ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
(ΚΑΤΕΥΘΥΝΣΗ ΜΑΘΗΜΑΤΙΚΟΥ ΕΦΑΡΜΟΓΩΝ)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΘΕΩΡΙΑ ΣΥΝΕΧΩΝ ΚΛΑΣΜΑΤΩΝ ΚΑΙ ΕΦΑΡΜΟΓΕΣ

ΤΟΥΡΛΑΚΗ ΜΑΡΓΑΡΙΤΑ

Εξεταστική επιτροπή: ΧΡΗΣΤΟΣ ΚΟΥΚΟΥΒΙΝΟΣ
ΑΛΕΞΑΝΔΡΟΣ ΠΑΠΑΪΩΑΝΝΟΥ (επιβλέπων)
ΠΕΤΡΟΣ ΣΤΕΦΑΝΕΑΣ

Αθήνα, 2011

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
(ΚΑΤΕΥΘΥΝΣΗ ΜΑΘΗΜΑΤΙΚΟΥ ΕΦΑΡΜΟΓΩΝ)

ΘΕΩΡΙΑ ΣΥΝΕΧΩΝ ΚΛΑΣΜΑΤΩΝ
ΚΑΙ ΕΦΑΡΜΟΓΕΣ

Αθήνα, 2011

Περίληψη

Στην εργασία αυτή αρχικά στο πρώτο κεφάλαιο παρουσιάζονται τα βασικά στοιχεία της θεωρίας συνεχών κλασμάτων, που αποτελεί κομμάτι και εργαλείο της θεωρίας αριθμών.

Τα συνεχή κλάσματα αναπτύχθηκαν (ή ανακαλύφθηκαν) εν μέρει ως απάντηση μιας ανάγκης να προσεγγιστούν οι άρρητοι αριθμοί. Από τότε έχουν διακριθεί ως σημαντικά εργαλεία για προβλήματα στη θεωρία πιθανοτήτων, την ανάλυση, την κρυπτογραφία και ειδικά τη θεωρία αριθμών.

Στη συνέχεια, στο δεύτερο κεφάλαιο παρουσιάζεται η μέθοδος κρυπτογράφησης RSA ώστε στο τρίτο κεφάλαιο να κατανοηθεί καλύτερα ο αλγόριθμος του Wiener, που είναι ένας αλγόριθμος παραγοντοποίησης ακεραίων που στοχεύει στην αποκρυπτογράφηση μηνυμάτων RSA και χρησιμοποιεί την θεωρία συνεχών κλασμάτων.

Τέλος, στο ίδιο κεφάλαιο περιγράφεται και ένας άλλος ενδιαφέρον αλγόριθμος παραγοντοποίησης άμεσα συνδεδεμένος με τα συνεχή κλάσματα.

Abstract

Initially, in the first chapter of this essay are represented the principal parts of continued fraction theory, which is piece and tool of number theory.

Continued fractions were developed (or discovered) as a response to a need to approximate irrational numbers. Since then they have distinguished themselves as important tools for solving problems in probability theory, analysis, cryptography and especially number theory.

Then, in the second chapter is represented the RSA encryption in order that in the third chapter is comprehended better the Wiener algorithm, which is an algorithm of factorization that aims in decoding RSA messages and uses continued fraction theory.

Finally, in the same chapter is described another interesting factorization algorithm directly connected with continued fracions.

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 1. Συνεχή κλάσματα

1.1. Πεπερασμένα συνεχή κλάσματα……..5
1.2. Άπειρα συνεχή κλάσματα……11
1.3. Τύποι συνεχών κλασμάτων…….....15
1.4 Συγκλίνοντες ρητοί…….....17
1.5. Εύρεση λύσης διοφαντικής εξίσωσης…….....27

Κεφάλαιο 2. Το κρυπτοσύστημα RSA

2.1. Βασικά στοιχεία…….31
2.2. Θεωρήματα…….....34

Κεφάλαιο 3. Παραγοντοποίηση ακεραίων με συνεχή κλάσματα

3.1. Ο αλγόριθμος του Wiener……...35
3.2. Ένας δεύτερος αλγόριθμος.....41

ΚΕΦΑΛΑΙΟ 1

Συνεχή κλάσματα

1.1 Πεπερασμένα συνεχή κλάσματα (Finite continued fractions)

Όπως γνωρίζουμε κάθε ρητός αριθμός μπορεί να εκφραστεί σύμφωνα με τον Ευκλείδειο αλγόριθμο* όπως παρακάτω:

Έστω ο ρητός $\frac{57}{13}$. Αν κάνουμε την διαίρεση θα πάρουμε

$$57 = 13 \cdot 4 + 5 \Rightarrow \frac{57}{13} = 4 + \frac{5}{13} \Rightarrow \frac{57}{13} = 4 + \frac{1}{\frac{13}{5}}$$

Συνεχίζοντας έχουμε

$$13 = 5 \cdot 2 + 3 \Rightarrow \frac{13}{5} = 2 + \frac{3}{5} \Rightarrow \frac{13}{5} = 2 + \frac{1}{\frac{5}{3}}$$

Ομοίως

$$5 = 3 \cdot 1 + 2 \Rightarrow \frac{5}{3} = 1 + \frac{2}{3} \Rightarrow \frac{5}{3} = 1 + \frac{1}{\frac{3}{2}}$$

$$3 = 2 \cdot 1 + 1 \Rightarrow \frac{3}{2} = 1 + \frac{1}{2}$$

$$2 = 1 \cdot 2 + 0$$

* Θεώρημα διαίρεσης του Ευκλείδη: Για κάθε ακεραίους k ($k > 0$) και j υπάρχουν μοναδικοί ακέραιοι q και r με $0 \le r < k$ και $j = qk + r$.

Τελικά συνδυάζοντας τα παραπάνω παίρνουμε:

$$\frac{57}{13} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}}$$

Το κλάσμα που προκύπτει λέγεται συνεχές κλάσμα.

Ορισμός **Πεπερασμένο συνεχές κλάσμα (finite continued fraction)** ονομάζεται μία επαναλαμβανόμενη ακολουθία της μορφής

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

όπου οι μεταβλητές a_i είναι πραγματικοί αριθμοί και $a_i > 0$, για $1 \le i \le n$. Για να συμβολίσουμε ένα συνεχές κλάσμα θα χρησιμοποιούμε τον συμβολισμό που υιοθέτησε ο Dirichlet το 1854

$$[a_0,\ a_1,\ \ldots,\ a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

Αν οι μεταβλητές a_i είναι ακέραιοι αριθμοί, τότε η προκύπτουσα έκφραση ονομάζεται **απλό πεπερασμένο συνεχές κλάσμα (simple finite continued fraction)**.

Ενώ το πεπερασμένο κλάσμα της μορφής

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{\ddots + \cfrac{b_{n-1}}{a_{n-1} + \cfrac{b_n}{a_n}}}}}$$

ονομάζεται **γενικευμένο πεπερασμένο συνεχές κλάσμα (generalized finite continued fraction).**

ΘΕΩΡΗΜΑ *Κάθε ρητός αριθμός μπορεί να εκφραστεί σαν απλό πεπερασμένο συνεχές κλάσμα και κάθε απλό πεπερασμένο συνεχές κλάσμα αναπαριστά έναν ρητό αριθμό.*

Απόδειξη

Ένα απλό πεπερασμένο συνεχές κλάσμα μήκους ένα παριστάνει έναν ακέραιο αριθμό και κατά συνέπεια ρητό. Ας υποθέσουμε τώρα ότι κάθε απλό πεπερασμένο συνεχές κλάσμα με k όρους είναι ρητός και έστω το κλάσμα $[a_1, a_2, \ldots, a_k, a_{k+1}]$. Έχουμε

$[a_1, a_2, \ldots, a_k, a_{k+1}] = a_1 + \dfrac{1}{[a_2, \ldots, a_k, \alpha_{k+1}]}$ που είναι το άθροισμα δύο ρητών,

οπότε το $[a_1, a_2, \ldots, a_k, a_{k+1}]$ είναι ρητός αριθμός.

Αντίστροφα, έστω ο ρητός $\dfrac{a}{b}$ με $b > 0$. Από τον Ευκλείδειο αλγόριθμο συμπεραίνουμε ότι

$a = bq_1 + r_1$, όπου $0 \le r_1 < b$

$b = r_1q_2 + r_2$, όπου $0 \le r_2 < r_1$

$r_1 = r_2q_3 + r_3$, όπου $0 \le r_3 < r_2$

…

$r_{n-2} = r_{n-1}q_n + r_n$, όπου $0 \le r_n < r_{n-1}$

$r_{n-1} = r_nq_{n+1}$

Διαιρώντας κατάλληλα έχουμε

$$\frac{a}{b} = q_1 + \frac{r_1}{b} = q_1 + \frac{1}{\frac{b}{r_1}}$$

$$\frac{b}{r_1} = q_2 + \frac{r_2}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}}$$

$$\frac{r_1}{r_2} = q_3 + \frac{r_3}{r_2} = q_3 + \frac{1}{\frac{r_2}{r_3}}$$

$$\dots$$

$$\frac{r_{n-1}}{r_n} = q_{n+1}$$

Ο πολλαπλασιαστικός αντίστροφος του τελευταίου κλάσματος της k-στης σειράς είναι ο πρώτος όρος στην $(k+1)$ σειρά. Έτσι, με αντικατάσταση, λαμβάνουμε:

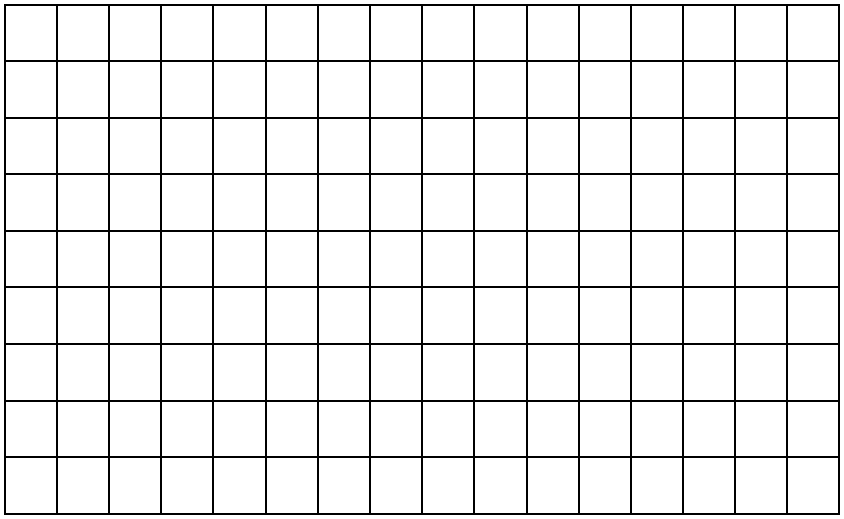
$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_n + \cfrac{1}{q_{n+1}}}}}}$$

Αυτό σημαίνει $\frac{a}{b} = [q_1,\ q_2,\ \dots,\ q_{n+1}]$. Δηλαδή εκφράσαμε έναν τυχαίο ρητό σε μορφή απλού πεπερασμένου συνεχούς κλάσματος.

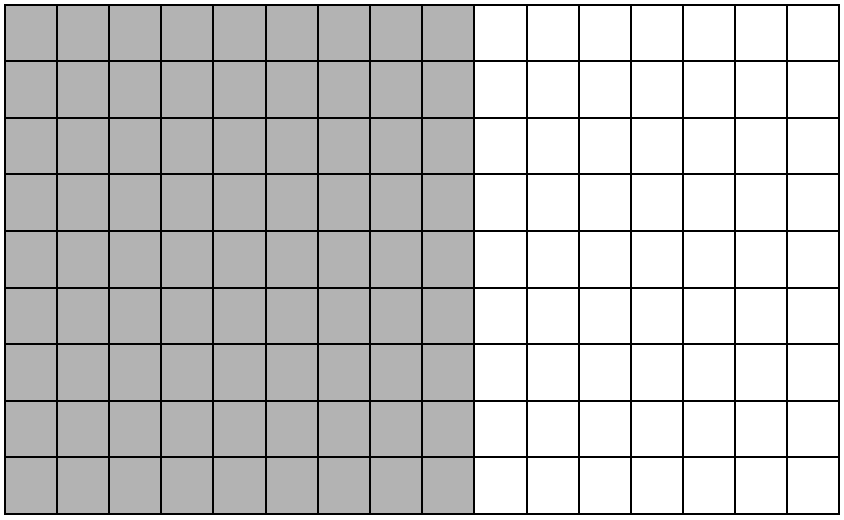
<u>Ένας γραφικός τρόπος εύρεσης του συνεχούς κλάσματος ρητού αριθμού (που είναι μικρότερος από τη μονάδα)</u>.

Θα εκφράσουμε ως συνεχές κλάσμα τον αριθμό $\frac{9}{16}$.

Φτιάχνουμε ένα πλέγμα που αποτελείται από 16 τετράγωνα οριζοντίως και 9 τετράγωνα καθέτως.



