό βαθμό* $e_i > 0$. *Ορίζουμε* $e = \max(e_1, \ldots, e_n)$ *και για κάθε* $1 \le i \le e$,

$$J_i = \{j : e_j = i\}, \quad s_i(x) = \prod_{j \in J_i} p_j(x).$$

Προφανώς, ισχύει η σχέση

$$p(x) = \prod_{i=1}^{e} s_i^i(x)$$

η οποία ονομάζεται ***ανάλυση σε παράγοντες ελεύθερους από τετράγωνα*** (squarefree factorization). *Τα πολυώνυμα* $s_i(x)$ *είναι οι* ***παράγοντες οι ελεύθεροι από τετράγωνα*** (squarefree factors) *και μερικοί από αυτούς μπορεί να είναι ίσοι με την μονάδα. Το* $s_1(x)$ *είναι το γινόμενο όλων των παραγόντων με απλές ρίζες, το* $s_2(x)$ *είναι το γινόμενο όλων των παραγόντων με διπλές ρίζες, κοκ.*

Τα πολυώνυμα $s_i(x)$ *υπολογίζονται με την βοήθεια του θεωρήματος ως εξής: Πρώτα υπολογίζουμε το* $r(x)$, *τον μέγιστο κοινό διαιρέτη (μκδ) των* $p(x)$, *και* $p'(x)$

$$r(x) = \gcd(p(x), p'(x)) = \prod_{i=1}^{n} p_i^{e_i-1}(x) = \prod_{i=1}^{e} s_i^{i-1}(x),$$

όπου δεν εμφανίζεται το $s_1(x)$. *Κατόπιν, βρίσκουμε το* $t(x)$, *που είναι για το* $p(x)$ *ο μεγαλύτερος διαιρέτης του ελεύθερος από τετράγωνα*

$$t(x) = \frac{p(x)}{r(x)} = \prod_{i=1}^{n} p_i(x) = \prod_{i=1}^{e} s_i(x).$$

Τέλος, βρίσκοντας τον μκδ των $r(x)$ *και* $t(x)$

$$v(x) = \gcd(r(x), t(x)) = \prod_{i=2}^{e} s_i(x)$$

προκύπτει πως $s_1(x) = \frac{t(x)}{v(x)}$. *Δηλαδή ο πρώτος παράγοντας ελεύθερος από τετράγωνα,* $s_1(x)$, *βρίσκεται με παραγώγιση, υπολογισμούς μκδ και διαίρεση.*

Επαναλαμβάνοντας την παραπάνω διαδικασία με το $r(x)$ στον ρόλο του $p(x)$ βρίσκουμε τον δεύτερο παράγοντα ελεύθερο από τετράγωνα, $s_2(x)$, κοκ.

Προσοχή:
Αν ακολουθήσουμε την παραπάνω διαδικασία θα εκτελέσουμε **δύο** υπολογισμούς μκδ για κάθε παράγοντα $s_i(x)$. Επειδή όμως γνωρίζουμε την μορφή των πολυωνύμων $r(x)$ μπορούμε να εκτελέσουμε **έναν** υπολογισμό μκδ για κάθε παράγοντα $s_i(x)$ κάνοντας τις αντικαταστάσεις $r(x) \leftarrow \frac{r(x)}{v(x)}$ και $t(x) \leftarrow v(x)$. Έτσι ο αλγόριθμος είναι ως εξής:

Αλγόριθμος: Διάσπαση πολυωνύμου σε παράγοντες ελεύθερους από τετράγωνα.

Είσοδος: $p(x) \in J[x]$, ένα αρχέγονο πολυώνυμο θετικού βαθμού με συντελεστές από το J, μια περιοχή μοναδικής παραγοντοποίησης χαρακτηριστικής μηδέν.
Έξοδος: Η παραγοντοποίηση $p(x) = \prod_{i=1}^{e} s_i^i(x)$ σε παράγοντες ελεύθερους από τετράγωνα. Μερικά από τα πολυώνυμα $s_i(x)$ μπορεί να είναι ίσα με την μονάδα.

==========

1. (* έναρξη *)
sqfreefactorList = {}; $r(x) \leftarrow \gcd(p(x), p'(x))$; $t(x) \leftarrow \frac{p(x)}{r(x)}$.

2. (* υπολογισμός των $s_j(x)$ *)
Εφ' όσον ο βαθμός του $r(x)$ είναι μεγαλύτερος του μηδενός $\deg(r(x)) > 0$, **επαναλαμβάνουμε** την εξής διαδικασία: Υπολογίζουμε το $s_j(x)$ με τις εντολές $v(x) \leftarrow \gcd(r(x), t(x))$; $s_j(x) \leftarrow \frac{t(x)}{v(x)}$, το επισυνάπτουμε στην λίστα sqfreefactorList και ανανεώνουμε τα πολυώνυμα $r(x) \leftarrow \frac{r(x)}{v(x)}$ και $t(x) \leftarrow v(x)$. **Αλλιώς** επισυνάπτουμε στην λίστα sqfreefactorList το πολυώνυμο $t(x)$.

3. (* τέλος *)
Την λίστα sqfreefactorList την μετατρέπουμε κατόπιν στο γινόμενο $\prod_{i=1}^{e} s_i^i(x)$, όπου e ισούται με το μήκος της λίστας.
==========

Ακολουθεί ο παραπάνω αλγόριθμος εφαρμοσμένος στο *Mathematica*:

```
squareFreeFactors[f_] :=
 Module[{e, facList = {}, j = 1, r, s, sqfreefactorList = {},
   p = f, t, v, var = First[Variables[f]]},

  (*  step 1  *)
  r = PolynomialGCD[p, D[p, var]];
  t = PolynomialQuotient[p, r, var];

  (*  step 2  *)
  While[Exponent[r, var] > 0,
   v = PolynomialGCD[r, t];
   s = PolynomialQuotient[t, v, var];
   AppendTo[sqfreefactorList, s];
   r = PolynomialQuotient[r, v, var];
   t = v
  ];
  AppendTo[sqfreefactorList, t];

  (*  step 3  *)
  Map[(If[# =!= 1, AppendTo[facList, #^j]];
     j += 1) &, sqfreefactorList]; Apply[Times, facList]
 ]
```

Παράδειγμα:

Εφαρμόζοντας *τον αλγόριθμο* squareFreeFactors[] *στο πολυώνυμο* $p(x) = x^5 - x^4 - 2x^3 + 2x^2 + x - 1$ *προκύπτουν τα εξής ενδιάμεσα αποτελέσματα*:

Την ***πρώτη*** *φορά που εκτελείται ο βρόγχος* While[] , *ο βαθμός του* $p(x)$ *είναι* 5, $r(x) = x^3 - x^2 - x + 1$, $t(x) = x^2 - 1$, $v(x) = x^2 - 1$ *και* $s_1(x) = 1$, *που σημαίνει ότι δεν υπάρχουν παράγοντες πρώτου βαθμού*.

Την ***δεύτερη*** *φορά που εκτελείται ο βρόγχος* While[] , *ο βαθμός του* $p(x)$ *είναι* 3, $r(x) = x - 1$, $t(x) = x^2 - 1$, $v(x) = x - 1$ *και* $s_2(x) = x + 1$, *που σημαίνει ότι το* $(x + 1)^2$ *είναι παράγοντας δευτέρου βαθμού*.

Την ***τρίτη*** *— και τελευταία — φορά που εκτελείται ο βρόγχος* While[] , *ο βαθμός του* $p(x)$ *είναι* 1, $r(x) = 1$, $t(x) = x - 1$, $v(x) = 1$ *και* $s_3(x) = x - 1$, *που σημαίνει ότι το* $(x - 1)^3$ *είναι παράγοντας τρίτου βαθμού*.

Πράγματι, *το πολυώνυμο* $p(x) = x^5 - x^4 - 2x^3 + 2x^2 + x - 1$ *αναλύεται στο εξής γινόμενο παραγόντων ελεύθερων από τετράγωνα*:

```
p[x_] = x^5 - x^4 - 2 x^3 + 2 x^2 + x - 1; squareFreeFactors[p[x]]
```

```
(-1 + x)^3 (1 + x)^2
```

Το *αποτέλεσμα είναι το ίδιο με αυτό που προκύπτει χρησιμοποιώντας την συνάρτηση* FactorSquareFree[] *του Mathematica*.

```
FactorSquareFree[p[x]]
```

```
(-1 + x)^3 (1 + x)^2
```

***Ανάλυση του χρόνου υπολογισμού της παραγοντοποίησης σε παράγοντες ελεύθερους από τετράγωνα*:**
Είναι προφανές πως ο χρόνος υπολογισμού του αλγορίθμου αυτού καθορίζεται από τον χρόνο υπολογισμού των μκδ (gcd) στο 2ο βήμα. Επιπλέον, σημειώνουμε πως η πρώτη εκτέλεση του μκδ είναι και η πιο χρονοβόρα — από όλες τις άλλες.

Αν $n = \deg(p(x))$, τότε n είναι ένα πάνω φράγμα στον αριθμό εκτελέσεων του βρόγχου While[]. Διακρίνουμε 2 περιπτώσεις:

Περίπτωση 1η: Αν $p(x) \in J[x]$, και J είναι σώμα, τότε ο μκδ $\gcd(p(x), p'(x))$ υπολογίζεται σε χρόνο $O(n^2)$ και επομένως το 2ο βήμα — και συνεπώς ο αλγόριθμος — εκτελείται σε χρόνο $O(n^3)$.

Περίπτωση 2η: Αν $p(x) \in J[x]$, και $J = \mathbb{Z}$, τότε, όπως θα δούμε στο κεφάλαιο 7, ο μκδ $\gcd(p(x), p'(x))$ υπολογίζεται σε χρόνο $O(n^5 \log^2 | p(x) |_\infty)$ και επομένως το 2ο βήμα — και συνεπώς ο αλγόριθμος — εκτελείται σε χρόνο $O(n^6 \log^2 | p(x) |_\infty)$.

▪ 6.2.5 Πάνω και κάτω φράγμα στις τιμές των θετικών ριζών ενός πολυωνύμου

Στην ενότητα αυτή παρουσιάζουμε και αποδεικνύουμε το θεώρημα του Cauchy για την εύρεση ενός πάνω φράγματος στις τιμές των θετικών ριζών μιας πολυωνυμικής εξίσωσης $p(x) = 0$, με ακέραιους συντελεστές. Σημειώνουμε πως το σημαντικό αυτό αποτέλεσμα βρισκόταν ***μόνο*** στο βιβλίο του N. Obreschkoff στα **Γερμανικά** και πως πριν το 1978 δεν υπήρχε σε κανένα βιβλίο της Αγγλικής βιβλιογραφίας! Στην Αγγλική βιβλιογραφία, όπως αναφέραμε, υπήρχαν τύποι μόνο για την εύρεση ενός φράγματος στις απόλυτες τιμές των ριζών.

Εμείς χρησιμοποιούμε το θεώρημα του Cauchy και για την εύρεση ενός κάτω φράγματος στις τιμές των θετικών ριζών της $p(x) = 0$.

Θεώρημα (Cauchy):
Έστω $p(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = 0$ μία πολυωνυμική εξίσωση βαθμού $n > 0$, με **ακέραιους** συντελεστές και $c_{n-k} < 0$ για τουλάχιστον ένα k, $1 \le k \le n$. (Προσέξτε πως $c_n > 0$!) Αν λ είναι ο αριθμός των αρνητικών συντελεστών τότε

$$b = \max_{\{1 \le k \le n \,:\, c_{n-k} < 0\}} \sqrt[k]{-\frac{\lambda\, c_{n-k}}{c_n}}$$

είναι ένα πάνω φράγμα στις τιμές των θετικών ριζών της $p(x) = 0$.

Απόδειξη:
Από τον τρόπο ορισμού του b συνεπάγεται πως

$$b^k \ge \left(-\frac{\lambda\, c_{n-k}}{c_n}\right)$$

για κάθε k έτσι ώστε $c_{n-k} < 0$. Για αυτά τα k, η παραπάνω ανισότητα γράφεται και σαν

$$b^n \ge \left(-\frac{\lambda\, c_{n-k}}{c_n}\right) b^{n-k}.$$

Αθροίζοντας για όλα τα κατάλληλα k έχουμε

$$\lambda\, b^n \ge \lambda \sum_{1 \le k \le n \,:\, c_{n-k} < 0} \left(-\frac{c_{n-k}}{c_n}\right) b^{n-k}$$

ή

$$b^n \geq \sum_{1 \leq k \leq n \,:\, c_{n-k} < 0} \left(-\frac{c_{n-k}}{c_n} \right) b^{n-k}$$

Δηλαδή *αν διαιρέσουμε την* $p(x) = 0$ *με το* c_n, *κάνοντας μονάδα τον κύριο συντελεστή της, και αντικαταστήσουμε το* x *με το* b, $x \leftarrow b$, *τότε ο πρώτος όρος, δηλαδή το* b^n, *θα είναι* ***μεγαλύτερος από***, *ή* ***ίσος με***, *το άθροισμα των απόλυτων τιμών των όρων με αρνητικούς συντελεστές. Συνεπώς, για όλα τα* $x > b$, *το* $p(x) > 0$.//

Το *πάνω φράγμα* b *υπολογίζεται ευκολότατα από τον τύπο ορισμού του με το ακόλουθο πρόγραμμα στο Mathematica. Προσέξτε πως για να αποφύγουμε την περίπτωση της ισότητας στην έκφραση* $b^n \geq \sum_{1 \leq k \leq n \,:\, c_{n-k} < 0} \left(-\frac{c_{n-k}}{c_n} \right) b^{n-k}$, *στο τέλος του προγράμματος παίρνουμε σαν πάνω φράγμα την ποσότητα* $\lceil \frac{65}{64} b \rceil$.

```
CauchyPositiveRootUpperBound[p_] :=
 Module[{b = 0, cl, lc, lamda, n, cpos, tb},
cl = CoefficientList[p, Variables[p]];
  n = Length[cl]; lc = Last[cl];
  If[lc < 0, cl = -cl; lc = -lc];
lamda = Length[Select[cl, # < 0 &]];
  If[lamda == 0, Return[b]];
cpos = Position[cl, _?(# < 0 &)];
Do[tb = Sqrt[-lamda cl[[cpos[[k]]]]/lc, n-cpos[[k]]] // N // First;
   If[tb > b, b = tb], {k, lamda}]; Ceiling[65 / 64 b]]
```

Έτσι *βλέπουμε πως το* 3 *είναι ένα πάνω φράγμα στις τιμές των* ***θετικών*** *ριζών του* $p(x) = x^3 - 7x + 7$

```
p[x_] = x^3 - 7 x + 7;
CauchyPositiveRootUpperBound[p[x]]
```

```
3
```

ενώ το 4 *είναι ένα πάνω φράγμα στις τιμές των* ***αρνητικών*** *ριζών του* $p(x) = x^3 - 7x + 7$, *και βρίσκεται αντικαθιστώντας το* x *με το* $-x$, $x \leftarrow -x$.

```
CauchyPositiveRootUpperBound[p[-x]]
```

```
4
```

***Ανάλυση του χρόνου υπολογισμού ενός πάνω φράγματος στις τιμές των θετικών ριζών πολυωνύμου*:**

Είναι προφανές πως ο χρόνος υπολογισμού του αλγορίθμου αυτού καθορίζεται από τον χρόνο υπολογισμού των ριζών. Επειδή εδώ έχουμε αριθμητική κινητής υποδιαστολής, ένας υπολογισμός ριζικού εκτελείται σε χρόνο $O(1)$ και επομένως το πολύ n τέτοιοι υπολογισμοί εκτελούνται σε χρόνο $O(n)$.

Όπως θα δούμε στην ενότητα 6.3, στην μέθοδο απομόνωσης των ριζών με συνεχή κλάσματα θα χρειαστούμε και κάτω φράγματα στις τιμές των θετικών ριζών ενός πολυωνύμου $p(x)$. Αυτό το κάτω φράγμα στις τιμές των θετικών ριζών του $p(x)$ θα μπορούσε να βρεθεί ***αντιστρέφοντας*** το πάνω φράγμα στις τιμές των θετικών ριζών της πολυωνυμικής εξίσωσης $x^n \cdot p(\frac{1}{x}) = 0$, όπου $n = \deg(p(x))$.

Αντ' αυτού όμως παρουσιάζουμε έναν διαφορετικό αλγόριθμο, όπου δουλεύουμε με τους συντελεστές του $x^n \cdot p(\frac{1}{x})$, παίρνοντας τώρα σαν κύριο συντελεστή, lc = First[cl] — αντί του lc = Last[cl] που χρησιμοποιούσαμε για το πάνω φράγμα. Επί πλέον, προσέξτε πως στο τέλος το όριο είναι $2^{-\lceil \log_2 b \rceil}$.

```
CauchyPositiveRootLowerBound[p_] :=
 Module[{b = 0, cl, lc, lamda, n, cpos, tb},
cl = CoefficientList[p, Variables[p]];
  n = Length[cl]; lc = First[cl];
  If[lc < 0, cl = -cl; lc = -lc];
lamda = Length[Select[cl, # < 0 &]];
  If[lamda == 0, Return[b]];
cpos = Position[cl, _?(# < 0 &)];
Do[tb = Sqrt[-lamda cl[[cpos[[k]]]]/lc, cpos[[k]]-1] // N // First;
   If[tb > b, b = tb], {k, lamda}]; 2^(-Ceiling[Log[2, b]])]
```

Έτσι βλέπουμε πως το 1 είναι τόσο ένα κάτω φράγμα στις τιμές των ***θετικών*** ριζών του $p(x) = x^3 - 7x + 7$

```
p[x_] = x^3 - 7 x + 7;
CauchyPositiveRootLowerBound[p[x]]
```

```
1
```

όσο και ένα κάτω φράγμα στις τιμές των **αρνητικών** ριζών του $p(x) = x^3 - 7x + 7$, και βρίσκεται αντικαθιστώντας το x με το $-x$, $x \leftarrow -x$.

```
CauchyPositiveRootLowerBound[p[-x]]
```

```
1
```

■ 6.2.6 Κάτω φράγμα στην απόσταση μεταξύ δύο τυχαίων ριζών ενός πολυωνύμου

Στην ενότητα αυτή θα παρουσιάσουμε το θεώρημα του K. Mahler (1964) για τον υπολογισμό ενός κάτω φράγματος στην **ελάχιστη απόσταση Δ των ριζών** ενός πολυωνύμου $p(x)$. Το αποτέλεσμα αυτό είναι σημαντικότατο γιατί χρησιμοποιείται στην ανάλυση του χρόνου υπολογισμού όχι μόνο της μεθόδου Sturm αλλά και κάθε άλλης μεθόδου απομόνωσης των πραγματικών ριζών ενός πολυωνύμου.

Για την απόδειξη του θεωρήματος του Mahler χρειαζόμαστε το θεώρημα του Hadamard για τις ορίζουσες, το οποίο παρουσιάζουμε χωρίς απόδειξη, τους ορισμούς της διακρίνουσας και του μέτρου ενός πολυωνύμου, και τέλος την ανισότητα του Landau.

Θεώρημα (Hadamard, για ορίζουσες):
Αν τα στοιχεία d_{ij}, $i,j = 1, 2, \ldots, n$ του πίνακα

$$m = \begin{pmatrix} d_{11} & \ldots & d_{1n} \\ \vdots & \ddots & \vdots \\ d_{n1} & \ldots & d_{nn} \end{pmatrix}$$

είναι τυχαίοι μιγαδικοί αριθμοί, τότε για την ορίζουσα $d = \det(m)$ ισχύει η ανισότητα:

$$|d| \le \sqrt{\prod_{j=1}^{n} \left(\sum_{i=1}^{n} |d_{ij}|^2\right)}. \qquad \text{(H)}$$

Η ισότητα ισχύει εάν και μόνο εάν

$$\sum_{i=1}^{n} d_{ij}\,\overline{d}_{ik} = 0, \quad \text{για } 1 \le j < k \le n,$$

όπου $\overline{d}_{ik}$ ειναι ο συζυγής μιγαδικός του d_{ik}.

Ορισμός (*διακρίνουσας*):

Η ***διακρίνουσα*** (discriminant), discr($p(x)$), *ενός πολυωνύμου* $p(x) = c_n \prod_{i=1}^{n} (x - \alpha_i)$ *ορίζεται από την σχέση*

$$\text{discr}(p(x)) = c_n^{2\,n-2} \prod_{i=1}^{n} \prod_{j=i+1}^{n} (\alpha_i - \alpha_j)^2, \qquad \text{(D)}$$

η οποία γενικεύει τον τύπο $b^2 - 4ac$, *της διακρίνουσας πολυωνύμου δευτέρου βαθμού*. (*Προσέξτε πως* c_n *είναι ο συντελεστής του* x^n.)

Τονίζουμε πως η διακρίνουσα μας δίνει ένα μέτρο του πόσο κοντά είναι οι ρίζες του πολυωνύμου $p(x)$.

Ορισμός (*μέτρου ενός πολυωνύμου*):

Έστω $p(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = c_n \prod_{i=1}^{n} (x - \alpha_i) \in \mathbb{C}[x]$, *ένα πολυώνυμο με μιγαδικούς συντελεστές*, $c_n \neq 0$, *και ρίζες* α_i. *Το* ***μέτρο*** *του* $p(x)$, $\mu(p(x))$, *ορίζεται από τον τύπο*

$$\mu(p(x)) = |c_n| \prod_{i=1}^{n} \max(1, \ |\alpha_i|). \qquad (\mu)$$

Επιπλέον ισχύει και ***η ανισότητα του*** **Landau (1905)**

$$\mu(p(x)) \leq \ |p(x)|_2 \leq \ |p(x)|_1 \qquad \text{(L)}$$

όπου $|p(x)|_2$ *είναι η Ευκλείδεια νορμ*. *Την ανισότητα του* Landau *θα χρησιμοποιήσουμε στο ακόλουθο*:

Θεώρημα (Mahler, 1964):

Έστω $p(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$, *ένα πολυώνυμο βαθμού* $n \geq 2$, *μιας μεταβλητής*, *ελεύθερο από τετράγωνα*, *και με ακέραιους συντελεστές*. *Αν* Δ *είναι ελάχιστη απόσταση των ριζών του* $p(x)$, *τότε ισχύει η ανισότητα*

$$\Delta \geq \sqrt{3}\ n^{-(n+2)/2}\ |p(x)|_1^{-(n-1)}, \qquad \text{(M)}$$

όπου $|p(x)|_1$ *είναι η αθροιστική νορμ του* $p(x)$ — *δηλαδή το άθροισμα των απολύτων τιμών των συντελεστών*.

Απόδειξη:

Έστω ότι $\alpha_1, \alpha_2, \ldots, \alpha_n$ *είναι οι ρίζες του* $p(x)$. *Τις αριθμούμε έτσι ώστε*

$$|\alpha_1| \geq |\alpha_2| \geq \cdots \geq |\alpha_N| > 1 \geq |\alpha_{N+1}| \geq \cdots \geq |\alpha_n|$$

και ορίζουμε την ορίζουσα

$$\mathrm{vdm}(p(x)) = \prod_{i=1}^{n} \prod_{j=i+1}^{n} (\alpha_i - \alpha_j),$$

με την συνθήκη $\mathrm{vdm}(p(x)) = 1$, *για την* ***μη επιτρεπτή*** *περίπτωση* $n = 2$. Από *την ενότητα* 4.2 *του πρώτου τόμου*, *θυμόμαστε πως* $\mathrm{vdm}(p(x))$ *είναι η ορίζουσα του πίνακα* Vandermonde

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \dots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{pmatrix}.$$

Επιπλέον *ορίζουμε την* $\mathrm{vdm}^*(p(x)) = (\alpha_1\alpha_2 \cdots \alpha_N)^{-(n-1)}\mathrm{vdm}(p(x))$ *που είναι η ορίζουσα του πίνακα*

$$\begin{pmatrix} \alpha_1^{-(n-1)} & \alpha_1^{-(n-2)} & \alpha_1^{-(n-3)} & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_N^{-(n-1)} & \alpha_N^{-(n-2)} & \alpha_N^{-(n-3)} & \cdots & 1 \\ 1 & \alpha_{N+1} & \alpha_{N+1}^2 & \cdots & \alpha_{N+1}^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

Δηλαδή, *ο τελευταίος πίνακας προκύπτει αφού πολλαπλασιάσουμε την i-στή σειρά του πίνακα* Vandermonde *επί* $\alpha_i^{-(n-1)}$, $1 \leq i \leq N$. Επειδή *η απόλυτος τιμή κάθε στοιχείου στον τελευταίο πίνακα είναι* ≤ 1 *έπεται από την ανισότητα* (H) *του* Hadamard *πως*

$$|\mathrm{vdm}^*(p(x))| \leq \sqrt{n^n} = n^{n/2}.$$

Εδώ *η ισότητα ισχύει αν*

$$|\alpha_1| = |\alpha_2| = \cdots = |\alpha_n| = 1$$

και

$$\sum_{k=0}^{n-1} \overline{\alpha}_i^k \alpha_j^k = 0, \quad \gamma\iota\alpha\ 1 \leq i < j \leq n.$$

Για $i = 1$ (*και απαλείφοντας τον παρανομαστή του αντιστρόφου* α_1^{-1}) *το παραπάνω άθροισμα γίνεται*

$$\sum_{k=0}^{n-1} \overline{\alpha}_1^k \alpha_j^k = \sum_{k=0}^{n-1} (\alpha_1^{-1} \alpha_j)^k = \frac{(\frac{\alpha_j}{\alpha_1})^n - 1}{\frac{\alpha_j}{\alpha_1} - 1} = 0.$$

Πολλαπλασιάζοντας την τελευταία έκφραση με $\frac{\alpha_j}{a_1} - 1$, *προκύπτει* $\left(\frac{\alpha_j}{\alpha_1}\right)^n = 1$, *απ' όπου βλέπουμε πως τα* $\frac{\alpha_j}{\alpha_1}$, $1 \le j \le n$, *είναι οι n διαφορετικές ρίζες της εξίσωσης* $x^n - 1 = 0$. *Επομένως,*

$$x^n - 1 = \prod_{j=1}^{n} \left(x - \frac{\alpha_j}{\alpha_1}\right)$$

ή

$$\alpha_1^n x^n - \alpha_1^n = \prod_{j=1}^{n} (x - \alpha_j).$$

Άρα, $|\mathrm{vdm}^*(p(x))| = \sqrt{n^n} = n^{n/2}$ *μόνο στην περίπτωση που* $p(x) = c_n x^n + c_0$, *και* $|c_n| = |c_0| \neq 0$.

