Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών
Εθνικό Μετσόβιο Πολυτεχνείο

Τετραγωνικά Υπόλοιπα και Συνεχή Κλάσματα

Διπλωματική Εργασία

Κωνσταντίνος Μάστακας

2011

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ
Χρήστος Κουκουβίνος, Καθηγητής Σ.Ε.Μ.Φ.Ε
Αλέξανδρος Παπαϊωάννου, Αν. Καθηγητής Σ.Ε.Μ.Φ.Ε(επιβλέπων)
Πέτρος Στεφανέας, Λέκτορας Σ.Ε.Μ.Φ.Ε

ΠΡΟΛΟΓΟΣ

Η διπλωματική μου εργασία έχει σαν στόχο την μελέτη και ανάλυση της θεωρίας των "Τετραγωνικών Υπολοίπων" και των "Συνεχών Κλασμάτων", δύο πολύ βασικών κλάδων της θεωρίας αριθμών, που έχουν εφαρμογή στην Κρυπτογραφία.

Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή στην θεωρία αριθμών. Μελετάται η έννοια της διαιρετότητας, αποδεικνύεται η απειρία των πρώτων και το θεμελιώδες θεώρημα της αριθμητικής. Ακόμα, ορίζεται η ισοδυναμία μεταξύ δύο αριθμών και στο τέλος του κεφαλαίου αποδεικνύονται τα θεωρήματα Euler και Fermat.

Στο δεύτερο κεφάλαιο μελετάμε τα τετραγωνικά υπόλοιπα ενός αριθμού. Στην αρχή αποδεικνύουμε ιδιότητες των τετραγωνικών υπολοίπων περιττών πρώτων, εισάγουμε το σύμβολο του Legendre και διατυπώνουμε το κριτήριο Euler. Στην συνέχεια αποδεικνύουμε ένα από τα πιο βασικά θεωρήματα στην θεωρία αριθμών, τον "Νόμο της τετραγωνικής αντιστροφής". Τελειώνοντας το κεφάλαιο επεκτείνουμε το σύμβολο Legendre στο σύμβολο Jacobi και κλείνουμε το κεφάλαιο με έναν αλγόριθμο που υπολογίζει το σύμβολο Jacobi.

Στο τρίτο κεφάλαιο ενδιαφερόμαστε να βρούμε με αποδοτικό τρόπο τις τετραγωνικές ρίζες των τετραγωνικών υπολοίπων. Παραθέτουμε τους κλειστούς τύπους που υπάρχουν για τους πρώτους που αφήνουν υπόλοιπο 3 και 5 στην διαίρεση με το 4 και το 8 αντίστοιχα. Έπειτα παραθέτουμε τον αλγόριθμο των Tonelli και Shanks και τέλος αναπτύσουμε τον αλγόριθμο του Cornacchia.

Στο τέταρτο και τελευταίο κεφάλαιο κάνουμε μια εισαγωγή στα συνεχή κλάσματα. Στην αρχή τα ορίζουμε και μελετάμε τις ιδιότητες των συγκλίνοντών τους. Ύστερα δείχνουμε ότι κάθε πραγματικός αριθμός μπορεί να αναπαρασταθεί μοναδικά από ένα συνεχές κλάσμα και κλείνουμε το κεφάλαιο αποδεικνύοντας ότι τα συνεχή κλάσματα αποτελούν την καλύτερη προσέγγιση ενός πραγματικού αριθμού.

Ευχαριστίες

Θα ήθελα κατ' αρχάς να ευχαριστήσω όλους τους καθηγητές της σχολής μου για όλες τις πολύτιμες γνώσεις που μου έχουν χαρίσει. Θα ήθελα ιδιαίτερα να ευχαριστήσω τον κύριο Αλέξανδρο Παπαϊωάννου, ο οποίος ήταν ο επιβλέπων της διπλωματικής μου εργασίας, με προέτρεψε να ασχοληθώ με αυτό το θέμα και με βοήθησε να μάθω αρκετά πράγματα που δεν ήξερα στην θεωρία αριθμών. Θα ήθελα επίσης να ευχαριστήσω τον συμφοιτητή μου Βασίλη Παλασσόπουλο που μου συνέστησε το πρόγραμμα "lyx" για να γράφω σε "latex" και με βοήθησε να μάθω να γράφω στο πρόγραμμα αυτό. Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου για ό,τι έχουν κάνει για εμένα μέχρι τώρα.

Contents

1 Εισαγωγή στην Θεωρία Αριθμών

1.1 Διαιρετότητα

Theorem 1.1.1 (Ευκλείδια διαίρεση). *Έστω a, b ακέραιοι αριθμοί, με $b \neq 0$, τότε υπάρχουν μοναδικοί ακέραιοι q, r τέτοιοι ώστε:*

$$a = bq + r, \ \mu\epsilon \ 0 \leq r < |b|$$

Οι αριθμοι q, r ονομάζονται πηλίκο, υπόλοιπο αντίστοιχα της διαίρεσης του a δια του b.

Proof. Έστω το σύνολο $S = \{a - bx : x\epsilon\mathbb{Z}\}$ και $A = \{z \in A : z \geq 0\}$.

Το A είναι ένα μη κενό σύνολο καθώς για $x = -|a|\frac{|b|}{b}$, έχουμε ότι :

$$a - b\left(-|a|\frac{|b|}{b}\right) = a + |a||b| \geq a + |a| \geq 0.$$

Τότε, έστω $r = \min A$.

Τότε $r = a - bq$ για κάποιον $q \in \mathbb{Z}$ οπότε $a = bq + r$.

Θα αποδείξουμε ότι $r < |b|$.

Έστω ότι $r \geq |b|$, τότε θα έχουμε ότι: $0 \leq r - |b| < r$.

Όμως, $0 \leq r - |b| = (a - bq) - b\frac{|b|}{b} = a - b\left(q + \frac{|b|}{b}\right)\epsilon A$.

Οπότε το $r - |b|$ είναι στοιχείο του A μικρότερο από το r.

Άτοπο, καθώς έχουμε επιλέξει το r ως το ελάχιστο στοιχείο του A.

Άρα $r < |b|$.

Για την μοναδικότητα των q και r , θεωρώ ότι υπάρχουν δυο άλλοι ακέραιοι q' και r' τέτοιοι ώστε :

$$a = bq + r = bq' + r'$$

όπου

$$0 \leq r, r' < |b|.$$

.

Τότε, από τις παραπάνω προκύπτει ότι:

$$0 \leq |r - r'| < |b| \text{ και } |r - r'| = |b||q - q'|.$$

Αν $q \neq q'$ τότε $|q - q'| \neq 0$, οπότε $|r - r'| \geq |b|$, το οποίο είναι άτοπο.
Άρα $q = q'$.
Οπότε, $r = r'$.
Οπότε οι αριθμοί q, r είναι μοναδικοί. □

Remark. Το πηλίκο και το υπόλοιπο της ευκλείδιας διαίρεσης είναι μοναδικά γιατί ισχύει ότι $0 \leq r < |b|$. Αν αυτή η συνθήκη δεν ίσχυε, τότε δεν θα ήταν μοναδικά.

Το υπόλοιπο και το πηλίκο της διαίρεσης του a δια του b θα το γράφουμε και ως $a\mathrm{mod}b$ και $a\mathrm{div}b$ αντίστοιχα.

Example. Για $a = 14$ και $b = 3$ έχουμε ότι $14 = 3 \cdot 4 + 2$, οπότε $q = 4$ και $r = 2$
Ενώ, για $a = 14$ και $b = -3$ έχουμε ότι $14 = (-3) \cdot (-4) + 2$, οπότε $q = -4$ και $r = 2$

Definition. Έστω a, b ακέραιοι αριθμοί, αν το υπόλοιπο της διαίρεσης του a δια του b είναι μηδέν, τότε θα λέμε ότι ο b διαιρεί τον a ή ισοδύναμα ο a είναι πολλαπλάσιο του b και θα γράφουμε $b|a$ (ο αριθμός b διαιρεί τον a)

Remark. Ο παραπάνω ορισμός είναι ισοδύναμος με το να λέμε ότι για τους ακέραιους a, b, ο b διαιρεί τον a αν και μόνο αν υπάρχει ακέραιος k τέτοιος ώστε $a = kb$

Proposition 1.1.2 (Ιδιότητες διαιρετότητας)**.** *Έστω οι ακέραιοι αριθμοί a, b, c, d τότε ισχύουν τα ακόλουθα*

1. Αν $a|b$ και $b|c$ τότε $a|c$
2. Αν $a|b$ τότε $a|mb$ για κάθε ακέραιο m
3. Αν $ab|c$ τότε $a|c$ και $b|c$ με $a, b \neq 0$
4. Αν $a|b$ και $c|d$ τότε $ac|bd$
5. Αν $a|b$ και $b \neq 0$ τότε $|a| \leq |b|$
6. Αν $a|b$ και $a|c$ τότε για κάθε $x, y \in \mathbb{Z}$ ισχύει ότι $a|\,(bx + cy)$
7. Αν $a|b$ και $b|a$ τότε $a = \pm b$

Η απόδειξη των παραπάνω παραλείπεται

Definition. Έστω $a, b, c \in \mathbb{Z}$ με $(a, b) \neq (0, 0)$, θα λέμε ότι ο c είναι ο μέγιστος κοινός διαιρέτης των a, b αν ικανοποιεί τα εξής:

1. $c|a$ και $c|b$
2. αν $d|a$ και $d|b$, τότε $d \leq c$

Τον μέγιστο κοινό διαιρέτη των a, b θα τον συμβολίζουμε ως $\mathrm{ΜΚΔ}(a, b)$ ή $\mathrm{GCD}(a, b)$ ή (a, b).

Remark. Προφανώς $\text{ΜΚΔ}(a,b) = \text{ΜΚΔ}(-a,b) = \text{ΜΚΔ}(a,-b) = \text{ΜΚΔ}(-a,-b)$. Οπότε για να βρούμε τον μέγιστο κοινό διαιρέτη δύο ακεραίων αρκεί να βρούμε τον μέγιστο κοινό διαιρέτη των απόλυτων τιμών τους.

Ένας τρόπος για να βρούμε τον μέγιστο κοινό διαιρέτη των αριθμών a, b είναι να καταγράψουμε όλους τους θετικούς διαιρέτες του a και όλους τους θετικούς διαιρέτες του b και μετά να διαλέξουμε τον μεγαλύτερο αριθμό που εμφανίζεται στην λίστα.

Example. Για $a = 60$ και $b = 42$ οι θετικοί διαιρέτες των a, b είναι οι
$a : 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$
$b : 1, 2, 3, 6, 7, 14, 21, 42$
Οπότε, ο μεγαλύτερος αριθμός που εμφανίζεται στις δύο λίστες είναι το 6

Παρ' όλα αυτά, υπάρχει πολύ γρηγορότερος υπολογιστικά τρόπος να βρούμε τον μέγιστο κοινό διαιρέτη δύο αριθμών, χρησιμοποιώντας τον Ευκλείδιο αλγόριθμο

Lemma. *Αν* $a = qb + r$, *τότε* $\text{ΜΚΔ}(a,b) = \text{ΜΚΔ}(b,r)$

Proof. Έστω $d_1 = \text{ΜΚΔ}(a,b)$ και $d_2 = \text{ΜΚΔ}(b,r)$ τότε $d_1|(a - qb) \Rightarrow d_1|r$ και αφού $d_1|b$ τότε ο d_1 είναι κοινός διαιρέτης των b, r, οπότε $d_1 \leq d_2$. Με τον ίδιο τρόπο $d_2|(qb + r)$, οπότε $d_2|a$ και άρα $d_2 \leq d_1$. Συνδυάζοντας τις δύο ανισότητες έχουμε ότι $d_1 = d_2$.
Οπότε, $\text{ΜΚΔ}(a,b) = \text{ΜΚΔ}(b,r)$. □

Ο αλγόριθμος του Ευκλείδη βασίζεται πάνω σε αυτήν την υπόθεση και διατυπώνεται ως εξής:

Lemma 1.1.3 (Αλγόριθμος του Ευκλείδη). *Έστω οι θετικοί ακέραιοι* a, b, $\mu\epsilon$ $b \leq a$, *τότε:*

$$\text{ΜΚΔ}(a,b) = \text{ΜΚΔ}(b,r_1) = \text{ΜΚΔ}(r_1,r_2) = \ldots \text{ΜΚΔ}(r_{n-1},r_n) = \text{ΜΚΔ}(r_n,0) = r_n$$

όπου
$a = bq_1 + r_1$
$b = r_1q_2 + r_2$
$r_1 = r_2q_3 + r_3$
.
.
.
$r_{n-1} = r_nq_{n+1} + 0$

Ο αλγόριθμος σε μορφή ψευδοκώδικα είναι ο εξής:

```
GCD(a,b)
i:=a;
j:=b;
WHILE i>0 AND j>0
    IF i>j THEN i:=iMODj;
    ELSE j:=jMODi;
RETURN i+j;
```

Remark. Ο αλγόριθμος του Ευκλείδη παρουσιάζει την χειρότερή του απόδοση αν του δοθούν ως είσοδος δυο διαδοχικοί αριθμοί της ακολουθίας Fibonacci: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2},\ n \geq 2$

Η χρονική πολυπλοκότητα του αλγορίθμου του Ευκλείδη είναι $\Theta(\log(a+b))$.

Example. Θα βρώ τον μέγιστο κοινό διαιρέτη των αριθμών 450 και 140.

$450 = 140 \cdot 3 + 30,$

$140 = 30 \cdot 4 + 20,$

$30 = 20 \cdot 1 + 10,$

$20 = 10 \cdot 2 + 0.$

Οπότε, ο μέγιστος κοινός διαιρέτης των 450 και 140 είναι ο 10

Theorem 1.1.4. *Έστω οι μη μηδενικοί ακέραιοι a, b, αν $d = ΜΚΔ(a, b)$ τότε υπάρχουν ακέραιοι x, y τέτοιοι ώστε $d = ax + by$.*

Proof. Έστω $S = \{ax + by : x, y \epsilon \mathbb{Z}, ax + by > 0\}$ τότε προφανώς το S δεν είναι το κενό σύνολο καθώς για $x = \frac{|a|}{a}$ το $ax + 0b = |a| \in S$.

Οπότε, αφού το $S \subseteq \mathbb{N}$ θα έχει ελάχιστο στοιχείο.

Θα δείξουμε ότι $d = \min S$.

Έστω $m = \min S$ τότε υπάρχουν $x_0, y_0 \in \mathbb{Z}$ με $m = ax_0 + by_0$.

Σύμφωνα με το θεώρημα της Ευκλείδιας διαίρεσης υπάρχουν ακέραιοι q, r τέτοιοι ώστε $a = mq + r$ με $0 \leq r < m$.

Θα δείξουμε ότι $r = 0$.

Έστω ότι $r \neq 0$, οπότε $r > 0$, τότε

$$r = a - mq = a - (ax_0 + by_0)\, q = a\,(1 - x_0 q) + b\,(-y_0 q).$$

οπότε $r \epsilon S$ και $r < m$ οπότε το r είναι μικρότερο από το ελάχιστο στοιχείο του S κάτι που είναι άτοπο.

Οδηγηθήκαμε σε άτοπο καθώς υποθέσαμε ότι $r \neq 0$, οπότε θα έχουμε $r = 0$.

Τότε $m|a$.

Όμοια αποδεικνύεται ότι $m|b$, οπότε ο m είναι κοινός διαιρέτης των a, b.

Όμως για k κοινό διαιρέτη των a, b θα έχουμε ότι $k|\,(ax_0 + by_0) \Rightarrow k|m$. Άρα $k \leq m$.

Άρα $m = \min S = d$. □

Remark. Η απόδειξη του θεωρήματος μπορεί επίσης να γίνει χρησιμοποιώντας τον ευκλείδιο αλγόριθμο.

Proposition. *Τα x και y προκύπτουν από τον αλγόριθμο του Ευκλείδη αντικαθιστώντας από τις τελευταίες διαιρέσεις προς τις πρώτες, αφήνοντας τον μέγιστο κοινό διαιρέτη πάντα στα αριστερά. Η αλγοριθμική διαδικασία της πρότασης είναι γνωστή σαν Extended Euclidean Algorithm.*

Example. Χρησιμοποιώντας το προηγούμενο παράδειγμα έχουμε ότι $\text{ΜΚΔ}(450, 140) = 10$ και από το προηγούμενο παράδειγμα έχουμε τις Ευκλείδιες διαιρέσεις:

$450 = 140 \cdot 3 + 30,$

$140 = 30 \cdot 4 + 20$,
$30 = 20 \cdot 1 + 10$,
$20 = 10 \cdot 2 + 0$.

Πάντα ξεκινάμε από την προτελευταία εξίσωση πηγαίνοντας τον μέγιστο κοινό διαιρέτη στα αριστερά. Οπότε,

$10 = 30 - 20$ και αντικαθιστούμε την σχέση που έχουμε στην προηγούμενη, αντικαθιστώντας μόνο το προηγούμενο υπόλοιπο (εδώ το 20) και συνεχίζουμε αυτήν την διαδικασία μέχρι να φτάσουμε στην πρώτη εξίσωση. Οπότε,

$10 = 30 - 20 = 30 - (140 - 30 \cdot 4) = -140 + 30 \cdot 5 \Leftrightarrow$
$10 = -140 + (450 - 140 \cdot 3) \cdot 5 = 450 \cdot 5 + 140 \cdot (-16)$.

Theorem 1.1.5. *Έστω οι ακέραιοι αριθμοί a, b και d θετικός κοινός διαιρέτης τους. Τότε ο d είναι ο μέγιστος κοινός διαιρέτης των a, b αν και μόνο αν για κάθε θετικό κοινό διαιρέτη d' των a, b ισχύει ότι $d'|d$.*

Proof. Αν $d = \text{ΜΚΔ}(a, b)$, τότε από το (1.1.4) υπάρχουν ακέραιοι x, y τέτοιοι ώστε

$$d = ax + by.$$

Οπότε, για κάθε d' κοινό διαιρέτη των a, b θα ισχύει ότι

$$d'|(ax + by) \Rightarrow d'|d.$$

Από την άλλη μεριά, αν ο d είναι ένας θετικός κοινός διαιρέτης των a, b και κάθε κοινός διαιρέτης d' των a, b τον διαιρει τότε προφανώς $d' \leq d$.

Οπότε, ο d είναι ο μέγιστος κοινός διαιρέτης των a, b. □

Definition. Έστω ο πραγματικός αριθμός x, τότε ορίζουμε ως $\lfloor x \rfloor$ τον μεγαλύτερο ακέραιο που είναι μικρότερος ή ίσος από τον x.

Remark. Από τον ορισμό προκύπτει άμεσα ότι $x - 1 < \lfloor x \rfloor \leq x$.

1.2 Πρώτοι Αριθμοί

Definition. Ονομάζουμε *πρώτο αριθμό* κάθε θετικό ακέραιο μεγαλύτερο της μονάδας, ο οποίος έχει θετικούς διαιρέτες μόνο τον εαυτό του και την μονάδα.

Example. Οι αριθμοί $2, 3, 5, 7, 11$ είναι πρώτοι.

Lemma 1.2.1. *Έστω p πρώτος αριθμός και a ακέραιος. Τότε ή ο p θα διαιρεί τον a ή $ΜΚΔ(a, p) = 1$*

Proof. Σύμφωνα με τον ορισμό του, ο p έχει θετικούς διαιρέτες μόνο τον εαυτό του και την μονάδα, οπότε $\text{ΜΚΔ}(a, p) = 1$ ή $\text{ΜΚΔ}(a, p) = p$.

Αν $\text{ΜΚΔ}(a, p) = p$ τότε προφανώς $p|a$. □

Definition. Ονομάζουμε *σύνθετο αριθμό* κάθε ακέραιο αριθμό μεγαλύτερο της μονάδας που δεν είναι πρώτος.

Example. Για τους αριθμούς $2, 3, 4, ..., 10$ έχουμε ότι οι $2, 3, 5, 7$ είναι πρώτοι ενώ οι $4, 6, 8, 9, 10$ είναι σύνθετοι.

Remark. Ο αριθμός 1 δεν είναι ούτε πρώτος ούτε σύνθετος.

Definition. Οι ακέραιοι a, β ονομάζονται σχετικά πρώτοι αν ο μέγιστος κοινός διαιρέτης τους είναι η μονάδα.

Example. Οι ακέραιοι 14 και 25 είναι σχετικά πρώτοι καθώς $\text{ΜΚΔ}(14, 25) = 1$, ενώ οι $8, 18$ όχι καθώς $\text{ΜΚΔ}(8, 18) = 2$

Theorem 1.2.2. *Έστω p πρώτος αριθμός και $a, b \epsilon \mathbb{Z}$. Αν $p|ab$, τότε $p|a$ ή $p|b$*

Proof. Αν $p|a$ το θεώρημα ισχύει.

Αλλιώς, αν $p \nmid a$. Τότε από το (1.2.1) έχουμε ότι $\text{ΜΚΔ}(a, p) = 1$. Τότε, από το (1.1.4) υπάρχουν $x, y \epsilon \mathbb{Z}$ με

$$1 = ax + py \Rightarrow b = abx + pby.$$

Όπότε, αφού $p|ab$ και $p|p$, τότε $p|\,(abx + pby) \Rightarrow p|b$. □

Theorem 1.2.3. *Έστω a, b, c ακέραιοι με a, c σχετικά πρώτους και $c|ab$, τότε $c|b$.*

Proof. Αφού $\text{ΜΚΔ}(a, c) = 1$, τότε από (1.1.4) υπάρχουν ακέραιοι $x, y \epsilon \mathbb{Z}$ με $cx + ay = 1$.

