ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
ΤΜΗΜΑ ΜΕΘΟΔΟΛΟΓΙΑΣ ΙΣΤΟΡΙΑΣ ΚΑΙ ΘΕΩΡΙΑΣ ΤΗΣ ΕΠΙΣΤΗΜΗΣ
ΤΜΗΜΑ ΦΙΛΟΣΟΦΙΑΣ - ΠΑΙΔΑΓΩΓΙΚΩΝ - ΨΥΧΟΛΟΓΙΑΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΚΥΠΡΟΥ

ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΣΤΑΤΙΣΤΙΚΗΣ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΩΝ ΑΓΩΓΗΣ

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ - ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
"ΔΙΔΑΚΤΙΚΗ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΑ ΤΩΝ ΜΑΘΗΜΑΤΙΚΩΝ"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Εφαρμογές της Θεωρίας Αριθμών»

Μαραγκός Νικόλαος
Δ 201024

Επιβλέπων καθηγητής:
Ευάγγελος Ράπτης

Μάιος 2014

Η παρούσα Διπλωματική Εργασία

εκπονήθηκε στα πλαίσια των σπουδών

για την απόκτηση του

Μεταπτυχιακού Διπλώματος Ειδίκευσης

που απονέμει το

Διαπανεπιστημιακό – Διατμηματικό Πρόγραμμα Μεπταπτυχιακών Σπουδών

«Διδακτική και Μεθοδολογία των Μαθηματικών»

Εγκρίθηκε την 02-05-2014 από Εξεταστική Επιτροπή αποτελούμενη από τους:

Ονοματεπώνυμο	Βαθμίδα	Υπογραφή
1) ΕΥΑΓΓΕΛΟΣ ΡΑΠΤΗΣ (ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ)	ΚΑΘΗΓΗΤΗΣ	
2) ΔΙΟΝΥΣΙΟΣ ΛΑΠΠΑΣ	ΑΝΑΠΛ. ΚΑΘΗΓΗΤΗΣ	
3) ΠΑΝΑΓΙΩΤΗΣ ΣΠΥΡΟΥ	ΑΝΑΠΛ. ΚΑΘΗΓΗΤΗΣ	

Στη γυναίκα μου Μαίρη,

στον αδελφό μου Βασίλη,

στους γονείς μου Κυριάκο & Κατερίνα

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον **επιβλέποντα καθηγητή κ. Ευάγγελο Ράπτη**, για την υποστήριξη του στην διάρκεια της εκπόνησης της εργασίας αυτής, καθώς και τους **καθηγητές κ. Σπύρου** και **κ. Διονύσιο Λάππα**, για την τιμή που μου έκαναν να είναι μέλη της εξεταστικής επιτροπής.

Τέλος, θα ήθελα να ευχαριστήσω όλους τους συντελεστές του Προγράμματος Μεταπτυχιακών Σπουδών για την συνεργασία τους καθ΄όλη τη διάρκεια του Προγράμματος.

Πίνακας Περιεχομένων

ΠΕΡΙΛΗΨΗ

Η εργασία αυτή απευθύνεται σε μαθητές που ενδιαφέρονται να έχουν κάποια πληροφόρηση, συμβατή με το σχολικό βιβλίο αλλά και λίγο πιο πέρα από αυτό. Μπορεί, επίσης, να αποτελέσει αφετηρία για τις λεγόμενες "συνθετικές" εργασίες.

Η παρούσα θέση της Θεωρίας Αριθμών στα σχολεία είναι περιορισμένη στο πιο ρηχό και μηχανικό μέρος της και συνεπώς στο πλέον ανούσιο: επαγωγή, η ταυτότητα της διαίρεσης και σε μικρή έκταση η διαιρετότητα. Η εργασία αυτή έχει στόχο να βοηθήσει κάποιους νέους, παράλληλα με τα μαθήματα τους, να κάνουν μία είσοδο σε αυτό το εξαίρετο ανθρώπινο διανοητικό δημιούργημα, τη Θεωρία Αριθμών, η διδασκαλία της οποίας βασικό στόχο έχει την **άσκηση των μαθητών στην αποδεικτική διαδικασία**.

Η εργασία αποτελείται από δύο μέρη. Στο **πρώτο μέρος** παρουσιάζονται οι κυριότερες έννοιες και τα βασικά Θεωρήματα της Θεωρίας Αριθμών και αποτελείται από 15 κεφάλαια. Στο **δεύτερο μέρος** παρουσιάζονται κάποιες από τις εφαρμογές της Θεωρίας Αριθμών και αποτελείται από 10 κεφάλαια.

Abstract

This paper applies to students who want to have some information, not only consistent with the textbook but also a little beyond that. Also, for some student it can be a starting point for dealing with "synthetic" exercises.

The present position of Number Theory in schools is limited to the most mechanical and insipid part of it: Induction, the identity of division plus at some extent divisibility. This paper aims to help some people, along their courses to make one entrance to this extraordinary human intellectual creation, the Number Theory, whose teaching has main objective the performance of students in “proof process”.

The paper consists of two parts: The first part introduces the main concepts and basic Theorems of number theory and consists of 15 chapters. The second part contains some applications of number theory and it consists of 10 chapters.

Πρόλογος

Η εργασία αυτή απευθύνεται σε μαθητές που ενδιαφέρονται να έχουν κάποια πληροφόρηση, συμβατή με το σχολικό βιβλίο αλλά και λίγο πιο πέρα από αυτό. Μπορεί, επίσης, να αποτελέσει αφετηρία για τις λεγόμενες "συνθετικές" εργασίες.

Η Θεωρία Αριθμών είναι πολιτιστικό επίτευγμα που έχει τις ρίζες της στον ανεπανάληπτο **πολιτισμό των Αρχαίων Ελλήνων**. Αποτελεί πιθανότατα τον πιο συναρπαστικό κλάδο των Μαθηματικών και ονομάστηκε από τον Gauss «**Βασίλισσα των Μαθηματικών**». Μάλλον όχι άδικα. Τα προβλήματα της ελκύουν το ενδιαφέρον ενός μεγάλου και ετερόκλητου κοινού: από ανθρώπους που απλώς έχουν τελειώσει το σχολείο έως μεγάλους μαθηματικούς που είναι κορυφαίοι στον τομέα τους. Προσφέρει χαρά, συγκίνηση και πιο σπάνια διάκριση. Από την άλλη μεριά η Θεωρία Αριθμών υπήρξε η κινητήρια δύναμη για την ανάπτυξη πλείστων περιοχών των Μαθηματικών.

Η παρούσα θέση της Θεωρίας Αριθμών στα σχολεία είναι περιορισμένη στο πιο ρηχό και μηχανικό μέρος της και συνεπώς στο πλέον ανούσιο: επαγωγή, η ταυτότητα της διαίρεσης και σε μικρή έκταση η διαιρετότητα. Η εργασία αυτή έχει στόχο να βοηθήσει κάποιους νέους, παράλληλα με τα μαθήματα τους, να κάνουν μία είσοδο σε αυτό το εξαίρετο ανθρώπινο διανοητικό δημιούργημα, τη Θεωρία Αριθμών, η διδασκαλία της οποίας βασικό στόχο έχει την **άσκηση των μαθητών στην αποδεικτική διαδικασία**.

Η εργασία αποτελείται από δύο μέρη. Στο **πρώτο μέρος** παρουσιάζονται οι κυριότερες έννοιες και τα βασικά Θεωρήματα της Θεωρίας Αριθμών και αποτελείται από 14 κεφάλαια. Στο **δεύτερο μέρος** παρουσιάζονται κάποιες από τις εφαρμογές της Θεωρίας Αριθμών και αποτελείται από 10 κεφάλαια.

Πιο συγκεκριμένα το **πρώτο μέρος** αναφέρεται:

στις στοιχειώδης ιδιότητες της Διαιρετότητας, την μέθοδο απόδειξης με την εις άτοπο απαγωγή, την μαθηματική επαγωγή, τον Μέγιστο Κοινό Διαιρέτη, την παραγοντοποίηση πρώτων αριθμών και το Θεμελιώδες Θεώρημα της Αριθμητικής Ισοτιμίες και η αριθμητική των ισοϋπόλοιπων, Γραμμικές Εξισώσεις Ισοτιμίας, Euler's Phi Συνάρτηση και Θεώρημα Fermat – Euler, Πρωταρχικές ρίζες, Τετράγωνα modulo p και τετραγωνικά ισοϋπόλοιπα, ο Νόμος της τετραγωνικής Αντιστροφής και Διοφαντικές εξισώσεις.

Στο **δεύτερο μέρος** παρουσιάζονται οι εξής εφαρμογές:

Αριθμοί Fibonacci και Γραμμική Αναδρομικότητα, οι πρώτοι αριθμοί του Mersenne και οι

τέλειοι αριθμοί, Δυνάμεις Ισοϋπόλοιπων, υπολογισμός ριζών κ-τάξης modulo p, RSA – Public key – Κρυπτογραφία, Πυθαγόρειες Τριάδες, οι πρώτοι αριθμοί που είναι άθροισμα δύο τετραγώνων, οι Γεωμετρικοί Αριθμοί, οι Τετράγωνοι – Τριγωνικοί Αριθμοί, η Εξίσωση του Pell και τέλος το Θεώρημα του Pick.

ΜΕΡΟΣ Α

ΕΝΝΟΙΕΣ ΚΑΙ ΒΑΣΙΚΑ ΘΕΩΡΗΜΑΤΑ

ΤΗΣ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ

Κεφάλαιο 1ο
Στοιχειώδεις Ιδιότητες της Διαιρετότητας

Μια από τις θεμελιώδης ιδέες της θεωρίας αριθμών είναι η έννοια της **διαιρετότητας**.

Ορισμός 1.1 Αν a και b είναι ακέραιοι με $a \neq 0$, και αν υπάρχει ακέραιος c τέτοιος ώστε $a \cdot c = b$

τότε λέμε a διαιρεί τον b, και γράφουμε $a \mid b$. Αν a δεν διαιρεί τον b τότε γράφουμε $a \nmid b$.

Για παράδειγμα

$2 \mid 18,\ 1 \mid 42,\ 3 \mid (-6),\ -7 \mid 49,\ 9 \nmid 80,\ -6 \nmid 31.$

Θεώρημα 1.1 Ιδιότητες της Διαιρετότητας

1. Αν a, b, c, m, n **είναι ακέραιοι τέτοιοι ώστε** $c \mid a$ **και** $c \mid b$ **τότε** $c \mid (a \cdot m + n \cdot b)$**.**

2. Αν x, y, z **είναι ακέραιοι τέτοιοι ώστε** $x \mid y$ **και** $y \mid z$ **τότε** $x \mid z$**.**

Απόδειξη

Αφού $c \mid a$ και $c \mid b$ υπάρχουν ακέραιοι s, t τέτοιοι ώστε $s \cdot c = a \quad t \cdot c = b$ τότε

$a \cdot m + n \cdot b = c \cdot (s \cdot m + t \cdot n)$.

