Αλγόριθμοι για την παραγοντοποίηση ακεραίων αριθμών

Αλέξανδρος Γ. Συγκελάκης *

3 Απριλίου 2006

1 Μέθοδος Συνεχών Κλασμάτων

1.1 Θεωρητικό Υπόβαθρο Συνεχών Κλασμάτων

Περίληψη

Στο κομμάτι αυτό θα περιγράψουμε μία μέθοδο, η οποία οφείλεται στον Legendre για την εύρεση "αρκετών" b, τέτοιων ώστε να ισχύει $|b^2 \mod n| < 2\sqrt{n}$. Η μέθοδος αυτή χρησιμοποιεί τη θεωρία των συνεχών κλασμάτων της οποίας θα κάνουμε μία σύντομη εισαγωγή με τα εντελώς απαραίτητα αποτελέσματα, τα οποία και θα αποδείξουμε, χωρίς να τα θεωρήσουμε τετριμμένα.

Θεωρούμε $x \in \mathbb{R}$ και κατασκευάζουμε το **συνεχές κλάσμα** αυτού, που ορίζεται αναδρομικά ως εξής: Έστω $a_0 = [x]$, όπου $[x]$ συμβολίζει το ακέραιο μέρος του αριθμού x, δηλαδή τον μεγαλύτερο ακέραιο που δεν υπερβαίνει το x (Για παράδειγμα $[-3.2] = -4, [2.6] = 2, [3] = 3$ κ.τ.λ.). Θέτουμε $x_0 = x - a_0$ και παίρνουμε $a_1 = \left[\frac{1}{x_0}\right] > 0$ και $x_1 = \frac{1}{x_0} - a_1$. Για $i > 1$ έστω $a_i = \left[\frac{1}{x_{i-1}}\right] > 0$ και $x_i = \frac{1}{x_{i-1}} - a_i$ ή $x_{i-1} = \frac{1}{a_i + x_i}$. Όταν/Εαν βρούμε οτι ο $\frac{1}{x_{i-1}}$ είναι ακέραιος τότε έχουμε $x_i = 0$ και η διαδικασία σταματά. Δεν είναι δύσκολο να δούμε οτι η διαδικασία σταματά αν-ν ο x είναι ρητός (διότι σε αυτή την περίπτωση, τα x_i είναι ρητοί αριθμοί με αύξοντες παρανομαστές).

Έτσι λοιπόν,

$$\begin{aligned} x = a_0 + x_0 &= a_0 + \frac{1}{a_1 + x_1} \\ &= a_0 + \frac{1}{a_1 + \dfrac{1}{a_2 + x_2}} \end{aligned}$$

*Τμήμα Μαθηματικών, Πανεπιστήμιο Κρήτης

$$= \cdots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots \cfrac{1}{a_i + x_i}}}}$$

το οποίο συνήθως γράφεται στην πιο συνεπτυγμένη μορφή, $x =< a_0, a_1, \ldots, a_i, x_i >$.

Παράδειγμα 1.1 *Θα αναπτύξουμε σε συνεχές κλάσμα τον αριθμό* $\sqrt{2}$. *Σύμφωνα με τα παραπάνω* $a_0 = [\sqrt{2}] = 1$ *και* $x_0 = \sqrt{2} - 1$. *Τότε* $a_1 = [\frac{1}{\sqrt{2}-1}] = [\sqrt{2}+1] = 2$ *και* $x_1 = \frac{1}{x_0} - a_1 = \frac{1}{\sqrt{2}-1} - 2 = \sqrt{2} - 1$ *και συνεχίζοντας παίρνουμε* $a_i = 2$ *και* $x_i = \sqrt{2} - 1, i = 2, 3, \ldots$ *συνεπώς το ανάπτυγμα του αριθμού* $\sqrt{2}$ *σε συνεχές κλάσμα είναι το* $\sqrt{2} =< 1, 2, 2, 2, \ldots >$.

Ας υποθέσουμε οτι ο x είναι άρρητος. Εαν εφαρμόσουμε την παραπάνω μορφή μέχρι να πάρουμε τον i-οστό όρο και μετά σβήσουμε το x_i, τότε παίρνουμε τον i**-οστό συγκλίνων ρητό στο** x, έστω $\frac{b_i}{c_i} :=< a_0, a_1, \ldots, a_i >$, με $(b_i, c_i) = 1$ και $c_i > 0$.

Πρόταση 1 *Ισχύουν οι εξής αναγωγικοί τύποι:*

$$b_0 = a_0, c_0 = 1, b_1 = a_0 a_1 + 1, c_1 = a_1$$

$$\text{και } \forall\, i \geq 2 : b_i = a_i b_{i-1} + b_{i-2}, c_i = a_i c_{i-1} + c_{i-2}$$

Απόδειξη:

Εύκολα επαληθεύουμε οτι οι παραπάνω τύποι ισχύουν για $i = 0, 1, 2$. Υποθέτουμε οτι ισχύουν για $i = k - 1 \geq 2$[1].

Είναι τότε $x = a_0 + \frac{1}{x_i}$ και $x_1 =< a_1, a_2, \ldots >$. Έστω r_j, s_j ακέραιοι με $(r_j, s_j) = 1$ ώστε $\frac{r_j}{s_j} =< a_1, a_2, \ldots, a_{j+1} > (j = 0, 1, \ldots)$, δηλαδή ο ρητός στον οποίο αντιστοιχεί το συνεχές κλάσμα $< a_1, a_2, \ldots, a_{j+1} >$.

Εφαρμόζουμε την υπόθεση της επαγωγής στους ακεραίους r_j, s_j και παίρνουμε:

$$r_{k-1} = a_k r_{k-2} + r_{k-3} \text{ και } s_{j-1} = a_k s_{k-2} + s_{k-3}$$

Καθώς $\frac{b_j}{c_j} =< a_0, a_1, \ldots, a_j >= a_0 + \frac{1}{< a_1, a_2, \ldots, a_j >} = a_0 + \frac{1}{\frac{r_{j-1}}{s_{j-1}}}$ και $(r_{j-1}, s_{j-1}) = 1$, παίρνουμε

$$b_j = a_0 r_{j-1} + s_{j-1}, c_j = r_{j-1} \tag{1.1}$$

[1] Δεν μπορούμε να προχωρήσουμε αμέσως στο επαγωγικό βήμα για $i = k$, καθώς θα εμφανιστεί το $< a_1, a_2, \ldots, a_k >$ το οποίο δεν είναι φανερό με τί ισούται σε σχέση με τα b_{i-1}, c_{i-1} που εμείς γνωρίζουμε λόγω της υπόθεσης της επαγωγής. Για το λόγο αυτό βάζουμε στο ¨παιχνίδι¨ και το $< a_1, a_2, \ldots, a_{j+1} >$.