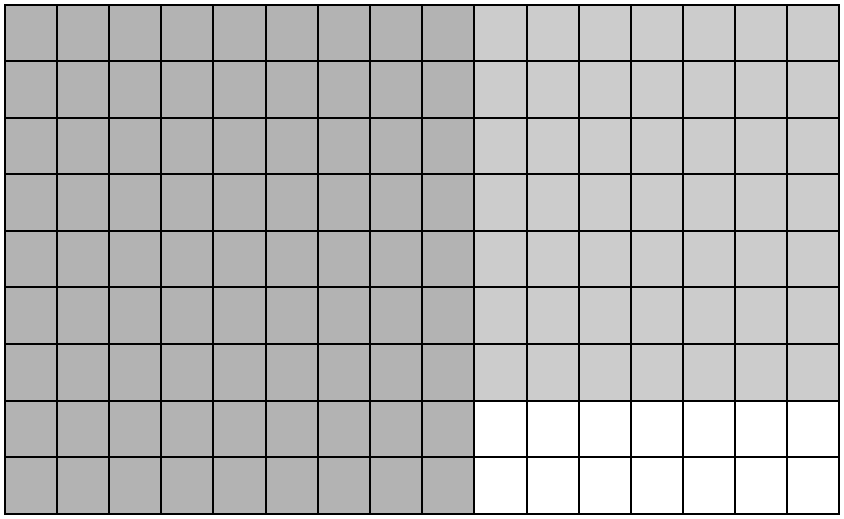
Σχεδιάζουμε το μεγαλύτερο τετράγωνο που μπορούμε σ' αυτό το πλέγμα.



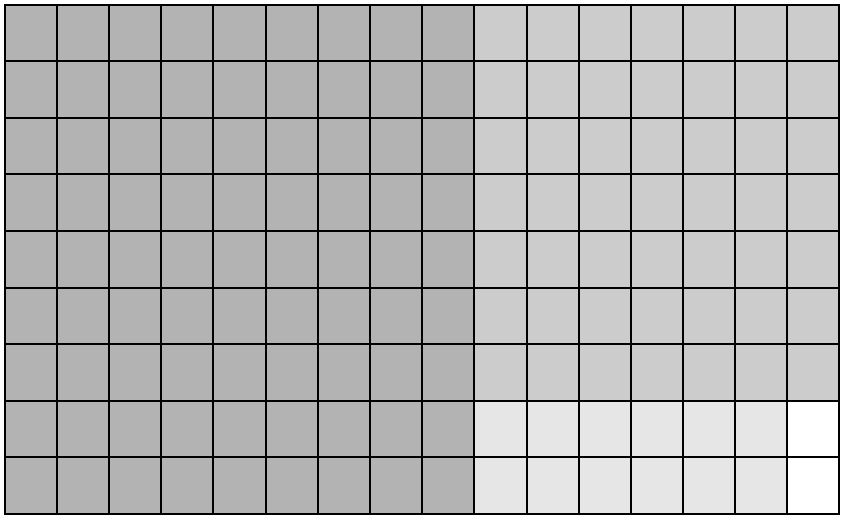
Ο αριθμός των τετραγώνων αυτού του μεγέθους είναι το a_1 του συνεχούς κλάσματος. Εδώ μπορούμε να σχεδιάσουμε 1 τετράγωνο 9×9, άρα $a_1 = 1$.

Μας έχει μείνει ένα ορθογώνιο 7×9 και επαναλαμβάνουμε την διαδικασία. Σχεδιάζουμε το μεγαλύτερο τετράγωνο που μπορούμε. Αυτό είναι ένα τετράγωνο 7×7 και πάλι μπορούμε να σχεδιάσουμε ένα μόνο. Συνεπώς $a_2 = 1$.

Τώρα έχει μείνει ένα ορθογώνιο 7×2.



Εδώ τώρα μπορούμε να σχεδιάσουμε 3 τετράγωνα 2×2.



Οπότε $a_3 = 3$. Στον εναπομείναντα χώρο μπορούμε να σχεδιάσουμε 2 τετράγωνα 1×1, δηλαδή $a_4 = 2$.

Τελικά

$$\frac{9}{16} = [0,1,1,3,2]$$

ή $$\frac{9}{16} = 0 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{2}}}}.$$

1.2 Άπειρα συνεχή κλάσματα (Infinite continued fractions)

Και ένας άρρητος μπορεί να εκφραστεί σαν συνεχές κλάσμα. Παραδείγματος χάριν, έστω ο άρρητος $\sqrt{2}$. Είναι

$$\sqrt{2}=1+(\sqrt{2}-1)=1+\frac{1}{\frac{1}{\sqrt{2}-1}}=1+\frac{1}{\frac{\sqrt{2}+1}{(\sqrt{2}-1)(\sqrt{2}+1)}}=1+\frac{1}{\sqrt{2}+1}=1+\frac{1}{2+(\sqrt{2}-1)}=$$

$$=1+\frac{1}{2+\frac{1}{\sqrt{2}+1}}=1+\frac{1}{2+\frac{1}{2+\frac{1}{\sqrt{2}+1}}}=1+\frac{1}{2+\frac{1}{2+\frac{1}{2+\ddots}}}$$

και η διαδικασία συνεχίζεται χωρίς τέλος. Δηλαδή $\sqrt{2}=[1,\ 2,\ 2,\ 2,\ ...]$.

Ας υποθέσουμε τώρα ότι θέλουμε να βρούμε την θετική ρίζα της εξίσωσης

$$x^2-x-2=0$$

που είναι ο αριθμός 2. Γράφουμε τώρα την εξίσωση ως εξής

$$x^2=x+2$$

και διαιρώντας με x (αφού x θετικός) παίρνουμε

$$x=1+\frac{2}{x}$$

και εφόσον $x=2$, λαμβάνουμε $2=1+\frac{2}{x}$. Αντικαθιστώντας το x ξανά έχουμε ότι

$$2=1+\frac{2}{1+\frac{2}{x}}$$

Τελικά επαναλαμβάνοντας άπειρες φορές

$$2=1+\frac{2}{1+\frac{2}{1+\frac{2}{1+\ddots}}}$$

Το πρώτο συνεχές κλάσμα καταγράφηκε από τον Άγγλο μαθηματικό Lord Brouncker (1620 – 1684) και είναι το παρακάτω

$$\frac{\pi}{4}=\cfrac{1}{1+\cfrac{1^2}{2+\cfrac{3^2}{2+\cfrac{5^2}{2+\cfrac{7^2}{2+\cfrac{9^2}{2+\ddots}}}}}}$$

Ο e αναπαρίσταται σαν συνεχές κλάσμα ως εξής

$$e=2+\cfrac{2}{2+\cfrac{3}{3+\cfrac{4}{4+\cfrac{5}{5+\ddots}}}}=1+\cfrac{1}{0+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\ddots}}}}}}}$$

Ορισμός **Άπειρο συνεχές κλάσμα (infinite continued fraction)** ονομάζεται μία έκφραση της μορφής

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ddots}}}$$

όπου οι μεταβλητές a_i, για $i=0, 1, \ldots$, εκτός από την a_0 που μπορεί να είναι αρνητική, είναι θετικοί πραγματικοί αριθμοί. Συμβολίζεται $[a_0, a_1, a_2, \ldots]$. Αν οι μεταβλητές a_i, για $i\geq 0$, είναι ακέραιοι τότε η έκφραση λέγεται απλό άπειρο συνεχές κλάσμα (simple infinite continued fraction). Όπως τα απλά πεπερασμένα συνεχή κλάσματα αναπαριστούν ρητούς αριθμούς, τα απλά άπειρα συνεχή κλάσματα αναπαριστούν άρρητους αριθμούς.

Γενικευμένο άπειρο συνεχές κλάσμα (generalized infinite continued fraction) λέγεται ένα κλάσμα της μορφής

$$a_0+\cfrac{b_1}{a_1+\cfrac{b_2}{a_2+\cfrac{b_3}{a_3+\cfrac{b_4}{\ddots}}}}$$

ΘΕΩΡΗΜΑ (Σύνδεση συνεχών κλασμάτων με σειρές) *Έστω* $a_1, a_2, a_3, \ldots$ *μη μηδενικοί πραγματικοί αριθμοί με* $a_k \neq a_{k-1}$ *για όλα τα* k. *Τότε για κάθε* $n \in \mathbb{N}$ *ισχύει*

$$\sum_{k=1}^{n}\frac{(-1)^{k-1}}{a_k}=\cfrac{1}{a_1+\cfrac{a_1^2}{a_2-a_1+\cfrac{a_2^2}{\alpha_3-\alpha_2+\cfrac{\alpha_3^2}{\ddots+\cfrac{\alpha_{n-1}^2}{a_n-a_{n-1}}}}}}$$

Ειδικότερα, για $n\to\infty$ *παίρνουμε*

$$\sum_{k=1}^{\infty}\frac{(-1)^{k-1}}{a_k}=\cfrac{1}{a_1+\cfrac{a_1^2}{a_2-a_1+\cfrac{a_2^2}{\alpha_3-\alpha_2+\cfrac{\alpha_3^2}{a_4-a_3+\cfrac{a_4^2}{\ddots}}}}}$$

Απόδειξη

Για την απόδειξη θα εφαρμόσουμε την μέθοδο της μαθηματικής επαγωγής. Το θεώρημα προφανώς ισχύει για $n=1$. Έστω τώρα ότι ισχύει για την τιμή n. Θα δείξουμε ότι ισχύει και για την τιμή $n+1$. Έχουμε

$$\begin{aligned}\sum_{k=1}^{n+1}\frac{(-1)^{k-1}}{a_k}&=\frac{1}{a_1}-\frac{1}{a_2}+\cdots+\frac{(-1)^{n-1}}{a_n}+\frac{(-1)^n}{a_{n+1}}\\&=\frac{1}{a_1}-\frac{1}{a_2}+\cdots+(-1)^{n-1}\left(\frac{1}{a_n}-\frac{1}{a_{n+1}}\right)\\&=\frac{1}{a_1}-\frac{1}{a_2}+\cdots+(-1)^{n-1}\left(\frac{a_{n+1}-a_n}{a_n\cdot a_{n+1}}\right)\end{aligned}$$

$$= \frac{1}{a_1} - \frac{1}{a_2} + \cdots + (-1)^{n-1} \frac{1}{\frac{a_n \cdot a_{n+1}}{a_{n+1} - a_n}}$$

Αυτό είναι ένα άθροισμα n όρων κα σύμφωνα με την υπόθεση που κάναμε μπορούμε να γράψουμε

$$\sum_{k=1}^{n+1} \frac{(-1)^{k-1}}{a_k} = \cfrac{1}{a_1 + \cfrac{a_1^2}{a_2 - a_1 + \cfrac{a_3^2}{\ddots + \cfrac{a_{n-1}^2}{\frac{a_n \cdot a_{n+1}}{a_{n+1} - a_n} - a_{n-1}}}}}} \qquad (1)$$

Όμως

$$\begin{aligned} \frac{a_n \cdot a_{n+1}}{a_{n+1} - a_n} - a_{n-1} &= \frac{a_n \cdot a_{n+1} - a_n^2 + a_n^2}{a_{n+1} - a_n} - a_{n-1} \\ &= \frac{a_n (a_{n+1} - a_n) + a_n^2}{a_{n+1} - a_n} - a_{n-1} \\ &= a_n - a_{n-1} + \frac{a_n^2}{a_{n+1} - a_n} \end{aligned}$$

Οπότε αντικαθιστώντας στην (1) παίρνουμε

$$\sum_{k=1}^{n+1} \frac{(-1)^{k-1}}{a_k} = \cfrac{1}{a_1 + \cfrac{a_1^2}{a_2 - a_1 + \cfrac{a_3^2}{\ddots + \cfrac{a_{n-1}^2}{a_n - a_{n-1} + \cfrac{a_n^2}{a_{n+1} - a_n}}}}}$$

που μας δίνει το ζητούμενο. Δ

<u>Παράδειγμα</u>

Γνωρίζουμε ότι $\log 2 = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} = \frac{1}{1} - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots$ και θέτοντας $a_k = k$ μπορούμε να γράψουμε $\log 2 = \cfrac{1}{1 + \cfrac{1^2}{1 + \cfrac{2^2}{1 + \cfrac{3^2}{1 + \cfrac{4^2}{\ddots}}}}}$

ΘΕΩΡΗΜΑ *Για κάθε ακολουθία πραγματικών αριθμών* $a_1, a_2, a_3, \ldots$ *με* $a_k \neq 0,1$ *έχουμε*

$$\sum_{k=1}^{n} \frac{(-1)^{k-1}}{a_1 \cdots a_k} = \cfrac{1}{a_1 + \cfrac{a_1}{a_2 - 1 + \cfrac{a_2}{a_3 - 1 + \cfrac{a_3}{\ddots + \cfrac{a_{n-1}}{a_n - 1}}}}}$$

Ειδικότερα, για $n \to \infty$ *έχουμε*

$$\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{a_1 \cdots a_k} = \cfrac{1}{a_1 + \cfrac{a_1}{a_2 - 1 + \cfrac{a_2}{a_3 - 1 + \cfrac{a_3}{a_4 - 1 + \cfrac{a_4}{\ddots}}}}}$$

1.3 Τύποι συνεχών κλασμάτων

1. Το συνεχές κλάσμα τύπου Stieltjes (Stieltjes fraction) (Thomas Joannes Stieltjes 1856 – 1894, Ολλανδός μαθηματικός) είναι της μορφής

$$\cfrac{1}{a_1 z + \cfrac{1}{a_2 + \cfrac{1}{a_3 z + \cfrac{1}{\ddots + \cfrac{1}{a_{2n} + \cfrac{1}{a_{2n+1} z + \ddots}}}}}}$$

όπου $a_k \in \mathbb{R}^+$, $k = 1,\ 2,\ 3,\ \ldots$

Αν θέσουμε $b_0 = \frac{1}{a_1}$ και $b_n = \frac{1}{a_n a_{n+1}}$ με $n \geq 1$ και $z = \frac{1}{t}$ μπορεί να γραφεί στην μορφή

$$\cfrac{b_0}{z+\cfrac{b_1}{1+\cfrac{b_2}{z+\cfrac{b_3}{1+\cfrac{b_4}{\ddots}}}}} = \cfrac{b_0}{1+\cfrac{b_1 t}{1+\cfrac{b_2 t}{1+\cfrac{b_3 t}{1+\cfrac{b_4 t}{\ddots}}}}}$$