Άρα, $cbx + aby = b$. Οπότε, όπως στο προηγούμενο θεώρημα $c|(cbx + aby) \Rightarrow c|b$. □

Proposition 1.2.4 (Κριτήριο Ρίζας)**.** *Κάθε σύνθετος αριθμός $a > 1$ έχει έναν τουλάχιστον πρώτο παράγοντα $p \leq \sqrt{a}$*

Proof. Έστω ο σύνθετος αριθμός a, τότε θεωρούμε p τον ελάχιστο θετικό διαιρέτη του a με $p > 1$. Τότε, ο p θα είναι πρώτος αριθμός, καθώς αν δεν ήταν θα υπήρχαν θετικοί ακέραιοι x, y διαφορετικοί της μονάδας με $p = xy$ οπότε οι x, y θα ήταν διαιρέτες του a μικρότεροι από τον p, άτοπο. Τότε, ο a θα είναι στην μορφή $a = pb$, με $1 < p \leq b < a$ οπότε $p^2 \leq pb = a$. Οπότε ο a θα έχει έναν τουλάχιστον πρώτο διαιρέτη p με $p \leq \sqrt{a}$. □

Remark. Από την παραπάνω πρόταση προκύπτει ένα κριτήριο με το οποίο εξετάζουμε αν ένας αριθμός είναι πρώτος. Για να εξετάσουμε αν ο αριθμός a είναι πρώτος αρκεί να εξετάσουμε αν υπάρχει πρώτος αριθμός μικρότερος από $\sqrt{a}$ που να διαιρεί τον a. Αν υπάρχει τέτοιος πρώτος, ο a δεν είναι πρώτος. Αν κανένας πρώτος μικρότερος από $\sqrt{a}$ δεν διαιρεί τον a τότε ο a είναι πρώτος.

Theorem. *Οι πρώτοι αριθμοί είναι άπειροι*

Proof. Έστω ότι το πλήθος των πρώτων είναι πεπερασμένο, έστω n. Έστω ότι οι πρώτοι είναι οι

$$p_1, p_2, \ldots p_n.$$

Τότε, θεωρώ τον αριθμό

$$A = p_1 p_2 \dots p_n + 1.$$

Κατ' αρχάς, ο A δεν είναι πρώτος, καθώς είναι μεγαλύτερος από κάθε πρώτο. Οπότε, σύμφωνα με το (1.2.4) ο A θα έχει κάποιο πρώτο διαιρέτη έστω τον p_k με $k \in \{1, 2, \dots n\}$, τότε

$$p_k | A \text{ και } p_k | p_1 p_2 \dots p_n \text{ οπότε } p_k | (A - p_1 p_2 \dots p_n) \Rightarrow p_k | 1$$

το οποίο είναι άτοπο. Καταλήξαμε σε άτοπο γιατί υποθέσαμε ότι το πλήθος των πρώτων είναι πεπερασμένο.

Οπότε, οι πρώτοι αριθμοί είναι άπειροι. □

Theorem 1.2.5 (Θεμελιώδες θεώρημα της αριθμητικής). *Κάθε θετικός ακέραιος μπορεί να αναπαρασταθεί ως γινόμενο δυνάμεων πρώτων παραγόντων κατά μοναδικό τρόπο.*

Proof. Έστω n ακέραιος αριθμός και p_1 ο ελάχιστος πρώτος διαιρέτης του . Αν ο n είναι πρώτος, τότε $n = p_1$, αλλιώς $1 < p_1 < n$. Τότε, $n = p_1 n_1, n_1 \epsilon \mathbb{N}$. Με τον ίδιο τρόπο ο n_1 έχει ελάχιστο πρώτο διαιρέτη p_2. Τότε, $n = p_1 p_2 n_2$, $n_2 \epsilon \mathbb{N}$. Συνεχίζοντας αυτήν την διαδικασία θα προκύψει οτι ο n μπορεί να γραφεί σαν γινόμενο πρώτων όχι κατ' ανάγκη διαφορετικών μεταξύ τους.

Οπότε, ο n θα γραφεί στην μορφή

$$n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}, k \epsilon \mathbb{N}.$$

Θα δείξουμε ότι η αναπαράσταση είναι μοναδική.
Έστω ότι ο n έχει αναπαρασταθεί ως γινόμενο δυνάμεων πρώτων παραγόντων κατά δύο διαφορετικούς τρόπους.

Τότε,

$$p_1^{a_1} p_2^{a_2} ... p_k^{a_k} = q_1^{b_1} q_2^{b_2} ... q_l^{b_l}, k, l \epsilon \mathbb{N}$$

οπότε,

$$p_i | p_1^{a_1} p_2^{a_2} ... p_k^{a_k} \Rightarrow p_i | q_1^{b_1} q_2^{b_2} ... q_l^{b_l} \Rightarrow p_i | q_j \text{ για κάποια } i, j.$$

Άρα κάθε p_i είναι ίσο με κάποιο q_j. Οπότε $k = l$.

Τότε, θεωρώ ότι

$$p_i = q_i, \ i = 1, 2, ..., k$$

αρκεί να αποδείξουμε ότι

$$a_i = b_i, \ i = 1, 2, ..., k.$$

Έστω ότι για κάποιο $i \epsilon \{1, 2, ..., k\}$ ισχύει ότι $a_i \neq b_i$.

Χωρίς βλάβη της γενικότητας θεωρώ ότι $a_i > b_i$.
Τότε,

$$p_1^{a_1}p_2^{a_2}...p_i^{a_i}...p_k^{a_k} = p_1^{b1}p_2^{b_2}...p_i^{b_i}...p_k^{b_k} \Leftrightarrow p_1^{a_1}p_2^{a_2}...p_i^{a_i-b_i}...p_k^{a_k} = p_1^{b1}p_2^{b_2}...p_{i-1}^{b_{i-1}}p_{i+1}^{b_{i+1}}...p_k^{b_k}.$$

Επειδή $a_i - b_i > 0$, τότε

$$p_i | p_1^{a_1}p_2^{a_2}...p_i^{a_i-b_i}...p_k^{a_k} \text{ ενώ } p_i \nmid p_1^{b1}p_2^{b_2}...p_{i-1}^{b_{i-1}}p_{i+1}^{b_{i+1}}...p_k^{b_k}.$$

Το οποίο είναι αδύνατο.
Οπότε, $a_i = b_i,\ i = 1, 2, ..., k$.
Οπότε η αναπαράσταση ως γινόμενο δυνάμεων πρώτων αριθμών είναι μοναδική. □

Example. $60 = 2^2 \cdot 3 \cdot 5$

1.3 Συνάρτηση Euler

Definition (Συνάρτηση Euler)**.** Έστω ένας θετικός ακέραιος n. Ορίζουμε την συνάρτηση Euler $\phi(n)$ να είναι το πλήθος των θετικών ακεραίων, οι οποίοι ειναι μικρότεροι ή ίσοι με το n και σχετικά πρώτοι με το n.

Corollary. *Από τον ορισμό προκύπτει αμεσα ότι* $\phi(1) = 1$ *και* $\phi(p) = p-1$ *για κάθε πρώτο* p*.*

Theorem 1.3.1 (Αρχή Εγκλεισμού Αποκλεισμού)**.** *Έστω* S *ένα σύνολο στοιχείων και* $A_1, A_2, \dots A_m \subseteq S$ *, τότε:*

$$|A_1 \cup A_2 \cup \dots A_m| = \sum |A_i| - \sum |A_i \cap A_j| + \dots + (-1)^{m+1}|A_1 \cap A_2 \cap \dots \cap A_m|$$

Proposition 1.3.2. *Από την αρχή Εγκλεισμού Αποκλεισμού προκύπτει άμεσα ότι αν* $A_1, A_2, \dots A_m \subseteq S$*, τότε:*

$$|A_1^c \cup A_2^c \cup \dots A_m^c| = |S| - \sum |A_i| + \sum |A_i \cap A_j| - \sum |A_i \cap A_j \cap A_k| + \dots + (-1)^m|A_1 \cap A_2 \cap \dots \cap A_m|$$

όπου A^c *είναι το συμπλήρωμα του* A

Theorem 1.3.3. *Για κάθε φυσικό αριθμό* $n = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$ *ισχύει ότι:*

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\dots(1 - \frac{1}{p_k})$$

Proof. Θα υπολογίσουμε την $\phi(n)$ με την βοήθεια της αρχής Εγκλεισμού Αποκλεισμού.

Οι πρώτοι διαιρέτες του αριθμού n είναι οι $p_1, p_2, \dots p_k$.

Έστω A_i το σύνολο των αριθμών $\{1, 2, \dots, n\}$ που διαιρούνται από τον p_i. Τότε, ο αριθμός $\phi(n)$ περιγράφει το πλήθος των στοιχείων του συνόλου $\{1, 2 \dots, n\}$ που δεν ανήκουν σε κανένα από τα σύνολα A_i. Οπότε,

$$\phi(n) = |A_1^c \cup A_2^c \cup \dots A_k^c| = |S| - \sum |A_i| + \sum |A_i \cap A_j| - \sum |A_i \cap A_j \cap A_k| + \dots + (-1)^k |A_1 \cap A_2 \cap \dots \cap A_k| =$$
$$n - \sum |A_i| + \sum |A_i \cap A_j| - \sum |A_i \cap A_j \cap A_k| + \dots + (-1)^k |A_1 \cap A_2 \cap \dots \cap A_k|$$

Το πλήθος των ακεραίων στο $\{1, 2, \dots, n\}$ που διαιρούνται από τον πρώτο p_i είναι $\frac{n}{p_i}$ καθώς είναι οι αριθμοί

$$p_i, 2p_i, \dots, (\frac{n}{p_i})p_i$$

όμοια οι αριθμοί που διαιρούνται από τον $p_{i_1} p_{i_2} \dots p_{i_m}$ είναι $\frac{n}{p_{i_1} p_{i_2} \dots p_{i_m}}$.

Οπότε,

$$\phi(n) = n - \sum \frac{n}{p_i} + \sum \frac{n}{p_i p_j} + \dots + (-1)^k \frac{n}{p_1 p_2 \dots p_k} = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$$

□

Example. Για $n = 60 = 2^2 \cdot 3 \cdot 5$, έχουμε ότι $\phi(60) = 60(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16$

1.4 Ισοδυναμίες ή ισοτιμίες

Definition. Έστω οι ακέραιοι αριθμοί a, b, m, με $m > 0$. Θα λέμε ότι ο a είναι ισοδύναμος (ή ισότιμος) του b modulo m, αν η διαφορά $a - b$ είναι ακέραιο πολλαπλάσιο του m. Τότε θα γράφουμε $a \equiv b \mathrm{mod} m$.

Example. Για παράδειγμα $8 \equiv 2\mathrm{mod}3$ καθώς $8 - 2 = 6 = 2 \cdot 3$, ενώ $9 \neq 6\mathrm{mod}5$ καθώς $9 - 6 = 3$ που δεν είναι πολλαπλάσιο του 5.

Proposition. *Η σχέση $a \equiv b mod m$ είναι σχέση ισοδυναμίας.*

Proof. Έστω a, b, c, m ακέραιοι αριθμοί και $m > 0$, τότε:

1.$a \equiv a\mathrm{mod}m$ καθώς $a - a = 0 = 0 \cdot m$

2.Αν $a \equiv b\mathrm{mod}m$ τότε και $b \equiv a\mathrm{mod}m$.

Αφού $a \equiv b\mathrm{mod}m$ τότε υπάρχει $k \epsilon \mathbb{Z}$, τέτοιος ώστε $a - b = km$.

Τότε

$$b - a = -(a - b) = -km \text{ άρα } b \equiv a\mathrm{mod}m$$

3.Αν $a \equiv b \mathrm{mod} m$ και $b \equiv c \mathrm{mod} m$, τότε $a \equiv c \mathrm{mod} m$.
Αφού $a \equiv b \mathrm{mod} m$ και $b \equiv c \mathrm{mod} m$ τότε

$$a - b = km \text{ και } b - c = lm \text{ για κάποιους } k, l \epsilon \mathbb{Z}$$

οπότε

$$a - c = a - b + b - c = km + lm = (k + l) m$$

άρα

$$a \equiv c \mathrm{mod} m$$

□

Proposition. *Έστω a, b, c, m ακέραιοι αριθμοί, $m > 0$*
Τα επόμενα είναι ισοδύναμα:
1) $a \equiv b mod m$
2) *Το $b - a$ είναι πολλαπλάσιο του m*
3) $m | (b - a)$
4) *Ο αριθμός $\frac{b-a}{m}$ είναι ακέραιος*
5) *Οι a, b αφήνουν το ίδιο υπόλοιπο στην ευκλείδια διαίρεση με το m*

Proof. Τα 1,2,3,4 προκύπτουν άμεσα από τον ορισμό.
Θα αποδείξω οτι 1⇔5
1⇒5.
Έστω ότι $a \equiv b \mathrm{mod} m$ και έστω ότι

$$a = q_a m + r_a,\ b = q_b m + r_b \text{ με } q_a,\ q_b,\ r_a,\ r_b \epsilon \mathbb{Z} \text{ και } 0 \leq r_a, r_b < m$$

τότε απο την υπόθεση έχω ότι $a \equiv b \mathrm{mod} m$, οπότε ο $a - b$ είναι πολλαπλάσιο του m, οπότε $(q_a - q_b) m + r_a - r_b$ είναι πολλαπλάσιο του m.
Τότε, θα πρέπει το $r_a - r_b$ να είναι πολλαπλάσιο του m , όμως $-m < r_a - r_b < m$ και επειδή το μόνο πολλαπλάσιο του m που υπάρχει μεταξύ του $-m$ και m είναι το 0 θα πρέπει να ισχύει $r_a = r_b$, και άρα οι a, b είναι ισοϋπόλοιποι στην διαίρεση με το m.
$5 \Rightarrow 1$.
Έστω ότι οι a, b αφήνουν το ίδιο υπόλοιπο στην ευκλείδια διαίρεση με το m, τότε

$$a = q_a m + r,\ b = q_b m + r,\ q_a,\ q_b,\ r \epsilon \mathbb{Z} \text{ με } 0 \leq r < m$$

οπότε

$$a - b = (q_a - q_b) m$$

Τότε ο αριθμός $a - b$ είναι πολλαπλάσιο του m , οπότε $a \equiv b \mathrm{mod} m$.
Άρα 1⇔5. □

Proposition. *Αν* $a \equiv a' mod m$ *και* $b \equiv b' mod m$, *τότε* $a \pm b \equiv a' \pm b' mod m$ *και* $ab \equiv a'b' mod m$.

Proof. Από την υπόθεση υπάρχουν $k, l \in \mathbb{Z}$ με $a - a' = km$ και $b - b' = lm$.
Τότε,

$$a = a' + km \text{ και } b = b' + lm.$$

Οπότε,

$$a \pm b = a' \pm b' + (k \pm l)\, m.$$

Άρα

$$a \pm b \equiv a' \pm b' \mathrm{mod} m.$$

Επίσης,

$$ab = \left(a' + km\right)\left(b' + lm\right) = a'b' + m\left(kb' + la' + klm\right)$$

Οπότε,

$$ab \equiv a'b' \mathrm{mod} m.$$

□

Proposition 1.4.1 (Κανόνας απλοποίησης)**.** *Έστω οι ακέραιοι* a, a', b, m *με* $m > 0$ *και* $MK\Delta(b, m) = 1$. *Αν* $ab \equiv a'b mod m$ *τότε* $a \equiv a' mod m$.

Proof. Αφού $m|b\,(a - a')$ και επειδή $\mathrm{MK\Delta}(b, m) = 1$, τότε από το (1.2.3) έχουμε ότι $m|\,(a - a') \Rightarrow a \equiv a' \mathrm{mod} m$ □

Definition. Έστω $a \in \mathbb{Z}$. Αν υπάρχει ακέραιος b τέτοιος ώστε $ab \equiv 1 \mathrm{mod} n$, τότε ο b θα λέγεται αντίστροφος του $a \mathrm{mod} n$.

Theorem 1.4.2. *Ο αντίστροφος του θετικού ακέραιου* $a mod n$ *υπάρχει αν και μόνο αν* $MK\Delta(a, n) = 1$

Proof. Αν $\mathrm{MK\Delta}(a, n) = 1$ τότε σύμφωνα με το ((1.1.4)) υπάρχουν ακέραιοι x, y τέτοιοι ώστε

$$ax + ny = 1$$

τότε

$$1 = ax + ny \equiv ax \mathrm{mod} n.$$

Δηλαδή, ο x είναι αντίστροφος του $a \mathrm{mod} n$
Αντίστροφα, αν υπάρχει ακέραιος x με $ax \equiv 1 \mathrm{mod} n$, τότε $n|\,(ax - 1)$.
Επειδή, $\mathrm{MK\Delta}(a, n)|n$, από (1.1.2) θα έχουμε ότι $\mathrm{MK\Delta}(a, n)|(ax - 1)$.
Όμως, $\mathrm{MK\Delta}(a, n)|a$, οπότε $\mathrm{MK\Delta}(a, n)|ax$.
Τότε $\mathrm{MK\Delta}(a, n)|\,[ax - (ax - 1)]$ οπότε $\mathrm{MK\Delta}(a, n)|1$ οπότε $\mathrm{MK\Delta}(a, n) = 1$ □

Remark. Από το παραπάνω θεώρημα έπεται ότι για να βρούμε τον αντίστροφο του $a \mathrm{mod} n$ αρκεί να βρούμε τα x, y για τα οποία $ax + ny = 1$ και τότε το x θα είναι ο αντιστροφός του.

Theorem 1.4.3. *Ο αντίστροφος ενός φυσικού $a \mathrm{mod} n$ αν υπάρχει είναι μοναδικός $\mathrm{mod} n$*

Proof. Έστω ότι οι x, y είναι ταυτόχρονα αντίστροφοι του $a \mathrm{mod} n$ δηλαδή

$$ax \equiv ay \equiv 1 \mathrm{mod} n.$$

Τότε, $n|a(x-y)$ και επειδη $\mathrm{MK}\Delta(a,n) = 1$(από 1.4.2), τότε $n|\,(x-y)$.
Άρα $x \equiv y \mathrm{mod} n$ δηλαδή ο αντίστροφος είναι μοναδικός $\mathrm{mod} n$ □

1.5 Γραμμική Διοφαντική Εξίσωση

Definition. Η εξίσωση $ax + by = c$, όπου a, b, c ακέραιοι και x, y άγνωστοι ακέραιοι ονομάζεται γραμμική διοφαντική εξίσωση.

Theorem 1.5.1. *Η γραμμική διοφαντική εξίσωση $ax + by = c$ έχει λύση αν και μόνο αν ο $d = MK\Delta(a,b)$ διαιρεί τον c.*

Proof. Έστω ότι η εξίσωση έχει λύση και έστω (x_0, y_0) μία λύση της.
Τότε,

$$ax_0 + by_0 = c$$

Τότε, αφού $d = \mathrm{MK}\Delta(a,b)$ υπάρχουν ακέραιοι k, l με $a = kd$ και $b = ld$, με $\mathrm{MK}\Delta(k,l) = 1$.
Οπότε,

$$c = ax_0 + by_0 = d(kx_0 + ly_0)$$

Οπότε, $d|c$.
Αντίστροφα, ας θεωρήσουμε ότι $d|c$.
Τότε, υπάρχει ακέραιος m τέτοιος ώστε $c = d \cdot m$.
Από το (1.1.4) υπάρχουν ακέραιοι k, l τέτοιοι ώστε:

$$ka + lb = d \Rightarrow$$
$$a(km) + b(lm) = dm = c$$

άρα η διοφαντική εξίσωση έχει λύση. □

Theorem 1.5.2. *Αν (x_0, y_0) μια λύση της διοφαντικής εξίσωσης $ax + by = c$ και $d = MK\Delta(a,b)$ τότε οι λύσεις της διοφαντικής εξίσωσης είναι οι:*

$$x = x_0 + \frac{b}{d} \cdot n,\ y = y_0 - \frac{a}{d} \cdot n,\ n \in Z$$

Proof. Έστω (x_0, y_0) μια λύση της εξίσωσης $ax + by = c$ και έστω (x', y') μια άλλη λύση της, τότε:

$$\begin{aligned} ax_0 + by_0 =& ax' + by' \Rightarrow \\ a(x' - x_0) =& b(y_0 - y') \end{aligned}$$

και διαιρώντας με $d = \text{ΜΚΔ}(a, b)$ έχουμε ότι

$$k(x' - x_0) = l(y_o - y')$$

όπου οι $k = \frac{a}{d}$ και $l = \frac{b}{d}$ είναι σχετικά πρώτοι. Επομένως έχουμε ότι $k|l(y_0 - y')$ και $\text{ΜΚΔ}(k, l) = 1$, οπότε από το (1.2.3) έχουμε ότι $k|(y_0 - y')$. Δηλαδή, υπάρχει ακέραιος n τέτοιος ώστε $y_0 - y' = kn$. Όμοια αποδεικνύεται ότι $x' - x_0 = ln$. Οπότε,

$$x' = x_0 + \frac{b}{d} \cdot n,\ n \in \mathbb{Z}$$

$$y' = y_0 - \frac{a}{d} \cdot n,\ n \in \mathbb{Z}$$

□

Definition. Η εξίσωση $ax \equiv b \text{mod} m$, όπου a, b γνωστοί ακέραιοι, m ακέραιος με $m > 0$ και x άγνωστος ακέραιος ονομάζεται γραμμική ισοτιμια.