Θέτοντας $j = k$, έχουμε:

$$\begin{aligned} b_k &= a_0 r_{k-1} + s_{k-1} \\ &= a_0(a_k r_{k-2} + r_{k-3}) + (a_k s_{k-2} + s_{k-3}) \\ &= a_k(a_0 r_{k-2} + s_{k-2}) + (a_0 r_{k-3} + s_{k-1}) \end{aligned} \tag{1.2}$$

και

$$c_k = r_{k-1} = a_k r_{k-2} + r_{k-3}. \tag{1.3}$$

Για $j = k-1, k-2$, κάνοντας χρήση των σχέσεων 1.1, παίρνουμε

$$\begin{aligned} b_{k-1} &= a_0 r_{k-2} + s_{k-2}, c_{k-1} = r_{k-2} \\ b_{k-2} &= a_0 r_{k-3} + s_{k-3}, c_{k-2} = r_{k-3} \end{aligned} \tag{1.4}$$

και συνδιάζοντας τις $1.2, 1.3, 1.4$ παίρνουμε οτι

$$b_k = a_k b_{k-1} + b_{k-2}, c_k = a_k c_{k-1} + c_{k-2}$$

και έτσι ολοκληρώνεται η επαγωγή στο k.

□

Πόρισμα 1.1 *Προφανώς η ακολουθία των c_i είναι γνησίως αύξουσα.*

Πρόταση 2 *Ισχύει $b_i c_{i-1} - b_{i-1} c_i = (-1)^{i-1},\ \forall\, i \geq 1$*

Απόδειξη:
Για $i = 1$ ισχύει καθώς $b_1 c_0 - b_0 c_1 = (a_0 a_1 + 1) \cdot 1 - a_0 a_1 = 1 = (-1)^0$.
Υποθέτουμε οτι ισχύει για $i = k \geq 2$ δηλαδή $b_k c_{k-1} - b_{k-1} c_k = (-1)^{k-1}$.
Τότε

$$\begin{aligned} b_{k+1} c_k - b_k c_{k+1} &= (a_{k+1} b_k + b_{k-1}) c_k - b_k (a_{k+1} c_k + c_{k-1}) \\ &= b_{k-1} c_k - b_k c_{k-1} = (-1)(b_k c_{k-1} - b_{k-1} c_k) \\ (\text{υπόθ. επαγωγής}) &= (-1)(-1)^{k-1} = (-1)^k \end{aligned}$$

□

Πόρισμα 1.2 *Ισχύει, $\dfrac{b_i}{c_i} - \dfrac{b_{i-1}}{c_{i-1}} = \dfrac{(-1)^{i-1}}{c_i c_{i-1}}$ (Αρκεί να διαιρέσουμε την παραπάνω σχέση με $c_i c_{i-1}$).*

Πόρισμα 1.3 *Απ'το Πόρισμα 1.2, για τις υπακολουθίες $\dfrac{b_{2i}}{c_{2i}}, \dfrac{b_{2i+1}}{c_{2i+1}}$ της $\dfrac{b_i}{c_i}$, έχουμε:*

$$\frac{b_{2i}}{c_{2i}} < \frac{b_{2i+2}}{c_{2i+2}} \text{ και} \frac{b_{2i+1}}{c_{2i+1}} > \frac{b_{2i+3}}{c_{2i+3}} \tag{1.5}$$

(Λαμβάνουτας υπόψιν οτι η ακολουθία θετικών ακεραίων c_i είναι γνησίως αύξουσα).

Πρόταση 3 *Για κάθε φυσικό $i \geq 2$ ισχύει:*

$$x = \frac{x_i b_{i-1} + b_i}{x_i c_{i-1} + c_i} \tag{1.6}$$

Απόδειξη:
Για $i = 2$ έχουμε:

$$\begin{aligned} x =< a_0, a_1, a_2 > &= a_0 + \frac{1}{a_1 + \frac{1}{a_2}} \\ &= a_0 + \frac{1}{a_1 + x_1} \\ &= \frac{a_0 a_1 + x_1 a_0 + 1}{a_1 + x_1} \\ &= \frac{(a_0 a_1 + 1) + x_1 a_0}{a_1 + x_1} \end{aligned}$$

και καθώς $b_1 = a_0 a_1 + 1, b_0 = a_0, x_1 = a_1, c_0 = 1$, η παραπάνω γίνεται $x = \frac{b_1 + x_1 b_0}{c_1 + x_1 c_0}$ που είναι η 1.6 για $i = 2$.

Έστω τώρα $i \geq 2$ και έστω οτι η 1.6 ισχύει για $i = k$, δηλαδή $x = \frac{x_k b_{k-1} + b_k}{x_k c_{k-1} + c_k}$.

Στον ορισμό όμως του συνεχούς κλάσματος, είχαμε πάρει $x_k = \frac{1}{a_{k+1} + x_{k+1}}$ απ'οπου,

$$\begin{aligned} x &= \frac{\frac{1}{a_{k+1} + x_{k+1}} \cdot b_{k-1} + b_k}{\frac{1}{a_{k+1} + x_{k+1}} \cdot c_{k-1} + c_k} \\ &= \frac{b_{k-1} + b_k a_{k+1} + b_k x_{k+1}}{c_{k-1} + b_k a_{k+1} + b_k x_{k+1}} \\ &= \frac{b_{k+1} + b_k x_{k+1}}{c_{k+1} + c_k x_{k+1}} \end{aligned}$$

και η απόδειξη ολοκληρώθηκε.

□

Παρατήρηση: Είδαμε ότι η ακολουθία a_i σταματά εαν ο x είναι ρητός. Μπορεί να δειχθεί επίσης ότι η a_i γίνεται περιοδική αν-ν $x \in \mathbb{Q}(\sqrt{n})$, $n \neq \square$ δηλαδή ο x είναι της μορφής $x_1 + x_2\sqrt{n}$, όπου $x_1, x_2 \in \mathbb{Q}$ και $n \neq \square$. Συγκεκριμένα είδαμε το Παράδειγμα 1.1, για το $\sqrt{2}$.