Έστω τώρα r,s έτσι ώστε $1 \le r < s \le n$. *Θα βρούμε ένα πάνω φράγμα στην έκφραση* $|\frac{\mathrm{vdm}^*(p(x))}{\alpha_r - \alpha_s}|$ *και με την βοήθειά του θα αποδείξουμε το θεώρημα.*

Στον πίνακα Vandermonde *αφαιρούμε την s-στή σειρά από την r-στή σειρά και το αποτέλεσμα είναι η* ***νέα*** *σειρά r, που αποτελείται από τα στοιχεία*

$$0, \alpha_r - \alpha_s, \alpha_r^2 - \alpha_s^2, \ldots, \alpha_r^{n-1} - \alpha_s^{n-1}$$

τα οποία είναι όλα τους πολλαπλάσια του $\alpha_r - \alpha_s$. *Διαιρούμε την σειρά r με* $\alpha_r - \alpha_s$ *και έστω* $q_0, q_1, \ldots, q_{n-1}$ *τα νέα στοιχεία της σειράς αυτής, όπου* $q_0 = 0$, *και* $q_i = \frac{\alpha_r^i - \alpha_s^i}{\alpha_r - \alpha_s} = \sum_{k=0}^{i-1} \alpha_r^{i-1-k} \alpha_s^k$, $1 \le i \le n - 1$. *Η ορίζουσα του* ***νέου πίνακα*** *— που διαφέρει από τον αρχικό ως προς την σειρά r — είναι προφανώς* $\frac{\mathrm{vdm}(p(x))}{\alpha_r - \alpha_s}$. *Αν στην συνέχεια, στον νέο αυτό πίνακα διαιρέσουμε — όπως και πριν — την 1η, 2η, …, N-στή σειρά με τους όρους* $\alpha_1^{n-1}, \alpha_2^{n-1}, \ldots, \alpha_N^{n-1}$, *αντίστοιχα, προκύπτει πίνακας η ορίζουσα του οποίου είναι* $\frac{\mathrm{vdm}^*(p(x))}{\alpha_r - \alpha_s}$! *Στον νέο αυτό πίνακα η r-στή σειρά αποτελείται από τα στοιχεία*

$$q_0 \alpha_r^{-(n-1)}, q_1 \alpha_r^{-(n-1)}, \ldots, q_{n-1} \alpha_r^{-(n-1)}$$

αν $r \le N$, *ή από τα στοιχεία*

$q_0, q_1, \ldots, q_{n-1}$

αν $r > N$. *Επειδή δε* $|\alpha_r| \geq |\alpha_s|$ *και* $|\alpha_r| = \begin{cases} >1 & \text{για } r \leq N \\ <1 & \text{για } r > N \end{cases}$, *έπεται πως οι απόλυτες τιμές των διαδοχικών στοιχείων της r-στής σειράς του νέου πίνακα δεν υπερβαίνουν τις τιμές* 0, 1, 2, …, *n* - 2, *n* - 1, *αντίστοιχα*. Αυτό "*αποδεικνύεται*" *και με το Mathematica με την χρήση της συνάρτησης* Assuming[] — *όπου αντί για* α_r *και* α_s *χρησιμοποιούμε a και b*:

```
(*  r ≤ N  *)
Clear[n, i]; n = 10; answer = {};
Do[Assuming[a ∈ Reals && b ∈ Reals && Abs[a] > Abs[b] &&
   Abs[a] > 1 && i ∈ Integers && i > 1,
  AppendTo[answer, Refine[a^-(n-1) Sum[a^(i-1-k) b^k ≤ i, {k, 0, i-1}]]], {i, 2, n}]; answer
```

```
{True, True, True, True, True, True, True, True, True}
```

```
(*  r > N  *)
Clear[n, i]; n = 10; answer = {};
Do[Assuming[a ∈ Reals && b ∈ Reals && Abs[a] > Abs[b] &&
   Abs[a] < 1 && i ∈ Integers && i > 1,
  AppendTo[answer, Refine[Sum[a^(i-1-k) b^k ≤ i, {k, 0, i-1}]]], {i, 2, n}]; answer
```

```
{True, True, True, True, True, True, True, True, True}
```

Οσον αφορά τις απόλυτες τιμές των διαδοχικών στοιχείων των υπόλοιπων *n* - 1 *σειρών του νέου πίνακα — εκτός r-στής σειράς — αυτές δεν υπερβαίνουν την μονάδα*. Επομένως, *από την ανισότητα* (H) *του* Hadamard *έχουμε*

$$\left| \frac{\mathrm{vdm}^*(p(x))}{\alpha_r - \alpha_s} \right|^2 \leq (n-1)^{n-1} \sum_{i=0}^{n-1} i^2 < n^{n-1} \sum_{i=0}^{n-1} i^2.$$

όπου το άθροισμα $\sum_{i=0}^{n-1} i^2$ *είναι μόνο για την r-στή σειρά και ο πρώτος όρος* $(n-1)^{n-1} = \prod_{j=0}^{n-2} (\sum_{i=0}^{n-2} 1)$ *είναι για τις υπόλοιπες*. Επειδή όμως *το άθροισμα* $\sum_{i=0}^{n-1} i^2 = \frac{n(n-1)(2n-1)}{6}$, *προκύπτει*

$$\left| \frac{\mathrm{vdm}^*(p(x))}{\alpha_r - \alpha_s} \right|^2 < \frac{n^{n+2}}{3}.$$

Λύνουμε την παραπάνω ανισότητα ως προς $|\alpha_r - \alpha_s|^2$ *και έχουμε*

$$| \alpha_r - \alpha_s |^2 > 3\, n^{-(n+2)} \, | \mathrm{vdm}^* (p(x)) |^2,$$

ή

$$| \alpha_r - \alpha_s |^2 > 3\, n^{-(n+2)} (\alpha_1 \alpha_2 \cdots \alpha_N)^{-2(n-1)} \, | \mathrm{vdm}(p(x)) |^2.$$

ή

$$| \alpha_r - \alpha_s |^2 > 3\, n^{-(n+2)} (c_n \alpha_1 \alpha_2 \cdots \alpha_N)^{-2(n-1)} \, c_n^{2n-2} \, | \mathrm{vdm}(p(x)) |^2.$$

Από *τους τύπους* (μ) *του μέτρου και* (D) *της διακρίνουσας βλέπουμε πως η παραπάνω ανισότητα γράφεται και σαν*

$$| \alpha_r - \alpha_s |^2 > 3\, n^{-(n+2)} \, (\mu(p(x)))^{-2(n-1)} \, c_n^{2n-2} \mathrm{discr}(p(x)).$$

Επειδή *οι συντελεστές του* $p(x)$ *είναι ακέραιοι*, $|\mathrm{discr}(p(x))| \geq 1$. Επιπλέον *επιλέγοντες τους δείκτες* r, s *έτσι ώστε* $\Delta = | \alpha_r - \alpha_s |$ *και χρησιμοποιούντες την ανισότητα του* Landau (L) *αποδεικνύεται η ζητούμενη ανισότητα* (M).//

Παράδειγμα:

Για *το πολυώνυμο* $p(x) = x^3 - 7x + 7$ *βλέπουμε πως*

$$\Delta \geq \sqrt{3}\; 3^{-5/2}\, 15^{-2} = \frac{\sqrt{3}}{\sqrt{3^5}\; 15^2} \approx 0.000493827.$$

Αυτό *σημαίνει πως οι ρίζες του* $p(x)$ *δεν μπορούν να έχουν απόσταση μικρότερη από* 0.000493827.

6.3 Το *θεώρημα του* Budan *και η μέθοδος των* Vincent-Akritas-Strzebonski *για την απομόνωση πραγματικών ριζών με συνεχή κλασματα*

Στην προηγούμενη ενότητα εξετάσαμε το θεώρημα του Fourier, από το οποίο απορρέουν το θεώρημα του Sturm και η μέθοδος του Sturm για την απομόνωση πραγματικών ριζών με διχοτόμηση. Η μέθοδος αυτή ήταν η πρώτη που αναπτύχθηκε και αποτέλεσε σταθμό στην ιστορία των μαθηματικών. Χρησιμοποιήθηκε πολύ μέχρι το 1976.

Όμως το 1975/76 — με τροποποίηση του θεωρήματος του Vincent που μόλις είχε ανακαλύψει ο γράφων — αναπτύχθηκε η μέθοδος των Collins-Akritas για την απομόνωση πραγματικών ριζών με διχοτόμηση. Η μέθοδος αυτή — που είναι πολύ πιο γρήγορη από την μέθοδο του Sturm — εφαρμόσθηκε στο σύστημα υπολογιστικής άλγεβρας maple, και έκτοτε χρησιμοποιείται ευρέως. Με το πέρασμα του χρόνου αποδείχθηκε πως ***η μέθοδος των* Collins-Akritas *είναι η πιο γρήγορη μέθοδος για την απομόνωση πραγματικών ριζών με διχοτόμηση.***

Στην ενότητα αυτή θα εξετάσουμε το θεώρημα του Budan από το οποίο απορρέουν το θεώρημα του Vincent και η μέθοδος των Vincent-Akritas-Strzebonski για την απομόνωση πραγματικών ριζών με συνεχή κλάσματα. Ο Vincent (1836) ήταν ο πρώτος που ανέπτυξε την μέθοδο των συνεχών κλασμάτων αλλά ο χρόνος υπολογισμού της μεθόδου του ήταν εκθετικός. Στην συνέχεια ο γράφων βελτίωσε την μέθοδο αυτή (1978) και την έκανε όχι μόνο πολυωνυμική, αλλά και την ***πιο γρήγορη μέθοδο απομόνωσης πραγματικών ριζών στον κόσμο***. Με τον Strzebonski (1994) βελτιώθηκε η μέθοδος ως προς ένα ακόμα σημείο.

▪ 6.3.1 Το *θεώρημα του* Budan

Όπως *έχουμε αναφέρει το θεώρημα του* Budan *εμφανίστηκε πριν από το θεώρημα του* Fourier, *αλλά παρά όλα αυτά είχε ξεχαστεί. Στην βιβλιογραφία αναφερόταν μεν το όνομα* Budan *αλλά η διατύπωση του θεωρήματος ήταν εκείνη του* Fourier. *Ο γράφων βρήκε την διατύπωση του θεωρήματος του* Budan *στο άρθρο του* Vincent *του* 1836 *και την παρουσιάζει — λίγο διασκευασμένα — σε αναλογία με το θεώρημα του* Fourier:

Θεώρημα του Budan (1807): (Υπολογισμός *ενός πάνω φράγματος στον αριθμό των πραγματικών ριζών που έχει μία εξίσωση σε ένα ανοιχτό διάστημα*.)

Στην πολυωνυμική εξίσωση $p(x) = 0$, *βαθμού* $n > 0$, *κάνουμε τις δύο αντικαταστάσεις*, $x \leftarrow x + \ell$ *και* $x \leftarrow x + r$, *όπου* ℓ *και* r *είναι πραγματικοί αριθμοί έτσι ώστε* $\ell < r$. *Αν* v_ℓ *και* v_r *είναι οι μεταβολές προσήμου στις ακολουθίες των συντελεστών των πολυωνύμων* $p(x + \ell)$ *και* $p(x + r)$, *αντίστοιχα*, *τότε ισχύουν τα ακόλουθα*:

i. *Το πολυώνυμο* $p(x + \ell)$ *δεν μπορεί να έχει λιγότερες μεταβολές προσήμου από το πολυώνυμο* $p(x + r)$. *Δηλαδή*, $v_\ell \geq v_r$.
ii. *Ο αριθμός* ρ *των πραγματικών ριζών της εξίσωσης* $p(x) = 0$ *που βρίσκονται στο διάστημα* (ℓ, r) *ποτέ δεν μπορεί να είναι μεγαλύτερος από τον αριθμό των μεταβολών προσήμου που χάνονται κατά την μετάβασή μας από το πολυώνυμο* $p(x + \ell)$ *στο πολυώνυμο* $p(x + r)$. *Δηλαδή*, $\rho \leq v_\ell - v_r$.
iii. *Όταν ο αριθμός* ρ *των πραγματικών ριζών της εξίσωσης* $p(x) = 0$ *που βρίσκονται στο διάστημα* (ℓ, r) *είναι γνήσια μικρότερος από τον αριθμό των μεταβολών προσήμου που χάνονται κατά την μετάβασή μας από το πολυώνυμο* $p(x + \ell)$ *στο πολυώνυμο* $p(x + r)$, *τότε η διαφορά είναι άρτιος αριθμός. Δηλαδή*, $\rho = v_\ell - v_r - 2\lambda$, *όπου* $\lambda \in \mathbb{Z}_{>0}$.

Ισοδυναμία:
Το *θεώρημα του* Budan *είναι* ***ισοδύναμο*** *με το θεώρημα του* Fourier. *Αυτό φαίνεται από το γεγονός ότι για το πολυώνυμο* $p(x)$, *βαθμού* $n > 0$, *στην ακολουθία* Fseq(t) (*που προκύπτει από την αντικατάσταση* $x \leftarrow t$) *οι* $n + 1$ *αριθμοί* ***έχουν το ίδιο πρόσημο***, *και είναι ανάλογοι με τους αντίστοιχους*

συντελεστές του πολυωνύμου $p(x + t) = \sum_{i=0}^{n} \frac{p^{(i)}(t)}{i!} x^i$, *όπως προκύπτουν από τον μετασχηματισμό* Taylor — *ή την αντικατάσταση* $x \leftarrow x + t$.

Επομένως, *το θεώρημα του* Budan *μας δίνει επίσης ένα* ***πάνω φράγμα*** *στον αριθμό των πραγματικών ριζών που έχει η εξίσωση* $p(x) = 0$ *μέσα στο διάστημα* (ℓ, r). *Προσέξτε όμως πως αντί για ακολουθίες παραγώγων χρησιμοποιούνται οι αντικαταστάσεις* $x \leftarrow x + \ell$ *και* $x \leftarrow x + r$. *Οι αντικαταστάσεις αυτές ονομάζονται* **Möbius** *ή* ***γραμμικές κλασματικές αντικαταστάσεις*** *και στην επόμενη υποενότητα εξετάζουμε την επίδρασή τους στις ρίζες των πολυωνύμων*.

Προσοχή:
Με *τις αντικαταστάσεις* $x \leftarrow x + \ell$ *και* $x \leftarrow x + r$ *μπορούμε να βρούμε τον ακριβή αριθμό των ριζών στο διάστημα* (ℓ, r) *μόνο στις εξής* ***δύο*** *περιπτώσεις*: **(*α*)** *αν δεν χάνεται καμία μεταβολή προσήμου τότε δεν υπάρχει καμία ρίζα στο* (ℓ, r), *και* **(*β*)** *αν χάνεται μία μεταβολή προσήμου τότε υπάρχει μία πραγματική ρίζα στο* (ℓ, r). **Τα *αντίστροφα των* (*α*) *και* (*β*) *δεν ισχύουν***!

Παράδειγμα: (*υπολογισμός ενός πάνω φράγματος στον αριθμό των πραγματικών ριζών μέσα σε ένα διάστημα με την βοήθεια του θεωρήματος του* Budan)
Έστω *πάλι το πολυώνυμο* $p(x) = x^3 - 7x + 7$. *Για να βρούμε, με το θεώρημα του* Budan, *ένα πάνω φράγμα στον αριθμό των πραγματικών ριζών που έχει το πολυώνυμο αυτό στο διάστημα* (0, 2) *υπολογίζουμε την διαφορά των μεταβολών προσήμου στα πολυώνυμα* $p(x + 0)$ *και* $p(x + 2)$:

```
p[x_] = x^3 - 7 x + 7; variations[p[x + 0]] - variations[p[x + 2]]
```

```
2
```

Δηλαδή χάνονται δύο μεταβολές προσήμου, και αυτό σημαίνει πως στο διάστημα (0, 2) *το πολυώνυμο είτε έχει δύο πραγματικές ρίζες ή καμία, κάτι που πρέπει να διερευνηθεί. Υπενθυμίζουμε πως οι συντελεστές του πολυωνύμου που προκύπτει από την αντικατάσταση* $x \leftarrow x + \alpha$ *υπολογίζονται με την μέθοδο των* Rufini-Horner *που εξετάσαμε στην ενότητα* 4.1 *του πρώτου τόμου*.

▪ 6.3.2 Αντικαταστάσεις Möbius και η επίδρασή τους στις ρίζες πολυωνυμικών εξισώσεων

Όπως θα δούμε στην επόμενη υποενότητα 6.3.3, σημαντικότατο ρόλο στο θεώρημα του Vincent παίζουν οι αντικαταστάσεις της μορφής $x \leftarrow \alpha + \frac{1}{x}$. Οι αντικαταστάσεις αυτές ανήκουν στην κατηγορία των ***γραμμικών κλασματικών αντικαταστάσεων*** ή ***αντικαταστάσεων* Möbius**, που ονομάστηκαν έτσι προς τιμήν του A.F. Möbius (1790-1868) ο οποίος πρώτος τις μελέτησε στην προβολική γεωμετρία.

Ορισμός:

Ονομάζουμε ***αντικατάσταση* Möbius** την έκφραση

$$x \leftarrow \mathrm{M}(x) = \frac{a\,x + b}{c\,x + d},$$

όπου a, b, c, d είναι μιγαδικοί αριθμοί έτσι ώστε η ορίζουσά τους είναι διάφορη του μηδενός — δηλαδή έχουμε $ad - bc \neq 0$. Την αντικατάσταση αυτή συμβολίζουμε ως $x \leftarrow \mathrm{M}(x)$, $\det(\mathrm{M}) \neq 0$.

Για τυχαίο $x \in \mathbb{C}$, η αντικατάσταση $x \leftarrow \mathrm{M}(x)$ ορίζεται από την έκφραση του ορισμού, με την προϋπόθεση ότι $cx + d \neq 0$. Αλλιώς, ορίζουμε $\mathrm{M}(\frac{-d}{c}) = \infty$. Αν $c = 0$, τότε πρέπει να έχουμε $ad \neq 0$ — επειδή η ορίζουσα πρέπει να είναι διάφορη του μηδενός — και η αντικατάσταση ορίζεται από την έκφραση

$$x \leftarrow \mathrm{M}(x) = \frac{a}{d}\,x + \frac{b}{d}.$$

Προσέξτε πως στην περίπτωση $c = 0$ ισχύει $\mathrm{M}(\infty) = \infty$, ενώ αν $c \neq 0$, τότε $\mathrm{M}(\infty) = \frac{a}{c}$.

Είναι προφανές ότι σε κάθε αντικατάσταση Möbius ***αντιστοιχεί*** ο τετράγωνος πίνακας των συντελεστών του, και αυτό πλήρως ορίζει την αντικατάσταση. Ορίζουμε λοιπόν

$$\boldsymbol{\mathcal{M}} = \{\mathrm{M}(x) : x \leftarrow \mathrm{M}(x),\ \mathrm{M} = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix},\ \det(\mathrm{M}) \neq 0,\ x \in \mathbb{C}\},$$

το σύνολο όλων των αντικαταστάσεων Möbius και $\mathbb{C}' = \mathbb{C} \cup \{\infty\}$, το συμπαγές μιγαδικό επίπεδο.

Προσοχή:

Στην συνέχεια ο συμβολισμός $\begin{pmatrix} a & b \\ c & d \end{pmatrix}(x)$ **υπονοεί** την σχέση:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(x) = \frac{a\,x+b}{c\,x+d}.$$

Θεώρημα:

Το σύνολο $\boldsymbol{\mathcal{M}}$ των αντικαταστάσεων Möbius αποτελεί ομάδα ισομορφική με την ομάδα τετραγώνων πινάκων τάξης 2.

Απόδειξη:

Στο σύνολο $\boldsymbol{\mathcal{M}}$ εισάγουμε κατ' αρχάς μια σχέση **ισότητας** ως εξής: Δύο αντικαταστάσεις $A(x), B(x) \in \boldsymbol{\mathcal{M}}$ ταυτίζονται, δηλαδή $\forall x \in \mathbb{C}'$ ισχύει $A(x) = B(x)$, εάν και μόνο εάν $\exists \lambda \in \mathbb{C}$, $\lambda \neq 0$, έτσι ώστε $A = \lambda B$ — όπου η τελευταία είναι ισότητα πινάκων.

Ο λόγος που ορίζουμε την ισότητα έτσι είναι διότι αν σε ένα πολυώνυμο $p(x)$ κάνουμε την αντικατάσταση $x \leftarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}(x)$ ή την αντικατάσταση $x \leftarrow \lambda\begin{pmatrix} a & b \\ c & d \end{pmatrix}(x)$ το αποτέλεσμα είναι το ίδιο. Αυτό φαίνεται από το ακόλουθο παράδειγμα όπου κάνουμε τις αντικαταστάσεις $x \leftarrow \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}(x)$ και $x \leftarrow 3\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}(x)$ στο πολυώνυμο $p(x) = x^3 - 7x + 7$. Προσέξτε πως για να αποφύγουμε ρητές εκφράσεις πολλαπλασιάζουμε επί $(x+1)^3$.

```
Clear[p]; p[x_] = x^3 - 7 x + 7; p[1/(1 + x)] (x + 1)^3 // Simplify
```

$$1 + 7x + 14x^2 + 7x^3$$

```
p[3/(3 + 3 x)] (x + 1)^3 // Simplify
```

$$1 + 7x + 14x^2 + 7x^3$$

Κατόπιν ορίζουμε το **γινόμενο** δύο αντικαταστάσεων $A(x), B(x) \in \boldsymbol{\mathcal{M}}$ ως το γινόμενο των πινάκων τους $AB(x)$. Προσέξτε όμως τον **τρόπο εφαρμογής** του γινομένου αντικαταστάσεων: **πρώτα** εφαρμόζεται η αντικατάσταση $A(x)$ και

ύστερα η αντικατάσταση B(x). Το γινόμενο αυτό είναι επίσης μια αντικατάσταση διότι

$$x \leftarrow \mathrm{AB}(x) = \mathrm{A}(\mathrm{B}(x)) = \frac{a_{11}\,B(x)+a_{12}}{a_{21}\,B(x)+a_{22}} =$$

$$= \frac{a_{11}\,\frac{b_{11}\,x+b_{12}}{b_{21}\,x+b_{22}} + a_{12}}{a_{21}\,\frac{b_{11}\,x+b_{12}}{b_{21}\,x+b_{22}} + a_{22}} = \frac{(a_{11}\,b_{11}+a_{12}\,b_{21})\,x + a_{11}\,b_{12}+a_{12}\,b_{22}}{(a_{21}\,b_{11}+a_{22}\,b_{21})\,x + a_{21}\,b_{12}+a_{22}\,b_{22}}$$

$$= \begin{pmatrix} a_{11}\,b_{11} + a_{12}\,b_{21} & a_{11}\,b_{12} + a_{12}\,b_{22} \\ a_{21}\,b_{11} + a_{22}\,b_{21} & a_{21}\,b_{12} + a_{22}\,b_{22} \end{pmatrix}(x) = (\mathrm{AB})(x).$$

Σαν το μοναδιαίο στοιχείο του συνόλου $\boldsymbol{\mathcal{M}}$ ορίζουμε την ταυτοτική αντικατάσταση $x \leftarrow x$, που αντιστοιχεί στον πίνακα

$$\mathrm{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Από τον τρόπο που ορίσαμε την ισότητα βλέπουμε πως $\lambda\mathrm{I}$, $\lambda \in \mathbb{C}$ και $\lambda \neq 0$, συμπίπτει με την ταυτοτική αντικατάσταση. Για τυχαία αντικατάσταση $x \leftarrow \mathrm{M}(x) \in \boldsymbol{\mathcal{M}}$, όπου $\mathrm{M} = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$, η αντίστροφη αντικατάσταση είναι $x \leftarrow M^{-1}(x)$, όπου το M^{-1} είναι **είτε**

$$M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{pmatrix}$$

δηλαδή ο αντίστροφος πίνακας του M, **είτε**, λόγω ορισμού της ισότητας,

$$M^{-1} = \begin{pmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{pmatrix}.$$

Προφανώς $\det(M^{-1}) \neq 0$.//

Η ομάδα δεν είναι Αβελιανή διότι γενικά $\mathrm{A}(x)\,\mathrm{B}(x) \neq \mathrm{B}(x)\,\mathrm{A}(x)$.

Ορισμός:

Οι ακόλουθοι τρεις αντικαταστάσεις Möbius ονομάζονται **γεννήτριες αντικαταστάσεις** (generating substitutions) της ομάδας $\boldsymbol{\mathcal{M}}$:

ι. **Αντιστροφή** (inversion): $x \leftarrow \frac{1}{x} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}(x)$

ιι. **Μετάθεση** (translation): $x \leftarrow x + a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}(x)$

ιιι. **Τάνυσμα** (stretching): $x \leftarrow a\,x = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}(x)$

Όταν το $a \in \mathbb{C}$ το τάνυσμα λέγεται ***στροφή*** (rotation).

Το θεώρημα που ακολουθεί τονίζει την σημασία των γεννητριών αντικαταστάσεων.

Θεώρημα (*γεννητριών αντικαταστάσεων*):
Κάθε αντικαταστάση $\mathrm{M}(x) \in \boldsymbol{\mathcal{M}}$ προκύπτει από κατάλληλο πολλαπλασιασμό των γεννητριών αντικαταστάσεων. (Μην ξεχνάτε πως σε ένα ***γινόμενο αντικαταστάσεων, αυτές εφαρμόζονται μία-μία από τα αριστερά προς τα δεξιά***.) Επομένως κάθε αντικατάσταση προκύπτει από μία ακολουθία γεννητριών αντικαταστάσεων.

Απόδειξη:
Έστω

$$\mathrm{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Για να αποδείξουμε το θεώρημα διακρίνουμε τις εξής δύο περιπτώσεις:

$\boldsymbol{c = 0}$: Στην περίπτωση αυτή εύκολα μπορούμε να δούμε πως $\mathrm{M} = M_1 M_2$, όπου

$$M_1 = \begin{pmatrix} 1 & \frac{b}{d} \\ 0 & 1 \end{pmatrix} \quad \text{και} \quad M_2 = \begin{pmatrix} \frac{a}{d} & 0 \\ 0 & 1 \end{pmatrix}.$$

Πράγματι, το γινόμενό τους είναι

$$M_1 M_2 = \begin{pmatrix} \frac{a}{d} & \frac{b}{d} \\ 0 & 1 \end{pmatrix} = \frac{1}{d}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

που σημαίνει πως αν $c = 0$, η αντικατάσταση $\mathrm{M}(x)$ είναι ισοδύναμη προς μία ***μετάθεση***, $M_1(x)$, ***ακολουθούμενη*** από ένα ***τάνυσμα***, $M_2(x)$.