Theorem 1.5.3. *Έστω οι ακέραιοι αριθμοί a, b, m με $m > 0$ και $d = ΜΚΔ(a, m)$.*

Αν $d|b$ τότε η γραμμική ισοτιμία $ax \equiv b mod m$ έχει d ανά δυο διαφορετικές μεταξύ τους $(mod m)$ λύσεις.

Αν $d \nmid b$ η γραμμική ισοτιμία δεν έχει λύσεις.

Proof. Αν $d|b$ τότε αν η γραμμική ισοτιμία $ax \equiv b \text{mod} m$ έχει λύση θα υπάρχει $y \in \mathbb{Z}$ τέτοιο ώστε $ax - b = my$ ή ισοδύναμα $ax - my = b$.

Οπότε, η γραμμική ισοτιμία $ax \equiv b \text{mod} m$ έχει λύση αν και μόνο αν η διοφαντική εξίσωση $ax - my = b$ έχει λύση.

Τότε, σύμφωνα με το (1.5.2) αν x_0 μια λύση της $ax \equiv b \text{mod} m$, τότε όλες οι λύσεις της θα είναι οι

$$x = x_0 - \frac{m}{d} \cdot n,\ n \in \mathbb{Z}$$

Θα αποδείξουμε ότι μόνο d από τις λύσεις είναι ανα δυο διαφορετικές μεταξύ τους.

Προφανώς, οι

$$x_0, x_0 - \frac{m}{d}, x_0 - 2\frac{m}{d}, \ldots, x_0 - (d-1)\frac{m}{d}$$

είναι λύσεις της γραμμικής ισοτιμίας και είναι ανα δυο διαφορετικές μεταξύ τους καθώς αν

$$x_0 - n_1\frac{m}{d} \equiv x_0 - n_2\frac{m}{d} \mathrm{mod} m$$

για $n_1, n_2 \in \mathbb{N}$ με $1 \leq n_1, n_2 \leq d-1$ τότε

$$n_1\frac{m}{d} \equiv n_2\frac{m}{d} \mathrm{mod} m \Rightarrow m|(n_1 - n_2)\frac{m}{d}$$

Οπότε, θα πρέπει να ισχύει ότι $m \leq |n_1 - n_2|\frac{m}{d}$ ή $n_1 = n_2$.

Αν $n_1 \neq n_2$ τότε $|n_1 - n_2| \leq d-1$, άρα $|n_1 - n_2|\frac{m}{d} < m$.

Οπότε $n_1 = n_2$.

Επομένως, οι λύσεις

$$x_0, x_0 - \frac{m}{d}, x_0 - 2\frac{m}{d}, \ldots, x_0 - (d-1)\frac{m}{d}$$

είναι ανα δύο διαφορετικές μεταξύ τους.

Θα αποδείξουμε ότι αυτές είναι όλες οι μη ισοδύναμες μεταξύ τους λύσεις.

Έστω $c \in \mathbb{Z}$ διαφορετική λύση από τις προηγούμενες, τότε

$$ac \equiv ax_0 \mathrm{mod} m.$$

Όμως, $\mathrm{ΜΚΔ}(a, m) = d$. Τότε,

$$a = rd, m = sd \text{ για } r, s \in \mathbb{Z} \text{ με } \mathrm{ΜΚΔ}(r, s) = 1$$

οπότε

$$sd|rd(c - x_0) \Rightarrow s|r(c - x_0)$$

όμως $\mathrm{ΜΚΔ}(s, r) = 1$. Επομένως,

$$s|\,(c - x_0).$$

Άρα, υπάρχει ακέραιος n με: $c = x_0 + ns$.

Τότε, θα έχουμε ότι

$$n = dq + t,\ q, t \in \mathbb{Z} \text{ με } 0 \leq t < d.$$

Οπότε,

$$c = x_0 + (dq + t)s = x_0 + dsq + st = x_0 + mq + \frac{m}{d}t.$$

Οπότε,

$$c \equiv x_0 + \frac{m}{d}t \mathrm{mod} m.$$

Άρα, η c δεν είναι διαφορετική λύση από αυτές που έχουμε βρει.

Αν $d \nmid b$ τότε η διοφαντικη εξίσωση $ax - my = b$ δεν έχει λύσεις οπότε και η γραμμική ισοτιμία $ax \equiv b \mathrm{mod} m$ δεν θα έχει λύσεις. □

Theorem 1.5.4 (Κινέζικο Θεώρημα Υπολοίπων). *Έστω $n_1, n_2, \ldots, n_k$ θετικοί ακέραιοι ανά δυο σχετικά πρώτοι μεταξύ τους και $a_1, a_2, \ldots, a_k$ ακέραιοι. Το σύστημα γραμμικων ισοτιμιών:*

$$\begin{aligned} x &\equiv a_1 mod n_1 \\ x &\equiv a_2 mod n_2 \\ &\cdot \\ &\cdot \\ &\cdot \\ x &\equiv a_k mod n_k \end{aligned}$$

έχει μοναδική λύση $mod n_1 n_2 \ldots n_k$.

Proof. Έστω $n = n_1 n_2 \ldots n_k$.

Για $i = 1, 2, \ldots, k$ έχουμε ΜΚΔ$(\frac{n}{n_i}, n_i) = 1$, τότε, ο $\frac{n}{n_i}$ έχει αντίστροφο modn_i, οπότε υπάρχει y_i τέτοιος ώστε

$$\frac{n}{n_i} y_i \equiv 1 \text{mod} n_i.$$

Επίσης,

$$\frac{n}{n_i} y_i \equiv 0 \text{mod} n_j, \text{ για } i \neq j.$$

Τότε, ο ακέραιος

$$x = \frac{n}{n_1} y_1 a_1 + \frac{n}{n_2} y_2 a_2 + \cdots + \frac{n}{n_k} y_k a_k$$

είναι λύση, αφού για κάθε $i = 1, 2, \ldots, k$ έχουμε ότι:

$$x \equiv \frac{n}{n_1} y_1 a_1 + \frac{n}{n_2} y_2 a_2 + \cdots + \frac{n}{n_k} y_k a_k \text{mod} n_i \equiv \frac{n}{n_i} y_i a_i \text{mod} n_i \equiv a_i \text{mod} n_i.$$

Για την μοναδικότητα, έστω x_1, x_2 δύο διαφορετικές λύσεις του συστήματος ισοτιμιών, τότε $x_1 \equiv x_2 \text{mod} n_i$, οπότε $n_i | (x_1 - x_2)$ για κάθε $i = 1, 2, \ldots, k$.

Αφού οι $n_1, n_2, \ldots, n_k$ είναι σχετικά πρώτοι ανά δύο, προκύπτει ότι $n | (x_1 - x_2)$, δηλαδή $x_1 \equiv x_2 \text{mod} n$.

Οπότε, η λύση είναι μοναδική mod$n_1 n_2 \ldots n_k$.

□

1.6 Θεωρήματα Euler - Fermat

Theorem 1.6.1 (Θεώρημα Euler). *Αν* $a, m \in \mathbb{Z}$ *με* $m > 0$ *και* $ΜΚΔ(a, m) = 1$, *τότε* $a^{\phi(m)} \equiv 1 mod m$.

Proof. Για $m = 2$ προφανώς ισχύει, αφού αν $\text{ΜΚΔ}(a, 2) = 1$, ο a είναι περιττος.

Για $m \geq 3$, θεωρούμε τους αριθμούς:

$$r_1, r_2, \ldots r_{\phi(m)}$$

που είναι σχετικά πρώτοι με το m. Αν πολλαπλασιάσουμε όλους τους αριθμούς με το $a \text{mod} m$ τότε θα έχουμε τους αριθμούς:

$$a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(m)} \text{mod} m$$

Επειδή $\text{ΜΚΔ}(a, m) = 1$, τότε ο $a \cdot r_i$ είναι σχετικά πρώτος με τον m για κάθε i. Όμως, οι αριθμοί $r_1, r_2, \ldots, r_{\phi(m)}$ είναι όλοι οι σχετικά πρώτοι με τον $m \text{mod} m$, οπότε $ar_i = r_j$ για κάποιο j.

Επίσης, δεν μπορεί να ισχύει ότι $ar_i \equiv ar_j \text{mod} m$ για κάποιους r_i, r_j, αφού τότε θα είχαμε $r_i \equiv r_j \text{mod} m$ από τον νόμο της διαγραφής, αφού $\text{ΜΚΔ}(a, m) = 1$, άτοπο.

Έτσι οι αριθμοί $ar_1, ar_2, \ldots, ar_{\phi(m)} \text{mod} m$ είναι οι ίδιοι με τους $r_1, r_2, \ldots, r_{\phi(m)} \text{mod} m$.

Οπότε,

$(ar_1)(ar_2)\ldots(ar_{\phi(m)}) \equiv r_1 r_2 \ldots r_{\phi(m)} \text{mod} m \Leftrightarrow$

$a^{\phi(m)} r_1 r_2 \ldots r_{\phi(m)} \equiv r_1 r_2 \ldots r_{\phi(m)} \text{mod} m \Leftrightarrow$

$a^{\phi(m)} \equiv 1 \text{mod} m$ σύμφωνα με το (1.4.1) αφού $\text{ΜΚΔ}(m, r_i) = 1$ για κάθε i.

Άρα, $a^{\phi(m)} \equiv 1 \text{mod} m$ □

Theorem 1.6.2 (Μικρό θεώρημα του Fermat). *Αν* p *είναι ένας πρώτος αριθμός και* $a \in \mathbb{Z}$ *με* $ΜΚΔ(a, p) = 1$, *τότε* $a^{p-1} \equiv 1 \ mod p$

Proof. Προκύπτει ως ειδική περίπτωση του θεωρήματος του Euler. □

2 Τετραγωνικά υπόλοιπα

2.1 Σύμβολο Legendre

Definition. Έστω οι ακέραιοι αριθμοί a, m με $m > 0$. Ο a ονομάζεται τετραγωνικό υπόλοιπο του m, αν $\text{ΜΚΔ}(a, m) = 1$ και η ισοτιμία $x^2 \equiv a \text{mod} m$ έχει λύση.

Example. Το 2 είναι τετραγωνικό υπόλοιπο του 7 καθώς $\text{ΜΚΔ}(2, 7) = 1$ και $3^2 \equiv 2 \text{mod} 7$.

Theorem 2.1.1. *Έστω p περιττός πρώτος αριθμός και a ακέραιος με $ΜΚΔ(a, p) = 1$. Τότε η ισοδυναμία $x^2 \equiv a mod p$ είτε δεν θα έχει καμμία λύση ή θα έχει δυο διαφορετικές λύσεις $mod p$.*

Proof. Έστω ότι η ισοτιμία $x^2 \equiv a \text{mod} p$ έχει λύση και έστω $x_0 \epsilon \mathbb{Z}$ με $x_0^2 \equiv a \text{mod} p$.

Τότε, προφανώς και η $-x_0$ είναι λύση της ισοτιμίας καθώς

$$(-x_0)^2 = x_0^2 \equiv a \text{mod} p$$

όπου

$$-x_0 \equiv p - x_0 \text{mod} p.$$

Ισχύει ότι $x_0 \neq -x_0 \text{mod} p$ καθώς αν $x_0 \equiv -x_0 \text{mod} p$, τότε $p|2x_0$, οπότε $p|x_0$.

Τότε $p|x_0^2$ και επειδή $x_0^2 \equiv a \text{mod} p$ θα έχουμε επίσης $p|\left(x_0^2 - a\right)$ και άρα $p|\left(x_0^2 - \left(x_0^2 - a\right)\right) \Rightarrow p|a$ κάτι που είναι άτοπο από την υπόθεση.

Θα αποδείξουμε οτι δεν υπάρχουν άλλες λύσεις της $x^2 \equiv a \text{mod} p$.

Έστω y τυχαία λύση της $x^2 \equiv a \text{mod} p$, τότε:

$$x_0^2 \equiv y^2 \text{mod} p$$

Συνεπώς,

$$p|\left(x_0^2 - y^2\right) \Rightarrow p|\left(x_0 - y\right)\left(x_0 + y\right)$$

οπότε

$$p|\left(x_0 - y\right) \text{ ή } p|\left(x_0 + y\right)$$

άρα

$$y \equiv x_0 \text{mod} p \text{ ή } y \equiv -x_0 \text{mod} p.$$

Άρα οι μοναδικές λύσεις $\text{mod} p$ είναι οι x_0 και $-x_0$. □

Remark 2.1.2. Το 1 είναι τετραγωνικό υπόλοιπο mod$p$ για κάθε περιττό πρώτο p και οι δύο διαφορετικές λύσεις της $x^2 \equiv 1 \text{mod} p$ είναι οι $x_1 = 1, x_2 = p-1 \equiv -1 \text{mod} p$.

Proposition 2.1.3. *Έστω p περιττός πρώτος αριθμός, τότε για κάθε $x \in \{2, 3, \dots p-2\}$ υπάρχει μοναδικός $y \in \{2, 3, \dots, p-2\}, y \neq x$ με $xy \equiv 1 mod p$*

Proof. Επειδή $x < p$ τότε ΜΚΔ$(x, p) = 1$, οπότε από το (1.4.2) υπάρχει μοναδικός(mod$p$) y τέτοιος ώστε $xy \equiv 1 \text{mod} p$.

Για τον y έχουμε ότι $y \neq 0, 1, p-1 \text{mod} p$, γιατί αν έπαιρνε κάποια τέτοια τιμή, τότε θα είχαμε αντίστοιχα $xy \equiv 0, x, -x \text{mod} p$ που καμία από τις παραπάνω τιμές δεν είναι $1 \text{mod} p$.

Το y δεν μπορεί επίσης να πάρει την τιμή x καθώς τότε θα ίσχυε ότι $x^2 \equiv 1 \text{mod} p$, οπότε από (2.1.2) το $x \equiv 1$ ή -1 mod$p$ κάτι που είναι αντίθετο με την υπόθεση.

Οπότε, $y \in \{2, 3, \dots, p-2\}$ με $y \neq x$. □

Theorem 2.1.4 (Θεώρημα Wilson). *Ο φυσικός αριθμός $p > 2$ είναι πρώτος αν και μόνο αν*

$$(p-1)! = -1 mod p$$

Proof. Αφού ο p είναι πρώτος, τότε σύμφωνα με το (2.1.3) οι αριθμοί $2, 3, \dots p-2$ αποτελούν ζεύγη αντιστρόφων mod$p$, οπότε

$$2 \cdot 3 \cdots (p-2) \equiv 1 \text{mod} p$$

άρα,

$$(p-1)! = 2 \cdot 3 \cdots (p-2)\,(p-1) \equiv -1 \text{mod} p.$$

Από την άλλη μεριά, έστω ότι $(p-1)! \equiv -1 \text{mod} p$ και ο p είναι σύνθετος.

Τότε $p > 4$ καθώς $(4-1)! = 6 \neq -1$ mod4.

Αφού ο p είναι σύνθετος, τότε υπάρχουν ακέραιοι a, b με $1 < a, b < p$ τέτοιοι ώστε $p = ab$.

Οι a, b θα εμφανίζονται στο παραγοντικό $(p-1)!$ οπότε $(p-1)! \equiv 0$ mod$p$ εκτός αν $p = q^2$, με q πρώτο.

Τότε όμως ο αριθμός $2q$ εμφανίζεται στο γινόμενο οπότε $(p-1)! \equiv 0$ mod$p$, το οποίο όμως είναι άτοπο γιατί υποθέσαμε ότι $(p-1)! \equiv -1 \text{mod} p$.

Άρα, ο p είναι πρώτος. □

Remark. Το θεώρημα Wilson αποτελεί ένα από τα λίγα καθολικά κριτήρια με το οποίο μπορούμε να εξετάσουμε αν ένας αριθμός είναι πρώτος. Παρ' όλα αυτά δεν είναι καθόλου αποδοτικό στην πράξη και γι' αυτό δεν χρησιμοποιείται.

Theorem 2.1.5. *Έστω p περιττός πρώτος αριθμός, τότε υπάρχουν ακριβώς $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα μη ισοδύναμα $mod p$ και αυτά είναι τα*

$$1^2 mod p, 2^2 mod p, \ldots, \left(\frac{p-1}{2}\right)^2 mod p.$$

Proof. Έστω το τετραγωνικό υπόλοιπο a και x_a ακέραιος τέτοιος ώστε $x_a^2 \equiv a \mathrm{mod} p$.

Προφανώς $x_a \neq 0 \mathrm{mod} p$ καθώς αν $x_a \equiv 0 \mathrm{mod} p$ τότε $p|a$ οπότε το a δεν είναι τετραγωνικό υπόλοιπο $\mathrm{mod} p$.

Επίσης, αν $x \equiv x_a \mathrm{mod} p$ τότε $x^2 \equiv x_a^2 \mathrm{mod} p$ οπότε $x^2 \equiv a \mathrm{mod} p$.

Επειδή κάθε ακέραιος x που δεν είναι πολλαπλάσιο του πρώτου p είναι ισοδύναμος με έναν ακριβώς από τους ακέραιους $1, 2, \ldots, p-1$ για να βρω ποια είναι τα τετραγωνικά υπόλοιπα που δεν είναι ισοδύναμα μεταξύ τους $\mathrm{mod} p$ αρκεί να βρω ποια από τα $1^2, 2^2, \ldots, (p-1)^2 \mathrm{mod} p$ δεν είναι ισοδύναμα μεταξύ τους.

Έστω $A = \left\{1, 2, \ldots, \left(\frac{p-1}{2}\right)\right\}$ τότε $p - A = \left\{\frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1\right\}$.

Οπότε $\{1, 2, \ldots, p-1\} = A \cup (p - A)$ και $A \cap (p - A) = \emptyset$.

Τότε τα τετραγωνικά υπόλοιπα που παράγονται από το $\{1, 2, \ldots, p-1\}$ είναι όσα παράγονται από το A καθώς

$$x^2 \equiv (p-x)^2 \mathrm{mod} p$$

οπότε το σύνολο $\left\{1^2 \mathrm{mod} p, 2^2 \mathrm{mod} p, ..., \left(\frac{p-1}{2}\right)^2 \mathrm{mod} p\right\}$ περιέχει όλα τα τετραγωνικά υπόλοιπα (τα μη ισοδύναμα $\mathrm{mod} p$).

Θα αποδείξουμε, ότι οι ακέραιοι $1^2 \mathrm{mod} p, 2^2 \mathrm{mod} p, ..., \left(\frac{p-1}{2}\right)^2 \mathrm{mod} p$ είναι και ανα δυο μη ισοδύναμοι $\mathrm{mod} p$.

Έστω $x_1, x_2 \epsilon \left\{1, 2, ..., \frac{p-1}{2}\right\}$.

Αν $x_1^2 \equiv x_2^2 \mathrm{mod} p$ με $x_1 \neq x_2$, τότε $p|\,(x_1 - x_2)\,(x_1 + x_2)$, οπότε $p|\,(x_1 - x_2)$ ή $p|\,(x_1 + x_2)$.

Επειδή $1 < x_1 + x_2 < p$, τότε $p \nmid (x_1 + x_2)$.

Οπότε $p|\,(x_1 - x_2)$.

Όμως, $-p < x_1 - x_2 < p$.

Οπότε, $x_1 = x_2$ κάτι που είναι άτοπο.

Άρα το σύνολο των μη ισοδύναμων τετραγωνικών υπολοίπων $\mathrm{mod} p$ είναι το σύνολο $\left\{i^2 \mathrm{mod} p : i \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}\right\}$. □

Remark. Από το προηγούμενο θεώρημα προκύπτει ένας αλγόριθμος με τον οποίο εξετάζουμε αν ένας ακέραιος a είναι τετραγωνικό υπόλοιπο $\mathrm{mod} p$.

Θεωρούμε ένα διάνυσμα μήκους $\frac{p-1}{2}$ στο οποίο εκχωρούμε τα $i^2 \mathrm{mod} p$ για $i = 1, 2, \ldots, \frac{p-1}{2}$ και μετά εξετάζουμε για τον ακέραιο a αν ο a είναι ισοϋπόλοιπος με κάποιο από τα στοιχεία του διανύσματος.

Αν είναι, τότε το a είναι τετραγωνικό υπόλοιπο $\mathrm{mod} p$. Αν όχι, δεν είναι.

Ο αλγόριθμος σε μορφή ψευδοκώδικα είναι ο εξής:

```
Input: integer a, odd prime p
        a:=aMODp;
        FOR i:=1 TO (p-1)/2
            A[i]:=i*iMODp;
        state:=false;
        FOR i:=1 TO (p-1)/2
             IF a=A[i]
                  state:=true;
                  break;
        RETURN state;
```

Example 2.1.6. Τα τετραγωνικά υπόλοιπα του 19 είναι τα $\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$.

Remark. Ο αλγόριθμος μπορεί να χρησιμοποιηθεί για μικρούς πρώτους αριθμούς.

Definition (Σύμβολο Legendre)**.** Έστω p περιττός πρώτος αριθμός και a ένας ακέραιος αριθμός με $\text{ΜΚΔ}(a, p) = 1$. Τότε, ορίζουμε το σύμβολο του Legendre $\left(\frac{a}{p}\right)$ ως εξής:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{αν ο α είναι τετραγωνικό υπόλοιπο mod} \quad p \\ -1, \text{ αλλιώς} \end{cases}$$

Το σύμβολο του Legendre γενικεύεται και στην περίπτωση όπου $p|a$. Τότε $\left(\frac{a}{p}\right) = 0$.

