Αναδρομικές ακολουθίες
και
Θεωρία Αριθμών

Εμμανουήλ Καπνόπουλος

Επιβλέπων καθηγητής
Ιωάννης Αντωνιάδης

Μεταπτυχιακή Εργασία

Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών
Πανεπιστήμιο Κρήτης
Ηράκλειο
Οκτώβριος 2015

Η παρούσα μεταπτυχιακή εργασία κατατέθηκε στο τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών του Πανεπιστημίου Κρήτης τον Οκτώβριο του 2015 στα πλαίσια του μεταπτυχιακού προγράμματος "Μαθηματικά και Εφαρμογές τους΄΄ στην κατεύθυνση "Μαθηματικά για την Εκπαίδευση΄΄.
Την επιτροπή αξιολόγησης αποτέλεσαν οι:

Ιωάννης Αντωνιάδης, (επιβλέπων),
Νικόλαος Τζανάκης,
Χρήστος Κουρουνιώτης,

τους οποίους ευχαριστώ για την συμμετοχή τους στην επιτροπή αυτή.
Ιδιαίτερα ευχαριστώ τον κ. Αντωνιάδη για την καθοδήγησή του, αλλά και για την ψυχολογική υποστήριξη κατά την εκπόνηση αυτής της εργασίας.
Ακόμα, ευχαριστώ τον κ. Δημήτρη Καλοψικάκη για την βοήθειά του στο τρίτο μέρος αυτής της εργασίας όπου χρειάστηκα ένα πρόγραμμα στη γλώσσα Python και ο κ. Καλοψικάκης το υλοποίησε.
Τέλος, νιώθω την ανάγκη να ευχαριστήσω τον κ. Μιχάλη Παπαδημητράκη αλλά και την κα. Μαρία Λουκάκη για όλη τους την βοήθεια κατά την διάρκεια των σπουδών μου.

Στους γονείς μου, Παντελή και Ειρήνη
και στον αδερφό μου Αναστάσιο.

Περιεχόμενα

Εισαγωγή

Ο στόχος της παρούσας μεταπτυχιακής εργασίας είναι η μελέτη των αναδρομικών ακολουθιών γενικά και ιδιαίτερα αυτών τάξεως 2. Η ακολουθία $U_n, n \in \mathbb{N}$ θα ονομάζεται αναδρομική αν ικανοποιεί μία σχέση της μορφής

$$U_{n+k} = a_1 U_{n+k-1} + a_2 U_{n+k-2} + \cdots + a_k U_n$$

και ο αριθμός k θα ονομάζεται τάξη της ακολουθίας.

Στο πρώτο κεφάλαιο της εργασίας ασχολούμαστε με την κατασκευή μιας γενικότερης θεωρίας για τις αναδρομικές ακολουθίες. Ορίζουμε την χαρακτηριστική εξίσωση της αναδρομικής σχέσης και μελετούμε υπό ποιες προϋποθέσεις οι ρίζες αυτής της εξίσωσης αποτελούν την βάση της αναδρομικής ακολουθίας. Για να πετύχουμε το σκοπό μας, ξεχωρίζουμε τρεις περιπτώσεις, ανάλογα με την πολλαπλότητα των ριζών της χαρακτηριστικής εξίσωσης, δηλαδή αν η χαρακτηριστική εξίσωση έχει όλες τις ρίζες της απλές, αν έχει μόνο μία ρίζα πολλαπλότητας $k > 1$ και φυσικά αν έχεις ρίζες $q_1, q_2, \ldots, q_m$ πολλαπλότητας $r_1, r_2, \ldots, r_m$ αντίστοιχα. Ως ειδικές περιπτώσεις μελετούμε την αριθμητική και την γεωμετρική πρόοδο, ακολουθίες που διδάσκονται οι μαθητές στο Λύκειο. Ακόμα, ορίζουμε την ακολουθία F_n του Fibonacci και την ακολουθία L_n του Lucas, και εφαρμόζουμε την θεωρία που αναπτύσσουμε και σε αυτές. Οι δύο τελευταίες ακολουθίες θα μελετηθούν εκτενέστερα στα επόμενα δύο κεφάλαια.

Στο δεύτερο μέρος της εργασίας ορίζουμε τις γενικευμένες ακολουθίες του Lucas $U_n, V_n, n \in \mathbb{N}$. Οι δύο αυτές ακολουθίες αποτελούν γενικεύσεις των ακολουθιών F_n, L_n. Αποδεικνύουμε ορισμένες ταυτότητες των ακολουθιών U_n και V_n και μελετούμε τους κανόνες διαιρετότητας των ακολουθιών αυτών. Στο τέλος του δεύτερου κεφαλαίο αποδεικνύουμε δύο αλγοριθμικά tests για την πιστοποίηση πρώτων αριθμών, tests που βασίζονται στις γενικευμένες ακολουθίες Lucas.

Στο τρίτο και τελευταίο μέρος της εργασίας μελετούμε τους όρους που ειναι τρίγωνοι αριθμοί στις ακολουθιες F_n, L_n και P_n. Ένας φυσικός αριθμός l θα ονομάζεται τρίγωνος αν και μόνον αν $l = \frac{1}{2}m(m+1)$, για κάποιο φυσικό αριθμό m. Αν ο αριθμός l είναι τρίγωνος, τότε ο αριθμός $8l+1$ είναι τέλειο τετράγωνο ενός φυσικούς αριθμού, επομένως στην απόδειξη αρκεί να βρούμε για ποιους n ο $8F_n + 1$, $8L_n + 1$ ή $8P_n + 1$ είναι τέλειο τετράγωνο. Αυτό θα γίνει με τη βοήθεια ενός κριτηρίου στο οποίο χρησιμοποιούμε το σύμβολο του Jacobi. Καταλήγουμε στο συμπέρασμα ότι στην ακολουθία Fibonacci, οι μόνοι όροι που είναι τρίγωνοι αριθμοί είναι οι $F_{\pm 1}, F_2, F_4, F_8, F_{10}$. Στην ακολουθία Lucas, οι μόνοι όροι που είναι τρίγωνοι αριθμοί είναι οι $L_1, L_{\pm 2}, L_{\pm 18}$, ενώ για την ακολουθία του Pell, οι όροι που είναι τριγωνοι αριθμοί είναι αυτοί με δείκτη ± 1, δηλαδή οι $P_{\pm 1}$.

Κεφάλαιο 1

Αναδρομικές ακολουθίες

1.1 Ακολουθίες

ΟΡΙΣΜΟΣ 1.1.1 (Ακολουθία και τάξη ακολουθίας)**:** Κάθε συνάρτηση $f(n)$ με πεδίο ορισμού τους φυσικούς αριθμούς $\mathbb{N}$ ονομάζεται ακολουθία. Συνήθως, αντί για $f(n)$ χρησιμοποιούμε τον συμβολισμό U_n και οι όροι της ακολουθίας συμβολίζονται με $U_1, U_2, \ldots, U_n, \ldots$ όπου $n \in \mathbb{N}$.

Αν υπάρχουν φυσικοί αριθμοί k, m και $a_1, a_2, \ldots, a_k \in \mathbb{C}$ τέτοιοι ώστε:

$$U_{n+k} = a_1 U_{n+k-1} + a_2 U_{n+k-2} + \cdots + a_k U_n \quad \forall n \geq m \geq 1 \tag{1.1}$$

η U_n ονομάζεται *αναδρομική ακολουθία τάξεως* k ενώ η (1.1) ονομάζεται *αναδρομική σχέση τάξεως* k.

Παραδείγματα αναδρομικών ακολουθιών

1. Γεωμετρική πρόοδος:

   $U_1 = a, U_2 = aq, U_3 = aq^2, \ldots U_n = aq^{n-1}, \ldots$

   Άρα

   $$U_{n+1} = qU_n$$

   επομένως η γεωμετρική πρόοδος ειναι αναδρομική ακολουθία τάξεως $k = 1$.

2. Αριθμητική πρόοδος:

   $U_1 = a, U_2 = a + d, U_3 = a + 2d, \ldots U_n = a + (n-1)d, \ldots$

   Άρα,

   $$U_{n+1} = U_n + d.$$

   Η τελευταία σχέση, όμως, δεν είναι της μορφής (1.1). Γι'αυτό, στην τελευταία σχέση αυξάνουμε το n κατά μία μονάδα και προκύπτει

   $$U_{n+2} = U_{n+1} + d$$

Οπότε, αν αφαιρέσουμε κατά μέλη τις δύο σχέσεις, προκύπτει ότι:

$$U_{n+2} - U_{n+1} = U_{n+1} - U_n$$

ή ισοδύναμα

$$U_{n+2} = 2U_{n+1} - U_n$$

Επομένως, κάθε αριθμητική πρόοδος ειναι αναδρομική ακολουθία τάξεως $k = 2$.

3. Μια ακολουθία που θα μας απασχολήσει ιδιαίτερα είναι αυτή των αριθμών Fibonacci. Το πρόβλημα του οποίου η λύση είναι η ακολουθία Fibonacci συνίσταται στο πόσα ζευγάρια κουνελιών θα αποκτήσουμε σε n μήνες αν κάθε ενήλικο ζευγάρι κουνελιών γεννάει ένα ζευγάρι κάθε μήνα και κάθε ζευγάρι κουνελιών ενηλικιώνεται σε περίοδο ενός μήνα. Αν με F_n συμβολίσουμε τους όρους της ακολουθίας που προκύπτει, τότε: $F_1 = 1, F_2 = 1, F_3 = 2$ Ας υποθέσουμε ότι έχουμε υπολογίσει το πλήθος των ζευγαριών μετά από $(n-1)-$ μήνες κι έστω ότι αυτό είναι F_n και το πλήθος των ζευγαριών μετά από n μήνες, έστω F_{n+1}. Σε αυτόν το μήνα, κάθε ζευγάρι θα δώσει από ένα νέο ζευγάρι άρα μετά από $(n+1)-$ μήνες θα έχουμε ότι το πλήθος των ζευγαριών F_{n+2} θα ισούται με:

$$F_{n+2} = F_{n+1} + F_n$$

Επομένως η ακολουθία των αριθμών Fibonacci είναι αναδρομική τάξεως $k = 2$.

4. Έστω η ακολουθία των τετραγώνων των φυσικών αριθμών, δηλαδή

$$U_1 = 1^2, U_2 = 2^2, U_3 = 3^2, \ldots, U_n = n^2, \ldots$$

Τότε $U_{n+1} = (n+1)^2 = n^2 + 2n + 1 = U_n + 2n + 1$, άρα

$$U_{n+1} = U_n + 2n + 1$$

Αν σε αυτήν τη σχέση αυξήσουμε το n κατά ένα, προκύπτει ότι

$$U_{n+2} = U_{n+1} + 2n + 3.$$

Αφαιρούμε κατά μέλη τις δύο αυτές σχέσεις και προκύπτει:

$$U_{n+2} = 2U_{n+1} - U_n + 2$$

Επαναλαμβάνουμε την διαδικασία, δηλαδή στην τελευταία σχέση αντικαθιστούμε το n με $n+1$ κι έχουμε $U_{n+3} = 2U_{n+2} - U_{n+1} + 2$ οπότε αν αφαιρέσουμε τις δύο τελευταίες σχέσεις κατά μέλη προκύπτει ότι:

$$U_{n+3} = 3U_{n+2} - 3U_{n+1} + U_n.$$

Επομένως, πρόκειται για μια αναδρομική ακολουθία με τάξη $k = 3$.

5. Έστω η ακολουθία των κύβων των φυσικών αριθμών, δηλαδή

$$U_1 = 1^3, U_2 = 2^3, U_3 = 3^3, \ldots, U_n = n^3, \ldots$$

Τότε $U_{n+1} = (n+1)^3 = n^3 + 3n^2 + 3n + 1$, δηλαδή

$$U_{n+1} = U_n + 3n^2 + 3n + 1$$

Αν σε αυτήν αυξήσουμε το n κατά μία μονάδα προκύπτει:

$$U_{n+2} = U_{n+1} + 3n^2 + 9n + 4$$

Αφαιρούμε τις δύο τελευταίες σχέσεις κατά μέλη και έχουμε:

$$U_{n+2} = 2U_{n+1} - U_n + 6n + 3$$

Ομοίως, αυξάνουμε το n κατά ένα στην τελευταία σχέση και παίρνουμε:

$$U_{n+3} = 2U_{n+2}3U_{n+1} + 6n + 9$$

Αφαιρούμε τις δύο τελευταίες σχέσεις κατά μέλη κι έχουμε:

$$U_{n+3} = 3U_{n+2} - 3U_{n+1} + U_n + 6$$

Επαναλαμβάνουμε για τελευταία φορά τη διαδικασία, δηλαδή στην τελευταία σχέση αυξάνουμε κατά μία μονάδα το n και από την σχέση που προκύπτει, αφαιρούμε την $U_{n+3} = 3U_{n+2} - 3U_{n+1} + U_n + 6$ και τελικά έχουμε

$$U_{n+4} = 4U_{n+3} - 6U_{n+2} + 4U_{n+1} - U_n$$

και επομένως πρόκειται για μια αναδρομική ακολουθία τάξεως $k = 4$.

6. Μία ακολουθία U_n ονομάζεται περιοδική με περίοδο L αν ισχύει $U_n = U_{n+k\cdot L}, \forall k \in \mathbb{Z}, \forall n \in \mathbb{N}$. Κάθε περιοδική ακολουθία είναι αναδρομική. Για παράδειγμα, θεωρούμε το ανάπτυγμα στο δεκαδικό σύστημα αρίθμησης του κλάσματος $\frac{761}{1332} = 0.57132132132\ldots$ Η ακολουθία που προκύπτει είναι η $U_{n+3} = U_n, \forall n \geq 3$ που προφανώς είναι μία αναδρομική ακολουθία με τάξη $k = 3$.

7. Θεωρούμε την ακολουθία της οποίας οι όροι είναι οι συντελεστές του πηλίκου που προκύπτει από την διαίρεση δύο πολυωνύμων, όταν αυτό ειναι γραμμένο σε αύξουσα σειρά ως προς τις δυνάμεις του X.
Έστω $P(X) = A_0 + A_1X + \cdots + A_lX^l$ και $Q(X) = B_0 + B_1X \cdots + B_kX^k$, με $B_0 \neq 0$.
Διαιρούμε το $P(X)$ με το $Q(X)$. Αν η διαίρεση δεν είναι τέλεια, τότε το πηλίκο θα περιέχει άπειρους όρους και θα είναι της μορφής $D_0 + D_1X + \cdots + D_nX^n + \cdots$. Η ακολουθία που προκύπτει, δηλαδή, είναι η $U_1 = D_0, U_2 = D_1, ..., U_n = D_{n-1}, ...$
Θα αποδείξουμε οτι η ακολουθία U_n που προκύπτει είναι μια ακολουθία τάξεως k (ο βαθμός του διαιρέτη). Διαλέγουμε έναν φυσικό αριθμό n τέτοιο ώστε $n \geq l - k + 1$. Στην διαίρεση, σταματάμε στον όρο που έχει βαθμό $n+k$. Το υπόλοιπο θα είναι ένα πολυώνυμο βαθμού μεγαλύτερο του $n + k$. Αν γράψουμε την σχέση που προκύπτει από την ευκλείδεια διαίρεση, έχουμε

$$A_0 + A_1X + \cdots + A_lX^l = (B_0 + \cdots + B_kX^k) \cdot (D_0 + \cdots D_{n+k}X^{n+k}) + R(X)$$

Συγκρίνουμε τους συντελεστές του X^{n+k} σε κάθε μέλος της ταυτότητας:

- Στο αριστερό μέλος, αφού $n + k \geq l + 1$, δεν έχουμε όρο βαθμού $n + k$, άρα ο συντελεστής του είναι 0.
- Στο δεξί μέλος της ισότητας, το υπόλοιπο είναι βαθμού $\geq n + k + 1$, άρα μόνο στο γινόμενο εμφανίζεται ο ζητούμενος όρος. Ο συντελεστής αυτός είναι $D_{n+k} \cdot B_0 + D_{n+k-1} \cdot B_1 + \cdots + D_n \cdot B_k$.

Άρα, $D_{n+k} \cdot B_0 + \cdots + D_n \cdot B_k = 0$, και άρα, αφού $B_0 \neq 0$,

$$D_{n+k} = \frac{B_1}{B_0} \cdot D_{n+k-1} - \cdots - \frac{B_k}{B_0} \cdot D_n$$

όπου $n \geq l - k + 1$.
Ως εκ τούτου, η U_n είναι αναδρομική ακολουθία τάξεως k.

Θα δείξουμε, τώρα ότι κάθε ακολουθία που ικανοποιεί την σχέση

$$U_{n+k} = a_1 U_{n+k-1} + a_2 U_{n+k-2} + \cdots + a_k U_n, \quad n \geq m \geq 1$$

συμπίπτει με μια ακολουθία της οποίας οι όροι είναι οι συντελεστές του πηλίκου ενός πολυωνύμου $P(X)$ όταν αυτό διαιρεθεί με το $Q(X) = 1 - a_1 X - \cdots - a_k X^k$.
Έστω n φυσικός αριθμός τέτοιος ώστε $n > k + m - 2$. Πολλαπλασιάζοντας το $Q(X)$ με $U_1 + U_2 X + \cdots + U_{n+1} X^n$:

$$\begin{aligned}
& (1 - a_1 X - a_2 X^2 - \cdots - a_k X^k) \cdot (U_1 + U_2 X + \cdots + U_{k+m-1} X^{k+m-2} + \cdots + U_{n+1} X^n) \\
= \ & [U_1 + (U_2 - a_1 U_1) X + \cdots + (U_{k+m-1} - a_1 U_{k+m-2} - \cdots - a_k U_{m-1}) X^{k+m-2}] \\
+ \ & [(U_{k+m} - a_1 U_{k+m-1} - \cdots - a_k U_m) X^{k+m-1}) + \cdots + (U_{n+1} - a_1 U_n - \cdots - a_k U_{n-k+1}) X^n] \\
- \ & [(a_1 U_{n+1} + \cdots + a_k U_{n-k+2}) X^{n+1} + \cdots + a_k U_{n+1} X^{n+k}]. \qquad (1.2)
\end{aligned}$$

Το πολυώνυμο στην πρώτη αγκύλη είναι βαθμού το πολύ $l = k + m - 2$, και οι συντελεστές του είναι ανεξάρτητοι του n. Ας το ονομάσουμε $P(X)$.
Άρα,

$$P(X) = U_1 + (U_2 - a_1 U_1) X + \cdots + (U_{k+m-1} - a_1 U_{k+m-2} - \cdots - a_k U_{m-1}) X^{k+m-2} \qquad (1.3)$$

Στην δεύτερη αγκύλη του δεξιού μέλους της (1.2), όλοι οι συντελεστές είναι μηδέν, αφού η U_n είναι αναδρομική ακολουθία τάξεως k, άρα ικανοποιεί την

$$U_{n+k} = a_1 U_{n+k-1} + a_2 U_{n+k-2} + \cdots + a_k U_n$$

όπως υποθέσαμε.
Στην τρίτη αγκύλη του δεξιού μέλους της (1.2), οι συντελεστές εξαρτώνται από το αριθμό n. Το πολυώνυμο αυτό θα το συμβολίσουμε με $R_n(X)$.
Επομένως, έχουμε:

$$P(X) = (1 - a_1 X - a_2 X^2 - \cdots - a_k X^k) \cdot (U_1 + U_2 X + \cdots + U_{n+1} X^n) + R_n(X)$$

Άρα, το πολυώνυμο $U_1 + U_2 X + \cdots U_{n+1} X^n$ είναι το πηλίκο της διαίρεσης του $P(X)$ με το $Q(X)$ και το $R(X)$ είναι το υπόλοιπο της διαίρεσης αυτής. Η ακολουθία $U_1, U_2, ..., U_n, ...$ είναι όντως η ακολουθία των συντελεστών του πηλίκου διαίρεσης ενός πολυωνύμου με το $Q(X)$.
Ας θεωρήσουμε για παράδειγμα την ακολουθία Fibonacci. Όπως δείξαμε, ο αναδρομικός τύπος αυτής της ακολουθίας είναι $F_{n+2} = F_{n+1} + F_n, n \geq 0$. Άρα $m = 1, k = 2, a_1 = 1, a_2 = 1$ οπότε $Q(X) = 1 - X - X^2$. Το $P(X)$ δεν πρέπει να έχει βαθμό μεγαλύτερο από $k + m - 2 = 1$.
Από την (1.3) προκύπτει ότι $P(X) = 1 + (1 - 1 \cdot 1) X$, άρα $P(X) \equiv 1$. Οπότε, η ακολουθία Fibonacci συμπίπτει με τους όρους της ακολουθίας που είναι οι συντελεστές του πηλίκου της διαίρεσης του 1 με το πολυώνυμο $1 - X - X^2$.

1.2 Άθροισμα n πρώτων όρων ακολουθίας

Ένα από τα ζητήματα που συναντάμε στο Λύκειο είναι το άθροισμα n όρων μιας αναδρομικής ακολουθίας, για παράδειγμα μιας αριθμητικής πρόοδου. Έστω $U_1, U_2, ..., U_n, ...$ να είναι μια αναδρομική ακολουθία τάξεως k, δηλαδή

$$U_{n+k} = a_1U_{n+k-1} + a_2U_{n+k-2} + \cdots + a_kU_n \quad (n \geq m \geq 1)$$

Ας θεωρήσουμε μια νέα ακολουθία: $s_1 = U_1, s_2 = U_1+U_2, ..., s_n = U_1+U_2+\cdots+U_n, ...$ Θα αποδείξουμε ότι η s_n είναι μια αναδρομική ακολουθία τάξεως $k+1$ και ότι οι όροι της ικανοποιούν την σχέση $s_{n+k+1} = (1+a_1)s_{n+k} + (a_2-a_1)s_{n+k-1} + \cdots + (a_k - a_{k-1})s_{n+1} - a_ks_n$. Σημειώνουμε ότι $U_1 = s_1, U_2 = s_2 - U_1 = s_2 - s_1, ...U_n = s_n - (U_1 + U_2 + \cdots + U_{n-1}) = s_n - s_{n-1} \quad n \geq m$ Υποθέτουμε ότι $s_0 = 0$ άρα $U_1 = s_1 - s_0$. Οπότε, αν το αντικαταστήσουμε στην αναδρομική σχέση που ικανοποιεί η U_n προκύπτει:

$$s_{n+k} - s_{n+k-1} = a_1(s_{n+k-1} - s_{n+k-2}) + a_2(s_{n+k-2} - s_{n+k-3}) + \cdots + a_k(s_n - s_{n-1})$$

απ'όπου έχουμε

$$s_{n+k} = (1+a_1)s_{n+k-1} + (a_2-a_1)s_{n+k-2} + \cdots + (a_k - a_{k-1})s_n - a_ks_{n-1}$$

Στην τελευταία σχέση, αν αυξήσουμε το n κατά ένα προκύπτει:

$$s_{n+k+1} = (1+a_1)s_{n+k} + (a_2-a_1)s_{n+k-1} + \cdots + (a_k - a_{k-1})s_{n+1} - a_ks_n \quad \forall n \geq m-1$$

Από την τελευταία σχέση προκύπτει ότι η s_n είναι ανδρομική ακολουθία τάξεως $k+1$.

Ορισμένα παραδείγματα

1. Η γεωμετρική πρόοδος $U_n = aq^{n-1}$:
   Ο $n-$οστός όρος του αθροίσματος είναι $s_n = U_1+U_2+...+U_n = a+aq+...+aq^{n-1}$. Όπως είδαμε, η U_n ικανοποιεί την αναδρομική σχέση $U_{n+1} = qU_n$, άρα σύμφωνα με τον τύπο που δείξαμε, η ακολουθία του αθροίσματος ικανοποιεί την σχέση:
   $$s_{n+2} = (1+q)s_{n+1} - qs_n.$$

2. Η ακολουθία των τετραγώνων των φυσικών αριθμών:
   Εδώ έχουμε $U_n = n^2$. Όπως είδαμε, η αναδρομική σχέση αυτής ακολουθίας είναι $U_{n+3} = 3U_{n+2} - 3U_{n+1} + U_n, (a_1 = 3, a_2 = -3, a_3 = 1)$, άρα η ακολουθία του αντίστοιχου αθροίσματος ικανοποιεί την σχέση
   $$s_{n+4} = 4s_{n+3} - 6s_{n+2} + 4s_{n+1} - s_n$$

3. Η ακολουθία των κύβων των φυσικών αριθμών:
   Εδώ είναι $U_n = n^3$. Όπως είδαμε, η αναδρομική σχέση αυτής της ακολουθίας είναι $U_{n+4} = 4U_{n+3} - 5U_{n+2} + 2U_{n+1}$, δηλαδή, $a_1 = 4, a_2 = -5, a_3 = 2$ και επομένως η ακολουθία του αντίστοιχου αθροίσματος ικανοποιεί την αναδρομική σχέση
   $$s_{n+5} = 5s_{n+4} - 10s_{n+3} + 10s_{n+2} - 5s_{n+1} + s_n$$

4. Ακολουθία Fibonacci:
   Όπως είδαμε, η αναδρομική σχέση αυτής της ακολουθίας είναι $F_{n+2} = F_{n+1} + F_n$. Άρα
   $$s_{n+3} = 2s_{n+2} - s_n$$

1.3 Βάση της αναδρομικής ακολουθίας

Στις απλές μορφές αναδρομικών ακολουθιών (για παράδειγμα αριθμητική ή γεωμετρική πρόοδο), οποιοσδήποτε όρος μπορεί να υπολογισθεί χωρίς να είναι ανάγκη να βρούμε προηγούμενους όρους. Όμως, στην περίπτωση πιο σύνθετων ακολουθιών, όπως αυτή του Fibonacci ή η ακολουθία συντελεστών του πηλίκου που προκύπτει από την διαίρεση δύο πολυωνύμων, αυτό φάινεται αδύνατο.
Θα προσπαθήσουμε να αναπτύξουμε μια γενική θεωρία, η οποία θα μας επιτρέψει τον υπολογισμό όρων μιας αναδρομικής ακολουθίας χωρίς την χρήση προηγούμενων όρων.
Έστω η αναδρομική ακολουθία U_n τάξεως k, δηλαδή

$$U_{n+k} = a_1 U_{n+k-1} + a_2 U_{n+k-2} + \cdots + a_k U_n \tag{1.4}$$

η οποία ισχύει για κάθε φυσικό αριθμό n.
Αν υποθέσουμε ότι $n = 1$, έχουμε

$$U_{k+1} = a_1 U_k + a_2 U_{k-1} + \cdots + a_k U_1$$

οπότε αν γνωρίζουμε τις τιμές $U_1, U_2, ..., U_k$, μπορούμε να υπολογίσουμε τον όρο U_{k+1}.
Ομοίως, αν θεωρήσουμε ότι $n = 2$ στην (1.4), έχουμε ότι

$$U_{k+2} = a_1 U_{k+1} + a_2 U_k + \cdots a_k U_2$$

άρα μπορούμε να υπολογίσουμε τον όρο U_{k+2}, αν γνωρίζουμε τους $U_1, U_2, ..., U_{k+1}$.
Γενικά, αν $m \in \mathbb{N}$ και έχουμε υπολογίσει τους $m + k - 1$ πρώτους όρους, αν θεωρήσουμε ότι $n = m$ στην (1.4), τότε μπορούμε να υπολογίσουμε τον όρο U_{m+k}. Υπάρχουν άπειρες ακολουθίες που να ικανοποιούν την αναδρομική σχέση, αυτές προκύπτουν αν αλλάξουμε τις αρχικές τιμές, δηλαδή τους $U_1, U_2, ..., U_k$ ή έστω έναν από αυτούς. Για παράδειγμα, αν στην ακολουθία $F_{n+2} = F_{n+1} + F_n$, αντί για τις τιμές $F_1 = 1$ και $F_2 = 1$, ορίσουμε να είναι $F_1 = -3$ και $F_2 = 1$ προκύπτει η ακολουθία $-3, 1, -2, -1, -3, -4, -7,$
$-11, -18, -29, ...$
Έστω ότι έχουμε έναν συγκεκριμένο αριθμό ακολουθιών που ικανοποιούν την αναδρομική σχέση

$$U_{n+k} = a_1 U_{n+k-1} + \cdots + a_k U_n$$

τις $x_n, y_n, ..., z_n$ ή αλλιώς τις

$$x_1, x_2, ..., x_n, ...$$
$$y_1, y_2, ..., y_n, ...$$
$$z_1, z_2, ..., z_n, ...$$

Οι ακόλουθες εξισώσεις ισχύουν:

$$\left.\begin{array}{rcl} x_{n+k} &=& a_1 x_{n+k-1} + a_2 x_{n+k-2} + \cdots + a_k x_n \\ y_{n+k} &=& a_1 y_{n+k-1} + a_2 y_{n+k-2} + \cdots + a_k y_n \\ & \vdots & \\ z_{n+k} &=& a_1 z_{n+k-1} + a_2 z_{n+k-2} + \cdots + a_k z_n \end{array}\right\} (*)$$

Έστω τυχαία $A, B, ..., C$ (πλήθος αυτών των αριθμών όσες και οι ακολουθίες $x_n, y_n, \ldots, z_n$).
Στο $(*)$, πολλαπλασιάζουμε την πρώτη ισότητα με A, την δεύτερη με B κ.ο.κ., προσθέτουμε κατά μέλη και προκύπτει

$$\begin{array}{rcl} Ax_{n+k} + By_{n+k} + \cdots + Cz_{n+k} &=& a_1(Ax_{n+k-1} + By_{n+k-1} + \cdots + Cz_{n+k-1}) \\ &+& a_2(Ax_{n+k-2} + By_{n+k-2} + \cdots + Cz_{n+k-2}) \\ &+& \cdots + a_k(Ax_n + By_n + \cdots + Cz_n) \end{array}$$

Προκύπτει, δηλαδή, ότι η ακολουθία $t_n = Ax_n + By_n + \cdots + Cz_n$ είναι αναδρομική τάξεως k, δηλαδή ικανοποιεί την αναδρομική σχέση

$$U_{n+k} = a_1 U_{n+k-1} + a_2 U_{n+k-2} + \cdots + a_k U_n$$

Αφού οι σταθερές $A, B, ..., C$ είναι αυθαίρετες, μπορούμε, αν τις αλλάξουμε, να αποκτήσουμε διαφορετικές τιμές για την ακολουθία t_n.
Το ερώτημα που προκύπτει είναι αν μπορούμε να δώσουμε τέτοιες τιμές στους $A, B, ..., C$ έτσι ώστε οι πρώτοι k όροι της t_n να συμπίπτουν με τους k πρώτους όρους της U_n. Αν ναι, τότε $U_n = Ax_n + By_n + \cdots + Cz_n$ κι έτσι για τον υπολογισμό των όρων της U_n, δεν θα χρειάζονται οι προηγούμενοι όροι.
Αρκεί δηλαδή το σύστημα

$$\left.\begin{array}{rcl} Ax_1 + By_1 + \cdots + Cz_1 &=& U_1 \\ Ax_2 + By_2 + \cdots + Cz_2 &=& U_2 \\ & \vdots & \\ Ax_k + By_k + \cdots + Cz_k &=& U_k \end{array}\right\} (\Sigma)$$

να έχει λύση ως προς τους αγνώστους $A, B, ..., C$. Είναι γνωστό από την γραμμική άλγεβρα ότι το (Σ) έχει μοναδική λύση αν και μόνον αν το αντίστοιχο ομογενές έχει μοναδική λύση την μηδενική, δηλαδή αν και μόνο αν ισχύει η συνεπαγωγή:

$$\left.\begin{array}{rcl} Ax_1 + By_1 + \cdots + Cz_1 &=& 0 \\ Ax_2 + By_2 + \cdots + Cz_2 &=& 0 \\ & \vdots & \\ Ax_k + By_k + \cdots + Cz_k &=& 0 \end{array}\right\} \Rightarrow \{A = B = ... = C = 0\}$$

Έχουμε αποδείξει δηλαδή το εξής Θεώρημα:

ΘΕΩΡΗΜΑ 1.3.1: Για κάθε αναδρομική σχέση τάξεως k υπάρχουν άπειρες το πλήθος διαφορετικές ακολουθίες που ικανοποιούν την σχέση. Η βάση της αναδρομικής σχεσης αποτελείται από k το πλήθος γεωμετρικές προόδους και κάθε ακολουθία που ικανοποιεί την αναδρομική σχέση μπορεί να γραφεί σαν γραμμικός συνδυασμός της βάσης.