Παράδειγμα 1.2 *Εαν αναπτύξουμε τον αριθμό $\sqrt{3}$ σε συνεχές κλάσμα θα πάρουμε $\sqrt{3} =< 1, 1, 2, 1, 2, 1, 2, 1, \cdots >$. Σ'αυτό το σημείο ισχυριζόμαστε οτι τα a_i, εναλλάσσονται μεταξύ του 1 και του 2. Για να το αποδείξουμε αυτό, ας είναι x το άπειρο*

συνεχές κλασμα στο δεξί μέλος, του οποίου οι όροι εναλλασσονται μεταξύ του 1 *και του* 2*, δηλαδή* $x =< 1,1,2,1,2,\cdots >$*. Τότε*

$$x = 1 + \frac{1}{1 + \frac{1}{2+\frac{1}{1+\frac{1}{2+\cdots}}}} = 1 + \frac{1}{1 + \frac{1}{\underbrace{1 + 1 + \frac{1}{1+\frac{1}{2+\cdots}}}_{x}}}} = 1 + \frac{1}{1 + \frac{1}{1+x}}$$

απ'οπου λύνοντας ως προς x *την δευτεροβάθμια εξίσωση που προκύπτει, παίρνουμε* $x = \sqrt{3}$*, όπως ακριβώς θέλαμε.*

Πρόταση 4

$$\begin{aligned} &\textit{Ισχύει} \quad \frac{b_0}{c_0} < \frac{b_2}{c_2} < \cdots < \frac{b_{2k}}{c_{2k}} < \cdots < x < \cdots < \frac{b_{2k+1}}{c_{2k+1}} < \cdots < \frac{b_3}{c_3} < \frac{b_1}{c_1} \\ &\textit{και} \quad \left|x - \frac{b_i}{c_i}\right| < \frac{1}{c_i^2} \end{aligned} \tag{1.7}$$

Απόδειξη:

Χρησιμοποιώντας τις Προτάσεις 2 και 3 έχουμε

$$\begin{aligned} x - \frac{b_i}{c_i} &= \frac{x_{i+1}b_i + b_{i+1}}{x_{i+1}c_i + c_{i+1}} - \frac{b_i}{c_i} \\ &= \frac{c_i b_{i+1} - b_i c_{i+1}}{c_i(x_{i+1}c_i + c_{i+1})} \\ &= \frac{(-1)^i}{c_i(x_{i+1}c_i + c_{i+1})} \end{aligned}$$

συνεπώς επειδή οι αριθμοί x_i, c_{i-1} είναι θετικοί για $i \geq 1$, από την παραπάνω ισότητα και το Πόρισμα 1.3, έχουμε πράγματι την ισχύ της πρώτης προς απόδειξη σχέσης και καθώς

$$\left|x - \frac{b_i}{c_i}\right| = \frac{1}{c_i(x_{i+1}c_i + c_{i+1})} < \frac{1}{c_i^2}$$

□

Πόρισμα 1.4 *Ισχύει* $\lim_{i\to+\infty} \frac{b_i}{c_i} = x$

(Η απόδειξη αυτού είναι άμεση εαν λάβουμε υπ'όψιν την ανισότητα 1.7 *και οτι η ακολουθία των* c_i *είναι γνησίως αύξουσα.)*

Πρόταση 5 *Έστω* $x > 1$ *πραγματικός, του οποίου η ανάπτυξη σε συνεχές κλάσμα έχει* i*-οστό συγκλίνων ρητό στο* x*, το* $\frac{b_i}{c_i}$*. Τότε* $\forall\ i$ *ισχύει* $\left|b_i^2 - x^2 c_i^2\right| < 2x$*.*

Απόδειξη:

$$\left|b_i^2 - x^2 c_i^2\right| = c_i^2 \left|x - \frac{b_i}{c_i}\right| \left|x + \frac{b_i}{c_i}\right|$$

- **Εαν i άρτιος**, τότε $\frac{b_i}{c_i} < x < \frac{b_{i+1}}{c_{i+1}}$ και η παραπάνω σχέση γίνεται $c_i^2|x - \frac{b_i}{c_i}||x + \frac{b_i}{c_i}| < c_i^2 \cdot \frac{1}{c_i^2}|x + \frac{b_i}{c_i}| = |x + \frac{b_i}{c_i}| = x + \frac{b_i}{c_i} < 2x$ (καθώς $x > 1$).

- **Εαν i περιττός**, τότε $\frac{b_{i+1}}{c_{i+1}} < x < \frac{b_i}{c_i}$ οπότε $|x - \frac{b_i}{c_i}| < |\frac{b_i}{c_i} - \frac{b_{i+1}}{c_{i+1}}| = \frac{1}{c_i c_{i+1}}$ και τότε η παραπάνω σχέση γίνεται $c_i^2|x - \frac{b_i}{c_i}||x + \frac{b_i}{c_i}| < c_i^2 \frac{1}{c_i c_{i+1}}(x + \frac{b_i}{c_i}) = \frac{c_i}{c_{i+1}}(x + \frac{b_i}{c_i})$

  Όμως $\frac{b_i}{c_i} - \frac{b_{i+1}}{c_{i+1}} = \frac{1}{c_i c_{i+1}}$ άρα $\frac{b_i}{c_i} - \frac{1}{c_i c_{i+1}} = \frac{b_{i+1}}{c_{i+1}} < x$ απ'όπου $\frac{b_i}{c_i} < x + \frac{1}{c_i c_{i+1}}$

  άρα, συνεχίζοντας την προηγούμενη σχέση έχουμε
  $\frac{c_i}{c_{i+1}}(x + \frac{b_i}{c_i}) < \frac{c_i}{c_{i+1}}(2x + \frac{1}{c_i c_{i+1}})$ οπότε,

$$\begin{aligned} \frac{c_i}{c_{i+1}}(2x + \frac{1}{c_i c_{i+1}}) - 2x &= 2x(\frac{c_i}{c_{i+1}} + \frac{1}{2x c_i c_{i+1}} \cdot \frac{c_i}{c_{i+1}} - 1) \\ (\text{Ισχύει } 2x c_{i+1}^2 > c_{i+1}) &< 2x(-1 + \frac{c_i}{c_{i+1}} + \frac{1}{c_{i+1}}) \\ &\leq 2x(-1 + \frac{c_{i+1}}{c_{i+1}}) = 0 \end{aligned}$$

□

Πρόταση 6 *Έστω n θετικός ακέραιος ο οποίος δεν είναι τετράγωνο ακεραίου και $\frac{b_i}{c_i}$, ο i-οστός συγκλίνων ρητός της ανάπτυξης σε συνεχές κλάσμα του $\sqrt{n}$. Τότε το υπόλοιπο της διαίρεσης του b_i^2 modulo n (Το οποίο εμείς θεωρούμε οτι είναι μεταξύ του $-n/2$ έως το $n/2$. Δηλαδή επιτρέπουμε στο υπόλοιπο, να είναι και αρνητικός), είναι μικρότερο του $2\sqrt{n}$.*

Απόδειξη:

Εφαρμόζουμε την προηγούμενη πρόταση για $x = \sqrt{n}$ και παίρνουμε οτι $|b_i^2 - nc_i^2| < 2\sqrt{n}$. Όμως $b_i^2 \equiv b_i^2 - nc_i^2 \pmod{n}$ και συνεπώς αφού $|b_i^2 - nc_i^2| < 2\sqrt{n}$ άρα $|b_i^2| \pmod{n} < 2\sqrt{n}$.