Οπότε $c \mid (a \cdot m + b \cdot n)$.

Όμοια αφού $x \mid y$ και $y \mid z$ τότε υπάρχουν ακέραιοι u, v με $x \cdot u = y$ και $y \cdot v = z$. Επομένως $x \cdot u \cdot v = z$ δηλαδή $x \mid z$.

Θεώρημα 1.2 Αν $a \mid b$ και $a \mid (b + c)$ τότε $a \mid c$

Απόδειξη

Αφού $a \mid b$ τότε υπάρχει ακέραιος s τέτοιος ώστε $a \cdot s = b$. Αφού $a \mid (b + c)$ τότε υπάρχει ακέραιος t τέτοιος ώστε $a \cdot t = b + c$. Οπότε

$$a \cdot t - b = c$$
$$a \cdot t - a \cdot s = c$$
$$a \cdot (t - s) = c$$

Εφόσον t και s είναι και οι δύο ακέραιοι τότε ο $t - s$ είναι και αυτός ακέραιος, οπότε $a \mid c$.

Παράδειγμα 1.1

Να βρείτε όλους τους θετικούς ακεραίους $n \geq 1$ για τους οποίους ισχύει $(n+1) \mid (n^2 + 1)$.

Λύση

$n^2+1=n^2-1+2=(n-1)(n+1)+2$. Οπότε αν $(n+1)\,|\,(n^2+1)$ τότε θα πρέπει να έχουμε $(n+1)\,|\,2$ αφού $(n+1)\,|\,(n-1)(n+1)$. Επομένως $n+1=1$ ή $n+1=2$.

Αφού $n\geq 1$ τότε $n+1\neq 1$. Καταλήγουμε στο συμπέρασμα ότι $n+1=2$, οπότε το μοναδικό n τέτοιο ώστε

$(n+1)\,|\,(n^2+1)$ είναι το $n=1$.

Παράδειγμα 1.2

Αν $7\,|\,(3\cdot x+2)$ να αποδείξετε ότι $7\,|\,(15x^2-11\cdot x-14)$.

Λύση

Παρατηρούμε ότι $15\cdot x^2-11\cdot x-14=(3\cdot x+2)\cdot(5\cdot x-7)$. Αφού $7\,|\,(3\cdot x+2)$ έχουμε ότι $7\cdot s=(3\cdot x+2)$

για κάποιο ακέραιο αριθμό s.

Επομένως $15\cdot x^2-11\cdot x-14=7\cdot s\cdot(5\cdot x-7)$.

Οπότε $7\,|\,(15\cdot x^2-11\cdot x-14)$.

Θεώρημα 1.3 Ο Αλγόριθμος της Διαίρεσης

Αν a και b είναι θετικοί ακέραιοι τότε υπάρχουν μοναδικοί ακέραιοι q και r τέτοιοι ώστε

$a=b\cdot q+r \quad 0\leq r<b$.

Ονομάσαμε το παραπάνω θεώρημα ως αλγόριθμο γιατί μπορούμε να βρίσκουμε το πηλίκο q και το υπόλοιπο r χρησιμοποιώντας την κλασική διαίρεση του a με το b.

Παρατηρούμε ότι $b\,|\,a$ αν και μονό αν $r=0$.

Κεφάλαιο 2ο
Απόδειξη με Εις άτοπον απαγωγή

Σε μια **απόδειξη με εις άτοπο με απαγωγή,** υποθέτουμε την λογική άρνηση της πρότασης που θέλουμε να αποδείξουμε και τότε καταλήγουμε σε κάποια αντίφαση (άτοπο).

Επομένως από τη στιγμή που καταλήξαμε σε αντίφαση καταλήγουμε στο συμπέρασμα ότι η αρχική μας υπόθεση (ή λογική άρνηση της πρότασης που θέλουμε να αποδείξουμε) είναι λανθασμένη, οπότε η πρόταση που προσπαθούμε να αποδείξουμε πρέπει να αληθεύει.

Παράδειγμα 2.1

Να αποδείξετε ότι $6-\sqrt{35}<\frac{1}{10}$ χωρίς να χρησιμοποιήσετε υπολογιστή τσέπης.

Λύση

Ας υποθέσουμε ότι $6-\sqrt{35}\geq\frac{1}{10}$. Τότε $6-\frac{1}{10}\geq\sqrt{35}$ οπότε $59\geq 10\cdot\sqrt{35}$.

Εφόσον και τα δύο μέλη είναι θετικά τα υψώνουμε στο τετράγωνο οπότε και προκύπτει $3481\geq 3500$ το οποίο είναι μια αντίφαση (άτοπο).

Οπότε η αρχική μας υπόθεση πρέπει να είναι λανθασμένη οπότε καταλήγουμε στο συμπέρασμα ότι $6-\sqrt{35}<\frac{1}{10}$.

Παράδειγμα 2.2

Έστω $a_1,a_2,...a_n$ είναι μια αυθαίρετη μετάθεση των αριθμών 1,2,…,n όπου n είναι περιττός αριθμός. Να αποδείξετε ότι το γινόμενο $(a_1-1)\cdot(a_2-2)\cdots(a_n-n)$ είναι άρτιος.

Λύση

Αρκεί να αποδείξουμε ότι κάποια διαφορά a_k-n είναι άρτιος.

Ας υποθέσουμε ότι όλες οι διαφορές a_k-k είναι περιττοί αριθμοί . Τότε προκύπτει ότι $S=(a_1-1)+(a_2-2)+\cdots+(a_n-n)=0$ αφού τα a_k είναι μια αναδιάταξη των 1,2,…,n.

Στην παραπάνω ισότητα λέμε ότι το S είναι ίσο με το μηδέν που το μηδέν είναι άρτιος αριθμός.

Δηλαδή το S είναι άρτιος αριθμός.

Το S όμως είναι περιττός αριθμός ως αθροίσματα περιττών ακεραίων a_k-k.

Αυτό είναι μια αντίφαση (άτοπο).

Οπότε η αρχική μας υπόθεση πρέπει να είναι λανθασμένη οπότε καταλήγουμε στο συμπέρασμα ότι ένας από τους όρους a_k-k είναι άρτιος, επομένως το γινόμενο είναι άρτιος.

Παράδειγμα 2.3

Να αποδείξετε ότι δεν υπάρχουν θετικές ακέραιες λύσεις στην εξίσωση $x^2 - y^2 = 1$.

Λύση

Ας υποθέσουμε ότι υπάρχει λύση (x, y) όπου x και y είναι θετικοί ακέραιοι.

Τότε μπορούμε να παραγοντοποιήσουμε το αριστερό μέλος της εξίσωσης οπότε και έχουμε $(x-y)\cdot(x+y)=1$.

Αφού x και y είναι και οι δύο θετικοί ακέραιοι τότε $x-y$ και $x+y$ είναι ακέραιοι.

Οπότε $x-y=1$ και $x+y=1$ ή $x-y=-1$ και $x+y=-1$.

Στην πρώτη περίπτωση προσθέτουμε κατά μέλη τις 2 εξισώσεις οπότε και καταλήγουμε στο συμπέρασμα ότι $x=1$ και $y=0$ που αυτό όμως έρχεται σε αντίφαση με το γεγονός ότι είναι και ο x και ο y είναι και οι δυο θετικοί.

Στη δεύτερη περίπτωση προσθέτουμε κατά μέλη τις 2 εξισώσεις οπότε και καταλήγουμε στο συμπέρασμα ότι $x=-1$ και $y=0$ που αυτό όμως έρχεται σε αντίφαση με το γεγονός ότι είναι και ο x και ο y είναι και οι δυο θετικοί.

Επομένως δεν υπάρχουν θετικές ακέραιες λύσεις της εξίσωσης $x^2 - y^2 = 1$.

Παράδειγμα 2.4

Αν a,b,c είναι περιττοί ακέραιοι να αποδείξετε ότι η εξίσωση $a\cdot x^2 + b\cdot x + c = 0$ δεν έχει λύση ρητό αριθμό.

Λύση

Ας υποθέσουμε ότι $\frac{p}{q}$ είναι ένας ρητός που είναι λύση της εξίσωσης. Μπορούμε να υποθέσουμε χωρίς βλάβη της γενικότητας ότι p και q δεν έχουν κοινούς πρώτους παράγοντες οπότε και ο p και ο q είναι περιττοί ή ο ένας είναι περιττός και ο άλλος είναι άρτιος.

Αφού ο $\frac{p}{q}$ είναι λύση θα επαληθεύει την εξίσωση.

Δηλαδή $a\cdot\left(\frac{p}{q}\right)^2 + b\cdot\left(\frac{p}{q}\right) + c = 0 \Rightarrow a\cdot p^2 + b\cdot p\cdot q + c\cdot q^2 = 0$.

Αν και οι δύο p και q είναι περιττοί, τότε ο $a\cdot p^2 + b\cdot p\cdot q + c\cdot q^2$ είναι και αυτός περιττός ως άθροισμα περιττών αριθμών οπότε θα είναι $\neq 0$ (ο 0 είναι άρτιος) που αυτό είναι άτοπο γιατί υποθέσαμε ότι $\frac{p}{q}$ είναι λύση. Όμοια αν ένας από τους δυο p και q είναι άρτιος κα ο άλλος είναι

περιττός τότε ο $a \cdot p^2 + b \cdot p \cdot q + c \cdot q^2$ είναι άρτιος ή ο $a \cdot p^2 + b \cdot p \cdot q + c \cdot q^2$ είναι περιττός. Αυτή η αντίφαση στην οποία και καταλήξαμε δηλώνει ότι η παραπάνω εξίσωση δεν έχει λύση ρητό αριθμό.

Παράδειγμα 2.5

Να αποδείξετε ότι ο $\sqrt{2}$ είναι άρρητος.

Λύση

Θα το αποδείξουμε με την εις άτοπο με απαγωγή. Έστω ότι ο $\sqrt{2}$ είναι ρητός. Τότε θα γράφετε ως εξής

$\sqrt{2} = \frac{r}{s}$ όπου r και s δεν έχουν κοινούς παράγοντες. Τότε αν υψώσουμε την παραπάνω εξίσωση στο τετράγωνο προκύπτει ότι $2 = \frac{r^2}{s^2}$.

Επομένως καταλήγουμε στο συμπέρασμα, δηλαδή $2 \cdot s^2 = r^2$.

Αυτό όμως σημαίνει ότι ο r^2 πρέπει να είναι άρτιος, οπότε ο r άρτιος. Δηλαδή $r = 2 \cdot c$.

Τότε $2 \cdot s^2 = (2 \cdot c)^2 = 4 \cdot c^2$.

Οπότε $s^2 = 2 \cdot c^2$.