Παραδείγματα

1. Έστω ότι έχουμε την αναδρομική σχέση

   $$U_{n+2} = 2U_{n+1} - U_n$$

   που είναι τάξεως $k = 2$.
   Τότε η βάση της θα αποτελείται από 2 ακολουθίες:

   $$\left\{ \begin{array}{l} x_1, x_2, ..., x_n, ... \\ y_1, y_2, ..., y_n, ... \end{array} \right\}$$

   Έστω ότι $x_1 = 1, x_2 = 1$ και $y_1 = 0, y_2 = 1$.
   Από την αναδρομική σχέση παρατηρούμε ότι $U_{n+2} - U_{n+1} = U_{n+1} - U_n$, δηλαδή η διαφορά δύο διαδοχικών όρων είναι σταθερά. Από αυτό προκύπτει ότι $x_n = 1, \forall n \in \mathbb{N}$ ενώ $y_n = n - 1, \forall n \in \mathbb{N}$.
   Για κάθε ακολουθία U_n που ικανοποιεί την αναδρομική σχέση ισχύει ότι κάθε όρος

της μπορεί να γραφεί σαν γραμμικός συνδυασμός των x_n, y_n, δηλαδή $U_n = Ax_n + By_n$ με $A, B \in \mathbb{C}$, δηλαδή $U_n = A \cdot 1 + B \cdot (n-1)$ ή αλλιώς $U_n = (A-B) + B \cdot n$ με $n \in \mathbb{N}$.
Για να βρούμε τις σταθερές A, B αρκεί να λύσουμε το σύστημα

$$\left\{ \begin{array}{l} U_1 = (A-B) + B \\ U_2 = (A-B) + 2B \end{array} \right\}$$

απ'όπου προκύπτει: $A = U_1, B = U_2 - U_1$.
Άρα $U_n = U_1 + (n-1)(U_2 - U_1), \forall n \in \mathbb{N}$

2. Έστω η αναδρομική σχέση $U_{n+2} = U_{n+1} + U_n$ τάξεως $k = 2$. Υποθέτουμε ότι η πρώτη ακολουθία της βάσης έχει αρχικούς όρους $F_1 = 1, F_2 = 1$ τότε η F_n είναι η ακολουθία Fibonacci, όπως είδαμε. Σαν δεύτερη ακολουθία U_n θα πάρουμε εκείνη που έχει αρχικούς όρους $y_1 = 0, y_1 = 1$.
Τότε $y_3 = y_2 + y_1 = 1, y_4 = y_3 + y_2 = 2, y_5 = y_4 + y_3 = 3$ και γενικά $y_n = F_{n-1}, \forall n = 2, 3, ...$
Τότε κάθε ακολουθία που ικανοποιεί την $U_{n+2} = U_{n+1} + U_n$ γράφεται ως γραμμικός συνδυασμός των F_n, y_n, δηλαδή $\exists A, B \in \mathbb{C}$ τέτοια ώστε $U_n = A \cdot F_n + B \cdot y_n$.
Θέτουμε $n = 1$ και $n = 2$ για να λύσουμε το σύστημα με αγνώστους τα A, B, δηλαδή

$$\left\{ \begin{array}{l} U_1 = A \cdot F_1 + B \cdot y_1 \\ U_2 = A \cdot F_2 + B \cdot y_2 \end{array} \right\}$$

δηλαδή

$$\left\{ \begin{array}{l} U_1 = A \\ U_2 = A + B \end{array} \right\}$$

άρα

$$\left\{ \begin{array}{l} A = U_1 \\ B = U_2 - U_1 \end{array} \right\}$$

οπότε $U_n = U_1 F_n + (U_2 - U_1) y_n$ όμως $y_n = F_{n-1}$, άρα $U_n = U_1 \cdot F_n + (U_2 - U_1) \cdot F_{n-1}$.
Άρα

$$U_n = U_1(F_n - F_{n-1}) + U_2 \cdot F_{n-1}$$

ή ισοδύναμα

$$U_n = U_1 \cdot F_{n-2} + U_2 \cdot F_{n-1}, \quad \forall n \geq 3$$

Θα δείξουμε τώρα ότι υπό κάποιες πολύ γενικές συνθήκες η βάση κάθε αναδρομικής ακολουθίας τάξεως k αποτελείται από k γεωμετρικές προόδους με διαφορετικό λόγο.
Ας εξετάσουμε πρώτα υπό ποιές προϋποθέσεις ικανοποιεί η γεωμετρική πρόοδος $x_1 = 1, x_2 = q, ..., x_n = q^{n-1}, q \neq 0$ την αναδρομική σχέση

$$U_{n+k} = a_1 U_{n+k-1} + a_2 U_{n+k-2} + \cdots a_k U_n \tag{1.5}$$

Αντικαθιστούμε στην σχέση (1.5) και προκύπτει:

$$q^{n+k-1} = a_1 q^{n+k-2} + a_2 q^{n+k-3} + \cdots + a_k q^{n-1}$$

απ'όπου προκύπτει

$$q^k = a_1 q^{k-1} + a_2 q^{k-2} + \cdots + a_k$$

Άρα, για να ικανοποιεί η γεωμετρική πρόοδος με λόγο q την αναδρομική σχέση

$$U_{n+k} = a_1 U_{n+k-1} + a_2 U_{n+k-2} + \cdots a_k U_n$$

θα πρέπει ο λόγος q να ικανοποιεί την σχέση

$$q^k = a_1 q^{k-1} + a_2 q^{k-2} + \cdots + a_k$$

Η τελευταία εξίσωση ονομάζεται *χαρακτηριστική εξίσωση της αναδρομικής σχέσης*.
Έστω $q = a \in \mathbb{C}$ μια ρίζα της χαρακτηριστικής εξίσωσης. Υποθέτοντας ότι $x_n = a^{n-1}$ $\forall n \in \mathbb{N}$, προκύπτει μια γεωμετρική πρόοδος με πρώτο όρο την μονάδα και λόγο a. Αφού a ρίζα της χαρακτηριστικής εξίσωσης, έχουμε ότι $a^k = a_1 \cdot a^{n+k-2} + \cdots + a_k \cdot a^{n-1}$. Άρα η x_n ικανοποιεί την αναδρομική σχέση $U_{n+k} = U_{n+k-1} \cdot a_1 + a_2 \cdot U_{n+k-2} + \cdots + a_k \cdot U_n$. Έτσι, σε κάθε ρίζα $q = a$ της χαρακτηριστικής εξίσωσης αντιστοιχεί μια γεωμετρική πρόοδος με λόγο a που ικανοποιεί την αναδρομική σχέση $U_{n+k} = a_1 \cdot U_{n+k-1} + a_2 \cdot U_{n+k-2} + \cdots + a_k \cdot U_n$.

1.3.1 Αν η χαρακτηριστική εξίσωση έχει μόνο απλές ρίζες

Για να κατασκευάσουμε την βάση της αναδρομικής σχέσης, ας υποθέσουμε αρχικά ότι η χαρακτηριστική εξίσωση έχει k διαφορετικές ρίζες (όλες απλές δηλαδή), τις $q_1 = \alpha, q_2 = \beta, ..., q_k = \gamma$.
Έχουμε δηλαδή k διαφορετικές γεωμετρικές προόδους που ικανοποιούν την αναδρομική σχέση τάξεως k:

$$\left.\begin{array}{cccc} 1, \alpha, \alpha^2, & ... & , \alpha^{n-1}, ... \\ 1, \beta, \beta^2, & ... & , \beta^{n-1}, ... \\ & \vdots & \\ 1, \gamma, \gamma^2, & ... & , \gamma^{n-1}, ... \end{array}\right\} (B)$$

Θα δείξουμε τώρα ότι το σύστημα των εξισώσεων (B) αποτελεί βάση της αναδρομικής σχέσης, δηλαδή ότι για κάθε ακολουθία U_n που ικανοποιεί την αναδρομική σχέση $U_{n+k} = a_1 \cdot U_{n+k-1} + \cdots + a_k \cdot U_n$ υπάρχουν σταθερές $A, B, ..., C$ τέτοιες ώστε $U_n = A \cdot \alpha^{n-1} + B \cdot \beta^{n-1} + \cdots + C \cdots \gamma^{n-1}$. Αρκεί, όπως προηγουμένως, το σύστημα

$$\left.\begin{array}{l} A + B + \cdots + C = U_1 \\ A \cdot \alpha + B \cdot \beta + \cdots + C \cdot \gamma = U_2 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ A \cdot \alpha^{k-1} + B \cdot \beta^{k-1} + \cdots + C \cdot \gamma^{k-1} = U_k \end{array}\right\} (\Sigma_1)$$

να έχει λύση ως προς τους αγνώστους $A, B, ..., C$. Αρκεί το αντίστοιχο ομογενές να έχει μοναδική λύση την μηδενική, δηλαδή, αν

$$\begin{array}{l} A + B + \cdots + C = 0 \\ A \cdot \alpha + B \cdot \beta + \cdots + C \cdot \gamma = 0 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ A \cdot \alpha^{k-1} + B \cdot \beta^{k-1} + \cdots + C \cdot \gamma^{k-1} = 0 \end{array}$$

τότε

$$A = B = ... = C = 0$$

Ας υποθέσουμε ότι υπάρχει λύση του ομογενούς κι ένας τουλάχιστον, έστω ο A, είναι διάφορος του μηδενός.
Για να οδηγηθούμε σε άτοπο, θα κατασκευάσουμε ένα πολυώνυμο $M(x)$ με $degM = k-1$ τέτοιο ώστε $M(\alpha) = 1$ και $M(\beta) = ... = M(\gamma) = 0$.
Αφού τα $\beta, ..., \gamma$ είναι $k-1$ το πλήθος, τότε

$$M(x) = \mu \cdot (x-\beta) \cdots (x-\gamma), \text{ με } \mu \in \mathbb{C}$$

Τότε, αφού $M(\alpha) = 1$, προκύπτει ότι

$$\mu = \frac{1}{(\alpha-\beta) \cdots (\alpha-\gamma)}$$

Άρα

$$M(x) = \frac{(x-\beta) \cdots (x-\gamma)}{(\alpha-\beta) \cdots (\alpha-\gamma)}$$

Αναπτύσσοντας τις παρενθέσεις και μαζεύοντας τις, προκύπτει ότι $M(x) = m_0 + m_1 \cdot x + \cdots + m_{k-1} \cdot x^{k-1}$. Πολλαπλασιάζοντας το ομογενές σύστημα με τις σταθερές $m_0, m_1, ..., m_{k-1}$ και προσθέτοντας κατά μέλη, προκύπτει ότι

$$\begin{aligned} A \cdot (m_0 + m_1 \cdot \alpha + \cdots + m_{k-1} \cdot \alpha^{k-1}) \quad &+ \quad B \cdot (m_0 + m_1 \cdot \beta + \cdots + m_{k-1} \cdot \beta^{k-1}) \\ &+ \quad \cdots + C \cdot (m_0 + m_1 \cdot \gamma + \cdots + m_{k-1} \cdot \gamma^{k-1}) = 0 \end{aligned}$$

ή αλλιώς

$$A \cdot \mu(\alpha) + B \cdot \mu(\beta) + \cdots + C \cdot \mu(\gamma) = 0$$

δηλαδή $A \cdot 1 = 0 \Rightarrow A = 0$ Άτοπο
Άρα το (Σ_1) έχει λύση.

Αποδείξαμε δηλαδή το εξής:

ΠΡΟΤΑΣΗ 1.3.1: Σε κάθε αναδρομική ακολουθία τάξεως k αντιστοιχεί μια αλγεβρική εξίσωση βαθμού k με τους ίδιους συντελεστές (η χαρακτηριστική της εξίσωση). Κάθε ρίζα της χαρακτηριστικής εξίσωσης είναι ο λόγος μίας γεωμετρικής προόδου που ικανοποιεί την αναδρομική σχέση. Εάν όλες οι ρίζες της χαρακτηριστικής εξίσωσης είναι *απλές*, τότε οι k γεωμετρικές προόδοι που προκύπτουν αποτελούν την βάση της αναδρομικής σχέσης.

Παραδείγματα

1. Θεωρούμε την ακολουθία Fibonacci F_n. Η αναδρομική της σχέση είναι $U_{n+2} = U_{n+1} + U_n$, κατά συνέπεια, η χαρακτηριστική της εξίσωση είναι $q^2 = q + 1$, το οποίο έχει ρίζες τις $\alpha = \frac{1+\sqrt{5}}{2}$ και $\beta = \frac{1-\sqrt{5}}{2}$. Ο γενικός όρος F_n της ακολουθίας Fibonacci μπορεί να γραφεί ως: $F_n = A \cdot \alpha^{n-1} + B \cdot \beta^{n-1}$ όπου A, B είναι δύο σταθερές. Για να τις βρούμε λύνουμε το σύστημα:

$$\left\{ \begin{array}{l} F_1 = A + B \\ F_2 = A \cdot \alpha + B \cdot \beta \end{array} \right\}$$

απ'όπου προκύπτει

$$A = \frac{\sqrt{5}+1}{2\sqrt{5}} \text{ και } B = \frac{\sqrt{5}-1}{2\sqrt{5}}$$

Ως εκ τούτου,

$$F_n = \frac{\sqrt{5}+1}{2\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^{n-1} + \frac{\sqrt{5}-1}{2\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}$$

ή αλλιώς

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n} - \left(\frac{1-\sqrt{5}}{2}\right)^{n}\right], \text{ με } n \in \mathbb{N}$$

Ο τύπος για τον γενικό όρο της ακολουθίας Fibonacci δεν φαίνεται ιδιαίτερα χρήσιμος για υπολογισμούς, αλλά κάτι τέτοιο δεν ισχύει. Για παράδειγμα από αυτόν τον τύπο προκύπτει ότι το άθροισμα των τετραγώνων δύο διαδοχικών αριθμών Fibonacci είναι πάλι όρος της ακολουθίας F_n. Όντως, $\forall n \in \mathbb{N}$ έχουμε

$$F_n^2 = \frac{1}{5}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{2n} + \left(\frac{1-\sqrt{5}}{2}\right)^{2n} - 2(-1)^n\right]$$

και

$$F_{n+1}^2 = \frac{1}{5}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{2n+2} + \left(\frac{1-\sqrt{5}}{2}\right)^{2n+2} - 2(-1)^{n+1}\right]$$

Έτσι,

$$F_{n+1}^2 + F_n^2 = \frac{1}{5}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{2n} \cdot \left(\frac{5+\sqrt{5}}{2}\right) + \left(\frac{1-\sqrt{5}}{2}\right)^{2n} \cdot \left(\frac{5-\sqrt{5}}{2}\right)\right] =$$

$$\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{2n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{2n+1}\right] = F_{2n+1}$$

Δηλαδή, μόλις δείξαμε ότι $F_{n+1}^2 + F_n^2 = F_{2n+1}^2$.
Για παράδειγμα, $F_{13} = F_7^2 + F_6^2 = 13^2 + 8^2 = 233$.
Ακόμα, με την βοήθεια του τύπου του γενικού όρου της ακολουθίας αποδεικνύεται η εξής πρόταση:

ΠΡΟΤΑΣΗ 1.3.2: Για δύο φυσικούς αριθμούς a, b με $a < b$, τα βήματα που απαιτούνται για την εύρεση του Μ.Κ.Δ.(a, b) είναι το πολύ $5n$, όπου n είναι το πλήθος των ψηφίων του a, όταν αυτός είναι γραμμένος στο δεκαδικό σύστημα.

Απόδειξη. Από τον ευκλείδιο αλγόριθμο έχουμε:

$b = ax' + y'$

$a = y'x'' + y''$

$y' = y''x''' + y'''$

$\vdots$

$y^{(k-2)} = y^{(k-1)}x^{(k)} + y^{(k)}$

$y^{(k-1)} = y^{(k)}x^{(k+1)}$

Προφανώς ισχύει $a > y' > y'' > \cdots > y^{(k-1)} > y^{(k)} \geq 1$. Άρα ο $y^{(k)}$ είναι ο Μ.Κ.Δ.(a, b) και k είναι το πλήθος των διαιρέσεων που χρειάστηκαν. Συγκρίνουμε

τους αριθμούς $y^{(k)}, y^{(k-1)}, \ldots, y', a$ με τους αριθμούς $F_1, F_2, F_3, \ldots$.
$y^{(k)} \geq 1 = F_2$ και αφού $y^{(k-1)} > y^{(k)}$, έχουμε ότι $y^{(k-1)} \geq 2 = F_3$.
Έτσι,
$y^{(k-2)} = y^{(k-1)}x^{(k)} + y^{(k)} \geq y^{(k-1)} \cdot 1 + y^{(k)} = y^{(k-1)} + y^{(k)} \geq F_3 + F_2 = F_4$.
Άρα $y^{(k)} \geq F_2, y^{(k-1)} \geq F_3, y^{(k-2)} \geq F_4$.
Υποθέτουμε ότι ισχύει για m, δηλαδή

$$y^{(m)} \geq F_{k-m+2}, y^{(m-1)} \geq F_{k-m+3} \quad \text{με} \quad m-1 \geq 2.$$

Τότε,

$$y^{(m-2)} \geq y^{(m-1)} + y^{(m)} \geq F_{k-m+3} + F_{k-m+2} = F_{k-m+4}.$$

Στο τελευταίο βήμα θα έχουμε $y'' \geq F_k, y' \geq F_{k+1}$ και άρα $a = y'x'' + y' \geq y' \cdot 1 + y'' \geq F_{k+1} + F_k = F_{k+2}$.
Από τον γενικό όρο της ακολουθίας Fibonacci έχουμε

$$F_{k+2} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+2}\right]$$

και επομένως

$$a \geq \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+2}\right] > \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+2} - 1\right]$$

αφού $|\frac{1-\sqrt{5}}{2}| < 1$.
Άρα,

$$\left(\frac{1+\sqrt{5}}{2}\right)^{k+2} < a \cdot \sqrt{5} + 1 < \sqrt{5}(a+1) < \left(\frac{1+\sqrt{5}}{2}\right)^{2}(a+1)$$

Έτσι, $\left(\frac{1+\sqrt{5}}{2}\right)^{k} < a+1$. Σημειώνουμε ότι

$$F_5 = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{5} - \left(\frac{1-\sqrt{5}}{2}\right)^{5}\right] < \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{5} + 1\right].$$

Έτσι, $\left(\frac{1+\sqrt{5}}{2}\right)^{5} > 5 \cdot \sqrt{5} - 1 > 10$. Συνεπώς,

$$10^k < \left(\frac{1+\sqrt{5}}{2}\right)^{5k} < (a+1)^5.$$

Αφού ο a έχει n ψηφία στο δεκαδικό σύστημα αρίθμησης, προφανώς ισχύει $10^{n-1} \leq a < 10^n$ και έτσι, αφού $10^k < (a+1)^5$, έχουμε

$$10^k < (a+1)^5 \leq 10^{5n}$$

δηλαδή

$$k < 5n$$

□

Συνεχίζουμε με τα παραδείγματα.

2. Έστω η αναδρομική ακολουθία

$$U_1 = 5, U_2 = 7, U_3 = 1, U_4 = 3, U_5 = 2, U_6 = 1, U_7 = 3, ...$$

Η αναδρομική σχέση αυτής της ακολουθίας είναι

$$U_{n+3} = U_n, \forall n \geq 3$$

Άρα η χαρακτηριστική εξίσωση είναι η $q^3 = 1$ με ρίζες τις

$$\alpha = 1, \quad \beta = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \quad \gamma = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

Άρα ο γενικός όρος της ακολουθίας U_n είναι ο

$$U_n = A \cdot \alpha^{n-1} + B \cdot \beta^{n-1} + C \cdot \gamma^{n-1}, \text{ όπου } A, B, C \text{ σταθερές}$$

άρα

$$U_n = A + B \cdot \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)^{n-1} + C \cdot \left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)^{n-1}, \forall n \geq 3$$

Όμως

$$-\frac{1}{2} + i\frac{\sqrt{3}}{2} = -(\cos\frac{\pi}{3} - i\sin\frac{\pi}{3})$$

και

$$-\frac{1}{2} - i\frac{\sqrt{3}}{2} = -(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3})$$

και από De Moivre έχουμε

$$\begin{aligned} U_n &= A + (-1)^{n-1} \cdot B \cdot \left(\cos\big((n-1)\frac{\pi}{3}\big) - i\sin\big((n-1)\frac{\pi}{3}\big)\right) \\ &+ (-1)^{n-1} \cdot C \cdot \left(\cos\big((n-1)\frac{\pi}{3}\big) + i\sin\big((n-1)\frac{\pi}{3}\big)\right) \\ &= A + (B+C) \cdot (-1)^{n-1} \cdot \cos\big((n-1)\frac{\pi}{3}\big) + i(C-B) \cdot (-1)^{n-1} \cdot \sin\big((n-1)\frac{\pi}{3}\big) \end{aligned}$$

και αν θέσουμε $A_1 = B + C$ και $A_2 = \big(C - B\big)i$ ο γενικός όρος παίρνει την μορφή:

$$U_n = A + A_1(-1)^{n-1}\cos\big((n-1)\frac{\pi}{3}\big) + A_2(-1)^{n-1}\sin\big((n-1)\frac{\pi}{3}\big), \quad \forall n \geq 3$$

Για να υπολογίσουμε τις σταθερές A, A_1, A_2, θα πρέπει να λύσουμε το σύστημα που προκύπτει από τις:

$$\left\{ \begin{array}{c} U_3 = 1 \\ U_4 = 3 \\ U_5 = 2 \end{array} \right\}$$

και βρίσκουμε ότι

$$A = 2, \quad A_1 = 1, \quad A_2 = -\frac{\sqrt{3}}{3}$$

άρα

$$U_n = 2 + (-1)^{n-1}\left[\cos\big((n-1)\frac{\pi}{3}\big) - \frac{\sqrt{3}}{3}\sin\big((n-1)\frac{\pi}{3}\big)\right]$$

ή αλλιώς

$$U_n = 2 + (-1)^n \cdot \frac{2\sqrt{3}}{3} \cdot \sin[(n-2) \cdot \frac{\pi}{3}], \quad \forall n \geq 3$$

Στο συγκεκριμένο παράδειγμα, ο γενικός όρος εκφράζεται μέσω τριγωνομετρικών συναρτήσεων κάτι το φυσιολογικό, αφού οι ρίζες της χαρακτηριστικής εξίσωσης είναι τρίτες ρίζες της μονάδος και ο γενικός όρος επηρεάζεται από την φύση των ριζών της χαρακτηριστικής εξίσωσης.

3. Έστω $P(x) = 3 + x^2 - x^5$, και $Q(x) = 2 - x - 2x^2 + x^3$. Έστω $\pi(x), r(x)$ το πηλίκο και το υπόλοιπο αντίστοιχα της (ευκλείδειας) διαίρεσης του $P(x)$ με το $Q(x)$.
Η ακολουθία συντελεστών του πηλίκου είναι

$$U_1 = D_0, \quad U_2 = D_1, \ldots, U_n = D_{n-1}, \ldots$$

που όπως δείχθηκε είναι μια αναδρομική ακολουθία της οποίας οι όροι ικανοποιούν την αναδρομική σχέση

$$D_{n+k} = -\frac{B_1}{B_0} \cdot D_{n+k-1} - \cdots - \frac{B_k}{B_0} \cdot D_n, \quad (n \geq l - k + 1)$$

όπου $k = degQ$, B_i οι συντελεστές του $Q(x)$ και $l = degP$.
Στο παράδειγμα μας, $k = 3, B_0 = 2, B_1 = -1, B_2 = -2, B_3 = 1, l = 5$, άρα

$$D_{n+3} = \frac{1}{2}D_{n+2} + D_{n+1} - \frac{1}{2}D_n, \quad n \geq 3$$

Η χαρακτηριστική εξίσωση είναι η

$$q^3 = \frac{1}{2}q^2 + q - \frac{1}{2} \Rightarrow$$

$$q^3 - \frac{1}{2}q^2 - q + \frac{1}{2} = 0 \Rightarrow$$

$$q^3 - q - \frac{1}{2}(q^2 - 1) = 0 \Rightarrow$$

$$(q - \frac{1}{2}) \cdot (q - 1) \cdot (q + 1) = 0$$

άρα

$$\alpha = \frac{1}{2}, \quad \beta = 1, \quad \gamma = -1$$

Και έτσι ο γενικός όρος της ακολουθίας D_n δίνεται από τον τύπο

$$D_n = A \cdot \left(\frac{1}{2}\right)^n + B \cdot 1^n + C \cdot (-1)^n$$

όπου A, B, C είναι αυθαίρετες στεθερές.
Για να τις υπολογίσουμε, αρκεί να λύσουμε το σύστημα:

$$\left\{ \begin{array}{l} D_3 = \frac{1}{8}A + B - C \\ D_4 = \frac{1}{16}A + B + C \\ D_5 = \frac{1}{32}A + B - C \end{array} \right\} (\Sigma_2)$$

στο οποίο άγνωστοι είναι όχι μόνο τα A, B, C αλλά και τα D_3, D_4, D_5, που μπορούν όμως να υπολογισθούν από την ευκλείδεια διαίρεση του $P(x) = 3 + x^2 - x^5$ με το $Q(x) = 2 - x - 2x^2 + x^2$.
Κάνουμε την διαίρεση και προκύπτει ότι

$$\pi(x) = \frac{3}{2} + \frac{3}{4}x + 2 \cdot \frac{3}{8}x^2 + 1 \cdot \frac{3}{16}x^3 + 2 \cdot \frac{19}{32}x^4$$

και

$$r(x) = \frac{19}{32}x^5 + 4x^6 - 2 \cdot \frac{19}{32}x^7$$

άρα

$$D_0 = \frac{3}{2}, \quad D_1 = \frac{3}{4}, \quad D_2 = 2 \cdot \frac{3}{8}, \quad D_3 = \frac{3}{16}, \quad D_4 = 2 \cdot \frac{19}{32}, \quad D_5 = \frac{51}{64}$$

Άρα το (Σ_2):

$$\left\{ \begin{array}{l} \frac{1}{8}A + B - C = \frac{3}{16} \\ \\ \frac{1}{16}A + B + C = 2 \cdot \frac{19}{32} \\ \\ \frac{1}{32}A + B - C = \frac{51}{64} \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} A = \frac{4}{6} \\ B = \frac{3}{2} \\ C = \frac{5}{6} \end{array} \right\}$$

Άρα

$$D_n = \frac{4}{6} \cdot \left(\frac{1}{2}\right)^n + \frac{3}{2} + \frac{5}{6} \cdot (-1)^n, \quad \forall n \geq 3$$

Έτσι μπορούμε να υπολογίσουμε οποιονδήποτε όρο της ακολουθίας θέλουμε. Για παράδειγμα, $D_6 = 2 \cdot \frac{51}{128}, D_7 = \frac{179}{256}, D_8 = 2 \cdot \frac{179}{512}$, κ.ο.κ.

1.3.2 Αν η χαρακτηριστική εξίσωση έχει ρίζες με πολλαπλότητα

Σε όλα τα παραδείγματα μέχρι στιγμής, η χαρακτηριστική εξίσωση είχε απλές ρίζες. Θεωρούμε την αναδρομική ακολουθία s_n, της οποίας η αναδρομική σχέση είναι η

$$s_{n+4} = 4s_{n+3} - 6s_{n+2} + 4s_{n+1} - s_n.$$

Πρόκειται δηλαδή για το άθροισμα των n πρώτων όρων της ακολουθίας $U_n = n^2$. Η χαρακτηριστική εξίσωση της s_n είναι

$$q^4 = 4q^3 - 6q^2 + 4q - 1$$

δηλαδή,

$$(q-1)^4 = 0.$$

Η παραπάνω εξίσωση έχει μία ρίζα, την $q_0 = 1$ με πολλαπλότητα 4. Παίρνουμε, δηλαδή μόνο μία γεωμετρική πρόοδο με λόγο 1, της οποίας οι όροι ικανοποιούν την αναδρομική σχέση. Σε αυτές τις περιπτώσεις, πρέπει να βρούμε άλλες αναδρομικές ακολουθίες, οι οποίες, μαζί με την παραπάνω γεωμετρική πρόοδο, αποτελούν την βάση της ακολουθίας. Έστω η αναδρομική σχέση

$$U_{n+k} = C_k^{k-1} a U_{n+k-1} - C_k^{k-2} a^2 U_{n+k-2} + \cdots + (-1)^{k-1} C_k^0 a^k U_n \tag{1.6}$$

όπου $C_k^{k-1}, C_k^{k-2}, \ldots, C_k^0$ είναι οι διωνυμικοί συντελεστές k τάξεως. Η αντίστοιχη χαρακτηριστική εξίσωση της ακολουθίας U_n είναι η

$$q^k = C_k^{k-1} a q^{k-1} - C_k^{k-2} a^2 q^{k-2} + \cdots + (-1)^{k-1} C_k^0 a^k$$

δηλαδή

$$(q-a)^k = 0$$

η οποία έχει μόνο μία ρίζα, την $q_0 = a$ με πολλαπλότητα k.
Προφανώς, $(a-a)^k = 0$, δηλαδή

$$a^k - C_k^{k-1} a^k + C_k^{k-2} a^k - \cdots + (-1)^k C_k^0 a^k = 0 \tag{1.7}$$

Η ισότητα αυτή ισχύει και για κάθε δύναμη μικρότερη του k, δηλαδή $(a-a)^{k-m} = 0$, ή ισοδύναμα

$$C_{k-m}^{k-m} a^{k-m} - C_{k-m}^{k-m+1} a^{k-m} + C_{k-m}^{k-m-2} a^{k-m} - \cdots + (-1)^{k-m} C_{k-m}^0 a^{k-m} = 0$$

όπου $m = 0, 1, \ldots, k-1$.
Η τελευταία ισότητα, για $a = 1$ γίνεται:

$$C_{k-m}^{k-m} - C_{k-m}^{k-m+1} + C_{k-m}^{k-m-2} - \cdots + (-1)^{k-m} C_{k-m}^0 = 0 \tag{1.8}$$

Η τελευταία ισότητα για $m = 0$ δίνει:

$$C_k^k - C_k^{k-1} + C_k^{k-2} - \cdots + (-1)^l C_k^{k-l} + \cdots + (-1)^k C_k^0 = 0. \tag{1.9}$$

Όμως,

$$C_k^{k-l} = \frac{k(k-1)\cdots(l+1)}{1 \cdot 2 \cdots (k-l)} = \frac{k(k-1)\cdots(k-m+1)}{(k-m-l+1)\cdots(k-l)} \cdot C_{k-m}^{k-m-l}$$

ή ισοδύναμα

$$k(k-1)\cdots(k-m+1) \cdot C_{k-m}^{k-m-l} = (k-m-l+1)\cdots(k-l) C_k^{k-l} \tag{1.10}$$

όπου $m = 1, 2, \ldots, k-1$ και $0 \le l \le k-m$.
Πολλαπλασιάζουμε κάθε μία από της ισότητες της (1.8) με τον αντίστοιχο όρο $k(k-1)\cdots(k-m+1)$. Τότε, με χρήση της (1.10) μπορούμε να γράψουμε

$$\begin{aligned}(k-m+1)\cdots k C_k^k - (k-m)\cdots(k-1) C_k^{k-1} + \cdots + \\ + (-1)^l (k-m-l+1)\ldots(k-l) C_k^{k-l} + \cdots + (-1)^{k-m} 1 \cdot 2 \cdots m \cdot C_k^0 = 0\end{aligned} \tag{1.11}$$

Θα αποδείξουμε τώρα ότι $\forall m = 0, 1, \ldots, k-1$, έχουμε

$$k^m C_k^k - (k-1)^m C_l^{k-1} + \cdots + + (-1)^l (k-l)^m C_k^{k-l} + \cdots + (-1)^k 0^m C_k^0 = 0 \tag{1.12}$$

Όντως, για $m = 0$ η (1.12) συμπίπτει με την (1.9).
Ας υποθέσουμε ότι η προς απόδειξη σχέση ισχύει $\forall m = 0, 1, \ldots, j, j \le k-2$.
Εξετάζουμε αν ισχύει για $m = j+1$.
Θεωρούμε το πολυώνυμο

$$f(X) = (X-j)(X-j+1)\cdots(X-1)X = X^{j+1} - b_j X^j - \cdots - b_1 X \tag{1.13}$$

Πολλαπλασιάζουμε κάθε μία εξίσωση της (1.12) με το αντίστοιχο b_i και έχουμε

$$b_1kC_k^k - b_1(k-1)C_k^{k-1} + \dots b_1(-1)^l(k-l)C_k^{k-l} + \cdots + b_1(-1)^k 0C_k^0 = 0$$

$$\vdots$$

$$b_jk^jC_k^k - b_j(k-1)^jC_k^{k-1} + \cdots + b_j(-1)^l(k-l)^jC_k^{k-l} + b_j(-1)^k 0C_k^0 = 0 \quad (1.14)$$

Παρατηρούμε ότι $f(k) = (k-j)\cdots k$, $f(k-1) = (k-j-1)\cdots(k-1)$,
$f(k-l) = (k-l-j)\cdots(k-j)$ κ.ο.κ.
Επομένως, η (1.9) για $m = j+1$ γράφεται:

$$f(k)C_k^k - f(k-1)C_k^{k-1} + \cdots + (-1)^l f(k-l)C_k^{k-l} + \dots (-1)^k f(0)C_k^0 = 0 \quad (1.15)$$

Προσθέτουμε τις (1.14) και (1.15) κατά μέλη και έχουμε:

$$[b_1k + \dots b_jk^j + f(k)]C_k^k - [b_1(k-1) + \cdots + b_j(k-1)^j + f(k-1)]C_k^{k-1} +$$

$$\cdots + (-1)^l[b_1(k-l) + \cdots + b_j(k-l) + f(k-l)]C_k^{k-l} + \cdots + (-1)^k[b_1 0 + \cdots + b_j 0^j + f(0)]C_k^0 = 0.$$