2.2 Κριτήριο του Euler

Lemma 2.2.1. *Αν p περιττός πρώτος και a ακέραιος με $ΜΚΔ(a, p) = 1$ τότε*

$$a^{\frac{p-1}{2}} \equiv 1 mod p \text{ ή } a^{\frac{p-1}{2}} \equiv -1 mod p$$

Proof. Αφού p πρώτος και $\text{ΜΚΔ}(a, p) = 1$, από το θεώρημα του Fermat έχουμε ότι

$$a^{p-1} \equiv 1 \text{mod} p \Leftrightarrow a^{p-1} - 1 \equiv 0 \text{mod} p.$$

Οπότε, $\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \text{mod} p$ οπότε ή $a^{\frac{p-1}{2}} \equiv 1 \text{mod} p$ ή $a^{\frac{p-1}{2}} \equiv -1 \text{mod} p$ □

Theorem 2.2.2 (Θεώρημα Dirichlet)**.** *Έστω p πρώτος αριθμός και a ακέραιος με $1 \leq a \leq p-1$. Αν η ισοδυναμία $x^2 \equiv a \ mod p$ δεν έχει λύσεις, τότε $p|(p-1)! - a^{\frac{p-1}{2}}$, ενώ αν η ισοδυναμία $x^2 \equiv a \ mod p$ έχει λύσεις, τότε $p|(p-1)! + a^{\frac{p-1}{2}}$.*

Proof. Για την απόδειξη ο αναγνώστης παραπέμπεται στο ([4]) □

Theorem 2.2.3 (Το κριτήριο του Euler)**.** *Έστω p περιττός πρώτος και a ακέραιος με $MK\Delta(a,p)=1$. Τότε, ισχύει ότι $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} mod p$*

Proof. Αν ο a είναι τετραγωνικό υπόλοιπο του p τότε υπάρχει ακέραιος x_0 τέτοιος ώστε $x_0^2 \equiv a \bmod p$.

Οπότε,

$$\left(x_0^2\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \bmod p$$

άρα

$$x_0^{p-1} \equiv a^{\frac{p-1}{2}} \bmod p.$$

Όμως, $\text{ΜΚΔ}(x_0,p)=1$ καθώς αν ίσχυε ότι $p|x_0$ τότε αφού $p|(x_0^2-a)$ θα έπρεπε να έχουμε ότι $p|a$. Άτοπο καθώς έχουμε ότι $\text{ΜΚΔ}(a,p)=1$.

Επομένως, από το (1.6.2) θα έχουμε ότι

$$x_0^{p-1} \equiv 1 \bmod p$$

Άρα,

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

Επειδή έχουμε υποθέσει ότι ο a είναι τετραγωνικό υπόλοιπο τότε $\left(\frac{a}{p}\right)=1$.

Οπότε,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Αν $(\frac{a}{p})=-1$, τότε η ισοτιμία $x^2 \equiv a \bmod p$ δεν έχει καμία λύση.

Οπότε, από το (2.2.2) έχουμε ότι

$$p|\,(p-1)!-a^{\frac{p-1}{2}}$$

άρα

$$a^{\frac{p-1}{2}} \equiv (p-1)! \bmod p$$

και από το θεώρημα του Wilson έχουμε

$$(p-1)! \equiv -1 \bmod p$$

οπότε,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

□

Remark. Από το κριτήριο του Euler έχουμε μια μέθοδο με την οποία απαντάμε αν ο ακέραιος a είναι τετραγωνικό υπόλοιπο του περιττού πρώτου p. Η μέθοδος είναι η εξής:

Υπολογίζουμε το $a^{\frac{p-1}{2}} \mathrm{mod} p$ και αν είναι 1 τότε το a είναι τετραγωνικό υπόλοιπο ενώ αν είναι $p-1$ ή -1 τότε δεν είναι.

Για να βρούμε το $a^{\frac{p-1}{2}}$ θα χρησιμοποιήσουμε τον αλγόριθμο της ύψωσης σε δύναμη με επαναλαμβανόμενο τετραγωνισμό.

```
fastPower(a,n)
   result:=1;
   WHILE n>0
       IF odd(n)
           result:=result*a;
       n:=nDIV2;
       a:=a*a;
RETURN result;
```

η πολυπλοκότητα του αλγορίθμου είναι O(log n).

Επειδή, έχω να βρω το $a^{\frac{p-1}{2}} \mathrm{mod} p$ και όχι το $a^{\frac{p-1}{2}}$ θα χρησιμοποιήσω έναν προσαρμοσμένο αλγόριθμο στον οποίο ο ακέραιος που θα επιστρέφεται θα είναι πολύ μικρότερος από αυτόν που θα επέστρεφε ο fastPower.

```
fastPowerMod(a,n,k)
   a:=aMODk;
   result:=1;
   WHILE n>0
       IF odd(n)
           result:=result*a;
           result:=resultMODk;
       n:=nDIV2;
       a:=a*a;
       a:=aMODk;
  RETURN result;
```

ο αλγόριθμος fastPowerMod μας επιστρέφει το $a^n \mathrm{mod} k$ και έχει ως παραμέτρους:

a: ο ακέραιος αριθμός που υψώνεται στην δύναμη

n: ο φυσικός εκθέτης

k: το modulo

Το πλεονέκτημα του fastPowerMod σε σχέση με τον fastPower είναι ότι εκμεταλευόμαστε το γεγονός ότι υπολογίζουμε την δύναμη $a^n \mathrm{mod} k$, οπότε μας ενδιαφέρει να επιστρέψουμε έναν αριθμό $\leq k$ οπότε δεν χρειαζόμαστε να αποθηκεύσουμε ολόκληρο τον a^n και μετά να πάρουμε το $a^n \mathrm{mod} k$. Αυτό που κάνει πιο λειτουργικό τον fastPowerMod είναι ότι ο ακέραιος που χρησιμοποιείται (result) θα είναι σε κάθε βήμα του αλγορίθμου $< k^2$. Σε

αντίθεση με αυτό, αν υπολογίσουμε πρώτα τον a^n ολόκληρο για αρκετά μεγάλο n θα έχουμε έναν τερατώδη αριθμό.

Για παράδειγμα αν θελήσουμε να βρούμε τον αριθμό $101^{1500}\text{mod}133$ με τον fastPowerMod σε κάθε βήμα ο result θα είναι μικρότερος από 133^2, οπότε θα έχει το πολύ 5 ψηφία. Από την άλλη μεριά, αν υπολογίσουμε τον 101^{1500} με τον αλγόριθμο fastPower θα πάρουμε έναν αριθμό που θα έχει τουλάχιστον 3000 ψηφία. Τρομακτική διαφορά από άποψη μνήμης που χρησιμοποιείται για το πρόβλημα.

Τώρα, θα υπολογίσουμε το σύμβολο Legendre με τον επόμενο αλγόριθμο:

```
Legendre(a,p)
    temp:=fastPowerMod(a,(p-1)/2,p);
    IF temp=p-1
        RETURN -1;
    ELSE
        RETURN 1;
```

2.3 Ιδιότητες Τετραγωνικών Υπολοίπων

Theorem 2.3.1. *Έστω p περιττός πρώτος και a ακέραιος με $ΜΚΔ(a,p)=1$.*
Αν $a \equiv b mod p$, τότε $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proof. Αν $\left(\frac{a}{p}\right) = 1$ τότε υπάρχει $x_0 \in \mathbb{Z}$ με $x_0^2 \equiv a\text{mod}p$ τότε $x_0^2 \equiv b\text{mod}p$ καθώς $a \equiv b\text{mod}p$. Επίσης, $\text{ΜΚΔ}(b,p)=1$ καθώς αν $p|b$ τότε $p|a$ αφού $a \equiv b\text{mod}p$. Οπότε το b είναι τετραγωνικό υπόλοιπο mod$p$. Οπότε, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$.

Αν $\left(\frac{a}{p}\right) = -1$ τότε για κάθε $x \in \mathbb{Z}$ θα έχουμε ότι $x^2 \neq a\text{mod}p$ και επειδή $a \equiv b\text{mod}p$ τότε $x^2 \neq b\text{mod}p$. Οπότε, το b δεν είναι τετραγωνικό υπόλοιπο mod$p$. Οπότε, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$.

Άρα, σε κάθε περίπτωση θα έχουμε $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. □

Theorem 2.3.2. *Έστω p περιττός πρώτος και οι ακέραιοι a, b με $ΜΚΔ(ab,p)=1$.*
Τότε, θα έχουμε ότι $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof. Σύμφωνα με το (2.2.3) ισχύει ότι:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \text{mod}p \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \text{mod}p \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \text{mod}p.$$

Οπότε,

$$p| \left[\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right].$$

Επειδή ο p είναι περιττός πρώτος αριθμός και τα $\left(\frac{ab}{p}\right), \left(\frac{a}{p}\right), \left(\frac{b}{p}\right)$ είναι ίσα με -1 ή 1, τότε θα πρέπει να έχουμε ότι

$$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0.$$

Άρα,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Lemma 2.3.3. *Έστω p περιττός πρώτος .*
Τότε $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \alpha\nu\ p \equiv 1 mod\ 4 \\ -1, & \alpha\nu\ p \equiv 3 mod\ 4 \end{cases}$

Proof. Χρησιμοποιώντας το (2.2.3) έχουμε ότι

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mathrm{mod} p.$$

Οπότε, όπως και στην προηγούμενη απόδειξη θα έχουμε ότι

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

□

Proposition 2.3.4. *Έστω x ακέραιος αριθμός, τότε $x^2 \equiv 0 mod 4$ ή $x^2 \equiv 1 mod 4$*

Proof. Αν ο x είναι άρτιος , τότε $x = 2n$, για κάποιο $n \epsilon \mathbb{Z}$, οπότε

$$x^2 = 4n^2 \equiv 0 \mathrm{mod} 4.$$

Αν ο x είναι περιττος, τότε $x = 2n + 1$ για κάποιο $n \epsilon Z$, οπότε

$$x^2 = 4n\,(n+1) + 1 \equiv 1 \mathrm{mod} 4.$$

□

Proposition 2.3.5. *Έστω x ακέραιος αριθμός, τότε $x^2 \equiv 0 mod 8$ ή $x^2 \equiv 1 mod 8$ ή $x^2 \equiv 4 mod 8$*

Proof. Αν ο x είναι άρτιος , τότε $x = 2n$, για κάποιο $n \epsilon \mathbb{Z}$, οπότε $x^2 = 4n^2$, οπότε αν ο n είναι άρτιος τότε

$$x^2 \equiv 0 \mathrm{mod} 8 \text{ ή } x^2 \equiv 4 \mathrm{mod} 8$$

Αν ο x είναι περιττος, τότε $x = 2n + 1$ για κάποιο $n \epsilon Z$, οπότε

$$x^2 = 4n\,(n+1) + 1 \equiv 1 \mathrm{mod} 8$$

καθώς το γινόμενο δυο διαδοχικών ακέραιων αριθμών είναι άρτιος, οπότε ο αριθμός $n\,(n+1)$ είναι άρτιος. □

2.4 Νόμος Τετραγωνικής Αντιστροφής

Theorem 2.4.1 (Το Λήμμα του Gauss). *Έστω p περιττός πρώτος και a ακέραιος με $MK\Delta(a,p)=1$. Έστω οι αριθμοί*

$$amodp, 2amodp, \ldots, \frac{p-1}{2}amodp.$$

Αν s είναι το πλήθος των αριθμών που είναι μεγαλύτεροι από τον $\frac{p}{2}$, τότε :

$$\left(\frac{a}{p}\right) = (-1)^s$$

Proof. Έστω

$$S = \left\{ k a \mathrm{mod} p : k \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}\right\}.$$

Επίσης, έστω

$$A = \left\{x \in S : x > \frac{p}{2}\right\} \text{ και } B = \left\{y \in S : y < \frac{p}{2}\right\}.$$

Τότε, προφανώς

$$A \cap B = \emptyset \text{ και } A \cup B = S.$$

Ακόμα σύμφωνα με την υπόθεση $|A| = s$ και $|B| = \frac{p-1}{2} - s$. Έστω $r = \frac{p-1}{2} - s$.
Τότε, θεωρώ ότι

$$A = \{a_1, a_2, \ldots, a_s\} \text{ και } B = \{b_1, b_2, \ldots, b_r\}.$$

Τότε θα έχουμε ότι:

$$a_1 a_2 \ldots a_s b_1 b_2 \ldots b_r \equiv a\,(2a) \ldots \left(\frac{p-1}{2}a\right) \mathrm{mod} p$$

οπότε,

$$a_1 a_2 \ldots a_s b_1 b_2 \ldots b_r \equiv \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \mathrm{mod} p. \tag{2.1}$$

Έστω το σύνολο

$$L = \{p - a_1, p - a_2, \ldots, p - a_s, b_1, b_2, \ldots, b_r\}$$

τότε κάθε στοιχείο του συνόλου είναι μικρότερο από $\frac{p}{2}$ καθώς

$$b_i < \frac{p}{2} \text{ για } i = 1, 2, \ldots, r$$

και

$$p - a_j < \frac{p}{2} \text{ καθώς } a_j > \frac{p}{2} \text{ για } j = 1, 2, \ldots, s.$$

Οπότε, $L \subseteq \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$.
Θα αποδείξουμε ότι $L = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$.
Αρκεί να δείξουμε ότι για $i = 1, 2, \ldots, r$ και $j = 1, 2, \ldots, s$ ισχύει ότι $b_i \neq p - a_j$.
Επείδη οι αριθμοί $b_i, p - a_j \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ αρκεί να δείξουμε ότι $b_i \neq p - a_j \mathrm{mod} p$.
Οπότε, έστω ότι

$$b_i \equiv p - a_j \mathrm{mod} p \Rightarrow a_j + b_i \equiv 0 \mathrm{mod} p.$$

Όμως, υπάρχουν k, l διαφορετικοί μεταξύ τους με

$$1 \leq k, l < \frac{p}{2} \text{ και } b_i \equiv ka \mathrm{mod} p,\ a_j \equiv la \mathrm{mod} p.$$

Οπότε,

$$p | (a_j + b_i) = (k + l) a.$$

Τότε, όμως θα πρέπει $p | (k + l)$ καθώς $\mathrm{ΜΚΔ}(a, p) = 1$.
Αυτό είναι άτοπο, καθώς $1 < k + l < p$.
Άρα, $b_i \neq p - a_j \mathrm{mod} p$ για $i = 1, 2, \ldots, r$ και $j = 1, 2, \ldots, s$.
Οπότε, $L = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ και τότε

$$\left(\frac{p-1}{2}\right)! = b_1 b_2 \ldots b_r (p - a_1)(p - a_2) \ldots (p - a_s) \equiv (-1)^s a_1 \ldots a_s b_1 \ldots b_r \mathrm{mod} p$$

και από την (2.1) θα έχουμε ότι:

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^s \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \mathrm{mod} p$$

Οπότε,

$$1 \equiv (-1)^s a^{\frac{p-1}{2}} \mathrm{mod} p$$

Οπότε,

$$a^{\frac{p-1}{2}} \equiv (-1)^s \mathrm{mod} p.$$

Άρα,

$$\left(\frac{a}{p}\right) = (-1)^s$$

□

Theorem 2.4.2. *Έστω p περιττός πρώτος. Τότε ισχύει ότι*

$$(\frac{2}{p}) = \begin{cases} 1, & \alpha\nu\ p \equiv \pm 1 mod\ 8 \\ -1, & \alpha\nu\ p \equiv \pm 3 mod\ 8 \end{cases} = (-1)^{\frac{p^2-1}{8}}$$

Proof. Έστω s το πλήθος των στοιχείων του $\left\{2, 4, 6, \ldots, 2 \cdot \frac{p-1}{2}\right\}$ που υπερβαίνουν το $\frac{p}{2}$.
Τότε, $s = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$.
Οπότε, για
$p = 8m+1$ θα έχουμε $s = 4m - \lfloor 2m + \frac{1}{4} \rfloor = 2m \equiv 0 \text{mod} 2$
$p = 8m+3$ θα έχουμε $s = 4m + 1 - \lfloor 2m + \frac{3}{4} \rfloor = 2m + 1 \equiv 1 \text{mod} 2$
$p = 8m+5$ θα έχουμε $s = 4m + 2 - \lfloor 2m + 1 + \frac{1}{4} \rfloor = 2m + 1 \equiv 1 \text{mod} 2$
$p = 8m+7$ θα έχουμε $s = 4m + 3 - \lfloor 2m + 1 + \frac{3}{4} \rfloor = 2m + 2 \equiv 0 \text{mod} 2$.
Οπότε,

$$(\frac{2}{p}) = \begin{cases} 1, & \alpha\nu\ p \equiv \pm 1 \text{mod}\ 8 \\ -1, & \alpha\nu\ p \equiv \pm 3 \text{mod}\ 8 \end{cases}$$

□

Proposition 2.4.3. *Έστω p περιττός πρώτος και a ακέραιος με $ΜΚΔ(a,p) = 1$. Αν s είναι το πλήθος των αριθμών*

$$amodp, 2amodp, \ldots, \frac{p-1}{2}amodp$$

που είναι μεγαλύτεροι από $\frac{p}{2}$ τότε ισχύει ότι

$$s \equiv (a-1)\frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor mod 2.$$

Proof. Για τους αριθμούς $a, 2a, \ldots, \frac{p-1}{2}a$ ισχύει ότι :

$$a = \lfloor \frac{a}{p} \rfloor p + r_1, 2a = \lfloor \frac{2a}{p} \rfloor p + r_2, \ldots, \frac{p-1}{2}a = \lfloor \frac{(p-1)\,a}{2p} \rfloor p + r_{\frac{p-1}{2}}$$

με

$$0 < r_i < p,\ i = 1, 2, \ldots, \frac{p-1}{2}.$$

Από την απόδειξη του λήμματος του Gauss ξέρουμε ότι για τα υπόλοιπα r_i υπάρχουν ακριβώς s που είναι μεγαλύτερα από $\frac{p}{2}$ έστω τα $a_1, a_2, \ldots, a_s$ και ότι υπάρχουν $\frac{p-1}{2} - s = r$ που είναι μικρότερα από $\frac{p}{2}$ έστω τα $b_1, b_2, \ldots, b_r$.

Επίσης ξέρουμε ότι για το σύνολο

$$L = \{p - a_1, p - a_2, \ldots, p - a_s, b_1, b_2, \ldots, b_r\}$$

ισχύει ότι

$$L = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$$

Τότε,

$$a + 2a + \cdots + \frac{p-1}{2}a = a\left(1 + 2 + \frac{p-1}{2}\right) = p\sum_{j=1}^{\frac{p-1}{2}}\lfloor\frac{ja}{p}\rfloor + \sum_{i=1}^{s}a_i + \sum_{i=1}^{r}b_i.$$

Όμως,

$$\sum_{i=1}^{s}(p - a_i) + \sum_{j=1}^{r}b_j = \sum_{i=1}^{\frac{p-1}{2}}i = \frac{p^2-1}{8}.$$

Οπότε,

$$\sum_{i=1}^{s}a_i + \sum_{i=1}^{r}b_i = \sum_{i=1}^{s}(p - a_i) + \sum_{j=1}^{r}b_j - sp + 2\sum_{i=1}^{s}a_i = \frac{p^2-1}{8} - sp + 2\sum_{i=1}^{s}a_i$$

Οπότε,

$$a\frac{p^2-1}{8} = p\sum_{j=1}^{\frac{p-1}{2}}\lfloor\frac{ja}{p}\rfloor + \frac{p^2-1}{8} - sp + 2\sum_{i=1}^{s}a_i$$

Οπότε,

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{\frac{p-1}{2}}\lfloor\frac{ja}{p}\rfloor + s \bmod 2$$

καθώς $p \equiv 1 \bmod 2$ και $-1 \equiv 1 \bmod 2$.

Οπότε,

$$s \equiv (a-1)\frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}}\lfloor\frac{ja}{p}\rfloor \bmod 2$$

□

Theorem 2.4.4 (Νόμος Τετραγωνικής Αντιστροφής). *Έστω p, q δυο διαφορετικοί περιττοί πρώτοι αριθμοί. Τότε, ισχύει ότι*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Proof. Για να αποδείξω τον νόμο της τετραγωνικής αντιστροφής θα χρησιμοποιήσω το λήμμα του Gauss και το (2.4.3).

Έστω s_p το πλήθος των στοιχείων του συνόλου $A_p = \left\{kp \mathrm{mod} q : k = 1, 2, \ldots, \frac{q-1}{2}\right\}$ που είναι μεγαλύτερα από $\frac{q}{2}$.

Επίσης, έστω s_q το πλήθος των στοιχείων του συνόλου $A_q = \left\{kq \mathrm{mod} p : k = 1, 2, \ldots, \frac{p-1}{2}\right\}$ που είναι μεγαλύτερα από $\frac{p}{2}$.

Τότε, σύμφωνα με το λήμμα του Gauss θα ισχύει $\left(\frac{p}{q}\right) = (-1)^{s_p}$ και $\left(\frac{q}{p}\right) = (-1)^{s_q}$.

Οπότε,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{s_p + s_q}.$$

Τότε, αρκεί να δείξουμε ότι

$$s_p + s_q \equiv \frac{(p-1)(q-1)}{4} \mathrm{mod} 2$$

όμως, σύμφωνα με το (2.4.3) θα έχουμε ότι

$$s_p \equiv (p-1)\frac{q^2-1}{8} + \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor \mathrm{mod} 2 \equiv \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor \mathrm{mod} 2$$

καθώς ο p είναι περιττός πρώτος οπότε $p - 1 \equiv 0 \mathrm{mod} 2$.