Δηλαδή ο s είναι και αυτός άρτιος.

Καταλήξαμε σε αντίφαση αφού οι r και s δεν έχουν κοινούς παράγοντες.

Επομένως ο $\sqrt{2}$ είναι άρρητος.

Στην συνέχεια αναφέρουμε δύο σημαντικά αποτελέσματα.

Θεώρημα 2.1

Αν n είναι ένας ακέραιος μεγαλύτερος από το 1 τότε ο n μπορεί να γραφεί ως πεπερασμένο γινόμενο πρώτων αριθμών.

Απόδειξη

Θα το αποδείξουμε με την εις άτοπο με απαγωγή.

Ας υποθέσουμε ότι δεν ισχύει . Δηλαδή θα υπάρχουν σύνθετοι αριθμοί (οι αριθμοί που δεν είναι πρώτοι) που δεν θα μπορούν να γραφούν ως πεπερασμένο γινόμενο πρώτων.

Έστω N είναι ο πιο μικρός από τους παραπάνω αριθμούς. Αφού N είναι ο πιο μικρός από αυτούς τους αριθμούς τότε αν $1 < n < N$ τότε το θεώρημα αληθεύει για το n.

Έστω p είναι ένας πρώτος αριθμός που είναι και διαιρέτης του N. Καθώς ο N είναι σύνθετος τότε

$1 < \frac{N}{p} < N$.

Επομένως, το θεώρημα αληθεύει για το $\frac{N}{p}$.

Επομένως υπάρχουν πρώτοι αριθμοί $p_1, p_2 \cdots p_k$ τέτοιοι ώστε $\frac{N}{p} = p_1 \cdot p_2 \cdots p_k$. Δηλαδή $N = p \cdot p_1 \cdot p_2 \cdots p_k$.

Είναι ένα πεπερασμένο γινόμενο πρώτων.

Αυτό όμως είναι μια αντίφαση γιατί υποθέσαμε ότι οι σύνθετοι αριθμοί δεν μπορούν να γραφούν ως πεπερασμένο γινόμενο πρώτων.

Επομένως καταλήγουμε στο συμπέρασμα ότι μεγαλύτερος από το 1 τότε ο n μπορεί να γραφεί ως πεπερασμένο γινόμενο πρώτων αριθμών.

Θεώρημα 2.2

Υπάρχουν άπειροι πρώτοι αριθμοί.

Απόδειξη

Θα το αποδείξουμε με την εις άτοπο με απαγωγή.

Η παρακάτω απόδειξη που είναι αρκετά ενδιαφέρουσα οφείλεται στον Euclid.

Ας υποθέσουμε ότι υπάρχουν πεπερασμένοι στο πλήθος πρώτοι αριθμοί. Έστω n το πλήθος.

Τότε $\{p_1, p_2, ..., p_n\}$ είναι μια λίστα που εξαντλεί όλους τους πρώτους.

Ας Θεωρήσουμε τον αριθμό $N = p_1 \cdot p_2 \cdots p_n + 1$

Αυτός ο αριθμός είναι ένας θετικός αριθμός που είναι μεγαλύτερος του 1.

Ας παρατηρήσουμε ότι κανένας από τους πρώτους της λίστας $\{p_1, p_2, ..., p_n\}$ διαιρούν τον N, αφού καθένας από αυτούς τους πρώτους αφήνει υπόλοιπο 1. Καθώς ο N είναι ο μεγαλύτερος από όλους τους πρώτους που είναι μέσα στην λίστα τότε ή θα είναι πρώτος ή θα διαιρείται από έναν πρώτο που θα είναι στην λίστα. Οπότε αποδείξαμε ότι η υπόθεση ότι κάθε πεπερασμένη λίστα πρώτων αριθμών οδηγεί στην ύπαρξη πρώτου αριθμού έξω από την λίστα, που αυτό όμως οδηγεί σε αντίφαση. Επομένως καταλήγουμε στο συμπέρασμα ότι το πλήθος των πρώτων είναι άπειρο.

Κεφάλαιο 3ο Μαθηματική Επαγωγή

Η Μαθηματική επαγωγή είναι μια ισχυρή μέθοδος για να αποδεικνύουμε προτάσεις που αφορούν ακεραίους.

Για παράδειγμα την μαθηματική επαγωγή μπορούμε να την χρησιμοποιήσουμε για να αποδείξουμε τα παρακάτω:

- Το άθροισμα των εσωτερικών γωνιών κάθε ν-γώνου είναι $180\cdot(n-2)$ μοίρες.
- Η ανισότητα $n!>2^n$ αληθεύει για όλους τους ακεραίους $n\geq 4$.
- 7^n-1 διαιρείται από το 6 για όλους τους ακεραίους $n\geq 1$.

Κάθε ισχυρισμός (υπόθεση) μπορεί να τεθεί στην μορφή:

P(n) αληθεύει για όλους τους ακεραίους $n\geq n_o$, όπου P(n) είναι μια πρόταση που εμπεριέχει τον ακέραιο n και n_o είναι η «αφετηρία» ή βασική περίπτωση.

Για παράδειγμα για τον τρίτο ισχυρισμό (7^n-1 διαιρείται από το 6 για όλους τους ακεραίους $n\geq 1$) η P(n) είναι η πρόταση ότι το 7^n-1 διαιρείται από το 6 και η βασική περίπτωση είναι $n_o=1$.

Στη συνέχεια περιγράφουμε πως δουλεύει η μαθηματική επαγωγή:

(1) **Βασική περίπτωσ:** Αρχικά αποδεικνύουμε ότι η πρόταση P(n_o) αληθεύει.

(2) **Επαγωγικό Βήμα:** Στην συνέχεια αποδεικνύουμε ότι αν η πρόταση P(κ) αληθεύει τότε θα πρέπει να αληθεύει και η πρόταση P(κ+1).

Ας παρατηρήσουμε ότι αυτά τα δύο βήματα είναι επαρκή για να δείξουμε ότι η πρόταση P(n) αληθεύει για όλους τους ακεραίους $n\geq n_o$, καθώς P(n_o) αληθεύει από το βήμα (1) και το βήμα (2) φανερώνει ότι η πρόταση P(n_o+1) αληθεύει, που αυτό φανερώνει ότι και P(n_o+2) κ.τ.λ.

Μπορούμε να σκεφτούμε την μαθηματική επαγωγή όπως παρακάτω:

Ας υποθέσουμε ότι έχουμε τοποθετήσει απείρως πολλά dominos σε μια γραμμή, που αντιπροσωπεύουν τις προτάσεις P(1) P(2) P(3) … Αν κάνουμε το πρώτο domino να πέσει τότε θα είμαστε σίγουροι ότι όλα τα domino θα πέσουν, αφού κάθε φορά όταν πέφτει ένα domino τότε κτυπάει και ρίχνει κάτω το γειτονικό του.

Ρίχνοντας το πρώτο domino είναι ανάλογο με την βασική περίπτωση. Αποδεικνύοντας ότι κάθε domino που πέφτει ρίχνει κάτω το γειτονικό του είναι ισοδύναμο με το να αποδείξουμε ότι P(n) συνεπάγεται P(n+1).

Παράδειγμα 3.1 Να αποδείξετε ότι για κάθε ακέραιο $n \geq 1$

$$1+2+3+\ldots+n=\frac{n\cdot(n+1)}{2}.$$

Παράδειγμα 3.2 Να αποδείξετε ότι $n!>2^n$ για όλους τους ακεραίους $n \geq 4$.

Λύση

P(n) είναι η πρόταση $n!>2^n$. Η βασική περίπτωση είναι $n_o=4$.

(i) **Βασική περίπτωση** $4!>24>2^4=16$ επομένως η βασική περίπτωση P(4) αληθεύει.

(ii) **Επαγωγική Υπόθεση**

Ας υποθέσουμε ότι $n!>2^n$. Πρέπει να χρησιμοποιήσουμε αυτόν τον ισχυρισμό για να αποδείξουμε ότι $(n+1)!>2^{n+1}$.

Το αριστερό μέλος της επαγωγικής υπόθεσης είναι $n!$ και το αριστερό μέλος της πρότασης που θέλουμε να αποδείξουμε είναι $(n+1)!=(n+1)\cdot n!$. Επομένως είναι επακόλουθο να πολλαπλασιάσουμε και τα δύο μέλη της επαγωγικής υπόθεσης με τον όρο (n+1).

$$n!>2^n$$
$$(n+1)\cdot n!>(n+1)\cdot 2^n$$
$$(n+1)!>(n+1)\cdot 2^n$$

Τελικά αφού $(n+1)>2$ τότε

$$(n+1)!>(n+1)\cdot 2^n>2\cdot 2^n>2^{n+1}$$

Οπότε βγάζουμε το συμπέρασμα ότι $(n+1)!>2^{n+1}$ αυτό που θέλαμε να αποδείξουμε.

Επομένως $n!>2^n$ για όλους τους ακεραίους $n \geq 4$.

Παράδειγμα 3.3

Να αποδείξετε ότι η έκφραση $3^{3n+3}-26n-27$ είναι πολλαπλάσιο του 169 για όλους τους φυσικούς αριθμούς n.

Λύση

P(n) είναι ο ισχυρισμός ότι η έκφραση $3^{3n+3}-26n-27$ είναι πολλαπλάσιο του 169 και η βασική περίπτωση είναι $n_o=1$.

(i) **Βασική περίπτωση** Παρατηρούμε ότι $3^{3\cdot 1+3}-26(1)-27=676=4\cdot(169)$ επομένως η βασική περίπτωση P(1) αληθεύει.

(ii) **Επαγωγική Υπόθεση**

Ας υποθέσουμε ότι P(n) αληθεύει. Δηλαδή υπάρχει ακέραιος M τέτοιος ώστε $3^{3n+3}-26n-27=169\cdot M$. Πρέπει να χρησιμοποιήσουμε αυτόν τον ισχυρισμό για να αποδείξουμε

ότι υπάρχει ακέραιος Κ τέτοιος ώστε

$3^{3\cdot(n+1)+3}-26\cdot(n+1)-27=169K$.

Έχουμε

$$\begin{aligned}3^{3\cdot(n+1)+3}-26\cdot(n+1)-27 &= 3^{3\cdot n+3+3}-26\cdot n-26-27\\ &= 27\cdot(3^{3n+3})-26\cdot n-27-26\\ &= 27\cdot(3^{3n+3})-26\cdot n-26(26n)+26(26n)\\ &\quad -27-26(27)+26(27)-26\\ &= 27\cdot(3^{3n+3})-27(26\cdot n)-27(27)+26(26n)+26(27)-26\\ &= 27\cdot(3^{3n+3}-26\cdot n-27)+676n+676\\ &= 27\cdot(169M)+169\cdot 4n+169\cdot 4\\ &= 169(27M+4n+4)\end{aligned}$$

Επομένως $3^{3n+3}-26n-27$ είναι πολλαπλάσιο του 169 για όλους τους φυσικούς αριθμούς n.