όπου $b_k > 0$, $k = 1, 2, 3, \ldots$

2. Το συνεχές κλάσμα τύπου Jacobi (Jacobi fraction) (Carl Gustav Jacob Jacobi 1804 – 1851, Γερμανός μαθηματικός) είναι της μορφής

$$\cfrac{\lambda_0}{z+a_1-\cfrac{\lambda_1}{z+a_2-\cfrac{\lambda_2}{z+a_3-\cfrac{\lambda_3}{z+a_4-\ddots}}}}$$

3. Το συνεχές κλάσμα τύπου Euler. Ο Euler (Leonhard Euler 1707 – 1783, Ελβετός μαθηματικός και φυσικός) παρήγαγε τον τύπο ως ταυτότητα που συνδέει ένα πεπερασμένο άθροισμα παραγόντων με ένα πεπερασμένο συνεχές κλάσμα

$$a_0 + a_0 a_1 + a_0 a_1 a_2 + \cdots + a_0 a_1 a_2 \cdots a_n = \cfrac{a_0}{1-\cfrac{a_1}{1+a_1-\cfrac{a_2}{1+a_2-\cfrac{a_3}{\ddots-\cfrac{a_{n-1}}{1+a_{n-1}-\cfrac{a_n}{1+a_n}}}}}}$$

Επίσης ο Euler έδειξε ότι

$$\pi = 3+\cfrac{1^2}{6+\cfrac{3^2}{6+\cfrac{5^2}{6+\cfrac{7^2}{6+\ddots}}}}$$

4. Ο Gauss (Johann Carl Friedrich Gauss 1777 – 1855, Γερμανός μαθηματικός) το 1812 έδειξε ότι η υπερβολική εφαπτομένη εκφράζεται σαν συνεχές κλάσμα ως εξής

$$\tanh x = \cfrac{x}{1+\cfrac{x^2}{3+\cfrac{x^2}{5+\cfrac{x^2}{\ddots}}}}$$

5. Ο τύπος του Perron (Oscar Perron 1880 – 1975, Γερμανός μαθηματικός γνωστός για το βιβλίο του στα συνεχή κλάσματα Die Lehre von den Kettenbrüchen - 1913)

$$\int_0^z \frac{t^\mu}{1+t}\,dt = \cfrac{z}{\mu+1+\cfrac{(\mu+1)^2 z}{(\mu+2)-(\mu+1)z+\cfrac{(\mu+2)^2 z}{(\mu+3)-(\mu+2)z+\cfrac{(\mu+3)^2 z}{\ddots}}}}$$

6. Το συνεχές κλάσμα τύπου Rogers – Ramanujan (Srinivasa Ramanujan 1887 – 1920, Ινδός μαθηματικός και Leonard James Rogers 1862 – 1933, Άγγλος μαθηματικός)

$$1+\cfrac{q}{1+\cfrac{q^2}{1+\cfrac{q^3}{1+\cfrac{q^4}{\ddots}}}} = 1+q-q^3+q^5-\ldots$$

1.4 Συγκλίνοντες ρητοί

Έστω ένας πραγματικός αριθμός θ. Η αναπαράσταση του θ σε συνεχές κλάσμα είναι $\theta = [a_0,\ a_1,\ \ldots,\ a_n]$ ή $\theta = [a_0,\ a_1,\ \ldots,\ a_n,\ \ldots]$.

Συμβολικά

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{\theta_n}}}}}$$

Ο αριθμός $[a_0,\ a_1,\ \ldots,\ a_n]$ λέγεται **n-οστός συγκλίνων** ρητός στο θ. Έστω

$$\frac{p_n}{q_n} = [a_0,\ a_1,\ \ldots,\ a_n]$$

όπου p_n, q_n είναι ακέραιοι πρώτοι μεταξύ τους και $q_n > 0$.

ΠΡΟΤΑΣΗ 1 Ισχύουν οι αναγωγικοί τύποι:

$$p_n = a_n p_{n-1} + p_{n-2} \ \ (n \geq 2) \ \text{με} \ \ p_0 = a_0,\ \ p_1 = a_0 a_1 + 1$$

$$q_n = a_n q_{n-1} + q_{n-2} \ \ (n \geq 2) \ \text{με} \ \ q_0 = 1,\ \ q_1 = a_1$$

Απόδειξη

Για $n = 0$: $\frac{p_0}{q_0} = [a_0] \ \Rightarrow \ p_0 = a_0$ και $q_0 = 1$

Για $n = 1$: $\frac{p_1}{q_1} = [a_0, a_1] \ \Rightarrow \ \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} \ \Rightarrow \ p_1 = a_0 a_1 + 1$ και $q_1 = a_1$

Έστω ότι οι τύποι ισχύουν για $n = m - 1 \geq 2$. Θα δείξουμε ότι ισχύουν και για $n + 1 = m$. Έστω ακέραιοι r_j, s_j πρώτοι μεταξύ τους τέτοιοι ώστε

$$\frac{r_j}{s_j} = [a_1,\ a_2,\ \ldots,\ a_{j+1}],\ \ j = 0,\ 1,\ \ldots$$

Εφαρμόζουμε τους τύπους για τους r_j, s_j και έχουμε

$$r_{m-1} = a_m r_{m-2} + r_{m-3}$$

$$s_{m-1} = a_m s_{m-2} + s_{m-3}$$

Επίσης

$$\frac{p_j}{q_j} = [a_0,\ a_1,\ \ldots,\ a_j] = a_0 + \frac{1}{[a_1,\ \ldots,\ a_j]} = a_0 + \frac{1}{\frac{r_{j-1}}{s_{j-1}}}$$

και επειδή οι r_{j-1}, s_{j-1} είναι πρώτοι μεταξύ τους συνεπάγεται ότι

$$p_j = a_0 r_{j-1} + s_{j-1} \text{ και } q_j = r_{j-1}$$

Τώρα θέτουμε $j = m$ και παίρνουμε

$$p_m = a_0 r_{m-1} + s_{m-1} \Rightarrow p_m = a_0(a_m r_{m-2} + r_{m-3}) + a_m s_{m-2} + s_{m-3}$$

$$\Rightarrow p_m = a_m(a_0 r_{m-2} + s_{m-2}) + a_0 r_{m-3} + s_{m-3}$$

$$q_m = r_{m-1} \Rightarrow q_m = a_m r_{m-2} + r_{m-3}$$

Όμως για $j = m-1$

$$p_{m-1} = a_0 r_{m-2} + s_{m-2}$$

$$q_{m-1} = r_{m-2}$$

Και για $j = m-2$

$$p_{m-2} = a_0 r_{m-3} + s_{m-3}$$

$$q_{m-2} = r_{m-3}$$

Οπότε τελικά

$$p_m = a_m p_{m-1} + p_{m-2}$$

$$q_m = a_m q_{m-1} + q_{m-2}$$

ΠΡΟΤΑΣΗ 2 Για κάθε $n \in \mathbb{N}$ ισχύει

$i)$ $p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}$

$ii)$ $p_n q_{n+2} - p_{n+2} q_n = (-1)^{n+1} a_{n+2}$

Απόδειξη

$i)$ Θα αποδείξουμε την ισότητα με επαγωγή.

Για $n = 0$: $p_0 q_1 - p_1 q_0 = a_0 a_1 - (a_0 a_1 + 1) = -1$, ισχύει.

Υποθέτουμε ότι η ισότητα ισχύει για n. Θα δείξουμε ότι ισχύει και για $n+1$. Δηλαδή θα δείξουμε ότι $p_{n+1}q_{n+2} - p_{n+2}q_{n+1} = (-1)^{n+2}$. Από την προηγούμενη πρόταση έχουμε ότι

$$p_{n+1}q_{n+2} - p_{n+2}q_{n+1} = p_{n+1}(a_{n+2}q_{n+1} + q_n) - (a_{n+2}p_{n+1} + p_n) =$$
$$= (-1)(-1)^{n+1} = (-1)^{n+2}$$
$$= (-1)(-1)^{n+1} = (-1)^{n+2}$$

$ii)$ Χρησιμοποιώντας πάλι την προηγούμενη πρόταση παίρνουμε

$$p_nq_{n+2} - p_{n+2}q_n = p_n(a_{n+2}q_{n+1} + q_n) - (a_{n+2}p_{n+1} + p_n)q_n =$$
$$= p_na_{n+2}q_{n+1} - a_{n+2}p_{n+1}q_n = a_{n+2}(p_nq_{n+1} - p_{n+1}q_n)$$

Τώρα σύμφωνα με το $i)$ έχουμε

$$p_nq_{n+2} - p_{n+2}q_n = a_{n+2}(-1)^{n+1}$$

<u>Πόρισμα1</u> Για κάθε $k,\ l \in \mathbb{N}$ ισχύουν οι ανισότητες

$i)$ $\dfrac{p_{2k}}{q_{2k}} < \dfrac{p_{2k+2}}{q_{2k+2}}$

$ii)$ $\dfrac{p_{2l+1}}{q_{2l+1}} > \dfrac{p_{2l+3}}{q_{2l+3}}$

$iii)$ $\dfrac{p_{2k}}{q_{2k}} < \dfrac{p_{2l+1}}{q_{2l+1}}$

Απόδειξη

$i)$ Θα χρησιμοποιήσουμε την δεύτερη ισότητα της προηγούμενης πρότασης για $n = 2k,\ k \in \mathbb{N}$

$p_{2k}q_{2k+2} - p_{2k+2}q_{2k} = (-1)^{2k+1}a_{2k+2} = -a_{2k+2} \Rightarrow p_{2k}q_{2k+2} - p_{2k+2}q_{2k} < 0 \Rightarrow$

$\Rightarrow p_{2k}q_{2k+2} < p_{2k+2}q_{2k} \Rightarrow \dfrac{p_{2k}}{q_{2k}} < \dfrac{p_{2k+2}}{q_{2k+2}}$

$ii)$ Όπως πριν για $n = 2l+1,\ l \in \mathbb{N}$ παίρνουμε

$$p_{2l+1}q_{2l+3} - p_{2l+3}q_{2l+1} = (-1)^{2l+2}a_{2l+3} = a_{2l+3} \Rightarrow p_{2l+1}q_{2l+3} - p_{2l+3}q_{2l+1} > 0 \Rightarrow$$

$$\Rightarrow p_{2l+1}q_{2l+3} > p_{2l+3}q_{2l+1} \Rightarrow \frac{p_{2l+1}}{q_{2l+1}} > \frac{p_{2l+3}}{q_{2l+3}}$$

iii) Ομοίως από την πρώτη ισότητα της προηγούμενης πρότασης μπορούμε να συμπεράνουμε ότι

$$\frac{p_{2k}}{q_{2k}} < \frac{p_{2k+1}}{q_{2k+1}}$$

Οπότε

$$\frac{p_{2k}}{q_{2k}} < \frac{p_{2k+2l}}{q_{2k+2l}} < \frac{p_{2k+2l+1}}{q_{2k+2l+1}} < \frac{p_{2l+1}}{q_{2l+1}}$$

ΠΡΟΤΑΣΗ 3 Για κάθε φυσικό $n \geq 1$ ισχύει

$$\theta = \frac{p_n\theta_{n+1} + p_{n-1}}{q_n\theta_{n+1} + q_{n-1}}$$

Απόδειξη

Θα αποδείξουμε την πρόταση με επαγωγή. Από την πρόταση 1 για $n = 1$, έχουμε

$$\theta = [a_0, a_1, \theta_2] = \frac{(a_0a_1 + 1)\theta_2 + \alpha_0}{a_1\theta_2 + 1} = \frac{p_1\theta_2 + p_0}{q_1\theta_2 + q_0}$$

Έστω τώρα $n \geq 2$ και έστω ότι η ισότητα που θέλουμε να αποδείξουμε ισχύει για $n = k$,

δηλαδή $\theta = \frac{p_k\theta_{k+1} + p_{k-1}}{q_k\theta_{k+1} + q_{k-1}}$. Θα δείξουμε ότι ισχύει και για $n = k+1$, δηλαδή θα δείξουμε ότι $\theta = \frac{p_{k+1}\theta_{k+2} + p_k}{q_{k+1}\theta_{k+2} + q_k}$.