$\boldsymbol{c \neq 0}$: Στην περίπτωση αυτή μπορούμε επίσης εύκολα να δούμε η αντικατάσταση $\mathrm{M}(x)$ είναι ισοδύναμη προς μία ***μετάθεση***, $M_1(x)$,

ακολουθούμενη *από μία* ***αντιστροφή***, $M_2(x)$, ***ακολουθούμενη*** *από μία ακόμα* ***μετάθεση***, $M_3(x)$, ***ακολουθούμενη*** *από ένα* ***τάνυσμα***, $M_4(x)$, *όπου*

$$M_1 = \begin{pmatrix} 1 & \frac{a}{c} \\ 0 & 1 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 1 & \frac{c\,d}{b\,c-a\,d} \\ 0 & 1 \end{pmatrix} \quad \textit{και} \quad M_4 = \begin{pmatrix} \frac{c^2}{b\,c-a\,d} & 0 \\ 0 & 1 \end{pmatrix}.$$

Πράγματι, *το γινόμενό τους είναι*

$$M_1M_2M_3M_4 = \begin{pmatrix} \frac{a}{c} & 1 \\ 1 & 0 \end{pmatrix} M_3\, M_4 = \begin{pmatrix} \frac{a}{c} & \frac{b\,c}{b\,c-a\,d} \\ 1 & \frac{c\,d}{b\,c-a\,d} \end{pmatrix} M_4$$

$$= \begin{pmatrix} \frac{a\,c}{b\,c-a\,d} & \frac{b\,c}{b\,c-a\,d} \\ \frac{c^2}{b\,c-a\,d} & \frac{c\,d}{b\,c-a\,d} \end{pmatrix} = \frac{c}{b\,c-a\,d} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ c & d \end{pmatrix}.//$$

Παράδειγμα:

Ας *θεωρήσουμε την αντικαταστάση* $x \leftarrow \frac{1}{1+x}$, *στην οποία αντιστοιχεί ο πίνακας* $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. *Εφαρμόζοντας το παραπάνω θεώρημα έχουμε την ακόλουθη ανάλυση σε γινόμενο γενητριών αντικαταστάσεων*:

$M_1(x) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}(x)$, *ταυτοτική αντικατάσταση*,

$M_2(x) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}(x)$, *αντιστροφή*,

$M_3(x) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}(x)$, *μοναδιαία μετάθεση, και*

$M_4(x) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}(x)$, *ταυτοτική αντικατάσταση*.

Συνεπώς, *αντικαταστάση* $x \leftarrow \frac{1}{1+x}$ *είναι ισοδύναμη με μία αντιστροφή*, $M_2(x)$, *ακολουθούμενη από μία μετάθεση κατά μονάδα*, $M_3(x)$.

Από *τα παραπάνω γίνεται φανερό πως οι* ***k*** *αντικαταστάσεις* $x \leftarrow 1 + x$, $x \leftarrow 1 + x$, …, $x \leftarrow 1 + x$ *ακολουθούμενες από την αντικατάσταση* $x \leftarrow \frac{1}{1+x}$ *είναι*

ισοδύναμες *με την αντικατάσταση* $x \leftarrow \boldsymbol{k} + \frac{1}{x}$ *ακολουθούμενη από την* $x \leftarrow 1 + x$.

Ας *δούμε τώρα την επίδραση των αντικαταστάσεων* Möbius, ή *ισοδύναμα των γεννητριών αντικαταστάσεων*, *στις ρίζες μιας πολυωνυμικής εξίσωσης* $p(x) = 0$ *με* ***ακέραιους*** *συντελεστές*, ***βαθμού n*** *και με* ***μία*** *μεταβλητή*. Έστω λοιπόν ότι

$$p(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0 = c_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = 0.$$

Αν *στο* $p(x)$ *κάνουμε την αντικατάσταση* $x \leftarrow \frac{1}{x}$, (***αντιστροφή***) *τότε προκύπτει το πολυώνυμο*

$$\begin{aligned} p(\tfrac{1}{x}) = p_i(x) \quad &= \tfrac{c_n}{x^n} + \tfrac{c_{n-1}}{x^{n-1}} + \cdots + \tfrac{c_1}{x} + c_0 \\ &= c_n \tfrac{1}{x^n} (1 - x\alpha_1)(1 - x\alpha_2) \cdots (1 - x\alpha_n) \\ &= c_n (\alpha_1\alpha_2\cdots\alpha_n) \tfrac{(-1)^n}{x^n} (x - \tfrac{1}{\alpha_1})(x - \tfrac{1}{\alpha_2}) \cdots (x - \tfrac{1}{\alpha_n}) \\ &= c_0 \tfrac{(-1)^n}{x^n} (x - \tfrac{1}{\alpha_1})(x - \tfrac{1}{\alpha_2}) \cdots (x - \tfrac{1}{\alpha_n}) = 0, \end{aligned}$$

επειδή $c_0 = c_n(\alpha_1\alpha_2\cdots\alpha_n)$. Πολλαπλασιάζοντας *την παραπάνω εξίσωση επί* $(-1)^n x^n$ *έχουμε*

$$\begin{aligned} (-1)^n x^n p(\tfrac{1}{x}) \quad &= c_0 x^n + c_1 x^{n-1} + \cdots + c_n \\ &= c_0 (x - \tfrac{1}{\alpha_1})(x - \tfrac{1}{\alpha_2}) \cdots (x - \tfrac{1}{\alpha_n}) = 0. \end{aligned}$$

Δηλαδή βλέπουμε πως ύστερα από την αντικατάσταση $x \leftarrow \frac{1}{x}$, ***οι συντελεστές και οι ρίζες του πολυωνύμου αντιστρέφονται!***

Όταν *στο* $p(x)$ *κάνουμε την αντικατάσταση* $x \leftarrow k + x$, $k \in \mathbb{Q}$, (***μετάθεση***) *τότε προκύπτει το πολυώνυμο*

$$\begin{aligned} p(k + x) = p_t(x) &= c_n(k + x - \alpha_1)(k + x - \alpha_2) \cdots (k + x - \alpha_n) \\ &= c_n(x - (\alpha_1 - k))(x - (\alpha_2 - k)) \cdots (x - (\alpha_n - k)) = 0. \end{aligned}$$

Δηλαδή, ύστερα από μία μετάθεση το **πραγματικό μέρος των ριζών** του νέου πολυωνύμου $p(k + x)$ **θα μικρύνει ή θα μεγαλώσει**, ανάλογα με το αν το k είναι θετικό ή αρνητικό, αντίστοιχα.

Προσέξτε πως οι συντελεστές του νέου πολυωνύμου είναι ακέραιοι μόνο στην περίπτωση που $k \in \mathbb{Z}$. Στην περίπτωση που $k \in \mathbb{Q}$, $k = \frac{a}{b} \gtrless 1$, για να κάνουμε τους συντελεστές ακεραίους πρέπει να πολλαπλασιάσουμε το νέο πολυώνυμο που προκύπτει επί b^n.

```
p[x_] = x^3 - 7 x + 7; 2^3 p[x + 3/2] // Expand
```

```
-1 - 2 x + 36 x^2 + 8 x^3
```

Τέλος, όταν στο $p(x)$ κάνουμε την αντικατάσταση $x \leftarrow kx$, $k \in \mathbb{Q}$ και $k \neq 0$, (***τάνυσμα***) τότε προκύπτει το πολυώνυμο

$$p(k\,x) = p_s(x) \quad = c_n\,(k\,x)^n + c_{n-1}\,(k\,x)^{n-1} + \cdots + c_0$$

$$= c_n(k\,x - \alpha_1)(k\,x - \alpha_2) \cdots (k\,x - \alpha_n)$$

$$= c_n\,k^n\,(x - \tfrac{\alpha_1}{k})(x - \tfrac{\alpha_2}{k}) \cdots (x - \tfrac{\alpha_n}{k}) = 0.$$

Βλέπουμε λοιπόν πως ύστερα από ένα τάνυσμα οι ρίζες του νέου πολυωνύμου $p(k\,x)$ ***θα μικρύνουν*** ή ***θα μεγαλώσουν*** ανάλογα με το αν το k είναι > 1 ή < 1, αντίστοιχα.

Και σε αυτήν την περίπτωση οι συντελεστές του νέου πολυωνύμου είναι ακέραιοι μόνο στην περίπτωση που $k \in \mathbb{Z}$. Στην περίπτωση που $k \in \mathbb{Q}$, $k = \frac{a}{b} \gtrless 1$, για να κάνουμε τους συντελεστές ακεραίους πρέπει να πολλαπλασιάσουμε το νέο πολυώνυμο που προκύπτει επί b^n. Για παράδειγμα

```
p[x_] = x^3 - 7 x + 7; 2^3 p[3/2 x] // Expand
```

```
56 - 84 x + 27 x^3
```

ή

```
p[x_] = x^3 - 7 x + 7; 3^3 p[2/3 x] // Expand
```

```
189 - 126 x + 8 x^3
```

Αναφέρουμε εν παρόδω ότι αν $k = b > 0$, όπου b είναι ένα ***πάνω*** *φράγμα στις απόλυτες τιμές των ριζών του* $p(x)$, *τότε το νέο πολυώνυμο* $p(bx) = p_s(x) = 0$ *θα έχει όλες τις ρίζες του μέσα στον μοναδιαίο κύκλο*.

Έχοντας *δει την επίδραση των γεννητριών αντικαταστάσεων, στις ρίζες μιας πολυωνυμικής εξίσωσης* $p(x) = 0$ *με ακέραιους συντελεστές και με μία μεταβλητή θα εξετάσουμε στην συνέχεια πως* ***εκτελούνται*** *αυτές οι αντικαταστάσεις*.

Η *αντιστροφή*, $x \leftarrow \frac{1}{x}$, *και το τάνυσμα*, $x \leftarrow kx$, *εκτελούνται ευκολότατα — η μεν πρώτη* (*αντικατάσταση*) *με απλή αντιστροφή της τάξης* (*σειράς*) *των συντελεστών του πολυωνύμου η δε δεύτερη κλιμακώνοντας τους συντελστές με δυνάμεις του* k.

Η *μετάθεση*, $x \leftarrow k + x$, *είναι η αντικατάσταση με το μεγαλύτερο ενδιαφέρον*. Εκτός *από τον υπολογισμό της με το ανάπτυγμα κατά* Taylor, *εκτελείται πολυ αποτελεσματικά και με την μέθοδο των* Ruffini-Horner — *εδάφιο* 4.1 *του πρώτου τόμου*.

■ 6.3.3 Το *θεώρημα του* Vincent: *επέκτασή του και εφαρμογή του*

Στο *εδάφιο αυτό θα εξετάσουμε το θεώρημα του* Vincent *του* 1836, *το οποίο αποτελεί την βάση της μεθόδου των συνεχών κλασμάτων για την απομόνωση των πραγματικών ριζών πολυωνυμικών εξισώσεων*.

Αρχίζουμε *με μία πιο λεπτομερή μελέτη του θεωρήματος των* Cardano-Descartes. Όπως *είδαμε, βάσει του θεωρήματος αυτού ο αριθμός* ρ_+ *των θετικών ριζών μιας πολυωνυμικής εξίσωσης* $p(x) = 0$ *δεν μπορεί να είναι μεγαλύτερος από τον αριθμό* ν *των μεταβολών προσήμου της ακολουθίας των συντελεστών του, και στην περίπτωση μη ισότητας ισχύει η σχέση* $\boldsymbol{\nu = \rho_+ + 2\lambda}$, *όπου* $\lambda \in \mathbb{Z}_{\geq 0}$.

Το θεώρημα των Cardano-Descartes είναι σχετικά αδύνατο διότι μας δίνει τον ακριβή αριθμό των ριζών μόνο στις εξής δύο περιπτώσεις:

- αν στους συντελεστές ενός πολυωνύμου δεν υπάρχει **καμία** μεταβολή προσήμου, δηλαδή $\boldsymbol{v = 0}$, τότε δεν υπάρχει **καμία** θετική ρίζα, δηλαδή $\boldsymbol{\rho_+ = 0}$, και
- αν στους συντελεστές ενός πολυωνύμου υπάρχει **μία** μεταβολή προσήμου, δηλαδή $\boldsymbol{v = 1}$, τότε υπάρχει **μία** θετική ρίζα, δηλαδή $\boldsymbol{\rho_+ = 1}$.

Όπως θα δούμε στην συνέχεια οι περιπτώσεις αυτές χρησιμοποιούνται (εκτός των άλλων) σαν κριτήριο τερματισμού στην μέθοδο απομόνωσης πραγματικών ριζών με συνεχή κλάσματα. **Το αξιοσημείωτο είναι πως από τις παραπάνω δύο περιπτώσεις μόνο στην πρώτη ισχύει και το αντίστροφο**! Δηλαδή ισχύει το εξής:

Λήμμα (Stodola):
Αν η πολυωνυμική εξίσωση

$$p(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0 = 0, \qquad (c_n > 0)$$

με πραγματικούς συντελεστές c_i, $0 \le i \le n$, έχει ρίζες με **μόνο αρνητικά πραγματικά μέρη**, τότε όλοι οι συντελεστές της είναι θετικοί και επομένως δεν παρουσιάζουν καμία μεταβολή προσήμου.

Απόδειξη:
Έστω ότι $-\alpha_p$, $p = 1, 2, \ldots, k$ είναι οι αρνητικές ρίζες, και $-\gamma_q \pm i\delta_q$, $q = 1, 2, \ldots, \ell$ είναι οι μιγαδικές ρίζες της $p(x) = 0$, όπου $\alpha_p > 0$ και $\gamma_q > 0$ για όλα τα p και q. Το πολυώνυμο $p(x)$ μπορεί να γραφτεί σαν το γινόμενο γραμμικών όρων όλων των ρίζών του, δηλαδή σαν

$$p(x) = c_n \prod_{p=1}^{k} (x + \alpha_p) \prod_{q=1}^{\ell} ((x + \gamma_q)^2 + \delta_q^2)$$

όπου όλοι οι παράγοντες έχουν θετικούς συντελεστές. Συνεπώς, οι συντελεστές του γινομένου θα είναι όλοι τους θετικοί και δεν θα παρουσιάζουν καμία μεταβολή προσήμου.//

Χωρίς προϋποθέσεις, το αντίστροφο της δεύτερης περίπτωσης δεν ισχύει: *δηλαδή αν ένα πολυώνυμο έχει* ***μία*** *θετική ρίζα τότε* ***δεν συνεπάγεται*** *πως αναγκαστικά θα υπάρχει στους συντελεστές του* ***μία*** *μεταβολή προσήμου.* Αυτό *φαίνεται καθαρά από το πολυώνυμο*

$$(x - 1)(x - i)(x + i) = x^3 - x^2 + x - 1,$$

το οποίο ενώ έχει ***μία θετική ρίζα*** *— και δύο μιγαδικές — παρουσιάζει* ***τρεις μεταβολές προσήμου***. Με *ορισμένες προϋποθέσεις όμως ισχύει και στην δεύτερη περίπτωση το αντιστροφο.* Ισχύει *το εξής*:

Λήμμα (Akritas - Danielopoulos):
Έτσω $p(x) = 0$ *μία πολυωνυμική εξίσωση βαθμού* $n > 1$, *με πραγματικούς συντελεστές, χωρίς πολλαπλές ρίζες και η οποία έχει μόνο* ***μία θετική*** *ρίζα* $\alpha \neq 0$ *και* ***n - 1 ρίζες*** $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ ***με αρνητικό πραγματικό μέρος*** *— εκ των οποίων οι μιγαδικές ρίζες εμφανίζονται σε συζυγοί ζεύγοι.* Έστω *επιπλέον ότι οι* n - 1 *ρίζες με το αρνητικό πραγματικό μέρος μπορούν να γραφτούν σαν*

$$\alpha_j = -(1 + \beta_j), \qquad j = 1, 2, \ldots, n - 1$$

με όλα τα β_j *να ικανοποιούν την* ***ανισότητα*** $|\beta_j| < \varepsilon_n$, *όπου*

$$\varepsilon_n = (1 + \tfrac{1}{n})^{1/(n-1)} - 1.$$

Δηλαδή, *οι* n - 1 *ρίζες με το αρνητικό πραγματικό μέρος βρίσκονται όλες μέσα σε έναν κύκλο με κέντρο το* -1 *και ακτίνα* ε_n. Τότε *η ακολουθία των συντελεστών του* $p(x)$ ***παρουσιάζει ακριβώς μία μεταβολή προσήμου***.

Απόδειξη:
Εκτός από *έναν σταθερό παράγοντα το πολυώνυμο γράφεται και ως*

$$\begin{aligned} p(x) &= (x - \alpha)(x - \alpha_1)\cdots(x - \alpha_{n-1}) \\ &= (x - \alpha)(x + 1 + \beta_1)\cdots(x + 1 + \beta_{n-1}) \\ &= (x - \alpha)(x^{n-1} + c_1 x^{n-2} + \cdots + c_{n-1}). \end{aligned}$$

Για *τους συντελεστές* c_k, $1 \le k \le n - 1$, *ισχύει*

$$c_k = \sum (1 + \beta_1)(1 + \beta_2)\cdots(1 + \beta_k),$$

όπου το άθροισμα αποτελείται από $\binom{n-1}{k}$ όρους. Προφανώς, το πολυώνυμο $p(x)$ μπορεί να γραφτεί επιπλέον και ως

$$p(x) = x^n + (c_1 - \alpha)x^{n-1} + (c_2 - c_1\alpha)x^{n-2} + \cdots + (c_{n-1} - c_{n-2}\alpha)x - c_{n-1}\alpha.$$

Αν τώρα αποδείξουμε πως $c_k > 0$, $1 \le k \le n-1$, ***και*** πως ο λόγος $\frac{c_k}{c_{k-1}}$, όπου $c_0 = 1$, ελαττώνεται για αυξάνοντα k, τότε προφανώς το πολυώνυμο $p(x)$ ***έχει ακριβώς μία μεταβολή προσήμου***.

$c_k > 0$: Χρησιμοποιώντας το λήμμα του Stodola που αναφέραμε παραπάνω η απόδειξη του $c_k > 0$, $1 \le k \le n-1$, είναι άμεση διότι αυτοί είναι συντελεστές του πολυωνύμου μέσα στην παρένθεση $p(x) = (x - \alpha)(x^{n-1} + c_1 x^{n-2} + \cdots + c_{n-1})$ που έχει ρίζες μόνο με αρνητικά πραγματικά μέρη.

$\frac{c_{k+1}}{c_k} < \frac{c_k}{c_{k-1}}$: Για να αποδείξουμε πως ο λόγος $\frac{c_k}{c_{k-1}}$, όπου $c_0 = 1$, ελαττώνεται για αυξάνοντα k, $1 \le k \le n-1$, πρέπει να βρούμε με τι ισούνται οι συντελεστές c_k. Παρατηρούμε πως για κάθε έναν από τους $\binom{n-1}{k}$ όρους του αθροίσματος έχουμε

$$|(1+\beta_1)(1+\beta_2)\cdots(1+\beta_k) - 1| \le (1+|\beta_1|)(1+|\beta_2|)\cdots(1+|\beta_k|) - 1$$

και επειδή εξ υποθέσεως έχουμε $|\beta_j| < \varepsilon_n$, $1 \le j \le n-1$, προκύπτει

$$\begin{aligned}(1+|\beta_1|)(1+|\beta_2|)\cdots(1+|\beta_k|) - 1 &\le (1+\varepsilon_n)^k - 1 \\ &\le (1+\varepsilon_n)^{n-1} - 1 = \frac{1}{n}.\end{aligned}$$

Επομένως μπορούμε να γράψουμε

$$c_k = \binom{n-1}{k}(1+\gamma_k),$$

όπου $|\gamma_k| \le \frac{1}{n}$. Για μία ακόμα φορά φαίνεται πως $c_k > 0$, $1 \le k \le n-1$.

Χρησιμοποιώντας την έκφραση $c_k = \binom{n-1}{k}(1+\gamma_k)$, προκύπτει

$$\frac{c_k}{c_{k-1}} = \frac{n-k}{k}\,\frac{1+\gamma_k}{1+\gamma_{k-1}}$$

και

$$\frac{c_{k+1}}{c_k} = \frac{n-k-1}{k+1}\,\frac{1+\gamma_{k+1}}{1+\gamma_k}.$$

Επομένως *για να δείξουμε πως* $\frac{c_{k+1}}{c_k} < \frac{c_k}{c_{k-1}}$ *πρέπει να αποδείξουμε πως*

$$\frac{k(n-k-1)}{(k+1)(n-k)} < \frac{(1+\gamma_k)^2}{(1+\gamma_{k-1})(1+\gamma_{k+1})}.$$

Αυτό όμως *ισχύει διότι αφ' ενός μεν έχουμε*

$$\frac{k(n-k-1)}{(k+1)(n-k)} = 1 - \frac{n}{(k+1)(n-k)} \le 1 - \frac{4n}{(n+1)^2} = \frac{(n-1)^2}{(n+1)^2}$$

επειδή $\frac{n}{(k+1)(n-k)} \ge \frac{4n}{(n+1)^2}$, όπως *βλέπουμε και με το Mathematica*

```
Assuming[{n, k} ∈ Integers && n > k && k ≥ 1,
 Refine[n/((k + 1) (n - k)) ≥ 4 n/(n + 1)^2]]
```

```
True
```

αφ' ετέρου δε, λόγω της σχέσης $|\gamma_k| \le \frac{1}{n}$,

$$\frac{(1+\gamma_k)^2}{(1+\gamma_{k-1})(1+\gamma_{k+1})} > \frac{\left(1-\frac{1}{n}\right)^2}{\left(1+\frac{1}{n}\right)^2} = \frac{(n-1)^2}{(n+1)^2}.$$

Επειδή *λοιπόν αφ' ενός μεν* $c_k > 0$, $1 \le k \le n - 1$, *αφ' ετέρου δε ο λόγος* $\frac{c_k}{c_{k-1}}$, *όπου* $c_0 = 1$, *ελαττώνεται για αυξάνοντα* k, $1 \le k \le n - 1$, *το πολυώνυμο* $p(x)$ *παρουσιάζει μία μεταβολή προσήμου*.//

Το *θεώρημα του* Vincent *που ακολουθεί στηρίζεται στα δύο προηγούμενα λήμματα*.

Θεώρημα του Vincent (1836):
Αν *σε μία πολυωνυμική εξίσωση με ρητούς συντελεστές και χωρίς πολλαπλές ρίζες κάνουμε διαδοχικές αντικαταστάσεις της μορφής*

$$x \leftarrow a_1 + \frac{1}{x},\ x \leftarrow a_2 + \frac{1}{x},\ x \leftarrow a_3 + \frac{1}{x},\ \ldots$$

όπου $a_1 \ge 0$ *είναι τυχαίος* ***μη αρνητικός*** *ακέραιος και* a_2, a_3, … *είναι τυχαίοι* ***θετικοί*** *ακέραιοι*, $a_i > 0$, $i > 1$, *τότε το νέο πολυώνυμο που προκύπτει* ***είτε*** *δεν*

έχει καμία, **είτε** έχει μία μεταβολή προσήμου. Στην τελευταία περίπτωση η εξίσωση έχει ακριβώς μία θετική ρίζα που παρίσταται από το συνεχές κλάσμα

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}$$

ενώ στην πρώτη περίπτωση δεν υπάρχει θετική ρίζα.

Απόδειξη:
Η απόδειξη βρίσκεται στο άρθρο του Vincent του 1836 και παραλείπεται. Αντ' αυτής θα παρουσιάσουμε πιο κάτω την απόδειξη ενός γενικότερου θεωρήματος.//

Προφανώς, το θεώρημα του Vincent απομονώνει μόνο τις θετικές ρίζες ενός πολυωνύμου $p(x)$. Οι αρνητικές ρίζες απομονώνονται — όπως ακριβώς πρότεινε ο Sturm — αφού γίνουν πρώτα θετικές, με την αντικατάσταση $x \leftarrow -x$ στο $p(x)$. Η γενικότητα του θεωρήματος του Vincent δεν περιορίζεται από τον όρο να μην έχει το πολυώνυμο $p(x)$ πολλαπλές ρίζες, διότι στην αντίθετη περίπτωση το διασπάμε σε παράγοντες ελεύθερους από τετράγωνα — και απομονώνουμε τις ρίζες κάθε ενός από αυτούς.

Ο ίδιος ο Vincent αναφέρει πως το θεώρημα αυτό το υπαινίχθηκε ο Fourier το 1827, αλλά ποτέ δεν το απέδειξε — ή αν το απέδειξε, η απόδειξη δεν βρέθηκε ποτέ. Επιπλέον η βασική ιδέα του θεωρήματος χρησιμοποιήθηκε πολύ πιο πριν από τον Lagrange.

Η εξάρτηση του θεωρήματος του Vincent από εκείνο του Budan φαίνεται εύκολα αν κάθε αντικατάσταση της μορφής $x \leftarrow a_i + \frac{1}{x}$ αντικατασταθεί από τις ισοδύναμες αντικαταστάσεις $\{x \leftarrow a_i + x, x \leftarrow \frac{1}{x}\}$.

Μιλώντας ***διαισθητικά***, ο σκοπός των διαδοχικών αντικαταστάσεων της μορφής $x \leftarrow a_i + \frac{1}{x}$ που γίνεται στο πολυώνυμο $p(x)$, ***βαθμού n***, για να απομονωθούν οι ρίζες του είναι ***διπλός***:

σκοπός 1ος: αναγκάζει τις αρνητικές ρίζες να ***μπουν*** σε έναν κύκλο με κέντρο το -1 και ακτίνα $\varepsilon_n = (1 + \frac{1}{n})^{1/(n-1)} - 1$ — βλέπε και το λήμμα των Akritas-Danielopoulos που αναφέραμε πιο πάνω.

σκοπός 2ος: *αναγκάζει τις θετικές ρίζες να* ***κατανεμηθούν*** *σύμφωνα με έναν από τους εξής δύο τρόπους*: ***είτε*** *μία από τις θετικές ρίζες είναι στο διάστημα* (0, 1) *ενώ οι υπόλοιπες είναι στο διάστημα* (1, ∞) ***είτε*** *μία από τις θετικές ρίζες είναι στο διάστημα* (1, ∞) *ενώ οι υπόλοιπες είναι στο διάστημα* (0, 1) — *εξαιρώντας την περίπτωση να είναι το* 1 *ρίζα του* $p(x)$.

Α*ν μία από τις θετικές ρίζες είναι στο διάστημα* (0, 1), *ενώ οι υπόλοιπες είναι στο διάστημα* (1, ∞), *τότε από την επιπλέον αντικατάσταση της μορφής* $x \leftarrow \frac{1}{1+x}$ *προκύπτει ένα πολυώνυμο με μία θετική ρίζα και μία μεταβολή προσήμου*! Αντίθετα, *αν μία από τις θετικές ρίζες είναι στο διάστημα* (1, ∞), *ενώ οι υπόλοιπες είναι στο διάστημα* (0, 1), *τότε από την επιπλέον αντικατάσταση της μορφής* $x \leftarrow 1 + x$ *προκύπτει ένα πολυώνυμο με μία θετική ρίζα και μία μεταβολή προσήμου*!

Σ*το θεώρημα του* Vincent *εύκολα γιεννέται η ερώτηση σχετικά με τον μέγιστο αριθμό αντικαταστάσεων που πρέπει να γίνουν για να προκύψει το πολυώνυμο με το πολύ μία μεταβολή προσήμου*.