Αλλά από την (1.13) μπορούμε να γράψουμε

$$b_1X + b_2X^2 + \dots b_jX^j + f(X) = X^{j+1}$$

και άρα η τελευταία ισότητα γίνεται

$$k^{j+1}C_k^k - (k-1)^{j+1}C_k^{k-1} + \cdots + (-1)^l(k-l)C_k^{k-l} + \cdots + (-1)^k 0^{j+1}C_k^0 = 0$$

που είναι η η ζητούμενη σχέση για $m = j+1$.
Έστω τώρα το πολυώνυμο

$$P(X) = A_{k-1}X^{k-1} + A_{k-2}X^{k-2} + \cdots + A_0 \quad (1.16)$$

του οποίου ο βαθμός δεν ξεπερνάει το $k-1$. Πολλαπλασιάζουμε κάθε εξίσωση της (1.12) με το αντίστοιχο A_i και παίρνουμε:

- $A_0C_k^k - A_0C_k^{k-1} + \cdots + (-1)^l A_0C_k^{k-l} + \cdots + (-1)^k A_0C_k^0 = 0$
- $A_1C_k^k - A_1(k-1)C_k^{k-1} + \cdots + (-1)^l A_1(k-l)C_k^{k-l} + \cdots + (-1)^k A_1C_k^0 = 0$

$$\vdots$$

- $A_{k+1}k^{k-1}C_k^k - A_{k-1}(k-1)^{k-1}C_k^{k-1} + \cdots + (-1)^l A_{k-1}(k-l)^{k-1}C_k^{k-l} + \cdots + (-1)^k A_{k-1}0^{k-1}C_k^0 = 0$

Προσθέτουμε τις παραπάνω σχέσεις κατά μέλη και προκύπτει:

$$[A_0 + A_1k + \dots A_{k-1}k^{k-1}]C_k^k - [A_0 + A_1(k-1) + \cdots + A_{k-1}(k-1)^{k-1}]C_k^{k-1} + \cdots +$$

$$+(-1)^l[A_0 + A_1(k-l) + \cdots + A_{k-1}(k-l)^{k-1}]C_k^{k-l} + \cdots + (-1)^k[A_0 + A_1 0 + \cdots + A_{k-1}0]C_k^0 = 0$$

ή ισοδύναμα

$$P(k)C_k^k - P(k-1)C_k^{k-1} + \cdots + (-1)^k P(0) = 0 \quad (1.17)$$

Επειδή το $P(X)$ είναι τυχαίο, κάθε πολυώνυμο του οποίου ο βαθμός δεν ξεπερνάει το $k-1$ ικανοποιεί την (1.17) άρα και το $P(X)=(X+n-1)^m$, όπου $n\in\mathbb{N}$ και $m\in\mathbb{Z}$ τέτοιο ώστε $0\leq m\leq k-1$.
Έτσι, η (1.17) γίνεται:

$$(k+n-1)^m C_k^k-(k_n-2)^m C_k^{k-1}+\cdots+(-1)^k(m-1)^m C_k^0=0.$$

Πολλαπλασιάζουμε την τελευταία ισότητα με a^{k+n-1} και αφού $C_k^k=1$, προκύπτει

$$(k+n-1)^m a^{k+n-1}=C_k^{k-1}a(k+n-2)A^{k+n-2}-C_k^{k-2}a^2(k+n-3)^m a^{k+n-3}+\cdots+$$

$$+(-1)^{k-1}C_k^0 a^k(n-1)^m a^{n-1} \tag{1.18}$$

Συγκρίνοντας την (1.18) με την (1.6), έχουμε ότι κάθε μία από τις παρακάτω ακολουθιες (k το πλήθος) ικανοποιούν την (1.6):

$$\left.\begin{array}{l} 1,a,a^2,\ldots,a^{n-1},\ldots \\ 0,a,2a^2,\ldots,(n-1)a^{n-1},\ldots \\ 0,a,2^2a^2,\ldots,(n-1)^2a^{n-1},\ldots \\ \qquad\qquad\qquad\qquad\qquad\qquad\vdots \\ 0,a,2^{k-1}a^2,\ldots,(n-1)^{k-1}a^{n-1} \end{array}\right\} \tag{1.19}$$

όπου η πρώτη ακολουθία είναι για $m=0$, η δεύτερη για $m=1$ κ.ο.κ.
Για να είναι όντως η παραπάνω ακολουθίες βάση, θα πρέπει ο γενικός όρος της ακολουθίας (1), δηλαδή της

$$U_{n+k}=C_k^{k-1}aU_{n+k-1}-C_k^{k-2}a^2U_{n+k-2}+\cdots+(-1)^{k-1}C_k^0a^kU_n$$

να έχει τη μορφή

$$U_n=[B_0+B_1(n-1)+\cdots+B_{k-1}(n-1)^{k-1}]a^{n-1}\quad\text{ή αλλιώς}\quad U_n=Q(n-1)a^{n-1} \tag{1.20}$$

όπου $Q(X)=B_0+B_1X+\cdots+B_{k-1}X^{k-1}$ είναι ένα πολυώνυμο βαθμού το πολύ $k-1$.
Για να είναι η (1.19) βάση της ακολουθίας, είναι αρκετό να δείξουμε ότι το ακόλουθο σύστημα των k στο πλήθος γραμμικών εξισώσεων

$$\begin{array}{l} B_0+B_1 0+\cdots+B_{k-1}0^{k-1}=U_1 \\ B_0+B_1\cdot 1+\cdots+B_{k-1}\cdot 1^{k-1}=U_2 \\ \vdots \\ B_0+B_1(k-1)+\cdots+B_{k-1}(k-1)^{k-1}=U_k \end{array}$$

έχει λύση, με αγνώστους τα $B_1,B_2,\ldots,B_k$.
Ομοίως με την περίπτωση όπου όλες οι ρίζες της χαρακτηριστικής εξίσωσης είναι απλές, αρκεί το σύστημα

$$B_0=0$$

$$B_0+B_1+\cdots+B_{k-1}=0$$

$$\vdots$$

$$B_0 + (k-1)B_1 + \cdots + (k-1)^{k-1}B_{k-1} = 0$$

να έχει λύση μόνο την $B_i = 0, \forall i = 0, 1, \ldots, k-1$. Όμως, οι εξισώσεις του τελευταίου συστήματος ισοδυναμούν με $Q(0) = Q(1) = \cdots = Q(k-1) = 0$. Έχουμε, επομένως, ένα πολυώνυμο βαθμού το πολύ $k-1$ με τουλάχιστον k διαφορετικές ρίζες. Ως εκ τούτου, $Q(X) \equiv 0$ και άρα $B_i = 0, \forall i = 0, 1, \ldots, k-1$ και άρα το (1.19) αποτελεί βάση της αναδρομικής ακολουθίας

$$U_{n+k} = C_k^{k-1} a U_{n+k-1} - C_k^{k-2} a^2 U_{n+k-2} + \cdots + (-1)^{k-1} C_k^0 a^k U_n$$

Αν η αναδρομική ακολουθία ικανοποιεί την γενική αναδρομική σχέση

$$U_{n+k} = a_1 U_{n+k-1} + a_2 U_{n+k-2} + \cdots + a_k U_n, \quad a_k \neq 0 \tag{1.21}$$

τότε η χαρακτηριστική της εξίσωση είναι η

$$q^k = a_1 q^{k-1} + \cdots + a_k \tag{1.22}$$

η οποία μπορεί να έχει ρίζες τις $a, b, \ldots, c$ με πολλαπλότητες $m_1, m_2, \ldots, m_r$ αντίστοιχα. Ισχύει ότι $m_1 + m_2 + \cdots + m_r = k$.
Σ'αυτή τη γενική περίπτωση αποδεικνύεται ότι η βάση της αναδρομικής ακολουθίας θα αποτελείται από τις παρακάτω, k το πλήθος ακολουθίες:

$$\left.\begin{array}{l} 1, a, a^2, \ldots, a^{n-1}, \ldots \\ \vdots \\ 0, a, 2^{m_1-1}a^2, \ldots, (n-1)^{m_1-1}a^{n-1}, \ldots \\ \\ 1, b, b^2, \ldots, b^{n-1}, \ldots \\ \vdots \\ 0, b, 2^{m_2-1}b^2, \ldots, (n-1)^{m_2-1}b^{n-1} \ldots \\ 1, c, c^2, \ldots, c^{n-1}, \ldots \\ \vdots \\ 0, c, 2^{m_r-1}c^2, \ldots, (n-1)^{m_r-1}c^{n-1}, \ldots \end{array}\right\} \tag{1.23}$$

Έτσι,

$$U_n = Q(n-1)a^{n-1} + R(n-1)b^{n-1} + \cdots + S(n-1)c^{n-1} \tag{1.24}$$

όπου $Q(X), R(X), \ldots, S(X)$ είναι πολυώνυμα βαθμού το πολύ $m_1-1, m_2-1, \ldots, m_r-1$ αντίστοιχα. Άρα, ο γενικός όρος U_n οποιασδήποτε αναδρομικής ακολουθίας μπορεί να γραφεί ως το άθροισμα γινομένων ενός πολυωνύμου στη θέση $n-1$ με τον γενικό όρο μιας γεωμετρικής ακολουθίας της οποίας ο λόγος είναι ρίζα της χαρακτηριστικής εξίσωσης της U_n.
Αν όλες οι ρίζες της (1.22) είναι απλές, τα πολυώνυμα είναι σταθερά και άρα ο γενικός όρος σε αυτήν την περίπτωση είναι ένας γραμμικός συνδυασμός όρων κάποιων γεωμετρικών προόδων.
Ισχύει και το αντίστροφο, δηλαδή αν για μία ακολουθία U_n ο γενικός όρος μπορεί να γραφεί όπως στην (1.24), τότε η U_n είναι μια αναδρομική ακολουθία.

Η (1.22) έχει κατασκευαστεί χρησιμοποιώντας τις ρίζες $a, b, \ldots, c$ του χαρακτηριστικού πολυωνύμου με τις αντίστοιχες πολλαπλότητές τους (που είναι οι μεγιστοβάθμιες δυνάμεις των πολυωνύμων αυξημένες κατά μία μονάδα). Έτσι, η αναδρομική σχέση μπορεί να βρεθεί αμέσως. Για παράδειγμα, αν $U_n = (n-1)^2 2^{n-1} + 3^{n-1}$. Συγκρίνοντας την με την (1.24), βλέπουμε ότι οι ρίζες της χαρακτηριστικής εξίσωσης είναι οι $a = 2$ και $b = 2$ με πολλαπλότητα $m_1 = 3$ και $m_2 = 1$ αντίστοιχα. Επομένως, η χαρακτηριστική εξίσωση της ακολουθίας είναι η $(q-2)^3(q-3) = 0$, δηλαδή $q^4 = 9q^3 - 30q^2 + 44q - 24q$ και άρα η αναδρομική σχέση της U_n είναι η

$$U_{n+4} = 9U_{n+3} - 30U_{n+2} + 44U_{n+1} - 24U_n.$$

Ας παραθέσουμε τώρα τα αποτελέσματα σε μερικά παραδείγματα. Έχουμε δει ότι η αριθμητική πρόοδος ικανοποιεί την αναδρομική σχέση $U_{n+2} = 2U_{n+1} - U_n$, η ακολουθία των τετραγώνων των φυσικών αριθμών την $U_{n+3} = 3U_{n+2} - 3U_{n+1} + U_n$, ενώ η ακολουθία $U_n = n^3$ ικανοποιεί την αναδρομική σχέση $U_{n+4} = 4U_{n+3} - 6U_{n+2} + 4U_{n+1} - U_n$. Προφανώς, οι σχέσεις αυτές είναι της μορφής (1.6) για $a = 1$. Ο γενικός όρος σε κάθε περίπτωση πρέπει να είναι της μορφής (1.20), δηλαδή $U_n = B_0 + B_1(n-1) + \cdots + B_{k-1}(n-1)^{k-1}$. Για να βρούμε τα $B_i, i = 0, 1, , \ldots, k-1$ πρέπει να λύσουμε το ακόλουθο σύστημα των $k-1$ εξισώσεων

$$\left.\begin{array}{l} B_0 = U_1 \\ B_0 + B_1 + \cdots + B_{k-1} = U_2 \\ \vdots \\ B_0 + B_1(k-1) + \cdots + B_{k-1}(k-1)^{k-1} \end{array}\right\} \tag{1.25}$$

Στην περίπτωση της αριθμητικής πρόοδου ($k = 2$), η (1.20) γίνεται $U_n = B_0 + B_1(n-1)$ και το (1.25) γίνεται $B_0 = U_1$ και $B_0 + B_1 = U_2$. Επομένως $B_0 = U_1$ που είναι ο πρώτος όρος της ακολουθίας και $B_1 = U_2 - U - 1 = d$, δηλαδή ο λόγος της αριθμητικής πρόοδου. Επομένως $U_n = U_1 + d(n-1)$.

Δεν υπάρχει κανένα ενδιαφέρον στην περίπτωση των ακολουθιών των τετραγώνων και των κύβων των φυσικών αριθμών καθώς ο γενικός όρος αυτών των ακολουθιών είναι $U_n = n^2$ και $U_n = n^3$ αντίστοιχα. Παρ'όλα αυτά, θα εφαρμόσουμε τη θεωρία για να βρούμε τον γενικό όρο για την ακολουθία s_n του αθροίσματος των n πρώτων όρων των ακολουθιών αυτών.

Έχουμε δει ότι αν η $\{U_n\}_{n\in\mathbb{N}}$ ικανοποιεί την αναδρομική σχέση $U_{n+k} = a_1 U_{n+k-1} + a_2 U_{n+k-2} + \cdots + a_k U_n$, τότε η s_n ικανοποιεί την $s_{n+k+1} = (1+a_1)s_{n+k} + (a_2 - a_1)s_{n+k-1} + \cdots + (a_k - a_{k-1})s_{n+1} + a_k s_n$.

Για την (1.6) έχουμε:

$$\begin{gathered} 1 + a_1 = 1 + C_k^1 = C_{k+1}^1 \\ a_2 - a_1 = -(C_k^2 + C_k^1) = -C_{k+1}^2 \\ a_3 - a_2 = C_k^3 + C_k^2 = C_{k+1}^3 \\ \vdots \\ a_k - a_{k-1} = (-1)^{k-1}(C_k^k + C_k^{k-1}) = (-1)^{k-1} C_{k+1}^k \\ -a_k = (-1)^k C_k^k = (-1)^k C_{k+1}^{k+1} \end{gathered}$$

και άρα η αναδρομική σχέση για την $\{s_n\}_{n\in\mathbb{N}}$ γίνεται

$$s_{n+k+1} = C_{k+1}^1 s_{n+k} - C_{k+1}^2 s_{n+k-1} + \cdots + (-1)^k C_{k+1}^{k+1} s_n.$$

- Για το άθροισμα των n πρώτων όρων μιας αριθμητικής πρόοδου U_n

  Όπως είδαμε, αφού η ακολουθία U_n είναι τάξεως $k = 2$, η αντίστοιχη ακολουθια s_n είναι αναδρομική ακολουθία τάξεως $k = 3$ και άρα ο γενικός όρος είναι της μορφής
  $$s_n = B_0 + B_1(n-1) + B_2(n-1)^2$$
  Οι συντελεστές $B_i, i = 0, 1, 2$ θα βρεθούν από το παρακάτω σύστημα:
  $B_0 = s_1 = U_1$
  $B_0 + B_1 + B_2 = s_2 = U_1 + U_2 = 2U_1 + d$
  $B_0 + 2B_1 + 2^2B_2 = s_3 = U_1 + U_2 + U_3 = 3U_1 + d$

  Επομένως, $B_0 = U_1, B_1 = U_1 + \frac{1}{2}U_1, B_2 = \frac{1}{2}d$ και άρα
  $$s_n = U_1 + (U_1 + \frac{1}{2}d)(n-1) + \frac{1}{2}(n-1)^2 = nU_1 + \frac{1}{2}d(n-1)n =$$
  $$= \frac{n[2U_1 + (n-1)d]}{2} = \frac{n[U_1 + U_1 + (n-1)d]}{2} = \frac{n(U_1 + U_n)}{2}$$

- Για το άθροισμα των n πρώτων όρων της $U_n = n^2$

  Όπως είδαμε, η U_n σε αυτή τη περίπτωση είναι μια αναδρομική ακολουθία τάξεως $k = 3$ και άρα η αντίστοιχη s_n είναι μια αναδρομική ακολουθία τάξεως $k = 4$ και επομένως
  $$s_n = B_0 + B_1(n-1) + B_2(n-1)^2 + B_3(n-1)^3.$$
  Τα $B_i, i = 0, 1, 2, 3$ θα βρεθούν από το σύστημα:
  $B_0 = s_1 = 1$
  $B_0 + B_1 + B_2 + B_3 = s_2 = 1 + 2^2 = 5$ $B_0 + 2B_1 + 2^2B_2 + 2^3B_3 = s_3 = 1 + 2^2 + 3^2 = 15$
  $B_0 + 3B_1 + 3^2B_2 + 3^3B_3 = s_4 = 1 + 2^2 + 3^2 + 4^2 = 30.$
  Επομένως $B_0 = 1, B_1 = \frac{13}{6}, B_2 = \frac{3}{2}, B_3 = \frac{1}{3}$ και άρα
  $$s_n = 1 + \frac{13}{6}(n-1) + \frac{3}{2}(n-1)^2 + \frac{1}{3}(n-1)^3 =$$
  $$= \frac{1}{6}n + \frac{1}{2}n^2 + \frac{1}{3}n^3 = \frac{n(n+1)(2n+1)}{6}$$

- Για το άθροισμα των n πρώτων όρων της $U_n = n^3$

  Όπως έχουμε δει, η U_n είναι αναδρομική ακολουθία τάξεως $k = 4$ και επομένως η αντίστοιχη s_n είναι αναδρομική ακολουθία τάξεως $k = 5$.
  Επομένως
  $$s_n = B_0 + B_1(n-1) + B_2(n-1)^2 + B_3(n-1)^3 + B_4(n-1)^4$$
  Οι συντελεστές $B_i, i = 0, 1, 2, 3, 4$ θα βρεθούν από την επίλυση του παρακάτω συστήματος:
  $B_0 = s_1 = 1$
  $B_0 + B_1 + B_2 + B_3 + B_4 = s_2 = 9$

$B_0 + 2B_1 + 4B_2 + 8B_3 + 16B_4 = s_3 = 36$
$B_0 + 3B_1 + 9B_2 + 27B_3 + 64B_4 = s_4 = 100$
$B_0 + 4B_1 + 16B_2 + 64B_3 + 256B_4 = s_5 = 225$

Επομένως, $B_0 = 1, B_1 = 3, B_2 = \frac{13}{4}, B_3 = \frac{3}{2}, B_4 = -\frac{1}{4}$

και άρα

$$s_n = \frac{n^2(n+1)^2}{4}$$

Τέλος, θεωρούμε την $U_n = na^n, n \in \mathbb{N}$, με $a \neq 0, 1$. Παρατηρούμε ότι $2aU_{n+1} - a^2U_n = 2a(n+1)a^{n+1} - a^2na^n = 2a^{n+2}(n+1) - na^{n+2} = (n+2)a^{n+2} = U_{n+2}$.
Επομένως η U_n είναι αναδρομική τάξεως $k = 2$ και έτσι, η s_n θα είναι μια αναδρομική ακολουθία τάξεως $k = 3$ και η αναδρομική της σχέση θα είναι η

$$s_{n+3} = (2a+1)S_{n+2} - (a^2+2a)s_{n+1} + a^2s_n.$$

Η χαρακτηριστική εξίσωση αυτής της ακολουθίας θα είναι η

$$q^3 = (2a+1)q^2 - (a^2+2a)q + a^2.$$

Μία προφανής ρίζα αυτής της εξίσωσης είναι η $q_0 = a$. Για να βρούμε τις υπόλοιπες ρίζες, διαιρούμε το πολυώνυμο $q^3 - (2a+1)q^2 + (a^2+2a)q - a$ με το $q - a$ και το πηλίκο που προκύπτει είναι το $q^2 - (a+1)q + a$, του οποίου οι ρίζες είναι οι $q_1 = a$ και $q_2 = 1$. Επομένως, η χαρατηριστική εξίσωση της s_n έχει ρίζες τις $q_1 = a$, με πολλαπλότητα $m_1 = 2$ και $q_2 = 1$ με πολλαπλότητα $m_2 = 1$. Έτσι, η (1.20) γίνεται

$$s_n = [B_0 + B_1(n-1)]a^{n-1} + C_0.$$

Οι συντελεστές B_0, B_1, C_0 θα βρεθούν λύνοντας το σύστημα:

$B_0 + C_0 = s_1 = a$
$(B_0 + B_1)a + C_0 = s_2 = a + 2a^2$
$(B_0 + 2B_1)a^2 + C_0 = s_3 = a + 2a^2 + 3a^3.$

Έτσι, $B_0 = \frac{a^3-2a^2}{(a-1)^2}, B_1 = \frac{a^2}{(a-1)^2}, C_0 = \frac{a}{(a-1)^2}$
και επομένως

$$s_n = \frac{na^{n+2} - (n+1)a^{n+1} + a}{(a-1)^2} = \frac{U_na^2 - (U_{n+1} - U_1)}{(a-1)^2}$$

Κεφάλαιο 2

Ακολουθίες Lucas

2.1 Ορισμός

Έστω $P, Q \in \mathbb{Z}$ τέτοιοι ώστε $P^2 - 4Q > 0$ και όχι τέλειο τετράγωνο κι έστω το πολυώνυμο $f(X) = X^2 - PX + Q$. Αν με D συμβολίσουμε την διακρίνουσα του πολυωνύμου, τότε $D > 0$ κι άρα το $f(X)$ έχει δύο διακεκριμένες πραγματικές ρίζες, τις $a = \frac{P+\sqrt{D}}{2}$ και $b = \frac{P-\sqrt{D}}{2}$. Από τους τύπους του Vieta, έχουμε:

- $a - b = \sqrt{D}$
- $a + b = P$
- $ab = Q$

Ορίζουμε τώρα τις ακολουθίες $U_n(P, Q) = \frac{a^n - b^n}{\sqrt{D}}, V_n(P, Q) = a^n + b^n, \forall n \in \mathbb{N}$, οι οποίες ονομάζονται πρώτη και δεύτερη, αντίστοιχα, ακολουθία Lucas. Για συντομία, γράφουμε $U_n = U_n(P, Q)$ και $V_n = V_n(P, Q)$, επομένως

$$U_0 = 0, U_1 = 1, V_0 = 2 \text{ και } V_1 = a + b = P.$$

Παρατηρούμε ότι $PU_{n-1} - QU_{n-2} = (a + b)\frac{a^{n-1} - b^{n-1}}{\sqrt{D}} - (ab)\frac{a^{n-2} - b^{n-2}}{\sqrt{D}} = \frac{a^n - b^n}{\sqrt{D}} = U_n$. Επομένως, η ακολουθία U_n είναι αναδρομική ακολουθία τάξεως $k = 2$ και η αναδρομική της σχέση είναι η

$$U_n = PU_{n-1} - QU_{n-2}.$$

Εντελώς όμοια μπορεί κάποιος να δείξει ότι κι η ακολουθία V_n είναι αναδρομική ακολουθία τάξεως $k = 2$ με αναδρομική σχέση:

$$V_n = PV_{n-1} - QV_{n-2}.$$

Οι ακολουθίες U_n, V_nαποτελούν γενικεύσεις τον αριθμών Fibonacci και Lucas, καθώς οι αριθμοί αυτοί προκύπτουν σαν ειδική περίπτωση των ακολουθιών Lucas ως προς το ζευγάρι $(P, Q) = (1, -1)$, δηλαδή $U_n(1, -1) = F_n$ και $V_n(1, -1) = L_n$. [1]

[1] Η ακολουθία L_n ικανοποιεί την ίδια αναδρομική σχέση με την F_n, δηλαδή $L_{n+2} = L_{n+1} + L_n$ με αρχικούς όρους $L_0 = 2, L_1 = 1$

2.2 Ταυτότητες και ιδιότητες των ακολουθιών Lucas

1. $V_n^2 - DU_n^2 = 4Q^n, n \in \mathbb{N}$

Απόδειξη.

$$\begin{aligned} V_n^2 - DU_n^2 &= (a^n + b^n)^2 - D(\frac{a^n - b^n}{\sqrt{D}})^2 \\ &= (a^n + b^n)^2 - (a^n - b^n)^2 \\ &= a^{2n} + b^{2n} + 2(ab)^n - a^{2n} - b^{2n} + 2(ab)^n \\ &= 2Q^n + 2Q^n \\ &= 4Q^n \end{aligned}$$

□

2. $DU_n = V_{n+1} - QV_{n-1}, n \geq 1$

Απόδειξη.

$$\begin{aligned} V_{n+1} - QV_{n-1} &= a^{n+1} + b^{n+1} - Q(a^{n-1} + b^{n-1}) \\ &= a^{n+1} + b^{n+1} - ab(a^{n-1} + b^{n-1}) \\ &= a^{n+1} + b^{n+1} - a^n b - ab^n \\ &= a^n(a - b) - b^n(a - b) \\ &= (a - b)(a^n - b^n) \\ &= \sqrt{D}(a^n - b^n) \\ &= D\frac{a^n - b^n}{\sqrt{D}} \\ &= DU_n \end{aligned}$$

□

3. $V_n = U_{n+1} - QU_{n-1}, n \geq 1$

Απόδειξη.

$$\begin{aligned} U_{n+1} - QU_{n-1} &= \frac{a^{n+1} - b^{n+1}}{\sqrt{D}} - ab\frac{a^{n-1} - b^{n-1}}{\sqrt{D}} \\ &= \frac{a^{n+1} - b^{n+1} - a^n b + ab^n}{a - b} \\ &= \frac{a^n(a - b) + b^n(a - b)}{a - b} \\ &= a^n + b^n \\ &= V_n \end{aligned}$$

□

4. $U_{m+n} = U_m V_n - Q^n U_{m-n}, m, n \in \mathbb{N}, m \geq n$

Απόδειξη.

$$\begin{aligned} U_m V_n - Q^n U_{m-n} &= \frac{(a^m - b^m)(a^n + b^n)}{\sqrt{D}} - Q^n \frac{a^{m-n} - b^{m-n}}{\sqrt{D}} \\ &= \frac{a^{m+n} + a^m b^n - a^n b^m - b^{m+n} - Q^n a^{m-n} + Q^n b^{m-n}}{\sqrt{D}} \\ &= \frac{a^{m+n} - b^{m+n}}{\sqrt{D}} + \frac{a^{m-n} a^n b^n - a^n b^n b^{m-n} - Q^n a^{m-n} + Q^n b^m - n}{\sqrt{D}} \\ &= U_{m+n} + \frac{a^{m-n} Q^n - Q^n b^{m-n} - Q^n a^{m-n} + Q^n b^{m-n}}{\sqrt{D}} \\ &= U_{m+n} \end{aligned}$$

□

5. $V_{m+n} = V_m V_n - Q^n V_{m-n}, m, n \in \mathbb{N}, m \geq n$

Απόδειξη.

$$\begin{aligned} V_m V_n - Q^n V_{m-n} &= (a^m + b^m)(a^n + b^n) - Q^n (a^{m-n} + b^{m-n}) \\ &= a^{m+n} + a^m b^n + b^m a^n + b^{m+n} - Q^n a^{m-n} - Q^n b^{m-n} \\ &= a^{m+n} + b^{m+n} + a^n b^n a^{m-n} + b^n a^n b^{m-n} - Q^n a^{m-n} - Q^n b^{m-n} \\ &= V_{m+n} + a^{m-n} Q^n + b^{m-n} Q^n - Q^n a^{m-n} - Q^n b^{m-n} \\ &= V_{m+n} \end{aligned}$$

□

6. $2U_{m+n} = U_m V_n + U_n V_m, m, n \in \mathbb{N}$

Απόδειξη.

$$\begin{aligned} U_m V_n + U_n V_m &= \frac{a^m - b^m}{\sqrt{D}}(a^n + b^n) + \frac{a^n - b^n}{\sqrt{D}}(a^m + b^m) \\ &= \frac{a^{m+n} + a^m b^n - b^m a^n - b^{m+n} + a^{m+n} + a^n b^m - a^m b^n - b^{m+n}}{\sqrt{D}} \\ &= \frac{2a^{m+n} - 2b^{m+n}}{\sqrt{D}} \\ &= 2\Big(\frac{a^{m+n} - b^{m+n}}{\sqrt{D}}\Big) \\ &= 2U_{m+n} \end{aligned}$$

□

7. $2V_{m+n} = V_m V_n + DU_m U_n, m, n \in \mathbb{N}$

Απόδειξη.

$$\begin{aligned} V_m V_n + DU_m U_n &= (a^m + b^m)(a^n + b^n) + D\Big(\frac{a^m - b^m}{\sqrt{D}}\Big)\Big(\frac{a^n - b^n}{\sqrt{D}}\Big) \\ &= a^{m+n} + a^m b^n + a^n b^m + b^{m+n} + a^{m+n} - a^m b^n - a^n b^m + b^{m+n} \\ &= 2a^{m+n} + 2b^{m+n} \\ &= 2(a^{m+n} + b^{m+n}) \\ &= 2V_{m+n} \end{aligned}$$

□

8. $2Q^n U_{m-n} = U_m V_n - U_n V_m, m, n \in \mathbb{N}, m \geq n$

Απόδειξη.

$$\begin{aligned} U_m V_n - U_n V_m &= \Big(\frac{a^m - b^m}{\sqrt{D}}\Big)(a^n + b^n) - \Big(\frac{a^n - b^n}{\sqrt{D}}\Big)(a^m + b^m) \\ &= \frac{a^{m+n} + a^m b^n - a^n b^m - b^{m+n} - a^{m+n} - a^n b^m + a^m b^n + b^{m+n}}{\sqrt{D}} \\ &= \frac{2a^m b^n - 2a^n b^m}{\sqrt{D}} \\ &= \frac{2a^n a^{m-n} b^n - 2a^n b^n b^{m-n}}{\sqrt{D}} \\ &= 2(ab)^n\Big(\frac{a^{m-n} - b^{m-n}}{\sqrt{D}}\Big) \\ &= 2Q^n U_{m-n} \end{aligned}$$

□

9. $U_{2n} = U_n V_n, n \in \mathbb{N}$

Απόδειξη. Στην ταυτότητα 4. θέτουμε $m = n$:

$$\begin{aligned} U_{2n} &= U_n V_n - Q^n U_0 \\ &\overset{U_0=0}{=} U_n V_n \end{aligned}$$

□

10. $V_{2n} = V_n^2 - 2Q^n, n \in \mathbb{N}$

Απόδειξη. Στην ταυτότητα 5. θέτουμε $m = n$:

$$\begin{aligned} V_{2n} &= V_n V_n - Q^n V_0 \\ &\overset{V_0=2}{=} V_n^2 - 2Q^n \end{aligned}$$

□

11. $U_{3n} = U_n(V_n^2 - Q^n) = U_n(DU_n^2 + 3Q^n), \quad n \in \mathbb{N}$

Απόδειξη. Στην ταυτότητα 4. θέτουμε $m = 2n$:

$$\begin{aligned} U_{3n} &= U_{2n} V_n - Q^n U_n \\ &\overset{9}{=} U_n V_n V_n - Q^n U_n \\ &= U_n(V_n^2 - Q^n) \end{aligned}$$

Αντικαθιστώντας το V_n^2 από την 1 καταλήγουμε στην:

$$\begin{aligned} U_{3n} = U_n(V_n^2 - Q^n) &= U_n(DU_n^2 + 4Q^n - Q^n) \\ &= U_n(DU_n^2 + 3Q^n) \end{aligned}$$

□

12. $V_{3n} = V_n(V_n^2 - 3Q^n), n \in \mathbb{N}$

Απόδειξη. Στην ταυτότητα 5. θέτουμε $m = 2n$:

$$\begin{aligned} V_{3n} &= V_{2n} V_n - Q^n N_n \\ &\overset{10}{=} (V_n^2 - 2Q^n)V_n - Q^n V_n \\ &= V_n^3 - 2V_n Q^n - Q^n V_n \\ &= V_n^3 - 3Q^n V_n \\ &= V_n(V_n^2 - 3Q^n) \end{aligned}$$

□

13. $V_{n+1}V_{n-1} - V_n^2 = DQ^{n-1}, n \geq 1$

Απόδειξη.

$$\begin{aligned}
V_{n+1}V_{n-1} - V_n^2 &= (a^{n+1} + b^{n+1})(a^{n-1} + b^{n-1}) - (a^n + b^n)^2 \\
&= a^{2n} + a^{n+1}b^{n-1} + a^{n-1}b^{n+1} + b^{2n} - a^{2n} - b^{2n} - 2(ab)^n \\
&= (ab)^{n-1}(a^2 + b^2 - 2ab) \\
&= Q^{n-1}(a^2 + b^2 - 2ab) \\
&= Q^{n-1}\Big[\Big(\frac{P+\sqrt{D}}{2}\Big)^2 + \Big(\frac{P-\sqrt{D}}{2}\Big)^2 - 2Q\Big] \\
&= Q^{n-1}\Big(\frac{P^2 + D + 2P\sqrt{D} + P^2 + D - 2P\sqrt{D}}{4} - 2Q\Big) \\
&= Q^{n-1}\Big(\frac{2P^2 + 2D - 8Q}{4}\Big) \\
&= Q^{n-1}\Big(\frac{2P^2 + 2P^2 - 8Q - 8Q}{4}\Big) \\
&= Q^{n-1}(P^2 - 4Q) \\
&= Q^{n-1}D
\end{aligned}$$

□

Αν εφαρμόσουμε τις παραπάνω ταυτότητες για το ζευγάρι $(P, Q) = (1, -1)$ (άρα $D = 5$) προκύπτουν άμεσα οι γνωστές ταυτότητες για τους αριθμούς Fibonacci και Lucas.