Παράδειγμα 3.4

Να αποδείξετε ότι αν k είναι περιττός τότε ο 2^{n+2} διαιρεί τον $k^{2^n}-1$ για όλους τους φυσικούς αριθμούς n.

Λύση

Ας υποθέσουμε ότι k είναι περιττός. Τότε η πρόταση P(n) έχει ως εξής: "ο 2^{n+2} διαιρεί τον $k^{2^n}-1$" και η βασική περίπτωση είναι $n_o=1$.

(i) **Βασική περίπτωση** Ο $k^2-1=(k-1)(k+1)$ διαιρείται από τον $2^{1+2}=8$ για κάθε περιττό φυσικό αριθμό k αφού k-1 και k+1 είναι διαδοχικό άρτιοι ακέραιοι αριθμοί,

(ii) **Επαγωγική Υπόθεση**

Ας υποθέσουμε ότι 2^{n+2} διαιρεί τον $k^{2^n}-1$. Τότε υπάρχει ακέραιος α τέτοιος ώστε $2^{n+2}\cdot a=k^{2^n}-1$. Τότε

$k^{2^{n+1}}-1=(k^{2^n}-1)(k^{2^n}+1)=2^{n+2}\cdot a\cdot(k^{2^n}+1)$.

Αφού ο k είναι περιττός τότε ο $k^{2^n}+1$ είναι περιττός και επομένως $k^{2^n}+1=2b$ για κάποιο ακέραιο b.

Δηλαδή $k^{2^{n+1}}-1=2^{n+2}\cdot a\cdot(k^{2^n}+1)=2^{n+3}\cdot a\cdot b$.

Επομένως ο ισχυρισμός αποδείχτηκε με μαθηματική επαγωγή.

Παράδειγμα 3.5 (Αριθμοί Fibonacci)

Οι αριθμοί **Fibonacci** δίνονται από τις παρακάτω σχέσεις:

$F_0 = 0, F_1 = 1 \quad F_{n+1} = F_n + F_{n-1} \quad n \geq 1$

Με άλλα λόγια κάθε αριθμός μετά τον δεύτερο όρο προκύπτει ως το άθροισμα των 2 προηγούμενων όρων**.**

Οι αριθμοί **Fibonacci** που προκύπτουν είναι**:** $0,1,1,2,3,5,8,13,21,....$

Να αποδείξετε για όλους τους ακεραίους $n \geq 1$ ότι $F_{n-1} \cdot F_{n+1} = F_n^2 + (-1)^{n+1}$**.**

Λύση

Η πρόταση P(n) είναι η πρόταση $F_{n-1} \cdot F_{n+1} = F_n^2 + (-1)^{n+1}$**.**

Και η βασική περίπτωση είναι $n_o = 1$.

(i) **Βασική περίπτωση** Αν $n = 1$ τότε Ο $F_0 \cdot F_2 = 1^2 + (-1)^1$,

(ii) **Επαγωγική Υπόθεση** Έστω $F_{n-1} \cdot F_{n+1} = F_n^2 + (-1)^{n+1}$ τότε χρησιμοποιώντας το γεγονός ότι $F_{n+2} \cdot F_n = F_{n+1}$

$$\begin{aligned} F_n \cdot F_{n+2} &= F_n(F_n + F_{n+1}) \\ &= F_n^2 + F_n \cdot F_{n+1} \\ \text{Θα έχουμε} \quad &= F_{n-1} \cdot F_{n+1} - (-1)^n + F_n \cdot F_{n+1} \\ &= F_{n+1} \cdot (F_{n-1} + F_n) + (-1)^{n+1} \\ &= F_{n+1}^2 + (-1)^{n+1} \end{aligned}$$

Το οποίο και αποδεικνύει τον ισχυρισμό μας με την μαθηματική επαγωγή.

Παράδειγμα 3.6

Να αποδείξετε ότι ο $\frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$ είναι ένας ακέραιος για όλους τους ακεραίους $n \geq 0$.

Λύση

Η πρόταση P(n) είναι: "ο $\frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$ είναι ένας ακέραιος" και η βασική περίπτωση είναι $n_o = 0$.

(i) **Βασική περίπτωση:** Αφού ο 0 είναι ακέραιος η πρόταση αληθεύει για $n = 0$,

(ii) **Επαγωγική Υπόθεση:** Έστω ότι ο $\frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$ είναι ένας ακέραιος.

Θα πρέπει να αποδείξουμε ότι ο $\frac{(n+1)^5}{5} + \frac{(n+1)^4}{2} + \frac{(n+1)^3}{3} - \frac{n+1}{30}$ είναι και αυτός ακέραιος.

$$\frac{(n+1)^5}{5}+\frac{(n+1)^4}{2}+\frac{(n+1)^3}{3}-\frac{n+1}{30}=$$

Έχουμε $$=\frac{n^5+5n^4+10n^3+5n+1}{5}+\frac{n^4+4n^3+6n^2+4n+1}{2}+\frac{n^3+3n^2+3n+1}{3}-\frac{n+1}{30}$$

$$=\left[\frac{n^5}{5}+\frac{n^4}{2}+\frac{n^3}{3}-\frac{n}{30}\right]+\left[n^4+2n^3+2n^2+n+2n^3+3n^2+2n+n^2+n+1\right]$$

που είναι ένας ακέραιος από την επαγωγική υπόθεση για τον πρώτο όρο του αθροίσματος και ο δεύτερος όρος του παραπάνω αθροίσματος είναι ακέραιος ως αθροίσματα ακέραιων.

Κεφάλαιο 4^{ο} Ο Μέγιστος Κοινός Διαιρέτης

Ορισμός 4.1 Έστω a και b είναι ακέραιοι, αλλά όχι και οι δύο ταυτόχρονα μηδέν. Έστω d ο μεγαλύτερος αριθμός από το σύνολο των κοινών διαιρετών των a και b. Τον αριθμό d τον ονομάζουμε **Μέγιστο Κοινό Διαιρέτη** των a και b και τον συμβολίζουμε ως εξής:

$$d = \text{ΜΚΔ}(a,b)$$

ή πιο απλά $d = (a.b)$.

Παράδειγμα 4.1 Στη συνέχεια υπολογίζουμε μερικούς μέγιστους κοινούς διαιρέτες:

- $(6,4) = 2$
- $(3,5) = 1$
- $(16,24) = 8$
- $(4,0) = 4$
- $(5,5) = 5$
- $(3,12) = 3$

Ορισμός 4.2 Αν $(a,b) = 1$ τότε ονομάζουμε τους a,b **σχετικά πρώτους.**

Στη γενική περίπτωση, Θέλουμε να έχουμε την δυνατότητα να υπολογίζουμε τον μέγιστο κοινό διαιρέτη (a,b) χωρίς να γράφουμε κάθε φορά όλους τους παράγοντες των a και b. Ο ευκλείδειος αλγόριθμος είναι η πιο γνωστή και αποτελεσματική μέθοδος για τον υπολογισμό του μέγιστου κοινού Διαιρέτη.

Παράδειγμα 4.2

Να υπολογιστεί ο $\text{ΜΚΔ}(54,21)$.

Λύση

Το πρώτο βήμα είναι να διαιρέσουμε το 54 με το 21, το οποίο δίνει πηλίκο 2 και υπόλοιπο 12. Δηλαδή $54 = 2 \cdot 21 + 12$. Το δεύτερο βήμα είναι να διαιρέσουμε το 21 με το 12, το οποίο δίνει πηλίκο 1 και υπόλοιπο 9 . Δηλαδή $21 = 1 \cdot 12 + 9$.

Το τρίτο βήμα είναι να διαιρέσουμε το 12 με το 9, το οποίο δίνει πηλίκο 1 και υπόλοιπο 3. Δηλαδή $12 = 1 \cdot 9 + 3$. Το τέταρτο βήμα είναι να διαιρέσουμε το 9 με το 3, το οποίο δίνει πηλίκο 3 και υπόλοιπο 0. Δηλαδή $9 = 3 \cdot 3 + 0$.

Ο **ευκλείδειος αλγόριθμος** μας λέει ότι σταματάμε τα βήματα όταν το υπόλοιπο μας γίνει ίσο με

το μηδέν, και ότι το υπόλοιπο από το προηγούμενο βήμα είναι ο μέγιστος κοινός διαιρέτης των αρχικών δυο ακέραιων αριθμών. Επομένως:

$$(54,21) = 3$$

Το θέμα είναι **γιατί** αυτή η διαδικασία μας δίνει πράγματι τον μέγιστο κοινό διαιρέτη;

Η απάντηση βρίσκεται στις παραπάνω εξισώσεις κοιτάζοντας από το τέλος προς την αρχή. Από την τελευταία εξίσωση είναι σαφές ότι $3 \mid 9$, οπότε $3 \mid 12$, στη συνέχεια $3 \mid 21$ και τέλος $3 \mid 54$. Άρα ο 3 είναι ο μέγιστος κοινός διαιρέτης του 21 και του 54. Αλλά γιατί είναι ο μέγιστος κοινός διαιρέτης; Ας υποθέσουμε ότι d είναι ένας άλλος μέγιστος κοινός διαιρέτης του 21 και του 54. Θα πρέπει να δείξουμε ότι $d \leq 3$, δηλαδή ο 3 είναι ο μέγιστος κοινός διαιρέτης του 54 και του 21.

Παράδειγμα 4.3

Υπολογίστε τον Μέγιστο Κοινό Διαιρέτη (36,132) και χρησιμοποιείστε τον υπολογισμό αυτό για να βρείτε ακεραίους x και y τέτοιους ώστε $(36,132) = 36 \cdot x + 132 \cdot y$.

Λύση

$$\begin{aligned} 132 &= 3 \cdot 36 + 24 \quad (1) \\ 36 &= 1 \cdot 24 + 12 \quad (2) \\ 24 &= 2 \cdot 12 + 0 \quad (3) \end{aligned}$$

Επομένως:

$$(36,132) = 12$$

Ξεκινώντας από την σχέση (3) και πηγαίνοντας προς την σχέση (1) έχουμε:

$$\begin{aligned} 12 &= 36 - 1 \cdot 24 \\ &= 36 - 1 \cdot (132 - 3 \cdot 36) \\ &= 4 \cdot 36 - 1 \cdot 132 \end{aligned}$$

Καταλήγουμε ότι:

$$(36,132) = 12 = 4 \cdot 36 - 1 \cdot 132 .$$

Παράδειγμα 4.4

Υπολογίστε τον Μέγιστο Κοινό Διαιρέτη $(53,77)$ και χρησιμοποιείστε τον υπολογισμό αυτό για να βρείτε ακεραίους x και y τέτοιους ώστε $(53,77) = 53 \cdot x + 77 \cdot y$.