Η *απάντηση στο ερώτημα αυτό δόθηκε από τον* Uspensky *που γενίκευσε το θεώρημα του* Vincent *και απέκτησε ένα πάνω φράγμα στον αριθμό των αντικαταστάσεων*. *Όμως η παρουσίασή του* Uspensky *είχε ορισμένα λάθη στην διατύπωση και απόδειξη τα οποία διορθώθηκαν από τον γράφοντα*. Α*κολουθεί το γενικευμένο θεώρημα*:

Θεώ*ρημα* (Vincent-Uspensky-Akritas):
Έ*στω* $p(x) = 0$ *μία πολυωνυμική εξίσωση βαθμού* $n > 1$, *με ρητούς συντελεστές και χωρίς πολλαπλές ρίζες και έστω επιπλέον ότι* $\Delta > 0$ *είναι η* ***ελάχιστη απόσταση*** *των ριζών του* $p(x)$ — *όπως αυτή ορίσθηκε στην ενότητα* 6.2.3. Α*ς συμβολίσουμε επιπλέον με* m *τον μικρότερο δείκτη έτσι ώστε*

$$F_{m-1}\frac{\Delta}{2} > 1, \quad \textit{και} \quad F_{m-1}F_m\Delta > 1 + \frac{1}{\varepsilon_n}, \tag{1}$$

όπου F_k *είναι το* k*-στό μέλος της ακολουθίας* Fibonacci 1, 1, 2, 3, 5, 8, 13, … *και*

$$\varepsilon_n = (1 + \tfrac{1}{n})^{1/(n-1)} - 1, \tag{2}$$

η ακτίνα του κύκλου γύρω από το -1 — *που αναφέραμε πριν από το θεώρημα αυτό.* Τέλος *έστω* $a_1 \geq 0$ *τυχαίος* ***μη αρνητικός*** *ακέραιος και* $a_2, a_3, \ldots, a_m$ *τυχαίοι* ***θετικοί*** *ακέραιοι,* $a_i > 0$, $1 < i \leq m$. Τότε *με την αντικατάσταση*

$$x \leftarrow a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_m + \cfrac{1}{x}}}}, \tag{3}$$

που είναι ισοδύναμη με την ακολουθία των διαδοχικών αντικαταστάσεων της μορφής $x \leftarrow a_i + \frac{1}{x}$, $1 \leq i \leq m$, *από την εξίσωση* $p(x) = 0$ *προκύπτει η εξίσωση* $p_{\text{ti}}(x) = 0$, *που έχει* ***το πολύ μία μεταβολή προσήμου***.

Απόδειξη:

Για *να αποδείξουμε το θεώρημα αρκεί να δείξουμε πως μετά τις διαδοχικές αντικαταστάσεις της μορφής* $x \leftarrow a_i + \frac{1}{x}$, $1 \leq i \leq m$, *τα πραγματικά μέρη* όλων *των μιγαδικών ριζών γίνονται αρνητικά,* όπως *επίσης γίνονται αρνητικές και* όλες *οι πραγματικές ρίζες* ***εκτός από το πολύ μία***. **Σημειώστε** *πως οι ρίζες της εξίσωσης* $p_{\text{ti}}(x) = 0$, "***μαζεύονται***" *μέσα σε έναν μικρό κύκλο γύρω από το* -1.

Πράγματι, *έστω ότι* $\frac{p_k}{q_k}$ *είναι η k-στή* ***συγκλίνουσα*** *στο συνεχές κλάσμα*

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}$$

Από *το εδάφιο* 3.5 *του πρώτου τόμου ξέρουμε πως για* $k \geq 0$, $p_{-1} = 0$, $p_0 = 1$, $q_{-1} = 1$ *και* $q_0 = 0$, *ισχύουν οι τύποι*

$$\begin{aligned} p_{k+1} &= a_{k+1} p_k + p_{k-1}, \\ q_{k+1} &= a_{k+1} q_k + q_{k-1}. \end{aligned}$$

Επειδή $q_1 = 1$ *και* $q_2 = a_2 \geq 1$, *έπεται πως* $q_k \geq F_k$. Επιπλέον, *η αντικατάσταση* (3) *μπορει να γραφεί ως*

$$x \leftarrow \frac{p_m x + p_{m-1}}{q_m x + q_{m-1}}$$

από την οποία προκύπτει το πολυώνυμο $p_{\text{ti}}(x)$. Δηλαδή

$$p_{\text{ti}}(x) = p\left(\frac{p_m x + p_{m-1}}{q_m x + q_{m-1}}\right).$$

Προφανώς, *με την αντίστροφη αντικατάσταση*

$$x \leftarrow -\frac{p_{m-1}-q_{m-1}\,x}{p_m - q_m\,x},$$

αποκτούμε πάλι το πολυώνυμο $p(x)$. *Δηλαδή*

$$p(x) = p_{\text{ti}}(-\frac{p_{m-1}-q_{m-1}\,x}{p_m - q_m\,x}).$$

Προσέξτε πως η αντίστροφη αντικατάσταση που αναφέραμε αντιστοιχεί στον πίνακα $\begin{pmatrix} q_{m-1} & -p_{m-1} \\ -q_m & p_m \end{pmatrix}$, *τον αντίστροφο του πίνακα* $\begin{pmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{pmatrix}$ *με την ισότητα που ορίσαμε.*

Επομένως, *αν* α *είναι μία ρίζα της εξίσωσης* $p(x) = 0$, *η* ***ποσότητα***

$$\tilde{\alpha} = -\frac{p_{m-1}-q_{m-1}\,\alpha}{p_m - q_m\,\alpha} \tag{4}$$

που ορίζεται είναι η ***αντίστοιχη ρίζα*** *της εξίσωσης* $p_{\text{ti}}(x) = 0$. *Θα εξετάσουμε τις* ***περιπτώσεις*** *όπου η ρίζα* α *της εξίσωσης* $p(x) = 0$ *είναι μιγαδική ή πραγματική και θα δείξουμε πως οι αντίστοιχες ρίζες της εξίσωσης* $p_{\text{ti}}(x) = 0$ *έχουν όλες αρνητικό πραγματικό μέρος — **εκτός από μία το πολύ πραγματική ρίζα** — και είναι μέσα σε έναν μικρό κύκλο γύρω από το* -1.

Μιγαδική ρίζα:

Έστω ότι α *είναι μία μιγαδική ρίζα της εξίσωσης* $p(x) = 0$. *Έστω δηλαδή* $\alpha = a \pm ib$, $b \neq 0$. *Στην περίπτωση αυτή κάνοντας τις πράξεις βλέπουμε πως το* $\pi\mu(\tilde{\alpha})$, *το* ***πραγματικό μέρος*** *της* $\tilde{\alpha}$, *της αντίστοιχης ρίζας της εξίσωσης* $p_{\text{ti}}(x) = 0$, *είναι*

$$\pi\mu(\tilde{\alpha}) = -\frac{(p_{m-1} - q_{m-1}\,a)\,(p_m - q_m\,a) + q_{m-1}\,q_m\,b^2}{(p_m - q_m\,a)^2 + q_m^2\,b^2} \tag{5}$$

Θέλουμε να αποδείξουμε πως $\pi\mu(\tilde{\alpha}) < 0$. *Στην περίπτωση που στην* (5) $(p_{m-1} - q_{m-1}\,a)\,(p_m - q_m\,a) \geq 0$ *προφανώς το* $\pi\mu(\tilde{\alpha})$ *είναι αρνητικό και τελειώσαμε. Στην περίπτωση όμως που* $(p_{m-1} - q_{m-1}\,a)\,(p_m - q_m\,a) < 0$, *πρέπει να αποδείξουμε πως* $q_{m-1}\,q_m\,b^2 > |(p_{m-1} - q_{m-1}\,a)\,(p_m - q_m\,a)|$. *Προς τούτο προσέξτε πως η τιμή του* a *περιέχεται ανάμεσα στις δύο διαδοχικές συγκλίνουσες* $\frac{p_{m-1}}{q_{m-1}}$ *και* $\frac{p_m}{q_m}$, *η διαφορά των οποίων σε απόλυτη τιμή είναι* $\frac{1}{q_{m-1}\,q_m}$. *Επομένως, έχουμε τις ανισότητες*

$$\left| \frac{p_{m-1}}{q_{m-1}} - a \right| < \frac{1}{q_{m-1}\, q_m} \quad \text{και} \quad \left| \frac{p_m}{q_m} - a \right| < \frac{1}{q_{m-1}\, q_m},$$

από τις οποίες συνεπάγεται ότι

$$|(p_{m-1} - q_{m-1}\, a)\,(p_m - q_m\, a)| < \frac{1}{q_{m-1}\, q_m} \le 1. \qquad (6)$$

Από τις (5) και (6) συμπεραίνουμε πως το $\pi\mu(\tilde{\alpha})$ θα είναι αρνητικό **αν**

$$q_{m-1}\, q_m\, b^2 > 1.$$

Για να αποδείξουμε την τελευταία ανισότητα προσέξτε πως επειδή Δ είναι η ελάχιστη απόσταση των ριζών του $p(x)$ έχουμε

$$|(a + ib) - (a - ib)| = |2ib| = 2|b| \ge \Delta,$$

από την οποία προκύπτει $|b| \ge \frac{\Delta}{2}$. Επιπλέον ξέρουμε πως $q_m \ge q_{m-1} \ge F_{m-1}$, και από την (1) πως $F_{m-1}\frac{\Delta}{2} > 1$. Επομένως ισχύει $F_{m-1}|b| > 1$, από την οποία έπονται και οι ανισότητες

$$q_{m-1}|b| > 1 \quad \text{και} \quad q_m|b| > 1.$$

Από αυτές τις τελευταίες δύο ανισότητες προκύπτει $q_{m-1}\, q_m\, b^2 > 1$, το οποίο αποδεικνύει πως το $\pi\mu(\tilde{\alpha})$ **είναι αρνητικό**. Αυτό φυσικά ισχύει για **όλες** τις μιγαδικές ρίζες της εξίσωσης $p_{\text{ti}}(x) = 0$. Υπενθυμίζουμε πως η $p_{\text{ti}}(x) = 0$ προκύπτει από την $p(x) = 0$ με αντικατάσταση της μορφής (3).

Πραγματική ρίζα:

Ας θεωρήσουμε κατ' αρχάς την περίπτωση ότι για **όλες** τις πραγματικές ρίζες α_i της εξίσωσης $p(x) = 0$ ισχύει η ανισότητα

$$(p_{m-1} - q_{m-1}\, \alpha_i)\,(p_m - q_m\, \alpha_i) > 0.$$

Από τις (4) και (5) έπεται πως όλες οι πραγματικές ρίζες της εξίσωσης $p_{\text{ti}}(x) = 0$ θα είναι αρνητικές. Επιπλέον ξέρουμε πως όλες οι μιγαδικές ρίζες της εξίσωσης $p_{\text{ti}}(x) = 0$ έχουν αρνητικό πραγματικό μέρος. Συνεπώς, από το Λήμμα του Stodola προκύπτει πως δεν υπάρχει μεταβολή προσήμου στο πολυώνυμο $p_{\text{ti}}(x)$.

Έστω λοιπόν τώρα ότι για **κάποια** πραγματική ρίζα α της εξίσωσης $p(x) = 0$ ισχύει

$$(p_{m-1} - q_{m-1}\,\alpha)\,(p_m - q_m\,\alpha) \le 0. \tag{7}$$

Τότε προφανώς η ρίζα α περιέχεται ανάμεσα στις δύο διαδοχικές συγκλίνουσες $\frac{p_{m-1}}{q_{m-1}}$ και $\frac{p_m}{q_m}$, **είναι θετική** και ισχύει $\left|\frac{p_m}{q_m} - \alpha\right| < \frac{1}{q_{m-1}\,q_m}$. Έστω ότι $\alpha_k \neq \alpha$, είναι μία **άλλη** ρίζα, πραγματική ή μιγαδική, της εξίσωσης $p(x) = 0$, διάφορη της ρίζας α, και έστω ότι

$$\tilde{\alpha}_k = -\frac{p_{m-1} - q_{m-1}\,\alpha_k}{p_m - q_m\,\alpha_k}$$

είναι η αντίστοιχη ρίζα της $p_{\text{ti}}(x) = 0$. Τότε αν λάβουμε υπ' όψη ότι

$$p_m\,q_{m-1} - p_{m-1}\,q_m = (-1)^m,$$

και προσθέσουμε στην ρίζα $\tilde{\alpha}_k$ την ποσότητα $\frac{q_{m-1}}{q_m}$ προκύπτει η ισότητα

$$\tilde{\alpha}_k + \frac{q_{m-1}}{q_m} = \frac{(-1)^m}{q_m(p_m - q_m\,\alpha_k)}$$

που γράφεται και

$$\tilde{\alpha}_k = -\frac{q_{m-1}}{q_m}\left(1 - \frac{(-1)^m}{q_{m-1}\,q_m\left(\frac{p_m}{q_m} - \alpha_k\right)}\right) = -\frac{q_{m-1}}{q_m}(1 + \beta_k),$$

όπου

$$\beta_k = \frac{(-1)^{m-1}}{q_{m-1}\,q_m\left(\frac{p_m}{q_m} - \alpha_k\right)}.$$

Επειδή δε ξέρουμε πως $q_m \ge q_{m-1} \ge F_{m-1}$, και από την (1) πως $F_{m-1}\frac{\Delta}{2} > 1$, ισχύει

$$\left|\frac{p_m}{q_m} - \alpha_k\right| = \left|\frac{p_m}{q_m} - \alpha + \alpha - \alpha_k\right| \ge |\alpha - \alpha_k| - \left|\frac{p_m}{q_m} - \alpha\right|$$

$$\ge \Delta - \frac{1}{q_{m-1}\,q_m} > 0$$

και συνεπώς

$$|\beta_k| \le \frac{1}{q_{m-1}\,q_m\,\Delta - 1} \le \frac{1}{F_{m-1}\,F_m\,\Delta - 1}.$$

Από την παραπάνω ανισότητα και την ανισότητα $F_{m-1}F_m\,\Delta > 1 + \frac{1}{\varepsilon_n}$ της (1) συνεπάγεται πως

$|\beta_k| \le \varepsilon_n$.

Εκτός λοιπόν από την **θετική** ρίζα $\tilde{\alpha}$, όλες οι υπόλοιπες ρίζες $\tilde{\alpha}_k$ της εξίσωσης $p_{\text{ti}}(x) = 0$ που αντιστοιχούν στις ρίζες α_k της εξίσωσης $p(x) = 0$ — και που είναι όλες διάφορες της ρίζας α — είναι της μορφής

$$\tilde{\alpha}_k = -\frac{q_{m-1}}{q_m}(1 + \beta_k), \quad |\beta_k| \le \varepsilon_n, \quad 1 \le k \le n - 1. \tag{8}$$

Δηλαδή, οι $n - 1$ ρίζες της εξίσωσης $p_{\text{ti}}(x) = 0$ — που προκύπτει από την $p(x) = 0$ με αντικατάσταση της μορφής (3) — έχουν όλες τους αρνητικό πραγματικό μέρος και έχουν μαζευτεί γύρω από το -1.

Ορίζουμε τώρα το πολυώνυμο

$$q_{\text{ti}}(x) = (x - \tilde{\alpha})(x + (1 + \beta_1))\cdots(x + (1 + \beta_k)),$$

το οποίο πληρεί τις συνθήκες του Λήμματος των Akritas-Danielopoulos και επομένως **παρουσιάζει μία μεταβολή προσήμου**! Επειδή όμως ισχύει

$$p_{\text{ti}}(x) = \left(\frac{q_{m-1}}{q_m}\right)^{n-1} q(x)$$

έπεται πως και το $p_{\text{ti}}(x)$ επίσης **παρουσιάζει μία μεταβολή προσήμου**!

Το μόνο που μένει να εξετάσουμε είναι η περίπτωση που η (7) είναι ισότητα, δηλαδή

$$(p_{m-1} - q_{m-1}\,\alpha)\,(p_m - q_m\,\alpha) = 0.$$

Αν $p_{m-1} - q_{m-1}\,\alpha = 0$, τότε έπεται πως $\tilde{\alpha} = -\frac{p_{m-1} - q_{m-1}\,\alpha}{p_m - q_m\,\alpha} = 0$, και η εξίσωση $p_{\text{ti}}(x) = 0$ δεν έχει μεταβολή προσήμου (Λήμμα του Stodola). Αν πάλι $p_m - q_m\,\alpha = 0$, τότε έπεται πως $\tilde{\alpha} = -\frac{p_{m-1} - q_{m-1}\,\alpha}{p_m - q_m\,\alpha} = \infty$, και η εξίσωση $p_{\text{ti}}(x) = 0$ ***μετασχηματίζεται σε εξίσωση βαθμού n - 1***. Επειδή δε όλες οι ρίζες της μετασχηματισμένης εξίσωσης έχουν αρνητικό πραγματικό μέρος, συμπεραίνουμε (Λήμμα του Stodola) πως η $p_{\text{ti}}(x) = 0$ δεν παρουσιάζει καμία μεταβολή προσήμου. Έτσι αποδείχθηκε το θεώρημα εντελώς.//

Από το παραπάνω θεώρημα βλέπουμε πως m είναι ένα πάνω φράγμα στον αριθμό των αντικαταστάσεων της μορφής $x \leftarrow a_i + \frac{1}{x}$ που πρέπει να

εκτελεσθούν έτσι ώστε το πολυώνυμο που προκύπτει να έχει το πολύ μία μεταβολή προσήμου. Ισχύει το εξής:

Λήμμα:
Με *τις προϋποθέσεις του παραπάνω θεωρήματος ισχύει*

$$m = O(\, n \log n \; + \; n \log |\; p(x) \;|_\infty \,).$$

Απόδειξη:
Εξ *ορισμού* m *είναι ο μικρότερος δείκτης έτσι ώστε να ισχύουν και οι δύο ανισότητες στην* (1). Προφανώς, *μία από αυτές τις δύο ανισότητες — και πιθανόν και οι δύο — δεν θα ισχύει αν ελαττώσουμε το* m *κατά ένα. Έστω ότι "χαλάει" η πρώτη ανισότητα της* (1) *και γίνεται*

$$F_{m-2}\,\tfrac{\Delta}{2} \le 1. \tag{9}$$

Εφαρμόζοντας *την σχέση* $F_k = \frac{\phi^k}{\sqrt{5}}$, *όπου* $\phi = 1.618...$ *και η στρογγύλευση γίνεται προς τον πλησιέστερο ακέραιο, προκύπτει* $\phi^{m-2} \le 2\sqrt{5}\,\frac{1}{\Delta}$ *και συνεπώς,*

$$m \le 2 + \log_\phi 2 + \tfrac{1}{2}\log_\phi 5 - \log_\phi \Delta. \tag{10}$$

Επιπλέον *από το θεώρημα του* Mahler *έχουμε*

$$\Delta \ge \sqrt{3}\; n^{-(n+2)/2} \;|\; p(x) \;|_1^{-(n-1)} \tag{11}$$

οπότε συνδιάζοντας τις (10) *και* (11) *αποδεικνύουμε το ζητούμενο — αν αντί του* $|\; p(x) \;|_1$ *χρησιμοποιούμε το* $|\; p(x) \;|_\infty$ *που είναι της ίδιας τάξης μεγέθους.* Το *ίδιο αποτέλεσμα προκύπτει αν υποθέσουμε ότι "χαλάει" η δεύτερη ανισότητα της* (1).//

Λαμβάνοντας υπ' όψη ότι το β*-μήκος του βαθμού των πολυωνύμων για τις περιπτώσεις που εξετάζουμε είναι* $\lambda(n) = 1$, ή $\log n = 1$, *προκύπτει*

$$m = O(\, n \log |\; p(x) \;|_\infty \,). \tag{12}$$

Το *θεώρημα του* Vincent *μπορεί να χρησιμοποιηθεί για την απομόνωση των πραγματικών ριζών μιας πολυωνυμικής εξίσωσης.* Προσέξτε *ότι εδώ — σε αντίθεση με το θεώρημα του* Sturm — ***δεν έχουμε άλλη επιλογή*** *από το να απομονώσουμε πρώτα τις θετικές και ύστερα τις αρνητικές ρίζες* (*κάνοντας την*

αντικατάσταση $x \leftarrow -x$). Για να δείτε την εφαρμογή του προσέξτε τα ακόλουθα σημεία από την παραπάνω απόδειξη:

α. Η αντικατάσταση (3) του θεωρήματος που αποδείξαμε μπορεί να γραφτεί και ως

$$x \leftarrow \frac{p_m x + p_{m-1}}{q_m x + q_{m-1}}, \tag{13}$$

όπου $\frac{p_k}{q_k}$ είναι η k-στή ***συγκλίνουσα*** στο συνεχές κλάσμα

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}$$

και όπως αναφέραμε, για $k \geq 0$, $p_{-1} = 0$, $p_0 = 1$, $q_{-1} = 1$ και $q_0 = 0$, ισχύουν οι τύποι

$$\begin{aligned} p_{k+1} &= a_{k+1} p_k + p_{k-1}, \\ q_{k+1} &= a_{k+1}\, q_k + q_{k-1}. \end{aligned} \tag{14}$$

β. Η απόσταση μεταξύ δύο διαδοχικών συγκλινουσών είναι

$$\left| \frac{p_{m-1}}{q_{m-1}} - \frac{p_m}{q_m} \right| = \frac{1}{q_{m-1}\, q_m}.$$

Προφανώς, οι μικρότερες τιμές των q_m εμφανίζονται όταν $\forall i,\ a_i = 1$. Τότε $q_m = F_m$, ο m-στός αριθμός Fibonacci. Αυτό εξηγεί διαισθητικά την σχέση μεταξύ των αριθμών Fibonacci και την απόσταση Δ των ριζών.

γ. Έστω $p_{\text{ti}}(x) = 0$ η εξίσωση που προκύπτει από την $p(x) = 0$ με αντικατάσταση της μορφής (13) και έστω επιπλέον ότι ισχύουν οι προϋποθέσεις του θεωρήματος που αποδείξαμε και ότι το $p_{\text{ti}}(x)$ παρουσιάζει μία μεταβολή προσήμου. Τότε το πολυώνυμο $p_{\text{ti}}(x)$ θα έχει ***ακριβώς*** μία θετική ρίζα $\tilde{\alpha}$ στην οποία αντιστοιχεί μία θετική ρίζα α του πολυωνύμου $p(x)$. Οι ρίζες των δύο αυτών πολυωνύμων σχετίζονται με τον τύπο

$$\tilde{\alpha} = -\frac{p_{m-1} - q_{m-1}\,\alpha}{p_m - q_m\,\alpha},$$

δηλαδή την σχέση (4) που συναντήσαμε στην απόδειξη του θεωρήματος. Προσέξτε πως η αντικατάσταση (13) ***απεικονίζει το διάστημα*** $(0, \infty)$ — μέσα στο οποίο βρίσκεται η μοναδική θετική ρίζα $\tilde{\alpha}$ του $p_{\text{ti}}(x)$ — ***πάνω στο διάστημα*** με άκρα τα σημεία $\frac{p_{m-1}}{q_{m-1}}$ και $\frac{p_m}{q_m}$ — μέσα στο οποίο βρίσκεται μία θετική ρίζα α

του $p(x)$. *Τα άκρα του διαστήματος,* $\frac{p_{m-1}}{q_{m-1}}$ *και* $\frac{p_m}{q_m}$, *βρίσκονται αν στην έκφραση* $\frac{p_m x+p_{m-1}}{q_m x+q_{m-1}}$ *της* (13) *αντικαταστήσουμε το* x *πρώτα με το* 0 *και ύστερα με το* ∞, *αντίστοιχα*.

- **6.3.4 Απομόνωση των θετικών ριζών με συνεχή κλάσματα**

Από *την παραπάνω συζήτηση είναι φανερό πως η απομόνωση των θετικών ριζών ενός πολυωνύμου* $p(x)$ *με συνεχή κλάσματα δεν είναι τίποτε άλλο από τον* ***υπολογισμό των μερικών πηλίκων*** $a_1, a_2, \ldots, a_m$ *για αντικαταστάσεις της μορφής* (3) *που οδηγούν σε πολυώνυμα* $p_{\text{ti}}(x)$ *με* ***ακριβώς μία μεταβολή προσήμου***.

Υψίστης *σημασίας είναι το γεγονός πως το θεώρημα του* Budan — *με την δική του ιδιόμορφη διατύπωση — χρησιμοποιείται σαν ένα είδος "****τερματικού τεστ****" στον υπολογισμό κάθε ενός από τα μερικά πηλίκα* $a_1, a_2, \ldots, a_m$. *Για παράδειγμα, αν τα πολυώνυμα* $p_{\text{ti}}(x + a_i)$ *και* $p_{\text{ti}}(x + a_i + 1)$ *έχουν τον ίδιο αριθμό μεταβολών προσήμου, θέτουμε* $a_i \leftarrow a_i + 1$ *και συνεχίζουμε τον υπολογισμό του* a_i. **Αν** *όμως πηγαίνοντας από* ***κάποιο ενδιάμεσο*** *πολυώνυμο* $p_{\text{ti}}(x + a_i)$ *στο πολυώνυμο* $p_{\text{ti}}(x + a_i + 1)$ "***χάσουμε***" *μεταβολές προσήμου,* ***τότε*** *η τιμή του τυχαίου μερικού πηλίκου* a_i *έχει υπολογισθεί. Έχοντας υπολογίσει το* a_i *εκτελούμε την αντικατάσταση* $x \leftarrow \frac{1}{x+1}$, *για να αρχίσουμε τον υπολογισμό του επόμενου μερικού πηλίκου* a_{i+1} *ή να σταματήσουμε.*

Υπάρχουν ***δύο τρόποι υπολογισμού*** *των μερικών πηλίκων* a_i — *και συνεπώς δύο μέθοδοι απομόνωσης των θετικών ριζών ενός πολυωνύμου* $p(x)$ *με συνεχή κλάσματα. Ο πρώτος τρόπος αναπτύχθηκε από τον* Vincent *το* 1836 *ενώ ο δεύτερος αναπτύχθηκε από τον γράφοντα το* 1978. *Η διαφορά ανάμεσα στους δύο αυτούς τρόπους υπολογισμού των* a_i *είναι ανάλογη της διαφοράς που υπάρχει ανάμεσα στα ολοκληρώματα κατά* Riemann *και κατά* Lebesgue. *Δηλαδή, όπως ξέρουμε, το άθροισμα* 1 + 1 + 1 + 1 + 1 *μπορεί να υπολογισθεί κατά δύο τρόπους:* ***κατά*** **Riemann** *υπολογίζεται ως* 1 + 1 = 2, 2 + 1 = 3, 3 + 1 = 4, 4 + 1 = 5, *ενώ* ***κατά*** **Lebesgue** *υπολογίζεται ως* $5 \cdot 1 = 5$.

Εκτός *από τους* ***δύο*** *προαναφερθέντες τρόπους υπολογισμού των μερικών πηλίκων* a_i, *στην συνέχεια αναφέρουμε και μία "αποτυχημένη" προσπάθεια του*

Uspensky. Η αποτυχία αυτή οφείλεται στο γεγονός ότι ο Uspensky δεν γνώριζε το θεώρημα του Budan.

Υπολογισμός τυχαίου μερικού πηλίκου a_i κατά Vincent:
Ο Vincent στο άρθρο του τού 1836 υπολογίζει την τιμή του τυχαίου μερικού πηλίκου a_i με μοναδιαίες αυξήσεις της μορφής $a_i \leftarrow a_i + 1$. Σε κάθε τέτοια αύξηση αντιστοιχεί η αντικατάσταση $x \leftarrow x + 1$ που εκτελείται σε κάποιο ενδιάμεσο πολυώνυμο $p_{\text{ti}}(x)$ και ακολουθεί έλεγχος για πιθανό "χάσιμο" μεταβολών προσήμου — χάσιμο που σηματοδοτεί και το τέλος του υπολογισμού του εν λόγω a_i.