□

Παρατήρηση: Η τελευταία Πρόταση είναι και το κλειδί για τον αλγόριθμο παραγοντοποίησης με συνεχή κλάσματα που θα αναφέρουμε αμέσως μετά, διότι μας βεβαιώνει οτι μπορούμε να βρούμε μία ακολουθία απο b_i, των οποίων τα τετράγωνα έχουν μικρά υπόλοιπα modulo n, παίρνοντας τους αριθμητές των συγκλίνοντων ρητών στην ανάπτυξη του $\sqrt{n}$ σε συνεχές κλάσμα. Ας σημειωθεί

οτι δεν χρειάζεται να βρούμε τον ακριβή συγκλίνοντα ρητό, αλλά μας αρκεί μόνο ο αριθμητής b_i modulo n. Συνεπώς το γεγονός οτι ο αριθμητής και ο παρανομαστής του συγκλίνοντα ρητού θα γίνουν γρήγορα πολύ μεγάλοι, δε μας ανησυχεί. Δεν χρειάζεται ποτέ να δουλέψουμε με ακέραιους μεγαλύτερους από n^2 (Όταν πολλαπλασιάσουμε ακεραίους modulo n).

1.2 Αλγόριθμος Παραγοντοποίησης ακεραίων με χρήση Συνεχών Κλασμάτων

Ορισμός 1.1 ***Βάση παραγόντων*** *είναι ενα σύνολο $B = \{p_1, p_2, \ldots, p_h\}$ διακεκριμένων πρώτων και με το p_1 να μπορεί να είναι το -1. Λέμε οτι το τετράγωνο ακεραίου b είναι* ***B-αριθμός*** *(για δοσμένο n), εαν το ελάχιστο κατ'απόλυτη τιμή πηλίκο του $b^2 \pmod n$ μπορεί να γραφτεί ως γινόμενο αριθμών από το B.*

Παράδειγμα 1.3 *Για $n = 4633$ και $B = \{-1, 2, 3\}$. Τα τετράγωνα των τριών ακεραίων $67, 68, 69$ είναι B-αριθμοί διότι $67^2 \equiv -144 \pmod{4633}, 68^2 \equiv -9 \pmod{4633}, 69^2 \equiv 128 \pmod{4633}$ και αντίστοιχα έχουμε $144 = 2^4 \cdot 3^2, 9 = 3^2, 128 = 2^7$.*

Ας συμβολίσουμε με $\mathbb{F}_2^h$, τον διανυσματικό χώρο πάνω από το σώμα με δύο στοιχεία, το οποίο περιέχει h-άδες από το σύνολο $\{0, 1\}$. Δοσμένου του n και της βάσης παραγόντων B η οποία περιέχει h αριθμούς, θα δείξουμε πώς θα αντιστοιχίσουμε ένα διάνυσμα $\overrightarrow{\epsilon} \in \mathbb{F}_2^h$ σε κάθε B-αριθμό. Γράφουμε καταρχήν το $b^2 \pmod n$ στη μορφή $\prod_{j=1}^{h} p_j^{a_j}$ και θέτουμε την j συντεταγμένη ϵ_j, ίση με $a_j \pmod 2$. Με άλλα λόγια $\epsilon_j = 0$ εαν ο a_j είναι άρτιος, και $\epsilon_j = 1$, εαν ο a_j είναι περιττός.

Παράδειγμα 1.4 *Στο παραπάνω παράδειγμα το διάνυσμα που αντιστοιχεί στο 67, είναι το $\{1, 0, 0\}$, στο 68 είναι το $\{1, 0, 0\}$ και στο 69 είναι το $\{0, 1, 0\}$.*

Έστω τώρα ότι έχουμε κάποιους από τους B-αριθμούς $b_i^2 \pmod n$, τέτοιους ώστε τα αντίστοιχα διανύσματα $\overrightarrow{\epsilon_i} = \{\epsilon_{i1}, \epsilon_{i2}, \ldots, \epsilon_{ih}\}$ όταν προστεθούν δίνουν το μηδενικό διάνυσμα του $\mathbb{F}_2^h$. Τότε προφανώς το γινόμενο των ελαχίστων (κατ'απόλυτη τιμή) υπολοίπων $b_i^2 \pmod 2$, είναι ίσο με ένα γινόμενο αρτίων δυνάμεων όλων των $p_j \in B$, το οποίο σημαίνει οτι εαν $\forall\ i$, συμβολίσουμε με a_i το ελάχιστο κατ'απόλυτη τιμή υπόλοιπο $b_i^2 \pmod n$ και γράψουμε

$$a_i = \prod_{j=1}^{h} p_j^{a_{ij}}, \quad \text{τότε παίρνουμε} \quad \prod a_i = \prod_{j=1}^{h} p_j^{\sum_i a_{ij}}$$

με τον εκθέτη του κάθε πρώτου p_j στο δεξί μέλος της παραπάνω, να είναι άρτιος. Τότε το δεξί μέλος, είναι τετράγωνο του $\prod_j p_j^{\gamma_j}$ με $\gamma_j = \frac{1}{2}\sum_i a_{ij}$. Εαν θέσουμε λοιπόν $b = \prod_i b_i \pmod n$ (παίρνουμε το ελάχιστο κατ'απόλυτη τιμή υπόλοιπο) και $c = \prod_i p_j^{\gamma_j} \pmod n$ (παίρνουμε το ελάχιστο κατ'απόλυτη τιμή υπόλοιπο και

πάλι), παίρνουμε δύο αριθμούς b, c που ενώ κατασκευάστηκαν με διαφορετικό τρόπο (ο ένας ως γινόμενο των b_i και ο άλλος ως γινόμενο των p_j), έχουν $b^2 \equiv c^2 \pmod{n}$. Εαν λοιπόν $b \not\equiv \pm c \pmod{n}$ τότε έχουμε βρει ένα μη τετριμμένο διαιρέτη του n παίρνοντας το $(b+c, n)$ ή το $(b-c, n)$.

Εαν όμως $b \equiv \pm c \pmod{n}$, τότε χρειάζεται να επαναλάβουμε τη διαδικασία μεγαλώνοντας την βάση παραγόντων B που αρχικά απιλέξαμε.