Από την υπόθεση που κάναμε παίρνουμε $\theta = \frac{p_k\theta_{k+1} + p_{k-1}}{q_k\theta_{k+1} + q_{k-1}}$. Από τον ορισμό του συνεχούς κλάσματος έχουμε ότι $\theta_k = a_k + \frac{1}{\theta_{k+1}}$. Άρα

$$\theta = \frac{p_k(a_{k+1} + \frac{1}{\theta_{k+2}}) + p_{k-1}}{q_k(a_{k+1} + \frac{1}{\theta_{k+2}}) + q_{k-1}} = \frac{p_k a_{k+1} + \frac{p_k}{\theta_{k+2}} + p_{k-1}}{q_k a_{k+1} + \frac{q_k}{\theta_{k+2}} + q_{k-1}} = \frac{p_k a_{k+1}\theta_{k+2} + p_k + p_{k-1}\theta_{k+2}}{q_k a_{k+1}\theta_{k+2} + q_k + q_{k-1}\theta_{k+2}} =$$

$$= \frac{(p_k a_{k+1} + p_{k-1})\theta_{k+2} + p_k}{(q_k a_{k+1} + q_{k-1})\theta_{k+2} + q_k} = \frac{p_{k+1}\theta_{k+2} + p_k}{q_{k+1}\theta_{k+2} + q_k}.$$

ΠΡΟΤΑΣΗ 4 Ισχύουν

$$i)\ \frac{p_0}{q_0} < \frac{p_2}{q_2} < \ldots < \frac{p_{2k}}{q_{2k}} < \ldots < \theta < \ldots < \frac{p_{2k+1}}{q_{2k+1}} < \ldots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

$$ii)\ \left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n^{\,2}}$$

Απόδειξη

$i)$ Από την πρόταση 3 παίρνουμε

$$\theta - \frac{p_n}{q_n} = \frac{p_n\theta_{n+1} + p_{n-1}}{q_n\theta_{n+1} + q_{n-1}} - \frac{p_n}{q_n} = \frac{(p_n\theta_{n+1} + p_{n-1})q_n - p_n(q_n\theta_{n+1} + q_{n-1})}{(q_n\theta_{n+1} + q_{n-1})q_n} = \frac{p_{n-1}q_n - p_n q_{n-1}}{(q_n\theta_{n+1} + q_{n-1})q_n}$$

και τώρα από την πρόταση 2

$$\theta - \frac{p_n}{q_n} = \frac{(-1)^n}{(q_n\theta_{n+1} + q_{n-1})q_n}$$

Επειδή οι αριθμοί q_n, θ_{n+1}, q_{n-1} $(n \geq 0)$ είναι θετικοί από το πόρισμα 1(για $n = 2k$ και $n = 2k+1$) προκύπτει

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \ldots < \frac{p_{2k}}{q_{2k}} < \ldots < \theta < \ldots < \frac{p_{2k+1}}{q_{2k+1}} < \ldots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

$ii)$ Για $n \geq 1$

$$\left|\theta-\frac{p_n}{q_n}\right|=\frac{1}{(q_n\theta_{n+1}+q_{n-1})q_n}=\frac{1}{{q_n}^2\theta_{n+1}+q_{n-1}q_n}<\frac{1}{{q_n}^2}\,.$$

ΠΡΟΤΑΣΗ 5 Έστω $\theta>1$ πραγματικός αριθμός του οποίου η ανάπτυξη σε συνεχές κλάσμα έχει n-οστό συγκλίνων ρητό στο θ το $\frac{p_n}{q_n}$. Τότε για κάθε n ισχύει $\left|{p_n}^2-\theta^2{q_n}^2\right|<2\theta$.

Απόδειξη

Έχουμε

$$\left|{p_n}^2-\theta^2{q_n}^2\right|={q_n}^2\left|\theta-\frac{p_n}{q_n}\right|\left|\theta+\frac{p_n}{q_n}\right|$$

· Αν n άρτιος, τότε από την προηγούμενη πρόταση

$\frac{p_n}{q_n}<\theta<\frac{p_{n+1}}{q_{n+1}}$ και $0<\left|\theta-\frac{p_n}{q_n}\right|<\frac{1}{{q_n}^2}$.

Δηλαδή

$$\left|{p_n}^2-\theta^2{q_n}^2\right|<{q_n}^2\frac{1}{{q_n}^2}\left|\theta+\frac{p_n}{q_n}\right|=\left|\theta+\frac{p_n}{q_n}\right|=\theta+\frac{p_n}{q_n}<2\theta\text{, αφού }\theta>1.$$

· Αν n περιττός, τότε

$$\frac{p_{n+1}}{q_{n+1}}<\theta<\frac{p_n}{q_n}\Rightarrow\frac{p_{n+1}}{q_{n+1}}-\frac{p_n}{q_n}<\theta-\frac{p_n}{q_n}<0\Rightarrow\left|\theta-\frac{p_n}{q_n}\right|<\left|\frac{p_{n+1}}{q_{n+1}}-\frac{p_n}{q_n}\right|=\left|\frac{p_{n+1}q_n-p_nq_{n+1}}{q_{n+1}q_n}\right|$$

Από την πρόταση 2

$$\left|\theta-\frac{p_n}{q_n}\right|<\left|\frac{-(-1)^{n+1}}{q_{n+1}q_n}\right|=\frac{1}{q_{n+1}q_n}$$

Άρα

$$\left|{p_n}^2-\theta^2{q_n}^2\right|<{q_n}^2\frac{1}{q_{n+1}q_n}\left|\theta+\frac{p_n}{q_n}\right|=\frac{q_n}{q_{n+1}}\left|\theta+\frac{p_n}{q_n}\right|=\frac{q_n}{q_{n+1}}(\theta+\frac{p_n}{q_n})\ (*)$$

Όμως

$$\frac{p_n}{q_n}-\frac{p_{n+1}}{q_{n+1}}=\frac{1}{q_{n+1}q_n}\Rightarrow\frac{p_n}{q_n}-\frac{1}{q_{n+1}q_n}=\frac{p_{n+1}}{q_{n+1}}<\theta\Rightarrow\frac{p_n}{q_n}<\theta+\frac{1}{q_{n+1}q_n}$$

Επομένως

$$\frac{q_n}{q_{n+1}}(2\theta+\frac{1}{q_{n+1}q_n})-2\theta=2\theta(\frac{q_n}{q_{n+1}}+\frac{1}{2\theta q_{n+1}q_n}\frac{q_n}{q_{n+1}}-1)=2\theta(\frac{q_n}{q_{n+1}}+\frac{1}{2\theta {q_{n+1}}^2}-1)$$

Ισχύει: $2\theta {q_{n+1}}^2>q_{n+1}\Rightarrow\frac{1}{2\theta {q_{n+1}}^2}<\frac{1}{q_{n+1}}$

Οπότε

$$\frac{q_n}{q_{n+1}}(2\theta+\frac{1}{q_{n+1}q_n})-2\theta<2\theta(\frac{q_n}{q_{n+1}}+\frac{1}{q_{n+1}}-1)$$

Λαμβάνοντας υπ' όψιν ότι η ακολουθία q_n είναι γνησίως αύξουσα παίρνουμε

$$\frac{q_n}{q_{n+1}}(2\theta+\frac{1}{q_{n+1}q_n})-2\theta\le2\theta(\frac{q_{n+1}}{q_{n+1}}-1)=0\Rightarrow\frac{q_n}{q_{n+1}}(2\theta+\frac{1}{q_{n+1}q_n})\le2\theta$$

Από την (*) και την προηγούμενη ανισότητα έχουμε το ζητούμενο

$\left|{p_n}^2-\theta^2{q_n}^2\right|<2\theta$.

ΠΡΟΤΑΣΗ 6 Έστω m θετικός ακέραιος ο οποίος δεν είναι τετράγωνο ακεραίου και $\frac{p_n}{q_n}$, ο n-οστός συγκλίνων ρητός της ανάπτυξης σε συνεχές κλάσμα του $\sqrt{m}$.

Τότε το υπόλοιπο της διαίρεσης του ${p_n}^2 \bmod \mathrm{m}$ (το οποίο θεωρούμε ότι είναι μεταξύ του $-m/2$ και του $m/2$ - επιτρέπουμε στο υπόλοιπο να είναι και αρνητικός) είναι μικρότερο του $2\sqrt{n}$.

Απόδειξη

Εφαρμόζουμε την προηγούμενη πρόταση για $\theta=\sqrt{m}$ και έχουμε

$\left|{p_n}^2-m{q_n}^2\right|<2\sqrt{m}$. Όμως ${p_n}^2\equiv{p_n}^2-m{q_n}^2(\bmod m)$. Άρα $\left|{p_n}^2\right|(\bmod m)<2\sqrt{m}$.

ΘΕΩΡΗΜΑ *Έστω θ ένας πραγματικός άρρητος και* $\theta=[\alpha_0,\alpha_1,\ldots]$ *το ανάπτυγμά του σε συνεχές κλάσμα. Ο αριθμός θ είναι τετραγωνικός άρρητος αν και μόνο αν η ακολουθία* $(\alpha_n)_{n\in\mathbb{N}}$ *είναι περιοδική.*

Απόδειξη

Υποθέτουμε ότι η ακολουθία $(\alpha_n)_{n\in\mathbb{N}}$ είναι περιοδική. Άρα υπάρχουν ελάχιστοι φυσικοί k και $m\geq 1$ τέτοιοι ώστε

$$\theta=[a_0,a_1,\ldots,a_{k-1},\overline{a_k,\ldots,a_{k+m-1}}]$$

Θέτουμε $\varphi=[\overline{a_k,\ldots,a_{k+m-1}}]$. Ο φ είναι άρρητος.

Αν $m=1$, τότε $\varphi=[\overline{a_k}]=[a_k,\varphi]$. Άρα $\varphi=a_k+\frac{1}{\varphi}$ και παίρνουμε ότι $\varphi^2-a_k\varphi-1=0$.

Επομένως ο φ είναι και τετραγωνικός.

Έστω $m\geq 2$. Τότε

$$\varphi=[\overline{a_k,\ldots,\alpha_{k+m-1}}]=[a_k,\ldots,a_{k+m-1},\varphi]$$

Αν $\frac{r_n}{s_n}$ είναι οι συγκλίνοντες ρητοί στο φ, από την πρόταση 3 παίρνουμε

$$\varphi=\frac{r_{m-1}\varphi+r_{m-2}}{s_{m-1}\varphi+s_{m-2}}$$

Επομένως, ο φ είναι ρίζα μιας εξίσωσης δευτέρου βαθμού.

Αν $k=0$, τότε $\theta=\varphi$.

Αν $k=1$, τότε $\theta=[a_0,\varphi]=a_0+\frac{1}{\varphi}$. Και αφού ο άρρητος φ είναι τετραγωνικός,

έχουμε $\varphi=\frac{a+\sqrt{b}}{g}$, όπου $a,b,g\in\mathbb{Z}$ με $b>0$ και ο b δεν είναι τέλειο τετράγωνο ακεραίου. Οπότε ο θ θα είναι της ίδιας μορφής, δηλαδή ένας τετραγωνικός άρρητος.

Αν $k\geq 2$ και $\frac{p_n}{q_n}$ οι συγκλίνοντες ρητοί στο θ από την πρόταση 3 έχουμε

$$\theta=\frac{p_{k-1}\varphi+p_{k-2}}{q_{k-1}\varphi+q_{k-2}}$$

Οπότε, επειδή ο φ είναι τετραγωνικός άρρητος, η παραπάνω ισότητα συνεπάγεται ότι ο θ είναι επίσης τετραγωνικός άρρητος.

Αντίστροφα, υποθέτουμε ότι ο θ είναι τετραγωνικός άρρητος. Τότε ο θ ικανοποιεί μια εξίσωση της μορφής

$$\alpha x^2 + \beta x + \gamma = 0$$

όπου $\alpha, \beta, \gamma \in \mathbb{Z}$ με διακρίνουσα $\delta = \beta^2 - 4\alpha\gamma$ > 0. Θεωρούμε την δυαδική μορφή

$$f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$$

και τους πίνακες

$$A(n) = \begin{pmatrix} p_n & \mathrm{q}_n \\ p_{n-1} & \mathrm{q}_{n-1} \end{pmatrix}, \mathrm{n}=1,2,\ldots$$

όπου $\frac{p_n}{q_n}$ οι συγκλίνοντες ρητοί στο θ. Σύμφωνα με την πρόταση 2, η ορίζουσα του $A(n)$ ισούται με ± 1. Οπότε η δυαδική μορφή $f(x, y)$ είναι ισοδύναμη με την

$$f_n(x, y) = f(\mu_{A(n)}(x, y)) = \alpha_n x^2 + \beta_n xy + \gamma_n y^2$$

Έτσι έχουμε $a_n = f(p_n, q_n)$ και $\gamma_n = f(p_{n-1}, q_{n-1}) = \alpha_{n-1}$, Επίσης η διακρίνουσα της μορφής $f_n(x, y)$ ισούται με δ. Καθώς $f(\theta, 1) = 0$, έχουμε

$$\frac{\alpha_n}{q_n^2} = \frac{f(p_n, q_n)}{q_n^2} = f\left(\frac{p_n}{q_n}, 1\right) - f(\theta, 1) = a\left(\left(\frac{p_n}{q_n}\right)^2 - \theta^2\right) + \beta\left(\frac{p_n}{q_n} - \theta\right)$$

Από την πρόταση 4 έχουμε ότι $\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$ απ' όπου

$$\left|\left(\frac{p_n}{q_n}\right)^2 - \theta^2\right| < \frac{\left|\theta + \frac{p_n}{q_n}\right|}{q_n^2} < \frac{2|\theta| + 1}{q_n^2}$$

Άρα

$$|\alpha_n| < (2|\theta| + 1)|\alpha| + |\beta|$$

Εφόσον $\gamma_n = \alpha_{n-1}$ και $\delta = \beta_n^2 - 4\alpha_n\gamma_n$, οι ακέραιοι β_n και γ_n είναι επίσης φραγμένοι ανεξάρτητα του n.