Τονίζουμε πως **μόνο αν** πηγαίνοντας από κάποιο ενδιάμεσο πολυώνυμο $p_{\text{ti}}(x + a_i)$ στο πολυώνυμο $p_{\text{ti}}(x + a_i + 1)$ "**χαθούν**" μεταβολές προσήμου **τότε, και μόνον τότε, εκτελεί** ο Vincent στο πολυώνυμο $p_{\text{ti}}(x + a_i)$ την αντικατάσταση $x \leftarrow \frac{1}{x+1}$, με σκοπό να αρχίσει τον υπολογισμό του επόμενου μερικού πηλίκου a_{i+1} ή να σταματήσει.

Η μέθοδος αυτή του Vincent οδηγεί σε μία **εκθετική** μέθοδο απομόνωσης των θετικών ριζών, κάτι που είχε γίνει αντιληπτό και από τον Sturm και από τον Uspensky. Η εκθετική αυτή συμπεριφορά εμφανίζεται μόνο στην περίπτωση μεγάλων μερικών πηλίκων a_i. Για μικρά a_i η μέθοδος του Vincent είναι πολύ ικανοποιητική.

Παράδειγμα:
Έστω ότι θέλουμε να απομονώσουνε τις ρίζες του πολυωνύμου

$$p(x) = (x - \alpha)(x - \beta).$$

Επιλέγουμε $\alpha = 10^k + \epsilon$, όπου $0 < \epsilon < 1$, $k \in \mathbb{Z}_{>0}$ και αρκετά μεγάλο, και $\beta = \alpha + \epsilon$. Στην περίπτωση αυτή, το πρώτο μερικό πηλίκο a_1 είναι το ακέραιο μέρος της ρίζας α, δηλαδή $a_1 = \lfloor \alpha \rfloor = 10^k$.

Για να υπολογίσουμε το a_1 με τον τρόπο του Vincent θέτουμε $a_1 \leftarrow 1$, $p_{\text{ti}}(x) \leftarrow p(x)$, υπολογίζουμε το $p_{\text{ti}}(x + 1)$ και ελέγχουμε για μείωση του αριθμού των μεταβολών προσήμου. Επειδή τα πολυώνυμα $p_{\text{ti}}(x)$ και $p_{\text{ti}}(x + 1)$ έχουν τον ίδιο αριθμό μεταβολών προσήμου ξέρουμε από το θεώρημα του Budan πως δεν υπάρχει ρίζα του $p(x)$ στο διάστημα $(0, 1)$. Αυξάνουμε λοιπόν το a_1 κατά

μονάδα, $a_1 \leftarrow a_1 + 1$, *θέτουμε* $p_{ti}(x) \leftarrow p_{ti}(x + 1)$, *υπολογίζουμε το* $p_{ti}(x + 1)$ *και ελέγχουμε ξανά για μείωση του αριθμού των μεταβολών προσήμου*. Η *διαδικασία αυτή επαναλαμβάνεται* 10^k *φορές και — αν το* k *επιλεχθεί κατάλληλα — μπορεί να διαρκέσει χρόνια στον γρηγορότερο υπολογιστή*.

Υπολογισμός τυχαίου μερικού πηλίκου a_i κατά Uspensky:
Όπως *είδαμε παραπάνω η τιμή του τυχαίου μερικού πηλίκου* a_i *υπολογίζεται με την χρήση του θεωρήματος του* Budan. *Έτσι, αν τα πολυώνυμα* $p_{ti}(x)$ *και* $p_{ti}(x + 1)$ *έχουν τον ίδιο αριθμό μεταβολών προσήμου ο* Vincent *προχωρεί στην επόμενη μοναδιαία αύξηση* $a_i \leftarrow a_i + 1$ *— και φυσικά και στην επόμενη αντικατάσταση* $x \leftarrow x + 1$. Και *αυτό επειδή ξέρει πως δεν υπάρχει ρίζα του* $p_{ti}(x)$ *στο διάστημα* (0, 1).

Ο Uspensky *στο βιβλίο του* (1949) *υπολογίζει την τιμή του τυχαίου μερικού πηλίκου* a_i *επίσης με μοναδιαίες αυξήσεις της μορφής* $a_i \leftarrow a_i + 1$ *— και φυσικά αντικαταστάσεις της μορφής* $x \leftarrow x + 1$. Μ*ην γνωρίζοντας όμως το θεώρημα του* Budan, *ο* Uspensky ***δεν μπορει να συμπεράνει*** *ότι το* $p_{ti}(x)$ *δεν έχει ρίζα στο διάστημα* (0, 1), *αν τα πολυώνυμα* $p_{ti}(x)$ *και* $p_{ti}(x + 1)$ *έχουν τον ίδιο αριθμό μεταβολών προσήμου*. *Έτσι λοιπόν, για να βεβαιωθεί πως το* $p_{ti}(x)$ *δεν έχει ρίζα στο διάστημα* (0, 1), *ο* Uspensky *κάνει* ***σε κάθε βήμα***, *εκτός από την αντικατάσταση* $x \leftarrow x + 1$, ***και*** *την αντικατάσταση* $x \leftarrow \frac{1}{x+1}$ *— από την οποία στην προκειμένη περίπτωση προκύπτει ένα πολυώνυμο χωρίς καμία μεταβολή προσήμου*. *Διευκρινίζουμε πως με την αντικατάσταση* $x \leftarrow \frac{1}{x+1}$ *οι ρίζες του* $p_{ti}(x)$ *που είναι* > 1 *γίνονται* ***αρνητικές*** *ενώ οι ρίζες που είναι* < 1 *γίνονται* > 1.

Έτσι *ο* Uspensky *το μόνο που κατόρθωσε ήταν να* ***διπλασιάσει*** *τον χρόνο υπολογισμού της μεθόδου του* Vincent. *Συνεπώς οι ισχυρισμοί του — στην εισαγωγή του βιβλίου του — ότι δήθεν ανακάλυψε μία νέα μέθοδο για την απομόνωση των ριζών δεν ευσταθούν*.

Η ***συμβολή του*** **Uspensky** *έγκειται στα εξής*:

α. *Για την αντικατάσταση* $x \leftarrow x + 1$ *χρησιμοποίησε την μέθοδο των* Ruffini-Horner, *ενώ ο* Vincent *το ανάπτυγμα* Taylor.

β. Για να εξαφανίσει την εκθετική συμπεριφορά της μεθόδου πρότεινε αντί των αντικαταστάσεων $x \leftarrow x + 1$ να γίνονται αντικαταστάσεις της μορφής $x \leftarrow x + k$, όπου k επιλέγεται τυχαία και διαδοχικά αυξάνεται — κάτι που δεν πέτυχε. Προφανώς δεν είχε γίνει κατανοητή η γεωμετρική σημασία των μερικών πηλίκων a_i.

Υπολογισμός τυχαίου μερικού πηλίκου a_i κατά τον γράφοντα:
Στην διδακτορική του διατριβή, 1978, ο γράφων ***με την βοήθεια του θεωρήματος του*** **Cauchy** (ενότητα 6.2.5) υπολόγισε το τυχαίο μερικό πηλίκο a_i σαν ένα ***κάτω φράγμα***, ℓb, στις τιμές των ***θετικών*** ριζών κάποιου ενδιάμεσου πολυωνύμου $p_{\text{ti}}(x)$. Θεωρητικά λοιπόν ο υπολογισμός του a_i γίνεται άμεσα θέτοντες $a_i \leftarrow \ell b$, $\ell b \geq 1$, και αυτό αντιστοιχεί στην αντικατάσταση $x \leftarrow x + \ell b$ που εκτελείται στο $p_{\text{ti}}(x)$. Δεδομένου ότι οι αντικαταστάσεις $x \leftarrow x + 1$ και $x \leftarrow x + \ell b$, $\ell b \geq 1$, εκτελούνται στον ίδιο περίπου χρόνο είναι προφανές ότι η εκθετική συμπεριφορά της μεθόδου εξαφανίσθηκε.

Προσέξτε πως για $\forall i$, $a_i = \lfloor \alpha_s \rfloor$, όπου α_s είναι η μικρότερη θετική ρίζα κάποιου ενδιάμεσου πολυωνύμου $p_{\text{ti}}(x)$. Επειδή γενικά το κάτω φράγμα δεν μας δίνει το ακέραιο μέρος της μικρότερης ρίζας, το θεώρημα του Cauchy θα χρειαστεί να εφαρμοσθεί περισσότερες από μία φορά για τον υπολογισμό του $\lfloor \alpha_s \rfloor$. Έτσι, στο παράδειγμα που είδαμε παραπάνω, για να υπολογισθεί το $\lfloor \alpha \rfloor$, $\alpha = 5 \cdot 10^9 + \epsilon$, χρειάστηκαν 18 εφαρμογές.

Συνθήκη 1η:
Δεδομένου ότι ο αριθμός εφαρμογών του θεωρήματος του Cauchy δεν μπορεί να προβλεφθεί και είναι πολύ μικρός σχετικά με την τιμή του a_i, στην ***θεωρητική ανάλυση*** της μεθόδου θα θεωρήσουμε πως για το κάτω φράγμα ισχύει $\ell b = \lfloor \alpha_s \rfloor$. Αυτό δεν περιορίζει την γενικότητα διότι, όπως είδαμε, το κόστος κάθε εφαρμογής του θεωρήματος του Cauchy είναι πολύ μικρό.

Αν αναλογισθούμε ότι ο σκοπός των αντικαταστάσεων είναι ***είτε*** μία από τις θετικές ρίζες να μπει στο διάστημα $(0, 1)$ ενώ οι υπόλοιπες να μπουν στο διάστημα $(1, \infty)$ ***είτε*** μία από τις θετικές ρίζες να μπει στο διάστημα $(1, \infty)$ ενώ οι υπόλοιπες να μπουν στο διάστημα $(0, 1)$ — βλέπε και την συζήτηση πριν την

απόδειξη του θεωρήματος του Vincent — *τότε εύλογα δικαιολογείται η ερμηνεία που δώσαμε στα μερικά πηλίκα*. Τα *ακόλουθα λήμματα είναι σχετικά*.

Λήμμα (*για την αντιστροφή πραγματικών ριζών*):
Έστω $p(x)$ *μία πολυωνυμική εξίσωση μιας μεταβλητής*, *βαθμού* $d \geq 2$, *με ακέραιους συντελεστές και χωρίς πολλαπλές ρίζες*, *η οποία έχει* t *πραγματικές ρίζες μέσα στο διάστημα* $(0, 1)$, $2 \leq t \leq d$, *και έστω* $\Delta > 0$, *η ελάχιστη απόστασή τους*. Τότε *αν στο* $p(x)$ *κάνουμε την αντιστροφή* $x \leftarrow \frac{1}{x}$, *οι* t *ρίζες απεικονίζονται στο διάστημα* $(1, \infty)$, *όπου τώρα η ελάχιστη απόστασή τους είναι* $\Delta' > \Delta$.

Απόδειξη:
Έστω ότι $0 < \alpha_1 < \cdots < \alpha_k < \alpha_\ell < \cdots < \alpha_m < \alpha_n < \cdots < \alpha_t < 1$ *είναι οι* t *ρίζες του* $p(x)$ *μέσα στο διάστημα* $(0, 1)$, *και έστω ότι* $\Delta = \alpha_\ell - \alpha_k$, *ενώ* $\Delta' = \frac{1}{\alpha_m} - \frac{1}{\alpha_n}$. Η *απόδειξη του λήμματος φαίνεται αμέσως από το*

$$\Delta' = \frac{1}{\alpha_m} - \frac{1}{\alpha_n} = \frac{\alpha_n - \alpha_m}{\alpha_m \alpha_n} > \alpha_n - \alpha_m \geq \alpha_\ell - \alpha_k = \Delta.//$$

Λήμμα (*για την αντιστροφή μιγαδικών ριζών*):
Έστω $p(x)$ *μία πολυωνυμική εξίσωση μιας μεταβλητής*, *βαθμού* $d \geq 2$, *με ακέραιους συντελεστές και χωρίς πολλαπλές ρίζες*, *η οποία έχει δύο μιγαδικές συζυγείς ρίζες*, α_1 *και* α_2 *μέσα στον κύκλο με κέντρο* $(\frac{1}{2}, 0)$ *και ακτίνα* $\frac{1}{2}$, *και έστω επιπλέον* $\delta = |\alpha_1 - \alpha_2|$. Τότε *αν στο* $p(x)$ *κάνουμε την αντιστροφή* $x \leftarrow \frac{1}{x}$, *οι* 2 *μιγαδικές ρίζες απεικονίζονται στο ημιεπίπεδο με πραγματικό μέρος* > 1, *όπου τώρα η απόστασή τους είναι* $\delta' > \delta$.

Απόδειξη:
Όμοια *με την προηγούμενη*.//

Ακολουθεί *μια λεπτομερέστερη περιγραφή της απομόνωσης πραγματικών ριζών με συνεχή κλάσματα*.

Ας *θεωρήσουμε ένα άπειρο δυαδικό δένδρο σε κάθε κορυφή του οποίου αντιστοιχούμε μία τριάδα της μορφής* $\{f(x), \mathrm{M}(x), v_f\}$, *όπου το πολυώνυμο* $f(x)$ *προκύπτει από το αρχικό πολυώνυμο* $p(x)$ *ύστερα από την αντικατάσταση* $x \leftarrow \mathrm{M}(x) = \frac{a\,x + b}{c\,x + d}$, *και* v_f *είναι ο αριθμός των μεταβολών προσήμου στην ακολουθία των συντελεστών του* $f(x)$.

Από την προηγούμενη συζήτηση γνωρίζουμε πως αν $f(x) = p(\frac{ax+b}{cx+d})$, τότε οι θετικές ρίζες του $f(x)$ αντιστοιχούν σε **εκείνες** τις θετικές ρίζες του $p(x)$ που βρίσκονται μέσα στο διάστημα με άκρα $\frac{b}{d}$ και $\frac{a}{c}$. Προσέξτε πως η διάταξη των $\frac{b}{d}$, $\frac{a}{c}$ **δεν είναι γνωστή**, και έτσι για ευκολία το διάστημα αυτό θα το συμβολίζουμε ως *interval*(a, b, c, d). Υπενθυμίζουμε πως τα άκρα αυτά προέρχονται από την έκφραση $\frac{ax+b}{cx+d}$ αντικαθιστώντες το x με το 0 και το ∞, αντίστοιχα.

Αν $p(x)$ είναι το αρχικό πολυώνυμο με ν μεταβολές προσήμου στην ακολουθία των συντελεστών του, τότε στην ρίζα του δυαδικού δένδρου αντιστοιχεί η τριάδα $\{f(x) \leftarrow p(x), \mathrm{M}(x) \leftarrow x, v_f \leftarrow v\}$.

Ο δρόμος από κάθε **κορυφή** ή **κόμβο** (node) προς τον δεξιό απόγονο αντιστοιχεί στην αντικατάσταση $x \leftarrow x + 1$, ενώ ο δρόμος προς τον αριστερό απόγονο αντιστοιχεί στην αντικατάσταση $x \leftarrow \frac{1}{x+1}$. Προσέξτε πως για κάθε μερικό πηλίκο a_i, μια σειρά από a_i διαδοχικές αντικαταστάσεις της μορφής $x \leftarrow x + 1$ ακολουθούμενες από την $x \leftarrow \frac{1}{x+1}$ είναι ισοδύναμες με την $x \leftarrow a_i + \frac{1}{x}$ ακολουθούμενη από την $x \leftarrow x + 1$.

Όλες οι κόμβοι που ανήκουν σε κάποιο **δρόμο** (path), πεπερασμένο ή άπειρο, θα θεωρούνται μέλη μη τεμνομένων συνόλων τριών τύπων. Ένα σύνολο τύπου V_0, V_1 ή V_n περιέχει κόμβους που αντιστοιχούν σε πολυώνυμα με 0, 1 ή περισσότερες μεταβολές προσήμου, αντίστοιχα. Τα σύνολα τύπου V_0 ή V_1 καλούνται **τερματικά σύνολα**. Στην περίπτωση που σύνολα ανήκουν στον ίδιο δρόμο λέμε πως το σύνολο X **προηγείται** του συνόλου Y εάν και μόνον εάν $\forall x \in X$ και $\forall y \in Y$ το μήκος του δρόμου(x) < το μήκος του δρόμου(y). Σε ένα τερματικό σύνολο, ο κόμβος με την μικρότερη απόσταση από την κορυφή λέγεται **τερματικός κόμβος**.

ΣΧΗΜΑ 7.3.1 από το βιβλίο

Σχετικά με το δυαδικό αυτό δένδρο έχουμε και την ακόλουθη υπόθεση, όπου το πολυώνυμο $f(x)$ αντιστοιχεί σε κάποιο κόμβο και τα πολυώνυμα $f(x+1)$ και $f(\frac{1}{x+1})$ είναι οι δύο απόγονοί του. Η υπόθεση αυτή χρησιμοποιείται στηνανάλυση της χρήσης μνήμης του υπολογιστή από την μέθοδο των συνεχών κλασμάτων.

Υπόθεση (Strzebonski-Akritas):
Έστω το πολυώνυμο $f(x)$ βαθμού n, $f(0) \neq 0$, με ρητούς συντελεστές και ***χωρίς πολλαπλές ρίζες*** και έστω επιπλέον ότι με $sv(f(x))$ συμβολίζουμε τις μεταβολές προσήμου στην ακολουθία των συντελεστών του. Τότε για τα πολυώνυμα $f(x+1)$ και $f(\frac{1}{x+1})$, ισχύει ***η ανισότητα των μεταβολών προσήμου***

$$sv(f(x+1)) + sv((x+1)^n f(\tfrac{1}{x+1})) \leq sv(f(x)).$$

Συζήτηση:
Η ισχύς της υπόθεσης αυτής έχει επιβεβαιωθεί από έναν πάρα πολύ μεγάλο αριθμό πειραμάτων. Δυστυχώς όμως η απόδειξη μας διαφεύγει. Θα μπορούσε να είναι ως εξής:

Όπως ξέρουμε από την απόδειξη των θεωρημάτων του Fourier και Cardano-Descartes — για την γενική περίπτωση που επιτρέπονται πολλαπλές ρίζες (ενότητα 6.2) — ο αριθμός των μεταβολών προσήμου του $f(x)$ **είτε** ισούται ακριβώς με τον αριθμό των θετικών ριζών του $f(x)$ **είτε** τον υπερβαίνει κατά κάποιο άρτιο αριθμό που οφείλεται σε κάποιες ρίζες ορισμένων παραγώγων του $f(x)$. Για παράδειγμα το πολυώνυμο

```
f[x_] = (x - 7/3) (x - i) (x + i) // Expand
```

$$-\frac{7}{3} + x - \frac{7x^2}{3} + x^3$$

με μία θετική ρίζα και τρεις μεταβολές προσήμου οφείλει τις δύο παραπάνω μεταβολές προσήμου στην ρίζα 0.25662 της πρώτης του παραγώγου

```
Solve[ f'[x] == 0] // N
```

```
{{x → 0.25662}, {x → 1.29894}}
```

```
Solve[ f''[x] == 0] // N
```

```
{{x → 0.777778}}
```

Αυτό *φαίνεται από το γεγονός ότι κατά το "πέρασμα" από την ρίζα* 0.25662 *η ακολουθία* Fourier *χάνει δύο μεταβολές προσήμου*

```
Fseq[x_] = createFourierSequence[ f[x]];
variations[Fseq[0.25]] - variations[Fseq[0.26]]
```

```
2
```

Λέμε *λοιπόν πως η ρίζα* 0.25662 *της πρώτης παραγώγου* ***συνεισφέρει*** *στο* $f(x)$ 2 *μεταβολές προσήμου*. Η *δεύτερη ρίζα της πρώτης παραγώγου*, 1.29894, *καθώς και η μοναδική ρίζα της δεύτερης παραγώγου*, 0.777778, *δεν συνισφέρουν καμία μεταβολή προσήμου*

```
variations[Fseq[1.29]] - variations[Fseq[1.30]]
```

```
0
```

```
variations[Fseq[0.77]] - variations[Fseq[0.78]]
```

```
0
```

Από *το θεώρημα* Fourier *λοιπόν συμπεραίνουμε πως ο αριθμός των μεταβολών προσήμου*, $sv(f(x))$, *αποτελείται από τις συνεισφορές των θετικών ριζών του* $f(x)$ — ***μία μεταβολή προσήμου ανά θετική ρίζα*** — *και από τις πιθανές συνεισφορές κάποιων ριζών ορισμένων παραγώγων του* $f(x)$ — ***άρτιος αριθμός μεταβολών προσήμου ανά θετική ρίζα παραγώγου***.

Απόπειρα απόδειξης με την ακολουθία Fourier:
Όσον *αφορά την αντικατάσταση* $x \leftarrow x + 1$, *όπως βλέπουμε από το ανάπτυγμα κατά* Taylor *του* $f(x + 1)$

```
Series[ f[x + 1], {x, 0, 4}] // Normal
```

$$f[1] + x\, f'[1] + \frac{1}{2} x^2 f''[1] + \frac{1}{6} x^3 f^{(3)}[1] + \frac{1}{24} x^4 f^{(4)}[1]$$

το πολυώνυμο $f(x + 1)$ *θα έχει τόσες μεταβολές προσήμου όσες έχει και η* Fseq(1) — *η ακολουθία* Fourier *του* $f(x)$ *υπολογισμένη στην τιμή* $x = 1$:

```
{ f[x], f'[x], f''[x], f'''[x], f''''[x]} /. x → 1
```

Από *το θεώρημα του* Fourier *ξέρουμε όμως πως για κάθε πολυώνυμο* $f(x)$ *και την αντίστοιχη ακολουθία του* Fseq(x) *ισχύει* $sv(\text{Fseq}(0)) \geq sv(\text{Fseq}(1))$ *και επομένως*

$$sv(f(x+1)) = sv(\text{Fseq}(1)) \leq sv(\text{Fseq}(0)) = sv(f(x)).$$

Μέχρις εδώ *ο τρόπος αυτός πάει καλά. Για την αντικατάσταση όμως* $x \leftarrow \frac{1}{x+1}$ *από την ακολουθία* Fourier

```
{ f[x], f'[x], f''[x], f'''[x], f''''[x]} /. x → 1
```

και το ανάπτυγμα κατά Taylor *του* $(x + 1)^n f(\frac{1}{x+1})$

```
Series[(x + 1)^4 f[1/(x + 1)], {x, 0, 4}] // Normal
```

$$f[1] + x\,(4 f[1] - f'[1]) + x^2 \left(6 f[1] - 3 f'[1] + \frac{f''[1]}{2}\right) + x^3 \left(4 f[1] - 3 f'[1] + f''[1] - \frac{1}{6} f^{(3)}[1]\right) + x^4 \left(f[1] - f'[1] + \frac{f''[1]}{2} - \frac{1}{6} f^{(3)}[1] + \frac{1}{24} f^{(4)}[1]\right)$$

που γράφεται και σαν

```
Collect[%, { f[1], f'[1], f''[1], f'''[1], f''''[1]}]
```

$$(1 + 4x + 6x^2 + 4x^3 + x^4) f[1] + (-x - 3x^2 - 3x^3 - x^4) f'[1] + \left(\frac{x^2}{2} + x^3 + \frac{x^4}{2}\right) f''[1] + \left(-\frac{x^3}{6} - \frac{x^4}{6}\right) f^{(3)}[1] + \frac{1}{24} x^4 f^{(4)}[1]$$

βλέπουμε πως δεν μπορούμε να κάνουμε καμία πρόβλεψη για τον αριθμό των μεταβολών προσήμου του $(x + 1)^n f(\frac{1}{x+1})$. *Πρέπει να ξέρουμε τις τιμές των παραγώγων για* $x = 1$.

Απόπειρα απόδειξης με τις ρίζες:

Για ευκολία χωρίζουμε τις θετικές ρίζες ρ_+ του $f(x)$ σε μικρότερες, ίση και μεγαλύτερες απο το 1. Δηλαδή $\rho_+ = \rho_{<1} + 1 + \rho_{>1}$. Κατά τον ίδιο τρόπο χωρίζουμε και τις θετικές ρίζες των παραγώγων του $f(x)$ που **συνεισφέρουν** στις μεταβολές προσήμου. Δηλαδή έχουμε $\pi_+ = \pi_{<1} + \pi_{=1} + \pi_{>1}$. Συνεπώς, ο αριθμός των μεταβολών προσήμου είναι

$$sv(f(x)) = (\rho_{<1} + 2\, j\, \pi_{<1}) + (1 + 2\, k\, \pi_{=1}) + (\rho_{>1} + 2\, \ell\, \pi_{>1}).$$

Με την αντικατάσταση $x \leftarrow x + 1$ οι ρίζες του $f(x)$ και εκείνες των παραγώγων του που βρίσκονται στο διάστημα $(0, 1)$ θα μετακινηθούν στο διάστημα $(-1, 0)$, και έτσι το πολυώνυμο $f(x + 1)$ θα έχει $sv(f(x + 1))$ μεταβολές προσήμου, όπου

$$sv(f(x + 1)) \le \rho_{>1} + 2\, \ell\, \pi_{>1}.$$

Από την άλλη, με την αντικατάσταση $x \leftarrow \frac{1}{x+1}$ — που είναι ισοδύναμη με την αντικατάσταση $x \leftarrow \frac{1}{x}$ ακολουθούμενη από την $x \leftarrow x + 1$ (βλέπε 6.3.1) — έρχεται η σειρά των ριζών του $f(x)$ και εκείνων των παραγώγων του που βρίσκονται στο διάστημα $(1, \infty)$ να μετακινηθούν στο διάστημα $(-1, 0)$. Έτσι το πολυώνυμο $(x + 1)^n f(\frac{1}{x+1})$ θα έχει $sv((x + 1)^n f(\frac{1}{x+1}))$ μεταβολές προσήμου, όπου

$$sv((x + 1)^n f(\tfrac{1}{x+1})) \le \rho_{<1} + 2\, j\, \pi_{<1}.$$

Στην περίπτωση αυτή όμως μπορεί να συμβεί το εξής: μία θετική ρίζα παραγώγου που μένει στο διάστημα $(0, \infty)$ μετά την αντικατάσταση $x \leftarrow \frac{1}{x+1}$ σταματάει να συνεισφέρει μεταβολές προσήμου στο $(x + 1)^n f(\frac{1}{x+1})$ και το "έργο" αυτό "αναλαμβάνει" μια θετική ρίζα **άλλης** παραγώγου. Βλέπε για παράδειγμα το πολυώνυμο, $f(x) = 924x^7 - 86x^6 - 962x^5 - 715x^4 + 112x^3 + 831x^2 - 518x + 91$ (Strzebonski). Πως μπορούμε να διαβεβαιώσουμε πως με την αλλαγή συνεισφοράς δεν εμφανίζονται περισσότερες μεταβολές προσήμου;

Από τα παραπάνω βλέπουμε πως η αντικατάσταση $x \leftarrow \frac{1}{x+1}$ είναι η προβληματική περίπτωση. Αν μπορέσουμε να δείξουμε πως $sv((x + 1)^n f(\frac{1}{x+1})) \le sv(f(x)) - sv(f(x + 1))$, τότε θα έχουμε το ζητούμενο

$$sv(f(x + 1)) + sv((x + 1)^n f(\tfrac{1}{x+1})) \le sv(f(x)),$$

και η ισότητα θα ισχύει μόνον όταν $\rho_+ = \rho_{<1} + \rho_{>1}$ *και* $\pi_+ = 0$.//

Ακολουθεί *μία ακόμα συνθήκη πριν παρουσιάσουμε τον αλγόριθμο*.