Αλγόριθμος Παραγοντοποίησης

Ας θεωρήσουμε n ένα ακέραιο τον οποίο θέλουμε να παραγοντοποιήσουμε. Όλες οι πράξεις παρακάτω θα γίνουν modulo n παίρνοντας το ελάχιστο μη αρνητικό υπόλοιπο (ή το ελάχιστο κατ'απόλυτη τιμή υπόλοιπο, στο Βήμα 3 του Αλγορίθμου). Θέτουμε αρχικά $b_{-1} = 1, b_0 = a_0 = [\sqrt{n}]$ και τέλος $x_0 = \sqrt{n} - a_0$. Λογαριάζουμε το $b_0^2 \pmod{n}$ (το οποίο θα είναι το $b_0^2 - n$). Αμέσως μετά για $i = 1, 2, \ldots$ ακολουθούμε τα παρακάτω βήματα διαδοχικά:

1. Θέτουμε $a_i = \big[\frac{1}{x_{i-1}}\big]$ και μετά $x_i = \frac{1}{x_{i-1}} - a_i$.

2. Υπολογίζουμε το $b_i = a_i b_{i-1} + b_{i-2} \pmod{n}$.

3. Υπολογίζουμε το $b_i^2 \pmod{n}$. Κάνοντας τον υπολογισμό αυτό για μερικά i, διάλεξε εκείνους τους αριθμούς στο βήμα 3, οι οποίοι παραγοντοποιούνται $\pm$ ως γινόμενο μικρών πρώτων και πάρε μία βάση παραγόντων B που να περιέχει το -1, καθώς επίσης και τους πρώτους που εμφανίζονται περισσότερες από μία φορές στο $b_i^2 \pmod{n}$ (ή που εμφανίζονται σε άρτια δύναμη σε ένα και μόνο $b_i^2 \pmod{n}$). Κάνε μετά μία λίστα που να περιέχει τους αριθμούς $b_i^2 \pmod{n}$ απ'τους οποίους προέκυψε η βάση B, και τα αντίστοιχα διανύσματα $\overrightarrow{\epsilon}$, που να περιέχουν μηδενικά και άσσους, τα οποία είναι τα διανύσματα ανάλυσης του αριθμού στην βάση B που έχουμε επιλέξει. Εαν είναι δυνατόν, να βρεθεί ένα υποσύνολο αυτών των αριθμών, των οποίων το άθροισμα των αντίστοιχων διανύσμάτων να κάνει μηδέν modulo κάποιο οποιοδήποτε αριθμό που διαλέγω. Θέτουμε $b = \prod b_i$ (δουλεύοντας modulo n και παίρνοντας το γινόμενο πάνω από το υποσύνολο για το οποίο $\sum \overrightarrow{\epsilon} = 0$). Θέτουμε $c = \prod p_j^{\gamma_j}$, όπου τα p_j είναι στοιχεία του B (εκτός του -1), και $\gamma_j = \frac{1}{2}\sum a_{ij}$.

   Εαν $b \equiv \pm c \pmod{n}$, τότε ψάχνουμε για κάποιο άλλο υποσύνολο δεικτών i τέτοιων ώστε $\sum \overrightarrow{\epsilon_i} = 0$. Εαν κάτι τέτοιο δεν είναι εφικτό, τότε πρέπει να υπολογίσουμε κι άλλα a_i, b_i και $b_i^2 \pmod{n}$, ώστε να μεγαλώσουμε την βάση παραγόντων B.

□

Παρατήρηση: Για να μπορούμε εύκολα να υπολογίζουμε το $c = \prod p_j^{\gamma_j}$, είναι αρκετό εαν για κάθε B-αριθμό $b_i^2 \pmod{n}$ πάρουμε το διάνυσμα $\overrightarrow{\alpha_i} = \{\ldots, a_{ij}, \ldots\}_j$ αντί του $\overrightarrow{\epsilon_i}$, το οποίο είναι ίδιο με το $\overrightarrow{\alpha_i}$ υπολογισμένο $\pmod{2}$.

Παράδειγμα 1.5 *Θα χρησιμοποιήσουμε τον παραπάνω αλγόριθμο για να παραγοντοποιήσουμε τον αριθμό* 9073. *Κάνουμε καταρχήν μία λίστα με τα* a_i, b_i *(όπου* b_i*, είναι το ελάχιστο μη αρνητικό υπόλοιπο modulo* n *του* $a_i b_{i-1} + b_{i-2}$*) καθώς επίσης και το ελάχιστο κατ'απόλυτη τιμή υπόλοιπο modulo* n *του* b_i^2*:*

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

$(48 = 2^4 \cdot 3, 87 = 3 \cdot 29, 27 = 3^3)$

Παρατηρώντας λοιπόν την τελευταία γραμμή του παραπάνω πίνακα βλέπουμε οτι είναι λογικό να πάρουμε ως βάση παραγόντων B=$\{-1, 2, 3, 7\}$. *Τότε το* $b_i^2 \pmod n$ *είναι* B*-αριθμός για* $i = 0, 2, 4$. *Τα αντίστοιχα διανύσματα* $\overrightarrow{\alpha_i}$*, είναι* $\{1, 4, 1, 0\}, \{1, 0, 0, 1\}$ *και* $\{1, 0, 3, 0\}$. *Το άθροισμα του πρώτου και τρίτου διανύσματος είναι μηδέν modulo* 2. *Διαλέγουμε λοιπόν* $b = 95 \cdot 2619 \equiv 3834 \pmod{9073}$*, και* $c = 2^2 \cdot 3^2 = 36$. *Συνεπώς με αυτό τον τρόπο έχουμε* $3834^2 \equiv 36^2 \pmod{9073}$ *και καθώς* $3834 \not\equiv \pm 36 \pmod{9073}$*, παίρνουμε τον μη τετριμμένο παράγοντα* $(3834 + 36, 9073) = 43$. *Τελικά λοιπόν* $9073 = 43 \cdot 211$.