Αν θ_n (n=1,2,…) είναι τα πλήρη πηλίκα του θ, τότε από την πρόταση 3

$$\theta = \frac{p_n\theta_{n+1} + p_{n-1}}{q_n\theta_{n+1} + q_{n-1}}$$

Άρα

$$f_n(\theta_{n+1},1) = f(p_n\theta_{n+1}+p_{n-1}, q_n\theta_{n+1}+q_{n-1}) = (q_n\theta_{n+1}+q_{n-1})^2 f\left(\frac{p_n\theta_{n+1}+p_{n-1}}{q_n\theta_{n+1}+q_{n-1}},1\right) =$$

$$= (p_{n-1}, q_n\theta_{n+1}+q_{n-1})^2 f(\theta,1) = 0$$

Και εφόσον οι ακέραιοι α_n, β_n και γ_n είναι φραγμένοι ανεξάρτητα του n, έπεται ότι το σύνολο $[\theta_1,\theta_2,\ldots]$ είναι πεπερασμένο. Άρα υπάρχουν φυσικοί m,l > 0 έτσι ώστε $\theta_{l+m} = \theta_l$, απ' όπου έπεται ότι η ακολουθία $(\alpha_n)_{n\in\mathbb{N}}$ *είναι περιοδική.*

1.5 Εύρεση λύσης διοφαντικής εξίσωσης

Ο Έλληνας μαθηματικός Διόφαντος (περίπου 200 – 298) έζησε τον τρίτο αιώνα στην Αλεξάνδρεια της Αιγύπτου. Είναι γνωστός για δύο πράγματα: πρώτον, για το σύγγραμμά του «Αριθμητικά», που είναι το αρχαιότερο ελληνικό σύγγραμμα άλγεβρας και είναι μια εργασία πάνω στην θεωρία αριθμών στην οποία εκτός άλλων μελέτησε εξισώσεις που δέχονται ως λύσεις μόνο ακέραιους αριθμούς και προς τιμή του ονομάστηκαν διοφαντικές. Δεύτερον, για τον παρακάτω γρίφο, που ήταν η επιγραφή στον τάφο του κατόπιν δικής του επιθυμίας:

> *«Διαβάτη, σ' αυτόν τον τάφο αναπαύεται ο Διόφαντος. Σε εσένα που είσαι σοφός, η επιστήμη θα δώσει το μέτρο της ζωής του. Άκουσε. Ο Θεός του επέτρεψε να είναι νέος για το ένα έκτο της ζωής του. Ακόμα ένα δωδέκατο και φύτρωσε το μαύρο γένι του. Μετά από ένα έβδομο ακόμα, ήρθε του γάμου του η μέρα. Τον πέμπτο χρόνο αυτού του γάμου γεννήθηκε ένα παιδί. Τι κρίμα, για το νεαρό του γιο. Αφού έζησε μονάχα τα μισά χρόνια από τον πατέρα του, γνώρισε την παγωνιά του θανάτου. Τέσσερα χρόνια αργότερα, Ο Διόφαντος βρήκε παρηγοριά στη θλίψη του, φτάνοντας στο τέλος της ζωής του.»*

Για να βρούμε πόσο χρονών πέθανε ο Διόφαντος μπορούμε να χρησιμοποιήσουμε στοιχειώδη άλγεβρα. Αν x είναι το ζητούμενο, τότε πρέπει να λύσουμε την εξίσωση $\frac{x}{6}+\frac{x}{12}+\frac{x}{7}+5+\frac{x}{2}+4=x$ και παίρνουμε το αποτέλεσμα $x=84$. Ένας εύκολος τρόπος για να λύσουμε τον γρίφο είναι να παρατηρήσουμε

ότι το $1/12$ της ζωής του ήταν νέος και το $1/7$ ήταν ανύπαντρος. Δηλαδή η ηλικία του πρέπει να διαιρεί τους αριθμούς 12 και 7. Ο μόνος ακέραιος που έχει αυτή την ιδιότητα και είναι στα όρια του ανθρώπινου προσδόκιμου ζωής είναι ο αριθμός $12\cdot 7=84$. Ειδικότερα, ο Διόφαντος πέρασε $84/6=14$ χρόνια ως παιδί, $84/12=7$ χρόνια ως έφηβος και σε $84/7=12$ χρόνια ακόμα έγινε ο γάμος του. Επομένως παντρεύτηκε στα $14+7+12=33$ του χρόνια. Όταν ήταν $33+5=38$ γεννήθηκε ο γιος του, ο οποίος αργότερα κατέληξε όταν ήταν $84/2=42$ χρονών, ενώ ο Διόφαντος ήταν 80. Τελικά, μετά από 4 χρόνια πέθανε και ο ίδιος στην ώριμη ηλικία των 84 ετών.

ΘΕΩΡΗΜΑ *Έστω $a,b\in\mathbb{N}$ περιττοί αριθμοί που βρίσκονται κοντά μεταξύ τους. Τότε για κάθε $c\in\mathbb{Z}$ η εξίσωση*

$$ax-by=c$$

έχει άπειρες ακέραιες λύσεις (x,y). Επίσης αν (x_0,y_0) είναι μια ακέραια λύση της εξίσωσης με $c=1$, τότε για $c\in\mathbb{Z}$ οι λύσεις της εξίσωσης είναι της μορφής

$$x=cx_0+bt,\ \ y=cy_0+at,\ \ t\in\mathbb{Z}.$$

Απόδειξη

Πρώτα θα λύσουμε την εξίσωση $ax-by=1$. Γράφουμε το a/b ως απλό πεπερασμένο συνεχές κλάσμα, $\frac{a}{b}=[a_0,a_1,\ldots,a_n]$ και επιλέγουμε ο n να είναι περιττός. Τότε το a/b είναι ίσο με τον n-οστό συγκλίνων p_n/q_n, οπότε συμπεραίνουμε ότι $p_n=a$ και $q_n=b$. Επίσης ξέρουμε ότι

$$p_{n-1}q_n-p_nq_{n-1}=(-1)^{n-1}=1$$

αφού θεωρήσαμε ότι ο n είναι περιττός. Τότε $aq_{n-1}-p_{n-1}b=1$. Οπότε

$$(x_0,y_0)=(q_{n-1},p_{n-1})\ \ (*)$$

είναι η λύση της εξίσωσης $ax_0 - by_0 = 1$. Πολλαπλασιάζουμε τώρα με c και έχουμε

$$a(cx_0) - b(cy_0) = c$$

Συνδυάζοντας με την $ax - by = c$ παίρνουμε

$$a(cx_0) - b(cy_0) = ax - by$$

$$a(cx_0 - x) = b(cy_0 - y)$$

Αυτό σημαίνει ότι ο a διαιρεί τον $b(cy_0 - y)$. Και επειδή οι a, b είναι κοντινοί περιττοί, συνεπάγεται ότι ο a διαιρεί τον $(cy_0 - y)$. Οπότε $cy_0 - y = at$ για κάποιο $t \in \mathbb{Z}$.

Αντικαθιστώντας το αποτέλεσμα αυτό στην εξίσωση $a(cx_0 - x) = b(cy_0 - y)$ παίρνουμε $a(cx_0 - x) = b(at)$ και απαλείφοντας το a έχουμε $cx_0 - x = bt$.

Παρατηρήσεις: Σημειώνουμε ότι οι a, b ΠΡΕΠΕΙ να είναι περιττοί που δεν απέχουν πολύ μεταξύ τους. Παραδείγματος χάριν, η εξίσωση $2x - 4y = 1$ δεν έχει ακέραιες λύσεις (γιατί το αριστερό μέλος παραμένει πάντα ζυγό, οπότε δεν μπορεί να είναι ίσο με 1). Ακόμη να σημειώσουμε ότι η σχέση (*) της παραπάνω απόδειξης μας δείχνει *πώς* να βρίσκουμε το (x_0, y_0): γράφουμε το a/b ως απλό πεπερασμένο συνεχές κλάσμα, $\frac{a}{b} = [a_0, a_1, \ldots, a_n]$, όπου n περιττός και υπολογίζουμε τον $n-1$ συγκλίνων για να βρούμε το $(x_0, y_0) = (q_{n-1}, p_{n-1})$.

<u>Παράδειγμα</u>

Έστω η διοφαντική εξίσωση $157x - 68y = 12$.

Θα γράψουμε το $157/68$ ως συνεχές κλάσμα. Έχουμε

$157 = 2 \cdot 68 + 21$

$68 = 3 \cdot 21 + 5$

$21 = 4 \cdot 5 + 1$

$5 = 5 \cdot 1 + 0$

Άρα $\frac{157}{68} = 2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{5}}}$. Δηλαδή $\frac{157}{68} = [2,3,4,5] = [a_0, a_1, a_2, a_3] \Rightarrow n = 3$

και $(x_0, y_0) = (q_{n-1}, p_{n-1}) = (q_2, p_2)$

$$\frac{p_2}{q_2} = 2 + \frac{1}{3 + \frac{1}{4}} = 2 + \frac{1}{\frac{13}{4}} = 2 + \frac{4}{13} = \frac{30}{13}$$

Τελικά η $(x_0, y_0) = (13,30)$ είναι μία λύση της $157x - 68y = 1$. Οπότε $cx_0 = 12 \cdot 13 = 156$, $cy_0 = 12 \cdot 30 = 360$ και η γενική λύση της εξίσωσης $157x - 68y = 12$ είναι $x = 156 + 68t$, $y = 360 + 157t$, $t \in \mathbb{Z}$.

ΚΕΦΑΛΑΙΟ 2

Το κρυπτοσύστημα RSA

2.1 Βασικά στοιχεία

Το κρυπτοσύστημα RSA είναι μία μέθοδος κωδικοποίησης με δημόσιο κλειδί. Πήρε το όνομά του από τα αρχικά των δημιουργών της R.Rivest, A.Shamir και L.Adleman.

Βασίζεται στην ιδέα ότι είναι πολύ απλό να πολλαπλασιάσουμε δύο μεγάλους αριθμούς, ειδικά με Η/Υ, αλλά είναι αρκετά δύσκολο να παραγοντοποιήσουμε τέτοιους αριθμούς.

Παραδείγματος χάριν, έστω ότι θέλουμε να παραγοντοποιήσουμε τον αριθμό 1459160519 σε δύο παράγοντες. Ένας Η/Υ μπορεί να παραγοντοποιήσει αυτόν τον αριθμό πολύ γρήγορα, αλλά στην ουσία το κάνει δοκιμάζοντας όλους τους πιθανούς συνδυασμούς. Γενικά, ο υπολογιστής πρέπει να εξετάσει όλους τους αριθμούς τάξεως μεγέθους έως την τετραγωνική ρίζα του αριθμού προς παραγοντοποίηση. Εδώ, η τετραγωνική ρίζα του 1459160519 είναι περίπου 38000. Βέβαια, δεν παίρνει πολύ ώρα στον υπολογιστή να δοκιμάσει 38000 συνδυασμούς, αλλά τι γίνεται αν ο αριθμός που θέλουμε να παραγοντοποιήσουμε έχει πάνω από 400 ψηφία; Η τετραγωνική ρίζα ενός τέτοιου αριθμού έχει πάνω από 200 ψηφία. Η διάρκεια ζωής του σύμπαντος είναι περίπου 10^{18} δευτερόλεπτα – αριθμός με 18 ψηφία. Αν λάβουμε υπ' όψιν ότι ένας υπολογιστής μπορεί να πραγματοποιήσει ένα εκατομμύριο δοκιμές το δευτερόλεπτο, στη διάρκεια ζωής του σύμπαντος θα μπορούσε να εξετάσει 10^{24} πιθανές παραγοντοποιήσεις. Αλλά για ένα γινόμενο με 400 ψηφία, υπάρχουν 10^{200} πιθανές δοκιμές. Αυτό σημαίνει ότι ο υπολογιστής θα χρειαζόταν χρόνο

10^{176} φορές την ζωή του σύμπαντος για να παραγοντοποιήσει έναν τέτοιο αριθμό.

Όμως είναι πολύ πιο εύκολο να αποφανθούμε αν ένας αριθμός είναι πρώτος – με άλλα λόγια να βρούμε ότι δεν παραγοντοποιείται. Αν δεν είναι πρώτος, είναι δύσκολο να παραγοντοποιηθεί αλλά αν είναι πρώτος, δεν είναι δύσκολο να το δείξουμε.

Το κρυπτοσύστημα RSA λοιπόν λειτουργεί ως εξής: Βρίσκω δύο μεγάλους πρώτους αριθμούς p και q, οι οποίοι έχουν 100 ή ακόμα και 200 ψηφία ο καθένας. Κρατώ αυτούς τους αριθμούς κρυφούς (είναι το ιδιωτικό μου κλειδί) και τους πολλαπλασιάζω ώστε να πάρω τον αριθμό $N = p \cdot q$. Ο αριθμός N είναι μέρος του δημόσιου κλειδιού μου. Αλλά πώς ακριβώς χρησιμοποιείται ο N για να κρυπτογραφηθεί ένα μήνυμα και πώς οι p ,q για να αποκρυπτογραφηθεί; Ακολουθεί ένα παράδειγμα όπου θα χρησιμοποιήσουμε μικρούς πρώτους για να γίνονται εύκολα οι πράξεις. Στην πραγματικότητα όμως, οι αριθμοί αυτοί είναι πολύ μεγαλύτεροι.

Ο Α θέλει να δημιουργήσει ένα δημόσιο κλειδί και ο Β θέλει να χρησιμοποιήσει αυτό το κλειδί για να στείλει στον Α ένα μήνυμα. Το μήνυμα είναι ένα αριθμός, αφού υποθέτουμε ότι οι Α και Β έχουν συμφωνήσει σε μία μέθοδο κωδικοποίησης κειμένων σε αριθμούς. Τα βήματα είναι τα παρακάτω:

1. Ο Α επιλέγει δύο πρώτους αριθμούς. Έστω $p = 23$ και $q = 41$.
2. Πολλαπλασιάζει τους p ,q και παίρνει $n = p \cdot q = 23 \cdot 41 = 943$. Ο 943 είναι μέρος του δημόσιου κλειδιού, το οποίο δημοσιοποιεί στον Β και σε όποιον άλλο θέλει.
3. Επίσης ο Α επιλέγει ακόμα έναν αριθμό, τον e, ο οποίος πρέπει να είναι πρώτος σε σχέση με τον $(p-1)(q-1)$. Έχουμε $(p-1)(q-1) = 22 \cdot 40 = 880$. Οπότε ο $e = 7$ μας κάνει $((880,7) = 1)$. Ο e είναι το δεύτερο και τελευταίο μέρος του δημόσιου κλειδιού, άρα ο Α αποκαλύπτει στον Β και την τιμή του e (το ζευγάρι (n, e) είναι το δημόσιο κλειδί).
4. Τώρα ο Β ξέρει αρκετά για να κρυπτογραφήσει ένα μήνυμα για τον Α. Έστω ότι το μήνυμα αυτό είναι ο αριθμός $M = 35$.