Συνθήκη 2η:
Έστω $p(x) = 0$ *μία πολυωνυμική εξίσωση βαθμού* $n > 1$, *με ρητούς συντελεστές και χωρίς πολλαπλές ρίζες που αντιστοιχεί στην κορυφή του δυαδικού δένδρου που προαναφέραμε. Έστω επιπλέον ότι η αντικατάσταση*

$$x \leftarrow a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_h + \cfrac{1}{x}}}},$$

όπου $a_1 \geq 0$ *τυχαίος μη αρνητικός ακέραιος και* $a_2, a_3, \ldots, a_m$ *τυχαίοι θετικοί ακέραιοι,* $a_i > 0$, $1 < i \leq h \leq m$, (*το m ορίζεται από την* (1) *του θεωρήματος του* Vincent) *μετασχηματίζει την πολυωνυμική εξίσωση* $p(x) = 0$ *σε μία άλλη που αντιστοιχεί σε* V_0 ή V_1 *τερματικό κόμβο. Τότε για όλα τα* i, $1 \leq i \leq h$ *ισχύει*

$$a_i = O(\mid p(x) \mid_\infty)$$

Συζήτηση:
Η *δεύτερη αυτή συνθήκη, όπως και η* 1η, *μας χρειάζεται για την* ***θεωρητική ανάλυση*** *της μεθόδου των συνεχών κλασμάτων*.

Όπως *είδαμε η μέθοδος των συνεχών κλασμάτων κατά* Vincent *παρουσιάζει εκθετική συμπεριφορά σχετικά με τον* ***αριθμό*** *των αντικαταστάσεων της μορφής* $x \leftarrow x + 1$ *που πρέπει να εκτελεσθούν για τον υπολογισμό κάποιου μερικού πηλίκου* a_i.

Η *εκθετική συμπεριφορά της μεθόδου των συνεχών κλασμάτων εξαλείφθηκε από τον γράφοντα που υπολογίζει, με την βοήθεια του θεωρήματος του* Cauchy (*ενότητα* 6.2.5), *τα* a_i *σαν τα κάτω φράγματα θετικών ριζών πολυωνύμων. Έτσι, στον ίδιο περίπου χρόνο που χρειάζεται να εκτελεσθεί* ***μία*** *αντικατάσταση της μορφής* $x \leftarrow x + 1$ *εκτελείται η αντικατάσταση* $x \leftarrow x + a_i$.

Υπάρχει όμως και το εξής πρόβλημα: *το* ***μέγεθος*** *των ακέραιων συντελεστών των πολυωνύμων που προκύπτουν από την αντικατάσταση* $x \leftarrow x + a_i$ *αυξάνεται και για πάρα πολύ μεγάλα* a_i ***επιβραδύνει*** *τους υπολογισμούς*.

Γεννιέται λοιπόν το ερώτημα αν υπάρχει **ένα πάνω φράγμα στις τιμές των a_i** για να μπορέσουμε να προβλέψουμε τον χρόνο υπολογισμού της μεθόδου.

Διακρίνουμε δύο περιπτώσεις:

Α. Οι ρίζες α_i του πολυωνύμου επιλέγονται από εμάς και το πολυώνυμο γράφεται ως $p(x) = (x - \alpha_1)\cdots(x - \alpha_n)$. Στην περίπτωση αυτή είναι προφανές πως ισχύει

$$a_i = O(\mid p(x) \mid_\infty),$$

διότι όπως ξέρουμε η σταθερά του πολυωνύμου ισούται με το γινόμενο των ριζών και $\mid p(x) \mid_\infty$ είναι ο μεγαλύτερος συντελεστής σε απόλυτη τιμή.

Β. Οι ρίζες είναι τυχαίες. Στην περίπτωση αυτή τα πράγματα είναι λίγο πιο σύνθετα.

Από την μία μεριά είναι γνωστό πως όταν αναπτύσουμε άρρητους αριθμούς σε συνεχή κλάσματα εμφανίζονται μεγάλα μερικά πηλίκα για τα οποία ***δεν είναι γνωστό κανένα πάνω φράγμα***. Για παράδειγμα, το 432ο μερικό πηλίκο στην ανάπτυξη του π είναι 20776, κάτι που δεν θα μπορούσαμε να το φανταστούμε.

```
Last[ContinuedFraction[π, 432]]
```

```
20776
```

Από την άλλη μεριά έχουμε το θεώρημα των Gauss-Kuzmin που μας λέει πως, για σχεδόν όλους τους αριθμούς, η ***πιθανότητα*** να είναι το a_i, το i-στό μερικό πηλίκο, ίσο με τον θετικό ακέραιο j είναι

$$\log_2 \frac{(j+1)^2}{j(j+2)}.$$

Αυτό σημαίνει πως, για σχεδόν όλους τους αριθμούς, $a_i = 1$ με πιθανόνητα 0.41. Ομοίως $a_i = 20776$ με πιθανότητα $3.34\cdot10^{-9}$ ή ≈ 0.

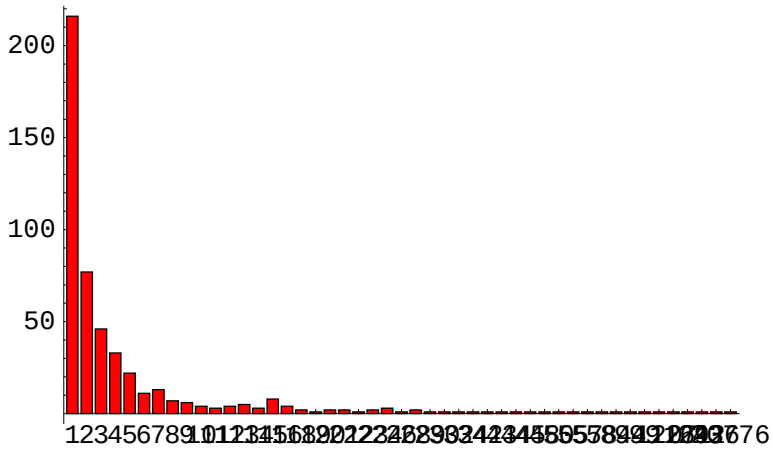
Η στατιστική ανάλυση των μερικών πηλίκων του π συμφωνεί με το θεώρημα των Gauss-Kuzmin.

```
<< Statistics`DataManipulation`
```

```
freq = Frequencies[ContinuedFraction[π, 500]];

<< Graphics`Graphics`

BarChart[freq];
```



Από *τα* 500 *μερικά πηλίκα τα* 216 *ήταν* 1, *δηλαδή ποσοστό περίπου* 43%.

Γενικά *λοιπόν, το θεώρημα των* Gauss-Kuzmin *μας λέει πως δεν μπορούμε να βρούμε ένα πάνω φράγμα στις τιμές των* a_i. **Ειδικά όμως για την περίπτωσή μας**, *επειδή χρησιμοποιούμε πολύ λίγα μερικά πηλίκα για να απομονώσουμε τις ρίζες, το ίδιο το θεώρημα των* Gauss-Kuzmin *μας λέει πως η πιθανότητα εμφάνισης μεγάλων μερικών πηλίκων είναι ίση με μηδέν. Άρα λοιπόν η συνθήκη μας είναι δικαιολογημένη.*//

Συμπέρασμα: Από *την συζήτηση της* 2*ης συνθήκης προκύπτει ότι* ***η μέθοδος των συνεχών κλασμάτων θα είναι λίγο αργή για πάρα πολύ μεγάλα*** *μερικά πηλίκα. Το συμπέρασμα αυτό επιβεβαιώνεται και πειραματικά στην επόμενη ενότητα όπου εμείς επιλέγουμε ρίζες — και άρα αναγκάζουμε τα μερικά πηλίκα να είναι — της τάξης* 10^{300} (1000 bits)! **Σε όλες τις άλλες περιπτώσεις είναι η μέθοδος των συνεχών κλασμάτων είναι η πιο γρήγορη στον κόσμο**.

Ακολουθεί *ο αλγόριθμος για την απομόνωση των θετικών ριζών όπου αλλάζουμε λίγο την μορφή της τριάδας* $\{f(x), \mathrm{M}(x), v_f\}$ *και — δεδομένου ότι* $\mathrm{M}(x) = \frac{a\,x+b}{c\,x+d}$, *για μη αρνητικούς ακέραιους* a, b, c, *και* d *έτσι ώστε* $ad - bc \neq 0$ *— την γράφουμε σαν* $\{a, b, c, d, f, v\}$. *Όπως και πριν το διάστημα με άκρα* $\frac{b}{d}$, *και* $\frac{a}{c}$

(*η διάταξη των οποίων* ***δεν είναι γνωστή***) *συμβολίζεται ως interval*(*a*, *b*, *c*, *d*). Η *κλιμάκωση των ριζών στο* 4*ο βήμα του αλγορίθμου οφείλεται στον* Strzebonski (1994). Η *τιμή της παραμέτρου* ℓb_0 *στο βήμα αυτό βρίσκεται εμπειρικά και στον αλγόριθμό μας είναι* $\ell b_0 = 16$.

Αλγόριθμος: Ο *κλασσικός αλγόριθμος των* Vincent - Akritas - Strzebonski (1836, 1978, 1994) *για τις θετικές ρίζες*.

Είσοδος: $p(x) = 0$, *μία πολυωνυμική εξίσωση με ακέραιους συντελεστές, χωρίς πολλαπλές ρίζες και* $p(0) \neq 0$.
Έξοδος: Τ*α διαστήματα απομόνωσης των* ***θετικών*** *ριζών του* $p(x)$ ή *οι ακριβείς θετικές ρίζες σε μορφή διαστημάτων*.

==========

1. Α*ρχικοποιούμε την λίστα των διαστημάτων απομόνωσης των ριζών rootIsolationIntervals* = {}. Θ*έτουμε* $f \leftarrow p(x)$ *και υπολογίζουμε* $v \leftarrow sv(f)$. Α*ν* $v = 0$ *επιστρέφουμε την άδεια λίστα* {}. Α*ν* $v = 1$ *επιστρέφουμε την λίστα* $\{(0, \boldsymbol{ub})\}$, *όπου* ***ub*** *είναι ένα πάνω φράγμα στις θετικές ρίζες του f που υπολογίζεται με την συνάρτηση* CauchyPositiveRootUpperBound[]. Θ*έτουμε την* "*τριάδα*" {1, 0, 0, 1, *f*, *v*} *στην λίστα των διαστημάτων προς εξέταση intervalsToBeProcessed***.**

2. (* *επεξεργασία διαστήματος* (*βήματα* 3-10) *)
Α*ν η λίστα intervalsToBeProcessed είναι άδεια επιστρέφουμε την λίστα rootIsolationIntervals*, *αλλιώς* ***επαναλαμβάνουμε*** *την εξής διαδικασία*: *βγάζουμε την* ***πρώτη*** "*τριάδα*" {*a*, *b*, *c*, *d*, *f*, *v*} *από την λίστα intervalsToBeProcessed*.

3. Μ*ε την συνάρτηση* CauchyPositiveRootLowerBound[] *υπολογίζουμε ένα κάτω φράγμα* ℓb *στις θετικές ρίζες του f*.

4. Α*ν* $\ell b > \ell b_0$ θ*έτουμε* $f(x) \leftarrow f(\ell b \cdot x)$, $a \leftarrow \ell b \cdot a$, $c \leftarrow \ell b \cdot c$, *και* $\ell b \leftarrow 1$.

5. Α*ν* $\ell b \geq 1$ *θέτουμε* $f(x) \leftarrow f(x + \ell b)$, $b \leftarrow \ell b \cdot a + b$, *και* $d \leftarrow \ell b \cdot c + d$. Α*ν* $f(0) = 0$, *επισυνάπτουμε το διάστημα* $\{\frac{b}{d}, \frac{b}{d}\}$ *στην λίστα rootIsolationIntervals και θέτουμε* $f(x) \leftarrow \frac{f(x)}{x}$. Υ*πολογίζουμε* $v \leftarrow sv(f)$. Α*ν* $v = 0$ *πηγαίνουμε στο βήμα* 2. Α*ν* $v = 1$ *επισυνάπτουμε το διάστημα interval*(*a*, *b*, *c*, *d*) *στην λίστα rootIsolationIntervals και πηγαίνουμε στο βήμα* 2.

6. Υπολογίζουμε $f_1(x) \leftarrow f(x+1)$ και θέτουμε $a_1 \leftarrow a$, $b_1 \leftarrow a+b$, $c_1 \leftarrow c$, $d_1 \leftarrow c+d$, και $r \leftarrow 0$. Αν $f_1(0) = 0$, επισυνάπτουμε το διάστημα $\{\frac{b_1}{d_1}, \frac{b_1}{d_1}\}$ στην λίστα *rootIsolationIntervals* και θέτουμε $f_1(x) \leftarrow \frac{f_1(x)}{x}$, και $r \leftarrow 1$. Υπολογίζουμε $v_1 \leftarrow sv(f_1)$ και θέτουμε $v_2 \leftarrow v - v_1 - r$, $a_2 \leftarrow b$, $b_2 \leftarrow a+b$, $c_2 \leftarrow d$, και $d_2 \leftarrow c+d$.

7. Αν $v_2 > 1$, υπολογίζουμε $f_2(x) \leftarrow (x+1)^m f(\frac{1}{x+1})$ όπου είναι ο βαθμός του f. Αν $f_2(0) = 0$, θέτουμε $f_2(x) \leftarrow \frac{f_2(x)}{x}$ και υπολογίζουμε $v_2 \leftarrow sv(f_2)$.

8. Αν $v_1 < v_2$, ανταλλάσσουμε (swap) το $\{a_1, b_1, c_1, d_1, f_1, v_1\}$ με το $\{a_2, b_2, c_2, d_2, f_2, v_2\}$.

9. Αν $v_1 = 0$, πηγαίνουμε στο βήμα 2. Αν $v_1 = 1$ επισυνάπτουμε το διάστημα $interval(a_1, b_1, c_1, d_1)$ στην λίστα *rootIsolationIntervals*, αλλιώς επισυνάπτουμε την "τριάδα" $\{a_1, b_1, c_1, d_1, f_1, v_1\}$ στην **αρχή** της λίστας *intervalsToBeProcessed*.

10. Αν $v_2 = 0$, πηγαίνουμε στο βήμα 2. Αν $v_2 = 1$ επισυνάπτουμε το διάστημα $interval(a_2, b_2, c_2, d_2)$ στην λίστα *rootIsolationIntervals*, αλλιώς επισυνάπτουμε την "τριάδα" $\{a_2, b_2, c_2, d_2, f_2, v_2\}$ στην **αρχή** της λίστας *intervalsToBeProcessed*. Πηγαίνουμε στο βήμα 2.

==========

Όπως και στην μέθοδο του Sturm, για την απομόνωση των **αρνητικών ριζών** πρώτα εξετάζουμε αν $p(x) = p(-x)$. Αν ισχύει η ισότητα, αυτό σημαίνει πως οι αρνητικές ρίζες είναι συμμετρικές με τις θετικές για τις οποίες έχουμε ήδη υπολογίσει τα διαστήματα απομόνωσής τους. Άρα στην περίπτωση αυτή τα διαστήματα απομόνωσης των αρνητικών ριζών βρίσκονται στοιχειωδώς. Αν $p(x) \neq p(-x)$ τότε θέτουμε $p(x) \leftarrow p(-x)$, επαναλαμβάνουμε τον παραπάνω αλγόριθμο ακόμα μία φορά και στο τέλος απεικονίζουμε τα διαστήματα απομόνωσης των ριζών στον αρνητικό ημιάξονα.

Όσον αφορά το 0, εύκολα ελέγχουμε αν $p(0) = 0$, και στην περίπτωση αυτή θέτουμε $p(x) = \frac{p(x)}{x}$.

Απαιτήσεις σε μνήμη:

Με την βοήθεια της υπόθεσης των Strzebonski-Akritas μπορούμε να αποδείξουμε πως ο μέγιστος αριθμός των τριάδων της μορφής $\{f(x), M(x), v_f\}$,

ή *ισοδύναμα της μορφής* $\{a, b, c, d, f, v\}$, *που πρέπει να αποθηκευτούν στην λίστα intervalsToBeProcessed κατά την διάρκεια εκτέλεσης της μεθόδου των συνεχών κλασμάτων είναι το πολύ*

$$1 + \log_2 n,$$

όπου n είναι ο βαθμός του αρχικού πολυωνύμου.

Πράγματι, *αν υποθέσουμε πως ισχύει η ανισότητα των μεταβολών προσήμου που αναφέραμε έπεται πως ο αριθμός των μεταβολών προσήμου κάθε τριάδας αποθηκευμένης στην λίστα είναι τουλάχιστον ίσος με τον ολικό αριθμό των μεταβολών προσήμου σε όλες τις τριάδες που προηγούνται. Επειδή ο αριθμός των μεταβολών προσήμου στην* ***πρώτη*** *τριάδα της λίστας είναι τουλάχιστον* 2, *και ο ολικός αριθμός των μεταβολών προσήμου σε όλες τις τριάδες της λίστας είναι το πολύ n, όπου n είναι ο βαθμός του αρχικού πολυωνύμου, έπεται πως ο αριθμός των τριάδων στην λίστα είναι το πολύ* $\log_2 n$. *Επομένως ο μέγιστος αριθμός μετασχηματισμένων πολυωνύμων που χρειάζεται να αποθηκεύσουμε στην λίστα είναι το πολύ* $1 + \log_2 n$.

Ακολουθεί *ο παραπάνω αλγόριθμος σε* ***αναγωγική μορφή*** (recursive) *εφαρμοσμένος στο Mathematica. Για τον αλγόριθμο αυτό χρειάζεται η νέα συνάρτηση*

```
intrv[a_,b_] := If[a>b,{b,a},{a,b}]
```

και να έχουν ενεργοποιηθεί οι παλαιότερες συναρτήσεις variations[], CauchyPositiveRootUpperBound[], *και* CauchyPositiveRootLowerBound[].

```
VASposRootIsol[p_] := Module[
  {a, b, c, d, a1, b1, c1, d1, a2, b2, c3, d2, at, bt, ct, dt,
   intervalsToBeProcessed = {}, lb, rootIsolationIntervals = {},
   f = p, f1, f2, ft, r, ub, v, v1, v2, vt, x},

  (*  step 1*)
  x = First[Variables[f]];
  v = variations[f];
  ub = CauchyPositiveRootUpperBound[f];
  If[v == 0, Return[rootIsolationIntervals]];
  If[v == 1, Return[{{0, ub}}]];
  PrependTo[intervalsToBeProcessed, {1, 0, 0, 1, f, v}];
```

```
(*  step 2  *)
While[intervalsToBeProcessed ≠ {},
 {a, b, c, d, f, v} = First[intervalsToBeProcessed];
 intervalsToBeProcessed = Rest[intervalsToBeProcessed];

 (*  step 3  *)
 lb = CauchyPositiveRootLowerBound[f];

 (*  step 4  *)
 If[lb > 16,
  f = (f /. x → lb x) // Expand; a = lb a; c = lb c; lb = 1];

 (*  step 5  *)
 If[lb ≥ 1,
  f = (f /. x → lb + x) // Expand; b = lb a + b; d = lb c + d];
 If[(f /. x → 0) == 0, AppendTo[rootIsolationIntervals, {b/d, b/d}];
  f = Cancel[f/x]]; v = variations[f];
 If[v == 0, Continue[];
  If[v == 1,
   AppendTo[rootIsolationIntervals, If[c ≠ 0, intrv[a/c, b/d],
     {b, b + CauchyPositiveRootUpperBound[f]}]]; Continue[]]];

 (*  step 6  *)
 f1 = (f /. x → x + 1) // Expand;
 a1 = a; b1 = a + b; c1 = c; d1 = c + d; r = 0;
 If[(f1 /. x → 0) == 0, AppendTo[rootIsolationIntervals,
   {b1/d1, b1/d1}]; f1 = Cancel[f1/x]; r = 1];
 v1 = variations[f1]; v2 = v - v1 - r; a2 = b;
 b2 = a + b; c2 = d; d2 = c + d;

 (*  step 7  *)
 If[v2 > 1,
  f2 = ((x + 1)^Exponent[f,x] (f /. x → 1/(x + 1))) // Expand // Simplify];
 If[(f2 /. x → 0) == 0, f2 = Cancel[f2/x];
  v2 = variations[f2]];

 (*  step 8  *)
 If[v1 < v2, {at, bt, ct, dt, ft, vt} = {a1, b1, c1, d1, f1, v1};
  {a1, b1, c1, d1, f1, v1} = {a2, b2, c2, d2, f2, v2};
  {a2, b2, c2, d2, f2, v2} = {at, bt, ct, dt, ft, vt}];
```

```
  (*  step 9  *)
  If[v1 == 0, Continue[]];
  If[v1 == 1,
   AppendTo[rootIsolationIntervals, If[c1 ≠ 0, intrv[a1/c1, b1/d1],
     {b1, b1 + CauchyPositiveRootUpperBound[f1]}]],
   PrependTo[intervalsToBeProcessed, {a1, b1, c1, d1, f1, v1}]];

  (*  step 10  *)
  If[v2 == 0, Continue[]];
  If[v2 == 1,
   AppendTo[rootIsolationIntervals, If[c2 ≠ 0, intrv[a2/c2, b2/d2],
     {b2, b2 + CauchyPositiveRootUpperBound[f2]}]],
   PrependTo[intervalsToBeProcessed, {a2, b2, c2, d2, f2, v2}]]
  ];
  Sort[rootIsolationIntervals]
 ]
```

Έτσι *βλέπουμε πως οι* ***θετικές*** *ρίζες του πολυωνύμου* $p(x) = x^3 - 7x + 7$ *βρίσκονται στα διαστήματα απομόνωσης* $(1, \frac{3}{2})$ *και* $(\frac{3}{2}, 2)$:

```
p[x_] = x^3 - 7 x + 7; VASposRootIsol[p[x]]
```

$$\left\{\left\{1, \frac{3}{2}\right\}, \left\{\frac{3}{2}, 2\right\}\right\}$$

ενώ η μοναδική ***αρνητική*** *βρίσκεται στο διάστημα* (-4, 0).

```
VASposRootIsol[p[-x]]
```

```
{{0, 4}}
```

Ανάλυση του χρόνου υπολογισμού της μεθόδου τ:

Έστω $p(x)$ *το πολυώνυμο βαθμού* n *του οποίου θέλουμε να απομονώσουμε τις ρίζες*. Από *την ενότητα* 4.1 *του πρώτου τόμου ξέρουμε πως η αντικατάσταση της μορφής* $x \leftarrow a_i + x$ *εκτελείται σε χρόνο*

$$O(n^3 \log^2 a_i + n^2 \log a_i \log \mid p(x) \mid_\infty).$$

Από *την* (12) *ξέρουμε πως για κάθε πραγματική ρίζα του* $p(x)$ *ξέρουμε πως πρέπει να εκτελέσουμε το πολύ* m *τέτοιες αντικαταστάσεις*, *όπου*

$$m = O(n \log | p(x) |_\infty).$$

Επιπλέον, *από την δεύτερη συνθήκη ξέρουμε πως για κάθε ρίζα και για κάθε αντικατάσταση της μορφής* $x \leftarrow a_i + x$ *ισχύει*

$$a_i = O(| p(x) |_\infty).$$

Συνδιάζοντες *τα παραπάνω αποτελέσματα βλέπουμε πως μία ρίζα του* $p(x)$ *μπορεί να απομονωθεί σε χρόνο*

$$O(n^4 \log^3 | p(x) |_\infty).$$

Επομένως, *επειδή το* $p(x)$ *έχει το πολύ* n *πραγματικές ρίζες έπεται πως απομονώνονται σε χρόνο*

$$O(n^5 \log^3 | p(x) |_\infty).$$

Τόσο *θεωρητικά* όσο *και εμπειρικά η μέθοδος των συνεχών κλασμάτων για την απομόνωση των πραγματικών ριζών είναι η γρηγορότερη στον κόσμο*.

6.4 *Σύγκριση διαφόρων μεθόδων για την απομόνωση πραγματικών ριζών με διχοτόμηση*

Στην ενότητα αυτή παρουσιάζουμε πίνακες, ***διαφόρων εποχών****, που συγκρίνουν τις μεθόδους: των συνεχών κλασμάτων,* του Sturm, *των* Collins-Akritas *και μιας τροποποίησης της τελευταίας από τους* Rouillier *και* Zimmermann. *Το συμπέρασμα είναι πως η μέθοδος των συνεχών κλασμάτων* ***ήταν****, και* ***εξακολουθεί να είναι*** *η ταχύτερη μέθοδος απονόνωσης πραγματικών ριζών στον κόσμο*!

***Άνοιξη του* 1978:**

Οι πρώτοι τρεις πίνακες είναι από την διδακτορική διατριβή του γράφοντα. Εγιναν χρησιμοποιώντας το σύστημα **sac-1** *σε υπολογιστή* IBM S/370 Model 175 *και συγκρίνουν την μέθοδο των συνεχών κλασμάτων — χωρίς φυσικά την βελτίωση του* Strzebonski *— με εκείνη του* Sturm. *Προσέξτε πως στους πίνακες αυτούς ο βαθμός των πολυωνύμων είναι το πολύ* 20 *— βαθμός "απίστευτα" μεγάλος για την εποχή εκείνη*!

***Πολυώνυμα με ρίζες τυχαία επιλεγμένες από το διάστημα* $(0, 10^3)$**

Βαθμός πολυωνύμου	***συνεχή κλάσματα*** **V-A**	***διχοτόμηση*** **Sturm**
5	0.71	0.73
10	23.22	22.50
15	95.35	151.42
20	288.49	> 600

Πίνακας 6.4.1. *Κάθε πολυώνυμο βαθμού n,* (*όπου n* = 5, 10, 15 *και* 20) *στον πίνακα αυτό σχηματίστηκε παίρνοντας το γινόμενο αντίστοιχου αριθμού γραμμικών όρων.*

Πολυώνυμα με 10-ψήφιους συντελεστές τυχαία επιλεγμένους

Βαθμός πολυωνύμου	***συνεχή κλάσματα* V-A**	***διχοτόμηση* Sturm**
5	0.26	2.05
10	0.46	33.28
15	0.94	156.40
20	2.36	524.42

Πίνακας 6.4.2. Οι *συντελεστές κάθε πολυωνύμου στον πίνακα αυτό είναι όλοι τους διάφοροι του μηδενός*, 10-*ψήφιοι και τυχαία επιλεγμένοι*.