Παράδειγμα 1.6 *Θα παραγοντοποιήσουμε τον αριθμό* 17873. *'Οπως και στο προηγούμενο παράδειγμα φτιάχνουμε τον ίδιο πίνακα:*

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

$(184 = 2^3 \cdot 23, 56 = 2^3 \cdot 7, 64 = 2^6, 161 = 7 \cdot 23)$

Εαν θέσουμε B=$\{-1, 2, 7, 23\}$*, τότε έχουμε* B*-αριθμούς όταν* $i = 0, 2, 4, 5$. *Τα αντίστοιχα διανύσματα* $\overrightarrow{\alpha_i}$*, είναι* $\{1, 3, 0, 1\}, \{1, 3, 1, 0\}, \{1, 6, 0, 0\}, \{0, 0, 1, 1\}$. *Το άθροισμα του πρώτου, δεύτερου και τέταρτου από αυτά τα διανύσματα είναι μηδέν modulo* 2. *Εντούτοις υπολογίζουμε οτι* $b = 133 \cdot 401 \cdot 13369 \equiv 1288 \pmod{17873}$ *και οτι* $c = 2^3 \cdot 7 \cdot 23 = 1288$ *και έτσι βρίσκουμε οτι* $b \equiv c \pmod{17873}$. *Συνεπώς πρέπει να βρούμε κι άλλους* B*-αριθμούς των οποίων τα αντίστοιχα διανύσματα θα έχουν άθροισμα 0 modulo* 2. *Συνεχίζοντας του παραπάνω πίνακα για μερικά ακόμη* i *παίρνουμε:*

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

$(77 = 7 \cdot 11, 88 = 2^3 \cdot 11)$

Εαν προσθέσουμε στην βάση παραγόντων B, τον αριθμό 11*, δηλαδή B=* $\{-1, 2, 7, 11, 23\}$*, τότε για* $i = 0, 2, 4, 5, 6, 8$ *παίρνουμε B-αριθμούς, με αντίστοιχα διανύσματα* $\overrightarrow{\alpha_i}$ *τα* $\{1, 3, 0, 0, 1\}$*,* $\{1, 3, 1, 0, 0\}$*,* $\{1, 6, 0, 0, 0\}$*,* $\{0, 0, 1, 0, 1\}$*,* $\{1, 0, 1, 1, 0\}$*,* $\{1, 3, 0, 1, 0\}$*. Το άθροισμα του δεύτερου, τρίτου, πέμπτου και έκτου είναι 0 modulo* 2*. Τέλος* $b = 7272$*,* $c = 4928$*, και έτσι βρήκαμε ένα μη τετριμμένο διαιρέτη του* 17873*, τον* $(7272 + 4928, 17873) = 61$ *και έτσι* $17873 = 61 \cdot 293$*.*

2 rho Μέθοδος του Pollard

Περίληψη

Ας υποθέσουμε οτι ένας αρκετά μεγάλος ακέραιος n είναι σύνθετος. Για παράδειγμα έχουμε βρει οτι κάποιο από τα ¨primality tests¨ που έχουμε αναφέρει εως τώρα αποτυγχάνει. Αυτό βέβαια δεν συνεπάγεται οτι γνωρίζουμε για το τί ιδιότητες έχει ο παράγοντας του n. Μόνο ο πολύ αργός αλγόριθμος που εξετάζει όλους τους διαδοχικούς πρώτους μέχρι το $\sqrt{n}$ μας δίνει αποτέλεσμα για το αν ο n είναι πρώτος ή σύνθετος και εαν n σύνθετος τότε μας λέει και τους παράγοντές του. Στην πραγματικότητα ο αλγόριθμος αυτός μας δίνει ένα πρώτο παράγοντα στον ίδιο χρόνο που μας λέει εαν είναι σύνθετος ή όχι. Όλοι οι υπόλοιποι αλγόριθμοι οι οποίοι είναι γρηγορότεροι μας λένε μεν οτι ο n έχει κάποιο γνήσιο παράγοντα αλλά δε μας δίνουν περισσότερες πληροφορίες για το ποιός είναι. Η μέθοδος που εξετάζει όλους τους διαδοχικούς πρώτους μέχρι το $\sqrt{n}$ παίρνει περισσότερο χρόνο απο $O(\sqrt{n})$ 2-αδικές πράξεις. Ο απλούστερος αλγόριθμος παραγοντοποίησης, ο οποίος είναι πολύ ταχύτερος από τον προηγούμενο, είναι του **J.M. Pollard "Η rho μέθοδος**¨.

Το πρώτο βήμα στη rho μέθοδο είναι να διαλέξουμε μία εύκολα υπολογίσιμη απεικόνιση από το $\mathbb{Z}_n$ στον εαυτό του και συγκεκριμένα ένα απλό πολυώνυμο με ακέραιους συντελεστές (π.χ. $f(x) = x^2 + 1$). Στο επόμενο βήμα διαλέγουμε ένα συγκεκριμένο $x = x_0$ [συνήθως παίρνουμε το 1 ή το 2 είτε διαλέγουμε το x_0 με κάποιο τρόπο τυχαίο (randomly generated integer)], και υπολογίζουμε διαδοχικά τις συνθέσεις της f στο x: $x_1 = f(x_0), x_2 = f(f(x_0)), x_3 = f(f(f(x_0)))$, κ.ο.κ. το οποίο σημαίνει οτι ορίζουμε:

$$x_{j+1} = f(x_j), \quad j = 0, 1, 2, \ldots$$

Μετά κάνουμε σύγκριση μεταξύ των διαφορετικών x_j, ελπίζοντας οτι θα βρούμε δύο οι οποίοι ανήκουν σε διαφορετική κλάση υπολοίπων $modulon$, αλλά στην ίδια κλάση $modulo$ κάποιο διαιρέτη του n. Μόλις βρούμε τέτοια x_j, x_k, έχουμε τελειώσει καθώς $(x_j - x_k, n) = m$, όπου m ένας γνήσιος διαιρέτης του n.

Παράδειγμα 2.1 *Ας παραγοντοποιήσουμε το* 91 *με την παραπάνω μέθοδο διαλέγοντας* $f(x) = x^2 + 1, x_0 = 1$*. Τότε* $x_1 = 2, x_2 = 5, x_3 = 26$*, κ.τ.λ. Βρίσκουμε οτι* $(x_3 - x_2, n) = (21, 91) = 7$ *άρα το* 7 *είναι διαιρέτης του* 91*. Οπωσδήποτε αυτό είναι τετριμμένο παράδειγμα, το οποίο θα μπορούσαμε να το λύσουμε εξίσου γρήγορα δοκιμάζοντας τους πρώτους τους μικρότερους του* $\sqrt{91}$*.*

Στη rho μέθοδο είναι σημαντικό να διαλέξουμε ένα πολυώνυμο $f(x)$ το οποίο απεικονίζει το $\mathbb{Z}_n$ στον εαυτό του με τρόπο ανεξάρτητο, ¨τυχαίο¨. Για παράδειγμα θα δείξουμε αργότερα οτι το $f(x)$ δεν πρέπει να είναι ένα γραμμικό πολυώνυμο, καθώς επίσης να μη δίνει μία $1-1$ απεικόνιση.