5. Υπολογίζει την τιμή του $C = M^e (\text{mod n}) = 35^7 (\text{mod} 943) = = 64339296875 \ (\text{mod} 943) = 545$. Ο αριθμός 545 είναι το κρυπτογραφημένο μήνυμα που στέλνει ο Β στον Α.
6. Ο Α θέλει να αποκρυπτογραφήσει το μήνυμα. Για να το κάνει, πρέπει να βρει έναν αριθμό d τέτοιο ώστε $e \cdot d = 1 \ (\text{mod} \ (p-1)(q-1))$. Δηλαδή $7 \cdot d = 1 \ (\text{mod} 880)$. Μία λύση είναι $d = 503$, αφού $7 \cdot 503 = 3251 = = 4(880) + 1 = 1 \ (\text{mod} 880)$.
7. Για να διαβάσει το μήνυμα ο Α πρέπει να κάνει τον υπολογισμό $C^d \ (\text{mod n}) = 545^{503} \ (\text{mod} 943)$. Για να κάνουμε αυτή την πράξη, παρατηρούμε ότι $503 = 256 + 128 + 64 + 32 + 16 + 4 + 2 + 1$ (που είναι η δυαδική αναπαράσταση του 503). Αυτό σημαίνει ότι

$$545^{503} = 545^{256+128+64+32+16+4+2+1} = 545^{256} \cdot 545^{128} \cdots 545^{1}$$

Για να υπολογίσουμε το $545^{503} \ (\text{mod} 943)$ θα υπολογίσουμε ξεχωριστά τα $545^{256} \ (\text{mod } 943)$, $545^{128} \ (\text{mod } 943), \ldots, 545^{1} \ (\text{mod } 943)$ και θα τα πολλαπλασιάσουμε. Έχουμε

$545^{1} \ (\text{mod } 943) = 545$

$545^{2} \ (\text{mod } 943) = 297025 \ (\text{mod } 943) = 923$

$545^{4} \ (\text{mod } 943) = (545^{2})^{2} \ (\text{mod } 943) = 923 \cdot 923 = 851929 (\text{mod } 943) = 400$

$545^{16} (\text{mod} 943) = (545^{4})^{4} \ (\text{mod} 943) = 400^{4} = 25600000000 (\text{mod} 943) = 857$

$545^{32} \ (\text{mod} 943) = (545^{16})^{2} \ (\text{mod} 943) = 857^{2} = 734449 \ (\text{mod} 943) = 795$

$545^{64} \ (\text{mod} 943) = (545^{32})^{2} \ (\text{mod} 943) = 795^{2} = 632025 \ (\text{mod} 943) = 215$

$545^{128} \ (\text{mod} 943) = (545^{64})^{2} \ (\text{mod} 943) = 215^{2} = 46225 \ (\text{mod} 943) = 18$

$545^{256} \ (\text{mod} 943) = (545^{128})^{2} \ (\text{mod} 943) = 18^{2} = 324 \ (\text{mod} 943) = 324$

Άρα

$545^{503} \ (\text{mod} 943) = 324 \cdot 18 \cdot 215 \cdot 795 \cdot 857 \cdot 400 \cdot 923 \cdot 545 (\text{mod} 943) = 35$

Οπότε ο Α μπορεί να διαβάσει το μήνυμα που είναι $M = 35$.

2.2 Θεωρήματα

Το κρυπτοσύστημα RSA είναι βασισμένο στα ακόλουθα τρία θεωρήματα.

ΘΕΩΡΗΜΑ (Μικρό θεώρημα του Fermat) *Αν ο* p *είναι πρώτος αριθμός και ο* a *είναι ένας ακέραιος τέτοιος ώστε* $(p,a)=1$*, τότε*

$$a^{p-1}=1 \pmod{p}.$$

ΘΕΩΡΗΜΑ (Euler) *Αν* $(a,m)=1$*, τότε* $a^{\varphi(m)}=1 \pmod{m}$,
όπου $\varphi(m)$ *η συνάρτηση Euler που μας δίνει το πλήθος των θετικών ακεραίων των μικρότερων (ή μικρότερων και ίσων) του* m *που είναι πρώτοι προς τον* m*.*

Παρατηρώ ότι αν $m=p$ (πρώτος), τότε $\varphi(m)=p-1$ και έχουμε το προηγούμενο θεώρημα.

ΘΕΩΡΗΜΑ *Έστω* p,q *δύο αριθμοί (όχι απαραίτητα πρώτοι) αλλά πρώτοι μεταξύ τους. Τότε, αν* $a=b \pmod{p}$ *και* $a=b \pmod{q}$*, συνεπάγεται ότι* $a=b \pmod{pq}$*.*

ΚΕΦΑΛΑΙΟ 3

Παραγοντοποίηση ακεραίων και συνεχή κλάσματα

3.1 *Ο* αλγόριθμος του Wiener

Ο αλγόριθμος παραγοντοποίησης του Wiener χρησιμοποιείται στην αποκρυπτογράφηση μηνυμάτων που έχουν κρυπτογραφηθεί με την μέθοδο κρυπτογράφησης RSA.

Όπως πάντα, $n = p \cdot q$, όπου p, q πρώτοι. Τότε $\varphi(n) = (p-1)(q-1)$. Η μέθοδος του Wiener βρίσκει τον μυστικό εκθέτη αποκρυπτογράφησης d, όμως πρέπει να ισχύουν οι παρακάτω υποθέσεις (υποθέσεις που ισχύουν πολύ συχνά στο RSA)

$$3d < n^{1/4} \text{ και } q < p < 2q.$$

Αν ο n έχει l ψηφία στη δυαδική του αναπαράσταση, τότε η μέθοδος λειτουργεί όταν ο d έχει λιγότερα από $l/4 - 1$ ψηφία στη δική του δυαδική αναπαράσταση και οι p, q δεν απέχουν πολύ μεταξύ τους.

Αφού $e \cdot d = 1 \pmod{(\varphi(n))}$, συνεπάγεται ότι υπάρχει ακέραιος t τέτοιος ώστε

$$de - t\varphi(n) = 1$$

Επίσης $n = pq > q^2$. Οπότε $q < \sqrt{n}$.

Και $0 < n - \varphi(n) = pq - (p-1)(q-1) = p + q - 1 < 2q + q - 1 < 3q < 3\sqrt{n}$.

Τώρα παρατηρούμε ότι

$$\left|\frac{e}{n} - \frac{t}{d}\right| = \left|\frac{ed - tn}{nd}\right| = \left|\frac{1 + t\varphi(n) - tn}{nd}\right| =$$

$$= \left|\frac{1 + t(\varphi(n) - n)}{nd}\right| < \frac{3t\sqrt{n}}{nd} = \frac{3t}{d\sqrt{n}}.$$

Εφόσον $t < d$, έχουμε ότι $3t < 3d < n^{1/4}$ και

$$\left|\frac{e}{n} - \frac{t}{d}\right| < \frac{1}{dn^{1/4}}.$$

Τελικά, αφού $3d < n^{1/4}$ παίρνουμε ότι

$$\left|\frac{e}{n}-\frac{t}{d}\right| < \frac{1}{3d^2}.$$

Δηλαδή το κλάσμα t/d είναι μία πολύ καλή προσέγγιση του κλάσματος e/n. Το παρακάτω θεώρημα μας εξασφαλίζει ότι μία τόσο κοντινή προσέγγιση αναγκαστικά είναι ένας από τους n-στους συγκλίνοντες του e/n.

ΘΕΩΡΗΜΑ *Έστω ότι* $(a,b)=(c,d)=1$ *και* $\left|\frac{a}{b}-\frac{c}{d}\right| < \frac{1}{2d^2}$. *Τότε ο* $\frac{c}{d}$ *είναι ένας από τους συγκλίνοντες ρητούς του συνεχούς κλάσματος* $\frac{a}{b}$.

Έστω a και b δύο θετικοί ακέραιοι τέτοιοι ώστε $(a,b)=1$. Τότε μπορούμε να γράψουμε το a/b ως συνεχές κλάσμα $\frac{a}{b}=[q_1,\ldots,q_m]$. Και για $1\le j\le m$ ο $C_j=[q_1,\ldots,q_j]$ είναι ο $j-οστός$ συγκλίνων ρητός στο a/b. Κάθε C_j μπορεί να γραφεί σαν ρητός αριθμός c_j/d_j, όπου τα c_j και d_j ικανοποιούν τους παρακάτω αναδρομικούς τύπους

$$c_j=\begin{cases}1 & \alpha\nu\ j=0\\ q_1 & \alpha\nu\ j=1\\ q_jc_{j-1}+c_{j-2} & \alpha\nu\ j\ge 2\end{cases}$$

και

$$d_j=\begin{cases}0 & \alpha\nu\ j=0\\ 1 & \alpha\nu\ j=1\\ q_jd_{j-1}+d_{j-2} & \alpha\nu\ j\ge 2\end{cases}$$

Από την στιγμή που η τιμή που η τιμή του e/n είναι δημόσια πληροφορία, είναι εύκολο να υπολογίσουμε τους n-στους συγκλίνοντες στο e/n. Αυτό που χρειαζόμαστε παραπάνω είναι ένα μία μέθοδος για να εξετάζουμε κάθε

συγκλίνων ξεχωριστά ώστε να βρούμε τον σωστό και να βρούμε το ιδιωτικό κλειδί d.

Αυτό δεν είναι δύσκολο. Αν t/d είναι είναι ένας συγκλίνων του e/n, τότε μπορούμε να υπολογίσουμε την τιμή του $\varphi(n)$ να είναι $\varphi(n) = de-1/t$. Από την στιγμή που οι n και $\varphi(n)$ είναι γνωστοί, μπορούμε να παραγοντοποιήσουμε τον n λύνοντας την εξίσωση $x^2 - (n - \varphi(n) + 1)x + n = 0$. Δεν ξέρουμε ποιος n-στός συγκλίνων είναι ο σωστός και γι' αυτό κάνουμε δοκιμές.

Αν αυτή η μέθοδος δεν είναι αποτελεσματική, τότε δεν θα ικανοποιούνται οι υποθέσεις $3d < n^{1/4}$ και $q < p < 2q$.

Ακολουθεί ο αλγόριθμος του Wiener σε ψευδοκώδικα.

Winer's algorithm (n, b)
$(q_1, \ldots, q_m; r_m) \leftarrow$ *Euclidean* algorithm (b,n)
$c_0 \leftarrow 1$
$c_1 \leftarrow q_1$
$d_0 \leftarrow 0$
$d_1 \leftarrow 1$
for $j \leftarrow 2$ **to** m
do
- $c_j \leftarrow q_j c_{j-1} + c_{j-2}$
- $d_j \leftarrow q_j d_{j-1} + d_{j-2}$
- $n' \leftarrow \dfrac{(d_j b - 1)}{c_j}$
- **comment :** $n' = \phi(n)$ if $\dfrac{c_j}{d_j}$ is the correct convergent
- **if** n' is an integer
  - **then**
    - let p and q be the roots of the equation
    - $x^2 - (n - n' + 1)x + n = 0$
    - **if** p and q are positive integers less than n
      - **then return** (p, q)

return ("failure")

Παράδειγμα

Έστω ότι $n = 160523347$ και $b = 60728973$.

Η ανάπτυξη του b/n σε συνεχές κλάσμα είναι

$$60728973 = 0 \cdot 160523347 + 60728973$$

$$160523347 = 2 \cdot 60728973 + 39065401$$

$$60728973 = 1 \cdot 39065401 + 21663572$$

$$39065401 = 1 \cdot 21663572 + 17401829$$

$$21663572 = 1 \cdot 17401829 + 4261743$$

$$17401829 = 4 \cdot 4261743 + 354857$$

$$4261743 = 12 \cdot 354857 + 3459$$

$$354857 = 102 \cdot 3459 + 2039$$

$$3459 = 1 \cdot 2039 + 1420$$

$$2039 = 1 \cdot 1420 + 619$$

$$1420 = 2 \cdot 619 + 182$$

$$619 = 3 \cdot 182 + 73$$

$$182 = 2 \cdot 73 + 36$$

$$73 = 2 \cdot 36 + 1$$

$36 = 36 \cdot 1$

Επομένως $\frac{60728973}{160523347} = [0, 2, 1, 1, 1, 4, 12, 102, 1, 1, 2, 3, 2, 2, 36]$

Οι έξι πρώτοι συγκλίνοντες ρητοί είναι

$\frac{c_1}{d_1} = \frac{q_1}{1} = \frac{0}{1} = 0$

$\frac{c_2}{d_2} = \frac{q_2 c_1 + c_0}{q_2 d_1 + d_0} = \frac{2 \cdot 0 + 1}{2 \cdot 1 + 0} = \frac{1}{2}$

$\frac{c_3}{d_3} = \frac{q_3 c_2 + c_1}{q_3 d_2 + d_1} = \frac{1 \cdot 1 + 0}{1 \cdot 2 + 1} = \frac{1}{3}$

$\frac{c_4}{d_4} = \frac{q_4 c_3 + c_2}{q_4 d_3 + d_2} = \frac{1 \cdot 1 + 1}{1 \cdot 3 + 2} = \frac{2}{5}$,

$\frac{c_5}{d_5} = \frac{q_5 c_4 + c_3}{q_5 d_4 + d_3} = \frac{1 \cdot 2 + 1}{1 \cdot 5 + 3} = \frac{3}{8}$

$\frac{c_6}{d_6} = \frac{q_6 c_5 + c_4}{q_6 d_5 + d_4} = \frac{4 \cdot 3 + 2}{4 \cdot 8 + 5} = \frac{14}{37}$

Τώρα θα υπολογίσουμε το n'

Για $j = 2$,

$$n' = \frac{d_2 b - 1}{c_2} = \frac{2 \cdot 60728973 - 1}{1} = 121457945$$ που είναι ακέραιος.