Με τον ίδιο τρόπο έχουμε ότι

$$s_q \equiv \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{jq}{p} \rfloor \mathrm{mod} 2$$

οπότε αρκεί να δείξουμε ότι

$$\sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor + \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{jq}{p} \rfloor \equiv \frac{(p-1)(q-1)}{4} \mathrm{mod} 2.$$

Για την ακρίβεια θα αποδείξουμε κάτι πιο ισχυρό, θα αποδείξουμε ισότητα.

Δηλαδή, θα δείξουμε ότι

$$\sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor + \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{jq}{p} \rfloor = \frac{(p-1)(q-1)}{4}.$$

Τότε, έστω

$$S_p = \left\{1, 2, \ldots, \frac{p-1}{2}\right\} \text{ και } S_q = \left\{1, 2, \ldots, \frac{q-1}{2}\right\}$$

και έστω η συνάρτηση

$$f : S_p X S_q \to \mathbb{Z} \text{ με } f(x, y) = qx - py.$$

Η f είναι ένα $1-1$ καθώς αν

$$f(x, y) = f(x', y') \text{ τότε } q\left(x - x'\right) = p\left(y - y'\right)$$

και επειδή $\text{ΜΚΔ}(p, q) = 1$ θα πρέπει να ισχύει

$$p|\left(x - x'\right) \text{ και } q|\left(y - y'\right)$$

κάτι που σημαίνει ότι $x = x'$ και $y = y'$ καθώς

$$1 \leq x, x' \leq \frac{p-1}{2} \text{ και } 1 \leq y, y' \leq \frac{q-1}{2}$$

οπότε

$$|x - x'| < \frac{p}{2} \text{ και } |y - y'| < \frac{p}{2}.$$

Επίσης, η f δεν μηδενίζεται πουθενά.

Επειδή η f είναι 1-1 το σύνολο τιμών της f θα έχει τον ίδιο πληθάριθμο με το πεδίο ορισμού της f.

Οπότε

$$|range(f)| = \frac{(p-1)(q-1)}{4}.$$

Το πλήθος των θετικών τιμών της f είναι $\sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{xq}{p} \rfloor$ καθώς για κάθε $x \in S_p$ θα έχουμε $f(x, y) > 0$ αν $y < \frac{qx}{p}$.

Οπότε, για $x = 1, 2, \ldots \frac{p-1}{2}$ θα έχουμε $\lfloor \frac{xq}{p} \rfloor$τιμές του y για τις οποίες $f(x, y) > 0$.

Οπότε, το πλήθος των θετικών τιμών της f είναι $\sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{xq}{p} \rfloor$.

Με την ίδια λογική για το τυχαίο $y \in S_q$ θα έχουμε ότι $f(x, y) < 0$ αν $x < \frac{py}{q}$.

Οπότε, για $y = 1, 2, \ldots, \frac{q-1}{2}$ θα έχουμε $\lfloor \frac{yp}{q} \rfloor$ τιμές του x για τις οποίες $f(x, y) < 0$.

Οπότε, το πλήθος των αρνητικών τιμών της f είναι $\sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{yp}{q} \rfloor$.

Συνοψίζοντας τα παραπάνω θα έχουμε ότι

$$\sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{xq}{p} \rfloor + \sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{yp}{q} \rfloor = \frac{(p-1)(q-1)}{4}.$$

Οπότε, η απόδειξη έχει ολοκληρωθεί. □

Remark. Ο νόμος της τετραγωνικής αντιστροφής είναι ισοδύναμος με την επιλυσιμότητα των εξισώσεων

$$x^2 \equiv p \mathrm{mod} q \text{ και } x^2 \equiv q \mathrm{mod} p$$

και διατυπώνεται ως εξής:

Οι εξισώσεις

$$x^2 \equiv p \mathrm{mod} q \text{ και } x^2 \equiv q \mathrm{mod} p$$

είναι ταυτόχρονα επιλύσιμες ή είναι ταυτόχρονα μη επιλύσιμες αν και μόνο αν ένας τουλάχιστον από τους πρώτους $p, q \equiv 1 \mathrm{mod} 4$.

Αλλιώς, αν και ο p και ο q αφήνουν υπόλοιπο 3 στην διαίρεση με το 4 τότε μία ακριβώς εξίσωση είναι επιλύσιμη και η άλλη δεν είναι επιλύσιμη

Πολλοί σπουδαίοι μαθηματικοί είχαν ανακαλύψει τον νόμο της τετραγωνικής αντιστροφής χωρίς να έχουν καταφέρει να δώσουν μια απόδειξη γι' αυτόν. Ο πρώτος που τον απέδειξε ήταν ο Gauss σε ηλικία μόλις 18 χρόνων.

2.5 Γενική μορφή λύσης ισοτιμίας δευτέρου βαθμού

Theorem 2.5.1. *Έστω p περιττός πρώτος και ακέραιοι a, r με $r \geq 1$ και $ΜΚΔ(a, p) = 1$, τότε η ισοτιμία $x^2 \equiv a mod p^r$ έχει λύση αν και μόνο αν η $x^2 \equiv a mod p$ έχει λύση.*

Proof. Έστω x_0 μία λύση της $x^2 \equiv a \mathrm{mod} p^r$ τότε

$$x_0^2 \equiv a \mathrm{mod} p^r \Rightarrow p^r | \left(x_0^2 - a\right)$$

και αφού $p | p^r$ θα έχουμε ότι

$$p | \left(x_0^2 - a\right) \Rightarrow x_0^2 \equiv a \mathrm{mod} p.$$

Οπότε η x_0 θα είναι λύση και της $x^2 \equiv a \mathrm{mod} p$.

Από την άλλη μεριά, θεωρούμε ότι η $x^2 \equiv a \mathrm{mod} p$ είναι επιλύσιμη και θα αποδείξουμε οτι και η $x^2 \equiv a \mathrm{mod} p^r$ έχει λύση.

Για αυτό θα χρησιμοποιήσουμε επαγωγή.

Οπότε, έστω ότι η $x^2 \equiv a \mathrm{mod} p^{r-1}$ είναι επιλύσιμη και έστω x_0 μια λύση της.

Θα προσπαθήσω να βρω μια λύση για την $x^2 \equiv a \mathrm{mod} p^r$ ως συνάρτηση του x_0.

Για αυτό θεωρώ $x = x_0 + p^{r-1} y$ με άγνωστο y.

Τότε

$$\left(x_0 + p^{r-1} y\right)^2 \equiv a \mathrm{mod} p^r.$$

Οπότε

$$x_0^2 + 2 x_0 y p^{r-1} \equiv a \mathrm{mod} p^r.$$

Τότε

$$2x_0yp^{r-1} \equiv a - x_0^2 \mathrm{mod} p^r.$$

Όμως από την υπόθεση έχουμε ότι $p^{r-1} | \left(x_0^2 - a\right)$ άρα ο αριθμός $\frac{a-x_0^2}{p^{r-1}}$ είναι ακέραιος, οπότε:

$$2x_0y \equiv \frac{a - x_0^2}{p^{r-1}} \mathrm{mod} p$$

αυτή η εξίσωση έχει λύση ως προς y, αφού $\mathrm{ΜΚΔ}(x_0, p) = 1, p > 2$.

Οπότε, κατασκευάσαμε μια λύση της $x^2 \equiv a \mathrm{mod} p^r$. □

Theorem 2.5.2. *Έστω η ισοτιμία*

$$x^2 \equiv a mod m \text{ όπου } m = m_1 m_2 \dots m_k \text{ με } ΜΚΔ(m_i, m_j) = 1, i \neq j \text{ για κάθε } i, j.$$

Η ισοτιμία είναι επιλύσιμη αν και μόνο αν καθεμία από τις ισοτιμίες

$$x^2 \equiv a mod m_i, i = 1, 2, \dots, k$$

είναι επιλύσιμη.

Proof. Αν $x^2 \equiv a \mathrm{mod} m \Rightarrow m | \left(x^2 - a\right) \Rightarrow m_1 m_2 \dots m_k | \left(x^2 - a\right) \Rightarrow m_i | \left(x^2 - a\right)$ για κάθε i, δηλαδή $x^2 \equiv a \mathrm{mod} m_i, i = 1, 2, \dots, k$.

Αντίστροφα, αν $x^2 \equiv a \mathrm{mod} m_i, i = 1, 2, \dots k$ το ζητούμενο είναι προφανές. □

2.6 Σύμβολο Jacobi

Το σύμβολο Jacobi είναι μια επέκταση του συμβόλου Legendre. Στο σύμβολο Legendre μελετούσαμε την ισοτιμία $x^2 \equiv a \mathrm{mod} p$ με p περιττό πρώτο. Με το σύμβολο Jacobi μελετάμε την ισοτιμία $x^2 \equiv a \mathrm{mod} P$ με P περιττό θετικό ακέραιο.

Definition (Σύμβολο Jacobi)**.** Έστω P περιττός φυσικός αριθμός με $P = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$ να είναι η παραγοντοποίησή του σε πρώτους παράγοντες και a ένας ακέραιος αριθμός, με $\mathrm{ΜΚΔ}(a, P) = 1$. Τότε, ορίζουμε το σύμβολο του Jacobi $\left(\frac{a}{P}\right)$ ως εξής:

$$\left(\frac{a}{1}\right) = 1$$

και

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)^{m_1} \left(\frac{a}{p_2}\right)^{m_2} \dots \left(\frac{a}{p_k}\right)^{m_k}$$

όπου $\left(\frac{a}{p_i}\right)$ το σύμβολο του Legendre

Remark. Για P περιττό πρώτο, το σύμβολο του Jacobi είναι το σύμβολο του Legendre.

Example. $\left(\frac{9}{315}\right) = \left(\frac{9}{3^2 \cdot 5 \cdot 7}\right) = \left(\frac{9}{3}\right)^2 \left(\frac{9}{5}\right) \left(\frac{9}{7}\right)$

Proposition 2.6.1. *Για το σύμβολο Jacobi ισχύουν τα επόμενα:*

1. Αν $\left(\frac{a}{P}\right) = 1$ δεν ξέρουμε αν ο a είναι τετραγωνικό υπόλοιπο του P.
2. Αν ο a είναι τετραγωνικό υπόλοιπο του P τότε $\left(\frac{a}{P}\right) = 1$.
3. Αν $\left(\frac{a}{P}\right) = -1$, τότε ο a δεν είναι τετραγωνικό υπόλοιπο του P.

Proof. Για το 1. θα χρησιμοποιήσω ένα αντιπαράδειγμα.

Για $a = 2, P = 3^2$ έχουμε ότι $\left(\frac{2}{3^2}\right) = \left(\frac{2}{3}\right)^2 = 1$, όμως για κάθε ακέραιο x ισχύει ότι $x^2 \equiv 0, 1, 4, 7 \text{mod} 9$ οπότε το 2 δεν είναι τετραγωνικό υπόλοιπο mod9 και παρ' όλα αυτά $\left(\frac{2}{9}\right) = 1$

Το 2. προκύπτει άμεσα από (2.5.2) και (2.5.1) καθώς αν το a είναι τετραγωνικό υπόλοιπο του P τότε το a είναι τετραγωνικό υπόλοιπο κάθε πρώτου p_i διαιρέτη του P οπότε

$$\left(\frac{a}{p_i}\right) = 1, i = 1, 2, \ldots, k \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)^{m_1} \left(\frac{a}{p_2}\right)^{m_2} \ldots \left(\frac{a}{p_k}\right)^{m_k} = 1.$$

Για το 3. Αν $\left(\frac{a}{P}\right) = -1$ τότε ο a δεν είναι τετραγωνικό υπόλοιπο γιατί σύμφωνα με το 2. αν ήταν θα έπρεπε $\left(\frac{a}{P}\right) = 1$. □

Theorem 2.6.2. *Έστω a ακέραιος και P, Q περιττοί φυσικοί, με $ΜΚΔ(a, PQ) = 1$. Τότε*

$$\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$$

Proof. Έστω $P = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ και $Q = q_1^{b_1} q_2^{b_2} \ldots q_m^{b_m}$ η παραγοντοποίηση των P, Q σε πρώτους παράγοντες.

Τότε, έχουμε ότι

$$\left(\frac{a}{PQ}\right) = \left(\frac{a}{p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} q_1^{b_1} q_2^{b_2} \ldots q_m^{b_m}}\right) =$$
$$\left(\frac{a}{p_1}\right)^{a_1} \left(\frac{a}{p_2}\right)^{a_2} \ldots \left(\frac{a}{p_k}\right)^{a_k} \left(\frac{a}{q_1}\right)^{b_1} \left(\frac{a}{q_2}\right)^{b_2} \ldots \left(\frac{a}{q_m}\right)^{b_m} = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$$

□

Theorem 2.6.3. *Έστω P περιττός φυσικός και a, b ακέραιοι με $ΜΚΔ(ab, P) = 1$. Τότε*

$$\left(\frac{a}{P}\right)\left(\frac{b}{P}\right) = \left(\frac{ab}{P}\right)$$

Proof. Έστω $P = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}, k \in \mathbb{N}$ η παραγοντοποίηση του P σε πρώτους παράγοντες. Τότε,

$$\left(\frac{a}{P}\right)\left(\frac{b}{P}\right) = \left(\frac{a}{p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}}\right)\left(\frac{b}{p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}}\right) =$$

$$\left(\frac{a}{p_1}\right)^{a_1}\left(\frac{a}{p_2}\right)^{a_2}\dots\left(\frac{a}{p_k}\right)^{a_k}\left(\frac{b}{p_1}\right)^{a_1}\left(\frac{b}{p_2}\right)^{a_2}\dots\left(\frac{b}{p_k}\right)^{a_k}=$$

$$\left[\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\right]^{a_1}\cdot\left[\left(\frac{a}{p_2}\right)\left(\frac{b}{p_2}\right)\right]^{a_2}\dots\left[\left(\frac{a}{p_k}\right)\left(\frac{b}{p_k}\right)\right]^{a_k}$$

όμως, σύμφωνα με το (2.3.2) $\left[\left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right)\right]^{a_i}=\left(\frac{ab}{p_i}\right)^{a_i}, i=1,2,\dots,k.$

Οπότε,

$$\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)=\left(\frac{ab}{p_1}\right)^{a_1}\left(\frac{ab}{p_2}\right)^{a_2}\dots\left(\frac{ab}{p_k}\right)^{a_k}=\left(\frac{ab}{P}\right)$$

□

Theorem 2.6.4. *Έστω a,b ακέραιοι αριθμοί, με $ΜΚΔ(a,P)=1$. Αν $a\equiv b mod P$, τότε ισχύει ότι*

$$\left(\frac{a}{P}\right)=\left(\frac{b}{P}\right)$$

Proof. Αν $P=p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}, k\in\mathbb{N}$ με p_i πρώτο για $i=1,2,\dots,k$, τότε αφού $a\equiv b \mathrm{mod} P$ θα έχουμε ότι $a\equiv b \mathrm{mod} p_i$ για $i=1,2,\dots,k.$

Όμως σύμφωνα με το (2.3.1) $\left(\frac{a}{p_i}\right)=\left(\frac{b}{p_i}\right)$ για $i=1,2,\dots,k.$

Τότε,

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)^{a_1}\left(\frac{a}{p_2}\right)^{a_2}\dots\left(\frac{a}{p_k}\right)^{a_k}=\left(\frac{b}{p_1}\right)^{a_1}\left(\frac{b}{p_2}\right)^{a_2}\dots\left(\frac{b}{p_k}\right)^{a_k}=\left(\frac{b}{P}\right)$$

□

Theorem 2.6.5. *Έστω P περιττός θετικός ακέραιος. Τότε:*

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

Theorem 2.6.6. *Έστω P περιττός θετικος ακέραιος, τότε*

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

Theorem 2.6.7 (Νόμος Τετραγωνικής Αντιστροφής για σύμβολα Jacobi). *Έστω P, Q περιττοί φυσικοί με $ΜΚΔ(P,Q) = 1$. Τότε:*

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

Proof. Αν $P = p_1 p_2 \dots p_n, n \in \mathbb{N}$ και $Q = q_1 q_2 \dots q_m, m \in \mathbb{N}$ όπου οι αριθμοί $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_m$ είναι πρώτοι όχι κατ' ανάγκη διαφορετικοί ανά δύο.

Τότε

$$\left(\frac{P}{Q}\right) = \left(\frac{P}{q_1}\right)\left(\frac{P}{q_2}\right)\cdots\left(\frac{P}{q_m}\right) = \prod_{i=1}^{m}\left(\frac{P}{q_i}\right) = \prod_{i=1}^{m}\prod_{j=1}^{n}\left(\frac{p_j}{q_i}\right)$$

με τον ίδιο τρόπο έχουμε ότι

$$\left(\frac{Q}{P}\right) = \prod_{i=1}^{m}\prod_{j=1}^{n}\left(\frac{q_i}{p_j}\right)$$

οπότε

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i=1}^{m}\prod_{j=1}^{n}\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right)$$

όμως σύμφωνα με το (2.4.4) έχουμε ότι

$$\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right) = (-1)^{\frac{p_j-1}{2}\cdot\frac{q_i-1}{2}}$$

οπότε

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\sum_{j=1}^{n}\sum_{i=1}^{m}\frac{p_j-1}{2}\cdot\frac{q_i-1}{2}} = (-1)^{\sum_{j=1}^{n}\frac{p_j-1}{2}\cdot\sum_{i=1}^{m}\frac{q_i-1}{2}} \tag{2.2}$$

όμως,

$$P = p_1 p_2 \dots p_n = \prod_{j=1}^{n}(1 + (p_j - 1)) = 1 + \sum_{j=1}^{n}(p_j - 1) + 4s, s \in \mathbb{N}$$

οπότε

$$\frac{P-1}{2} \equiv \frac{\sum_{j=1}^{n}(p_j-1)}{2} \bmod 2$$

με τον ίδιο τρόπο έχουμε ότι

$$\frac{Q-1}{2} \equiv \frac{\sum_{i=1}^{m}(q_i-1)}{2} \bmod 2$$

οπότε από την (2.2) έχουμε ότι

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

□

2.7 Αλγόριθμος για την εύρεση του συμβόλου Jacobi

Για την εύρεση του συμβόλου Jacobi χρησιμοποιούμε τον παρακάτω αλγόριθμο ο οποίος προκύπτει άμεσα από τις ιδιότητες του συμβόλου Jacobi:

```
Algorithm for Jacobi Symbol
Input: integer a, odd integer n>2
       b:=aMODn; c:=n;
       s:=1;
       WHILE b>1
           WHILE bMOD4=0
               b:=bDIV4;
           IF bMOD2=0
               IF cMOD8=3 OR cMOD8=5
                   s:=-s;
               b:=bDIV2;
           IF b=1 break;
           IF bMOD4=cMOD4=3
               s:=-s;
           temp:=b;
           b:=cMODb;
           c:=temp;
RETURN s*b;
```

Example 2.7.1. Θα υπολογίσουμε το σύμβολο Jacobi $\left(\frac{1521}{587}\right)$.

Από τον αλγόριθμο προκύπτει ο παρακάτω πίνακας

b	c	s
347	587	1
347	587	-1
240	347	-1
60	347	-1
15	347	-1
15	347	1
2	15	1
1	15	1

και το σύμβολο Jacobi προκύπτει $\left(\frac{1521}{587}\right) = 1$.

Επειδή ο 587 είναι πρώτος και $\left(\frac{1521}{587}\right) = 1$ προκύπτει ότι το 1521 είναι τετραγωνικό υπόλοιπο του 587.

3 Τετραγωνικές ρίζες

3.1 Τετραγωνικές ρίζες $\mathbf{mod}p$ με $p \equiv 3\mathbf{mod}4$

Definition 3.1.1. Έστω ο ακέραιος a με $1 \leq a < n$. Ο a ονομάζεται τετραγωνική ρίζα της μονάδας $\mathrm{mod}n$ αν $a^2 \equiv 1\mathrm{mod}n$.

Remark. Από τον ορισμό προκύπτε άμεσα ότι οι αριθμοί 1 και $n-1$ είναι τετραγωνικές ρίζες της μονάδας $\mathrm{mod}n$. Αυτές ειναι οι τετριμμένες ρίζες της μονάδας. Αν ο n είναι πρώτος δεν υπάρχουν άλλες ρίζες της μονάδας $\mathrm{mod}n$.

Οπότε, για να βρούμε μη τετριμμένες ρίζες της μονάδας $\mathrm{mod}n$ θα πρέπει ο n να είναι σύνθετος.

Από το Κινέζικο θεώρημα υπολοίπων προκύπτει ότι αν $n = p_1 p_2 \dots p_k$ για διακεκριμένους περιττούς πρώτους αριθμούς $p_1, p_2, \dots, p_k$, τότε υπάρχουν ακριβώς 2^k ρίζες της μονάδας $\mathrm{mod}n$.

Proposition 3.1.2. *Έστω ο πρώτος $p \equiv 3mod4$, ο ακέραιος $y \neq 0modp$ και $x = y^{\frac{p+1}{4}} modp$.*

1. Αν ο y είναι τετραγωνικό υπόλοιπο $\mathrm{mod}p$ τότε οι τετραγωνικές ρίζες του είναι $\pm x$.
2. Αν ο y δεν είναι τετραγωνικό υπόλοιπο $\mathrm{mod}p$ τότε ο $-y$ είναι και οι τετραγωνικές του ρίζες είναι $\pm x$.

Proof. Από το θεώρημα του Fermat έχουμε ότι $y^{p-1} \equiv 1\mathrm{mod}p$.