Ας υποθέσουμε λοιπόν οτι η $f(x)$ είναι μία ¨τυχαία¨ απεικόνιση του $\mathbb{Z}_n$ στο $\mathbb{Z}_n$, και υπολογίζουμε πόσο χρόνο πρέπει να περιμένουμε πριν βρούμε δύο συνθέσεις x_j, x_k τέτοιες ώστε η διαφορά $x_j - x_k$ να είναι μη τετριμμένος διαιρέτης του n. Το κάνουμε αυτό παίρνοντας ένα συγκεκριμένο διαιρέτη r του n (ο οποίος στην πράξη, δεν είναι γνωστός ακόμη) και υπολογίζουμε μία προσέγγιση του πρώτου δείκτη k για τον οποίο υπάρχει $j < k$ με $x_j < x_k \pmod r$. Με άλλα λόγια θεωρούμε την απεικόνιση $f(x)$ από το $\mathbb{Z}_n$ στο $\mathbb{Z}_n$ και ζητούμε να βρούμε πόσες συνθέσεις χρειάστηκαν πριν ξαναβρούμε την πρώτη επανάληψη των τιμών $x_k = x_j$ στο $\mathbb{Z}_n$.

Πρόταση 7 *Έστω S ένα σύνολο με r στοιχεία και μία απεικόνιση $f : S \to S$ και $x_o \in S$. Έστω $x_{j+1} = f(x_j)$ για $j = 0, 1, 2, \ldots$. Θεωρούμε λ ένα θετικό ακέραιο αριθμό και $l = 1 + [\sqrt{2\lambda r}]$. Τότε η αναλογία ζευγών (f, x_o) για τα οποία τα $x_0, x_1, \ldots, x_l$ είναι διακεκριμένα και η f διατρέχει όλες τις δυνατές απεικονίσεις από το S στο S και το x_0 διατρέχει όλα τα στοιχεία του S, είναι μικρότερη από $e^{-\lambda}$.*

Απόδειξη:

Ο συνολικός αριθμός ζευγών είναι r^{r+1} καθώς υπάρχουν r επιλογές για το x_0 και για κάθε ένα από τα r διαφορετικά $x \in S$, υπάρχουν r επιλογές για το $f(x)$ (Γνωρίζουμε οτι εαν $f : S \to S$ είναι μία απεικόνιση και $|S| = r$ τότε οι δυνατές συναρτήσεις που μπορώ να κατασκευάσω είναι r^r). Πόσα ζεύγη (f, x_0) υπάρχουν για τα οποία τα $x_0, x_1, \ldots, x_l$ είναι διακεκριμένα; Υπάρχουν r επιλογές για το x_0, $r-1$ επιλογές για το $f(x_0) = x_1$ (αφού αυτό δεν μπορεί να είναι ίσο με το x_0),$r-2$ επιλογές για το $f(x_1) = x_2$, και συνεχίζοντας έτσι μέχρι να οριστεί η f για $x = x_0, x_1, \ldots, x_{l-1}$. Τότε η τιμή για κάθε ένα x από τα υπόλοιπα $r-l$ που μένουν, είναι αυθαίρετη, δηλάδή υπάρχουν r^{r-l} επιλογές για τις τιμές αυτές. Συνεπώς ο συνολικός αριθμός των επιλογών του x_0 και των τιμών $f(x)$ έτσι ώστε τα $x_0, x_1, \ldots, x_l$ να είναι διακεκριμένα είναι

$$r^{r-l} \prod_{j=0}^{l} (r-j)$$

και η αναλογία ζευγών που έχουν την παραπάνω ιδιότητα (δηλαδή ο παραπάνω αριθμός όταν διαιρεθεί με το r^{r+1}), είναι

$$r^{-l-1} \prod_{j=0}^{l} (r-j) = \prod_{j=1}^{l} (1 - \frac{j}{r})$$

Μένει λοιπόν να δείξουμε οτι ο λογάριθμος του παραπάνω είναι μικρότερος από $-\lambda$ (όπου $l = 1 + [\sqrt{2\lambda r}]$). Για να το αποδείξουμε αυτό παίρνουμε το λογάριθμο

του δεξιού μέλους και χρησιμοποιούμε και το γεγονός ότι $\log(1-x) < -x$ για $0 < x < 1$. Έτσι έχουμε

$$\begin{aligned} \log \prod_{j=1}^{l}(1-\frac{j}{r}) &< \sum_{j=1}^{l}(-\frac{j}{r}) = \frac{-l(l+1)}{2r} \\ &< \frac{-l^2}{2r} < \frac{-(\sqrt{2\lambda r})^2}{2r} = -\lambda \end{aligned}$$

όπως ακριβώς θέλαμε.

□

Η σημασία της Πρότασης αυτής είναι οτι δίνει μία εκτίμηση για τον πιθανό χρόνο που χρειάζεται η rho μέθοδος, εφόσον θεωρήσουμε δεδομένο οτι το πολυώνυμό μας συμπεριφέρεται περίπου σαν μία απεικόνιση από το $\mathbb{Z}_n$ στο $\mathbb{Z}_n$. Θα κάνουμε μία μικρή βελτίωση της rho μεθόδου ώστε να είναι αποτελεσματικότερη.

Ας θυμηθούμε καταρχήν οτι η rho μέθοδος δουλεύει υπολογίζοντας τις διαδοχικές συνθέσεις $x_k = f(x_{k-1})$ και συγκρίνει το x_k με τα προηγούμενα x_j μέχρι να βρει ένα ζεύγος που ικανοποιεί την $(x_k - x_j, n) = r > 1$. Όταν όμως το k μεγαλώσει αρκετά τότε είναι αρκετά χρονοβόρο να υπολογίζουμε το $(x_k - x_j, n)$ για κάθε $j < k$. Θα περιγράψουμε τώρα ένα τρόπο ώστε να χρειάζεται για κάθε k, να υπολογίζουμε κάθε φορά μόνο ένα Μ.Κ.Δ.. Καταρχήν παρατηρούμε οτι εαν υπάρχει ζεύγος (k_0, j_0), τέτοιο ώστε $x_{k_0} \equiv x_{j_0} \pmod r$ για κάποιο διαιρέτη $r|n$ τότε έχουμε την ίδια σχέση $x_k \equiv x_j \pmod r$ για κάθε ζεύγος δεικτών j, k που έχουν την ίδια διαφορά $k - j = k_0 - j_0$. Για να το δούμε αυτό, απλά θέτουμε $k = k_0 + m, j = j_0 + m$ και εφαρμόζουμε επανειλημμένως την συνάρτηση f και στα δύο μέλη της $x_{k_0} \equiv x_{j_0} \pmod r$, m φορές.

Θα περιγράψουμε τώρα πώς δουλεύει ο αλγόριθμος για την rho μέθοδο.