1. $L_n^2 - 5F_n^2 = 4(-1)^n$
2. $5F_n = L_{n+1} + L_{n-1}$
3. $L_n = F_{n+1} + F_{n-1}$
4. $F_{m+n} = F_m L_n - (-1)^n F_{m-n}$
5. $L_{m+n} = L_m L_n - (-1)^n L_{m-n}$
6. $2F_{m+n} = F_m L_n + F_n L_m$
7. $2L_{m+n} = L_m L_n + 5F_m F_n$
8. $F_m L_n - F_n L_m = 2(-1)^n F_{m-n}$
9. $F_{2n} = F_n L_n$
10. $L_{2n} = L_n^2 - 2(-1)^n$
11. $F_{3n} = F_n(L_n^2 - (-1)^n) = F_n(5F_n^2 + 3(-1)^n)$
12. $L_{3n} = L_n(L_n^2 - 3(-1)^n)$
13. $L_{n+1}L_{n-1} - L_n^2 = 5(-1)^n$

Οι ακολουθίες των Fibonacci και Lucas μπορούν να επεκταθούν και στους αρνητικούς ακεραίους ως εξής:
Αν $n \in$, τότε

$$F_{-n} = (-1)^{n+1} F_n$$

και

$$L_{-n} = (-1)^n L_n$$

και επομένως οι παραπάνω ταυτότητες έχουν νόημα $\forall m, n \in \mathbb{Z}$.

ΘΕΩΡΗΜΑ 2.2.1: Η ακολουθία του Fibonacci είναι περιοδική $\pmod m$ για κάθε φυσικό αριθμό $m \neq 0$ και μάλιστα ο m διαιρεί τουλάχιστον έναν από τους όρους $F_1, F_2, \ldots, F_{m^2}$.

Απόδειξη. Έστω $\overline{k}$ ο ελάχιστος φυσικός αριθμός τέτοιος ώστε $\overline{k} \equiv k \pmod m$. Σχηματίζουμε τα ζευγάρια $< \overline{F_1}, \overline{F_2} >, < \overline{F_2}, \overline{F_3} >, < \overline{F_3}, \overline{F_4} >, \ldots, < \overline{F_n}, \overline{F_{n+1}} >, \ldots$. Το πλήθος των δυνατών διαφορετικών μεταξύ τους ζευγαριών είναι m^2. Έστω $< \overline{F_k}, \overline{F_{k+1}} >$ το πρώτο ζευγάρι το οποίο εμφανίζεται στην ακολουθία για δεύτερη φορά. Ισχυριζόμαστε ότι αυτό είναι το $< 1, 1 >$. Έστω ότι το πρώτο ζευγάρι που εμφανίζεται ξανά είναι το $< \overline{F_k}, \overline{F_{k+1}} >$ για $k > 1$. Τότε υπάρχει $l \in \mathbb{N}$ με $l < k$ ώστε $< \overline{F_l}, \overline{F_{l+1}} >=< \overline{F_k}, \overline{F_{k+1}} >$. Αφού $F_{l-1} = F_{l+1} - F_l$ και $F_{k-1} = F_{k+1} - F_k$, προκύπτει ότι $\overline{F_{l-1}} = \overline{F_{k-1}}$ και άρα $< \overline{F_{l-1}}, \overline{F_l} >=< \overline{F_{k-1}}, \overline{F_k} >$, που είναι άτοπο αφού υποθέσαμε ότι το $< \overline{F_k}, \overline{F_{k+1}} >$ είναι το πρώτο ζευγάρι με αυτήν την ιδιότητα. Άρα το $< 1, 1 >$, επομένως η ακολουθία F_n είναι περιοδική $\pmod m$.
Επομένως, υπάρχει $t \in \mathbb{N}$ τέτοιος ώστε $< \overline{F_t}, \overline{F_{t+1}} >=< 1, 1 >$, δηλαδή $F_t \equiv 1 \pmod m$ αλλά και $F_{t+1} \equiv 1 \pmod m$. Τότε, $F_{t-1} \equiv F_{t+1} - F_t \equiv 1 - 1 \equiv 0 \pmod m$, επομένως ο m διαιρεί τον F_{t-1}. □

Όμοια μπορούμε να δείξουμε ότι και η ακολουθία L_n των αριθμών Lucas είναι περιοδική $\pmod m$, για κάθε φυσικό αριθμό m.

Τέλος, παραθέτουμε χωρίς απόδειξη δύο προτάσεις για τις ακολουθίες Lucas. Οι αποδείξεις αυτών βρίσκονται στα [10] και [11] αντίστοιχα.

ΠΡΟΤΑΣΗ 2.2.1: Έστω $P \geq 1, P, Q$ περιττοί, Μ.Κ.Δ.$(P, Q) = 1$ και $D = P^2 - 4Q > 0$. Τότε:

1. Αν ο U_n είναι τέλειο τετράγωνο, τότε κατ'ανάγκη $n = 1, 2, 3, 6$ ή 12.
2. Αν ο V_n είναι τέλειο τετράγωνο, τότε κατ'ανάγκη $n = 1, 3$ ή 5.
3. Αν ο U_n είναι διπλάσιο τέλειου τετραγώνου, τότε κατ'ανάγκη $n = 3$ ή 6.
4. Αν ο V_n είναι διπλάσιου τέλειου τετραγώνου, τότε κατ'ανάγκη $n = 3$ ή 6.

ΠΡΟΤΑΣΗ 2.2.2:
1. Αν $V_n = V_m \cdot x^2$ για κάποιο $x \in \mathbb{Z}$, τότε $m = n$.
2. Αν $V_n = 2 \cdot V_m \cdot x^2$ για κάποιο $x \in \mathbb{Z}$, τότε $m = 1$ και $n = 3$.
3. Αν $V_n = 3 \cdot V_m \cdot x^2$ για κάποιο $x \in \mathbb{Z}$, τότε $m = 1, n = 3, Q \equiv 1 \pmod 3$ και $Q \equiv 1$ ή $5 \pmod 8$.

2.3 Κανόνες διαιρετότητας στις ακολουθίες Lucas

ΠΡΟΤΑΣΗ 2.3.1: Αν $(P, Q) = 1$ τότε $(U_n, Q) = 1$ και $(V_n, Q) = 1$.

Απόδειξη.
- Αν $(U_n, Q) > 1$, τότε $\exists p \in \mathbb{P}$ τέτοιος ώστε $p|U_n$ και $p|Q$. Από τον αναδρομικό τύπο της $U_n = PU_{n-1} - QU_{n-2}$ έχουμε ότι $p|PU_{n-1}$ κι αφού $(P, Q) = 1$, έχουμε ότι $p|U_{n-1}$. Συνεχίζοντας το ίδιο επιχείρημα, καταλήγουμε ότι $p|U_1 = 1$, που είναι άτοπο, αφού ο p είναι πρώτος αριθμός. Άρα $(U_n, Q) = 1$.

- Εντελώς όμοια με πριν, αν $(V_n, Q) > 1$, υπάρχει πρώτος αριθμός $p \in \mathbb{P}$ τέτοιος ώστε $p|V_n$ και $p|Q$. Τότε, από την αναδρομική σχέση της ακολουθίας V_n, έχουμε ότι $p|PV_{n-1}$ κι αφού $P|Q$ και $(P, Q) = 1$, προκύπτει $p|V_{n-1}$. Συνεχίζοντας το ίδιο επιχείρημα, καταλήγουμε στο συμπέρασμα ότι $p|V_1 = P$, άτοπο αφού οι P, Q είναι μεταξύ τους πρώτοι. Άρα $(V_n, Q) = 1$.

□

ΠΡΟΤΑΣΗ 2.3.2: Ορίζουμε τον πίνακα $M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}$.
Τότε, $\forall n \in \mathbb{N}$ ισχύει:

$$M^n = \begin{pmatrix} U_{n+1} & -QU_n \\ U_n & -QU_{n-1} \end{pmatrix}$$

Απόδειξη. Θα δειχθεί με επαγωγή ως προς τον φυσικό αριθμό n.

- Για $n = 1$:

$$M^1 = M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}$$

ενώ

$$\begin{pmatrix} U_2 & -QU_1 \\ U_1 & -QU_0 \end{pmatrix} = \begin{pmatrix} \frac{a^2-b^2}{a-b} & -Q \cdot 1 \\ 1 & -Q \cdot 0 \end{pmatrix} = \begin{pmatrix} a+b & -Q \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}$$

επομένως η προς απόδειξη σχέση ισχύει για $n = 1$

- Έστω ότι ισχύει για τον τυχαίο φυσικό αριθμό k, δηλαδή

$$M^k = \begin{pmatrix} U_{k+1} & -QU_k \\ U_k & -QU_{k-1} \end{pmatrix}$$

- Εξετάζουμε τώρα για τον $k + 1$:

$$M^{k+1} = M^k M = \begin{pmatrix} U_{k+1} & -QU_k \\ U_k & -QU_{k-1} \end{pmatrix} \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix} =$$

$$\begin{pmatrix} PU_{k+1} - QU_k & -QU_{k+1} \\ PU_k - QU_{k-1} & -QU_k \end{pmatrix} = \begin{pmatrix} U_{k+2} & -QU + k + 1 \\ U_{k+1} & -QU_k \end{pmatrix}$$

Επομένως, $\forall n \in \mathbb{N}$ ισχύει $M^n = \begin{pmatrix} U_{n+1} & -QU_n \\ U_n & -QU_{n-1} \end{pmatrix}$.

□

ΠΡΟΤΑΣΗ 2.3.3: Αν $m|n$, τότε $U_m|U_n$.

Απόδειξη. Αφού $m|n$ έχουμε ότι $n = k \cdot m, k \in \mathbb{Z}$.

$$M^m = \begin{pmatrix} U_{m+1} & -QU_m \\ U_m & -QU_{m-1} \end{pmatrix} \equiv \begin{pmatrix} U_{m+1} & 0 \\ 0 & -QU_{m-1} \end{pmatrix} \pmod{U_m}.$$

Άρα ο M^m είναι διαγώνιος πίνακας $\pmod{U_m}$, άρα και κάθε δύναμή του θα είναι διαγώνιος πίνακας $\pmod{U_m}$, δηλαδή κι ο $(M^m)^k$ είναι διαγώνιος $\pmod{U_m}$. Επομένως, αφού $(M^m)^k = M^{mk} = M^n$, έχουμε ότι και $(M^m)^k \equiv M^n \pmod{U_m}$. Όμως:

$$(M^m)^k \equiv \begin{pmatrix} U_{m+1} & 0 \\ 0 & -QU_{m-1} \end{pmatrix}^k \equiv \begin{pmatrix} (U_{m+1})^k & 0 \\ 0 & (-QU_{m-1})^k \end{pmatrix} \pmod{U_m}$$

ενώ

$$M^n \equiv \begin{pmatrix} U_{n+1} & -QU_n \\ U_n & -QU_{n-1} \end{pmatrix} \pmod{U_m}$$

άρα $U_n \equiv 0 \pmod{U_m}$, δηλαδή $U_m|U_n$. □

ΠΡΟΤΑΣΗ 2.3.4: Αν $(P, Q) = 1$ και $d = (m, n)$, τότε $(U_m, U_n) = U_d$.

Απόδειξη. Αφού $d|m$ και $d|n$, από την προηγούμενη πρόταση έχουμε ότι $U_d|U_m$ και $U_d|U_n$. Άρα $U_d|(U_m, U_n)$. Επομένως, αρκεί να δείξουμε ότι $(U_m, U_n)|U_d$.
Αν $(U_m, U_n) = 1$. τότε, αφού $U_d|(U_m, U_n)$ προκύπτει ότι $U_d = 1$, επομένως $U_d = (U_m, U_n)$. Έστω $(U_m, U_n) > 1$. Αφού $d = (m, n)$, υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $d = xm + yn$. Τότε, $M^d = M^{xm+yn} = (M^m)^x(M^n)^y$. Αφού οι M^m, M^n είναι διαγώνιοι $(\mathrm{mod}\ (U_m, U_n))$, τότε και ο $(M^m)^x(M^n)^y = M^d$ θα είναι διαγώνιος $\pmod{(U_m, U_n)}$. Όμως, $M^d = \begin{pmatrix} U_{d+1} & -QU_d \\ U_d & -QU_{d-1} \end{pmatrix}$ Άρα, προκύπτει ότι $U_d \equiv 0 \pmod{(U_m, U_n)}$, δηλαδή $(U_m, U_n)|U_d$. Τελικά, $(U_m, U_n) = U_d$. □

ΛΗΜΜΑ 2.3.1: Υποθέτουμε ότι $(P, Q) = 1$ κι έστω $D = P^2 - 4Q$ η διακρίνουσα του $f(X) = X^2 - PX + Q$.

- Αν P άρτιος, τότε $4|D, V_n =$ άρτιος και $(\frac{V_n}{2}, \frac{D}{4}) = 1 \quad \forall n \in \mathbb{N}$.
- Αν P περιττός, τότε $(D, V_n) = 1, \forall n \geq 1$.

Απόδειξη.
- Αν P άρτιος, τότε $P = 2l, l \in \mathbb{Z}$ και προφανώς $4|D$.
  Για $n = 1$ έχουμε $V_1 = a + b = P$ που είναι άρτιος.
  Έστω ότι ο V_k είναι άρτιος για κάθε $k = 1, 2, \ldots, n-1$. Τότε $V_n = PV_{n-1} - QV_{n-2}$, δηλαδή ο V_n είναι άρτιος $\forall n \in \mathbb{N}$.
  Ακόμα, $(\frac{V_1}{2}, \frac{D}{4}) = (\frac{P}{2}, \frac{D}{4})$. Όμως, $D = P^2 - 4Q = 4l^2 - 4Q$,
  δηλαδή $\frac{D}{4} = l^2 - Q$ και άρα $(\frac{P}{2}, \frac{D}{4}) = (l, l^2 - Q) = (l, Q) = 1$, αφού $(P, Q) = 1$.
  Υποθέτουμε ότι ισχύει για $n = k$, δηλαδή $(\frac{V_k}{2}, \frac{D}{4}) = 1$.
  Εξετάζουμε για $n = k + 1$.
  Από την ταυτότητα (13) για τις ακολουθίες Lucas $V_{k+1}V_{k-1} - V_k^2 = DQ^{k-1}$ προκύπτει $\frac{V_{k+1}}{2}\frac{V_{k-1}}{2} - (\frac{V_k}{2})^2 = \frac{D}{4}Q^{k-1}$. Αν $(\frac{V_{k+1}}{2}, \frac{D}{4}) > 1, \exists p \in \mathbb{P}$ με $p|\frac{V_{k+1}}{2}$ και $p|\frac{D}{4}$, δηλαδή $p|(\frac{V_k}{2})^2$, δηλαδή $p|\frac{V_k}{2}$ που είναι άτοπο, αφού $(\frac{V_k}{2}, \frac{D}{4}) = 1$. Άρα ισχύει και για $n = k + 1$, δηλαδή $\forall n \in \mathbb{N}$ ισχύει $(\frac{V_n}{2}, \frac{D}{4}) = 1$.

- Αν P περιττός:
  Για $n = 1$, έχουμε $(D, V_1) = (P^2 - 4Q, P) = (-4Q, P)$. Αν ίσχυε $(-4P, Q) > 1$, τότε $\exists p \in \mathbb{P}$ τέτοιος ώστε $p| -4Q$ και $p|P$. Αφού, ο p είναι πρώτος και $p|4Q$, τότε $p|4$ ή $p|Q$, που και τα δύο οδηγούν σε άτοπο, αφού αν $p|4$ έχουμε ότι $p = 2$ και άρα $2|P$, ενώ ο P είναι περιττός, ενώ αν $p|Q$, τότε $p = 1$ αφού $(P, Q) = 1$. Επομένως $(-4Q, P) = 1$ και άρα $(D, V_1) = 1$.
  Έστω ότι $(D, V_n) = 1$ για κάθε $n = 1, 2, \ldots, k$.
  Εξετάζουμε για $n = k + 1$.
  Έστω ότι $(D, V_{k+1}) > 1$. Τότε υπάρχει πρώτος p τέτοιος ώστε $p|D$ και $p|V_{k+1}$ και άρα από την ταυτότητα 13. συμπαιρένουμε πάλι ότι $p|V_k$ που είναι άτοπο, αφού υποθέσαμε ότι $(D, V_k) = 1$. Επομένως η προς απόδειξη σχέση ισχύει για $n = k+1$ και άρα για κάθε φυσικό αριθμό n.

□

ΠΡΟΤΑΣΗ 2.3.5: Ορίζουμε τον πίνακα $Z = \begin{pmatrix} P & -2Q \\ 2 & -P \end{pmatrix}$. Για την δεύτερη ακολουθία Lucas V_n ισχύει:

$$ZM^n = \begin{pmatrix} V_{n+1} & -QV_n \\ V_n & -QV_{n-1} \end{pmatrix}$$

Απόδειξη. $ZM^n = \begin{pmatrix} P & -2Q \\ 2 & -Q \end{pmatrix} \begin{pmatrix} U_{n+1} & -QU_n \\ U_n & -QU_{n-1} \end{pmatrix} =$

$\begin{pmatrix} PU_{n+1} - 2QU_n & -PQU_n + 2Q^2U_{n-1} \\ 2U_{n+1} - PU_n & -2QU_n - PQU_{n-1} \end{pmatrix} =$

$\begin{pmatrix} PU_{n+1} - QU_n - QU_n & -Q(PU_n - QU_{n-1} - QU_{n-1} \\ PU_n - QU_{n-1} - QU_{n-1} & -Q(PU_{n-1} - 2QU_{n-2}) \end{pmatrix} = \begin{pmatrix} V_{n+1} & -QV_n \\ V_n & -QV_{n-1} \end{pmatrix}$ □

ΠΡΟΤΑΣΗ 2.3.6: Αν $m|n$ και $\frac{n}{m}$ περιττός, τότε $V_m|V_n$.

Απόδειξη. Έχουμε $m|n$ άρα $\exists k \in \mathbb{Z}$ περιττός τέτοιος ώστε $n = km$. Αν $|V_m| = 1$, τελειώσαμε, άρα υποθέτουμε ότι $|V_m| \neq 1$. Αφού k περιττός, τότε $k = 2l + 1, l \in \mathbb{Z}$.
Από την Πρόταση 2.3.5. ο ZM^m είναι διαγώνιος πίνακας $\pmod{V_m}$ που σημαίνει ότι και ο πίνακας $D^n ZM^{mk} = (ZM^m)^k$ είναι επίσης διαγώνιος πίνακας $\pmod{V_m}$.

- Αν ο P είναι περιττός, τότε από το Λήμμα 2.3.1.$(V_m, D) = 1$, άρα $V_m|V_{km}$, δηλαδή $V_m|V_n$.
- Αν ο P είναι άρτιος, τότε ο $\frac{1}{2}ZM^m$ είναι διαγώνιος πίνακας $\pmod{\frac{V_m}{2}}$, που σημαίνει ότι και ο $(\frac{1}{2}ZM^m)^k = \frac{1}{2^k}D^n Z^{mk}$ είναι διαγώνιος πίνακας $\pmod{\frac{V_m}{2}}$. Από το Λήμμα 2.3.1. έχουμε ότι $(\frac{V_m}{2}, \frac{D}{4}) = 1$, έχουμε ότι $\frac{V_m}{2}|\frac{V_{mk}}{2}$ ή ισοδύναμα $V_m|V_n$.

□

ΠΡΟΤΑΣΗ 2.3.7: Υποθέτουμε ότι $(P, Q) = 1, d = (m, n)$ και $\frac{m}{d}, \frac{n}{d}$ είναι και οι δύο περιττοί. Τότε $(V_m, V_n) = V_d$.

Απόδειξη. Αν $D = 0$ τότε $P^2 - 4Q = 0$ κι αφού P, Q μεταξύ τους πρώτοι, $P = 2, Q = 1$ και άρα $V_n = 2, \forall n \in \mathbb{N}$ και η προς απόδειξη σχέση ισχύει. Έστω $D \neq 0$. Ο Z είναι αντιστρέψιμος αφού $detZ = -D$. Από την πρόταση 2.3.6 αφού $d|m, d|n$ έχουμε ότι $V_d|V_m$ και $V_d|V_n$, άρα $V_d|(V_m, V_n)$. Άρα αρκεί να δείξουμε ότι $(V_m, V_n)|V_d$. Αν $(V_m, V_n) = 1$, τότε και $V_d = 1$, άρα ισχύει. Έστω $(V_m, V_n) > 1$. Αφού $d = (m, n)$, υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $xm + yn = d$. Αφού οι $\frac{m}{d}, \frac{n}{d}$ είναι περιττοί, ένας εκ των $\{x, y\}$ πρέπει να είναι άρτιος και ο άλλος περιττός.

- Έστω P περιττός:
  Οι ZM^m και ZM^n είναι διαγώνιοι πίνακες $\pmod{(V_m, V_n)}$, άρα και ο $(ZM^m)^x(ZM^n)^y = D^kZM^d$ είναι διαγώνιος πίνακας $\pmod{(V_m, V_n)}$, όπου $k \in \mathbb{Z}$. Άρα $(V_m, V_n)|V_d$ και επομένως $(V_m, V_n) = V_d$.

- Έστω P άρτιος:
  Τότε οι $\frac{1}{2}ZM^m$ και $\frac{1}{2}ZM^n$ είναι διαγώνιοι πίνακες $\pmod{(\frac{V_m}{2}, \frac{V_n}{2})}$. Έχουμε ότι $(\frac{D}{4})^{\frac{x+y-1}{2}}(\frac{1}{2})ZM^d) = ((\frac{1}{2})ZM^m)^x((\frac{1}{2})ZM^n)^y$ κι αφού $(\frac{D}{4}, \frac{V_n}{2}) = 1 \forall n \in \mathbb{N}$, έχουμε ότι $(\frac{1}{2})ZM^d$ είναι διαγώνιος $\pmod{(\frac{V_m}{2}, \frac{V_n}{2})}$. Άρα $(\frac{V_m}{2}, \frac{V_m}{2})|\frac{V_d}{2}$, άρα $(V_m, V_n)|V_d$. Τελικά, $V_d = (V_m, V_n)$.

□

ΠΡΟΤΑΣΗ 2.3.8: Έστω $m, n \in \mathbb{Z}$ και $d = (m, n)$. Τότε

$$(U_m, V_n) = \begin{cases} V_d & \text{αν } \frac{m}{d} \text{ άρτιος και } \frac{n}{d} \text{ περιττός} \\ 1 \text{ ή } 2 & \text{αλλιώς} \end{cases}$$

Μάλιστα, ο (U_m, V_n) είναι άρτιος αν και μόνον αν ο Q είναι περιττός και ισχύει ένα από τα εξής:

- Οι P, d είναι και οι δύο άρτιοι ή
- ο P είναι περιττός και $3|d$.

Για την απόδειξη της παραπάνω πρότασης παραπέμπουμε στο [6]

2.4 Test ελέγχου πρώτων αριθμών

ΠΡΟΤΑΣΗ 2.4.1: Έστω U_n η ακολουθία Lucas ως προς το ζευγάρι (P, Q) κι έστω $p \in \mathbb{P}$ τέτοιος ώστε $p \not| 2QD$. Τότε:

$$U_{p-\varepsilon_p} \equiv 0 \pmod{p}$$

όπου $\varepsilon_p = \left(\frac{D}{p}\right)$.

Απόδειξη.

$$a^n = \left(\frac{P + \sqrt{D}}{2}\right)^n = 2^{-n} \sum_{k=0}^{n} \binom{n}{k} P^{n-k} (\sqrt{D})^k$$

$$b^n = \left(\frac{P - \sqrt{D}}{2}\right)^n = 2^{-n} \sum_{k=0}^{n} \binom{n}{k} P^{n-k} (-1)^k (\sqrt{D})^k$$

Επομένως,

$$2^{n-1} U_n = \sum_{\substack{0 \le k \le n \\ \text{k περιττός}}} \binom{n}{k} P^{n-k} D^{\frac{k-1}{2}} \tag{2.1}$$

- Αν $\left(\frac{D}{p}\right) = 1$, τότε $\exists C$ τέτοιο ώστε $P^2 - 4Q = D \equiv C^2 \pmod{p}$ και αφού $p \not| 4Q$ (αφού $p \not| 2QD$), έχουμε $P^2 \not\equiv C^2 \pmod{p}$. Στην (2.1) θέτουμε $n = p - 1$: $2^{p-2}U_{p-1} = \binom{p-1}{1}P^{p-2} + \binom{p-1}{3}P^{p-4}D + \binom{p-1}{5}P^{p-6}D^2 + \cdots + \binom{p-1}{p-2}PD^{(\frac{p-3}{2})}$. Για τον διωνυμικό συντελεστή $\binom{p-1}{k}$ ισχύει $\binom{p-1}{k} \equiv -1 \pmod{p}$ για κάθε περιττό $k \in \mathbb{Z}$ και όταν ο $\binom{p-1}{k}$ ορίζεται, επομένως:

$$2^{p-2}U_{p-1} = \binom{p-1}{1}P^{p-2} + \binom{p-1}{3}P^{p-4}D + \binom{p-1}{5}P^{p-6}D^2 + \cdots + \binom{p-1}{p-2}PD^{\frac{p-3}{2}} \equiv$$

$$-[P^{p-2} + P^{p-4}D + P^{p-6}D^2 + \cdots + PD^{\frac{p-3}{2}}] \pmod{p} \equiv$$

$$-P\Big(\frac{P^{p-1} - D^{\frac{p-1}{2}}}{P^2 - D}\Big) \pmod{p} \equiv$$

$$-P\Big(\frac{P^{p-1} - C^{p-1}}{P^2 - C^2}\Big) \pmod{p} \equiv {}^2 0 \pmod{p}.$$

Άρα, προκύπτει ότι $2^{p-2}U_{p-1} \equiv 0 \pmod{p}$ κι αφού $p \not| 2$ έχουμε $U_{p-1} \equiv 0 \pmod{p}$. Άρα $p|U_{p-1}$.

- Αν $\left(\frac{D}{p}\right) = -1$, θέτουμε στην 2.1 όπου $n = p + 1$:

$$2^p U_{p+1} = \sum_{\substack{0 \le k \le p+1 \\ \text{k περιττός}}} \binom{p+1}{k} P^{p+1-k} D^{\frac{k-1}{2}}$$

Όμως, $\binom{p+1}{k} \equiv 0 \pmod{p} \forall k : 0 \le k \le p+1, k \ne 1, p+1$, άρα:

$$2^p U_{p+1} = \sum_{\substack{0 \le k \le p+1 \\ \text{k περιττός}}} \binom{p+1}{k} P^{p+1-k} D^{\frac{k-1}{2}} \equiv (p+1)P^p + PD^{\frac{p-1}{2}} \equiv P + PD^{\frac{p-1}{2}} \equiv$$

$$P + P\Big(\frac{D}{p}\Big) \equiv P - P \equiv 0 \pmod{p}$$

Επομένως, $2U_{p+1} \equiv 0 \pmod{p}$ κι αφού $p \not| 2$, έχουμε $U_{p+1} \equiv 0 \pmod{p}$, ή ισοδύναμα $p|U_{p+1}$.

□

Το αντίστροφο της τελευταίας πρότασης δεν ισχύει. Υπάρχουν σύνθετοι φυσικοί αριθμοί $n \in \mathbb{N}$ για τους οποίους η ισοτιμία $U_{n-\varepsilon_n} \equiv 0 \pmod{n}$ είναι αληθής. Τέτοιοι αριθμοί θα λέγονται *ψευδοπρώτοι Lucas* ως προς το ζευγάρι (P, Q), ενώ συγκεκριμένα για το ζευγάρι $(1, -1)$ θα λέγονται *ψευδοπρώτοι Fermat* (για παράδειγμα ο 323 είναι ένας ψευδοπρώτος Fermat).

ΟΡΙΣΜΟΣ 2.4.1: Έστω U_n μία ακολουθία Lucas ως προς το ζευγάρι (P, Q) κι έστω $n \in \mathbb{N}$ τέτοιος ώστε $(n, 2QD) = 1$. Τότε, ο ελάχιστος θετικός ακέραιος $l(n) := l_{(P,Q)}(n)$ για τον οποίο ισχύει $U_{l(n)} \equiv 0 \pmod{n}$ θα λέγεται σημείο εισόδου του n στην ακολουθία U_n.

ΠΡΟΤΑΣΗ 2.4.2: Ισχύει η ισοδυναμία $n|U_k \Leftrightarrow l(n)|k$.

[2] Από το μικρό θεώρημα του Fermat

Απόδειξη. Έστω $k = l(n) \cdot \pi + \upsilon, 0 \leq \upsilon < l(n)$ κι έστω ότι $\upsilon \neq 0$. Εξ ορισμού του $l(n)$, $n|U_{l(n)}$, άρα $n|U_{l(n)\cdot\pi}$. Ακόμα, από υπόθεση $n|U_k$. Στην ταυτότητα 8. των ακολουθιών Lucas θέτουμε $m = k$ και $n = l(n) \cdot \pi$ και έχουμε:

$$U_k V_{l(n)\cdot\pi} - U_{l(n)\cdot\pi} V_k = 2Q^{l(n)\cdot\pi} U_{k-l(n)\cdot\pi}$$

δηλαδή,

$$U_k V_{l(n)\cdot\pi} - U_{l(n)\cdot\pi} V_k = 2Q^{l(n)\cdot\pi} U_\upsilon.$$

Τώρα, αφού $n|U_k, U_{l(n)\cdot\pi}$ προκύπτει ότι $n|2Q^{l(n)\cdot\pi}U_\upsilon$ και αφού Μ.Κ.Δ.$(n, 2Q) = 1$, έχουμε ότι $n|U_\upsilon$ που είναι άτοπο αφού ο $l(n)$ είναι ο ελάχιστος θετικός ακέραιος με αυτή την ιδιότητα. Ως εκ τούτου $\upsilon = 0$ και άρα $k = l(n) \cdot \pi$, άρα $l(n)|k$.
Για το αντίστροφο, αφού $l(n)|k$, έχουμε $U_{l(n)}|U_k$ κι αφού $n|U_{l(n)}$, έχουμε ότι $n|U_k$. □

Παρακάτω δίνονται δύο tests πιστοποίησης πρώτων αριθμών.

ΠΡΟΤΑΣΗ 2.4.3: (Το test του Lucas) Έστω ότι μας δίνεται κάποια ακολουθία Lucas και ένας φυσικός αριθμός n τέτοιος ώστε $(n, 2Q) = 1$, $\left(\frac{D}{n}\right) = -1$ και $U_{n+1} \equiv 0 \pmod{n}$. Αν s είναι ένας διαιρέτης του $n+1$ και για κάθε πρώτο διαιρέτη q του s να ισχύει $(U_{\frac{n+1}{q}}, n) = 1$, τότε για κάθε πρώτο διαιρέτη p του n ισχύει $p \equiv \left(\frac{D}{p}\right) \pmod{s}$. Επιπλέον, αν $s > \sqrt{n} + 1$, τότε ο n είναι πρώτος αριθμός.

Απόδειξη. Επειδή $U_{n+1} \equiv 0 \pmod{n}$ έχουμε ότι $l(n)|n+1$. Επομένως, για κάθε πρώτο p που διαιρεί τον n ισχύει $l(p)|n+1$. Ακόμα, αφού $(U_{\frac{n+1}{q}}, n) = 1$, ο $p \not| U_{\frac{n+1}{q}}$, άρα $l(p)|\frac{n+1}{q}$.
Έστω $k \in \mathbb{N}$, τέτοιος ώστε ο q^k να είναι η μέγιστη δύναμη του q τέτοιος ώστε $q^k|s$ κι αφού $q|n+1$, έχουμε $q^k|n+1$. Άρα $q^k|l(p)$ κι αυτό ισχύει για κάθε πρώτο διαιρέτη του s, άρα και για το γινόμενό τους. Επομένως, $s|l(p)$. Από την πρόταση, αφού $U_{p-\varepsilon_p} \equiv 0 \pmod{p}$, έχουμε ότι $l(p)|p-\varepsilon_p$, άρα και $s|p-\varepsilon_p = p-\left(\frac{D}{p}\right)$ ή ισοδύναμα $p-\left(\frac{D}{p}\right)$, δηλαδή $p \equiv \left(\frac{D}{p}\right) \pmod{s}$.
Αν $s > \sqrt{n} + 1$, τότε για κάθε πρώτο p που διαιρεί τον n, έχουμε $p + 1 \geq p - \left(\frac{D}{p}\right) \geq s > \sqrt{n} + 1$, δηλαδή $p > \sqrt{n}$. Αν ο n δεν ήταν πρώτος, θα είχε έναν πρώτο διαιρέτη $r \leq \sqrt{n}$. □

ΠΡΟΤΑΣΗ 2.4.4: Για κάθε περιττό πρώτο p ισχύει $U_p \equiv \left(\frac{D}{p}\right) \pmod{p}$ και
$V_p \equiv P \pmod{p}$.