Από *τους δύο παραπάνω πίνακες είναι προφανές πως η μέθοδος των συνεχών κλασμάτων είναι κατά πολύ γρηγορότερη της μεθόδου του* Sturm. Πως *συγκρίνεται όμως με την μέθοδο των* Collins-Akritas — *μιας ακόμη μεθόδου διχοτόμησης — που είχε αναπτυχθεί μόλις δύο χρόνια νωρίτερα και που είναι και αυτή γρηγορότερη της μεθόδου του* Sturm;

Η *απάντηση την εποχή εκείνη δόθηκε έμμεσα ως εξής*: Τα *πολυώνυμα του Πίνακα* 6.4.2 *είναι τα ίδια με εκείνα που είχαν χρησιμοποιηθεί για να συγκριθεί η μέθοδος των* Collins-Akritas *με την μέθοδο του* Sturm. *Έτσι στον Πίνακα* 6.4.3 *συγκρίνουμε τους λόγους των χρόνων της μεθόδου των συνεχών κλασμάτων και της μεθόδου των* Collins-Akritas *προς τους αντίστοιχους χρόνους της μεθόδου του* Sturm.

Σύγκριση της μεθόδου των συνεχών κλασμάτων με την μέθοδο των Collins-Akritas *για τα πολυώνυμα του Πίνακα* 6.4.2

Βαθμός πολυωνύμου	***συνεχή κλάσματα* / Sturm**	**Collins-Akritas / Sturm**
5	0.13	0.28
10	0.014	0.10
15	0.004	0.05
20	0.0045	0.03

Πίνακας 6.4.3. Σύγκριση *των λόγων των χρόνων της μεθόδου των συνεχών κλασμάτων και της μεθόδου των* Collins-Akritas *προς τους αντίστοιχους χρόνους της μεθόδου του* Sturm.

Αν και η σύγκριση των δύο μεθόδων δεν ήταν εκτενής, από τον Πίνακα 6.4.3 βλέπουμε πως εμπειρικά η μέθοδος των συνεχών κλασμάτων είναι καλλίτερη της μεθόδου των Collins-Akritas. Δεδομένου ότι ο χρόνος υπολογισμού της τελευταία είναι $O(n^6 \log^2 |p(x)|_\infty)$, το συμπέρασμά μας συμφωνεί πλήρως με την θεωρητική ανάλυση των μεθόδων.

Άνοιξη του 2002:

Στην πρόσφατη εργασία τους οι Rouillier και Zimmermann (2002), παρουσιάζουν μία νέα μέθοδο απομόνωσης πραγματικών ριζών που είναι ***αφ' ενός*** μεν τόσο γρήγορη όσο και η μέθοδος των Collins-Akritas, ***αφ' ετέρου*** δε η καλλίτερη όσον αφορά την χρήση μνήμης του υπολογιστή.

Οι πίνακες που ακολουθούν συγκρίνουν την μέθοδο των συνεχών κλασμάτων (CF), όπως τροποποιήθηκε με την βελτίωση του Strzebonski, με την μέθοδο REL των Rouillier και Zimmermann. Και οι δύο μέθοδοι έγιναν μέρος του πυρήνα του *Mathematica*. Για σύγκριση βρίσκονται στην ιστοσελίδα

http://members.wolfram.com/webMathematica/Users/adams/RootIsolation.jsp

Οι δύο μέθοδοι δοκιμάστηκαν στα πολυώνυμα Chebyshev, Laguerre, Wilkinson και Mignotte, που χρησιμοποίησαν οι Rouillier και Zimmermann καθώς επίσης και σε τρεις τύπους τυχαίων πολυωνύμων που χρησιμοποιήθηκαν στην διδακτορική διατριβή του γράφοντα.

Όλοι οι υπολογισμοί έγιναν σε έναν 850 MHz Athlon PC με 256 MB RAM. Οι πληροφορίες σχετικά με την μνήμη του υπολογιστή που χρησιμοποιήθηκε αποκτήθηκαν με την συνάρτηση MaxMemoryUsed του *Mathematica*. Στην αρχή των υπολογισμών ο πυρήνας του *Mathematica* καταλαμβάνει 1.6 MB.

Ειδικά Πολυώνυμα

Πολυώνυμα	**Βαθμός**	**Αρ. ριζών**	**CF**	**REL**
			T (s)/M (MB)	T (s)/M (MB)
Chebyshev	1000	1000	2172/9.2	7368/8.5
Chebyshev	1200	1200	4851/12.8	15660/11.8
Laguerre	900	900	3790/8.7	22169/14.1
Laguerre	1000	1000	6210/10.4	34024/17.1
Wilkinson	800	800	73.4/3.24	3244/10
Wilkinson	900	900	143/3.66	5402/12.5
Wilkinson	1000	1000	256/4.1	8284/15.1
Mignotte	300	4	0.12/1.75	803/7.7
Mignotte	400	4	0.22/1.77	3422/15.8
Mignotte	600	4	0.54/1.89	26245/49.1

Πίνακας 6.4.4. *Για τα ειδικά πολυώνυμα η μέθοδος των συνεχών κλασμάτων είναι γρηγορότερη από την* REL *από* 3 *φορές — για τα πολυώνυμα* Chebyshev *— μέχρι περίπου* 50000 *φορές για τα πολυώνυμα* Mignotte.

Όπως *αναφέραμε, η μέθοδος των συνεχών κλασμάτων απομονώνει πρώτα τις θετικές ρίζες και ύστερα τις αρνητικές.* Αν *φυσικά το πολυώνυμο είναι συμμετρικό απομονώνουμε* ***μόνο τις θετικές*** *του ρίζες.* Τα *πολυώνυμα* Chebyshev *είναι συμμετρικά και έτσι εκμεταλλευόμαστε το γεγονός αυτό, κάτι που δεν κάνει η μέθοδος* REL.

Πολυώνυμα με τυχαία παραγόμενους συντελεστές (συν/στές)

Συν/στές ($\alpha\rho$. bits)	**Βαθμός**	**Αρ. ριζών**	**CF** T (s)/M (MB)	**REL** T (s)/M (MB)
10	500	3.6	0.78/2.2	1.66/2.81
10	1000	4.4	6.67/3.75	34.2/7.5
10	2000	5.6	215/11.4	562/22.8
1000	500	3.2	0.56/2.28	2.19/2.97
1000	1000	3.6	12.7/5.1	31.4/6.5
1000	2000	6	329/14.2	510/24.3

Πίνακας 6.4.5. Για *πολυώνυμα με τυχαία παραγόμενους συντελεστές η μέθοδος των συνεχών κλασμάτων* ήταν *γρηγορότερη από την* REL *από* 1.5 *μέχρι* 5 *φορές*.

Στον Πίνακα 6.4.5 *κάθε αποτέλεσμα ήταν ο μέσος όρος συνόλου* 5 *πολυωνύμων*. Ο *αριθμός των ριζών ήταν επίσης ο μέσος*. Τα *ίδια τυχαία πολυώνυμα χρησιμοποιήθηκαν και για τις* 2 *μεθόδους*.

Πολυώνυμα με τυχαία παραγόμενους συντελεστές και μοναδιαίο κύριο συντελεστή (συν/στή)

Συν/στές ($\alpha\rho$. bits)	**Βαθμός**	**Αρ. ριζών**	**CF** T (s)/M (MB)	**REL** T (s)/M (MB
10	500	5.2	1.43/2.48	8.48/3.84
10	1000	4.8	7.12/3.74	80.7/10.1
10	2000	6.8	263/11.4	1001/37.1
1000	100	4.4	0.01/1.75	56.8/5.5
1000	200	6	0.086/1.93	252/17
1000	500	5.6	0.57/2.28	1917/96.8
1000	1000	6	25.5/5.2	>5000/?

Πίνακας 6.4.6. Η *περίπτωση των πολυωνύμων με τυχαία παραγόμενους συντελεστές και μοναδιαίο κύριο συντελεστή αποδείχθηκε ιδιαίτερα* "*σκληρή*" *για την* REL *που ήταν πάλι χιλιάδες φορές αργότερη*.

Η βραδύτητα της μεθόδου REL στον Πίνακα 6.4.6 δεν είναι τυχαία. Πολυώνυμα με τυχαία παραγόμενους συντελεστές και μοναδιαίο κύριο συντελεστή έχουν ***και*** πολύ μεγάλες ***και*** πολύ μικρές ρίζες με συνέπεια μία μέθοδος διχοτόμησης να αρχίζει με ένα πάρα πολύ μεγάλο διάστημα που πρέπει να διχοτομηθεί πολλές φορές προτού απομονωθούν οι μικρές ρίζες.

Πολυώνυμα με τυχαίες παραγόμενες ρίζες

Ρίζες (αρ. bits)	**Βαθμός**	**Αρ. ριζών**	**CF** T (s)/M (MB)	**REL** T (s)/M (MB
10	100	100	0.8/1.82	0.61/1.92
10	200	200	2.45/2.07	10.1/2.64
10	500	500	33.9/2.07	878/8.4
1000	20	20	0.12/1.88	0.044/1.83
1000	50	50	16.7/3.18	4.27/2.86
1000	100	100	550/8.9	133/6.49

Πίνακας 6.4.7. Η περίπτωση των πολυωνύμων με τυχαία παραγόμενες ρίζες μεγέθους τάξης 10^{300} είναι η μόνη που η μέθοδος των συνεχών κλασμάτων είναι αργότερη της REL — και αυτό μόλις κατά 4 φορές.

Όπως αναμενόταν από την ανάλυση της μεθόδου των συνεχών κλασμάτων, το αδύνατο σημείο της μεθόδου μας είναι όταν οι ρίζες — και συνεπώς και τα μερικά πηλίκα a_i — είναι πάρα πολύ μεγάλα, δηλαδή τάξης 10^{300}. Αυτό επιβεβαιώνεται και από τον Πίνακα 6.4.7.

Από τα παραπάνω φαίνεται πως η μέθοδός μας των συνεχών κλασμάτων είναι σχεδόν πάντα γρηγορότερη από τις μεθόδους που βασίζονται στην διχοτόμηση. Και στην πράξη, η χρήση της μνήμης του υπολογιστή, αναφορικά με τα πολυώνυμα που χρειάζεται να αποθηκεύσει, είναι καλλίτερη από εκείνη της REL.

#31

Numer. Math. 52, 119–127 (1988)

Numerische Mathematik

A New Method for Computing Polynomial Greatest Common Divisors and Polynomial Remainder Sequences*

Alkiviadis G. Akritas
University of Kansas, Department of Computer Science, Lawrence, KS 66045, USA

Summary. A new method is presented for the computation of a greatest common divisor (gcd) of two polynomials, along with their polynomial remainder sequence (prs). This method is based on our generalization of a theorem by Van Vleck [12] and uniformly treats both normal and abnormal prs's, making use of Bareiss's [3] integer-preserving transformation algorithm for Gaussian elimination. Moreover, for the polynomials of the prs's, this method provides the smallest coefficients that can be expected without coefficient gcd computations (as in Bareiss [3]) and it clearly demonstrates the divisibility properties; hence, it combines the best of both the reduced and the subresultant prs algorithms.

Subject Classifications: AMS(MOS): 68C20, 68C25, 68-03, 01A55; CR: I.1.2.

1. Introduction

In this note we restrict our discussion to univariate polynomials with integer coefficients and to computations in $\mathbf{Z}[x]$, a unique factorization domain. Given the polynomial $p(x)=c_n x^n+c_{n-1}x^{n-1}+\ldots+c_0$, its degree is denoted by $\deg(p(x))$ and c_n, its leading coefficient, by $\mathrm{lc}(p)$; moreover, $p(x)$ is called *primitive* if its coefficients are relatively prime.

Consider now $p_1(x)$ and $p_2(x)$, two primitive, nonzero polynomials in $\mathbf{Z}[x]$, $\deg(p_1(x))=n$ and $\deg(p_2(x))=m$, $n\geqq m$. Clearly, the polynomial division (with remainder) algorithm, call it **PD**, that works over a field, cannot be used in $\mathbf{Z}[x]$ since it requires exact divisibility by $\mathrm{lc}(p_2)$. So we use *pseudo-division*, which always yields a pseudo-quotient and pseudo-remainder; in this process we have to premultiply $p_1(x)$ by $\mathrm{lc}(p_2)^{n-m+1}$ and then apply algorithm **PD**. Therefore we have:

$$\mathrm{lc}(p_2)^{n-m+1}\,p_1(x)=q(x)\,p_2(x)+p_3(x), \qquad \deg(p_3(x))<\deg(p_2(x)). \tag{1}$$

Applying the same process to $p_2(x)$ and $p_3(x)$, and then to $p_3(x)$ and $p_4(x)$, etc. (Euclid's algorithm), we obtain a *polynomial remainder sequence* (prs)

* This paper is affectionately dedicated to the memory of my father

$$p_1(x), p_2(x), p_3(x), \ldots, p_h(x), p_{h+1}(x) = 0,$$

where $p_h(x) \neq 0$ is a greatest common divisor of $p_1(x)$ and $p_2(x)$, $\gcd(p_1(x), p_2(x))$. If $n_i = \deg(p_i(x))$ and we have $n_i - n_{i+1} = 1$, for all i, the prs is called *normal*, otherwise, it is called *abnormal*. The problem with the above approach is that the coefficients of the polynomials in the prs grow exponentially and hence slow down the computations. We wish to control this coefficient growth. We observe that equation (1) can also be written more generally as

$$\begin{aligned} \mathrm{lc}(p_{i+1})^{n_i - n_{i+1}+1}\, p_i(x) &= q_i(x)\, p_{i+1}(x) + \beta_i\, p_{i+2}(x), \\ \deg(p_{i+2}(x)) &< \deg(p_{i+1}(x)), \end{aligned} \tag{2}$$

$i = 1, 2, \ldots, h-1$. That is, if a method for choosing β_i is given, the above equation provides an algorithm for constructing a prs. The obvious choice $\beta_i = 1$, for all i, is called the *Euclidean prs*; it was described above and leads to exponential growth of coefficients. Choosing β_i to be the greatest common divisor of the coefficients of $p_{i+2}(x)$ results in the *primitive prs*, and it is the best that can be done to control the coefficient growth. (Notice that here we are dividing $p_{i+2}(x)$ by the greatest common divisor of its coefficients before we use it again.) However, computing the greatest common divisor of the coefficients for each member of the prs (after the first two, of course) is an expensive operation and should be avoided. So far, in order both to control the coefficient growth and to avoid the coefficient gcd computations, either the *reduced* or the (improved) *subresultant* prs have been used. In the reduced prs we choose

$$\beta_1 = 1 \quad \text{and} \quad \beta_i = \mathrm{lc}(p_i)^{n_i - n_{i+1}+1}, \qquad i = 2, 3, \ldots, h-1, \tag{3}$$

whereas, in the subresultant prs we have

$$\beta_1 = (-1)^{n_1 - n_2 + 1} \quad \text{and} \quad \beta_i = (-1)^{n_i - n_{i+1}+1}\, \mathrm{lc}(p_i)\, H_i^{n_i - n_{i+1}}, \qquad i = 2, 3, \ldots, h-1, \tag{4}$$

where

$$H_2 = \mathrm{lc}(p_2)^{n_1 - n_2} \quad \text{and} \quad H_i = \mathrm{lc}(p_i)^{n_{i-1} - n_i} H_{i-1}^{1-(n_{i-1} - n_i)}, \qquad i = 3, 4, \ldots, h-1.$$

That is, in both cases above we divide $p_{i+2}(x)$ by the corresponding β_i before we use it again. The reduced prs algorithm is recommended if the prs is normal, whereas if the prs is abnormal the subresultant prs algorithm is to be preferred. The proofs that the β_i's shown in (3) and (4) exactly divide $p_{i+2}(x)$ are very complicated [6] and have up to now obscured simple divisibility properties [10], (see also [4] and [5]). For a simple proof of the validity of the reduced prs see [2]; analogous proof for the subresultant prs can be found in [8].

In what follows we present a method which uniformly treats both normal and abnormal prs's and provides the smallest coefficients in absolute value that can be expected without coefficient greatest common divisor computations [3]: moreover, this method clearly demonstrates the existing divisibility properties. We also present a theorem which is a generalization of a theorem by Van Vleck. (We have failed to detect prior use of Van Vleck's theorem in the literature.)

2. Gaussian Elimination and Sylvester's Form of the Resultant

Consider the two polynomials in $\mathbf{Z}[x]$, $p_1(x)=c_n x^n+c_{n-1}x^{n-1}+\ldots+c_0$ and $p_2(x)=d_m x^m+d_{m-1}x^{m-1}+\ldots+d_0$, $c_n\neq 0$, $d_m\neq 0$, $n\geqq m$. In the literature the most common encountered forms of the resultant of $p_1(x)$ and $p_2(x)$ are

$$\mathrm{res}_B(p_1,p_2)=\begin{vmatrix} c_n & c_{n-1} & \ldots & & c_0 & 0 & \ldots 0 \\ 0 & c_n & c_{n-1} & \ldots & & c_0 & \ldots 0 \\ & & & & & \vdots & \\ 0 & 0 & \ldots & & c_n & c_{n-1}\ldots & c_0 \\ d_m & d_{m-1} & \ldots & d_0 & 0 & 0 & \ldots 0 \\ 0 & d_m & d_{m-1} & \ldots & d_0 & 0 & \ldots 0 \\ & & & & \vdots & & \\ 0 & 0 & \ldots & d_m & d_{m-1} & & \ldots d_0 \end{vmatrix}$$

or

$$\mathrm{res}_T(p_1,p_2)=\begin{vmatrix} c_n & c_{n-1} & \ldots & & c_0 & 0 & \ldots 0 \\ 0 & c_n & c_{n-1} & \ldots & & c_0 & \ldots 0 \\ & & & & & \vdots & \\ 0 & 0 & \ldots & & c_n & c_{n-1}\ldots & c_0 \\ 0 & 0 & \ldots & d_m & d_{m-1} & \ldots & d_0 \\ & & & & \vdots & & \\ 0 & d_m & d_{m-1} & \ldots & d_0 & 0 & \ldots 0 \\ d_m & d_{m-1} & \ldots & d_0 & 0 & 0 & \ldots 0 \end{vmatrix}$$

where for both cases we have m rows of c's and n rows of d's; that is, the determinant is of order $m+n$. Contrary to established practice, we call the first Bruno's and the second Trudi's form of the resultant. (Actually, in the literature, Bruno's form is referred to as Sylvester's.) Notice that $\mathrm{res}_B(p_1,p_2)=(-1)^{n(n-1)/2}\,\mathrm{res}_T(p_1,p_2)$. However, we choose to call Sylvester's form the one described below; this form was "buried" in Sylvester's 1853 paper [11] and is only once mentioned in the literature in a paper by Van Vleck [12]. Sylvester indicates ([11], p. 426) that he had produced this form in 1839 or 1840 and some years later Cayley unconsciously reproduced it as well. It is Sylvester's form of the resultant that forms the foundation of our new method for computing polynomial remainder sequences; however, we first present the following theorem concerning Bruno's form of the resultant:

Theorem 1. (Laidacker [9]) *If we transform the matrix corresponding to* $\mathrm{res}_B(p_1,p_2)$ *into its upper triangular form* $T_B(R)$, *using row transformations only, then the last nonzero row of* $T_B(R)$ *gives the coefficients of a greatest common divisor of* $p_1(x)$ *and* $p_2(x)$.

The above theorem indicates that we can obtain only a greatest common divisor of $p_1(x)$ and $p_2(x)$ but none of the remainder polynomials. In order to compute both a $\gcd(p_1(x), p_2(x))$ and all the polynomial remainders we have

to use Sylvester's form of the resultant; this is of order $2n$ and of the following form ($p_2(x)$ has been transformed into a polynomial of degree n by introducing zero coefficients. Below $p_1(x)$ and $p_2(x)$ are replaced by $p(x)$ and $q(x)$, respectively):

$$\mathrm{res}_S(p,q)=\begin{vmatrix} c_n & c_{n-1} \dots c_0 & 0 & 0 \dots 0 \\ d_n & d_{n-1} \dots d_0 & 0 & 0 \dots 0 \\ 0 & c_n \dots & c_0 & 0 \dots 0 \\ 0 & d_n \dots & d_0 & 0 \dots 0 \\ & \dots & & \\ 0 \dots 0 & c_n & c_{n-1} & \dots c_0 \\ 0 \dots 0 & d_n & d_{n-1} & \dots d_0 \end{vmatrix} \tag{S}$$

Sylvester obtains this form from the system of equations ([11], pp. 427–428)

$$\begin{aligned} p(x)&=0 \\ q(x)&=0 \\ x\cdot p(x)&=0 \\ x\cdot q(x)&=0 \\ x^2\cdot p(x)&=0 \\ x^2\cdot q(x)&=0 \\ &\dots\dots\dots \\ x^{n-1}\cdot p(x)&=0 \\ x^{n-1}\cdot q(x)&=0 \end{aligned}$$

and he indicates that if we take k pairs of the above equations, the highest power of x appearing in any of them will be x^{n+k-1}. Therefore, we shall be able to eliminate so many powers of x, that x^{n-k} will be the highest power uneliminated and $n-k$ will be the degree of a member of the Sturmian polynomial remainder sequence generated by $p(x)$ and $q(x)$. Moreover, Sylvester showed that the polynomial remainders thus obtained are what he terms *simplified residues*; that is, the coefficients are the smallest possible obtained without integer gcd computations and without introducing rationals. Stated in other words, the polynomial remainders have been freed from their corresponding *allotrious factors.*

Example. Consider $p(x)=x^3-7x+7$ and $q(x)=3x^2-7$. Then

$$\mathrm{res}_S(p,q)=\begin{vmatrix} 1 & 0 & -7 & 7 & 0 & 0 \\ 0 & 3 & 0 & -7 & 0 & 0 \\ 0 & 1 & 0 & -7 & 7 & 0 \\ 0 & 0 & 3 & 0 & -7 & 0 \\ 0 & 0 & 1 & 0 & -7 & 7 \\ 0 & 0 & 0 & 3 & 0 & -7 \end{vmatrix}$$

and we can compute the negated coefficients of the first polynomial remainder (which is of degree $n-k=1$) if we take $k=n-1=2$ pairs of rows. So, the leading coefficient is

$$\begin{vmatrix} 1 & 0 & -7 & 7 \\ 0 & 3 & 0 & -7 \\ 0 & 1 & 0 & -7 \\ 0 & 0 & 3 & 0 \end{vmatrix} = 3 \cdot (21) - 1 \cdot 21 = 42$$

and the second coefficient is

$$\begin{vmatrix} 1 & 0 & -7 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 7 \\ 0 & 0 & 3 & -7 \end{vmatrix} = 3 \cdot (-21) = -63;$$

that is, the first polynomial remainder is $42x-63=(-1)p_3(x)$, where $p_3(x)$ was obtained from the Euclidean prs algorithm.

In general, if we have the polynomial remainder sequence $p_1(x)$, $p_2(x)$, $p_3(x)$, ..., $p_h(x)$, $\deg(p_1(x))=n$, $\deg(p_2(x))=m$, $n \geqq m$, we can obtain the (negated) coefficients of the $(i+1)$th member of the prs, $i=0, 1, 2, \ldots, h-1$, as minors formed from the first $2i$ rows of (S) by successively associating with the first $2i-1$ columns (of the $(2i)$ by $(2n)$ matrix) each succeeding column in turn.

Theorem 2. (Van Vleck [12]) *Given the polynomials in* $\mathbf{Z}[x]$ $p_1(x)=c_n x^n + c_{n-1} x^{n-1} + \ldots + c_0$ *and* $p_2(x)=d_m x^m + d_{m-1} x^{m-1} + \ldots + d_0$, $c_n \neq 0$, $d_m \neq 0$, $n \geqq m$ *then the successive polynomials which are formed from the first* $2i$ *rows of* (S) $i=1, 2, \ldots, n$ *constitute a Sturm sequence.*

From the above we see that Sylvester's form of the resultant can give us the Sturmian sequence of two polynomials (which is a normal polynomial remainder sequence). Moreover, and this is the most important fact, one does not have to compute determinants in order to find the coefficients. This is due to the fact that in the original determinant (*S*) the members of any two consecutive rows are the same as those of the two preceeding rows. So, if in any row the values of the members are changed by adding a multiple of the preceeding row, exactly the same change can be made in the members of each alternate row thereafter without altering the value of any minor which appears as a coefficient in one of our Sturm's polynomials. Therefore, we can bring the corresponding matrix into its upper triangular form without disturbing the repetitive character of the determinant. We therefore have:

Theorem 3. (Van Vleck [12]) *If we bring the matrix corresponding to Sylvester's form of the resultant, into its upper triangular form* $T_S(R)$, *then the even rows of* $T_S(R)$ *furnish the coefficients of the successive Sturm polynomial remainders. The coefficients taken from a given row are multiplied by* $(-1)^k$, *where* k *is the number of negative "constituents" in the principal diagonal above the row under consideration.*

Van Vleck demonstrated this theorem with an example [12]. However, the matrix corresponding to the resultant is transformed into its upper triangular form by performing elementary row operations and removing at each step the greatest common divisor of the coefficients, a computation which we want to avoid.

On the other hand, we transform the matrix corresponding to the resultant (S) into its upper triangular form using Bareiss's integer-preserving transformation algorithm [3]. That is: let $r_{00}^{(-1)}=1$, and $r_{ij}^{(0)}=r_{ij}$, $i,j=1,\ldots,n$; then for $k<i,j\leqq n$,

$$r_{ij}^{(k)}:=(1/r_{k-1,k-1}^{(k-2)})\cdot\begin{vmatrix} r_{kk}^{(k-1)} & r_{kj}^{(k-1)} \\ r_{ik}^{(k-1)} & r_{ij}^{(k-1)} \end{vmatrix} \tag{5}$$

Of particular importance in Bareiss's algorithm is the fact that the determinant of order 2 is divided *exactly* by $r_{k-1,k-1}^{(k-2)}$ (the proof is very short and clear and is described in Bareiss's paper [3]) and that the resulting coefficients are the smallest that can be expected without coefficient gcd computations and without introducing rationals. Notice how all the complicated expressions for β_i in the reduced and subresultant prs algorithms are mapped to the simple factor $r_{k-1,k-1}^{(k-2)}$ of this method.

It should be pointed out that using Bareiss's algorithm we will have to perform pivots (interchange two rows) which will result in a change of signs; see the example below. Therefore, care should be excercised in using Theorem 3. We also define the term *bubble* pivot as follows: if the diagonal element in row i is zero and the next nonzero element down the column is in row $i+j$, $j>1$, then row $i+j$ will become row i after pairwise interchanging it with the rows above it. Bubble pivot preserves the symmetry of the determinant.