Τότε,

$$x^4 = y^{p+1} = y^2 \cdot y^{p-1} \equiv y^2 \mathrm{mod}p$$

οπότε,

$$\left(x^2 + y\right)\left(x^2 - y\right) \equiv 0\mathrm{mod}p \Rightarrow x^2 \equiv \pm y\mathrm{mod}p$$

άρα ένα τουλάχιστον από τα y και $-y$ είναι τετραγωνικό υπόλοιπο $\mathrm{mod}p$.

Έστω ότι και το y και το $-y$ είναι τετραγωνικά υπόλοιπα $\mathrm{mod}p$.

Τότε,

$$y = a^2 \mathrm{mod}p, -y = b^2 \mathrm{mod}p \text{ για κάποιους ακέραιους } a, b$$

τότε

$$-1 \equiv \left(ab^{-1}\right)^2 \mathrm{mod}p$$

άρα το -1 είναι τετραγωνικό υπόλοιπο $\mathrm{mod}p$.

Αυτό όμως είναι άτοπο σύμφωνα με το (2.3.3).

Άρα ακριβώς ένα από τα y και $-y$ είναι τετραγωνικό υπόλοιπο $\mathrm{mod}p$ και οι τετραγωνικές του ρίζες είναι $\pm x$. □

Example 3.1.3. Να βρεθούν οι τετραγωνικές ρίζες του 11mod19.

$19 = 4 \cdot 4 + 3$ και ο 19 είναι πρώτος αριθμός, οπότε σύμφωνα με την προηγούμενη πρόταση αν ο αριθμός 11 έχει τετραγωνικές ρίζες mod19 τοτε θα είναι οι $\pm x$ με

$$x = 11^{\frac{19+1}{4}} = 11^5 \text{mod} 19 = 7 \text{mod} 19$$

τότε $7^2 = 49 \equiv 11 \text{mod} 19$.

Άρα, οι τετραγωνικές ρίζες του 11mod19 είναι οι $\pm 7 \text{mod} 19$.

Example 3.1.4. Να βρεθούν οι τετραγωνικές ρίζες του 49mod95.

Για τον 95 έχουμε ότι $95 = 5 \cdot 19$, οπότε αν για τον ακέραιο x ισχύει ότι $x^2 \equiv 49 \text{mod} 95$ τότε θα ισχύει ότι

$$x^2 \equiv 49 \text{mod} 5 \text{ και } x^2 \equiv 49 \text{mod} 19 \Leftrightarrow$$
$$x^2 \equiv 4 \text{mod} 5 \text{ και } x^2 \equiv 11 \text{mod} 19$$

οπότε αρκεί να λύσω το τελευταίο σύστημα και να βρώ τις κοινές λύσεις των δύο εξισώσεων.

Οπότε, $x^2 \equiv 4 \text{mod} 5 \Leftrightarrow x \equiv \pm 2 \text{mod} 5$ και $x^2 \equiv 11 \text{mod} 19 \Leftrightarrow x \equiv \pm 7 \text{mod} 19$ όπως είδαμε από το προηγούμενο παράδειγμα. Οπότε, θα έχουμε τέσσερις δυνατότητες:

- $x \equiv 2 \text{mod} 5 \Rightarrow x \in \{2, \langle 7 \rangle, 12, 17, 22, 27, 32, 37, 42, 47, 52, 57, 62, 67, 72, 77, 82, 87, 92\}$
  $x \equiv 7 \text{mod} 19 \Rightarrow x \in \{\langle 7 \rangle, 26, 45, 64, 83\}$
  οπότε το μόνο κοινο στοιχείο των δύο λιστών είναι το 7 οπότε από τον συνδυασμό $x \equiv 2 \text{mod} 5$ και $x \equiv 7 \text{mod} 19$ θα έχουμε την λύση $x \equiv 7 \text{mod} 95$

- $x \equiv 2 \text{mod} 5 \Rightarrow x \in \{2, 7, \langle 12 \rangle, 17, 22, 27, 32, 37, 42, 47, 52, 57, 62, 67, 72, 77, 82, 87, 92\}$
  $x \equiv -7 \text{mod} 19 \Rightarrow x \in \{\langle 12 \rangle, 31, 50, 69, 88\}$
  οπότε το μόνο κοινο στοιχείο των δύο λιστών είναι το 12 οπότε από τον συνδυασμό $x \equiv 2 \text{mod} 5$ και $x \equiv -7 \text{mod} 19$ θα έχουμε την λύση $x \equiv 12 \text{mod} 95$

- $x \equiv -2 \text{mod} 5 \Rightarrow x \in \{3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58, 63, 68, 73, 78, \langle 83 \rangle, 88, 93\}$
  $x \equiv 7 \text{mod} 19 \Rightarrow x \in \{7, 26, 45, 64, \langle 83 \rangle\}$
  οπότε το μόνο κοινο στοιχείο των δύο λιστών είναι το 83 οπότε από τον συνδυασμό $x \equiv -2 \text{mod} 5$ και $x \equiv 7 \text{mod} 19$ θα έχουμε την λύση $x \equiv 83 \text{mod} 95$

- $x \equiv -2 \text{mod} 5 \Rightarrow x \in \{3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58, 63, 68, 73, 78, 83, \langle 88 \rangle, 93\}$
  $x \equiv -7 \text{mod} 19 \Rightarrow x \in \{12, 31, 50, 69, \langle 88 \rangle\}$
  οπότε το μόνο κοινο στοιχείο των δύο λιστών είναι το 88 οπότε από τον συνδυασμό $x \equiv -2 \text{mod} 5$ και $x \equiv -7 \text{mod} 19$ θα έχουμε την λύση $x \equiv 88 \text{mod} 95$

Οπότε, οι λύσεις της εξίσωσης $x^2 \equiv 49 \text{mod} 95$ είναι οι $x \equiv 7, 12, 83, 88 \text{mod} 95$ ή ισοδύναμα οι $x \equiv \pm 7, \pm 12 \text{mod} 95$.

3.2 Τετραγωνικές ρίζες mod$p$ με $p \equiv 1 \mathrm{mod} 4$

Lemma 3.2.1. *Έστω ότι το a είναι τετραγωνικό υπόλοιπο $mod p$ με p πρώτο και $p \equiv 1 mod 4$, τότε $a^{\frac{p-1}{4}} \equiv \pm 1 mod p$*

Proof. Αφού το a είναι τετραγωνικό υπόλοιπο mod$p$, τότε $a^{\frac{p-1}{2}} \equiv 1 \mathrm{mod} p$ σύμφωνα με το κριτήριο του Euler.

Επίσης, από την υπόθεση έχουμε ότι $p \equiv 1 \mathrm{mod} 4$, οπότε ο αριθμός $\frac{p-1}{4}$ είναι ακέραιος.

Τότε,

$$a^{\frac{p-1}{2}} \equiv 1 \mathrm{mod} p \Rightarrow p | \left(a^{\frac{p-1}{2}} - 1\right) \Rightarrow p | \left(a^{\frac{p-1}{4}} - 1\right)\left(a^{\frac{p-1}{4}} + 1\right)$$

οπότε,

$$p | (a^{\frac{p-1}{4}} - 1) \text{ ή } p | (a^{\frac{p-1}{4}} + 1).$$

Άρα,

$$a^{\frac{p-1}{4}} \equiv \pm 1 \mathrm{mod} p.$$

□

Για τους πρώτους p με $p \equiv 1 \mathrm{mod} 4$ θα διακρίνουμε τις δύο κατηγορίες.

- $p \equiv 5 \mathrm{mod} 8$
- $p \equiv 1 \mathrm{mod} 8$

Πρώτα θα ασχοληθούμε με τους πρώτους $p \equiv 5 \mathrm{mod} 8$.

Theorem 3.2.2. *Έστω a τετραγωνικό υπόλοιπο $mod p$ με $a^{\frac{p-1}{4}} \equiv 1 mod p$ με πρώτο $p \equiv 5 mod 8$ τότε οι τετραγωνικές ρίζες του a $mod p$ είναι οι $\pm x$ με $x = a^{\frac{p+3}{8}} mod p$.*

Proof. Για $x = a^{\frac{p+3}{8}} \mathrm{mod} p$ έχουμε ότι $x^2 = a^{\frac{p+3}{4}} \mathrm{mod} p = a^{\frac{p-1}{4}} \cdot a = a \mathrm{mod} p$ και σύμφωνα με το (2.1.1) οι τετραγωνικές ρίζες του a είναι οι $\pm x$. □

Theorem 3.2.3. *Έστω a τετραγωνικό υπόλοιπο $mod p$ με $a^{\frac{p-1}{4}} \equiv -1 mod p$ με πρώτο $p \equiv 5 mod 8$ τότε οι τετραγωνικές ρίζες του a $mod p$ είναι οι $\pm x$ με $x = 2a \cdot (4a)^{\frac{p-5}{8}} mod p$.*

Proof. Από την εκφώνηση έχω ότι $p \equiv 5 \mathrm{mod} 8$ τότε σύμφωνα με το (2.4.2) έχουμε ότι $2^{\frac{p-1}{2}} \equiv -1 \mathrm{mod} p$, τότε για $x = 2a \cdot (4a)^{\frac{p-5}{8}} \mathrm{mod} p$ έχουμε ότι

$$x^2 = 4a^2 \cdot (4a)^{\frac{p-5}{4}} = 4^{\frac{p-1}{4}} \cdot a^{\frac{p+3}{4}} \mathrm{mod} p = 2^{\frac{p-1}{2}} \cdot a^{\frac{p-1}{4}} \cdot a \mathrm{mod} p = (-1)(-1)\, a = a \mathrm{mod} p.$$

Οπότε, οι τετραγωνικές ρίζες του a mod$p$ είναι οι $\pm x$. □

Με τα παραπάνω θεωρήματα έχουμε τελειώσει με τους πρώτους $p \equiv 5 \mathrm{mod} 8$

Για τους πρώτους $p \equiv 1 \mathrm{mod} 8$ θα χρησιμοποιήσουμε τον αλγόριθμο των Tonelli και Shanks.

Θα παραλείψω την απόδειξη του αλγορίθμου λόγω της δυσκολίας της. Ο ενδιαφερόμενος ας δει το [2].

Ο αλγόριθμος των Tonelli και Shanks είτε επιστρέφει μια τετραγωνική ρίζα του $a \mathrm{mod} p$, αν ο a είναι τετραγωνικό υπόλοιπο $\mathrm{mod} p$ ή αποφαίνεται ότι ο a δεν είναι τετραγωνικό υπόλοιπο $\mathrm{mod} p$.

Ο αλγόριθμος είναι πιθανοτικός αλγόριθμος καθώς επιλέγει στην τύχη έναν ακέραιο n με $\left(\frac{n}{p}\right) = -1$.

Επειδή υπάρχουν $\frac{p-1}{2p}$ ακέραιοι που δεν είναι τετραγωνικά υπόλοιπα $\mathrm{mod} p$ η πιθανότητα να μην έχουμε βρει έναν n μετά από πολλές επαναλήψεις είναι πολύ μικρή.

```
Tonelli and Shanks algorithm
Input:odd prime p ≡ 1mod8, integer a
      Compute integer e and odd q such that p − 1 = 2^e q
      Choose numbers n randomly until (n/p) = −1
      z := n^q MOD p
      y := z;
      r := e;
      x := a^((q−1)/2) MOD p;
      b := a x^2 MOD p;
      x := a x MOD p;
      WHILE b ≠ 1MOD p
          find the smallest m ≥ 1 such that b^(2^m) ≡ 1MOD p
          IF m = r
              a is not quadratic residue. Terminate
          t := y^(2^(r−m−1)) MOD p;
          y := t^2 MOD p;
          r := m MOD p;
          x := xt MOD p;
          b := by MOD p;
     RETURN x;
```

Example 3.2.4. Θα χρησιμοποιήσω τον αλγόριθμο των Tonelli και Shanks για τον πρώτο αριθμό 449 και τους ακέραιους $35, 223$

Τότε, για το ζευγάρι $(35, 449)$ θα έχουμε τον εξής πίνακα που προκύπτει από τον αλγόριθμο

x	b	y	r	m
67	372	391	6	0
67	372	391	6	4
439	67	349	4	0
439	67	349	4	2
127	448	67	2	0
127	448	67	2	1
427	1	448	1	0

απ' όπου προκύπτει ότι ο $x = 427$ είναι τετραγωνική ρίζα του 35 mod449.
Ενώ για το ζευγάρι $(223, 449)$ προκύπτει ο πίνακας

x	b	y	r	m
426	246	391	6	0
426	246	391	6	6

απ' όπου προκύπτει ότι ο 223 δεν είναι τετραγωνικό υπόλοιπο mod449 καθώς $m = r = 6$

3.3 Ο αλγόριθμος του Cornacchia

Theorem 3.3.1. *Ο περιττός πρώτος p είναι άθροισμα δύο τετραγώνων ακεραίων αριθμών αν και μόνο αν $p \equiv 1 mod 4$*

Remark. Το θεώρημα είναι ισοδύναμο με το να λέγαμε ότι ο περιττός πρώτος p είναι άθροισμα δύο τετραγώνων ακεραίων αριθμών αν και μόνο αν το -1 είναι τετραγωνικό υπόλοιπο mod$p$.

Από το παραπάνω θεώρημα είναι φυσικό να ζητάμε να υπολογίσουμε ακεραίους αριθμούς x, y τέτοιους ώστε $x^2 + y^2 = p$ και γενικότερα $x^2 + dy^2 = p$, όπου d ένας θετικός ακέραιος και p ένας περιττός πρώτος.

Proposition 3.3.2. *Αν η εξίσωση $x^2 + dy^2 = p$ έχει λύση, τότε το $-d$ είναι τετραγωνικό υπόλοιπο mod$p$.*

Proof. Έστω $x, y \in \mathbb{N}$ με $x^2 + dy^2 = p$ τότε προφανώς $y \neq 0 \text{mod} p$,
τότε

$$x^2 + dy^2 \equiv 0 \text{mod} p \Rightarrow \left(x^2 + dy^2\right)\left(y^{-1}\right)^2 \equiv 0 \text{mod} p \Rightarrow \left(xy^{-1}\right)^2 \equiv -d \text{mod} p.$$

Άρα το $-d$ είναι τετραγωνικό υπόλοιπο mod$p$. □

Τώρα θεωρούμε ότι η συνθήκη το $-d$ είναι τετραγωνικό υπόλοιπο mod$p$ ικανοποιείται.
Τότε θα υπολογίσουμε μια λύση της διοφαντικής εξίσωσης με τον αλγόριθμο του Cornacchia.
Ο αλγόριθμος κάνει τα εξής βήματα:
1. Βρίσκει x_0 με $\frac{p}{2} < x_0 < p$ τέτοιο ώστε $x_0^2 \equiv -d \text{mod} p$
2. Εφαρμόζει τον Ευκλείδιο αλγόριθμο στο ζεύγος $(a, b) = (p, x_0)$ μέχρι να έχουμε $b < \sqrt{p}$
3. Για $c = \frac{p-b^2}{d}$. Αν υπάρχει ακέραιος m με $c = m^2$ τότε η εξίσωση $x^2 + dy^2 = p$ έχει λύση $(x, y) = (b, m)$. Αλλιώς η εξίσωση δεν έχει λύση.

Ο αλγόριθμος του Cornacchia επιστρέφει μία λύση της διοφαντικής εξίσωσης αν έχει ή λέει ότι η διοφαντική εξίσωση δεν έχει λύση.

Ο αλγόριθμος σε μορφή ψευδοκώδικα:

```
CORNACCHIA ALGORITHM
Input:odd prime p,integer d with 0 < d < p
    IF −d is not quadratic residue mod p
       THEN the equation has no solutions.
    ELSE
       Find x_0 such that x_0^2 ≡ −d mod p
       Change x_0 into ±x_0 + np, n ∈ ℕ so that p/2 < x_0 < p
       a := p;
       b := x_0;
       sq:=⌊√p⌋;
       WHILE b > sq
          temp := aMODb;
          a := b;
          b := temp;
       IF  c := (p−b^2)/d is not the square of an integer
          THEN the equation has no solution.
       ELSE a solution is (x,y)=(b, √c)
```

Example 3.3.3. Για παράδειγμα αν θέλουμε να βρούμε τις λύσεις της διοφαντικής εξίσωσης $x^2 + 18y^2 = 283$ τότε χρησιμοποιώντας το κριτήριο του Euler μ έχουμε$\left(\frac{-18}{283}\right) = 1$.

Χρησιμοποιώντας τον αλγόριθμο Tonelli και Shanks παίρνουμε $x_0 = 185$ έχουμε $a = 283, b = 185, sq = 16$

Με τον Ευκλείδιο αλγόριθμο έχουμε ότι

$a = 98, b = 87$ και μετά $a = 87, b = 11$.

Τέλος, ο αριθμός $c = \frac{283-11^2}{18} = 9 = 3^2$ είναι τέλειο τετραγώνο, οπότε ο αλγόριθμος επιστρέφει το ζεύγος $(b, \sqrt{c}) = (11, 3)$ που αποτελεί την λύση της εξίσωσης.

4 Συνεχή Κλάσματα

4.1 Εισαγωγή στα Συνεχή Κλάσματα

Definition. Πεπερασμένο συνεχές κλάσμα θα καλείται μια έκφραση της μορφής

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots \\ + \quad \frac{1}{a_n}}}$$

την οποία θα γράφουμε ως εξής:

$$[a_0; a_1, a_2, \ldots, a_n]$$

Definition. Άπειρο συνεχές κλάσμα θα καλείται μια έκφραση της μορφής

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}}$$

την οποία θα γράφουμε ως εξής:

$$[a_0; a_1, a_2, \ldots]$$

Remark. Οι όροι $a_0, a_1, a_2, \ldots$ είναι ανεξάρτητες μεταβλητές σε κάποιο σύνολο. Στην εργασία μου, έχω ως στόχο να παρουσιάσω τα συνεχή κλάσματα ως αναπαραστάτες των πραγματικών αριθμών. Για αυτόν τον λόγο θα θεωρώ πάντα ότι τα $a_1, a_2, \ldots$ είναι θετικοί ακέραιοι και ο a_0 ακέραιος. Θα λέμε τις μεταβλητές $a_0, a_1, a_2, \ldots$ στοιχεία του συνεχούς κλάσματος.

Definition. Ένα πεπερασμένο συνεχές κλάσμα με $n+1$ στοιχεία, δηλαδή ένα συνεχές κλάσμα της μορφής

$$[a_0; a_1, a_2, \ldots, a_n]$$

θα λέμε ότι έχει τάξη n.

Επίσης, θα λέμε ότι κάθε άπειρο συνεχές κλάσμα έχει άπειρη τάξη.

Definition. Θα λέμε το συνεχές κλάσμα

$$s_k = [a_0; a_1, a_2, \ldots, a_k] \text{ με } 0 \leq k \leq n$$

τμήμα του πεπερασμένου συνεχούς κλάσματος

$$[a_0; a_1, a_2, \ldots, a_n].$$

Αντίστοιχα, θα λέμε το συνεχές κλάσμα

$$s_k = [a_0; a_1, a_2, \ldots, a_k] \text{ με } k \geq 0$$

τμήμα του άπειρου συνεχούς κλάσματος

$$[a_0; a_1, a_2, \ldots].$$

Definition. Θα λέμε το συνεχές κλάσμα

$$r_k = [a_k; a_{k+1}, \ldots, a_n], 0 \leq k \leq n$$

υπόλοιπο του συνεχούς κλάσματος

$$[a_0; a_1, a_2, \ldots, a_n]$$

και όμοια θα λέμε το συνεχές κλάσμα

$$r_k = [a_k; a_{k+1}, \ldots], k \geq 0$$

υπόλοιπο του συνεχούς κλάσματος

$$[a_0; a_1, a_2, \ldots].$$

Remark. Έστω ένα πεπερασμένο συνεχές κλάσμα τάξης n με $a_n = 1$ δηλαδή ένα κλάσμα της μορφής $[a_0; a_1, \ldots, a_{n-1}, 1]$. Τότε αυτό είναι ίσο με το συνεχές κλάσμα τάξης $n-1$ το $[a_0; a_1, \ldots, a_{n-1} + 1]$. Θα συμφωνούμε να γράφουμε κάθε κλάσμα της πρώτης μορφής με την δεύτερη για να έχουμε πάντα συνεχή κλάσματα που να έχουν τελευταίο στοιχείο μεγαλύτερο της μονάδας.

4.2 Συγκλίνοντες

Τα συνεχή κλάσματα ορίζονται αναδρομικά ως εξής:

$$[a_0] = a_0 \text{ και } [a_0; a_1, a_2, \ldots, a_n] = a_0 + \frac{1}{[a_1; a_2, \ldots, a_n]}.$$

Οπότε:

$$\begin{aligned}[a_0;a_1] =& a_0+\frac{1}{a_1}=\frac{a_0a_1+1}{a_1}\\ [a_0;a_1,a_2] =& a_0+\frac{1}{\frac{a_1a_2+1}{a_2}}=\frac{a_0a_1a_2+a_0+a_2}{a_1a_2+1}\end{aligned}$$

Definition. Ορίζουμε τα πολυώνυμα $Q_n(x_1,x_2,\ldots,x_n)$, $n\in\mathbb{N}$ ως εξής:

$$Q_n\left(x_1,x_2,\ldots,x_n\right)=\begin{cases}1 & \text{αν } n=0\\ x_1 & \text{αν } n=1\\ x_1Q_{n-1}\left(x_2,\ldots,x_n\right)+Q_{n-2}\left(x_3,\ldots,x_n\right) & \text{αν } n>1\end{cases}$$

Από τον ορισμό έχουμε ότι:

$$\begin{aligned}Q_1\left(x_1\right) =& x_1\\ Q_2\left(x_1,x_2\right) =& x_1x_2+1\\ Q_3\left(x_1,x_2,x_3\right) =& x_1x_2x_3+x_1+x_3\end{aligned}$$

Παρατηρούμε ότι

$$[a_0]=\frac{Q_1(a_0)}{Q_0},\ \ [a_0;a_1]=\frac{Q_2\left(a_0,a_1\right)}{Q_1\left(a_1\right)}\ \text{και}\ \ [a_0;a_1,a_2]=\frac{Q_3\left(a_0,a_1,a_2\right)}{Q_2\left(a_1,a_2\right)}$$

Τα παραπάνω αποτελέσματα δεν είναι τυχαία, αλλά ισχύει το επόμενο θεώρημα.