Απόδειξη. Στην 2.1 θέτουμε $n = p$ και έχουμε

$$2^{p-1}U_p = \sum_{\substack{0\leq k\leq p \\ \text{k περιττός}}} \binom{p}{k} P^{p-k} D^{\frac{k-1}{2}}$$

Αν θεωρήσουμε την τελευταία σχέση $\pmod{p}$, αφού $\binom{p}{k} \equiv 0 \pmod{p}$ για κάθε $k = 1, 2, \ldots, p-1$, έχουμε ότι

$$2^{p-1}U_p \equiv D^{\frac{p-1}{2}} \pmod{p}$$

κι αφού $(2, p) = 1$ από το μικρό θεώρημα Fermat έχουμε $2^{p-1} \equiv 1 \pmod{p}$. Τελικά, $U_p \equiv D^{\frac{p-1}{2}} \equiv \left(\frac{D}{p}\right) \pmod{p}$.
Για το $V_p \equiv P \pmod{p}$, η απόδειξη είναι παρόμοια, δηλαδή:

$$V_p = a^p + b^p = \left(\frac{P + \sqrt{D}}{2}\right)^p + \left(\frac{P - \sqrt{D}}{2}\right)^p$$

άρα

$$2^p V_p = \sum_{k=0}^{p} \binom{p}{k} P^{p-k} (\sqrt{D})^k + \sum_{k=0}^{p} \binom{p}{k} P^{p-k} (-1)^k (\sqrt{D})^k$$

Αν θεωρήσουμε $\pmod p$ την τελευταία σχέση και αφού $\binom{p}{k} \equiv 0 \pmod p$ για κάθε $k = 1, 2, \ldots, p-1$, προκύπτει ότι

$$2^p V_p \equiv P^p + (\sqrt{D})^p + P^p - (\sqrt{D})^p \pmod p$$

δηλαδή $2^{p-1} V_p = P^p$. Επειδή $(2, p) = (P, p) = 1$, έχουμε ότι $2^{p-1} \equiv 1 \pmod p$ και ότι $P^{p-1} \equiv 1 \pmod p$ από όπου προκύπτει ότι $P^p \equiv P \pmod p$.
Τελικά $V_p \equiv P \pmod p$. □

ΟΡΙΣΜΟΣ 2.4.2: Η ακολουθία $\{S_n\}_{n \in \mathbb{N}}$ με αναδρομικό τύπο $S_{n+1} = S_n^2 - 2, S_1 = 4$ λέγεται ακολουθία Lucas - Lehmer.

ΠΡΟΤΑΣΗ 2.4.5: (Test των Lucas - Lehmer για τους πρώτους αριθμούς Mersenne) Αν $p \in \mathbb{P}$, p περιττός, τότε ο $M_p := 2^p - 1$ είναι πρώτος αν και μόνον αν $M_p | S_{p-1}$.

Απόδειξη. Θεωρούμε την ακολουθία Lucas ως προς το ζευγάρι $(P, Q) = (2, -2)$, δηλαδη $D = 12, a = 1 + \sqrt{3}, b = 1 - \sqrt{3}$. Ισχύει ότι $U_p \equiv \left(\frac{3}{p}\right) \pmod p$ και $V_p \equiv 2 \pmod p$.
Υποθέτουμε ότι ο $M_p = 2^p - 1$ είναι πρώτος αριθμός, όπου p περιττός πρώτος αριθμός. Θα αποδείξουμε ότι $S_{p-1} \equiv 0 \pmod{M_p}$. Επειδή ο M_p είναι περιττός, η τελευταία ισοτιμία είναι ισοδύναμη με την $2^{2^{p-2}} \cdot S_{p-1} \equiv 0 \pmod{M_p}$. Για κάθε $i \geq 1$ ορίζουμε $T_i = 2^{2^{i-1}} \cdot S_i$. Συνεπώς $T_1 = 2^{2^0} \cdot S_1 = 2 \cdot 4 = 8$ και $T_{i+1} = 2^{2^{(i+1)-1}} \cdot S_{i+1} = (2^{2^{i-1}})^2 \cdot (S_i^2 - 2) = (2^{2^{i-1}} \cdot S_i)^2 - 2^{2^i+1} = T_i^2 - 2^{2^i+1}$.
Επομένως αρκεί να δείξουμε ότι:

$$T_{p-1} = 2^{2^{p-2}} \cdot S_{p-1} \equiv 0 \pmod{M_p}.$$

Αλλά, $T_p = T_{p-1}^2 - 1 - 4 \cdot 2^{(2^{p-1}+1)}$. Επειδή $M_p = 2^p - 1 \equiv 7 \pmod 8$, έπεται ότι

$$\left(\frac{2}{M_p}\right) = (-1)^{\frac{M_p^2 - 1}{8}} = 1.$$

Ακόμα, από το θεώρημα του Euler προκύπτει ότι:

$$2^{2^{p-1}-1} = 2^{\frac{M_p - 1}{2}} \equiv \left(\frac{2}{M_p}\right) \equiv 1 \pmod{M_p}.$$

Επομένως, αρκεί να αποδείξουμε ότι $T_p \equiv -4 \pmod{M_p}$.
Ισχυριζόμαστε ότι $T_i = V_{2^i}$. Πράγματι, για $i = 1$ έχουμε $T_1 = 8 - 2 + (-2)^2 = V_2$.
Υποθέτουμε ότι $T_{k-1} = V_{2^{k-1}}$ για κάποιο φυσικό k. Εξετάζουμε αν $T_k = V_{2^k}$.

$$T_k = T_{k-1}^2 - 2^{2^{k-1}+1} = V_{2^{k-1}}^2 - 2^{2^{k-1}+1}$$

Από την ταυτότητα 10. των ακολουθιών Lucas έχουμε ότι $V_n^2 - 2(-2^n)$ έπεται ότι:

$$T_k = V_{2^{k-1}}^2 + (-2)^{2^{k-1}+1} = V_{2 \cdot 2^{k-1}} = V_{2^k}.$$

Τώρα, από την ταυτότητα 7. έχουμε ότι:

$$2T_p = 2V_{2^p} = 2V_{(2^p-1)+1} = 2V_{M_p+1} = V_{M_p} V_1 + 12 U_{M_p} U_1 = 2V_{M_p} + 12 U_{M_p}.$$

Για κάθε πρώτο p ισχύουν $M_p \equiv 1 \pmod 3$ και $M_p \equiv 1 \pmod 4$. Επομένως:

$$U_{M_p} \equiv \left(\frac{3}{M_p}\right) \equiv -\left(\frac{M_p}{3}\right) \equiv -\left(\frac{1}{3}\right) \equiv -1 \pmod{M_p}$$

αλλά και $V_{M_p} \equiv 2 \pmod{M_p}$. Άρα:

$$T_p \equiv V_{M_p} + 6U_{M_p} \equiv 2 - 6 \equiv -4 \pmod{M_p}.$$

Στη συνέχεια θα αποδείξουμε το αντίστροφο. Υποθέτουμε ότι για κάποιον $n \in \mathbb{N}$ ισχύει η ισοτιμία $S_{n-1} \equiv 0 \pmod{M_n}$ και θα αποδείξουμε ότι ο $M_n = 2^n - 1$ είναι πρώτος αριθμός. Από την υπόθεση έχουμε ότι $M_n | S_{n-1}$ και επομένως $M_n | T_{n-1}$, δηλαδή $2^n - 1 | 2^{2^{n-1}-1} \cdot S_{n-1}$. Έστω p ένας πρώτος αριθμός τέτοιος ώστε $p | 2^n - 1$ (άρα ο p είναι περιττός πρώτος) και $t := l(p)$ ο δείκτης εισόδου του p στην ακολουθία $U_n(2, -2), n \in \mathbb{N}$. Επομένως $p | U_t$. Από την ταυτότητα 9. των ακολουθιών Lucas ($U_{2n} = U_n V_n$). έπεται ότι $U_{2^n} = U_{2^{n-1}} V_{2^{n-1}} = U_{2^{n-1}} T_{n-1}$. Επειδή $2^n - 1 | T_{n-1}$ έχουμε ότι $2^n - 1 | U_{2^n}$ και άρα $p | U_{2^n}$. Συνεπώς, $t | 2^n$. Θα αποδείξουμε ότι $t = 2^n$. Αν ίσχυε $t | 2^{n-1}$, θα είχαμε $p | U_{2^{n-1}}$, οπότε, αφού $p | T_{n-1} = V_{2^{n-1}}$, θα είχαμε $p | V_{2^{n-1}}^2 - 12U_{2^{n-1}} = 2^2 \cdot (-2)^{2^n - 1} =$ δύναμη του 2, που είναι άτοπο αφού ο p είναι περιττός πρώτος. Αποδείξαμε δηλαδή ότι $t = l(p) = 2^n$. Αλλά, επειδή $t = l(p) = 2^n \leq p + 1 \leq 2^n$, έπεται ότι $p = 2^n - 1$ και άρα ο $M_n = 2^n - 1$ είναι πρώτος αριθμος. □

Στο [2] αποδεικνύεται το test των Lucas και Lehmer για $(P, Q) = (2 + \sqrt{3}, 2 - \sqrt{3})$. Ας εφαρμόσουμε το test για $p = 11$ και $p = 13$.

- Για $p = 11$.
  Ο $M_{11} = 2^{11} - 1 = 2047$ δεν είναι πρώτος αριθμός. Πράγματι, $2047 = 23 \cdot 89$.
  Ας το διαπιστώσουμε και με τη βοήθεια του test.

  $S_1 \equiv 4 \pmod{2047}$
  $S_2 \equiv S_1^2 - 2 \equiv 14 \pmod{2047}$
  $S_3 \equiv S_2^2 - 2 \equiv 194 \pmod{2047}$
  $S_4 \equiv S_3^2 - 2 \equiv 788 \pmod{2047}$
  $S_5 \equiv S_4^2 - 2 \equiv 701 \pmod{2047}$
  $S_6 \equiv S_5^2 - 2 \equiv 119 \pmod{2047}$
  $S_7 \equiv S_6^2 - 2 \equiv 1877 \pmod{2047}$
  $S_8 \equiv S_7^2 - 2 \equiv 240 \pmod{2047}$
  $S_9 \equiv S_8^2 - 2 \equiv 282 \pmod{2047}$
  $S_{10} \equiv S_9^2 - 2 \equiv 1736 \pmod{2047}$

  Άρα $S_{10} \not\equiv 0 \pmod{M_{11}}$ και επομένως ο $M_{11} = 2047$ δεν είναι πρώτος αριθμός.

- Για $p = 13$.
  Ο $M_{13} = 8191$ είναι πρώτος αριθμός. Πράγματι, :

  $S_1 \equiv 4 \pmod{8191}$
  $S_2 \equiv S_1^2 - 2 \equiv 14 \pmod{8191}$
  $S_3 \equiv S_2^2 - 2 \equiv 194 \pmod{8191}$
  $S_4 \equiv S_3^2 - 2 \equiv 4870 \pmod{8191}$
  $S_5 \equiv S_4^2 - 2 \equiv 3953 \pmod{8191}$

$S_6 \equiv S_5^2 - 2 \equiv 5970 \pmod{8191}$
$S_7 \equiv S_6^2 - 2 \equiv 1857 \pmod{8191}$
$S_8 \equiv S_7^2 - 2 \equiv 36 \pmod{8191}$
$S_9 \equiv S_8^2 - 2 \equiv 1294 \pmod{8191}$
$S_{10} \equiv S_9^2 - 2 \equiv 3470 \pmod{8191}$
$S_{11} \equiv S_{10}^2 - 2 \equiv 128 \pmod{8191}$
$S_{12} \equiv S_{11}^2 - 2 \equiv 0 \pmod{8191}$

Άρα $S_{12} \equiv 0 \pmod{M_{13}}$ και επομένως ο $M_{13} = 8191$ είναι πρώτος αριθμός.

Κεφάλαιο 3

Τρίγωνοι αριθμοί στις γενικευμένες ακολουθίες Lucas

3.1 Εισαγωγή

Ένας φυσικός αριθμός n ονομάζεται τρίγωνος αν και μόνο αν μπορεί να γραφεί στην μορφή $n = \frac{1}{2} \cdot k \cdot (k+1)$, όπου $k \in \mathbb{N}$. Θα αποδείξουμε ότι οι μόνο τρίγωνοι αριθμοί στην ακολουθία Fibonacci F_n είναι αυτοί με δείκτη $n = \pm 1, 2, 4, 8, 10$. Όταν θα γράφουμε ότι $x = \square$, θα εννοούμε ότι ο αριθμός x είναι τέλειο τετράγωνο ακεραίου.

ΘΕΩΡΗΜΑ 3.1.1: Ο αριθμός $8F_n + 1$ είναι $\square$ αν και μόνο αν $n = \pm 1, 0, 2, 4, 8, 10$.

ΘΕΩΡΗΜΑ 3.1.2: Ο όρος F_n είναι τρίγωνος αριθμός αν και μόνο αν $n = \pm 1, 2, 4, 8, 10$.

Οι αποδείξεις θα ακολουθήσουν έπειτα. Μια μικρή σκιαγράφηση αυτών λέει ότι αν ο αριθμός F_n είναι τρίγωνος τότε ο $8F_n + 1$ είναι $\square$ μεγαλύτερο του 1. Αυτό γιατί αν υποθέσουμε ότι ο F_n είναι τρίγωνος αριθμός, δηλαδή $F_n = \frac{m(m+1)}{2}$ για κάποιο $m \in \mathbb{N}$, τότε $8F_n + 1 = 8 \cdot \frac{m(m+1)}{2} + 1 = 4m(m+1) + 1 = 4m^2 + 4m + 1 = (2m+1)^2$. Οπότε αρκεί να βρούμε όλους τους φυσικούς αριθμούς n για τους οποίους ο $8F_n + 1$ είναι τέλειο τετράγωνο. Για να γίνει αυτό, θα πρέπει να βρούμε έναν ακέραιο w_n τέτοιον ώστε αν ο $8F_n + 1$ δεν είναι $\square$ τότε $\left(\frac{8F_n+1}{w_n}\right) = -1$. Αυτό προκύπτει άμεσα από την παρακάτω πρόταση.

ΠΡΟΤΑΣΗ 3.1.1: Αν για τον ακέραιο a ισχύει η ισοτιμία $x^2 \equiv a \pmod{p}$ για κάθε πρώτο $p \in \mathbb{P}$, τότε ο a είναι τέλειο τετράγωνο ακεραίου.

Απόδειξη. Θα αποδείξουμε ότι αν ο a δεν είναι τέλειο τετράγωνο ακεραίου, τότε $\exists p \in \mathbb{P}$ για τον οποίο ισχύει $\left(\frac{a}{p}\right) = -1$ και επομένως η ισοτιμία $x^2 \equiv a \pmod{p}$ δεν έχει λύση, που είναι άτοπο.
Λόγω της πολλαπλασιαστικότητας του συμβόλου Jacobi, αρκεί να αποδείξουμε ότι υπάρχει ένας περιττός φυσικός αριθμός l τέτοιος ώστε $\left(\frac{a}{l}\right) = -1$. Αφού υποθέσαμε ότι ο a δεν είναι τέλειο τετράγωνο ακεραίου, θα ισχύουν μια από τις παρακάτω τρεις δυνατότητες:

1. $a = -b^2, b \in \mathbb{Z}$. Τότε, αν $c \in \mathbb{Z}, c > 0$ με $c \equiv 3 \pmod{4}$ και Μ.Κ.Δ.$(b, c) = 1$ έχουμε:
$$\left(\frac{a}{c}\right) = \left(\frac{-b^2}{c}\right) = \left(\frac{-1}{c}\right) = (-1)^{\frac{c-1}{2}} = -1$$

2. $a = \pm 2^t \cdot b$, όπου $t, b \in \mathbb{Z}$ περιττοί, θετικοί ακέραιοι. Τότε, αφού Μ.Κ.Δ.$(b, 2) = 1$, έχουμε και ότι Μ.Κ.Δ.$(8, b) = 1$ και άρα το σύστημα

$$x \equiv 5 \pmod 8$$

$$x \equiv 1 \pmod b$$

έχει λύση και έστω η λύση αυτού να είναι ο $c \in \mathbb{Z}, c > 0$. Τότε:

$$\left(\frac{-1}{c}\right) = (-1)^{\frac{c-1}{2}} = 1, \quad \text{αφού} \quad c \equiv 5 \pmod 8$$

και άρα, αφού ο t είναι περιττός, έχουμε:

$$\left(\frac{2^t}{c}\right) = \left(\frac{-2^t}{c}\right) = \left(\frac{2}{c}\right) = (-1)^{\frac{c^2-1}{8}} = -1$$

αλλά και

$$\left(\frac{b}{c}\right) = \left(\frac{c}{b}\right) \cdot (-1)^{\frac{b-1}{2} \cdot \frac{c-1}{2}} = \left(\frac{c}{b}\right) = \left(\frac{1}{b}\right) = 1$$

Επομένως $\left(\frac{a}{c}\right) = -1$.

3. $a = \pm 2^{2s} \cdot q^t \cdot b$, όπου $b, t \in \mathbb{Z}$ περιττοί με Μ.Κ.Δ. $(q, b) = 1, q \in \mathbb{P}, q \neq 2$. Θεωρούμε το σύστημα

$$x \equiv 1 \pmod{4b}$$

$$x \equiv d \pmod q$$

όπου d κάποιος ακέραιος. Το σύστημα έχει λύση αφού ο $q \neq 2$ και αφού οι q, b είναι μεταξύ τους πρώτοι, τότε και Μ.Κ.Δ.$(4b, q) = 1$. Έστω $d > 0$ κάποιο μη τετραγωνικό υπόλοιπο $\pmod q$ και $l > 0$ λύση του παραπάνω συστήματος. Τότε:

$$\left(\frac{2^{2s}}{l}\right) = \left(\frac{-2^{2s}}{l}\right) = 1$$

και

$$\left(\frac{b}{l}\right) = \left(\frac{l}{b}\right) \cdot (-1)^{\frac{b-1}{2} \cdot \frac{l-1}{2}} = \left(\frac{l}{b}\right) = \left(\frac{1}{b}\right) = 1$$

Όμως,

$$\left(\frac{q^t}{l}\right) = \left(\frac{q}{l}\right) = \left(\frac{l}{q}\right) \cdot (-1)^{\frac{l-1}{2} \cdot \frac{q-1}{2}} = \left(\frac{l}{q}\right) = \left(\frac{d}{q}\right) = -1$$

Και άρα $\left(\frac{a}{c}\right) = -1$.

□

Όπως ορίστηκε στο κεφάλαιο 2, η ακολουθία $L_n, n \in \mathbb{Z}$ έχει αναδρομικό τύπο

$$L_{n+2} = L_{n+1} + L_n, L_0 = 2, L_1 = 1.$$

Υπενθυμίζουμε τις παρακάτω ταυτότητες:

1. $F_{-n} = (-1)^{n+1} F_n \quad L_{-n} = (-1)^n L_n$

2. $2F_{m+n} = F_m L_n + F_n L_m \quad 2L_{m+n} = 5F_m F_n + L_m L_n$

3. $F_{2n} = F_n L_n \quad L_{2n} = L_n^2 + 2(-1)^{n+1}$

4. $L_n^2 - 5F_n^2 = 4(-1)^n$

5. $F_{2kt+n} \equiv (-1)^t F_n \pmod{L_k}$, όπου $n, m, t \in \mathbb{Z}$ και $k \equiv \pm 2 \pmod 6$.

   Απόδειξη. Προσθαφαιρούμε k στον δείκτη και έχουμε $F_{2kt+n} = F_{[k(2t-1)+n]+k}$. Έτσι, αν θέσουμε $s = k$ και $l = k(2t-1)+n$ στην ταυτότητα $F_{l+s} = F_l L_s - (-1)^s F_{l-s}$, προκύπτει:

   $$F_{2kt+n} \equiv -(-1)^k F_{[k(2t-1)+n]-k} \pmod{L_k}$$

   κι αφού $k \equiv \pm 2 \pmod 6$, άρα ο k είναι άρτιος, έχουμε

   $$F_{2kt+n} \equiv -F_{[k(2t-1)+n]-k} \pmod{L_k}$$

   Επαναλαμβάνουμε τη διαδικασία αυτή για τον $F_{[k(2t-1)+n]-k}$ και προκύπτει ότι

   $$F_{[k(2t-1)+n]-k} \equiv -(-1)^k F_{[k(2t-2)+n]-k} \equiv F_{[k(2t-2)+n]-k} \pmod{L_k}$$

   Παρατηρούμε ότι τα πρόσημα πηγαίνουν εναλλάξ και ότι σε άρτιο πλήθος βημάτων έχουμε θετικό πρόσημο, άρα μετά από $t-2$ βήματα ακόμα θα έχουμε το ζητούμενο, δηλαδή

   $$F_{2kt+n} \equiv (-1)^t F_n \pmod{L_k}.$$

   □

Επιπλέον, τα ζευγάρια $(x, y) = (F_n, L_n)$ είναι οι ακέραιες λύσεις της εξίσωσης $5X^2 - Y^2 = \pm 4$. Άρα, αν ο F_n είναι τρίγωνος αριθμός, δηλαδή $F_n = \frac{m(m+1)}{2}$ για κάποιο $m \in \mathbb{N}$, η εξίσωση μετασχηματίζεται ως εξής:

$$5 \cdot \frac{m^2(m+1)^2}{4} - Y^2 = \pm 4 \quad \text{ή ισοδύναμα} \quad 4Y^2 = 5m^4 + 10m^3 + 5m^2 \mp 16.$$

Το να βρούμε, δηλαδή, όλους τους τρίγωνους αριθμούς στην ακολουθία Fibonacci, ισοδυναμεί με το να βρούμε όλα τα ακέραια σημεία των δύο παραπάνω καμπυλών.

3.2 Κριτήριο με χρήση του συμβόλου Jacobi

Κριτήριο 3.2.1: Αν $a, n \in \mathbb{N}$ τέτοιοι ώστε $n \equiv \pm 2 \pmod 6$ και Μ.Κ.Δ.$(a, L_n) = 1$, τότε

$$\left(\frac{\pm 4aF_{2n} + 1}{L_{2n}}\right) = -\left(\frac{8aF_n \pm L_n}{64a^2 + 5}\right)$$

όταν τα σύμβολα Jacobi ορίζονται.

Απόδειξη. Αφού $n \equiv \pm 2 \pmod 6$ έχουμε $L_n \equiv 3 \pmod 4$. Αυτό το δείχνουμε με χρήση της μαθηματικής επαγωγής, δηλαδή, αφού $n \equiv 2 \pmod 6$, έχουμε ότι $n = 6k+2, k \in \mathbb{N}$

- Για $k = 0$, ο $n = 2$ άρα $L_2 = 3 \equiv 3 \pmod 4$, επομένως ισχύει.

- Έστω ότι ισχύει για $k = l$, δηλαδή $L_{6l+2} \equiv 3 \pmod 4$.
- Εξετάζουμε αν ισχύει για $k = l + 1$:
  $L_{6(l+1)+2} = L_{(6l+2)+6} \overset{(2)}{=} \frac{1}{2}\cdot 5\cdot F_6\cdot F_{6l+2}+\frac{1}{2}\cdot L_6\cdot L_{6l+2} = \frac{1}{2}\cdot 5\cdot 8\cdot F_{6l+2}+\frac{1}{2}\cdot 18\cdot L_{6l+2} = 20F_{6l+2}+9L_{6l+2} \equiv 0\cdot F_{6l+2}+1\cdot L_{6l+2} \equiv L_{6l+2} \equiv 3 \pmod 4$, λόγω της επαγωγικής υπόθεσης.

Άρα αν $n \equiv 2 \pmod 6$, έχουμε ότι $L_n \equiv 3 \pmod 4$. Αν $n \equiv -2 \pmod 6$ τότε $-n \equiv 2 \pmod 6$ κι από την ταυτότητα 1. έχουμε $L_{-n} = (-1)^n L_n = (-1)^{6z+2} L_n, \quad$ για κάποιο $\quad z \in \mathbb{Z}$ και άρα $L_{-n} = L_n \equiv 3 \pmod 4$, αφού $-n \equiv 2 \pmod 6$.

Ομοίως, αφού $2n \equiv \pm 4 \pmod{12}$ έχουμε $L_{2n} \equiv 7 \pmod 8$. Αποδεικνύουμε πάλι πρώτα την περίπτωση όπου $2n \equiv 4 \pmod{12}$, δηλαδή $n = 12k + 4$ για κάποιο $k \in \mathbb{N}$.

- Αν $k = 0$, τότε $L_n = L_4 = 7 \equiv 7 \pmod 8$, επομένως ισχύει για $k = 0$.
- Έστω ότι ισχύει για $k = l$, δηλαδή $L_{12l+1} \equiv 7 \pmod 8$.
- Εξετάζουμε για $k = l + 1$:
  $L_{12(l+1)+4} = L_{(12l+4)+12} \overset{(2)}{=} \frac{1}{2}\cdot 5\cdot F_{12}\cdot F_{12l+4}+\frac{1}{2}\cdot L_{12}\cdot L_{12l+4} = \frac{1}{2}\cdot 5\cdot 144\cdot F_{12l+4}+\frac{1}{2}\cdot 322\cdot L_{12l+4} = 5\cdot 72\cdot F_{12l+4}+161\cdot L_{12l+4} \equiv 0\cdot F_{12l+4}+L_{12l+4} \equiv L_{12l+4} \equiv 7 \pmod 8$, λόγω της επαγωγικής υπόθεσης.

Άρα, αν $2n \equiv 4 \pmod{12}$, έχουμε $L_{2n} \equiv 7 \pmod 8$.
Αν $2n \equiv -4 \pmod{12}$, τότε $-2n \equiv 4 \pmod{12}$ και άρα με χρήση της ταυτότητας 1., έχουμε ότι $L_{-2n} = (-1)^{2n}\cdot L_{2n} \equiv 7 \pmod 8$.
Έτσι:

$$\left(\frac{2}{L_{2n}}\right) = (-1)^{\frac{L_{2n}^2-1}{8}} = 1.$$

Επομένως

$$\left(\frac{\pm 4aF_{2n}+1}{L_{2n}}\right) = \left(\frac{2}{L_{2n}}\right)\cdot\left(\frac{\pm 4aF_{2n}+1}{L_{2n}}\right) = \left(\frac{\pm 8aF_{2n}+2}{L_{2n}}\right) = \left(\frac{\pm 8aF_nL_n+L_n^2}{L_{2n}}\right)$$

όπου η τελευταία ισότητα προκύπτει από την ταυτότητα 3. Εφαρμόζουμε τον τετραγωνικό νόμο αντιστροφής, έχουμε

$$\left(\frac{\pm 8aF_nL_n+L_n^2}{L_{2n}}\right) = \left(\frac{L_{2n}}{8aF_nL_n \pm L_n^2}\right)\cdot(-1)^{\frac{8aF_nL_n\pm L_n^2-1}{2}\cdot\frac{L_{2n}-1}{2}}$$

κι αφού $L_n \equiv 3 \pmod 4$, έχουμε ότι ο αριθμός $\frac{8aF_nL_n\pm L_n^2-1}{2}$ είναι άρτιος, άρα το τελευταίο είναι ίσο με

$$\left(\frac{L_{2n}}{8aF_nL_n \pm L_n^2}\right) = \left(\frac{L_{2n}}{L_n}\right)\left(\frac{L_{2n}}{8aF_n \pm L_n}\right)$$

Από τις ταυτότητες 2. και 3.το τελευταίο σύμβολο του Jacobi ισούται με:

$$\left(\frac{L_n^2-2}{L_n}\right)\cdot\left(\frac{\frac{1}{2}(5F_n^2+L_n^2)}{8aF_n \pm L_n}\right) = \left(\frac{-1}{L_n}\right)\cdot\left(\frac{2}{L_n}\right)\cdot\left(\frac{\frac{1}{2}(5F_n^2+L_n^2)}{8aF_n \pm L_n}\right) =$$

$$= (-1)^{\frac{L_n-1}{2}}\cdot\left(\frac{2}{L_n}\right)\cdot\left(\frac{\frac{1}{2}(5F_n^2+L_n^2)}{8aF_n \pm L_n}\right)$$

Καθώς $16a^2 = (4a)^2$, το $\left(\frac{16a}{8aF_n \pm L_n}\right) = 1$ και άρα μπορούμε να πολλαπλασιάσουμε με $\left(\frac{16a^2}{8aF_n \pm L_n}\right)$ χωρίς να αλλάξει πρόσημο η παράσταση. Έτσι,

$$(-1)^{\frac{L_n-1}{2}} \cdot \left(\frac{2}{L_n}\right) \cdot \left(\frac{\frac{1}{2}(5F_n^2 + L_n^2)}{8aF_n \pm L_n}\right) = -\left(\frac{2}{L_n}\right) \cdot \left(\frac{a}{8aF_n \pm L_n}\right) \cdot \left(\frac{40aF_n^2 + 8aL_n^2}{8aF_n \pm L_n}\right) =$$

$$= -\left(\frac{2}{L_n}\right) \cdot \left(\frac{a}{8aF_n \pm L_n}\right) \cdot \left(\frac{\pm(64a^2+5)F_nL_n}{8aF_n \pm L_n}\right) =$$

$$= -\left(\frac{2}{L_n}\right) \cdot \left(\frac{a}{8aF_n \pm L_n}\right) \cdot \left(\frac{\pm(64a^2+5)}{8aF_n \pm L_n}\right)\left(\frac{F_nL_n}{8aF_n \pm L_n}\right) =$$

$$= \pm\left(\frac{2}{L_n}\right) \cdot \left(\frac{a}{8aF_n \pm L_n}\right) \cdot \left(\frac{8aF_n \pm L_n}{\pm(64a^2+5)}\right) \cdot \left(\frac{F_nL_n}{8aF_n \pm L_n}\right)$$

- Αν $F_n \equiv 1 \pmod 4$, τότε

$$\left(\frac{F_n}{8aF_n \pm L_n}\right) = \left(\frac{8aF_n \pm L_n}{F_n}\right) \cdot (-1)^{\frac{F_n-1}{2} \cdot \frac{8aF_n \pm L_n - 1}{2}} = \left(\frac{\pm L_n}{F_n}\right)$$

  Όμως, $\left(\frac{-1}{F_n}\right) = (-1)^{\frac{F_n-1}{2}} = 1$, άρα

$$\left(\frac{\pm L_n}{F_n}\right) = \left(\frac{L_n}{F_n}\right) = \left(\frac{F_n}{L_n}\right) \cdot (-1)^{\frac{F_n-1}{1} \cdot \frac{L_n-1}{2}} = \left(\frac{F_n}{L_n}\right)$$

- Αν $F_n \equiv 3 \pmod 4$, τότε

$$\left(\frac{F_n}{8aF_n \pm L_n}\right) = \mp\left(\frac{8aF_n \pm L_n}{F_n}\right) = -\left(\frac{\pm L_n}{F_n}\right) = -\left(\frac{F_n}{L_n}\right) \cdot (-1)^{\frac{F_n-1}{2} \cdot \frac{L_n-1}{2}} = \left(\frac{F_n}{L_n}\right)$$

  Άρα σε κάθε περίπτωση έχουμε $\left(\frac{F_n}{8aF_n \pm L_n}\right) = \left(\frac{F_n}{L_n}\right)$.

Αφού $\left(\frac{L_n}{8aF_n \pm L_n}\right) = \mp\left(\frac{8aF_n \pm L_n}{L_n}\right) = \pm\left(\frac{2a}{L_n}\right) \cdot \left(\frac{F_n}{L_n}\right)$, έχουμε:

$$\left(\frac{\pm 4aF_{2n} + 1}{L_{2n}}\right) = -\left(\frac{a}{L_n}\right) \cdot \left(\frac{a}{8aF_n \pm L_n}\right) \cdot \left(\frac{8aF_n \pm L_n}{64a^2+5}\right) = -\left(\frac{a}{8aF_{2n} \pm L_n^2}\right) \cdot \left(\frac{8aF_n \pm L_n}{64a^2+5}\right)$$

Θέτουμε $a = 2^s \cdot b, s \geq 0, 2 \not| b$.