Example. Using $p_1(x)=x^3-7x+7$ and $p_2(x)=3x^2-7$ we have

$$\begin{bmatrix} 1 & 0 & -7 & 7 & 0 & 0 \\ 0 & 3 & 0 & -7 & 0 & 0 \\ 0 & 1 & 0 & -7 & 7 & 0 \\ 0 & 0 & 3 & 0 & -7 & 0 \\ 0 & 0 & 1 & 0 & -7 & 7 \\ 0 & 0 & 0 & 3 & 0 & -7 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & -7 & 7 & 0 & 0 \\ 0 & 3 & 0 & -7 & 0 & 0 \\ 0 & 0 & 9 & 0 & -21 & 0 \\ 0 & 0 & 0 & -42 & 63 & 0 \\ 0 & 0 & 0 & 0 & 196 & -294 \\ 0 & 0 & 0 & 0 & 0 & -49 \end{bmatrix} \quad *$$

The *-ed row indicates that a pivot was performed between the 3rd and 4th rows and this means that the Sturmian remainders are $42x-63$ and 49.

Note. If we consider the rows of $T_S(R)$ in the above example, we see that each corresponds to a given polynomial whose degree is one less than the number of elements *enclosed* between the leading and trailing zeros. The case might arise where one or more coefficients of the lower powers of x are zero; in that case the degree of the polynomial can be easily determined by examining the degrees of all the rows of the upper triangular form.

What we have said so far is valid for normal polynomial remainder sequences. In order to be able to deal with abnormal prs's we need the following theorem

which is our generalization of Theorem 3 (its proof is along the same lines as those of Theorem 3).

Theorem 4. [1] *Let $p_1(x)$ and $p_2(x)$ be two polynomials of degrees n and m respectively, $n \geqq m$. Using Bareiss's algorithm transform the matrix corresponding to* $\text{res}_S(p_1, p_2)$ *into its upper triangular form $T_S(R)$; let n_i be the degree of the polynomial corresponding to the* ith *row of $T_S(R)$, $i = 1, 2, \ldots, 2n$, and let $p_k(x)$, $k \geqq 2$, be the* kth *member of the (normal or abnormal) polynomial remainder sequence of $p_1(x)$ and $p_2(x)$. Then if $p_k(x)$ is in row i of $T_S(R)$, the coefficients of $p_{k+1}(x)$ (within sign) are obtained from row $i+j$ of $T_S(R)$, where j is the smallest integer such that $n_{i+j} < n_i$. (If $n = m$ associate both $p_1(x)$ and $p_2(x)$ with the first row of $T_S(R)$.)*

Notice that as a special case of the above theorem we obtain Theorem 3 for normal prs's. We see, therefore, that based on Theorem 4, we have a new method to compute the polynomial remainder sequence and a greatest common divisor of two polynomials. This new method uniformly treats both normal and abnormal prs's and provides the smallest coefficients that can be expected without coefficient gcd computation.

3. Our Method

The inputs are two (primitive) polynomials in $\mathbf{Z}[x]$, $p_1(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_0$ and $p_2(x) = d_m x^m + d_{m-1} x^{m-1} + \ldots + d_0$, $c_n \neq 0$, $d_m \neq 0$, $n \geqq m$.

Step 1. Form the resultant (*S*), $\text{res}_S(p_1, p_2)$, of the two polynomials $p_1(x)$ and $p_2(x)$.

Step 2. Using Bareiss's algorithm (described above) transform the resultant (*S*) into its upper triangular form $T_S(R)$; then the coefficients of all the members of the polynomial remainder sequence of $p_1(x)$ and $p_2(x)$ are obtained from the rows of $T_S(R)$ with the help of Theorem 4.

Example. If we consider the polynomials $p_1(x) = x^5 + 5x^4 + 10x^3 + 5x^2 + 5x + 2$ and $p_2(x) = x^4 + 4x^3 + 6x^2 + 2x + 1$ the upper triangular form of the matrix corresponding to $\text{res}_S(p_1, p_2)$ is

$$\begin{bmatrix}
1 & 5 & 10 & 5 & 5 & 2 & 0 & 0 & 0 & 0 \\
0 & 1 & 4 & 6 & 2 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 4 & 3 & 4 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 7 & 1 & 3 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 3 & -2 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 9 & -6 & -3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 58 & 50 & 18 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -266 & -112 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -756 & -532 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -980
\end{bmatrix} \quad *$$

The $*$-ed row indicates that a pivot took place. Therefore, the members of the prs generated by $p_1(x)$ and $p_2(x)$ are $3x^2 - 2x - 1$, $-266x - 112$ and -980.

Theorem 5. *Let* $p_1(x)=c_n x^n+c_{n-1}x^{n-1}+\ldots+c_0$ *and* $p_2(x)=d_m x^m+d_{m-1}x^{m-1}+\ldots+d_0$, $c_n\neq 0$, $d_m\neq 0$, $n\geqq m$ *be two (primitive) polynomials in* $\mathbf{Z}[x]$ *and for some polynomial* $P(x)$ *in* $\mathbf{Z}[x]$ *let* $|P|_\alpha$ *represent its maximum coefficient in absolute value. Then the method described above computes a greatest common divisor of* $p_1(x)$ *and* $p_2(x)$ *along with all the polynomial remainders in time*

$$O(n^5 L(|p|_\alpha)^2)$$

where $|p|_\alpha=\max(|p_1|_\alpha, |p_2|_\alpha)$.

Proof. Since we use exact integer arithmetic the cost of an operation on two integers depends not only on the operation itself but on the length (number of bits) of the operants as well. If A is an integer, we define $L(A)$, its length, by

$$L(A)=\begin{cases}1 & A=0\\ \lfloor \log_b |A|+1\rfloor & A\neq 0\end{cases}$$

where b indicates the base of the number system in which the operant A is represented when an operation is being performed. (Notice that $A\cdot B$ is computed in time $O(L(A)\cdot L(B))$.)

We know that if n is the highest degree of the two polynomials $p_1(x)$ and $p_2(x)$, then Sylvester's matrix will be $2n$ by $2n$. It is also known that, without taking advantage of the band form of this matrix, we can bring it into its upper triangular form (using Bareiss's method), performing $O(n^3)$ multiplications. In the worst case we assume that each integer multiplication is performed among the largest integers that will appear. These largest integers can be as large as $\mathrm{res}_S(p_1, p_2)$. Using Hadamard's inequality we have

$$|\mathrm{res}_S(p_1,p_2)|\leqq \prod_{1\leqq i\leqq 2n}\Big(\sum_{1\leqq j\leqq 2n} r_{ij}^2\Big)^{1/2}\leqq (2n)^n(|p|_\alpha)^{2n}$$

where $|p|_\alpha=\max(|p_1|_\alpha, |p_2|_\alpha)$.

Thus, the time for each multiplication (i.e. $(2n)^n(|p|_\alpha)^{2n}$ by itself) is $L((2n)^n(|p|_\alpha)^{2n})^2=[nL(2n)+2nL(|p|_\alpha)]^2=O(n^2L(|p|_\alpha)^2)$ from which follows the theorem.

4. Historical Remarks

1. According to Van Vleck [12], Sylvester used the above form (S) of the resultant to obtain from its minors the coefficients of all the polynomials of the prs of $p_1(x)$ and $p_2(x)$. That is, the coefficients of the $(i+1)$th polynomial of the prs, $i=0, 1, 2, \ldots h-1$, can be obtained as minors formed from the first $2i$ rows of (S) "by associating those constituents which are contained in the first $2i-1$ columns with those of each succeeding column in turn" ([12], pp. 3–4). A polynomial so constructed is called a *subresultant*. However, Van Vleck indicated that this approach is far more laborious than computing the corresponding polynomial by the usual process of (pseudo)division.

2. Brown, in both of his papers ([4], p. 485, [5], p. 238) attributes to Collins the discovery that every polynomial of a prs is proportional to some subresultant of the first two. This fact, which is known in the literature as the *fundamental theorem of subresultants*, was first proved by Sylvester in his 1853 paper [11] and was rediscovered by Freyer in 1959 [7].

References

1. Akritas, A.G.: A new method for computing polynomial greatest common divisors. TR-86-9, University of Kansas, Department of Computer Science, Lawrence, Ks 66045, 1986
2. Akritas, A.G.: A simple validity proof of the reduced prs algorithm. Computing **38**, 369–372 (1987)
3. Bareiss, E.H.: Sylvester's identity and multistep integer-preserving Gaussian elimination. Math. Comput. **22**, 565–578 (1968)
4. Brown, W.S.: On Euclid's algorithm and the computation of polynomial greatest common divisors. J ACM **18**, 476–504 (1971)
5. Brown, W.S.: The subresultant prs algorithm. ACM Trans. Math. Software **4**, 237–249 (1978)
6. Collins, G.E.: Subresultants and reduced polynomial remainder sequences. J ACM **14**, 128–142 (1967)
7. Fryer, W.D.: Applications of Routh's algorithm to network theory problems. IEEE Trans. Circuit Theo. **CT-6**, 144–149 (1959)
8. Habicht, W.: Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens. Comment. Math. Helv. **21**, 99–116 (1948)
9. Laidacker, M.A.: Another theorem relating Sylvester's matrix and the greatest common divisor. Math. Mag. **42**, 126–128 (1969)
10. Loos, R.: Generalized polynomial remainder sequences. In: Computer algebra symbolic and algebraic computations. (Computing Supplement) Buchberger, B., Collins, G.E., Loos, R. (eds.), Vol. 4, pp. 115–137. Wien, New York: Springer 1982
11. Sylvester, J.J.: On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraical common measure. Philos. Trans. **143**, 407–548 (1853)
12. Van Vleck, E.B.: On the determination of a series of Sturm's functions by the calculation of a single determinant. Ann. Math. (Second Series) **1**, 1–13 (1899–1900)

Received November 8, 1986/September 20, 1987

Note Added in Proof.

A. Normal/abnormal *prs*'s are also called complete/incomplete *prs*'s.

B. Historical remark 3. Like Brown, D.E. Knuth attributes to Collins the fundamental theorem of subresultants; see p. 410. The art of computer programming, Vol. 2: Seminumerical algorithms. Second edition. Addison-Wesley, Reading, Massachusetts, 1981.

Matrix Computation of Subresultant Polynomial Remainder Sequences in Integral Domains

Alkiviadis G. Akritas and Evgenia K. Akritas
University of Kansas, Lawrence, USA
and
Genadii I. Malaschonok
Kiev University, Kiev, Ukraine

current e-mail addresses: akritas@uth.gr and
malaschonok@math-iu.tstu.ru

Abstract

We present an improved variant of the matrix-triangularization subresultant prs method [2] for the computation of a greatest common divisor of two polynomials A and B (of degrees m and n, respectively) along with their polynomial remainder sequence. It is improved in the sense that we obtain complete theoretical results, independent of Van Vleck's theorem [13] (which is not always true [1], [6]), and, instead of transforming a matrix of order $2 \cdot \max(m, n)$ [2], we are now transforming a matrix of order $m + n$. An example is also included to clarify the concepts.

1 Introduction

Let I be an integral domain, and let

$$A_i = \sum_{j=1}^{m} c_{ij} x^{m-j},$$

where $c_{ij} \in I$, $i = 1, 2, \ldots, n$; then

$$mat(A_1, A_2, \ldots, A_n)$$

denotes the matrix (c_{ij}) of order $n \times m$. Moreover, let $A, B \in I[x], \deg A = m, \deg B = n$ and let

$$\begin{aligned} M_k &= mat(x^{n-k-1}A, x^{n-k-2}A, \ldots, A, x^{m-k-1}B, x^{m-k-2}B, \ldots, B), \\ & \quad 0 \leq k < \min(m, n) \end{aligned}$$

be the matrix of order $(m+n-2k)\times(m+n-k)$, where M_0 is the well-known Sylvester's matrix. Then, kth subresultant polynomial of A and B is called the polynomial

$$S_k = \sum_{i=0}^{k} M_k^i x^i,$$

of degree $\leq k$, where M_k^i is a minor of the matrix M_k of order $m+n-2k$, formed by the elements of columns $1, 2, \ldots, m+n-2k-1$ and column $m+n-k-i$. Habicht's known theorem [7] establishes a relation between the subresultant polynomials $S_0, S_1, \ldots, S_{\min(m,n)-1}$ and the polynomial remainder sequence(prs) of A and B, and also demonstrates the so-called *gap* structure. (For a surprisingly simple proof of Habicht's theorem see González et al [6].)

According to the matrix-triangularization subresultant prs method (see for example Akritas' book [1] or papers [2], [3]) all the subresultant polynomials of A and B can be computed *within sign* by transforming the matrix (suggested by Sylvester [12])

$$mat(x^{\max(m,n)-1}A, x^{\max(m,n)-1}B, x^{\max(m,n)-2}A, x^{\max(m,n)-2}B, \ldots, A, B),$$

of order $2\cdot\max(m,n)$, into its upper triangular form with the help of Dodgson's integer preserving transformations [5]; they are then located using an extension of a theorem by Van Vleck [2], [13]. (We depart from established practice and we give credit to Dodgson, and not to Bareiss [4], for the integer preserving transformations; see also the work of Waugh and Dwyer [14] where they use the same method as Bareiss, but 23 years earlier, and they name Dodgson as their source–differing from him only in the choice of the pivot element ([14], page 266). Charles Lutwidge Dodgson (1832–1898) is the same person widely known for his writing *Alice in Wonderland* under the pseudonym Lewis Carroll.)

Below we propose a matrix-triangularization subresultant prs method allowing us to *exactly* compute and locate the members of the prs (*without* using Van Vleck's theorem [13]) by applying Dodgson's integer preserving transformations to a matrix of order $m+n$.

2 Our Method and Its Theoretical Justification

We assume that $\deg A = m \geq \deg B = n$ and we denote by M the following matrix

$$M = mat(x^{m-1}B, x^{m-2}B, \ldots, x^{n-1}B, x^{n-1}A, x^{n-2}B, x^{n-2}A, \ldots, B, A)$$

of order $m+n$ with elements $a_{ij}(j, i = 1, 2, \ldots, m+n)$. (This matrix can be obtained from Sylvester's matrix M_0 after a rearrangement of its rows.)

Dodgson's integer preserving transformations (which can be easily proved using Sylvester's identity (S) below)

$$a_{ij}^{k+1} = \frac{(a_{ij}^k a_{kk}^k - a_{ik}^k a_{kj}^k)}{a_{k-1,k-1}^{k-1}} \qquad \text{(D)}$$

(see [4], [5], [9] or [14]) where we set $a_{00}^0 = 1$ and it is assumed that $a_{kk}^k \neq 0, k = 1, 2, \ldots, m+n$, are applied to the matrix $M = (a_{ij})$ and transform it to the upper-triangular matrix $M_D = (b_{ij}), (i, j = 1, 2, \ldots, m+n)$, where

$$b_{ij} = \begin{cases} 0 & \text{for } i > j \\ a_{ij}^i & \text{for } i \leq j \end{cases}$$

and, in general,

$$a_{ij}^k = \begin{vmatrix} a_{11} & \ldots & a_{1,k-1} & a_{1j} \\ \vdots & \ddots & \vdots & \vdots \\ a_{k-1,1} & \ldots & a_{k-1,k-1} & a_{k-1,j} \\ a_{i1} & \ldots & a_{i,k-1} & a_{ij} \end{vmatrix}$$

with $1 \leq k \leq m+n$, and $k \leq i,\ j \leq m+n$.

The following two theorems can be used to locate the members of the prs in the rows of M_D. The *correct* sign is computed.

> **Case 1:** If none of the diagonal minors of the matrix M is equal to zero, then we have:

Theorem 1. Dodgson's integer preserving transformation will transform matrix M to the upper triangular matrix M_D, which contains all n subresultants (located in rows $m+n-2k, k = 0, 1, 2, \ldots, n-1$)

$$S_k = \sum_{i=0}^{k} M_k^i x^i,$$

where

$$M_k^i = (-1)^{\sigma(k)} a_{m+n-2k,m+n-k-i}^{m+n-2k}$$

and

$$\begin{aligned} \sigma(k) &= (m-n+1) + \cdots + (m-k) \\ &= \frac{(n-k)(2m-n-k+1)}{2}, \\ k &= 0, 1, \ldots, n-1. \end{aligned}$$

Proof: It is easy to see that the submatrix located in the upper left corner of the matrix M (where the matrix M was defined in the beginning of *this section*) and having $m+n-2k$ rows and $m+n-k$ columns ($k = 0, 1, \ldots, n-1$) will be

$$M_k' = mat(x^{m-k-1}B, \ldots, x^{n-k-1}B, x^{n-k-1}A, x^{n-k-2}B, x^{n-k-2}A, \ldots, B, A).$$

M_k' differs from matrix M_k (mentioned above) only in the arrangement of the rows. That is, in order to obtain M_k from M_k' it is necessary to rearrange

$$\begin{aligned} \sigma(k) &= (m-n+1) + \cdots + (m-k) \\ &= \frac{(n-k)(2m-n-k+1)}{2}, \end{aligned}$$

adjacent rows.

Therefore we have

$$M_k^i = (-1)^{\sigma(k)} a_{m+n-2k,m+n-k-i}^{m+n-2k}$$

where $i = 0, 1, \ldots, k$, and $k = 0, 1, \ldots, n-1$. □

Before we proceed further, we state Sylvester's determinant identity [11] which is needed in the proof. If we set $\beta_{00}^0 = 1$, Sylvester's identity can be expressed as

$$detD_p(B) = (detB) \cdot (\beta_{p-1,p-1}^{p-1})^{r-p}, \quad 1 \le p \le r, \tag{S}$$

where $B = (b_{ij})$, $(i, j = 1, 2, \ldots, r)$,

$$D_p(B) = \begin{vmatrix} \beta_{p,p}^p & \beta_{p,p+1}^p & \cdots & \beta_{p,r}^p \\ \beta_{p+1,p}^p & \beta_{p+1,p+1}^p & \cdots & \beta_{p+1,r}^p \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{r,p}^p & \beta_{r,p+1}^p & \cdots & \beta_{r,r}^p \end{vmatrix}$$

of order $r-p+1$, and $\beta_{i,j}^p$ $(p, i, j = 1, 2, \ldots, r)$ are minors (just like a_{ij}^k defined above) obtained from matrix B by adding row i and column j to the (upper left) corner minor of order $p-1$ (see for example Malaschonok's work [9], ([10], pages 30–35), [4], or [8]).

> **Case 2:** If *not* all diagonal minors of the matrix M are nonzero, then we have the following theorem (the term *bubble pivot*, used below, means that, after pivoting, row i_p is *immediately* below row j_p):

Theorem 2. Dodgson's integer preserving transformations with *bubble pivot* and choice of the pivot element by column, will transform matrix M to the upper triangular matrix M_D, and at the same time will compute all subresultants S_k; if, in the process, s row replacements take place, namely row j_1 replaces row i_1, j_2 replaces $i_2, \ldots, j_s$ replaces i_s, (and after each replacement row i_p is immediately below row j_p, $p = 1, 2, \ldots, s$), then **(a)** $S_k = 0$, for all k such that $\frac{(m+n-i_p)}{2} > k > \frac{(m+n-j_p)}{2}$ and for all $p = 1, 2, \ldots, s$. **(b)** for all $p = 1, 2, \ldots, s$, if $k = \frac{(m+n-i_p)}{2}$ is an integer number not in (a), S_k is located in row i_p *before* it is replaced by row j_p. **(c)** for the remaining $k, (k = 0, 1, \ldots, n-1$ and those not in (a) or (b)) S_k is located in row $j = m + n - 2k$.

Moreover, in (b) and (c) the subresultant $S_k = \sum_{i=0}^k M_k^i x^i$, is located in row j in such a way that

$$M_k^i = (-1)^{\sigma(k)+\sigma(j)} a_{j,j+k-i}^j$$

where

$$\begin{aligned} \sigma(k) &= \frac{(n-k)(2m-n-k+1)}{2}, \\ \sigma(j) &= \sum_{p=1}^s j_p - \sum_{p=1}^s i_p, \ j_p \le j, i_p \le j. \end{aligned}$$

Proof: It is clear that the first $m-n+1$ diagonal minors are not equal to zero because a_{ss}, for $s = 1, 2, \ldots, m-n+1$, is the leading coefficient of B; therefore

$$a_{ss}^{s} = (a_{11})^{s} \neq 0, \ (s = 1, 2, \ldots, m-n+1).$$

Suppose now that for some $s > m-n+1$ we have $a_{ss}^{s} = 0$, with $a_{s-1,s-1}^{s-1} \neq 0$. In this case we have the following two subcases :

$$\textbf{I} \quad a_{is}^{s} = 0, \text{ for all } i = s, s+1, \ldots, m+n.$$

Here, making the correspondence $a_{ij}^{s} \leftrightarrow \beta_{i,j}^{p}$, $a_{ij}^{k} \leftrightarrow detB$, and $a_{s-1,s-1}^{s-1} \leftrightarrow \beta_{p-1,p-1}^{p-1}$ in Sylvester's identity, we see that $a_{is}^{s} = 0$ for $i = s, s+1, \ldots, m+n$ if and only if the first column of $D_p(B)$ is 0, and hence detB =0; that is all minors of the form a_{ij}^{k} $(k > s,\ i > s,\ j > s)$ are equal to zero, and therefore $S_k = 0$ for all $k \leq \frac{(m+n-s)}{2}$.

$$\textbf{II} \quad a_{is}^{s} = 0, \text{ for all } i = s, s+1, \ldots, p-1;\ a_{ps}^{s} \neq 0.$$

In this subcase, using again Sylvester's identity, we see that all minors $a_{ij}^{k} = 0$ $(s < k \leq p-1,\ i > s,\ j > s)$. Therefore, $S_k = 0$ for all k such that $\frac{(m+n-s-1)}{2} \geq k \geq \frac{(m+n-p+1)}{2}$. However it is necessary to continue the computation of the remaining subresultants S_k, $k \leq \frac{(m+n-p)}{2}$; in order to do this we use *bubble-pivot* to replace row s by row p, where $a_{ps}^{s} \neq 0$ plays the role of the corner mirror, and we now can continue Dodgson's integer preserving transformations. Such an interchange of rows results in all minors a_{ij}^{k} $(k > p)$ being multiplied by $(-1)^{(p-s)}$, that is, all subresultants $S_k, k = 0, 1, \ldots, k_1 (k_1 \leq \frac{(m+n-p)}{2})$ are being multiplied by $(-1)^{(p-s)}$.

Dodgson's transformations may be continued further, as long as situations **I** or **II** are not encountered. □

Note that in cases (b) and (c) Theorem 2 reduces to Theorem 1 in the case of a complete prs, and due to the fact that rows above row j change places, the sign changes by a factor $(-1)^{\sigma(j)}$.

3 Example

As in [2], it should be noted that if $|P|_\infty$ represents the maximum coefficient in absolute value of a polynomial P over the integers, then the theoretical computing time of this method is

$$O(n^5 L(|p|_\infty)^2)$$

where $|p|_\infty = max(|A|_\infty, |B|_\infty)$. Below, we present an example that helps clarify the method introduced above.

Example: If we triangularize the matrix M, of order 7, corresponding to the polynomials [1, Example 2, p. 270]

$$\begin{aligned} A = &\quad 2x^4 + 5x^3 + 5x^2 - 2x + 1 \text{ and} \\ B = &\quad 3x^3 + 3x^2 + 3x - 4 \end{aligned}$$

we obtain the following matrix:

$$\begin{pmatrix} 3 & 3 & 3 & -4 & 0 & 0 & 0 \\ 0 & 9 & 9 & 9 & -12 & 0 & 0 \\ 0 & 0 & 27 & 27 & 27 & -36 & 0 \\ 0 & 0 & 0 & -63 & 135 & 0 & 0 \\ 0 & 0 & 0 & 0 & 147 & -315 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3411 & -588 \\ 0 & 0 & 0 & 0 & 0 & 0 & 15683 \end{pmatrix}$$

along with the information that one pivot took place and row 3 was replaced by row 4.

The obtained polynomial remainder sequence is incomplete, and we only have the remainders $-63x + 135$ and 15683, of degree 1 and 0 respectively. However, we still have to determine the signs of these remainders; since pivoting took place, we are going to use Theorem 2 above.

In Theorem 2 we see have that we have to compute the quantity $(-1)^{\sigma(k)+\sigma(j)}$ for $k = 0,$ and 2, and $j = 4$, by which the two remainders are going to be multiplied. By the formula stated in the theorem, and given that the degrees are $m = 4$ and $n = 3$, we see that

- $\sigma(0) = (3-0)(2 \cdot 4 - 3 - 0 + 1)/2 = 9,$
- $\sigma(2) = (3-2)(2 \cdot 4 - 3 - 2 + 1)/2 = 2,$
- $\sigma(4) = 4 - 3 = 1$

Therefore, 15683, the remainder of degree 0, is multiplied times $(-1)^{9+1} = 1$ whereas, $S_2 = -63x + 135$, the remainder of degree 1, is multiplied times $(-1)^{2+1} = -1$.

References

[1] Akritas, A. G. *Elements of Computer Algebra with Applications*. J. Wiley Interscience, New York, 1989.

[2] Akritas, A. G. A new method for computing polynomial greatest common divisors and polynomial remainder sequences. Numerische Mathematik **52**, 119–127, 1988.

[3] Akritas, A. G. Exact algorithms for the matrix-triangularization subresultant prs method. Proceedings of the Conference on Computers and Mathematics, Boston, Massachusetts, 145–155, June 1989.

[4] Bareiss, E. H. Sylvester's identity and multistep integer-preserving Gaussian elimination. Mathematics of Computation **22**, 565–578, 1968.

[5] Dodgson, C. L. Condensation of determinants. Proceedings of the Royal Society of London **15**. 150–155, 1866.

[6] González, L., Lombardi, H., Recio, T., and Roy, M-F. Spécialization de la suite de Sturm et sous–résultants. University of Cantabria, Department of Mathematics, Statistics and Computation, Technical Report 8–1990, S-39071 Santander, Spain.

[7] Habicht, W. Eine Verallgemeinerung des Sturmschen Wurzelzaelverfahrens. Commentarii Mathematici Helvetici **21**, 99–116, 1948.

[8] Kowalewski, G. *Einfürung in die Determinantentheorie*. Chelsea, New York, 1948.

[9] Malaschonok, G. I. Solution of a system of linear equations in an integral domain. USSR Journal of Computational Mathematics and Mathematical Physics **23**, 1497–1500, 1983 (in Russian).

[10] Malaschonok, G. I. *System of Linear Equations over a Commutative Ring*. Academy of Sciences of Ukraine. Lvov, 1986 (in Russian).

[11] Sylvester, J. J. On the relation between the minor determinants of linearly equivalent quadratic functions. Philosophical Magazine **1** (Fourth Series), 259–305, 1851.

[12] Sylvester, J. J. On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest common measure. Philoshophical Transactions **143**, 407–548, 1853.

[13] Van Vleck, E. B. On the determination of a series of Sturm's functions by the calculation of a single determinant. Annals of Mathematics **1**, Second Series, 1–13, 1899–1900.

[14] Waugh, F. V. and P. S. Dwyer Compact computation of the inverse of a matrix. Annals of Mathematical Statistics **16**, 259–271, 1945.