Theorem 4.2.1. *Έστω το συνεχές κλάσμα* $[a_0;a_1,\ldots,a_n],n\in\mathbb{N}$ *τότε:*

$$[a_0;a_1,\ldots,a_n]=\frac{Q_{n+1}\left(a_0,a_1,\ldots,a_n\right)}{Q_n\left(a_1,a_2,\ldots,a_n\right)}$$

Proof. Θα χρησιμοποιήσω επαγωγή ως προς n.

Για $n=0$ ισχύει.

Έστω ότι το θεώρημα ισχύει για το n, τότε:

$$\begin{aligned}[a_0;a_1,\ldots,a_{n+1}] &= a_0+\frac{1}{[a_1;a_2,\ldots,a_{n+1}]}=\\ a_0+\frac{Q_n\left(a_2,a_3,\ldots,a_{n+1}\right)}{Q_{n+1}\left(a_1,a_2,\ldots,a_{n+1}\right)}= &\quad \frac{a_0Q_{n+1}\left(a_1,a_2,\ldots,a_{n+1}\right)+Q_n\left(a_2,a_3,\ldots,a_{n+1}\right)}{Q_{n+1}\left(a_1,a_2,\ldots,a_{n+1}\right)}=\\ &\quad \frac{Q_{n+2}\left(a_0,a_1,\ldots,a_{n+1}\right)}{Q_{n+1}\left(a_1,a_2,\ldots,a_{n+1}\right)}\end{aligned}$$

και η απόδειξη έχει ολοκληρωθεί. □

Theorem 4.2.2. *Έστω το συνεχές κλάσμα* $[a_0; a_1, \ldots, a_n], n \in \mathbb{N}$ *τότε υπάρχουν ακέραιοι αριθμοί* p_n, q_n *τέτοιοι ώστε*

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

Ο αριθμός $\frac{p_n}{q_n}$ *ονομάζεται κανονική έκφραση του συνεχούς κλάσματος.*

Proof. Σύμφωνα με το προηγούμενο θεώρημα έχουμε ότι

$$[a_0; a_1, \ldots, a_n] = \frac{Q_{n+1}(a_0, a_1, \ldots, a_n)}{Q_n(a_1, a_2, \ldots, a_n)}$$

.

Θέτοντας $p_n = Q_{n+1}(a_0, a_1, \ldots, a_n)$ και $q_n = Q_n(a_1, a_2, \ldots, a_n)$ προκύπτει άμεσα. □

Remark. Ορίζουμε επίσης ως $p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$.

Definition 4.2.3. Έστω το συνεχές κλάσμα $a = [a_0; a_1, \ldots]$ και $[a_0; a_1, \ldots, a_k], k \geq 0$ ένα τμήμα του, τότε η κανονική έκφραση $\frac{p_k}{q_k}$ του $[a_0; a_1, \ldots, a_k]$ ονομάζεται συγκλίνοντας k τάξης του a.

Με τον ίδιο τρόπο ορίζονται και οι συγκλίνοντες ενός πεπερασμένου συνεχούς κλάσματος.

Theorem 4.2.4. *Για ακέραιο* $k \geq 2$ *ισχύει ότι:*

$$\begin{aligned} p_k &= a_k p_{k-1} + p_{k-2} \\ q_k &= a_k q_{k-1} + q_{k-2} \end{aligned}$$

με $p_1 = a_0 a_1 + 1,\ q_1 = a_1,\ p_0 = a_0,\ q_0 = 1.$

Proof. Για $k = 2$ έχουμε ότι

$$[a_0; a_1, a_2] = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1} = \frac{p_2}{q_2}$$

οπότε έχουμε ότι:

$$p_2 = a_2(a_0 a_1 + 1) + a_0 = a_2 p_1 + p_0 \text{ και } q_2 = a_1 a_2 + 1 = a_2 q_1 + q_0$$

Άρα για $k = 2$ η υπόθεση ισχύει.
Έστω ότι η υπόθεση ισχύει για κάθε $k < n$.
Από τον ορισμό τους έχουμε ότι:

$$p_n = Q_{n+1}(a_0, a_1, \ldots, a_n) = a_0 Q_n(a_1, \ldots, a_n) + Q_{n-1}(a_2, \ldots, a_n) = a_0 p'_{n-1} + q'_{n-1}$$

και

$$q_n = Q_n(a_1, a_2, \ldots, a_n) = p'_{n-1}$$

όπου

$$\frac{p'_{n-1}}{q'_{n-1}} = [a_1; a_2, \ldots, a_n].$$

Επειδή για $n-1$ η υπόθεση ισχύει, έχουμε ότι:

$$\begin{aligned} p'_{n-1} =& a_n p'_{n-2} + p'_{n-3} \\ q'_{n-1} =& a_n q'_{n-2} + q'_{n-3} \end{aligned}$$

με

$$\frac{p'_{n-2}}{q'_{n-2}} = [a_1; a_2, \ldots, a_{n-1}] \text{ και } \frac{p'_{n-3}}{q'_{n-3}} = [a_1; a_2, \ldots, a_{n-2}].$$

Τότε,

$$\begin{aligned} p_n &= a_0 \left(a_n p'_{n-2} + p'_{n-3}\right) + \left(a_n q'_{n-2} + q'_{n-3}\right) \\ &= a_n \left(a_0 p'_{n-2} + q'_{n-2}\right) + \left(a_0 p'_{n-3} + q'_{n-3}\right) \\ &= a_n p_{n-1} + p_{n-2}, \\ q_n = p'_{n-1} = a_n p'_{n-2} + p'_{n-3} &= a_n q_{n-1} + q_{n-2} \end{aligned}$$

και η απόδειξη έχει ολοκληρωθεί. □

Theorem 4.2.5. *Για κάθε φυσικό k ισχύει ότι:*

$$q_k p_{k-1} - p_k q_{k-1} = (-1)^k$$

Proof. Από την προηγούμενη πρόταση έχουμε ότι:

$$\begin{aligned} p_k =& a_k p_{k-1} + p_{k-2} \\ q_k =& a_k q_{k-1} + q_{k-2} \end{aligned}$$

οπότε

$$\begin{aligned} p_k q_{k-1} =& a_k p_{k-1} q_{k-1} + p_{k-2} q_{k-1} \\ q_k p_{k-1} =& a_k q_{k-1} p_{k-1} + q_{k-2} p_{k-1} \end{aligned}$$

τότε

$$q_k p_{k-1} - p_k q_{k-1} = -\left(q_{k-1} p_{k-2} - p_{k-1} q_{k-2}\right)$$

οπότε

$$q_k p_{k-1} - p_k q_{k-1} = (-1)^k \left(q_0 p_{-1} - p_0 q_{-1}\right) = (-1)^k$$

□

Corollary 4.2.6. *Για θετικό ακέραιο k ισχύει ότι:*

$$\frac{p_{k-1}}{q_{k-1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k q_{k-1}}$$

Proposition 4.2.7. *Οι συγκλίνοντες $\frac{p_n}{q_n}$ είναι ανάγωγα κλάσματα.*

Proof. Έστω $d = \text{ΜΚΔ}(p_n, q_n)$ τότε

$$d|\left(q_n p_{n-1} - p_n q_{n-1}\right) \Rightarrow d|\left(-1\right)^n \Rightarrow d = 1.$$

άρα το $\frac{p_n}{q_n}$ είναι ανάγωγο. □

Theorem 4.2.8. *Για θετικό ακέραιο k ισχύει ότι:*

$$q_k p_{k-2} - p_k q_{k-2} = (-1)^{k-1} a_k$$

Proof. Σύμφωνα με το (4.2.4) έχουμε ότι

$$\begin{aligned} p_k &= a_k p_{k-1} + p_{k-2} \\ q_k &= a_k q_{k-1} + q_{k-2} \end{aligned}$$

οπότε

$$\begin{aligned} p_k q_{k-2} &= a_k p_{k-1} q_{k-2} + p_{k-2} q_{k-2} \\ q_k p_{k-2} &= a_k q_{k-1} p_{k-2} + q_{k-2} p_{k-2} \end{aligned}$$

οπότε

$$q_k p_{k-2} - p_k q_{k-2} = a_k \left(q_{k-1} p_{k-2} - p_{k-1} q_{k-2}\right)$$

οπότε σύμφωνα με το (4.2.5) θα έχουμε ότι

$$q_k p_{k-2} - p_k q_{k-2} = (-1)^{k-1} a_k$$

□

Corollary 4.2.9. *Για ακέραιο $k \geq 2$ ισχύει ότι:*

$$\frac{p_{k-2}}{q_{k-2}} - \frac{p_k}{q_k} = \frac{(-1)^{k-1} a_k}{q_k q_{k-2}}$$

Theorem 4.2.10. *Οι συγκλίνοντες άρτιας τάξης σχηματίζουν μια αύξουσα ακολουθία ενώ οι συγκλίνοντες περιττής τάξης σχηματίζουν μια φθίνουσα ακολουθία. Επίσης, κάθε άρτιας τάξης συγκλίνοντας είναι μικρότερος από κάθε συγκλίνοντα περιττής τάξης.*

Proof. Σύμφωνα με το (4.2.9) ισχύει ότι

$$\frac{p_{k-2}}{q_{k-2}} - \frac{p_k}{q_k} = \frac{(-1)^{k-1} a_k}{q_k q_{k-2}}$$

οπότε για τους συγκλίνοντες άρτιας τάξης θα έχουμε ότι για $k = 2n, n \in \mathbb{N}$

$$\frac{p_{2n-2}}{q_{2n-2}} - \frac{p_{2n}}{q_{2n}} = \frac{(-1)^{2n-1} a_{2n}}{q_{2n} q_{2n-2}} = -\frac{a_{2n}}{q_{2n} q_{2n-2}} < 0$$

άρα $\frac{p_{2n-2}}{q_{2n-2}} < \frac{p_{2n}}{q_{2n}}$ και άρα οι συγκλίνοντες άρτιας τάξης σχηματίζουν μια αύξουσα ακολουθία.

Για τους συγκλίνοντες περιττής τάξης θα έχουμε ότι $k = 2n+1, n \in N$ και

$$\frac{p_{2n-1}}{q_{2n-1}} - \frac{p_{2n+1}}{q_{2n+1}} = \frac{(-1)^{2n} a_{2n+1}}{q_{2n+1} q_{2n-1}} = \frac{a_{2n+1}}{q_{2n+1} q_{2n-1}} > 0$$

και άρα $\frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}}$ και άρα οι συγκλίνοντες περιττής τάξης σχηματίζουν φθίνουσα ακολουθία.

Για να δείξουμε ότι κάθε άρτιας τάξης συγκλίνοντας είναι μικρότερος από κάθε συγκλίνοντα περιττής τάξης θα χρησιμοποιήσουμε το (4.2.6).

Οπότε για κάθε $k \geq 1$ ισχύει ότι:

$$\frac{p_{k-1}}{q_{k-1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k q_{k-1}}$$

για k άρτιο έχουμε ότι $\frac{p_{k-1}}{q_{k-1}} > \frac{p_k}{q_k}$ οπότε κάθε περιττής τάξης συγκλίνοντας είναι μεγαλύτερος από τον επόμενο συγκλίνοντα (άρτιας τάξης).

Επειδή ξέρουμε ότι οι συγκλίνοντες άρτιας τάξης σχηματίζουν μια αύξουσα ακολουθία ενώ οι συγκλίνοντες περιττής τάξης σχηματίζουν μια φθίνουσα ακολουθία θα έχουμε ότι για κάθε $n \in \mathbb{N}$ ισχύει ότι

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_{2n}}{q_{2n}} < \frac{p_{2n-1}}{q_{2n-1}} < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

και το θεώρημα έχει αποδειχτεί. □

Theorem 4.2.11. *Για κάθε ακέραιο k με $1 \leq k \leq n$ ισχύει ότι*

$$[a_0; a_1, \ldots, a_n] = \frac{p_{k-1} r_k + p_{k-2}}{q_{k-1} r_k + q_{k-2}}$$

Proof. Ξέρουμε ότι

$$[a_0; a_1, \dots, a_n] = [a_0; a_1, \dots, a_{k-1}, r_k]$$

τότε

$$[a_0; a_1, \dots, a_{k-1}, r_k] = \frac{p'_k}{q'_k}$$

που σύμφωνα με το (4.2.4) θα έχουμε ότι

$$\begin{aligned} p'_k &= r_k p_{k-1} + p_{k-2} \\ q'_k &= r_k q_{k-1} + q_{k-2} \end{aligned}$$

οπότε

$$[a_0; a_1, \dots, a_n] = \frac{p_{k-1} r_k + p_{k-2}}{q_{k-1} r_k + q_{k-2}}$$

□

Definition. Έστω το άπειρο συνεχές κλάσμα $[a_0; a_1, \dots]$, αν η ακολουθία των συγκλινοντών $\frac{p_n}{q_n}$ συγκλίνει στο a τότε θα λέμε ότι το συνεχές κλάσμα συγκλίνει και θα γράφουμε ότι $a = [a_0; a_1, \dots]$. Αν η ακολουθία των συγκλινοντών δεν συγκλίνει θα λέμε ότι το συνεχές κλάσμα αποκλίνει.

Theorem 4.2.12. *Αν $a = [a_0; a_1, \dots]$ τότε το a είναι μεγαλύτερο από κάθε άρτιας τάξης συγκλίνοντα και μικρότερο από κάθε περιττής τάξης συγκλίνοντα. Δηλαδή*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \dots < \frac{p_{2n}}{q_{2n}} < \dots < a < \dots < \frac{p_{2k-1}}{q_{2k-1}} < \dots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

Proof. Αφού $a = [a_0; a_1, \dots]$, τότε

$$a = \lim \frac{p_n}{q_n} = \lim \frac{p_{2n}}{q_{2n}} = \lim \frac{p_{2n-1}}{q_{2n-1}}.$$

Όμως, η ακολουθία $\frac{p_{2n}}{q_{2n}}$ είναι αύξουσα, οπότε για κάθε $k \in \mathbb{N}$ έχουμε ότι

$$\frac{p_{2k}}{q_{2k}} < \lim \frac{p_{2n}}{q_{2n}} = a.$$

Όμοια, για κάθε $k \in \mathbb{N}$ ισχύει ότι $a < \frac{p_{2k-1}}{q_{2k-1}}$ και το θεώρημα έχει αποδειχτεί. □

Theorem 4.2.13. *Αν $a = [a_0; a_1, \dots]$, τότε για φυσικό k ισχύει ότι*

$$\left| a - \frac{p_k}{q_k} \right| < \frac{1}{q_k q_{k+1}}$$

Remark. Οπότε για να δείξουμε ότι το συνεχές κλάσμα συγκλίνει αρκεί να δείξουμε ότι $q_k q_{k+1} \to \infty$.

Theorem 4.2.14. *Για κάθε $k \geq 2$ ισχύει ότι $q_k \geq 2^{\frac{k-1}{2}}$*

Proof. Σύμφωνα με το (4.2.4) έχουμε ότι $q_k = a_k q_{k-1} + q_{k-2}$ και επειδή $a_k \geq 1$ και $q_{k-1} \geq q_{k-2}$ προκύπτει ότι $q_k \geq 2q_{k-2}$.

Οπότε για k άρτιο έχουμε:

$$q_k \geq 2^{\frac{k}{2}} q_0 = 2^{\frac{k}{2}}$$

για k περιττό έχουμε:

$$q_k \geq 2^{\frac{k-1}{2}} q_1 \geq 2^{\frac{k-1}{2}}$$

□

Theorem 4.2.15. *Κάθε άπειρο συνεχές κλάσμα $[a_0; a_1, \dots]$ με $a_0 \in \mathbb{Z}$ και $a_1, a_2, \cdots \in \mathbb{N}$ συγκλίνει*

Proof. Σύμφωνα με το προηγούμενο έχουμε ότι $q_k q_{k+1} \geq 2^k \to \infty$.

Οπότε, το άπειρο συνεχές κλάσμα συγκλίνει. □

Remark. Το αποτέλεσμα αυτό ισχύει επειδή έχω υποθέσει ότι για τα στοιχεία του συνεχούς κλάσματος ισχύουν τα εξής: $a_0 \in \mathbb{Z}$ και $a_1, a_2, \cdots \in \mathbb{N}/\{0\}$.

Αν τα $a_i, i \in \mathbb{N}$ είναι πραγματικοί αριθμοί τότε το συνεχές κλάσμα $[a_0; a_1, \dots]$ συγκλίνει αν και μόνο αν αποκλίνει η σειρά $\sum_{n=1}^{\infty} a_n$.

Proposition 4.2.16. *Έστω $a = [a_0; a_1, \dots]$ τότε η ακολουθία*

$$(x_{k,i})_{i=0}^{a_k} = \frac{p_{k-2} + i \cdot p_{k-1}}{q_{k-2} + i \cdot q_{k-1}}$$

είναι αύξουσα για k άρτιο και φθίνουσα για k περιττό.

Proof. $x_{k,i+1} - x_{k,i} = \frac{p_{k-2}+(i+1)\cdot p_{k-1}}{q_{k-2}+(i+1)\cdot q_{k-1}} - \frac{p_{k-2}+i\cdot p_{k-1}}{q_{k-2}+i\cdot q_{k-1}}$, για $i = 0, 1, \dots, a_k - 1$ τότε:

$$x_{k,i+1} - x_{k,i} = \frac{p_{k-1}q_{k-2} - q_{k-1}p_{k-2}}{[q_{k-2} + (i+1)\, q_{k-1}]\,[q_{k-2} + i \cdot q_{k-1}]}$$

και χρησιμοποιώντας το (4.2.5) έχουμε ότι

$$x_{k,i+1} - x_{k,i} = \frac{(-1)^k}{[q_{k-2} + (i+1)\, q_{k-1}]\,[q_{k-2} + i \cdot q_{k-1}]}$$

οπότε για k άρτιο έχουμε ότι $\frac{p_{k-2}+i\cdot p_{k-1}}{q_{k-2}+i\cdot q_{k-1}} < \frac{p_{k-2}+(i+1)\cdot p_{k-1}}{q_{k-2}+(i+1)\cdot q_{k-1}}$ για $i = 0, 1, \dots, a_k - 1$.

ενώ για k περιττό έχουμε ότι $\frac{p_{k-2}+(i+1)\cdot p_{k-1}}{q_{k-2}+(i+1)\cdot q_{k-1}} < \frac{p_{k-2}+i\cdot p_{k-1}}{q_{k-2}+i\cdot q_{k-1}}$ για $i = 0, 1, \dots, a_k - 1$. □

Corollary 4.2.17. *Για k άρτιο έχουμε ότι $\frac{p_k}{q_k} < \frac{p_k+i\cdot p_{k+1}}{q_k+i\cdot q_{k+1}} < \frac{p_{k+2}}{q_{k+2}} < a$*

και για k περιττό έχουμε ότι $a < \frac{p_{k+2}}{q_{k+2}} < \frac{p_k+i\cdot p_{k+1}}{q_k+i\cdot q_{k+1}} < \frac{p_k}{q_k}$ για $i = 1, 2, \dots, a_{k-1}$.

Definition. Τα κλάσματα

$$\frac{p_{k-2}+i\cdot p_{k-1}}{q_{k-2}+i\cdot q_{k-1}}, i=1,2,\ldots,a_k-1$$

θα λέγονται ενδιάμεσα κλάσματα των συγκλίνοντων $\frac{p_{k-2}}{q_{k-2}}$ και $\frac{p_k}{q_k}$.

Theorem 4.2.18. *Για φυσικό k ισχύει ότι:*

$$\left|a-\frac{p_k}{q_k}\right| > \frac{1}{q_k\left(q_{k+1}+q_k\right)}$$

Proof. Χρησιμοποιώντας την (4.2.17) έχουμε ότι

$$\left|a-\frac{p_k}{q_k}\right| > \left|\frac{p_k+p_{k+1}}{q_k+q_{k+1}}-\frac{p_k}{q_k}\right| = \frac{\left|q_{k+1}p_k-q_kp_{k+1}\right|}{q_k\left(q_k+q_{k+1}\right)}$$

οπότε σύμφωνα με το (4.2.5) θα έχουμε ότι

$$\left|a-\frac{p_k}{q_k}\right| > \frac{1}{q_k\left(q_{k+1}+q_k\right)}.$$

□

Remark 4.2.19. Πλέον για την απόσταση του a από τους συγκλινοντές του $\left|a-\frac{p_k}{q_k}\right|$ έχουμε ένα άνω και ένα κάτω φράγμα. Έχουμε ότι

$$\frac{1}{q_k\left(q_k+q_{k+1}\right)} < \left|a-\frac{p_k}{q_k}\right| < \frac{1}{q_kq_{k+1}}, k\geq 0$$

4.3 Η αναπαράσταση των πραγματικών σε συνεχή κλάσματα

Theorem 4.3.1. *Κάθε πραγματικός αριθμός a αναπαρίσταται μοναδικά από συνεχή κλάσματα.*

Proof. Αν ο a είναι ακέραιος τότε ο a αναπαρίσταται από το συνεχές κλάσμα $[a]$.