- Αν $b \equiv 1 \pmod 4$ και s άρτιος:

$$\left(\frac{a}{8aF_{2n} \pm L_n^2}\right) = \left(\frac{2^s \cdot b}{8aF_{2n} \pm L_n^2}\right) = \left(\frac{2^s}{8aF_{2n} \pm L_n^2}\right) \cdot \left(\frac{b}{8aF_{2n} \pm L_n^2}\right) =$$

$$\left(\frac{2}{8aF_{2n} \pm L_n^2}\right)^s \cdot \left(\frac{b}{8aF_{2n} \pm L_n^2}\right) = \left(\frac{b}{8aF_{2n} \pm L_n^2}\right) =$$

$$\left(\frac{8aF_{2n} \pm L_n^2}{b}\right) \cdot (-1)^{\frac{b-1}{2}\frac{8aF_{2n} \pm L_n^2}{2}} = \left(\frac{8aF_{2n} \pm L_n^2}{b}\right)$$

  κι αφού $b|a$ έχουμε τελικά:

$$\left(\frac{a}{8aF_{2n} \pm L_n^2}\right) = \left(\frac{\pm L_n^2}{b}\right) = \left(\frac{\pm L_n}{b}\right)^2 = 1$$

- Αν $b \equiv 1 \pmod 4$ και s περιττος:
  Τότε $8aF_{2n} \pm L_n^2 \equiv \pm 1 \pmod 8$ και άρα:

$$\left(\frac{a}{8aF_{2n} \pm L_n^2}\right) = \left(\frac{2^s \cdot b}{8aF_{2n} \pm L_n^2}\right) = \left(\frac{2^s}{8aF_{2n} \pm L_n^2}\right) \cdot \left(\frac{b}{8aF_{2n} \pm L_n^2}\right) =$$

$$= \left(\frac{2}{8aF_{2n} \pm L_n^2}\right)^s \cdot \left(\frac{b}{8aF_{2n} \pm L_n^2}\right) = \left(\frac{2}{8aF_{2n} \pm L_n^2}\right) \cdot \left(\frac{b}{8aF_{2n} \pm L_n^2}\right) =$$

$$= (-1)^{\frac{(8aF_{2n} \pm L_n^2)^2 - 1}{8}} = \left(\frac{b}{8aF_{2n} \pm L_n^2}\right) = \left(\frac{8aF_{2n} \pm L_n^2}{b}\right) \cdot (-1)^{\frac{b-1}{2}\frac{8aF_{2n} \pm L_n^2}{2}} = \left(\frac{8aF_{2n} \pm L_n^2}{b}\right)$$

  κι αφού $b|a$ έχουμε τελικά:

$$\left(\frac{a}{8aF_{2n} \pm L_n^2}\right) = \left(\frac{\pm L_n^2}{b}\right) = \left(\frac{\pm L_n}{b}\right)^2 = 1$$

- Αν $b \equiv 3 \pmod 4$, ομοίως με πριν:

$$\left(\frac{a}{8aF_{2n} \pm L_n^2}\right) = \left(\frac{b}{8aF_{2n} \pm L_n^2}\right) = \pm\left(\frac{8aF_{2n} \pm L_n^2}{b}\right) = \pm\left(\frac{\pm L_n^2}{b}\right) = 1$$

Άρα τελικά:

$$\left(\frac{\pm 4aF_{2n} + 1}{L_{2n}}\right) = -\left(\frac{8aF_n \pm L_n}{64a^2 + 5}\right)$$

□

3.3 Τρίγωνοι αριθμοί στην ακολουθία Fibonacci

Πριν την απόδειξη των δύο θεωρημάτων της εισαγωγής θα μελετήσουμε μερικές συνέπειες του Κριτηρίου με χρήση του συμβόλου Jacobi.

ΛΗΜΜΑ 3.3.1: Αν $n \equiv \pm 1 \pmod{2^5 \cdot 5}$, τότε ο $8F_n + 1 = \square$ μόνο για $n = \pm 1$.

Απόδειξη. Θεωρούμε την περίπτωση $n \equiv 1 \pmod{2^5 \cdot 5}$ και $n \neq 1$. Τότε θέτουμε $n = sgn(n-1) \cdot 3^r \cdot 2 \cdot 5m + 1$, όπου με $sgn(n-1)$ συμβολίζουμε το πρόσημο του $n-1, r \geq 0, \quad 3 \not| m, m > 0$. Επίσης ισχύει $m \equiv \pm 16 \pmod{48}$, αφού $2^4 = 16 | m, 16 | 48$ άρα $m \equiv 0$ ή 16 ή $32 \pmod{48}$. Αν $m \equiv 0 \pmod{48}$, επειδή $3|48$, θα είχαμε $3|m$, άτοπο. Άρα $m \equiv \pm 16 \pmod{48}$.
Ξεχωρίζουμε δύο περιπτώσεις:

- Αν $g = sgn(n-1) \cdot 3^r \equiv 1 \pmod 4$. Τότε θέτουμε $k = 5m$ αν $m \equiv 16 \pmod{48}$ ή $k = m$ αν $m \equiv 32 \pmod{48}$. Έτσι, έχουμε σε κάθε περίπτωση $k \equiv 32 \pmod{48}$.

  – Αν $k = 5m$.
    Τότε $n = g \cdot 2k + 1 = g \cdot 2k - 2k + 2k + 1 = 2k(g-1) + 2k + 1$.
    Η σχέση $F_{2lt+s} \equiv (-1)^t F_s \pmod{L_l}$, για $l = 2k, t = \frac{g-1}{2}$ και για $s = 2k+1$ γράφεται:

$$F_n = (-1)^{\frac{g-1}{2}} F_{2k+1} \pmod{L_{2k}}.$$

    Τώρα, επειδή $g \equiv 1 \pmod 4$, έχουμε ότι ο $\frac{g-1}{2}$ είναι άρτιος, δηλαδή

$$F_n \equiv F_{2k+1} \pmod{L_{2k}}$$

– Αν $k = m$.
Τότε $n = 5g \cdot 2k + 1 = 5g \cdot 2k + 1 + 2k - 2k = 2k(5g - 1) + 2k + 1$.
Η σχέση $F_{2lt+s} \equiv (-1)^t F_s \pmod{L_l}$, για $l = 2k$, $t = 5g$ και $s = 2k + 1$, γράφεται:

$$F_n \equiv (-1)^{\frac{5g-1}{2}} F_{2k+1}$$

Τώρα, επειδή $5g \equiv 1 \pmod 4$, έχουμε ότι ο $\frac{5g-1}{2}$ είναι άρτιος και άρα

$$F_n \equiv F_{2k+1} \pmod{L_{2k}}$$

Με χρήση της ταυτότητας 2. έχουμε:

$$8F_n + 1 \equiv 8F_{2k+1} + 1 \equiv 4 \cdot 2F_{2k+1} + 1 \equiv 4(F_{2k}L_1 + F_1 L_{2k}) + 1 \equiv 4F_{2k} + 4L_{2k} + 1$$

$$\equiv 4F_{2k} + 1 \pmod{L_{2k}}$$

Επομένως,

$$\left(\frac{8F_n + 1}{L_{2k}}\right) = \left(\frac{4F_{2k} + 1}{L_{2k}}\right) = -\left(\frac{8F_k + L_k}{69}\right)$$

όπου η τελευταία ισότητα προκύπτει από το κριτήριο για $a = 1$.

Η ακολουθία $\{8F_n + L_n\}_{n\in\mathbb{N}}$ είναι περιοδική $\pmod{69}$ με περίοδο 48 [1], δηλαδή $\forall k \in \mathbb{N}$ ισχύει $8F_{k+48} + L_{k+48} \equiv 8F_k + L_k \pmod{69}$ κι αφού $k \equiv 32 \pmod{48}$ έχουμε:

$$\left(\frac{8F_n + 1}{L_{2k}}\right) = \left(\frac{8F_k + L_k}{69}\right) = -\left(\frac{8F_{32} + L_{32}}{69}\right) = -\left(\frac{38}{69}\right) = -1$$

άρα $8F_n + 1 \neq \square$.

- Αν $g = sgn(n-1) \cdot 3^r \equiv 3 \pmod 4$.
Σ'αυτή την περίπτωση θέτουμε $k = m$ αν $m \equiv 16 \pmod{48}$ ή $k = 5m$ αν $m \equiv 32 \pmod{48}$. Έτσι, σε κάθε περίπτωση έχουμε $k \equiv 16 \pmod{48}$. Ομοίως, με χρήση των ταυτοτήτων 5. και 2. προκύπτει

$$\left(\frac{8F_n + 1}{L_{2k}}\right) = \left(\frac{-4F_{2k} + 1}{L_{2k}}\right) = -\left(\frac{8F_k - L_k}{69}\right)$$

Η ακολουθία $\{8F_n - L_n\}_{n\in\mathbb{N}}$ είναι περιοδική $\pmod{69}$ με περίοδο 48 κι αφού $k \equiv 16 \pmod{48}$ έχουμε $8F_k - L_k \equiv 8F_{16} - L_{16} \equiv 31 \pmod{69}$, άρα

$$\left(\frac{8F_n + 1}{L_{2k}}\right) = -\left(\frac{31}{69}\right) = -1$$

απ'όπου προκύπτει ότι και σε αυτή τη περίπτωση ο $8F_n + 1$ δεν είναι τέλειο τετράγωνο

[1] Γνωρίζουμε από το Κεφάλαιο 2 ότι η ακολουθίες των Fibonacci και Lucas είναι περιοδικές modulo κάποιον ακέραιο. Οι περίοδοι των ακολουθιών αυτών υπολογίστηκαν στο Sage και ο κώδικας του προγράμματος παρατίθεται στο παράρτημα αυτού του κεφαλαίου.

Αν $n \equiv -1 \pmod{2^5 \cdot 5}$ και $n \neq -1$, τότε από την (1) έχουμε ότι: $8F_n + 1 = 8F_{-n}(-1)^{n+1} + 1$. Όμως $n + 1 \equiv 0 \pmod{2^5 \cdot 5}$, άρα $2|n+1$, άρα $n+1$ άρτιος κι επομένως $8F_{-n} + 1 = 8F_n + 1$. Αφού $-n \equiv 1 \pmod{2^5 \cdot 5}$ και $-n \neq 1$, από το προηγούμενο επιχείρημα ο $8F_n + 1 \neq \square$.
Τέλος, αν $n = 1$ έχουμε $8F_n + 1 = 8F_1 + 1 = 8 + 1 = 9 = 3^2$, ενώ για $n = -1, 8F_n = 1 = 8F_{-1} + 1 = 8 + 1 = 9 = 3^2$, που ολοκληρώνει την απόδειξη. $\square$

ΛΗΜΜΑ 3.3.2: Αν $n \equiv 0 \pmod{2^2 \cdot 5^2}$, τότε ο $8F_n + 1$ είναι τέλειο τετράγωνο μόνο για $n = 0$.

Απόδειξη. Αν $n > 0$, θέτουμε $n = 2 \cdot 5^2 \cdot 2^s \cdot l, 2 \not| l, s \geq 1$ και ορίζουμε

$$k = \begin{cases} 2^s & \text{αν} \quad s \equiv 0 \pmod 3 \\ 5^2 \cdot 2^s & \text{αν} \quad s \equiv 1 \pmod 3 \\ 5 \cdot 2^s & \text{αν} \quad s \equiv 2 \pmod 3 \end{cases}$$

Έτσι $k \equiv \pm 6 \pmod{14}$, το οποίο το δείχνουμε επαγωγικά. Δηλαδή,

- Αν $s \equiv 0 \pmod 3$.
  Τότε $s = 3z, z \in \mathbb{N}$ και $k = 2^s = 2^{3z} = 8^z$.
  Για $z = 1 : k = 8 \equiv -6 \pmod{14}$.
  Έστω ότι ισχύει για $z = l, l \in \mathbb{N}$, δηλαδή $8^l \equiv \pm 6 \pmod{14}$.
  Εξετάζουμε για $z = l + 1$
  - Αν $8^l \equiv 6 \pmod{14}$, τότε $k = 8^{l+1} = 8^l \cdot 8 \equiv 6 \cdot 8 \equiv 48 \equiv 6 \pmod{14}$.
  - Αν $8^l \equiv -6 \pmod{14}$, τότε $k = 8^{l+1} = 8^l \cdot 8 \equiv (-6) \cdot 8 \equiv -48 \equiv -6 \pmod{14}$.

- Αν $s \equiv 1 \pmod 3$.
  Τότε $s = 3z + 1$ με $z \in \mathbb{N}$ και $k = 2^s \cdot 5^2 = 50 \cdot 8^z$.
  Για $z = 1 : k = 50 \cdot 8 \equiv 8 \cdot 8 \equiv 64 \equiv -6 \pmod{14}$.
  Έστω ότι ισχύει για $z = l, l \in \mathbb{N}$, δηλαδή $k = 50^l \cdot 8 \equiv \pm 6 \mod 14$.
  Εξετάζουμε για $z = l + 1$
  -Αν $50^l \cdot 8 \equiv 6 \pmod{14}$, τότε $k = 50 \cdot 8^{l+1} \equiv 50 \cdot 8^l \cdot 8 \equiv 6 \cdot 8 \equiv 48 \equiv 6 \pmod{14}$.
  - Αν $50 \cdot 8^l \equiv -6 \pmod{14}$, τότε $k = 50 \cdot 8^{l+1} \equiv 50 \cdot 8^l \cdot 8 \equiv (-6) \cdot 8 \equiv -48 \equiv -6 \pmod{14}$.

- $s \equiv 2 \pmod 3$.
  Τότε $s = 3z + 2, z \in \mathbb{N}$ και $k = 5 \cdot 2^s = 20 \cdot 8^z$.
  Για $z = 1 : k = 20 \cdot 8 \equiv 48\ 6 \pmod{14}$.
  Έστω ότι ισχύει για $z = l$, δηλαδή $20 \cdot 8^l \equiv \pm 6 \pmod{14}$.
  Εξετάζουμε για $z = l + 1$
  -Αν $20 \cdot 8^l \equiv 6 \pmod{14}$, τότε $k = 20 \cdot 8^{l+1} \equiv 20 \cdot 8^l \cdot 8 \equiv 6 \cdot 8 \equiv 6 \pmod{14}$.
  -An $20 \cdot 8^l \equiv -6 \pmod{14}$, τότε $k = 20 \cdot 8^{l+1} \equiv 20 \cdot 8^l \cdot 8 \equiv (-6.8 \equiv -48 \equiv -6 \pmod{14}$.

Αφού $k \equiv \pm 6 \pmod{14}$, έχουμε ότι Μ.Κ.Δ.$(2, L_k) = 1$. Ακόμα, αφού $2|k$, έχουμε ότι $k \equiv 0$ ή 2 ή $4 \pmod 6$. Όμως, αν $k = 0 \pmod 6$, αφού $3|6$, θα είχαμε $3|k$ που είναι άτοπο εξ ορισμού του k, επομένως $k \equiv \pm 2 \pmod 6$.
Εφαρμόζοντας την (5) (για κάθε επιλογή του k) και το κριτήριο για $a = 2$, προκύπτει ότι:

$$\left(\frac{8F_n + 1}{L_{2k}}\right) = \left(\frac{\pm 8 \cdot F_{2k} + 1}{L_{2k}}\right) = -\left(\frac{16F_k \pm L_k}{261}\right) = -\left(\frac{16F_k \pm L_k}{9 \cdot 29}\right) = -\left(\frac{16F_k \pm L_k}{29}\right)$$

Ισχυριζόμαστε ότι η τελευταία ισότητα ισχύει γιατί Μ.Κ.Δ.$(16F_K + L_k, 3) = 1$ για κάθε άρτιο $k \in \mathbb{N}$.
Οι ακολουθίες $\{16F_n \pm L_n\}_{n\in\mathbb{N}}$ είναι και οι δύο περιοδικές $\pmod{29}$ με περίοδο 14, δηλαδή $\forall n \in \mathbb{N}$ ισχύει $16F_{n+14} \pm L_{n+14} \equiv 16F_n \pm L_n \pmod{29}$.

- Αν $k \equiv 6 \pmod{14}$, τότε $16F_k + L_k \equiv 16F_6 + L_6 \equiv 146 \equiv 1 \pmod{29}$, ενώ $16F_k - L_k \equiv 16F_6 - L_6 \equiv 110 \equiv -6 \pmod{29}$.
- Αν $k \equiv -6 \pmod{14}$, τότε, $16F_k + L_k \equiv 16F_8 + L_8 \equiv 383 \equiv 6 \pmod{29}$, ενώ $16F_k - L_k \equiv 16F_8 - L_8 \equiv 289 \equiv 28 \equiv -1 \pmod{29}$.

Επειδή $(\frac{\pm 1}{29}) = (\frac{\pm 6}{29}) = 1$, έχουμε τελικά ότι

$$\left(\frac{8F_n + 1}{L_{2k}}\right) = -\left(\frac{16F_k \pm L_k}{29}\right) = -1$$

και άρα ο $8F_n + 1$ δεν είναι τέλειο τετράγωνο.
Μένει μόνο να αποδείξουμε τον ισχυρισμό

$$\text{"Για κάθε άρτιο} \quad k \in \mathbb{N} \quad \text{ισχύει ότι Μ.Κ.Δ.}(16F_k + L_k, 3) = 1\text{"}$$

Αφού k άρτιος έχουμε ότι $k \equiv 0, 2, 4, 6 \pmod{8}$.
Αρκεί, αφού ο 3 είναι πρώτος αριθμός, $16F_k + L_k \not\equiv 0 \pmod{3}$
(ομοίως $16F_k - L_k \not\equiv 0 \pmod{3}$).

(i) Αν $k \equiv 0 \pmod{8}$, τότε $F_k \equiv 0 \pmod{3}$ και $L_k \equiv 2 \pmod{3}$, επομένως $16F_k + L_k \equiv 2 \pmod{3}$.

(ii) Αν $k \equiv 2 \pmod{8}$, τότε $F_k \equiv 1 \pmod{3}$ και $L_k \equiv 0 \pmod{3}$, επομένως $16F_k + L_k \equiv 1 \pmod{3}$.

(iii) Αν $k \equiv 4 \pmod{8}$, τότε $F_k \equiv 0 \pmod{3}$ και $L_k \equiv 1 \pmod{3}$, επομένως $16F_k + L_k \equiv 1 \pmod{3}$.

(iv) Αν $k \equiv 6 \pmod{8}$, τότε $F_k \equiv 2 \pmod{3}$ και $L_k \equiv 0 \pmod{3}$, επομένως $16F_k + L_k \equiv 2 \pmod{3}$.

Πράγματι, για το (i), αφού $k \equiv 0 \pmod{8}$, έχουμε ότι $k = 8l, l \in \mathbb{N}$.
Για $l = 0$, έχουμε $k = 0$ και άρα $F_0 = 0 \equiv 0 \pmod{3}$.
Υποθέτουμε ότι ισχύει για $l = m, m \in \mathbb{N}$, δηλαδή $F_{8m} \equiv 0 \pmod{3}$.
Εξετάζουμε για $l = m + 1$:
Από την ταυτότητα 6. των ακολουθιών F_n και L_n της σελίδας 30, έχουμε:

$$2F_{8(m+1)} = 2F_{8m+8} = L_8F_{8m} + F_8L_{8m} = 47 \cdot F_{8m} + 21 \cdot L_{8m} \equiv$$

$$2 \cdot F_{8m} \equiv 0 \pmod{3}$$

άρα $\forall k \equiv 0 \pmod{8}$ ισχύει $F_k \equiv 0 \pmod{3}$.
Ακόμα, για $l = 0$ έχουμε $k = 0$ και άρα $L_0 = 2 \equiv 2 \pmod{3}$.
Υποθέτουμε ότι ισχύει για $l = m, m \in \mathbb{N}$, δηλαδή $L_{8m} \equiv 2 \pmod{3}$.
Εξετάζουμε αν ισχύει για $l = m + 1$:
Από την ταυτότητα 7. των ακολουθιών F_n και L_n της σελίδας 30, έχουμε:

$$2L_{8(m+1)} = 2L_{8m+8} = L_8 \cdot L_{8m} + 5 \cdot F_8 \cdot F_{8m} = 47 \cdot L_{8m} + 5 \cdot 21 \cdot F_{8m} \equiv$$

$$2 \cdot L_{8m} \equiv 1 \pmod 3$$

άρα $\forall k \equiv 0 \pmod 8$ έχουμε $L_k \equiv 2 \pmod 3$.
Τα (ii), (iii), (iv) ομοίως.
Για να ολοκληρωθεί η απόδειξη, αν $n = 0$ έχουμε $8F_n + 1 = 8F_0 + 1 = 9 = 3^2$.

□

ΛΗΜΜΑ 3.3.3: Αν $n \equiv 2 \pmod{2^5 \cdot 5^2}$, τότε ο $8F_n + 1 = \square$ μόνο για $n = 2$.

Απόδειξη. Αν $n > 2$, θέτουμε $n = 3^r \cdot 2 \cdot 5^2 \cdot l + 2$ με $3 \nmid l, l > 0$ και $l \equiv \pm 16 \pmod{48}$, όπως στο λήμμα 1. Θέτουμε $k = l$ ή $k = 5l$ ή $k = 5^2 \cdot l$, το οποίο θα καθοριστεί αργότερα. Αφού $4|k$, προκύπτει ότι Μ.Κ.Δ.$(3, L_k) = 1$. Πράγματι, αφού $4|k$, έχουμε ότι $k = 4z, z \in \mathbb{Z}$. Από την (1), $L_{4z} = L_{2z}^2 + 2 \cdot (-1)^{2z+1} = L_{2z}^2 - 2$. Αν $3|L_{4k}$, θα είχαμε ότι η κλάση του 2 θα ήταν τετραγωνικό ισοϋπόλοιπο $\pmod 3$. Όμως, $\left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$, άτοπο, κι αφού $3 \in \mathbb{P}$, έχουμε ότι Μ.Κ.Δ.$(3, L_k) = 1$. Ακόμα, $k \equiv 0$ ή 2 ή $4 \pmod 6$ γιατί $4 = 2^2 | k$, άρα $k \equiv 0$ ή 2 ή $2^2 \pmod 6$. Αν $k \equiv 0 \pmod 6$, αφού $3|6$, θα είχαμε ότι $3|k$ και άρα $3|l$, άτοπο.
Επομένως με χρήση πάλι της 5. (για κάθε περίπτωση του k), προκύπτει:

$$8F_n + 1 \equiv 8F_{2k+2} + 1 \equiv \pm 12F_{2k} + 1 \equiv \pm 4 \cdot 2F_{2k+2} + 1 \equiv \pm 4(F_{2k}L_2 + F_2L_{2k})$$

$\equiv \pm 12F_{2k} + 1 \pmod{L_{2k}}$ και επομένως

$$\left(\frac{8F_n + 1}{L_{2k}}\right) = \left(\frac{\pm 12F_{2k} + 1}{L_{2k}}\right) = \left(\frac{\pm 4 \cdot 3F_{2k} + 1}{L_{2k}}\right) = -\left(\frac{24F_k \pm L_k}{581}\right)$$

όπου η τελευτάια ισότητα προκύπτει από το κριτήριο για $a = 3$.
Οι ακολουθίες $\{24F_m \pm L_m\}_{m \in \mathbb{N}}$ είναι περιοδικές $\pmod{581}$ και μάλιστα έχουν και οι δύο την περίοδο που είναι 336.
Ισχύει ο ακόλουθος πίνακας:

$n \pmod{336}$	80	112	128	208	224	256
$24F_n + L_n \pmod{581}$	65	401	436	359	261	170
$24F_n - L_n \pmod{581}$	411	320	222	145	180	516

Με απλούς υπολογισμούς μπορούμε να δείξουμε ότι για κάθε κλάση $x \pmod{581}$ της δεύτερης και τρίτης γραμμής ισχύει $(\frac{x}{581}) = 1$ και άρα

$$\left(\frac{24F_n \pm L_n}{581}\right) = 1, \forall n \equiv 80, 112, 128, 208, 224, 256 \pmod{336}$$

Αφού $336 = 48 \cdot 7$ κι αφού $l \equiv \pm 16 \pmod{48}$, έχουμε ότι $l \equiv 16, 32, 64, 80, 112, 128, 160, 176, 208, 224, 256, 272, 304, 320 \pmod{336}$.
Επιλέγουμε, λοιπόν, το k ως εξής:

$$k = \begin{cases} l & \text{αν} \quad l \equiv 80, 112, 128, 208, 224, 256 \pmod{336} \\ 5 \cdot l & \text{αν} \quad l \equiv 16, 160, 176, 320 \pmod{336} \\ 5^2 \cdot l & \text{αν} \quad l \equiv 32, 64, 272, 304 \pmod{336} \end{cases}$$

Έτσι, $k \equiv 80, 112, 128, 208, 224, 256 \pmod{336}$ κι επομένως

$$\left(\frac{8F_n+1}{L_{2k}}\right) = -\left(\frac{24F_k \pm L_k}{581}\right) = -1$$

από όπου προκύπτει ότι ο $8F_n + 1 \neq \square$. Τέλος, για $n = 2$ έχουμε $8F_n + 1 = 8F_2 + 1 = 8 \cdot 1 + 1 = 9 = 3^2$, που ολοκληρώνει την απόδειξη. □

ΛΗΜΜΑ 3.3.4: Αν $n \equiv 4 \pmod{2^5}$, τότε ο $8F_n + 1$ είναι τέλειο τετράγωνο μόνο για $n = 4$.

Απόδειξη. Αν $n > 4$, θέτουμε $n = 2 \cdot 3^r \cdot k + 4$ όπου $r \geq 0, 3 \nmid k$ κι ομοίως προς το πρώτο λήμμα, $k \equiv \pm 16 \pmod{48}$. Έτσι, με χρήση της ταυτότητας 5. έχουμε:

$$8F_n + 1 \equiv 8(-1)^{3^r} F_4 + 1 \equiv -8F_4 + 1 \equiv -8 \cdot 4 + 1 \equiv -23 \pmod{L_k}$$

Η ακολουθία $L_n \pmod{23}, n \in \mathbb{N}$ είναι περιοδική με περίοδο 48, δηλαδή $\forall n \in \mathbb{N}$ ισχύει $L_{n+48} \equiv L_n \pmod{23}$ κι αφού $k \equiv \pm 16 \pmod{48}$, έχουμε ότι $L_k \equiv L_{16} \equiv 2207 \equiv -1 \pmod{23}$, επομένως:

$$\left(\frac{8F_n+1}{L_k}\right) = \left(\frac{-23}{L_k}\right) = \left(\frac{-1}{L_k}\right)\cdot\left(\frac{23}{L_k}\right) = (-1)^{\frac{L_k-1}{2}}\cdot\left(\frac{L_k}{23}\right)\cdot(-1)^{\frac{L_k-1}{2}\cdot\frac{23-1}{2}} = \left(\frac{L_k}{23}\right) =$$

$= \left(\frac{-1}{23}\right) = (-1)^{\frac{23-1}{2}} = -1$
από όπου προκύπτει ότι ο $8F_n + 1 \neq \square$.
Τέλος, για $n = 4$ έχουμε $8F_n + 1 = 8F_4 + 1 = 25 = 5^2$. □

ΛΗΜΜΑ 3.3.5: Αν $n \equiv 8 \pmod{2^5 \cdot 5}$, τότε $8F_n + 1 = \square$ μόνο για $n = 8$.

Απόδειξη. Αν $n > 8$, θέτουμε $n = 2 \cdot 3^r \cdot 5l + 8$ με $3 \nmid l$ και $l \equiv \pm 16 \pmod{48}$ (ομοίως με λήμμα 1). Έστω $k = l$ ή $k = 5l$, το οποίο θα καθοριστεί αργότερα.

- Αν $k = l$:

$$8F_n + 1 \equiv 8(-1)^{5\cdot 3^r} F_8 + 1 \equiv -8F_8 + 1 \equiv -167 \pmod{L_k}$$

- Αν $k = 5l$:

$$8F_n + 1 \equiv 8(-1)^{3^r} F_8 + 1 \equiv -8F_8 + 1 \equiv -167 \pmod{L_k}$$

Άρα, σε κάθε περίπτωση έχουμε $8F_n+1 \equiv -167 \pmod{L_k}$. Η ακολουθία $L_n \pmod{167}, n \in \mathbb{N}$ είναι περιοδική με περίοδο 336, δηλαδή $\forall n \in \mathbb{N} : L_{n+336} \equiv L_n \pmod{167}$. Ακόμα, ισχύει ο παρακάτω πίνακας:

$n \pmod{336}$	± 32	± 64	± 80	± 112	± 160
$L_n \pmod{167}$	125	91	17	166	120

Με απλούς υπολογισμούς προκύπτει ότι αν $x \equiv 125, 91, 17, 166, 120 \pmod{167}$, τότε $(\frac{x}{167}) = -1$, δηλαδή οι κλάσεις $\pmod{167}$ της δεύτερης γραμμής είναι τετραγωνικά ανισοϋπόλοιπα $\pmod{167}$.
Έστω $\mathbb{A}$ το σύνολο των υπολοίπων $\pmod{336}$ της πρώτης γραμμής του πίνακα. Επιλέγουμε τον k έτσι ώστε $k \pmod{336} \in \mathbb{A}$. Επειδή $48|336$ και $l \equiv \pm 16 \pmod{48}$, έχουμε

ότι $l \equiv 16, 32, 64, 80, 112, 128, 160, 176, 208, 224, 256, 272, 304, 320 \pmod{336}$. Οι παραπάνω κλάσεις, εκτός από τέσσερις και συγκεκριμένα τις $(16, 128, 208, 320 \pmod{336})$ ανήκουν στο $\mathbb{A}$. Για αυτές τις κλάσεις επιλέγουμε $k = l$. Για τις υπόλοιπες τέσσερις επιλέγουμε $k = 5l$, δηλαδή $k = \pm 32, \pm 80$ και έτσι σε κάθε περίπτωση έχουμε ότι $k \pmod{336} \in \mathbb{A}$. Επομένως, $\forall k$, ο L_k είναι τετραγωνικό ανισοϋπόλοιπο $\pmod{167}$. Άρα προκύπτει:

$$\left(\frac{8F_n+1}{L_k}\right) = \left(\frac{-167}{L_k}\right) = \left(\frac{-1}{L_k}\right)\cdot\left(\frac{167}{L_k}\right) = (-1)^{\frac{L_k-1}{2}}\cdot(-1)^{\frac{167-1}{2}\cdot\frac{L_k-1}{2}}\cdot\left(\frac{L_k}{167}\right) = -1$$

και άρα ο $8F_n + 1$ δεν είναι τέλειο τετράγωνο.
Για $n = 8$ έχουμε: $8F_n + 1 = 8F_8 + 1 = 8 \cdot 21 + 1 = 169 = 13^2$, που ολοκληρώνει την απόδειξη. □

ΛΗΜΜΑ 3.3.6: Αν $n \equiv 10 \pmod{2^2 \cdot 5 \cdot 11}$, ο $8F_n + 1$ είναι τέλειο τετράγωνο μόνο για $n = 10$.