- Υπολογίζουμε διαδοχικά τα x_k και για κάθε k προχωράμε ως εξής: Ας υποθέσουμε οτι ο k είναι ένας $(h+1)$-ψήφιος αριθμός στο 2-αδικό σύστημα (δηλαδή έχει όπως λέμε $(h+1)$-bits) οπότε $2^h \leq k < 2^{h+1}$ και έστω j ο μεγαλύτερος αριθμός με h-bits δηλαδή $j = 2^h - 1$. Συγκρίνουμε το x_k με αυτό το συγκεκριμένο x_j, δηλαδή υπολογίζουμε το $(x_k - x_j, n)$. Εαν ο Μ.Κ.Δ. δώσει ένα μη τετριμμένο παράγοντα του n σταματούμε. Διαφορετικά προχωράμε στο $k+1$.

Αυτή η λίγο παραλαγμένη μορφή της μεθόδου έχει το πλεονέκτημα οτι υπολογίζουμε μόνο ένα Μ.Κ.Δ. για κάθε ακέραιο k. Έχει όμως το μειονέκτημα οτι πιθανόν να μη βρει πότε για πρώτη φορά έχουμε κάποιο k_0, με $(x_{k_0} - x_{j_0}, n) = r > 1$ για κάποιο $j_0 < k_0$.

Παρόλ'αυτά κάποια στιγμή (όχι μετά από πολύ χρόνο), θα βρούμε ένα τέτοιο ζεύγος x_k, x_j του οποίου η διαφορά θα έχει κάποιο κοινό διαιρέτη με το n. Δηλαδή, ας υποθέσουμε οτι ο k_0 έχει $(h+1)$-bits. Θέτουμε τότε $j = 2^{h+1} - 1$ και $k = j + (k_0 - j_0)$ στην οποία περίπτωση το j είναι ο μεγαλύτερος ακέραιος με $(h+1)$-bits και ο k είναι ένας ακέραιος με $(h+2) - bits$ ώστε να ισχύει $(x_k - x_j, n) > 1$. Ας σημειωθεί οτι $k < 2^{h+2} = 4 \cdot 2^h \leq 4k_0$.

Παράδειγμα 2.2 *Ας επιστρέψουμε και πάλι στο παράδειγμα 2.1 αλλά ας συγκρίνουμε κάθε x_k μόνο με το αντίστοιχο x_j, το οποίο j είναι ο μεγαλύτερος ακέραιος $< k$ της μορφής $2^h - 1$. Για $n = 91, f(x) = x^2 + 1, x_0 = 1$ έχουμε $x_1 = 2, x_2 = 5, x_3 = 26$ όπως πριν, και $x_4 = 40$ (αφού $26^2 + 1 \equiv 40 \pmod{91}$). Ακολουθώντας τον αλγόριθμο που περιγράψαμε παραπάνω, βρίσκουμε για πρώτη φορά ένα παράγοντα του n όταν υπολογίσουμε το $(x_4 - x_3, n) = (14, 91) = 7$.*

Παράδειγμα 2.3 *Θα παραγοντοποιήσουμε τον αριθμό 4087 χρησιμοποιώντας το $f(x) = x^2 + x + 1$ και $x_0 = 2$. Οι υπολογισμοί μας σύμφωνα με τον παραπάνω αλγόριθμο φαίνονται παρακάτω*

$$\begin{aligned}
x_1 = f(2) = 7; (x_1 - x_0, n) &= (7 - 2, 4087) = 1 \\
x_2 = f(7) = 57; (x_2 - x_1, n) &= (57 - 7, 4087) = 1 \\
x_3 = f(57) = 3307; (x_3 - x_1, n) &= (3307 - 7, 4087) = 1 \\
x_4 = f(3307) \equiv 2745 \pmod{4087}; (x_4 - x_3, n) &= (2745 - 3307, 4087) = 1 \\
x_5 = f(2745) \equiv 1343 \pmod{4087}; (x_5 - x_3, n) &= (1343 - 3307, 4087) = 1 \\
x_6 = f(1343) \equiv 2626 \pmod{4087}; (x_6 - x_3, n) &= (2626 - 3307, 4087) = 1 \\
x_7 = f(2626) \equiv 3734 \pmod{4087}; (x_7 - x_3, n) &= (3734 - 3307, 4087) = 61
\end{aligned}$$

Άρα λοιπόν το 61 είναι διαιρέτης του 4087 και έτσι παίρνουμε $4087 = 61 \cdot 67$.

Παρατήρηση: Ένας άλλος τρόπος προσέγγισης του ίδιου αλγορίθμου είναι να λογαριάσουμε για $k \geq 2$, τις διαφορές $x_{2k-2} - x_{k-1}$. Έπειτα αρκεί να λογαριάσουμε τον Μ.Κ.Δ. των παραπάνω διαφορών με το n καθώς όπως αναφέραμε προηγουμένως, εαν υπάρχει κάποιο ζεύγος δεικτών k_0, j_0, για τους οποίους να έχουμε $x_{k_0} \equiv x_{j_0} \pmod{n}$, τότε ισχύει $x_k \equiv x_j \pmod{n}$, για k, j με $k - j = k_0 - j_0$. Συνεπώς εαν βρούμε $1 < (x_{2k-2} - x_{k-1}, n) < n$ για κάποιο $k = 2, 3, \ldots$ τότε έχουμε βρεί ένα γνήσιο διαιρέτη του n, ενώ εαν $(x_{2k-2} - x_{k-1}, n) = n$ για κάποιο k, τότε επιλέγουμε κάποιο διαφορετικό x_0 ή κάποιο διαφορετικό πολυώνυμο $f(x)$ για τους υπολογισμούς μας.

Αναφορές

[1] N. Koblitz, A Course in Number Theory and Cryptography, Second Edition (1994) p. 138–160.

[2] A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography. Fifth Printing (2001) p.91–92.

[3] S. Archava, Pollard's rho method using Maple, http://www.math.purdue.edu/∼archava/math490.html

[4] Ι. Αντωνιάδης, Διαλέξεις μαθημάτων στα Συνεχή Κλάσματα

[5] Κ. Λάκκης, Θεωρία Αριθμών (1980)

[6] Κ. Λάκκη-Γ.Τζιντζή, Ασκήσεις Θεωρίας Αριθμών (1991)

[7] Δ. Πουλάκης, Θεωρία αριθμών: Μια σύγχρονη θεώρηση της κλασσικής Θεωρίας Αριθμών (1997)

[8] Θ. Ν. Καζαντζή, Θεωρία Αριθμών, Β΄ Έκδοση (1997)