Αν ο a δεν είναι ακέραιος τότε έχουμε ότι

$$a = a_0+\frac{1}{r_1}$$

όπου

$$a_0 = \lfloor a\rfloor \text{ και } \frac{1}{r_1} = a-a_0$$

Ακολουθώντας την ίδια διαδικασία, αν ο r_1 είναι ακέραιος τοτε $a=[a_0;r_1]$

αλλιώς έχουμε ότι

$$r_1 = a_1 + \frac{1}{r_2} \text{ με } a_1 = \lfloor r_1 \rfloor \text{ και } \frac{1}{r_2} = r_1 - a_1$$

Γενικότερα αν ο r_n είναι ακέραιος τότε

$$a = [a_0; a_1, \ldots, a_{n-1}, r_n]$$

και σταματάμε την διαδικασία
ενώ, αν δεν είναι ακέραιος τοτε

$$r_n = a_n + \frac{1}{r_{n+1}}$$

όπου

$$a_n = \lfloor r_n \rfloor \text{ και } \frac{1}{r_{n+1}} = r_n - a_n$$

τότε

$$a = [a_0; a_1, \ldots, a_{n-1}, a_n, r_{n+1}]$$

και συνεχίζουμε την διαδικασία για το r_{n+1}.
Τώρα, αφού σε κάθε βήμα έχουμε ότι

$$a = [a_0; a_1, \ldots, a_{n-1}, r_n]$$

ισχύει ότι

$$a = \frac{p_{n-1} r_n + p_{n-2}}{q_{n-1} r_n + q_{n-2}},\ n \geq 2$$

επίσης,

$$\frac{p_n}{q_n} = \frac{p_{n-1} a_n + p_{n-2}}{q_{n-1} a_n + q_{n-2}}, n \geq 2$$

οπότε

$$a - \frac{p_n}{q_n} = \frac{(p_{n-1} q_{n-2} - q_{n-1} p_{n-2})\,(r_n - a_n)}{(q_{n-1} r_n + q_{n-2})\,(q_{n-1} a_n + q_{n-2})}$$

και επειδή

$$0 \leq r_n - a_n < 1, p_{n-1} q_{n-2} - q_{n-1} p_{n-2} = (-1)^n$$

θα έχουμε ότι

$$\left| a - \frac{p_n}{q_n} \right| < \frac{1}{(q_{n-1} r_n + q_{n-2})\,(q_{n-1} a_n + q_{n-2})}$$

όμως

$$r_n \geq a_n \text{ καθώς } a_n = \lfloor r_n \rfloor$$

οπότε

$$q_{n-1}r_n + q_{n-2} \geq q_{n-1}a_n + q_{n-2} = q_n$$

οπότε

$$\frac{1}{(q_{n-1}r_n + q_{n-2})\,(q_{n-1}a_n + q_{n-2})} \leq \frac{1}{q_n^2}$$

άρα

$$\left| a - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$

τότε σύμφωνα με το (4.2.14) θα είναι

$$q_n^2 \to \infty \text{ καθώς } n \to \infty$$

τότε

$$\frac{p_n}{q_n} \to a \text{ καθώς } n \to \infty$$

οπότε το συνεχές κλάσμα $[a_0; a_1, a_2, \dots]$ συγκλίνει στο a.

Για την μοναδικότητα αρκεί να δούμε ότι σε κάθε βήμα του αλγορίθμου τα επόμενα στοιχεία που παράγονται είναι μοναδικά.

Δηλαδή, αν έχουμε σε κάποιο βήμα του αλγορίθμου ότι

$$a = [a_0; a_1, \dots, a_{n-1}, r_n]$$

τότε από το r_n παράγονται μοναδικά τα a_n και r_{n+1} καθώς το ακέραιο μέρος του r_n είναι μοναδικό.

Επίσης, το a_n πρέπει να είναι το ακέραιοι μέρος του r_n σε κάθε βήμα γιατί αν δεν ήταν τότε το συνεχές κλάσμα $\left[a_n'; a_{n+1}', \dots\right]$ δεν θα ήταν ίσο με το r_n.

Οπότε, το συνεχές κλάσμα $\left[a_0; a_1, \dots, a_{n-1}, a_n', a_{n+1}'\right]$ δεν θα ήταν ίσο με το a. □

Remark. Η μοναδικότητα της αναπαράστασης ενός αριθμού από ένα συνεχές κλάσμα δεν θα ίσχυε αν επιτρέπαμε να έχουμε πεπερασμένα συνεχή κλάσματα με τελευταίο στοιχείο το 1. Αυτό θα συνέβαινε καθώς αν $a_{n+1} = 1$, τότε θα έπρεπε $r_n = a_n + 1$ οπότε $a_n \neq \lfloor r_n \rfloor$.

Theorem 4.3.2. *Το συνεχές κλάσμα που αναπαριστά τον πραγματικό αριθμό a είναι πεπερασμένο αν ο a είναι ρητός και άπειρο αν ο a είναι άρρητος.*

Proof. Αν ο a είναι ρητός, τότε όλα τα r_n που προκύπτουν από τον προηγούμενο αλγόριθμο θα είναι ρητοί.

Αν ο r_n είναι ακέραιος τότε ήδη καταλήξαμε ότι το συνεχές κλάσμα είναι πεπερασμένο.

Αλλιώς αν $r_n = \frac{a}{b}$ με $\text{ΜΚΔ}(a, b) = 1$ τότε

$$r_n - a_n = \frac{a - ba_n}{b} = \frac{c}{b} \text{ με } c < b \text{ καθώς } r_n - a_n < 1$$

Τότε,

$$r_{n+1} = \frac{b}{c}$$

οπότε ο r_{n+1} έχει μικρότερο παρονομαστή από τον r_n. Από αυτό έπεται ότι αν ξεκινήσουμε με το r_1 ως ρητό μετά από πεπερασμένο πλήθος βημάτων θα φτάσουμε σε ένα n τέτοιο ώστε ο r_n να έχει παρονομαστή 1 δηλαδή να είναι ακέραιος και εκεί τελειώνει η διαδικασία.

Αν ο a είναι άρρητος τότε τα r_n είναι άρρητοι αριθμοί και η διαδικασία είναι άπειρη. □

Example 4.3.3. $\frac{361}{29} = [12; 2, 4, 3]$.

Έχουμε ότι

$$361 = 12 \cdot 29 + 13$$

οπότε

$$\frac{361}{29} = \frac{12 \cdot 29 + 13}{29} = 12 + \frac{13}{29}.$$

Τώρα, το κλάσμα $\frac{13}{29}$ θα το γράψουμε ως $\frac{1}{\frac{29}{13}}$.

Οπότε,

$$\frac{361}{29} = 12 + \frac{1}{\frac{29}{13}}.$$

Με τον ίδιο τρόπο έχουμε ότι

$$29 = 2 \cdot 13 + 3$$

οπότε

$$\frac{29}{13} = \frac{2 \cdot 13 + 3}{13} = 2 + \frac{3}{13} = 2 + \frac{1}{\frac{13}{3}}.$$

Τότε,

$$\frac{361}{29} = 12 + \frac{1}{2 + \frac{1}{\frac{13}{3}}}.$$

Τότε

$$13 = 4 \cdot 3 + 1$$

οπότε

$$\frac{13}{3} = 4 + \frac{1}{3}.$$

Άρα,

$$\frac{361}{29} = 12 + \frac{1}{2 + \frac{1}{4+\frac{1}{3}}}.$$

Άρα

$$\frac{361}{29} = [12; 2, 4, 3].$$

Example 4.3.4. $\sqrt{2} = [1; 2, 2, 2, \dots]$

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

Τότε,

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

οπότε

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

και εφαρμόζοντας πάλι την προηγούμενη ταυτότητα για το $\sqrt{2}+1$ θα έχουμε ότι

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

οπότε αυτή η διαδικασία θα εφαρμόζεται επ' άπειρο.

Άρα,

$$\sqrt{2} = [1; 2, 2, 2, \dots].$$

4.4 Συγκλίνοντες - η καλύτερη προσέγγιση των πραγματικών αριθμών

Πολλές φορές θέλουμε να προσεγγίσουμε έναν άρρητο a από ένα ρητό. Αυτός ο ρητός μπορεί να είναι δεκαδικός αριθμός μπορεί και όχι. Επειδή δεν μπορούμε να έχουμε πολύ μεγάλους αριθμητές και παρονομαστές καθώς η μνήμη του υπολογιστή είναι πεπερασμένη, γεννάται το ερώτημα ποιά είναι η καλύτερη προσέγγιση του a από έναν ρητό που ο παρονομαστής του να μην ξεπερνάει έναν δοσμένο αριθμό.

Θα δείξουμε ότι οι συγκλίνοντες του a αποτελούν τις καλύτερες προσεγγίσεις για τον a.

Definition. Θα λέμε ότι ο ρητός $\frac{a}{b}$ με $\text{ΜΚΔ}(a,b) = 1$ και $b > 0$ αποτελεί την καλύτερη προσέγγιση πρώτου είδους για τον πραγματικό αριθμό A αν για κάθε άλλο κλάσμα $\frac{c}{d} \neq \frac{a}{b}$ με $0 < d \leq b$ ισχύει ότι:

$$\left|A - \frac{a}{b}\right| < \left|A - \frac{c}{d}\right|$$

Theorem 4.4.1. *Κάθε καλύτερη προσέγγιση πρώτου είδους του αριθμού A είναι είτε ένας συγκλίνοντας είτε ένα ενδιάμεσο κλάσμα των συγκλίνοντων του συνεχούς κλάσματος που αναπαριστά τον A.*

Proof. Έστω ότι $\frac{a}{b}$ είναι η καλύτερη προσέγγιση του αριθμού A.

Τότε, θα ισχύει ότι

$$a_0 \leq \frac{a}{b} \leq a_0 + 1$$

γιατί αν ήταν

$$\frac{a}{b} < a_0 = \frac{a_0}{1}$$

τότε επειδή $A > a_0$ θα είχαμε ότι

$$\frac{a}{b} < \frac{a_0}{1} < A$$

οπότε

$$|A - \frac{a_0}{1}| < |A - \frac{a}{b}|$$

τότε το $\frac{a_0}{1}$ θα ήταν καλύτερη προσέγγιση του A από το $\frac{a}{b}$.

Με τον ίδιο τρόπο αν

$$a_0 + 1 < \frac{a}{b}.$$

Τότε θα είχαμε ότι

$$A < \frac{a_0 + 1}{1} < \frac{a}{b}.$$

Άρα και πάλι το $\frac{a}{b}$ δεν είναι η καλύτερη προσέγγιση πρώτου είδους του A.

Οπότε, ξέρουμε ότι $a_0 \leq \frac{a}{b} \leq a_0 + 1$.

Αν $\frac{a}{b} = a_0$ ή $\frac{a}{b} = a_0 + 1$ τότε το θεώρημα ισχύει.

Αν το $\frac{a}{b}$ δεν είναι ίσο με κανέναν συγκλίνοντα και με κανένα ενδιάμεσο κλάσμα του A τότε θα βρίσκεται ανάμεσα σε δύο διαδοχικά ενδιάμεσα κλάσματα.

Οπότε θα υπάρχουν n, i με $n \geq 0$ και $0 \leq i < a_{n+1}$ τέτοια ώστε το $\frac{a}{b}$ να βρίσκεται ανάμεσα στα κλάσματα

$$\frac{p_n i + p_{n-1}}{q_n i + q_{n-1}} \text{ και } \frac{p_n (i+1) + p_{n-1}}{q_n (i+1) + q_{n-1}}$$

τότε

$$\left| \frac{a}{b} - \frac{p_n i + p_{n-1}}{q_n i + q_{n-1}} \right| < \left| \frac{p_n (i+1) + p_{n-1}}{q_n (i+1) + q_{n-1}} - \frac{p_n i + p_{n-1}}{q_n i + q_{n-1}} \right| = \frac{1}{[q_n (i+1) + q_{n-1}] [q_n i + q_{n-1}]}$$

επίσης,

$$\left| \frac{a}{b} - \frac{p_n i + p_{n-1}}{q_n i + q_{n-1}} \right| = \frac{k}{b (q_n i + q_{n-1})}$$

όπου k ακέραιος μεγαλύτερος της μονάδας.

Οπότε θα ισχύει ότι:

$$\frac{1}{b (q_n i + q_{n-1})} < \frac{1}{[q_n (i+1) + q_{n-1}] [q_n i + q_{n-1}]}$$

δηλαδή

$$q_n (i+1) + q_{n-1} < b.$$

Τότε το κλάσμα

$$\frac{p_n (i+1) + p_{n-1}}{q_n (i+1) + q_{n-1}}$$

θα είναι καλύτερη προσέγγιση πρώτου είδους από το $\frac{a}{b}$ καθώς έχει παρονομαστη μικρότερο από b και επίσης είναι πιο κοντά στον A από το $\frac{a}{b}$ καθώς το $\frac{a}{b}$ βρίσκεται ανάμεσα στα κλάσματα

$$\frac{p_n i + p_{n-1}}{q_n i + q_{n-1}} \text{ και } \frac{p_n (i+1) + p_{n-1}}{q_n (i+1) + q_{n-1}}$$

και το $\frac{p_n (i+1) + p_{n-1}}{q_n (i+1) + q_{n-1}}$ βρίσκεται πιο κοντά στο A από το $\frac{p_n i + p_{n-1}}{q_n i + q_{n-1}}$. Άτοπο.

Οδηγηθήκαμε σε άτοπο γιατί υποθέσαμε ότι το $\frac{a}{b}$ δεν είναι ίσο με κανένα συγκλίνοντα και με κανένα ενδιάμεσο κλάσμα του A.

Άρα, το $\frac{a}{b}$ είναι ίσο με κάποιο συγκλίνοντα ή με κάποιο ενδιάμεσο κλάσμα του A και το θεώρημα έχει αποδειχτεί. □

Definition. Θα λέμε ότι ο ρητός $\frac{a}{b}$ με $\text{ΜΚΔ}(a,b)=1$ και $b>0$ αποτελεί την καλύτερη προσέγγιση δευτέρου είδους ή δεύτερης τάξης για τον αριθμό A αν για κάθε άλλο κλάσμα $\frac{c}{d}\neq\frac{a}{b}$ με $0<d\leq b$ ισχύει ότι:

$$|bA-a|<|dA-c|$$

Proposition 4.4.2. *Κάθε καλύτερη προσέγγιση δευτέρου είδους είναι και καλύτερη προσέγγιση πρώτου είδους*

Proof. Έστω $\frac{a}{b}$ με $\text{ΜΚΔ}(a,b)=1$ και $b>0$ η καλύτερη προσέγγιση δευτέρου είδους για τον αριθμό A .

Τότε για κάθε άλλο κλάσμα $\frac{c}{d}\neq\frac{a}{b}$ με $0<d\leq b$ θα έχουμε ότι:

$$|bA-a|<|dA-c|$$

και επειδή $\frac{1}{b}\leq\frac{1}{d}$ θα έχουμε ότι

$$\frac{|bA-a|}{b}<\frac{|dA-c|}{d}\Rightarrow\left|A-\frac{a}{b}\right|<\left|A-\frac{c}{d}\right|$$

Άρα, το $\frac{a}{b}$ αποτελεί καλύτερη προσέγγιση πρώτου είδους.

Το αντίστροφο δεν ισχύει. □

Theorem 4.4.3. *Κάθε καλύτερη προσέγγιση δεύτερης τάξης είναι συγκλίνοντας.*

Proof. Έστω ότι ο ρητός $\frac{a}{b}$ είναι η καλύτερη προσέγγιση δεύτερης τάξης για τον A.

Τότε θα ισχύει ότι

$$\frac{p_0}{q_0}=a_0\leq\frac{a}{b}\leq\frac{p_1}{q_1}$$

καθώς αν $\frac{a}{b}<a_0$ τότε $\frac{a}{b}<a_0\leq A$ οπότε θα είχαμε ότι:

$$|1\cdot A-a_0|<\left|A-\frac{a}{b}\right|\leq|bA-a|$$

οπότε το $\frac{a}{b}$ δεν θα ήταν καλύτερη προσέγγιση δεύτερης τάξης.

Επίσης, αν $\frac{p_1}{q_1}<\frac{a}{b}$ τότε $A\leq\frac{p_1}{q_1}<\frac{a}{b}$ οπότε έχουμε ότι

$$\frac{1}{bq_1}\leq\left|\frac{p_1}{q_1}-\frac{a}{b}\right|<\left|A-\frac{a}{b}\right|$$

οπότε

$$\frac{1}{q_1}=\frac{1}{a_1}<|bA-a|$$

επίσης, έχουμε ότι $A=a_0+\frac{1}{r_1}$ με $r_1\geq a_1$, οπότε

$$|1\cdot A-a_0|=\frac{1}{r_1}\leq\frac{1}{a_1}$$

οπότε

$$|1 \cdot A - a_0| < |bA - a|$$

το οποίο είναι άτοπο καθώς έχουμε υποθέσει ότι ο $\frac{a}{b}$ είναι η καλύτερη προσέγγιση δεύτερης τάξης του A.

Τώρα, αν το κλάσμα $\frac{a}{b}$ δεν ισούται με κανέναν συγκλίνοντα τότε θα βρίσκεται μεταξύ δύο συγκλίνοντων έστω των

$$\frac{p_n}{q_n} \text{ και } \frac{p_{n+2}}{q_{n+2}}.$$

Τότε

$$\frac{1}{bq_n} \leq \frac{|aq_n - bp_n|}{bq_n} = \left|\frac{a}{b} - \frac{p_n}{q_n}\right|$$

και

$$\left|\frac{a}{b} - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}}$$

οπότε

$$\frac{1}{bq_n} < \frac{1}{q_n q_{n+1}}$$

άρα

$$q_{n+1} < b \tag{4.1}$$

επίσης

$$\frac{1}{bq_{n+2}} \leq \left|\frac{p_{n+2}}{q_{n+2}} - \frac{a}{b}\right| \leq \left|A - \frac{a}{b}\right|$$

οπότε

$$\frac{1}{q_{n+2}} \leq |bA - a|$$

και επειδή σύμφωνα με το (4.2.13) ισχύει ότι

$$|A - \frac{p_{n+1}}{q_{n+1}}| < \frac{1}{q_{n+1}q_{n+2}}$$

θα έχουμε ότι

$$|q_{n+1}A - p_{n+1}| < \frac{1}{q_{n+2}}$$

οπότε

$$|q_{n+1}A - p_{n+1}| < |bA - a| \tag{4.2}$$

από τις (4.1) και (4.2) προκύπτει ότι ο συγκλίνοντας $\frac{p_{n+1}}{q_{n+1}}$ είναι καλύτερη προσέγγιση δεύτερου είδους από το $\frac{a}{b}$. Άτοπο.

Οδηγηθήκαμε σε άτοπο γιατί υποθέσαμε ότι το $\frac{a}{b}$ δεν ισούται με κανέναν συγκλίνοντα.

Άρα, η καλύτερη προσέγγιση δεύτερης τάξης είναι συγκλίνοντας. □

Theorem 4.4.4. *Κάθε συγκλίνοντας είναι μια καλύτερη προσέγγιση δεύτερης τάξης, με μόνη εξαίρεση την περίπτωση*

$$a = a_0 + \frac{1}{2}, \frac{p_0}{q_0} = \frac{a_0}{1}$$

Proof. Για την απόδειξη ο αναγνώστης ας δει το ([3]). □

Bibliography

[1] Gareth A. Jones and J. Mary Jones, *Elementary Number Theory*, Springer

[2] Henri Cohen, *A course in Computational Algebraic Number Theory*, Springer

[3] A. Ya. Khinchin, *Continued Fractions*

[4] Αλέξανδρος Χ. Παπαϊωάννου, Μιχαήλ Θ. Ρασσιάς, *Εισαγωγή στην Θεωρία Αριθμών*, Αθήνα 2008

[5] Χ. Κουκουβίνος, Α. Παπαϊωάννου, *Κρυπτογραφία,* Αθήνα 2007

[6] Π. Βλάμος, Ε. Ράππος, Π. Ψαρράκος, *Θεωρία Αριθμών*, Ελληνική Μαθηματική Εταιρεία, Αθήνα 2000

[7] Αγγελίνα Ε. Βιδάλη, *Συνεχή Κλάσματα και ο Αφαιρετικός Ευκλείδιος Αλγόριθμος, 23 Σεπτεμβρίου*, 2005

[8] Π. Γ. Τσαγκάρης, *Θεωρία Αριθμών,* Εκδόσεις Συμμετρία, Αθήνα 2005

[9] Αλέξανδρος Χ. Παπαϊωάννου, *Διακριτά Μαθηματικά*, Αθήνα 2003

[10] Γεώργιος Ελευθερίου, *Υπολογιστική Θεωρία Αριθμών: Τεστ πιστοποίησης πρώτων και παραγοντοποίηση ακεραίων*, Αθήνα Μάιος 2011

[11] Στάθης Ζάχος, *Εισαγωγή στην Επιστήμη των Υπολογιστών Θεωρητική Πληροφορική Γλώσσες Προγραμματισμού Οργάνωση Υπολογιστών*, Αθήνα 2008

[12] Δημήτριος Μ. Πουλάκης, *Θεωρία Αριθμών*, Εκδόσεις ΖΗΤΗ, Θεσσαλονίκη 2001

[13] Μαργαρίτα Τουρλάκη, *Θεωρία Συνεχών Κλασμάτων και Εφαρμογές*, Αθήνα 2011