Απόδειξη. Η ακολουθία $\{L_n\}_{n\in\mathbb{N}}$ είναι περιοδική $\pmod{439}$ με περίοδο 438. Ισχύει ο ακόλουθος πίνακας:

$n \pmod{438}$	2	8	16	44	56	64	94	178	230	256	296	302	332	356	376
$L_n \pmod{439}$	3	47	12	306	54	407	395	24	79	101	394	202	184	135	74

Έστω $\mathbb{B}$ το σύνολο των κλάσεων $\pmod{438}$ της πρώτης γραμμής του πίνακα. Τότε $\forall n \in \mathbb{B}$ ο L_n είναι τετραγωνικό ανισοϋπόλοιπο $\pmod{439}$:

- $(\frac{3}{439}) = -(\frac{1}{3}) = -1$
- $(\frac{47}{439}) = -(\frac{16}{47}) = -(\frac{2^4}{47}) = -1$
- $(\frac{12}{439}) = (\frac{6}{439}) = (\frac{3}{439}) = -1$
- $(\frac{306}{439}) = (\frac{153}{439}) = (\frac{133}{153}) = (\frac{20}{133}) = -(\frac{10}{133}) = (\frac{5}{133}) = (\frac{3}{5}) = (\frac{2}{3}) = -1$
- $(\frac{54}{439}) = (\frac{27}{439}) = -(\frac{7}{27}) = (\frac{6}{7}) = (\frac{3}{7}) = -(\frac{1}{3}) = -1$
- $(\frac{407}{439}) = -(\frac{32}{407}) = -(\frac{16}{407}) = -(\frac{2^4}{407}) = -1$
- $(\frac{395}{439}) = -(\frac{44}{439}) = (\frac{22}{395}) = -(\frac{11}{395}) = (\frac{10}{11}) = -(\frac{5}{11}) = (\frac{1}{5}) = -1$
- $(\frac{24}{439}) = (\frac{12}{439}) = (\frac{3}{439}) = -(\frac{1}{3}) = -1$
- $(\frac{79}{439}) = -(\frac{44}{79}) = -(\frac{22}{79}) = -(\frac{11}{79}) = (\frac{2}{11}) = -1$
- $(\frac{101}{439}) = (\frac{35}{101}) = (\frac{31}{35}) = -(\frac{4}{31}) = -(\frac{2^2}{31}) = -1$
- $(\frac{394}{439}) = (\frac{197}{439}) = (\frac{45}{197}) = (\frac{17}{45}) = (\frac{11}{17}) = (\frac{6}{11}) = -(\frac{3}{11}) = (\frac{2}{3}) = -1$
- $(\frac{202}{439}) = (\frac{101}{439}) = (\frac{35}{101}) = (\frac{31}{35}) = -(\frac{4}{31}) = -(\frac{2^2}{31}) = -1$
- $(\frac{184}{439}) = (\frac{92}{439}) = (\frac{46}{439}) = (\frac{23}{439}) = -(\frac{2}{23}) = -1$
- $(\frac{135}{439}) = -(\frac{34}{135}) = -(\frac{17}{135}) = -(\frac{16}{17}) = -(\frac{8}{17}) = -(\frac{4}{17}) = -(\frac{2^2}{17}) = -1$

- $(\frac{74}{439}) = (\frac{37}{439}) = (\frac{32}{37}) = -(\frac{16}{17}) = -(\frac{2^4}{37}) = -1$

Αν $n > 10$, θέτουμε $n = 2 \cdot l \cdot 5 \cdot 11 \cdot 2^t + 10$, όπου $2 \not| l$ και $t \geq 1$.
Η ακολουθία $2^n \pmod{438}$ είναι περιοδική ως προς το n, με περίοδο 18.
Ισχύει ο παρακάτω πίνακας:

$t \pmod{18}$	1	2	3	4	5	6	7	8	9	10
$2^t \pmod{438}$	$\underline{2}$	4	$\underline{8}$	$\underline{16}$	32	$\underline{64}$	128	$\underline{256}$	74	148
$5 \cdot 2^t \pmod{438}$										$\underline{302}$
$11 \cdot 2^t \pmod{438}$		$\underline{44}$					$\underline{94}$		$\underline{376}$	
$5 \cdot 11 \cdot 2^t \pmod{438}$					$\underline{8}$					

$t \pmod{18}$	11	12	13	14	15	16	17	18
$2^t \pmod{438}$	$\underline{296}$	154	308	$\underline{178}$	$\underline{356}$	274	110	220
$5 \cdot 2^t \pmod{438}$		$\underline{332}$				$\underline{56}$		
$11 \cdot 2^t \pmod{438}$								$\underline{230}$
$5 \cdot 11 \cdot 2^t \pmod{438}$			$\underline{296}$				$\underline{356}$	

όπου οι υπογραμμισμένες κλάσεις $\pmod{438}$ ανήκουν στο $\mathbb{B}$.
Θέτουμε το k ως εξής:

$$k = \begin{cases} 2^t & \text{αν} \quad t \equiv 1,3,4,6,8,11,14,15 \pmod{18} \\ 5 \cdot 2^t & \text{αν} \quad t \equiv 10,12,16 \pmod{18} \\ 11 \cdot 2^t & \text{αν} \quad t \equiv 0,2,7,9 \pmod{18} \\ 5 \cdot 11 \cdot 2^t & \text{αν} \quad t \equiv 5,13,17 \pmod{18} \end{cases}$$

Έτσι έχουμε $k \pmod{438} \in \mathbb{B}$ κι επομένως $\forall k$ ο L_k είναι τετραγωνικό ανισοϋπόλοιπο $\pmod{439}$. Με χρήση της (5), για κάθε περίπτωση του k έχουμε:

$$8F_n + 1 \equiv -8F_{10} + 1 \equiv -439 \pmod{L_k}$$

Κι επομένως

$$\left(\frac{8F_n+1}{L_k}\right) = \left(\frac{-439}{L_k}\right) = \left(\frac{-1}{L_l}\right) \cdot \left(\frac{439}{L_k}\right) = (-1)^{\frac{L_k-1}{2}} \cdot (-1)^{\frac{L_k-1}{2} \cdot \frac{439-1}{2}} \cdot \left(\frac{L_k}{439}\right) = -1$$

και άρα ο $8F_n + 1 \neq \square$.
Για $n = 10$ έχουμε $8F_n + 1 = 8F_{10} + 1 = 8 \cdot 55 + 1 = 441 = 21^2$, που ολοκληρώνει την απόδειξη. $\square$

Από τα λήμματα 2 εώς 6 προκύπτει το παρακάτω πόρισμα.

ΠΟΡΙΣΜΑ 3.3.1: Υποθέτουμε ότι ο $n \equiv 0,2,4,8,10 \pmod{2^5 \cdot 5^2 \cdot 11}$. Τότε ο $8F_n + 1$ είναι τέλειο τετράγωνο μόνο για $n = 0,2,4,8,10$.

Στα λήμματα που έπονται, θα αποκτήσουμε μερικές αναγκαίες συνθήκες για το πότε ο $8F_n + 1$ είναι τέλειο τετράγωνο. Η ιδέα της απόδειξης είναι η εξής: Θα μελετούμε την ακολουθία $\{8F_n + 1\}_{n \in \mathbb{N}}$ modulo a_1. Η ακολουθία αυτή ξέρουμε ότι είναι περιοδική

με περίοδο έστω k_1 και θα αποκλείσουμε όλες τις τιμές του $n \pmod{k_1}$ για τις οποίες $\left(\frac{8F_n+1}{k_1}\right) = -1$. Έπειτα, θα μελετήσουμε την ίδια ακολουθία $\pmod{a_2}$ της οποίας η περίοδος θα είναι k_2. Η επιλογή του a_2 γίνεται με τέτοιο τρόπο έτσι ώστε $k_1|k_2$. Και σε αυτήν την περίπτωση θα εξαλείψουμε όλες τις τιμές του $n \pmod{k_2}$ για τις οποίες ο $8F_n + 1$ είναι τετραγωνικό ανισοϋπόλοιπο. Συνεχίζουμε αναλόγως μέχρι να φτάσουμε στο επιθυμητό αποτέλεσμα. Τα περισσότερα από τα a_i θα επιλεγούν να είναι πρώτοι αριθμοί και οι υπολογισμοί να προκύπτουν άμεσα από την σχέση

$$8F_{n+2} + 1 = (8F_{n+1} + 1) + (8F_n + 1) - 1$$

ΛΗΜΜΑ 3.3.7: Αν ο $8F_n + 1$ είναι τέλειο τετράγωνο, τότε
$n \equiv \pm 1, 0, 2, 4, 8, 10 \pmod{2^5 \cdot 5}$.

Απόδειξη.

- Modulo 11: Η ακολουθία $\{8F_n + 1\}_{n\in\mathbb{N}}$ είναι περιοδική $\pmod{11}$ με περίοδο 10. Μπορούμε να αποκλείσουμε τις κλάσεις $n \equiv 3, 5, 6, 7 \pmod{10}$ καθώς για αυτές τις τιμές του n έχουμε

  $$8F_n + 1 \equiv 6, 8, 10, 6 \pmod{11},$$

  κλάσεις οι οποίες είναι τετραγωνικά ανισοϋπόλοιπα $\pmod{11}$, καθώς:

  1. $\left(\frac{6}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{2}{3}\right) = -\left(\frac{1}{3}\right) = -1$
  2. $\left(\frac{8}{11}\right) = -\left(\frac{4}{11}\right) = -\left(\frac{2^2}{11}\right) = -1$
  3. $\left(\frac{10}{11}\right) = \left(\frac{-1}{11}\right) = (-1)^{\frac{11-1}{2}} = -1$

  Επομένως μένουν οι κλάσεις $n \equiv 0, 1, 2, 4, 8, 9 \pmod{10}$.

- Modulo 5: Μπορούμε να εξαιρέσουμε τις κλάσεις $n \equiv 9, 11, 12, 14, 18 \pmod{20}$ καθώς για αυτές τις τιμές του n έχουμε ότι

  $$8F_n + 1 \equiv \pm 2 \pmod{5},$$

  κλάσεις οι οποίες είναι τετραγωνικά ανισοϋπόλοιπα $\pmod{5}$, γιατί

  1. $\left(\frac{2}{5}\right) = -\left(\frac{1}{5}\right) = -1$
  2. $\left(\frac{-2}{5}\right) = \left(\frac{2}{5}\right) = -1$

  Επομένως απομένουν $n \equiv 0, 1, 2, 4, 8, 10, 19 \pmod{20}$.

- Modulo 3: Αποκλείουμε τις κλάσεις $n \equiv 3, 5, 6 \pmod{8}$ καθώς για αυτές τις τιμές του n έχουμε ότι

  $$8F_n + 1 \equiv 2 \pmod{3}$$

  , αφού η κλάση του 2 είναι τετραγωνικό ανισοπϋπόλοιπο $\pmod{3}$, άρα, αφού $8|40$, εξαιρούμε τις κλάσεις $n \equiv 19, 21, 22, 30 \pmod{40}$ και άρα απομένουν οι κλάσεις $n \equiv 0, 1, 2, 4, 8, 10, 20, 24, 28, 39 \pmod{40}$.

- Modulo 2161: Εξαιρούμε τις κλάσεις $n \equiv 28, 39, 41, 42, 44, 60, 68 \pmod{80}$ καθώς για αυτές τις τιμές του n έχουμε

  $$8F_n + 1 \equiv 1153, 2154, 2154, 2154, 2138, 2067, 1010 \pmod{2161},$$

  κλάσεις οι οποίες είναι τετραγωνικά ανισοϋπόλοιπα $\pmod{2161}$, αφού:

1. $\left(\frac{1153}{2161}\right) = \left(\frac{1008}{1153}\right) = \left(\frac{504}{1153}\right) = \left(\frac{252}{1153}\right) = \left(\frac{126}{1153}\right) = \left(\frac{63}{1153}\right) = \left(\frac{19}{63}\right) = -\left(\frac{6}{19}\right) = \left(\frac{3}{19}\right) = -\left(\frac{1}{3}\right) = 1.$
2. $\left(\frac{2154}{2161}\right) = \left(\frac{1077}{2161}\right) = \left(\frac{7}{1077}\right) = \left(\frac{6}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{1}{3}\right) = -1.$
3. $\left(\frac{2138}{2161}\right) = \left(\frac{1069}{2161}\right) = \left(\frac{23}{1069}\right) = \left(\frac{11}{23}\right) = -\left(\frac{1}{11}\right) = -1.$
4. $\left(\frac{2067}{2161}\right) = \left(\frac{94}{2067}\right) = -\left(\frac{47}{2067}\right) = \left(\frac{46}{47}\right) = \left(\frac{-1}{47}\right) = (-1)^{\frac{47-1}{2}} = -1$
5. $\left(\frac{1010}{2161}\right) = \left(\frac{505}{2161}\right) = \left(\frac{141}{505}\right) = \left(\frac{82}{141}\right) = -\left(\frac{41}{141}\right) = -\left(\frac{18}{41}\right) = -\left(\frac{9}{41}\right) = -\left(\frac{5}{9}\right) = -\left(\frac{4}{5}\right) = \left(\frac{2}{5}\right) = -\left(\frac{1}{3}\right) = -1$

- Modulo 3041: Εξαιρούμε τις κλάσεις $n \equiv 24, 40, 50, 64, 79, 81, 82, 84, 88, 90, 100, 104, 120, 128 \pmod{160}$ καθώς για αυτές τις τιμές του n έχουμε αντίστοιχα

  $$8F_n+1 \equiv -57, 2590, 2613, 1815, -7, -7, -7, -23, 2874, 2602, 619, 595, 447, 1500 \pmod{3041}.$$

  Οι παραπάνω κλάσεις όμως είναι τετραγωνικά ανισοϋπόλοιπα $\pmod{3041}$ αφού:

  1. $\left(\frac{1492}{3041}\right) = \left(\frac{746}{3041}\right) = \left(\frac{373}{3041}\right) = \left(\frac{57}{373}\right) = \left(\frac{31}{57}\right) = \left(\frac{26}{31}\right) = \left(\frac{26}{31}\right) = \left(\frac{13}{31}\right) = \left(\frac{5}{13}\right) = \left(\frac{3}{5}\right) = -1$
  2. $\left(\frac{2590}{3041}\right) = \left(\frac{1295}{3041}\right) = \left(\frac{451}{1295}\right) = -\left(\frac{393}{451}\right) = -\left(\frac{58}{393}\right) = -\left(\frac{29}{393}\right) = -\left(\frac{16}{29}\right) = -\left(\frac{2^4}{29}\right) = -1$
  3. $\left(\frac{1815}{3041}\right) = \left(\frac{428}{2613}\right) = -\left(\frac{214}{2613}\right) = \left(\frac{107}{2613}\right) = \left(\frac{45}{107}\right) = \left(\frac{17}{45}\right) = \left(\frac{11}{17}\right) = \left(\frac{6}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{2}{3}\right) = -1.$
  4. $\left(\frac{1815}{3041}\right) = \left(\frac{1226}{1815}\right) = \left(\frac{613}{1815}\right) = \left(\frac{589}{613}\right) = \left(\frac{24}{589}\right) = -\left(\frac{12}{589}\right) = \left(\frac{6}{589}\right) = -\left(\frac{3}{589}\right) = -\left(\frac{1}{3}\right) = -1$
  5. $\left(\frac{3034}{3041}\right) = \left(\frac{1517}{3041}\right) = \left(\frac{7}{1517}\right) = \left(\frac{5}{7}\right) = \left(\frac{2}{5}\right) = -1$
  6. $\left(\frac{3018}{3041}\right) = \left(\frac{1509}{3041}\right) = \left(\frac{23}{1509}\right) = \left(\frac{14}{23}\right) = \left(\frac{7}{23}\right) = -\left(\frac{2}{7}\right) = -1$
  7. $\left(\frac{2874}{3041}\right) = \left(\frac{1437}{3041}\right) = \left(\frac{167}{1437}\right) = \left(\frac{101}{167}\right) = \left(\frac{66}{101}\right) = -\left(\frac{33}{101}\right) = -\left(\frac{2}{33}\right) = -\left(\frac{1}{33}\right) = -1$
  8. $\left(\frac{2602}{3041}\right) = \left(\frac{1301}{3041}\right) = \left(\frac{439}{1301}\right) = \left(\frac{423}{439}\right) = -\left(\frac{16}{423}\right) = -\left(\frac{2^4}{423}\right) = -1$
  9. $\left(\frac{619}{3041}\right) = \left(\frac{565}{619}\right) = \left(\frac{54}{565}\right) = -\left(\frac{27}{565}\right) = -\left(\frac{25}{27}\right) = -\left(\frac{5^2}{27}\right) = -1$
  10. $\left(\frac{59}{3041}\right) = \left(\frac{32}{59}\right) = -\left(\frac{16}{59}\right) = -\left(\frac{2^4}{59}\right) = -1$
  11. $\left(\frac{447}{3041}\right) = \left(\frac{359}{447}\right) = -\left(\frac{44}{359}\right) = -\left(\frac{11}{359}\right) = \left(\frac{7}{11}\right) = -\left(\frac{4}{7}\right) = -\left(\frac{2^2}{7}\right) = -1$
  12. $\left(\frac{1500}{3041}\right) = \left(\frac{375}{3041}\right) = \left(\frac{41}{375}\right) = \left(\frac{6}{41}\right) = \left(\frac{3}{41}\right) = \left(\frac{2}{3}\right) = -1$

- Modulo 1601: Αποκλείουμε τις κλάσεις $n \equiv 130, 144 \pmod{160}$ καθώς για αυτές έχουμε

  $$8F_n + 1 \equiv 639, 110 \pmod{1601}$$

  κλάσεις οι οποίες είναι τετραγωνικά ανισοϋπόλοιπα $\pmod{1601}$. Πράγματι,

  1. $\left(\frac{639}{1601}\right) = \left(\frac{323}{639}\right) = -\left(\frac{316}{323}\right) = \left(\frac{158}{323}\right) = -\left(\frac{79}{323}\right) = \left(\frac{7}{79}\right) = -\left(\frac{2}{7}\right) = -1$
  2. $\left(\frac{110}{1601}\right) = \left(\frac{55}{1601}\right) = \left(\frac{6}{55}\right) = \left(\frac{3}{55}\right) = -\left(\frac{1}{3}\right) = -1$

  Επομένως μας απέμειναν οι κλάσεις $n \equiv 0, 1, 2, 4, 8, 10, 20, 48, 80, 159 \pmod{160}$.

- Modulo 2207. Εξαιρούμε τις κλάσεις $n \equiv 48, 80, 208, 240 \pmod{320}$ καθώς για αυτές τις κλάσεις
$$8F_n + 1 \equiv 933, 1276 \pmod{2207}$$
τα οποία δεν είναι τετραγωνικά ανισοϋπόλοιπα $\pmod{2207}$, καθώς:
  1. $\left(\frac{933}{2207}\right) = \left(\frac{341}{933}\right) = \left(\frac{251}{341}\right) = \left(\frac{90}{251}\right) = -\left(\frac{45}{251}\right) = -\left(\frac{26}{45}\right) = \left(\frac{13}{45}\right) = \left(\frac{6}{13}\right) = -\left(\frac{3}{13}\right) = -\left(\frac{1}{3}\right) = -1$
  2. $\left(\frac{1276}{1601}\right) = \left(\frac{638}{2207}\right) = \left(\frac{319}{2207}\right) = -\left(\frac{293}{319}\right) = -\left(\frac{26}{293}\right) = \left(\frac{13}{293}\right) = \left(\frac{7}{13}\right) = \left(\frac{6}{7}\right) = \left(\frac{-1}{7}\right) = (-1)^{\frac{7-1}{2}} = -1$

  Κι άρα απομένουν οι κλάσεις $n \equiv 0, 1, 2, 4, 8, 10, 20, 159 \pmod{160}$.

- Τέλος, μπορούμε να εξαιρέσουμε την κλάση $n \equiv 20 \pmod{160}$ καθώς αν θέσουμε $n = 160m + 20, m \in \mathbb{Z}$ και αφού $80 \equiv 2 \pmod 6$, από την ταυτότητα 5. έχουμε $F_{160m+20} \equiv \pm F_{20} \pmod{L_{80}}$, όπου το πρόσημο εξαρτάται από το εάν ο m είναι άρτιος ή περιττός. Με χρήση των ταυτοτήτων 3. και 4. προκύπτει:
$$\left(\frac{8F_{20}+1}{L_{80}}\right) = \left(\frac{L_{80}}{8F_{20}+1}\right) = \left(\frac{(L_{20}^2-2)^2-2}{8F_{20}+1}\right) = \left(\frac{(5F_{20}^2+2)^2-2}{8F_{20}+1}\right)$$
$$= \left(\frac{(5\cdot(8F_{20})^2+2\cdot 8^2)^2-2\cdot 8^4}{8F_{20}+1}\right) = \left(\frac{(5\cdot(8F_{20})^2+2\cdot 8^2)^2-2\cdot 8^4}{8F_{20}+1}\right) = \left(\frac{9497}{54121}\right) = -1$$
  Όμοια, $\left(\frac{-8F_{20}+1}{L_{80}}\right) = -1$.
  Άρα τελικά $n \equiv 0, 1, 2, 4, 8, 10, 159 \pmod{160}$.

□

Στο εξής θεωρούμε ότι ο n είναι άρτιος.

ΛΗΜΜΑ 3.3.8: Αν ο n είναι άρτιος και $8F_n+1 = \square$, τότε $n \equiv 0, 2, 4, 8, 10 \pmod{2^2\cdot 5^2}$.

Απόδειξη. Θα ξεκινήσουμε από το δεύτερο βήμα της απόδειξης του προηγούμενου λήμματος. Σημειώνουμε ότι αφού ο n είναι άρτιος έχουμε $n \equiv 0, 2, 4, 8, 10 \pmod{20}$.

- Modulo 101: Εξαιρούμε τις κλάσεις $n \equiv 12, 18, 20, 24, 32, 38, 40, 42, 44, 48 \pmod{50}$ καθώς για αυτές τις κλάσεις έχουμε αντίστοιχα:
$$8F_n + 1 \equiv 42, 69, 86, 73, 34, 61, 66, 35, 38, 94 \pmod{101}$$
κλάσεις οι οποίες είναι τετραγωνικά ανισοϋπόλοιπα $\pmod{101}$.

- Modulo 151: Αποκλείουμε τις κλάσεις $n \equiv 22, 28, 34 \pmod{50}$ αφού για αυτές προκύπτει:
$$8F_n + 1 \equiv 51, 102, 108 \pmod{151}$$
που είναι τετραγωνικά ανισοϋπόλοιπα και αυτά. Άρα απομένουν οι κλάσεις $n \equiv 0, 2, 4, 8, 10, 30, 50, 60, 64, 80 \pmod{100}$.

- Modulo 3001: Εξαιρούμε τις κλάσεις $n \equiv 60, 80 \pmod{100}$ καθώς για αυτές προκύπτει αντίστοιχα:
$$8F_n + 1 \equiv 2562, 2900 \pmod{3001}$$
για τις οποίες κλάσεις όμως ισχύει $\left(\frac{2562}{2900}\right) = \left(\frac{2900}{3001}\right) = -1$.

- Modulo 25: Εξαιρούμε την κλάση $n \equiv 64 \pmod{100}$ καθώς για αυτήν την κλάση έχουμε:

$$8F_n + 1 \equiv 10 \pmod{25}$$

που είναι τετραγωνικό ανισοϋπόλοιπο $\pmod{25}$. Άρα $n \equiv 0, 2, 4, 8, 10, 30, 50 \pmod{100}$.

- Modulo 401: Αποκλείουμε τις κλάσεις $n \equiv 30, 50, 130, 150 \pmod{200}$ καθώς για αυτές προκύπτει:

$$8F_n + 1 \equiv 122, 165, 281, 238 \pmod{401}$$

που είναι τετραγωνικά ανισοϋπόλοιπα $\pmod{401}$. Άρα τελικά $n \equiv 0, 2, 4, 8, 10 \pmod{100}$, που ολοκληρώνει την απόδειξη.

□

ΛΗΜΜΑ 3.3.9: Αν ο n είναι άρτιος και $8F_n + 1 = \square$,
τότε $n \equiv 0, 2, 4, 8, 10 \pmod{2^2 \cdot 5 \cdot 11}$.

Απόδειξη.

- Modulo 199: Εξαιρούμε τις κλάσεις $n \equiv 16, 18, 20 \pmod{22}$, αφού για αυτές τις κλάσεις έχουμε ότι

$$8F_n + 1 \equiv 136, 176, 192 \pmod{199}$$

που είναι τετραγωνικά ανισοϋπόλοιπα $\pmod{199}$. Ως εκ τούτου απομένουν οι κλάσεις $n \equiv 0, 2, 4, 6, 8, 10, 12, 14 \pmod{22}$.

- Modulo 89: Εξαιρούμε τις κλάσεις $n \equiv 6, 24, 26, 28, 32, 34 \pmod{44}$ αφού για αυτές, έχουμε αντίστοιχα

$$8F_n + 1 \equiv 65, 82, 66, 26, 6, 6 \pmod{89}$$

που δεν είναι τετραγωνικά ισοϋπόλοιποα $\pmod{89}$, άρα απομένουν οι κλάσεις $n \equiv 0, 2, 4, 8, 10, 12, 14, 22, 30, 36 \pmod{44}$. Ακόμα, στα δύο πρώτα βήματα του λήμματος 7 δείξαμε ότι είναι απαραίτητο $n \equiv 0, 2, 4, 8, 10 \pmod{20}$, άρα κι αφού $44|220$, έχουμε $n \equiv 0, 2, 4, 8, 10, 22, 30, 44, 48, 80, 88, 90, 100, 102, 110, 124, 140, 142, 144, 168, 180, 184, 188, 190 \pmod{220}$.

- Modulo 661: Αποκλείουμε τις κλάσεις $n \equiv 44, 48, 124, 144, 180, 184 \pmod{220}$ καθώς για αυτές έχουμε αντίστοιχα:

$$8F_n + 1 \equiv 544, 214, 290, 447, 379, 546 \pmod{661}$$

κλάσεις που δεν είναι τετραγωνικά ισοϋπόλοιπα $\pmod{661}$.

- Modulo 331: Εξαιρούμε τις κλάσεις $n \equiv 30, 58, 88, 102 \pmod{110}$ καθώς από αυτές προκύπτουν αντίστοιχα:

$$8F_n + 1 \equiv 242, 231, 312, 164 \pmod{331}$$

που είναι τετραγωνικά ανισοϋπόλοιπα $\pmod{331}$.

- Modulo 474541: Αποκλείουμε τις κλάσεις $n \equiv 80, 90, 142, 188 \pmod{220}$ καθώς για αυτές έχουμε αντίστοιχα:

$$8F_n + 1 \equiv 12747, 54121, 131546, 131546 \pmod{474541}$$

για τις οποίες κλάσεις ισχύει ότι δεν είναι τετραγωνικά ισοϋπόλοιπα $\pmod{474541}$. Από τις τρεις τελευταίες περιπτώσεις μαζί προκύπτει ότι $n \equiv 0, 2, 4, 8, 10, 22, 100, 110, 190 \pmod{220}$.

- Modulo 307: Εξαιρούμε τις κλάσεις $n \equiv 14, 22, 58, 66 \pmod{88}$ καθώς για αυτές τις κλάσεις προκύπτει αντίστοιχα:

$$8F_n + 1 \equiv 254, 162, 55, 147 \pmod{307}$$

που δεν είναι τετραγωνικά ισοϋπόλοιπα $\pmod{307}$. Αυτές οι κλάσεις είναι ισοδύναμες με $n \equiv 14, 22 \pmod{44}$, άρα μπορούμε να εξαιρέσουμε και τις $n \equiv 22, 110, 190 \pmod{220}$ από αυτές που έμειναν στο προηγούμενο βήμα και άρα απομένουν οι κλάσεις $n \equiv 0, 2, 4, 8, 10, 100 \pmod{220}$.

- Modulo 881: Μπορούμε να αποκλείσουμε τις κλάσεις $n \equiv 12, 56, 100, 144 \pmod{176}$, καθώς για αυτές έχουμε αντίστοιχα:

$$8F_n + 1 \equiv 272, 293, 611, 590 \pmod{881}$$

κλάσεις που είναι τετραγωνικά ανισοϋπόλοιπα $\pmod{881}$. Αυτές είναι ισοδύναμες με το $n \equiv 12 \pmod{44}$ αρα μπορούμε να εξαιρέσουμε και το $100 \pmod{220}$. Τελικά, $n \equiv 0, 2, 4, 8, 10 \pmod{220}$, που ολοκληρώνει την απόδειξη.

□

ΠΡΟΤΑΣΗ 3.3.1: Το σύστημα ισοδυναμιών:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

έχει λύση ακριβώς τότε όταν Μ.Κ.Δ.$(m_i, m_j) | (a_i - a_j), \forall i, j, i \neq j$. Η λύση, αν υπάρχει, είναι μοναδική $\pmod{m}$, όπου $m =$ Ε.Κ.Π.$(m_1, m_2, \ldots, m_r)$.

Για την απόδειξη της πρότασης 3.3.1. παραπέμπουμε στο [1] (σελίδα 150). Απο τα λήμματα 7 έως 9 προκύπτει το εξής πόρισμα:

ΠΟΡΙΣΜΑ 3.3.2: Αν ο n είναι άρτιος και $8F_n + 1 = \square$ τότε
$n \equiv 0, 2, 4, 8, 10 \pmod{2^5 \cdot 5^2 \cdot 11}$.

Απόδειξη. Αν υποθέσουμε ότι ο n είναι άρτιος και ότι ο $8F_n + 1$ είναι τέλειο τετράγωνο, τότε σύμφωνα με τα λήμματα 3.3.7 έως 3.3.9. ο n θα πρέπει να πληροί τις παρακάτω ισοδυναμίες:

1. $n \equiv c_1 \pmod{2^5 \cdot 5}$
2. $n \equiv c_2 \pmod{2^2 \cdot 5^2}$

3. $n \equiv c_3 \pmod{2^2 \cdot 5 \cdot 11}$

με τα $c_1, c_2, c_3 \in \{0, 2, 4, 8, 10\}$. Επειδή ο μέγιστος κοινός διαιρέτης των $2^5 \cdot 5, 2^2 \cdot 5^2, 2^2 \cdot 5 \cdot 11$ είναι 20 και η διαφορά δύο οποιωνδήποτε αριθμών από τους $\{0, 2, 4, 8, 10\}$ δεν ξεπερνάει το 10, από την Πρόταση 3.3.1 προκύπτει ότι $c_1 = c_2 = c_3$. Επιπλέον το ελάχιστο κοινό πολλαπλάσιο είναι $2^5 \cdot 5^2 \cdot 11$, έχουμε τελικά ότι
$n \equiv 0, 2, 4, 8, 10 \pmod{2^5 \cdot 5^2 \cdot 11}$ □

Είμαστε έτοιμο να δώσουμε τις αποδείξεις των θεωρημάτων.

Απόδειξη του πρώτου θεωρήματος: Αν ο $8F_n + 1 = \square$, τότε η απόδειξη έπεται από τα λήμματα 7 και 1, αν ο n είναι περιττός και απο τα πορίσματα 2 και 1 αν είναι άρτιος.

Απόδειξη του δεύτερου θεωρήματος: Αυτό έπεται άμεσα από το θεώρημα 1, αν εξαιρέσουμε το $F_0 = 0$ αφού εξ ορισμού ένας τρίγωνος αριθμός είναι φυσικός αριθμός. Πράγματι, $F_{\pm 1} = F_2 = 1 \cdot \frac{2}{2}, F_4 = 2 \cdot \frac{3}{2}, F_8 = 6 \cdot \frac{7}{2}, F_{10} = 10 \cdot \frac{11}{2}$.

Για τους αριθμούς Fibonacci με άρτιο δείκτη το αποτέλεσμα είχε αποδειχθεί το 1976 από τον R. Steiner. (βλέπε [12]).
Πεντάγωνος ονομάζεται ένας φυσικός αριθμός k αν και μόνον αν $k = \frac{1}{2}m(3m - 1)$. Το 1996 ο Luo Ming απέδειξε ότι οι μόνοι όροι της ακολουθίας Fibonacci που είναι πεντάγωνοι αριθμοί είναι οι $F_{\pm 1} = F_2 = 1$ και $F_{\pm 5} = 5$ (Βλέπε [9]).

ΠΟΡΙΣΜΑ 3.3.3: Η διοφαντική εξίσωση $5X^2(X+1)^2 - 4Y^2 = 16$ έχει ακέραιες λύσεις μόνο τις $(x, y) = (-2, \pm 1), (1, \pm 1)$.

Απόδειξη. Όπως είδαμε στην εισαγωγή, η παραπάνω εξίσωση συνεπάγεται $\frac{1}{2}x(x+1) = F_n$ και ο n είναι περιττός. Άρα από το θεώρημα 2 έχουμε ότι $\frac{1}{2}x(x+1) = 1$, από όπου προκύπτει ότι $x = -2$ ή $x = 1$. □

ΠΟΡΙΣΜΑ 3.3.4: Η διοφαντική εξίσωση $5 \cdot X^2 \cdot (X+1)^2 - 4 \cdot Y^2 = -16$ έχει ακέραιες λύσεις μόνο τις $(x, y) = (-1, \pm 2), (0, \pm 2), (-2, \pm 3), (1, \pm 3), (-3, \pm 7), (2, \pm 7), (-7, \pm 47), (6, \pm 47), (-11, \pm 123)$ και $(10, \pm 123)$.

Απόδειξη. Όπως και στο προηγούμενο θεώρημα, έχουμε ότι $\frac{1}{2} \cdot x \cdot (x+1) = F_n$ με τον δείκτη n να είναι άρτιος αριθμός. Έτσι, από το δεύτερο θεώρημα, αν προσθέσουμε και τον $F_0 = 0$ που δεν τον θεωρήσαμε τρίγωνο αριθμό, έχουμε ότι $\frac{1}{2} \cdot x \cdot (x+1) = 0, 1, 3, 21$ ή 55, δηλαδη $x = -1, 0, -2, 1, -3, 2, -7, 6, -11, 10$ όπου για όλες αυτές τις τιμές του x, ο αριθμός y που προκύπτει είναι ακέραιος. □

3.4 Τρίγωνοι αριθμοί στην ακολουθία Lucas L_n

Η απόδειξη σε αυτήν την ακολουθία είναι πανομοιότυπη με αυτή της ακολουθίας Fibonacci (δηλαδή αν ο L_n είναι τρίγωνος αριθμός, τότε ο $8L_n + 1 = \square$ οπότε αρκεί να βρούμε έναν ακέραιο $l(n)$ για τον οποίο ο $8L_n + 1$ είναι τετραγωνικό ανισοϋπόλοιπο $(\text{mod } l(n))$). Στην απόδειξη γίνεται χρήση του ίδιου κριτηρίου με το σύμβολο του Jacobi. Δίνονται, χωρίς απόδειξη, τα αποτελέσματα του κριτηρίου.

ΛΗΜΜΑ 3.4.1: Αν $n \equiv 1 \pmod{2^4 \cdot 5 \cdot 11}$ τότε ο $8L_n + 1$ είναι τέλειο τετράγωνο μόνο για $n = 1$.