Λύση

$$\begin{aligned} 77 &= 1 \cdot 53 + 24 \quad (1) \\ 53 &= 2 \cdot 24 + 5 \quad (2) \\ 24 &= 4 \cdot 5 + 4 \quad (3) \\ 5 &= 1 \cdot 4 + 1 \quad (4) \\ 4 &= 4 \cdot 1 + 0 \quad (5) \end{aligned}$$

Επομένως :

$(53,77)=1$, οπότε ο 53 και ο 57 είναι σχετικά πρώτοι.

Ξεκινώντας από την σχέση (5) και πηγαίνοντας προς την σχέση (1) έχουμε:

$$\begin{aligned}1&=5-1\cdot 4\\&=5-1\cdot(24-4\cdot 5)\\&=5\cdot 5-1\cdot 24\\&=5\cdot(53-2\cdot 24)-1\cdot 24\\&=5\cdot 53-11\cdot 24\\&=5\cdot 53-11\cdot(77-1\cdot 53)\\&=16\cdot 53-11\cdot 77.\end{aligned}$$

Καταλήγουμε ότι

$$(53,77)=1=16\cdot 53-11\cdot 77\,.$$

Θεώρημα 4.1: Έστω α και b είναι δύο ακέραιοι αριθμοί που δεν είναι και οι δύο μηδέν . Τότε ο μέγιστος κοινός διαιρέτης των α, b μπορεί να γραφεί ως γραμμικός συνδυασμός των α και b, οπότε υπάρχουν x και y τέτοιοι ώστε:

$$(a,b)=a\cdot x+b\cdot y$$

και οι ακέραιοι x και y μπορούν να βρεθούν από τον **ευκλείδειο αλγόριθμο** που υλοποιήσαμε σε προηγούμενα παραδείγματα.

Παρατηρούμε ότι αφού $(a,b)\mid a$ και $(a,b)\mid b$ τότε $(a,b)\mid a\cdot x+b\cdot y$ για όλους τους ακεραίους x και y. Από το **Θεώρημα 4.1**, μπορούμε πάντα να βρίσκουμε ακέραιους x και y τέτοιους ώστε $(a,b)=a\cdot x+b\cdot y$.

Στην γενική περίπτωση, ας θεωρήσουμε όλες τις πιθανές τιμές που μπορούμε να πάρουμε από αριθμούς της μορφής $a\cdot x+b\cdot y$, όταν αντικαθιστούμε όλους τους πιθανούς ακεραίους για x και y. Για παράδειγμα, ας θεωρήσουμε την περίπτωση $a=42$ και $b=30$. Παρατηρούμε ότι $(42,30)=6$. Στη συνέχεια συμπληρώνουμε τον παρακάτω πίνακα για τα συγκεκριμένα x και y από την μορφή $a\cdot x+b\cdot y$.

	$x=-3$	$x=-2$	$x=-1$	$x=0$	$x=1$	$x=2$	$x=3$
$y=-3$	-216	-174	-132	-90	12	-6	36
$y=-2$	-186	-144	-102	-60	-18	24	66
$y=-1$	-156	-114	-72	-30	12	54	96
$y=0$	-126	-84	-42	0	42	84	126
$y=1$	-96	-54	-12	30	72	114	256
$y=2$	-66	-24	18	60	102	144	186
$y=3$	-36	6	-12	90	132	174	216

Παρατηρούμε ότι $(42,30)=6$ το οποίο και εμφανίζεται στον παραπάνω πίνακα και είναι η

μικρότερη θετική τιμή του $a \cdot x + b \cdot y$. Στη γενική περίπτωση αυτό είναι πάντοτε αληθής (και μπορεί να αποδειχθεί μέσω του **ευκλείδειου αλγορίθμου**).

Θεώρημα 4.2: Έστω a και b είναι δυο ακέραιοι αριθμοί που δεν είναι και οι δυο μηδέν. Τότε η μικρότερη θετική τιμή του $a \cdot x + b \cdot y$ (που παίρνουμε για όλους τους ακεραίους) είναι ο μέγιστος κοινός διαιρέτης (a,b).

Απόδειξη

Ας υποθέσουμε ότι a,b,c είναι ακέραιοι και ότι $a \mid b \cdot c$. Ποια θα είναι η συνθήκη ώστε ο α να είναι και αυτός διαιρέτης του c; Για παράδειγμα $8 \mid 4 \cdot 10 = 40$, αλλά 8 $\nmid$ 4 και 8 $\nmid$ 10.

Μπορούμε να χρησιμοποιήσουμε το **Θεώρημα 4.1** για να απαντήσουμε στην παραπάνω ερώτηση.

Λήμμα 4.3 Αν $a \mid b \cdot c$ και $(a,b) = 1$ τότε $a \mid c$

Απόδειξη

Αφού $(a,b) = 1$, θα υπάρχουν ακέραιοι x και y τέτοιοι ώστε $a \cdot x + b \cdot y = 1$ και αφού $a \mid b \cdot c$, τότε υπάρχει ακέραιος k τέτοιος ώστε $a \cdot k = b \cdot c$.

$$
\begin{aligned}
c &= c \cdot 1 \\
&= c \cdot (a \cdot x + b \cdot y) \\
&= (a \cdot c \cdot x + a \cdot k \cdot y) \\
&= a \cdot (c \cdot x + k \cdot y)
\end{aligned}
$$

Επομένως $a \mid c$.

Κεφάλαιο 5ο
Παραγοντοποίηση Πρώτων αριθμών και το Θεμελιώδες Θεώρημα της Αριθμητικής

Θεώρημα 5.1 : Έστω p ένας πρώτος αριθμός. Και ας υποθέσουμε ότι $p \mid a \cdot b$. Τότε ή $p \mid a$ ή $p \mid b$ (ή p διαιρεί και τους δύο a και b).

Απόδειξη

Ας υποθέσουμε ότι ο p είναι πρώτος που διαιρεί το γινόμενο $a \cdot b$. Αν $p \mid a$ τότε δεν χρειάζεται να αποδείξουμε κάτι. Επομένως ας υποθέσουμε ότι p $\nmid$ a . Θεωρούμε τον μέγιστο κοινό διαιρέτη (a, p) .Όμως $(a, p) \mid p$, επομένως $(a, p) = 1$ ή $(a, p) = p$ αφού ο p είναι πρώτος. Άλλα, $(a, p) \neq p$ αφού $(a, p) \mid p$ και θεωρούμε ότι p $\nmid$ a. Επομένως $(a, p) = 1$. Άρα υπάρχουν ακέραιοι x και y τέτοιοι ώστε $a \cdot x + p \cdot y = 1$. Πολλαπλασιάζουμε και τα δύο μέλη της παραπάνω σχέσης με b οπότε προκύπτει $a \cdot b \cdot x + p \cdot b \cdot y = b$. Αφού $p \mid a \cdot b \cdot x$ και $p \mid p \cdot b \cdot y$ προκύπτει ότι $p \mid (a \cdot b \cdot x + p \cdot b \cdot y) = b$.

Θεώρημα 5.2 : Έστω p ένας πρώτος αριθμός, και ας υποθέσουμε ότι ο p διαιρεί το γινόμενο $\alpha_1 \cdot \alpha_2 \ldots \alpha_r$.Τότε ο p διαιρεί τουλάχιστον έναν από τους παράγοντες $\alpha_1, \alpha_2, \ldots \alpha_r$.

Απόδειξη

Αν $p \mid a_1$ τότε δεν χρειάζεται να αποδείξουμε κάτι .Επομένως ας υποθέσουμε ότι p $\nmid a_1$. Χρησιμοποιώντας το **Θεώρημα 5.1** για το γινόμενο $a_1 \cdot (a_2 \cdot a_3 \ldots a_r)$ καταλήγουμε στο συμπέρασμα ότι $p \mid a_2 \cdot a_3 \ldots a_r$. Αν τώρα $p \mid a_2$ τότε έχει ολοκληρωθεί η απόδειξη μας.

Οπότε ας υποθέσουμε ότι p $\nmid a_2$. Χρησιμοποιώντας το **Θεώρημα 5.1** για το γινόμενο $a_2 \cdot (a_3 \cdot a_4 \ldots a_r)$ καταλήγουμε στο συμπέρασμα ότι $p \mid a_3 \cdot a_4 \ldots a_r$.

Συνεχίζοντας τελικά βρίσκουμε κάποιο a_κ τέτοιο ώστε $p \mid a_k$.

Ο στόχος μας τώρα είναι να αποδείξουμε ότι κάθε ακέραιος $n \geq 2$ μπορεί να παραγοντοποιηθεί με μοναδικό τρόπο σε γινόμενο πρώτων $p_1 \cdot p_2 \cdot p_3 \ldots p_n$. Πριν το αποδείξουμε ας δούμε ένα παράδειγμα που θα υλοποιεί την παραγοντοποίηση σε πρώτους κατά μοναδικό τρόπο που δεν είναι και τόσο προφανές.

Παράδειγμα 5.1

Έστω το σύνολο $\mathrm{E} = \{\ldots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\}$ των άρτιων αριθμών. Ας θεωρήσουμε το $60 \in \mathrm{E}$.

- Παρατηρούμε ότι $60 = 2 \cdot 30 = 6 \cdot 10$.
- Παρατηρούμε ότι 2,6,10 και 30 είναι όλοι πρώτοι που ανήκουν στο E και δεν μπορούν να

παραγοντοποιηθούν στο Ε.

Επομένως, ο αριθμός 60 έχει 2 διαφορετικές παραγοντοποιήσεις στο Ε.

Παρόλο που το παραπάνω παράδειγμα το επινοήσαμε, πρέπει να μας πείσει ότι συγκεκριμένα αριθμητικά συστήματα έχουν μοναδική παραγοντοποίηση και άλλα συστήματα δεν έχουν.

Το σύνολο των ακεραίων έχει σημαντικές ιδιότητες όπου ικανοποιεί το παρακάτω θεώρημα της μοναδικότητας της παραγοντοποίησης.

Θεώρημα 5.3 (Θεμελιώδης Θεώρημα Αριθμητικής)

Κάθε ακέραιος $n \geq 2$ μπορεί να παραγοντοποιηθεί σε γινόμενο πρώτων

$$n = p_1 \cdot p_2 \ldots p_n$$

με μοναδικό τρόπο.

Απόδειξη

Το παραπάνω Θεώρημα ουσιαστικά αποτελείται από 2 μέρη.

1. Πρέπει να αποδείξουμε ότι κάθε ακέραιος $n \geq 2$ μπορεί να παραγοντοποιηθεί σε γινόμενο πρώτων.
2. Πρέπει να αποδείξουμε ότι υπάρχει μόνο ένας τέτοιος τρόπος παραγοντοποίησης.