Άρα θα λύσουμε την εξίσωση

$x^2 - (160523347 - 121457945 + 1)x + 160523347 = 0$ ή

$x^2 - 39065403x + 160523347 = 0$

η οποία έχει ρίζες $p = 39065398.89$ και $q = 4.1091$ που δεν είναι ακέραιοι. Άρα συνεχίζουμε να εκτελούμε τον αλγόριθμο.

Για $j = 3$,

$$n' = \frac{d_3 b - 1}{c_3} = \frac{3 \cdot 60728973 - 1}{1} = 182186918$$

Η δευτεροβάθμια εξίσωση που πρέπει να λύσουμε είναι

$x^2-(160523347-182186918+1)x+160523347=0$ ή

$x^2+21663570x+160523347=0$

που έχει ρίζες $p=-7.40984$ και $q=-21663562.59$ που δεν είναι ακέραιες άρα συνεχίζουμε.

Για $j=4$,

$$n'=\frac{d_4b-1}{c_4}=\frac{5\cdot 60728973-1}{2}=\frac{303644864}{2}=151822432$$

και η εξίσωση είναι

$x^2-(160523347-151822432+1)x+160523347=0$ ή

$x^2-8700916x+160523347=0$

με ρίζες $p=8700897.551$ και $q=18.449057$ που είναι δεκαδικοί και άρα απορρίπτονται.

Για $j=5$,

$$n'=\frac{d_5b-1}{c_5}=\frac{8\cdot 60728973-1}{3}=\frac{485831783}{3}=161943927.7$$

Ο n' σε αυτή την περίπτωση είναι δεκαδικός, οπότε προχωράμε στο επόμενο βήμα.

Για $j=6$,

$$n'=\frac{d_6b-1}{c_6}=\frac{37\cdot 60728973-1}{14}=\frac{2246972000}{14}=160498000$$

Οπότε σχηματίζουμε την εξίσωση

$x^2-(160523347-160498000+1)x+160523347=0$ ή

$x^2-25348x+160523347=0$

και βρίσκουμε τις ρίζες $p=12347$ και $q=13001$ που είναι θετικοί ακέραιοι. Άρα ο αλγόριθμος σταματάει γιατί βρήκαμε τους παράγοντες του 160523347 και είναι $160523347=12447\cdot 13001$.

3.2 Ένας δεύτερος αλγόριθμος

Θεωρητικό υπόβαθρο

Ορισμός Βάση παραγόντων είναι ένα σύνολο $B=\{d_1,d_2,\ldots,d_k\}$ διακεκριμένων πρώτων και d_1 να μπορεί να είναι το -1. Λέμε ότι το τετράγωνο ακεραίου b είναι $B-\alpha\rho\iota\theta\mu\acute{o}\varsigma$ (για δοσμένο m), αν το ελάχιστο κατ' απόλυτη τιμή πηλίκο του $b^2 \pmod m$ μπορεί να γραφτεί ως γινόμενο αριθμών από το B.

Παράδειγμα

Έστω $m=4633$ και $B=\{-1,2,3\}$. Τα τετράγωνα των αριθμών 67, 68, 69 είναι $B-\alpha\rho\iota\theta\mu o\acute{\iota}$ διότι

$67^2=4489\equiv -144 \pmod{4633}$ και $-144=(-1)^1 2^4 3^2$

$68^2=4624\equiv -9 \pmod{4633}$ και $-9=(-1)^1 3^2$

$69^2=4761\equiv 128 \pmod{4633}$ και $128=2^7$

Έστω τώρα $F_2^{\,k}$ ο διανυσματικός χώρος πάνω από το σώμα με δύο στοιχεία, το οποίο περιέχει $k-\acute{\alpha}\delta\varepsilon\varsigma$ από το σύνολο $\{0,1\}$. Δοσμένου του m και της βάσης παραγόντων B, η οποία περιέχει k αριθμούς, θα δείξουμε πώς θα αντιστοιχίσουμε ένα διάνυσμα $\vec{a}\in F_2^{\,k}$ σε κάθε $B-\alpha\rho\iota\theta\mu\acute{o}$:

Γράφουμε το $b^2 \pmod m$ στη μορφή $\prod_{j=1}^{k} b_j^{\,c_j}$ και θέτουμε την j συντεταγμένη του $\vec{a}$ ίση με $c_j \pmod 2$, δηλαδή $a_j=0$ αν ο c_j είναι άρτιος, και $a_j=1$ αν ο c_j είναι περιττός.

Στο προηγούμενο παράδειγμα το διάνυσμα που αντιστοιχεί στο 67 είναι το $\{1,0,0\}$, στο 68 το $\{1,0,0\}$ και στο 69 το $\{0,1,0\}$.

Έστω επίσης ότι έχουμε κάποιους από τους $B-\alpha\rho\iota\theta\mu o\acute{\upsilon}\varsigma$ $b_i^2 \pmod m$, τέτοιους ώστε τα αντίστοιχα διανύσματα $\vec{a_i} = \{a_{i1}, a_{i2}, \ldots, a_{ik}\}$ όταν προστεθούν δίνουν το μηδενικό διάνυσμα του F_2^k. Τότε το γινόμενο των ελαχίστων κατ' απόλυτη τιμή υπολοίπων $b_i^2 \pmod 2$ είναι ίσο με ένα γινόμενο αρτίων δυνάμεων όλων των $d_j \in B$. Δηλαδή αν για κάθε i συμβολίσουμε με a_i το ελάχιστο κατ' απόλυτη τιμή υπόλοιπο $b_i^2 \pmod m$ έχουμε

$$a_i = \prod_{j=1}^{k} d_j^{a_{ij}} \text{ και}$$

$$\prod a_i = \prod_{j=1}^{k} d_j^{\sum_i a_{ij}} ,$$

όπου ο εκθέτης του κάθε πρώτου d_j στο δεξί μέλος είναι άρτιος. Τότε το δεξί μέλος είναι τετράγωνο του $\prod_j d_j^{\gamma_j}$ με $\gamma_j = \frac{1}{2}\sum_i a_{ij}$.

Αν θέσουμε $b = \prod_i b_i \pmod m$ (παίρνουμε το ελάχιστο κατ' απόλυτη τιμή υπόλοιπο) και $c = \prod_i d_j^{\gamma_j} \pmod m$ (παίρνουμε πάλι το ελάχιστο κατ' απόλυτη τιμή υπόλοιπο) παίρνουμε δύο αριθμούς b, c που, ενώ κατασκευάστηκαν με διαφορετικό τρόπο (ο b ως γινόμενο των b_i και ο c ως γινόμενο των d_j), ισχύει $b^2 \equiv c^2 \pmod m$. Οπότε τώρα αν

· $b \neq c \pmod m$, τότε βρήκαμε ένα μη τετριμμένο διαιρέτη του m παίρνοντας το $(b+c, m)$ ή το $(b-c, m)$

· $b \equiv c \pmod m$, τότε επαναλαμβάνουμε την διαδικασία μεγαλώνοντας την βάση B που επιλέξαμε.

Ο αλγόριθμος

Έστω m ο ακέραιος που θέλουμε να παραγοντοποιήσουμε. Όλες οι πράξεις που θα κάνουμε παρακάτω θα γίνουν modulo m (παίρνοντας το ελάχιστο μη αρνητικό υπόλοιπο ή το ελάχιστο κατ' απόλυτη τιμή υπόλοιπο).

Θέτουμε $b_{-1}=1$

$$b_0=a_0=\left\lfloor \sqrt{m} \right\rfloor$$

$$x_0=\sqrt{m}-a_0$$

Υπολογίζουμε το $b_0^{\,2} \pmod m$, που είναι το $b_0^{\,2}-m$. Και για $i=1,2,\ldots$ εκτελούμε τα παρακάτω βήματα:

1. Θέτουμε $a_i=\left\lfloor \frac{1}{x_{i-1}} \right\rfloor$ και $x_i=\frac{1}{x_{i-1}}-a_i$
2. Υπολογίζουμε το $b_i=a_i b_{i-1}+b_{i-2} \pmod m$
3. Υπολογίζουμε το $b_i^{\,2} \pmod m$. Κάνουμε τον υπολογισμό για μερικά i και διαλέγουμε εκείνους τους αριθμούς οι οποίοι παραγοντοποιούνται ± ως γινόμενο μικρών πρώτων. Επιλέγουμε μία βάση παραγόντων B που να περιέχει το -1, όπως και τους πρώτους που εμφανίζονται περισσότερες από μία φορές στο $b_i^{\,2} \pmod m$ (ή που εμφανίζονται σε άρτια δύναμη σε ένα και μόνο $b_i^{\,2} \pmod m$). Δημιουργούμε μία λίστα που περιέχει τους αριθμούς $b_i^{\,2} \pmod m$, από τους οποίους προέκυψε η βάση B, και τα αντίστοιχα διανύσματα $\vec{a_i}$, που περιέχει μηδενικά και άσσους, τα οποία είναι τα διανύσματα ανάλυσης του αριθμού m στην βάση B που έχουμε επιλέξει. Εάν είναι δυνατό, βρίσκουμε ένα υποσύνολο αυτών των αριθμών, των οποίων το άθροισμα των αντίστοιχων διανυσμάτων να κάνει μηδέν modulo κάποιου αριθμού που διαλέγουμε. Θέτουμε $b=\prod b_i$ (δουλεύοντας modulo m και παίρνοντας το γινόμενο πάνω στο υποσύνολο για το οποίο $\sum \vec{a_i}=0$). Θέτουμε επίσης $c=\prod d_j^{\,\gamma_j}$, όπου τα d_j είναι στοιχεία του B (εκτός του -1) και $\gamma_j=\frac{1}{2}\sum a_{ij}$.

   Αν $b \equiv c \pmod m$ ή $b \equiv -c \pmod m$, τότε ψάχνουμε για κάποιο άλλο υποσύνολο δεικτών i τέτοιων ώστε $\sum \vec{a_i}=0$. Και αν κάτι τέτοιο δεν είναι εφικτό, τότε πρέπει να υπολογίσουμε κι άλλα a_i, b_i, $b_i^{\,2} \pmod m$ ώστε να μεγαλώσουμε την βάση παραγόντων B.

Παρατήρηση: Για να μπορούμε να υπολογίζουμε το $c = \prod d_j^{\gamma_j}$ πιο εύκολα, είναι αρκετό για κάθε $\mathrm{B}-\alpha\rho\iota\theta\mu\acute{o}$ $b_i^2 \pmod m$ να παίρνουμε το διάνυσμα $\vec{a_i} = (\ldots, a_{ij}, \ldots)_j$ αντί του $\vec{\varepsilon_i}$, το οποίο είναι το ίδιο με το $\vec{\varepsilon_i}$ υπολογισμένο $\pmod 2$.

Παράδειγμα 1

Θα χρησιμοποιήσουμε τον παραπάνω αλγόριθμο για να παραγοντοποιήσουμε τον αριθμό 9073.

Θέτουμε $b_{-1} = 1$

$$b_0 = a_0 = \left\lfloor \sqrt{9073} \right\rfloor = 95$$

$$x_0 = \sqrt{m} - a_0 = \sqrt{9073} - 95 = 0.25229656$$

Επίσης $b_0^2 \pmod m = 95^2 \pmod{9073} = 9025 = -48$

Βήμα 1. $a_i = \left\lfloor \frac{1}{x_{i-1}} \right\rfloor$

$$x_i = \frac{1}{x_{i-1}} - a_i$$

Για $i = 1 \Rightarrow a_1 = \left\lfloor \frac{1}{x_0} \right\rfloor = \left\lfloor \frac{1}{0.25229656} \right\rfloor = 3$

$$x_1 = \frac{1}{x_0} - a_1 = \frac{1}{0.25229656} - 3 = 0.963589515$$

Για $i = 2 \Rightarrow a_2 = \left\lfloor \frac{1}{x_1} \right\rfloor = \left\lfloor \frac{1}{0.963589515} \right\rfloor = 1$

$$x_2 = \frac{1}{x_1} - a_2 = \frac{1}{0.963589515} - 1 = 0.037786302$$

Για $i = 3 \Rightarrow a_3 = \left\lfloor \frac{1}{x_2} \right\rfloor = \left\lfloor \frac{1}{0.037786302} \right\rfloor = 26$

$$x_3 = \frac{1}{x_2} - a_3 = \frac{1}{0.037786302} - 26 = 0.464616728$$

Για $i = 4 \Rightarrow a_4 = \left\lfloor \frac{1}{x_3} \right\rfloor = \left\lfloor \frac{1}{0.464616728} \right\rfloor = 2$

Βήμα 2. $b_i = a_i b_{i-1} + b_{i-2} \pmod{m}$

Για $i = 1 \Rightarrow b_1 = a_1 b_0 + b_{-1} \pmod{9073} = 3 \cdot 95 + 1 \pmod{9073} = 286 \pmod{9073} = 286$

Για $i = 2 \Rightarrow b_2 = a_2 b_1 + b_0 \pmod{9073} = 1 \cdot 286 + 95 \pmod{9073} = 381 \pmod{9073} = 381$