ΛΗΜΜΑ 3.4.2: Αν $n \equiv \pm 2 \pmod{2^5}$, τότε ο $8L_n + 1 = \square$ μόνο για $n = \pm 2$.

ΛΗΜΜΑ 3.4.3: Αν $n \equiv \pm 18 \pmod{2^3 \cdot 5^2 \cdot 11}$ τότε ο $8L_n + 1$ είναι τέλειο τετράγωνο μόνο για $n = \pm 18$.

Τα παραπάνω τρία λήμματα συνοψίζονται στο εξής πόρισμα:

ΠΟΡΙΣΜΑ 3.4.1: Υποθέτουμε ότι $n \equiv 1, \pm 2, \pm 18 \pmod{2^5 \cdot 5^2 \cdot 11}$. Τότε ο $8L_n + 1 = \square$ μόνο για $n = 1, \pm 2, \pm 18$.

ΛΗΜΜΑ 3.4.4: Αν ο $8L_n + 1$ είναι τέλειο τετράγωνο, τότε κατ'ανάγκη $n \equiv 1, \pm 2, \pm 18 \pmod{2^5 \cdot 5}$.

ΛΗΜΜΑ 3.4.5: Αν ο $8L_n + 1$ είναι τέλειο τετράγωνο, τότε κατ'ανάγκη $n \equiv 1, \pm 2, \pm 18 \pmod{2^2 \cdot 5^2}$.

ΛΗΜΜΑ 3.4.6: Αν ο $8L_n + 1$ είναι τέλειο τετράγωνο, τότε κατ'ανάγκη $n \equiv 1, \pm 2, \pm 18 \pmod{2^3 \cdot 11}$.

ΛΗΜΜΑ 3.4.7: Αν ο $8L_n + 1$ είναι τέλειο τετράγωνο, τότε κατ'ανάγκη $n \equiv 1, \pm 2, \pm 18 \pmod{2^2 \cdot 5 \cdot 11}$.

Απο τα τέσσερα τελευταίο λήμματα προκύπτει το εξής:

ΠΟΡΙΣΜΑ 3.4.2: Αν ο $8L_n + 1$ είναι τέλειο τετράγωνο, τότε $n \equiv 1, \pm 2, \pm 18 \pmod{2^5 \cdot 5^2 \cdot 11}$.

Με την βοήθεια των δύο πορισμάτων αυτής της ενότητας αποδεικνύεται το εξής θεώρημα:

ΘΕΩΡΗΜΑ 3.4.1: Οι μόνοι όροι που είναι τρίγωνοι αριθμοί στην ακολουθία L_n είναι οι $L_1 = 1, L_{\pm 2} = 3$ και $L_{\pm 18} = 5778 = \frac{1}{2} \cdot 107 \cdot 108$.

ΠΟΡΙΣΜΑ 3.4.3: Η διοφαντική εξίσωση $20X^2 - Y^2(Y+1)^2 = 16$ έχει ακέραιες λύσεις τις $(\pm x, y) = (1, -2), (1, 1)$ μόνο.

ΠΟΡΙΣΜΑ 3.4.4: Η διοφαντική εξίσωση $20X^2 - Y^2(Y+1)^2 = -16$ έχει ακέραιες λύσεις τις $(\pm x, y) = (1, -3), (1, 2), (2584, -108), (2584, 107)$ μόνο.

3.5 Τρίγωνοι αριθμοί στην ακολουθία P_n

Θεωρούμε τις ακολουθίες U_n, V_n ως προς το ζευγάρι $(P, Q) = (2, -1)$. Αυτές συμβολίζονται P_n και Q_n και ονομάζονται ακολουθία του Pell και ακολουθία των Pell-Lucas αντίστοιχα. Οι αναδρομικές τους σχέσεις είναι οι

$$P_{n+2} = 2P_{n+1} + P_n, \quad P_0 = 0, P_1 = 1$$

και

$$Q_{n+2} = 2Q_{n+1} + Q_n, \quad Q_0 = 2, Q_1 = 1$$

Σε αυτήν την ενότητα θα βρούμε τους όρους που είναι τρίγωνοι αριθμοί στην ακολουθία P_n.
Ισχύουν οι παρακάτω ταυτότητες:

1. $P_{-m} = (-1)^{m+1}P_m \quad Q_{-m} = (-1)^m Q_m$
2. $P_{m+n} = P_m P_{n+1} + P_{m-1}P_n$
3. $P_{m+n} = 2P_m Q_n - (-1)^n P_{m-n}$
4. $P_{2^t m} = P_m(2Q_m)(2Q_{2m})(2Q_{4m})\ldots(2Q_{2^{t-1}m})$

   Απόδειξη. Η απόδειξη αυτής της ιδιότητας θα γίνει με επαγωγή στο t.
   Για $t = 1$: $P_{2m} \overset{(3)}{=} 2P_m Q_m - (-1)^m P_0 = P_m(2Q_m)$, επομένως ισχύει.
   Υποθέτουμε ότι ισχύει για $t = j$, δηλαδή $P_{2^j m} = P_m(2Q_m)(2Q_{2m})(2Q_{4m})\ldots(2Q_{2^{j-1}m})$.
   Εξετάζουμε αν ισχύει για $t = j+1$:
   $P_{2^{j+1}m} = P_{2\cdot 2^j m} \overset{(3)}{=} 2P_{2^j m}Q_{2^j m} - (-1)2^j m P_0 = P_{2^j m}(2Q_{2^j m}) = P_m(2Q_m)(2Q_{2m})\ldots(2Q_{2^j m})$,
   δηλαδή το ζητούμενο και επομένως η προς απόδειξη σχέση ισχύει για κάθε φυσικό αριθμό t. □

5. $Q_m^2 = 2P_m^2 + (-1)^m$
6. $Q_{2m} = 2Q_m^2 - (-1)^m$
7. Αν $d = \text{Μ.Κ.Δ.}(m,n)$, τότε

$$\begin{cases} (P_m, Q_n) = Q_d & \text{αν } \frac{m}{d} \quad \text{είναι άρτιος} \\ (P_m, Q_n) = 1 & \text{αλλιώς} \end{cases}$$

   Η ταυτότητα 7. προκύπτει από την Πρόταση 2.3.8. ως προς το ζευγάρι $(P,Q) = (2,-1)$.

Από την ταυτότητα 6. συμπεραίνουμε ότι αν $t > 1$, τότε $Q_{2^t} \equiv 1 \pmod 8$.
Πράγματι, για $t = 2$ έχουμε $Q_4 = 17 \equiv 1 \pmod 8$.
Έστω ότι ισχύει για $t = k$, δηλαδή $Q_{2^k} \equiv 1 \pmod 8$.
Εξετάζουμε για $t = k+1$:

$$Q_{2^{t+1}} = Q_{2\cdot 2^k} = 2Q_k^2 - (-1)^{2^t} \equiv 2\cdot 1 - 1 \equiv 1 \pmod 8$$

και άρα:

$$\text{Αν} \quad t > 1, \quad \text{τότε} \quad Q_{2^t} \equiv 1 \pmod 8 \tag{3.1}$$

ΛΗΜΜΑ 3.5.1: Έστω $k = 2^t, t \geq 1, g > 0$ με g περιττό και $m \in \mathbb{Z}$. Τότε:

(i) $P_{2kg+m} \equiv -P_m \pmod{Q_k}$

(ii) $P_{2kg} \equiv \pm P_{2k} \pmod{Q_{2k}}$

Απόδειξη. (i) $P_{2kg+m} = P_{[k(2g-1)+m]+k}$, άρα η σχέση $P_{l+s} = 2P_l Q_s - (-1)^s P_{l-s}$ για $l = k(2g-1)+m$ και $s = k$, γίνεται:

$$P_{[k(2g-1)+m]+k} = 2P_{[k(2g-1)+m]+k}Q_k - (-1)^k P_{k(2g-2)+m}$$

και άρα, αφού ο k είναι άρτιος, έχουμε

$$P_{2kg+m} \equiv -P_{k(2g-2)+m} \pmod{Q_k}$$

Επαναλαμβάνουμε την διαδικασία για τον $P_{k(2g-2)+m}$, δηλαδή $P_{k(2g-2)+m} = P_{[k(2g-3)+m]+k}$ και εφαρμόζουμε πάλι την σχέση για $l = k(2g-3)+m$ και $s = k$, επομένως:

$$P_{[k(2g-2)+m]+k} \equiv P_{k(2g-4)+m} \pmod{Q_k}$$

επομένως έχουμε

$$P_{2kg+m} \equiv P_{k(2g-4)+m} \pmod{Q_k}.$$

Παρατηρούμε ότι τα πρόσημα πηγαίνουν εναλλάξ και ότι σε άρτιο πλήθος βημάτων έχουμε θετικό πρόσημο, άρα μετά από $g-2$ ακόμα βήματα θα έχουμε

$$P_{2kg+m} \equiv (-1)^g P_m \pmod{Q_k}$$

κι αφού ο g είναι περιττός:

$$P_{2kg+m} \equiv -P_m \pmod{Q_k}$$

(ii) Αν $n = 2kg = 2k(g-1)+2k$, τότε

$$P_n = P_{2k(g-1)+2k} \overset{(3)}{=} 2P_{2k(g-1)}Q_{2k} - (-1)^{2k}P_{2k(g-2)} \equiv -P_{2k(g-2)} \pmod{Q_{2k}}.$$

Κάνουμε την ίδια διαδικασία για τον $P_{2k(g-2)}$ και προκύπτει ότι $P_{2k(g-2)} \equiv -P_{2k(g-4)} \pmod{Q_{2k}}$, άρα

$$P_n \equiv P_{2k(g-4)} \pmod{Q_{2k}}.$$

Πάλι τα πρόσημα πηγαίνουν εναλλάξ με το θετικό να βρίσκεται στο άρτιο πλήθος βημάτων. Έτσι, αν επαναλάβουμε την διαδικασία $\frac{g-1}{2}$ φορές συνολικά, προκύπτει το ζητούμενο, δηλαδή:

$$P_{2kg} \equiv (-1)^{\frac{g-1}{2}} P_{2k} \pmod{Q_{2k}}$$

□

ΛΗΜΜΑ 3.5.2: Αν $k = 2^t, t \geq 1$ τότε $\left(\frac{8P_{2k}+1}{Q_{2k}}\right) = \left(\frac{-8P_{2k}+1}{Q_{2k}}\right)$.

Απόδειξη. Κατ'αρχήν, κάθε σύμβολο Jabobi είναι καλώς ορισμένο. Όντως, αν $d =$Μ.Κ.Δ.$(8P_{2k}+1, Q_{2k})$ (ή Μ.Κ.Δ. $(-8P_{2k}+1, Q_{2k})$) τότε $d|(8P_{2k}+1)(-8P_{2k}+1)$, δηλαδή $d|1-64P_{2k}^2$. Όμως, από την ταυτότητα 5. έχουμε ότι $1-64P_{2k}^2 = 1-32(Q_{2k}^2-1) = 33-2Q_{2k}^2$. Τότε όμως $d|33$. Τότε $d|P_{12}$, αφού $P_{12} = 13860 = 33 \cdot 420$. Από την ταυτότητα 7. και αφού $t \geq 1$ έχουμε ότι $(P_{12}, Q_{2k}) = 2$ και άρα $d|2$, επομένως $d|$Μ.Κ.Δ.$(33, 2) = 1$, άρα $d = 1$.

$$\left(\frac{P_{2k}+1}{Q_{2k}}\right) \cdot \left(\frac{-8P_{2k}+1}{Q_{2k}}\right) = \left(\frac{1-64P_{2k}^2}{Q_{2k}}\right) = \left(\frac{33-2Q_{2k}^2}{Q_{2k}}\right) = \left(\frac{33}{Q_{2k}}\right) =$$

$$= (-1)^{\frac{33-1}{2}\cdot\frac{Q_{2k}-1}{2}} \cdot \left(\frac{Q_{2k}}{33}\right) = \left(\frac{Q_{2k}}{33}\right)$$

Εξετάζουμε ξεχωστιστά τις περιπτώσεις $t = 1$ και $t \geq 2$.

Για $t = 1$, δηλαδή Q_4, έχουμε:

$$\left(\frac{Q_4}{33}\right) = \left(\frac{17}{33}\right) = (-1)^{\frac{33-1}{2}\cdot\frac{17-1}{2}} \cdot \left(\frac{33}{17}\right) = \left(\frac{16}{17}\right) = \left(\frac{2^4}{17}\right) = 1$$

Ισχυρισμός: Αν $t \geq 2$, τότε $Q_{2^t} \equiv 16 \pmod{33}$ και άρα:

$$\left(\frac{Q_{2\cdot 2^t}}{33}\right) = \left(\frac{16}{33}\right) = \left(\frac{2^4}{33}\right) = 1$$

Αρκεί, για να ολοκληρωθεί η απόδειξη του λήμματος, να αποδείξουμε τον ισχυρισμό. Αυτό θα γίνει με χρήση της μαθηματικής επαγωγής. Πράγματι:

- Για $t = 2$ και με χρήση της ταυτότητας 6. έχουμε $Q_8 = 2Q_4^2 - 1 = 2 \cdot 17^2 - 1 \equiv 16 \pmod{33}$.
- Έστω ότι ισχύει για $t = l - 1$, δηλαδή $Q_{2^{l-1}} \equiv 16 \pmod{33}$.
- Εξετάζουμε για $t = l$:

  $Q_{2^{l+1}} = Q_{2\cdot 2^l} = 2Q_{2^l}^2 - (-1)^{2l} = 2Q_{2l}^2 - 1 \equiv 2{\cdot}16^2 - 1 \equiv 2{\cdot}256 - 1 \equiv 2{\cdot}25 - 1 \equiv 49 \equiv 16 \pmod{33}$

  Άρα $\forall t \geq 1$ έχουμε $\left(\frac{Q_{2k}}{33}\right) = 1$ και άρα

$$\left(\frac{8P_{2k}+1}{Q_{2k}}\right) = \left(\frac{-8P_{2k}+1}{Q_{2k}}\right)$$

□

ΛΗΜΜΑ 3.5.3: Αν $k = 2^t$ όπου $t \geq 2$ τότε $\left(\frac{8P_k+Q_k}{33}\right) = -1$.

Απόδειξη. Έχουμε $Q_4 = 3, Q_{17} = 17 \equiv -16 \pmod{33}$ και όπως είδαμε στο προηγούμενο λήμμα $Q_{2^j} \equiv 16 \pmod{33}, \forall j \geq 3$.
Έτσι, με χρήση της ταυτότητας 4. έχουμε:

$$8P_k = 8P_2(2Q_2)(2Q_4)\ldots(2Q_{2^{t-1}}) = 8 \cdot 2 \cdot 6 \cdot (\pm 1) \equiv \pm 3 \pmod{33}$$

Έτσι, $8P_k + Q_k \equiv \pm 13$ ή $19 \pmod{33}$ και άρα:

$$\left(\frac{8P_k+Q_k}{33}\right) = \left(\frac{\pm 13}{33}\right) \quad \text{ή} \quad \left(\frac{\pm 19}{33}\right) = -1$$

□

ΛΗΜΜΑ 3.5.4: Αν $n \equiv m \pmod{24}$, τότε $P_n \equiv P_m \pmod{9}$.

Απόδειξη. Κατ'αρχήν, έχουμε ότι $P_{24} = 543339720 = 9{\cdot}60371080$ και $P_{25} = 1311738121 = 9{\cdot}145748680{+}1$ και άρα $P_{24} \equiv 0 \pmod{9}$ και $P_{25} \equiv 1 \pmod{9}$. Άρα, από την ταυτότητα 2. προκύπτει:

$$P_{n+24} = P_n \cdot P_{25} + P_{n-1} \cdot P_{24} \equiv P_n \pmod{9}$$

□

ΘΕΩΡΗΜΑ 3.5.1: Ο όρος P_n είναι τρίγωνος αν και μόνον αν $n \pm 1$.

Απόδειξη. Αν $n{\pm}1$ τότε $P_{\pm 1} = 1$ που είναι τρίγωνος αριθμός. Από την 1. έχουμε ότι αν ο n είναι αρνητικός άρτιος αριθμός, τότε ο $8P_n{+}1$ είναι αρνητικός και άρα δεν μπορεί να είναι τρίγωνος (είδαμε και στην αντίστοιχη ενότητα για την ακολουθία Fibonacci ότι αν ένας φυσικός αριθμός k είναι τρίγωνος, τότε $8k + 1 = \square$). Αν ο n είναι αρνητικός περιττός, τότε $P_{-n} = P_n$ και έτσι αρκεί να δείξουμε ότι ο $8P_n + 1$ δεν είναι τέλειο τετράγωνο $\forall n \geq 2$. Θέτουμε $n = 2kg + m, k = 2^t, t \geq 1, g \geq 1$ περιττός αριθμός κι έστω, για να καταλήξουμε σε άτοπο, ότι ο P_n είναι τρίγωνος αριθμός (δηλαδή $\left(\frac{8P_n+1}{N}\right) = 1$ για κάθε περιττό θετικό αριθμό N).
Ξεχωρίζουμε τις περιπτώσεις:

- Έστω n περιττός, δηλαδή $n \equiv \pm 1 \pmod 4$.
  Τότε, με χρήση του λήμματος 3.5.1.

$$8P_n + 1 = 8P_{2kg\pm 1} + 1 \equiv -8P_{\pm 1} + 1 \equiv -8 + 1 \equiv -7 \pmod{Q_k}$$

  Ισχυρισμός: $Q_k \equiv 3 \pmod 7$. Επομένως:

$$\left(\frac{8P_n+1}{Q_k}\right) = \left(\frac{-7}{Q_k}\right) = \left(\frac{-1}{Q_k}\right)\cdot\left(\frac{7}{Q_k}\right) = (-1)^{\frac{Q_k-1}{2}}\cdot(-1)^{\frac{Q_k-1}{2}\cdot\frac{7-1}{2}}\left(\frac{Q_k}{7}\right) = \left(\frac{3}{7}\right) = -1$$

  άτοπο, αφού P_n είναι τρίγωνος και άρα $8P_n + 1 = \square$
  Η απόδειξη ισχυρισμού: $Q_{2^t} \equiv 3 \pmod 7$ θα γίνει κι αυτή επαγωγικά:

  - Για $t = 1$ έχουμε $Q_2 = 3 \equiv 3 \pmod 7$
  - Έστω ότι ισχύει για $t = k$, δηλαδή $Q_{2^k} \equiv 3 \pmod 7$.
  - Εξετάζουμε αν ισχύει για $t = k + 1$:

$$Q_{2^{k+1}} = Q_{2\cdot 2^k} \overset{(6)}{=} 2Q_{2^k}^2 - (-1)^{2k} \equiv 2\cdot 3^2 - 1 \equiv 17 \equiv 3 \pmod 7$$

- Έστω $n \equiv 2 \pmod 4$.
  Η ακολουθία $\{P_n\}_{n\in\mathbb{N}}$ είναι περιοδική $\pmod 7$ με περίοδο 6 κι έτσι, αφού υποθέσαμε ότι $\left(\frac{8P_n+1}{N}\right) = 1$ για κάθε N περιττό, έχουμε ότι $n \equiv 0 \pmod 6$. Άρα $n \equiv \pm 6 \pmod{24}$. Έτσι, από το Λήμμα 3.5.4. έχουμε:

$$8P_n + 1 \equiv 8P_{\pm 6} + 1 \equiv \pm 8P_6 + 1 \equiv 3 \quad \text{ή} \quad 8 \pmod 9.$$

  Όμως, οι κλάσεις 3 και 8 είναι τετραγωνικά ανισοϋπόλοιπα $\pmod 9$, άρα $8P_n + 1 \neq \square$, που είναι άτοπο.

- Έστω $n \equiv 0 \pmod 4$.
  Από το Λήμμα 3.5.1(ii) έχουμε $P_n \equiv P_{2k} \pmod{Q_{2k}}$ και έτσι, με χρήση του λήμματος 3.5.2. έχουμε

$$\left(\frac{8P_n+1}{Q_{2k}}\right) = \left(\frac{8P_{2k}+1}{Q_{2k}}\right).$$

  Αν $k = 2$, δηλαδή $t = 1$, έχουμε $\left(\frac{8P_{2k}+1}{Q_{2k}}\right) = \left(\frac{97}{17}\right) = -1$
  Υποθέτουμε ότι $t \geq 2$. Τότε, με χρήση των ταυτοτήτων 6. και 3. έχουμε

$$8P_{2k} + 1 \equiv 8P_{2k} + (2Q_k^2 - Q_{2k}) \equiv 2Q_k(8P_k + Q_k) \pmod{Q_{2k}}$$

  Θέτουμε $s_k = 8P_k + Q_k$. Από την 3.1 προκύπτει $s_k \equiv 1 \pmod 8$. Επομένως, από τις ταυτότητες 5. και 6.

$$\left(\frac{8P_{2k}+1}{Q_{2k}}\right) = \left(\frac{Q_k}{Q_{2k}}\right)\cdot\left(\frac{s_k}{Q_{2k}}\right) = \left(\frac{Q_{2k}}{Q_k}\right)\cdot\left(\frac{s_k}{Q_{2k}}\right)\cdot(-1)^{\frac{Q_{2k}-1}{2}\cdot\frac{Q_k-1}{2}}\cdot(-1)^{\frac{s_k-1}{2}\frac{Q_{2k}-1}{2}} =$$

$$= \left(\frac{Q_{2k}}{Q_k}\right)\cdot\left(\frac{Q_{2k}}{s_k}\right) = \left(\frac{2Q_k^2-1}{Q_k}\right)\cdot\left(\frac{2P_k^2+Q_k^2}{s_k}\right) =$$

$$= +1\cdot\left(\frac{2P_k^2+(s_k-8P_k)^2}{s_k}\right)\left(\frac{66P_k^2}{s_k}\right) = \left(\frac{33}{s_k}\right) = \left(\frac{s_k}{33}\right)\cdot(-1)^{\frac{s_k-1}{2}\cdot\frac{37-1}{2}} = \left(\frac{8P_k+Q_k}{33}\right) = -1.$$

  (η τελευταία ισότητα είναι από το Λήμμα 3.5.3.).
  Άρα $8P_n + 1 \neq \square, \forall n > 1$ και άρα $\forall n > 1$ ο P_n δεν μπορεί να είναι τρίγωνος αριθμός.

□

Τα ζευγάρια $(P_n, Q_n), n \in \mathbb{N})$ ικανοποιούν την

$$Q_n^2 - 8P_n^2 = 4 \cdot (-1)^n \tag{3.2}$$

Αυτό προκύπτει από την Ταυτότητα 1. των γενικευμένων ακολουθιών Lucas ως προς το ζευγάρι $(P, Q) = (2, -1)$ (σελίδα 26).
Οπότε αν ο P_n είναι τρίγωνος αριθμός, υπάρχει $X \in \mathbb{N}$ τέτοιος ώστε $P_n = \frac{1}{2}X(X+1)$ και άρα η (3.2) γίνεται:

$$Q_n^2 - 8\left(\frac{X(X+1)}{2}\right) = \pm 4$$

ή ισοδύναμα

$$Q_n^2 - 2X^4 - 4X^3 - 2X^2 = \pm 4.$$

Άρα το να βρούμε όλους τους τρίγωνους αριθμούς στην ακολουθία P_n ισοδυναμεί με το να βρούμε τα ακέραια σημεία των καμπυλών που ορίζονται από τις

$$Y^2 - 2X^4 - 4X^3 - 2X^2 = \pm 4.$$

Επομένως, προκύπτει το εξής πόρισμα:

ΠΟΡΙΣΜΑ 3.5.1: (i) Η εξίσωση $Y^2 - 2X^4 - 4X^3 - 2X^2 = 4$ έχει ακέραιες λύσεις τις $(x, y) = (0, \pm 2), (-1, \pm 2)$ μόνο.

(ii) Η εξίσωση $Y^2 - 2X^4 - 4X^3 - 2X^2 = -4$ έχει ακέραιες λύσεις τις $(x, y) = (1, \pm 2), (-2, \pm 2)$ μόνο.

Απόδειξη. (i) Προφανές, αφού δεν υπάρχει όρος της ακολουθίας P_n με άρτιο δείκτη που να είναι τρίγωνος αριθμός.

(ii) Η εξίσωση προέκυψε από την (3.2) με την υπόθεση ότι ο όρος P_n είναι τρίγωνος. Οι μόνοι τρίγωνοι όροι της ακολουθίας P_n είναι αυτοί με δείκτη ± 1, δηλαδή οι $P_{\pm 1} = 1$ και αφού $P_{\pm 1} = \frac{X(X+1)}{2}$, δηλαδή $1 = \frac{X(X+1)}{2}$ έχουμε ότι $X = 1$ ή $X = -2$. Για $X = 1$ προκύπτει ότι $Y = \pm 2$, ενώ για $X = -2$ προκύπτει πάλι ότι $Y = \pm 2$.

□

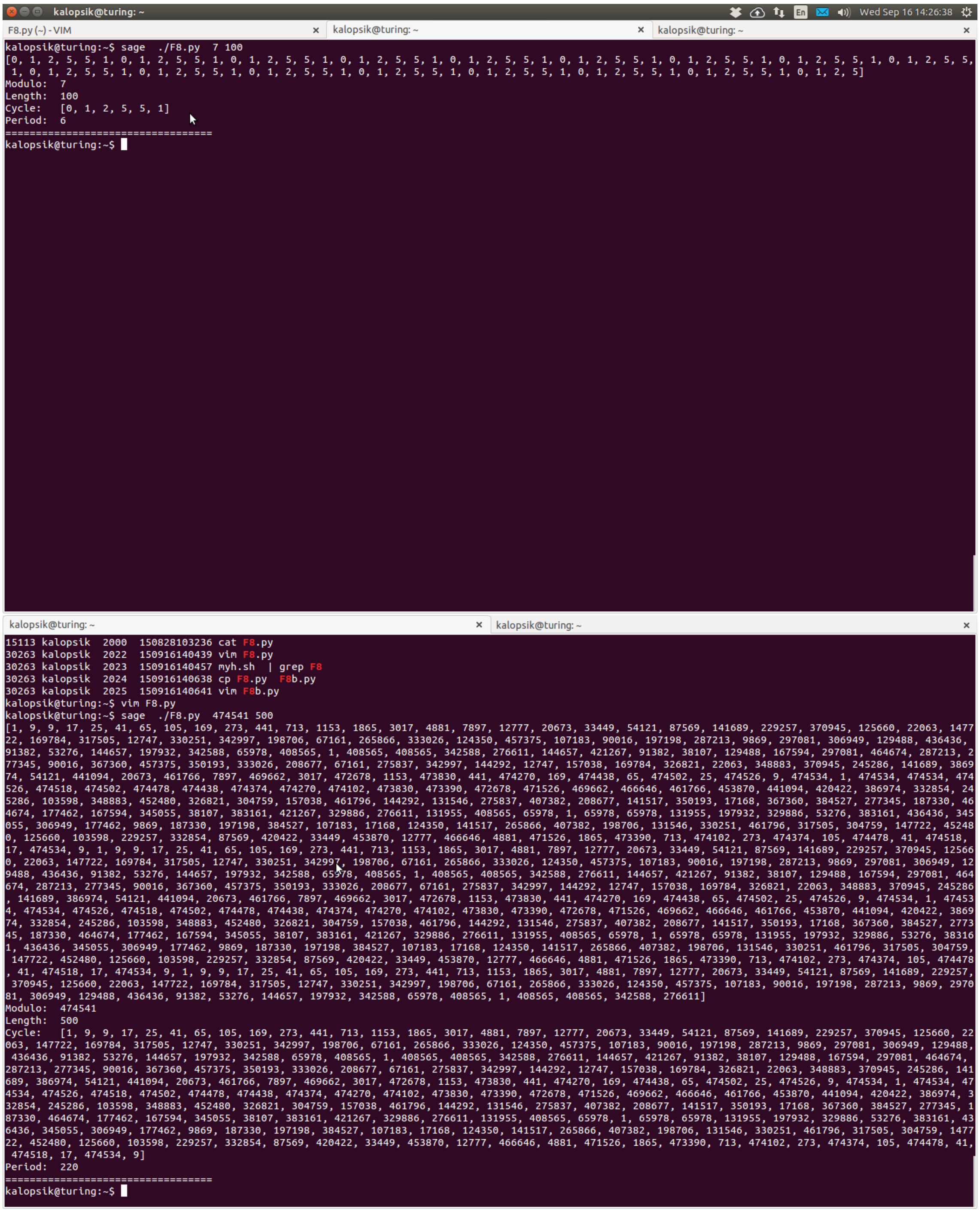
Παράρτημα

Το να υπολογίσουμε την περίοδο των ακολουθιών που προκύπτουν στις αποδείξεις των λημμάτων αυτού του κεφαλαίου είναι πολύ δύσκολο να γίνει χωρίς την χρήση υπολογιστή ή υπολογιστή τσέπης. Για το σκοπό αυτό χρησιμοποίησαμε το "SAGE" (http://www.sagemath.org/) και το πρόγραμμα που χρησιμοποιήθηκε υλοποιήθηκε στην γλώσσα προγραμματισμού Python. Το πρόγραμμα ζητάει από τον χρήστη δύο ακέραιους αριθμούς m_1 και m_2 και υπολογίζει τους πρώτους m_2 όρους καθώς και την περίοδο της ακολουθίας $k \cdot F_n + r \cdot L_n \pmod{m_1}$, όπου k και r είναι ακέραιοι αριθμοί. Ο κώδικας του πρόγραμματος είναι:

```
#!/usr/bin/python


import sys
from sage.all import *


def naive(nums):
    for x in range(2, len(nums)): # (starts at 2, assuming the sequence
        #print "L[" + str(x) + "] = " + str(nums[x])
        for y in range(0, x):
            # if x is already in numbers before it
            if nums[x] == nums[y]:
                seq = [nums[x]] # (re)start the sequence
                adder = 1       # (re)set the adder to 1
                ok = True       # (re)set ok to be True
                # while the sequence still matches (is ok) and
                # tail of y hasn't reached start of x
                while ok and y + adder < x:
                    if nums[x + adder] == nums[y + adder]:
# if next y and x match
                        seq.append(nums[x + adder])
# add the number to sequence
                        adder += 1
# increase adder
                    else:
                        ok = False
# else the sequence is broken
                # if the sequence wasn't broken and has at least 2 memb
                if ok and len(seq) > 1:
                    return seq


FibonnaciCombination = [ Mod(k*fibonacci(i)+1,sys.argv[1]) for i in xra
LucasCombination = [ Mod(lucas_number2(i,1,-1),sys.argv[1]) for i in xr
F8 = FibonnaciCombination
print F8
cycle = naive(F8)
print "Modulo: ", sys.argv[1]
```

```
print "Length: ", sys.argv[2]
print "Cycle:   ",  cycle
print "Period: ",  len(cycle)
print "=================================="
```

Στις επομένες δύο εικόνες ακολουθούν δύο παραδείγματα. Στην πρώτη εικόνα έχουμε ”τρέξει” το πρόγραμμα για την ακολουθία $P_n \pmod 7$, όπου βλέπουμε οτι είναι περιοδική με περίοδο 6, ενώ στην δεύτερη έχουμε δώσει την εντολή για την $8F_n{+}1 \pmod{474541}$ όπου βλέπουμε ότι η περίοδος είναι 220.



Βιβλιογραφία

[1] Ι. Αντωνιάδης και Α. Κοντογεώργης, *Θεωρία Αριθμών και Εφαρμογές*, Πρόγραμμα "Κάλλιπος", http://eclass.uoa.gr/modules/document/file.php/MATH443/NumberTheory21July.pdf, 2015.

[2] G.H. Hardy και E.M. Wright, *An introduction to the Theory of Numbers*, 4η έκδοση, Clarendon Press, Oxford 1959.

[3] T. Jeffery και R. Pereira, *Divisibility Properties of the Fibonacci, Lucas, and Related Sequences*, Hindawi Publishing Corporation, 2014.

[4] A.I. Markushevish, *Recursion Sequences*, Mir Publishers, Moscow 1975.

[5] W. L. McDaniel, *Triangular Numbers in the Pell Sequence*, Fibonacci Quarterly 34(2) (1996), 105-107.

[6] W. L. McDaniel, *The G.C.D. in Lucas sequences*, Fibonacci Quarterly 29 (1991), 24-29.

[7] L. Ming, *On triangular Fibonacci numbers*, Fibonacci Quarterly 27(2) (1989), 98-108.

[8] L. Ming, *On triangular Lucas numbers*, Eds. G.E. Bergum et. al., Applications of Fibonacci Numbers 4 (1991), 231-240.

[9] L. Ming, *Pentagonal Numbers in the Fibonacci Sequence*, Applications of Fibonacci Numbers 6 (1996), 349-354.

[10] P. Ribenboim και W. L. McDaniel, *Square classes of Lucas Sequences*, J. Number Theory 58 (1996), 104-123.

[11] Z. Şiar, *On square classes in generalized Lucas sequences*, International Journal of Number Theory 11 (2015), 661-672.

[12] R. Steiner, *On triangular Fibonacci Numbers*, Utilitas Mathematica 9 (1976), 319-327.