Αρχικά θα αποδείξουμε το πρώτο μέρος. Θα το αποδείξουμε με την μέθοδο απαγωγής σε άτοπο. Ας υποθέσουμε ότι υπάρχουν ακέραιοι μεγαλύτεροι του 2 που δεν μπορούν να γραφούν ως γινόμενο πρώτων. Τότε θα υπάρχει ένας ακέραιος έστω ο μικρότερος. Ονομάζουμε αυτόν τον μικρότερο ακέραιο με N. Αφού ο N δεν μπορεί να γραφεί ως γινόμενο πρώτων, μπορούμε να συμπεράνουμε ότι ο N δεν είναι πρώτος. Οπότε υπάρχουν ακέραιοι b και c τέτοιοι ώστε $\mathrm{N} = b \cdot c$ με $b, c > 1$ και $b, c < N$.

Αφού ο N είναι ο μικρότερος ακέραιος που δεν μπορεί να γραφεί ως γινόμενο πρώτων, b και c μπορούν να γραφούν ως γινόμενο πρώτων:

$b = p_1 \cdot p_2 \ldots p_k$, $c = q_1 \cdot q_2 \ldots q_l$, όπου όλοι οι p_i και q_i είναι πρώτοι.

Τότε ο $N = b \cdot c = p_1 \cdot p_2 \ldots p_k \cdot q_1 \cdot q_2 \ldots q_l$ μπορεί να γραφεί ως γινόμενο πρώτων.

Αυτή είναι όμως μια αντίφαση, οπότε καταλήγουμε στο συμπέρασμα ότι δεν υπάρχουν τέτοιοι ακέραιοι. Οπότε κάθε ακέραιος $n \geq 2$ μπορεί να παραγοντοποιηθεί σε γινόμενο πρώτων.

Στην συνέχεια θα αποδείξουμε το $2^{ο}$ μέρος.

Ας υποθέσουμε ότι υπάρχει ένας ακέραιος n που μπορεί να παραγοντοποιηθεί ως γινόμενο πρώτων με 2 τρόπους . Δηλαδή $n = p_1 \cdot p_2 \ldots p_k = q_1 \cdot q_2 \ldots q_l \quad (1)$

Θα πρέπει να αποδείξουμε ότι αυτές οι δυο παραγοντοποιήσεις είναι ίδιες, πιθανότατα αφού αλλάξουμε θέση στην σειρά των παραγόντων.

Αρχικά παρατηρούμε ότι $p_1 \mid n = q_1 \cdot q_2 ... q_l$ επομένως από το Θεώρημα 2.2 προκύπτει ότι p_1 θα διαιρεί ένα από τα q_i. Μπορούμε να αλλάξουμε την σειρά των q_i . ώστε $p_1 \mid q_1$.

Αλλά q_1 είναι ήδη πρώτος αριθμός, οπότε οι διαιρέτες του είναι ο 1 και ο q_1. Επομένως καταλήγουμε ότι $p_1 = q_1$ (2)

Από σχέσεις (1) και (2) διαγράφοντας τα p_1, q_1 και από τα 2 μέλη προκύπτει ότι

$p_2 \cdot p_3 ... p_k = q_2 \cdot q_3 ... q_l$ (3)

Αλλάζοντας το ίδιο όρισμα όπως πριν, θα παρατηρήσουμε ότι:

$$p_2 \mid q_1 \cdot q_2 ... q_l .$$

Επομένως, από το Θεώρημα 5.2 προκύπτει ότι p_2 θα διαιρεί ένα από τα q_i, και μετά από την εναλλαγή καταλήγουμε στο συμπέρασμα ότι $p_2 \mid q_2$, επομένως $p_2 = q_2$ (4) αφού ο q_2 είναι πρώτος.

Από σχέσεις (3) και (4) διαγράφοντας τα p_2 και q_2 από τα 2 μέλη προκύπτει ότι

$p_3 \cdot p_4 ... p_k = q_3 \cdot q_4 ... q_l$ (5)

Μπορούμε να συνεχίσουμε την συγκεκριμένη επιχειρηματολογία μέχρι καθένα από τα p_i ή καθένα από τα q_i να εξαντληθούν.

Αλλά αν όλα τα p_i εξαντληθούν, τότε το αριστερό μέλος της εξίσωσης θα είναι ίσο με 1, έτσι δεν θα υπάρχει κανένα q_i αντίστοιχα . Όμοια αν όλα τα q_i εξαντληθούν, τότε το δεξί μέλος της εξίσωσης θα είναι ίσο με 1, έτσι δεν θα υπάρχει κανένα p_i αντίστοιχα.

‘Οπότε το πλήθος των p_i θα πρέπει να είναι το ίδιο με το πλήθος των q_i, και μετά τις εναλλαγές θα έχουμε: $p_1 = q_1, p_2 = q_2, p_3 = q_3, ..., p_k = q_k$. Επομένως υπάρχει ένας μόνο τρόπος να γράψουμε έναν ακέραιο $n \geq 2$ ως γινόμενο πρώτων.

Παράδειγμα 5.2

Να αποδειχθεί ότι ο $\sqrt{2}$ είναι άρρητος.

Απόδειξη

Η απόδειξη θα γίνει με την μέθοδο της Εις άτοπον απαγωγής

Υποθέτουμε ότι ο $\sqrt{2}$ είναι ρητός. Τότε υπάρχουν ακέραιοι r και s τέτοιοι ώστε:

$\sqrt{2} = \frac{r}{s}$. Τότε $2 = \frac{r^2}{s^2}$.

Επομένως $2 \cdot s^2 = r^2$.

Έστω n το πλήθος των πρώτων παραγόντων στην παραγοντοποίηση πρώτων παραγόντων του s. Τότε υπάρχουν 2n πρώτοι παράγοντες στην παραγοντοποίηση πρώτων παραγόντων του s^2, και αφού ο 2 είναι πρώτος θα υπάρχουν 2n+1 πρώτοι παράγοντες στην παραγοντοποίηση πρώτων παραγόντων του $2 \cdot s^2$, επομένως ο $2 \cdot s^2$ έχει περιττό πλήθος πρώτων παραγόντων.

Στην συνέχεια αν Θεωρήσουμε m το πλήθος των πρώτων παραγόντων στην παραγοντοποίηση πρώτων παραγόντων του r. Τότε υπάρχουν 2m πρώτοι παράγοντες στην παραγοντοποίηση πρώτων παραγόντων του r^2, επομένως ο r^2 θα έχει άρτιο πλήθος πρώτων παραγόντων. Αυτό όμως έρχεται σε αντίθεση με το Θεμελιώδης Θεώρημα της Αριθμητικής αφού $2 \cdot s^2 = r^2$. Οπότε ο $\sqrt{2}$ είναι άρρητος.

Παράδειγμα 5.3

Ας υποθέσουμε ότι α και ν είναι θετικοί ακέραιοι και ότι $\sqrt[\nu]{\alpha}$ είναι ρητός. Να αποδειχθεί ότι ο $\sqrt[\nu]{\alpha}$ είναι ακέραιος.

Απόδειξη

Αφού ο $\sqrt[\nu]{\alpha}$ είναι ρητός και θετικός, υπάρχουν θετικοί ακέραιοι r και s τέτοιοι ώστε $\sqrt[\nu]{\alpha} = \frac{r}{s}$.

Οπότε $a \cdot s^n = r^n$. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $(r,s) = 1$ (σε περίπτωση που δεν είναι $(r,s) = 1$ τότε διαιρούμε τον αριθμητή και τον παρανομαστή με (r,s) ώστε το κλάσμα να γίνει ανάγωγο.

Θα χρησιμοποιήσουμε την μέθοδο της απαγωγής με άτοπο για να αποδείξουμε ότι s = 1 . Έστω s > 1 τότε υπάρχει πρώτος αριθμός p ο οποίος διαιρεί τον s, επομένως $p \mid a \cdot s^n = r^n$.

Από το Θεώρημα 2.2 προκύπτει ότι $p \mid r$.

Αλλά αυτό είναι άτοπο αφού $(r,s) = 1$. Οπότε s = 1 .

Άρα $\sqrt[\nu]{\alpha} = r$ είναι ένας ακέραιος. Μπορούμε να χρησιμοποιήσουμε αυτό το αποτέλεσμα, για παράδειγμα για να αποδείξουμε ότι ο $\sqrt{2}$ είναι άρρητος.

Αφού $1 < \sqrt{2} < 2$ και ο $\sqrt{2}$ δεν είναι ακέραιος, οπότε δεν είναι ρητός με βάση το αποτέλεσμα που καταλήξαμε σε αυτό το παράδειγμα.

Παράδειγμα 5.4

Να αποδειχθεί ότι ο $\log_{10} 2$ είναι άρρητος.

Απόδειξη

Θα χρησιμοποιήσουμε την μέθοδο της απαγωγής με άτοπο.

Ας υποθέσουμε ότι ο $\log_{10} 2$ είναι ρητός. Τότε υπάρχουν ακέραιοι r και s τέτοιοι ώστε: $\log_{10} 2 = \frac{r}{s}$.

Τότε $10^{\frac{r}{s}} = 2$, επομένως $10^r = 2^s$ ή $5^r \cdot 2^r = 2^s$ το οποίο έρχεται σε αντίθεση με το θεμελιώδης θεώρημα της Αριθμητικής. Επομένως ο $\log_{10} 2$ είναι άρρητος.

Παράδειγμα 5.5

Να αποδειχθεί ότι το πολυώνυμο $p(x) = a_0 \cdot x^n + a_1 \cdot x^{n-1} + \ldots + a_{n-1} \cdot x + a_n$ με ακέραιους συντελεστές του x, και με τιμή 7 για 4 ακέραιες τιμές του x τότε δεν μπορεί το πολυώνυμο να πάρει την τιμή 14 για οποιαδήποτε ακέραια τιμή του x.

Απόδειξη

Θα χρησιμοποιήσουμε την μέθοδο της απαγωγής με άτοπο.

Ας υποθέσουμε ότι υπάρχει ένας ακέραιος m τέτοιος ώστε $p(m) = 14$. Γνωρίζουμε ότι $p(a_k) - 7 = 0$ για 4 διαφορετικούς ακεραίους a_1, a_2, a_3, a_4. Τότε

$p(x) - 7 = (x - a_1) \cdot (x - a_2) \cdot (x - a_3) \cdot (x - a_4) \cdot q(x)$

Για κάποιο πολυώνυμο $q(x)$ με ακέραιους συντελεστές. Τότε

$14 - 7 = 7 = p(m) - 7 = (m - a_1) \cdot (m - a_2) \cdot (m - a_3) \cdot (m - a_4) \cdot q(m)$

Αφού οι παράγοντες $m - a_k$ είναι όλοι διαφορετικοί, έχουμε παραγοντοποιήσει τον ακέραιο 7 σε τουλάχιστον 4 διαφορετικούς παράγοντες.