Για $i = 3 \Rightarrow b_3 = a_3 b_2 + b_1 \pmod{9073} = 26 \cdot 381 + 286 \pmod{9073} = 10192 \pmod{9073} =$
$= 1119$

Για $i = 4 \Rightarrow b_4 = a_4 b_3 + b_2 \pmod{9073} = 2 \cdot 1119 + 381 \pmod{9073} = 2619 \pmod{9073} =$
$= 2619$

Βήμα 3. $b_i^2 \pmod{m}$

Για $i = 1 \Rightarrow b_1^2 \pmod{m} = 286^2 \pmod{9073} = 81796 \pmod{9073} = 139$

Για $i = 2 \Rightarrow b_2^2 \pmod{m} = 381^2 \pmod{9073} = 145161 \pmod{9073} = -7$

Για $i=3 \Rightarrow b_3^2 \pmod m = 1119^2 \pmod{9073} = 1252161 \pmod{9073} = 87$

Για $i=4 \Rightarrow b_4^2 \pmod m = 2619^2 \pmod{9073} = 6859161 \pmod{9073} = -27$

Άρα έχουμε τον πίνακα

i	0	1	2	3	4
a_i	95	3	1	26	2
b_i	95	286	381	1119	2619
$b_i^2 \pmod m$	-48	139	-7	87	-27

Παρατηρούμε ότι $48 = 2^4 \cdot 3$

$87 = 3 \cdot 29$

$27 = 3^3$

Επιλέγουμε ως βάση παραγόντων την $B = \{-1, 2, 3, 7\}$. Τότε το $b_i^2 \pmod m$ είναι $\mathrm{B}-\alpha\rho\iota\theta\mu\acute{o}\varsigma$ για $i = 0, 2, 4$. Τα αντίστοιχα διανύσματα $\overrightarrow{\alpha_i}$ είναι $\overrightarrow{a_0} = \{1, 4, 1, 0\}$, $\overrightarrow{a_2} = \{1, 0, 0, 1\}$, $\overrightarrow{a_4} = \{1, 0, 3, 0\}$. Το άθροισμα του $\overrightarrow{a_0}$ και του $\overrightarrow{a_4}$ είναι μηδέν modulo 2. Οπότε διαλέγουμε $b = 95 \cdot 2619 = 248805 \equiv 3834 \pmod{9073}$ και $c = 2^2 \cdot 3^2 = 36$. Δηλαδή, σύμφωνα με τον αλγόριθμο που εφαρμόσαμε, έχουμε $3834^2 \equiv 36^2 \pmod{9073}$ και εφόσον $3834 \neq 36 \pmod{9073}$ και $3834 \neq -36 \pmod{9073}$ παίρνουμε τον μη τετριμμένο παράγοντα του 9073 $(3834 + 36, 9073) = (3870, 90730) = 43$. Τελικά $9073 = 43 \cdot 211$.

Παράδειγμα 2

Με τον ίδιο τρόπο θα παραγοντοποιήσουμε τον αριθμό 17873.

Θέτουμε $b_{-1} = 1$

$$b_0 = a_0 = \left\lfloor \sqrt{17873} \right\rfloor = 133$$

$$x_0 = \sqrt{m} - a_0 = \sqrt{17873} - 133 = 0.689939786$$

Επίσης $b_0^{\,2} \pmod{m} = 133^2 \pmod{17873} = 17689 \pmod{17873} = -184$

- Βήμα 1

$$a_i = \left\lfloor \frac{1}{x_{i-1}} \right\rfloor$$

$$x_i = \frac{1}{x_{i-1}} - a_i$$

Για $i = 1 \Rightarrow a_1 = \left\lfloor \frac{1}{x_0} \right\rfloor = \left\lfloor \frac{1}{0.689939786} \right\rfloor = 1$

$$x_1 = \frac{1}{x_0} - a_1 = \frac{1}{0.689939786} - 1 = 0.449401846$$

Για $i = 2 \Rightarrow a_2 = \left\lfloor \frac{1}{x_1} \right\rfloor = \left\lfloor \frac{1}{0.449401846} \right\rfloor = 2$

$$x_2 = \frac{1}{x_1} - a_2 = \frac{1}{0.449401846} - 2 = 0.22518$$

Για $i = 3 \Rightarrow a_3 = \left\lfloor \frac{1}{x_2} \right\rfloor = \left\lfloor \frac{1}{0.22518} \right\rfloor = 4$

$$x_3 = \frac{1}{x_2} - a_3 = \frac{1}{0.22518} - 4 = 0.440891731$$

Για $i = 4 \Rightarrow a_4 = \left\lfloor \frac{1}{x_3} \right\rfloor = \left\lfloor \frac{1}{0.440891731} \right\rfloor = 2$

$$x_4 = \frac{1}{x_3} - a_4 = \frac{1}{0.440891731} - 2 = 0.26813054$$

Για $i = 5 \Rightarrow a_5 = \left\lfloor \frac{1}{x_4} \right\rfloor = \left\lfloor \frac{1}{0.26813054} \right\rfloor = 3$

- Βήμα 2

$b_i = a_i b_{i-1} + b_{i-2} \pmod{m}$

Για $i = 1 \Rightarrow b_1 = a_1 b_0 + b_{-1} \pmod{17873} = 1 \cdot 133 + 1 \pmod{17873} =$

$= 134 \pmod{17873} = 134$

Για $i = 2 \Rightarrow b_2 = a_2 b_1 + b_0 \pmod{17873} = 2 \cdot 134 + 133 \pmod{17873} =$

$= 401 \pmod{17873} = 401$

Για $i = 3 \Rightarrow b_3 = a_3 b_2 + b_1 \pmod{17873} = 4 \cdot 401 + 134 \pmod{17873} =$

$= 1738 \pmod{17873} = 1738$

Για $i = 4 \Rightarrow b_4 = a_4 b_3 + b_2 \pmod{17873} = 2 \cdot 1738 + 401 \pmod{17873} =$

$= 3877 \pmod{9073} = 3877$

Για $i = 5 \Rightarrow b_5 = a_5 b_4 + b_3 \pmod{17873} = 3 \cdot 3877 + 1738 \pmod{17873} =$

$= 13369 \pmod{9073} = 13369$

- Βήμα 3

$b_i^2 \pmod{m}$

Για $i = 1 \Rightarrow b_1^2 \pmod{m} = 134^2 \pmod{17873} = 17956 \pmod{17873} = 83$

Για $i = 2 \Rightarrow b_2^2 \pmod{m} = 401^2 \pmod{17873} = 160801 \pmod{17873} = -56$

Για $i = 3 \Rightarrow b_3^2 \pmod{m} = 1738^2 \pmod{17873} = 3020644 \pmod{17873} = 107$

Για $i=4 \Rightarrow b_4^{\,2} \pmod m = 3877^2 \pmod{17873} = 15031129 \pmod{17873} = -64$

Για $i=5 \Rightarrow b_5^{\,2} \pmod m = 13369^2 \pmod{17873} = 178730161 \pmod{17873} = 161$

Φτιάχνουμε τον πίνακα

i	0	1	2	3	4	5
a_i	133	1	2	4	2	3
b_i	133	134	401	1738	3877	13369
$b_i^{\,2} \pmod m$	-184	83	-56	107	-64	161

Παρατηρούμε $184 = 2^3 \cdot 23$

$56 = 2^3 \cdot 7$

$64 = 2^6$

$161 = 7 \cdot 23$

Θέτουμε $B = \{-1, 2, 7, 23\}$. Τότε έχουμε $\mathrm{B}-\alpha\rho\iota\theta\mu o\acute{\upsilon}\varsigma$ για $i = 0, 2, 4, 5$. Τα αντίστοιχα διανύσματα $\vec{\alpha_i}$ είναι $\vec{a_0} = \{1, 3, 0, 1\}$, $\vec{a_2} = \{1, 3, 1, 0\}$, $\vec{a_4} = \{1, 6, 0, 0\}$, $\vec{a_5} = \{0, 0, 1, 1\}$. Το άθροισμα των $\vec{a_0}$, $\vec{a_2}$ και $\vec{a_5}$ είναι μηδέν modulo 2. Άρα υπολογίζουμε ότι $b = 133 \cdot 401 \cdot 13369 = 713008877 \equiv 1288 \pmod{17873}$ και $c = 2^3 \cdot 7 \cdot 23 = 1288$. Δηλαδή $b \equiv c \pmod{17873}$. Τώρα πρέπει να βρούμε κι άλλους $\mathrm{B}-\alpha\rho\iota\theta\mu o\acute{\upsilon}\varsigma$ των οποίων το άθροισμα των αντίστοιχων διανυσμάτων να κάνει μηδέν modulo 2. Υπολογίζουμε τον πίνακα για μερικά i ακόμα

$$x_5 = \frac{1}{x_4} - a_5 = \frac{1}{0.26813054} - 3 = 0.72952667$$

Για $i=6 \Rightarrow a_6 = \left\lfloor \frac{1}{x_5} \right\rfloor = \left\lfloor \frac{1}{0.72952667} \right\rfloor = 1$

$$x_6 = \frac{1}{x_5} - a_6 = \frac{1}{0.72952667} - 1 = 0.370751805$$

Για $i=7 \Rightarrow a_7 = \left\lfloor \frac{1}{x_6} \right\rfloor = \left\lfloor \frac{1}{0.370751805} \right\rfloor = 2$

$$x_7 = \frac{1}{x_6} - a_7 = \frac{1}{0.370751805} - 2 = 0.69722218$$

Για $i=8 \Rightarrow a_8 = \left\lfloor \frac{1}{x_7} \right\rfloor = \left\lfloor \frac{1}{0.69722218} \right\rfloor = 1$

Και

$$b_6 = a_6 b_5 + b_4 \pmod{17873} = 1 \cdot 13369 + 3877 \pmod{17873} =$$
$$= 17246 \pmod{17873} = 17246$$

$$b_7 = a_7 b_6 + b_5 \pmod{17873} = 2 \cdot 17246 + 13369 \pmod{17873} =$$
$$= 47861 \pmod{17873} = 12115$$

$$b_8 = a_8 b_7 + b_6 \pmod{17873} = 1 \cdot 12115 + 17246 \pmod{17873} =$$
$$= 29361 \pmod{17873} = 11488$$

$$b_6^{\,2} \pmod{m} = 17246^2 \pmod{17873} = 297424516 \pmod{17873} = -77$$

$$b_7^{\,2} \pmod{m} = 12115^2 \pmod{17873} = 146773225 \pmod{17873} = 149$$

$$b_8^{\,2} \pmod{m} = 11488^2 \pmod{17873} = 131974144 \pmod{17873} = -88$$

Φτιάχνουμε τον πίνακα

i	6	7	8
a_i	1	2	1
b_i	17246	12115	11488
$b_i^2 \pmod m$	-77	149	-88

Έχουμε $77 = 7 \cdot 11$

$88 = 2^3 \cdot 11$

Στην καινούρια βάση παραγόντων θα προσθέσουμε τον αριθμό 11, δηλαδή $B = \{-1, 2, 7, 11, 23\}$. Τότε για $i = 0, 2, 4, 5, 6, 8$ παίρνουμε $\mathrm{B} - \alpha\rho\iota\theta\mu o\acute{\upsilon}\varsigma$ με αντίστοιχα διανύσματα $\overrightarrow{a_0} = \{1, 3, 0, 0, 1\}$, $\overrightarrow{a_2} = \{1, 3, 1, 0, 0\}$, $\overrightarrow{a_4} = \{1, 6, 0, 0, 0\}$, $\overrightarrow{a_5} = \{0, 0, 1, 0, 1\}$, $\overrightarrow{a_6} = \{1, 0, 1, 1, 0\}$ και $\overrightarrow{a_8} = \{1, 3, 0, 1, 0\}$. Το άθροισμα των $\overrightarrow{a_2}$, $\overrightarrow{a_4}$, $\overrightarrow{a_6}$ και $\overrightarrow{a_8}$ είναι μηδέν modulo 2. Άρα $b = 401 \cdot 3877 \cdot 17246 \cdot 11488 = 308015791218496 \equiv 7272 \pmod{17873}$ και $c = 2^3 \cdot 7 \cdot 11$ και έτσι βρήκαμε έναν μη τετριμμένο διαιρέτη του 17873, τον $(7272 + 4928, 17873) = (12200, 17873) = 61$. Οπότε $17873 = 61 \cdot 293$.

ΒΙΒΛΙΟΓΡΑΦΙΑ

JAMES TATERSALL, Elementary Number Theory in Nine Chapters, Cambridge University Press, 2001

WILLIAM LEVEQUE, Fundamentals of Number Theory, Dover Publications, 1977

ΔΗΜΗΤΡΙΟΣ ΠΟΥΛΑΚΗΣ, Θεωρία Αριθμών – Μια σύγχρονη θεώρηση της κλασσικής Θεωρίας Αριθμών, Εκδόσεις Ζήτη, Θεσσαλονίκη 2005

ΑΛΕΞΑΝΔΡΟΣ ΠΑΠΑΪΩΑΝΝΟΥ – ΧΡΗΣΤΟΣ ΚΟΥΚΟΥΒΙΝΟΣ, Κρυπτογραφία, Εκδόσεις Εθνικού Μετσόβιου Πολυτεχνείου, Αθήνα 2007

GODFREY HAROLD HARDY – EDWARD MAITLAND WRIGHT, An introduction to the theory of numbers, Oxford University Press, 1960

ALEKSANDR YAKOVLEVICH KHINCHIN, Continued fractions, Dover Publications Inc., 1997

THOMAS JOANNES STIELTJES, Recherches sur les fractions continues, Toulouse, 1894

DOUGLAS ROBERT STINSON, Cryptography: theory and practice, Chapman and Hall, 1995