Ωστόσο από το θεμελιώδης θεώρημα της Αριθμητικής ο ακέραιος 7 μπορεί να γραφεί ως γινόμενο το πολύ 3 διαφορετικών ακεραίων: $7 = (-7) \cdot (1) \cdot (-1)$. Επομένως έχουμε καταλήξει σε άτοπο, οπότε καταλήγουμε στο συμπέρασμα ότι το πολυώνυμο δεν μπορεί να πάρει την τιμή 14 για οποιαδήποτε ακέραια τιμή του x.

Παράδειγμα 5.6

Να αποδειχθεί ότι $m^5 + 3 \cdot m^4 \cdot n - 5 \cdot m^3 \cdot n^2 - 15 \cdot m^2 \cdot n^3 + 4m \cdot n^4 + 12 \cdot n^5$ δεν θα είναι ποτέ ίσο με 33.

Απόδειξη

Παρατηρούμε ότι $m^5 + 3 \cdot m^4 \cdot n - 5 \cdot m^3 \cdot n^2 - 15 \cdot m^2 \cdot n^3 + 4m \cdot n^4 + 12 \cdot n^5 =$

$= (m - 2 \cdot n) \cdot (m - n) \cdot (m + n) \cdot (m + 2 \cdot n) \cdot (m + 3 \cdot n)$

Το 33 μπορεί να παραγοντοποιηθεί ως γινόμενο το πολύ 4 ακεραίων.

$33 = (-11) \cdot (3) \cdot (1) \cdot (-1)$ ή $33 = (-3) \cdot (11) \cdot (1) \cdot (-1)$.

Αν $n \neq 0$ τότε οι παράγοντες στο παραπάνω γινόμενο είναι όλοι διαφορετικοί.

Από το θεμελιώδης θεώρημα της Αριθμητικής δεν μπορούν οι παράγοντες αυτοί αν πολλαπλασιαστούν να δώσουν 33, αφού το 33 είναι το γινόμενο το πολύ 4 διαφορετικών παραγόντων και η έκφραση παραπάνω είναι το γινόμενο 5 διαφορετικών παραγόντων για $n \neq 0$.

Αν $n = 0$, το γινόμενο των παραγόντων είναι m^5, και ο 33 δεν είναι σε Πέμπτη δύναμη. Επομένως $m^5 + 3 \cdot m^4 \cdot n - 5 \cdot m^3 \cdot n^2 - 15 \cdot m^2 \cdot n^3 + 4m \cdot n^4 + 12 \cdot n^5$ δεν είναι ποτέ ίσο με 33.

Παράδειγμα 5.7

Να αποδειχθεί ότι υπάρχει μόνο ένας φυσικός αριθμός n τέτοιος ώστε ο $2^8 + 2^{11} + 2^n$ να είναι τέλειο τετράγωνο.

Απόδειξη

Ας υποθέσουμε ότι k είναι ένας ακέραιος τέτοιος ώστε $k^2 = 2^8 + 2^{11} + 2^n = 2304 + 2^n = 48^2 + 2^n$.

Τότε $k^2 - 48^2 = (k - 48) \cdot (k + 48) = 2^n$

Από το θεμελιώδης θεώρημα της Αριθμητικής έχουμε $k - 48 = 2^s$ και $k + 48 = 2^t$, όπου $s + t = n$.

Αλλά τότε

$2^t - 2^s = 48 - (-48) = 96 = 3 \cdot 2^5$

Οπότε $2^s \cdot (2^{t-s} - 1) = 3 \cdot 2^5$.

Από το θεμελιώδης θεώρημα της Αριθμητικής, s = 5 και $t - s = 2$, έτσι $s + t = n = 12$.

Οπότε ο μόνος φυσικός αριθμός n τέτοιος ώστε ο $2^8 + 2^{11} + 2^n$ να είναι τέλειο τετράγωνο είναι ο $n = 12$.

Κεφάλαιο 6ο
Εισαγωγή στις Ισοτιμίες και η Αριθμητική των modulo

Συχνά συμβαίνει οι λύσεις προβλημάτων που αφορούν ακεραίους να εξαρτώνται μόνο από υπόλοιπα διαιρέσεων. Ας θεωρήσουμε ένα πολύ απλό παράδειγμα. Η απάντηση στο ερώτημα 'Ποια ημέρα της εβδομάδας θα είναι 7001 ημέρες από την επόμενη Κυριακή φαίνεται αμέσως αν σκεφθούμε ότι οι ημέρες της εβδομάδας επαναλαμβάνονται με περίοδο 7 και ότι $7001 = 7 \cdot 1000 + 1$. Συνεπώς η απάντηση είναι Δευτέρα. Στην ίδια απάντηση θα φθάναμε αν στη θέση του 7001 είχαμε 8, 15 η οποιοδήποτε φυσικό αριθμό της μορφής $7 \cdot m + 1$.

Ορισμός 6.1 Έστω m ένας ακέραιος. Δύο ακέραιοι α και b θα λέγονται **ισότιμοι** modulo m (ή ισοϋπόλοιποι modulo m) αν ο m διαιρεί τη διαφορά $a - b$. Στην περίπτωση αυτή γράφουμε $a \equiv b \bmod m$ δηλαδή $a \equiv b \bmod m \Leftrightarrow m \mid a - b$.

Ισοδύναμα μπορούμε να πούμε $a \equiv b \bmod m$ αν οι α και b αφήνουν το ίδιο υπόλοιπο όταν διαιρούνται με το m. Από τον αλγόριθμο της διαίρεσης, παρατηρούμε ότι $a \equiv b \bmod m$ αν και μόνο αν υπάρχει ακέραιος k τέτοιος ώστε $a = b + k \cdot m$.

Παράδειγμα 6.1 $7 \equiv 2 \bmod 5$ αφού $5 \mid (7 - 2)$. Παρατηρούμε επίσης ότι ο 7 και ο 2 αφήνουν υπόλοιπο 2 όταν διαιρεθούν με το 5.

Παράδειγμα 6.2 $47 \equiv 35 \equiv 5 \bmod 6$ αφού $6 \mid (47 - 35)$ και $6 \mid (35 - 5)$. Παρατηρούμε επίσης ότι ο 47 ο 35 και ο 5 αφήνουν υπόλοιπο 5 όταν διαιρεθούν με το 6.

Παράδειγμα 6.3 $9 \equiv 0 \bmod 3$ αφού $3 \mid 9$ και $6 \mid (35 - 5)$. Παρατηρούμε επίσης ότι ο 9 αφήνει υπόλοιπο 0 όταν διαιρεθεί με το 3.

Παράδειγμα 6.4 $15 \equiv 7 \equiv -1 \bmod 8$ αφού $8 \mid (15 - 7)$ και $8 \mid \left[7 - (-1)\right]$.

Παράδειγμα 6.5 Κατασκευάστε τον πίνακα της πρόσθεσης και πολλαπλασιασμού για την αριθμητική modulo 5.

Λύση

ΠΡΟΣΘΕΣΗ modulo 5

$a \setminus b$	**0**	**1**	**2**	**3**	**4**
0	**0**	**1**	**2**	**3**	**4**
1	**1**	**2**	**3**	**4**	**0**
2	**2**	**3**	**4**	**0**	**1**
3	**3**	**4**	**0**	**1**	**2**
4	**4**	**0**	**1**	**2**	**3**

ΠΟΛΛΑΠΛΑΣΙΑΣΜΟΣ modulo 5

$a \setminus b$	**0**	**1**	**2**	**3**	**4**
0	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**
2	**0**	**2**	**4**	**1**	**3**
3	**0**	**3**	**1**	**4**	**2**
4	**0**	**4**	**3**	**2**	**1**

Παρατηρούμε ότι αν ο α διαιρείται από τον m και αφήνει υπόλοιπο r τότε ο a είναι **ισότιμος** με **r modulo m.**

Από τον αλγόριθμο της Ευκλείδειας Διαίρεσης το υπόλοιπο r που παίρνουμε από την διαίρεση του α με το m

ικανοποιεί την παρακάτω σχέση:

$$0 \le r < m$$

Επομένως, κάθε ακέραιος α είναι ισότιμος modulo m, με τους ακεραίους που βρίσκονται μεταξύ 0 και $m-1$.

Αυτή είναι πολύ **βασική ιδέα** που θα επανέλθουμε αργότερα. Προς το παρών ας μελετήσουμε μερικές βασικές ιδιότητες των ισοτιμιών.

Θεώρημα 6.1 Θεμελιώδεις Ιδιότητες των Ισοτιμιών Μέρος 1

Έστω m είναι ένας ακέραιος αριθμός. Για όλους τους ακεραίους a, b, c ισχύουν οι παρακάτω προτάσεις:

1. $a \equiv a \bmod m$
2. Αν $a \equiv b \bmod m$ τότε $b \equiv a \bmod m$
3. Αν $a \equiv b \bmod m$ και $b \equiv c \bmod m$ τότε $a \equiv c \bmod m$

Απόδειξη

1. Αφού $m \mid 0 = (a - a)$ τότε $a \equiv a \bmod m$.

2. Έστω ότι $a \equiv b \bmod m$. Τότε $m \mid (a-b)$. Επομένως υπάρχει ένας ακέραιος k τέτοιος ώστε $(a-b) = k \cdot m \Rightarrow (b-a) = -k \cdot m$ οπότε $m \mid (b-a)$. Άρα $b \equiv a \bmod m$.
3. Έστω $a \equiv b \bmod m$ και $b \equiv c \bmod m$. Τότε $m \mid (a-b)$ και $m \mid (b-c)$. Τότε υπάρχουν ακέραιοι k και l τέτοιοι ώστε $(a-b) = k \cdot m$ και $(b-c) = l \cdot m$.

Επομένως $(a-c) = (a-b) + (b-c) = k \cdot m + l \cdot m = (k+l) \cdot m$.

Άρα $m \mid (a-c)$. Δηλαδή $a \equiv c \bmod m$.

Θεώρημα 6.2 Θεμελιώδεις Ιδιότητες των Ισοτιμιών Μέρος 2

Έστω $a \equiv b \bmod m$ και $c \equiv d \bmod m$.Τότε ισχύουν οι παρακάτω προτάσεις:

1. $(a+c) \equiv (b+d) \bmod m$
2. $(a-c) \equiv (b-d) \bmod m$
3. $a \cdot c \equiv b \cdot d \bmod m$
4. Για όλους τους ακεραίους $n \geq 1$, $a^n \equiv b^n \bmod m$

Απόδειξη

Αφού $a \equiv b \bmod m$ τότε $m \mid (a-b)$ οπότε υπάρχει ένας ακέραιος k τέτοιος ώστε $(a-b) = k \cdot m$.

Όμοια αφού $c \equiv d \bmod m$ τότε $m \mid (c-d)$ οπότε υπάρχει ένας ακέραιος l τέτοιος ώστε $(a-b) = l \cdot m$.

1. Για να αποδείξουμε την πρώτη ισοδυναμία, παρατηρούμε το επόμενο:

$$\begin{aligned}(a+c)-(b+d) &= (a-b)+(c-d)\\ &= k \cdot m + l \cdot m\\ &= (k+l) \cdot m\end{aligned}$$

Επομένως, $m \mid (a+c)-(b+d)$. Άρα $(a+c) \equiv (b+d) \bmod m$.

2. Για να αποδείξουμε την δεύτερη ισοδυναμία, παρατηρούμε το επόμενο:

$$\begin{aligned}(a-c)-(b-d) &= (a-b)+(d-c)\\ &= k \cdot m - l \cdot m\\ &= (k-l) \cdot m\end{aligned}$$

Επομένως, $m \mid (a-c)-(b-d)$. Άρα $(a-c) \equiv (b-d) \bmod m$.

3. Για να αποδείξουμε την τρίτη ισοδυναμία, παρατηρούμε το επόμενο:

$$\begin{aligned}a \cdot c - b \cdot d &= c \cdot (a-b) + b \cdot (c-d)\\ &= c \cdot k \cdot m + b \cdot l \cdot m\\ &= (c \cdot k + b \cdot l) \cdot m\end{aligned}$$

Επομένως, $m \mid (a \cdot c - b \cdot d)$. Άρα $a \cdot c \equiv b \cdot d \bmod m$.

Θεώρημα 6.3 Αν $a \equiv b \bmod m$ τότε για κάθε ακέραιο c $(a \pm c) \equiv (b \pm c) \bmod m$ και $a \cdot c \equiv b \cdot c \bmod m$.

Απόδειξη

Αφού $m \mid (a-b)$ τότε $m \mid (a-b)+(c-c) = (a+c)-(b+c)$ και $m \mid (a-b)-(c-c) = (a-c)-(b-c)$.

Επομένως $(a \pm c) \equiv (b \pm c) \bmod m$.

Όμοια $m \mid (a-b) \cdot c = a \cdot c - b \cdot c$ Επομένως $a \cdot c \equiv b \cdot c \bmod m$.

Πόρισμα 6.4

Έστω $f(x)$ ένα πολυώνυμο με ακέραιους συντελεστές. Αν $a \equiv b \bmod m$ τότε $f(a) \equiv f(b) \bmod m$.

Απόδειξη

$f(x) = a_k \cdot x^k + a_{k-1} \cdot x^{k-1} + \ldots + a_1 \cdot x + a_0$

Όπου $a_0, a_1, \ldots, a_k$ είναι ακέραιοι. Τότε από το Θεώρημα 6.2 θα ισχύει:

$a_k \cdot a^k + a_{k-1} \cdot a^{k-1} + \ldots + a_1 \cdot a + a_0 \equiv a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \ldots + a_1 \cdot b + a_0 \bmod m$.

Επομένως, $f(a) \equiv f(b) \bmod m$.

Ας παρατηρήσουμε ότι στην γενική περίπτωση **δεν επιτρέπεται να διαιρούμε στις ισοτιμίες**.

Για παράδειγμα $15 = 3 \cdot 5 \equiv 3 \cdot 1 \bmod 6$. Αλλά $5 \not\equiv 1 \mod 6$.

Επομένως, δεν μπορούμε να διαγράψουμε τα 3άρια. Ωστόσο ισχύει $3 \cdot 4 \equiv 3 \cdot 14 \bmod 15$ και $4 \equiv 14 \bmod 5$.

Άρα σε ορισμένες περιπτώσεις μπορούμε να διαγράψουμε.

Οπότε έρχεται επακόλουθο να αναρωτηθούμε υπό ποιες συνθήκες **μπορούμε να διαγράφουμε** μέσα στις ισοτιμίες.

Θεώρημα 6.5

Έστω $a \cdot c \equiv b \cdot c \bmod m$ και $(c, m) = 1$. Τότε $a \equiv b \bmod m$.

Απόδειξη

$m \mid (a \cdot c - b \cdot c) = (a-b) \cdot c$

Αφού $(m, c) = 1$ τότε $m \mid (a-b)$.

Κεφάλαιο 7ο
Εφαρμογές στις Ισοτιμίες και η Αριθμητική των modulo

Παράδειγμα 7.1

Να βρεθεί το υπόλοιπο της διαίρεσης του 6^{1987} με το 37.

Λύση

Παρατηρούμε ότι $6^2 \equiv -1 \bmod 37$ οπότε

$$\begin{aligned} 6^{1987} &\equiv 6 \cdot 6^{1986} \bmod 37 \\ &\equiv 6 \cdot \left(6^2\right)^{993} \bmod 37 \\ &\equiv 6 \cdot (-1)^{993} \bmod 37 \\ &\equiv -6 \bmod 37 \\ &31 \bmod 37 \end{aligned}$$

Επομένως το αναμενόμενο υπόλοιπο που ψάχναμε είναι 31.

Παράδειγμα 7.2

Να αποδείξετε ότι το 7 διαιρεί $3^{2n+1} + 2^{n+2}$ για όλους τους φυσικούς αριθμούς n.

Λύση

Παρατηρούμε ότι $3^{2n+1} \equiv 3 \cdot 9^n \equiv 3 \cdot 2^n \bmod 7$ και $2^{n+2} \equiv 4 \cdot 2^n \bmod 7$.

Επομένως $3^{2n+1} + 2^{n+2} \equiv 7 \cdot 2^n \equiv 0 \bmod 7$ για όλους τους φυσικούς αριθμούς n.

Παράδειγμα 7.3

Να αποδείξετε ότι $641 \mid (2^{32} + 1)$.

Λύση

Παρατηρούμε ότι $641 = 2^7 \cdot 5 + 1 = 2^4 + 5^4$.Επομένως $2^7 \cdot 5 \equiv -1 \bmod 641$ και $5^4 \equiv -2^4 \bmod 641$.

Άρα $5^4 \cdot 2^{28} \equiv \left(5 \cdot 2^7\right)^4 \equiv (-1)^4 \bmod 641 \equiv 1 \bmod 641$. Δηλαδή $-2^4 \cdot 2^{28} = -2^{32} \equiv 1 \bmod 641$.

Αυτό όμως δηλώνει ότι: $-2^{32} - 1 \equiv 0 \bmod 641$. Οπότε $641 \mid -(2^{32} + 1)$ άρα και $641 \mid (2^{32} + 1)$.

Παράδειγμα 7.4

Να αποδείξετε ότι δεν υπάρχουν ακέραιοι που να ικανοποιούν την σχέση $x^2 - 5 \cdot y^2 = 2$.

Λύση

Έστω ότι υπάρχουν ακέραιοι που ικανοποιούν την σχέση $x^2 - 5 \cdot y^2 = 2$ τότε $\left(x^2 - 5 \cdot y^2\right) \equiv 2 \bmod 5$

και άρα $5 \cdot y^2 \equiv 0 \bmod 5$. Όμως αυτό δηλώνει ότι: $x^2 \equiv 2 \bmod 5$.

Στη συνέχεια ας θεωρήσουμε τις περιπτώσεις για το x και x^2 modulo 5.

$x \bmod ulo 5$	$x^2 \bmod ulo 5$
0	0
1	1
2	4
3	4
4	1

Επομένως δεν υπάρχει κανένα x τέτοιο ώστε το x^2 να είναι **ισότιμο** με το 2 modulo 5, οπότε δεν υπάρχουν ακέραιοι x και y τέτοιοι ώστε $x^2 - 5 \cdot y^2 = 2$.

Παράδειγμα 7.5

Να βρείτε το ψηφίο των μονάδων του αριθμού 7^{100} (παράδειγμα για τον αριθμό 723 το ψηφίο των μονάδων είναι το 3).

Λύση

Για να βρούμε το ψηφίο των μονάδων του 7^{100} θα πρέπει να βρούμε το 7^{100} modulo 10.

$$7^2 \equiv -1 \bmod 10$$
$$7^3 \equiv 7 \cdot 7^2 \bmod 10$$
$$\equiv -7 \bmod 10$$
$$7^4 \equiv (7^2)^2 \bmod 10$$
$$\equiv (-1)^2 \bmod 10$$
$$\equiv 1 \bmod 10$$
$$7^{100} \equiv \left(7^4\right)^{25} \bmod 10$$
$$\equiv 1^{25} \bmod 10$$
$$\equiv 1 \bmod 10$$

Επομένως, το ψηφίο των μονάδων του αριθμού 7^{100} είναι το 1.

Παράδειγμα 7.6

Να βρείτε άπειρους ακεραίους n τέτοιους ώστε $2^n + 27$ να διαιρείται με το 7.

Λύση

Παρατηρούμε ότι

$$2^1 \equiv 2 \bmod 7$$
$$2^2 \equiv 4 \bmod 7$$
$$2^3 \equiv 1 \bmod 7$$
$$2^4 \equiv 2 \bmod 7$$
$$2^5 \equiv 4 \bmod 7$$
$$2^6 \equiv 1 \bmod 7$$

Οπότε, $2^{3k} \equiv \left(2^3\right)^k \equiv 1^k \bmod 7$ για όλους τους θετικούς ακεραίους k.

Επομένως, $2^{3k} + 27 \equiv 1 + 27 \equiv 28 \equiv 0 m \bmod 7$ για όλους τους θετικούς ακεραίους k, $7 \mid 2^{3k} + 27$

άρα $2^n + 27$ διαιρείται από το 7 για όλα τα θετικά πολλαπλάσια του 3.

Παράδειγμα 7.7

Να αποδείξετε ότι ο $2^k - 5$ για $k = 0, 1, 2, \ldots.$ δεν αφήνει ποτέ υπόλοιπο 1 όταν διαιρεθεί με το 7.

Λύση

Παρατηρούμε ότι

$2^1 \equiv 2 \bmod 7$

$2^2 \equiv 4 \bmod 7$

$2^3 \equiv 1 \bmod 7$

Και αυτός ο κύκλος θα επαναλαμβάνετε για κάθε k $2^k \equiv$ 2, 4, ή 1 mod 7. Άρα $\left(2^k - 5\right) \equiv$ -3, -1, $-4 \mod 7$. Οπότε ο $2^k - 5$ αφήνει υπόλοιπα μόνο 3, 4 και 6 όταν διαιρεθεί με το 7.

Παράδειγμα 7.8

Να αποδείξετε ότι ένας θετικός ακέραιος n διαιρείται από το 3 αν και μόνο αν το άθροισμα των ψηφίων του διαιρείται από το 3.

Λύση

Θα αποδείξουμε ότι ο n και το άθροισμα των ψηφίων είναι ισότιμοι modulo 3.

Ας υποθέσουμε ότι ο θετικός ακέραιος n γράφετε όπως παρακάτω (δεκαδικό του ανάπτυγμα)

$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.

Παρατηρούμε ότι $10 \equiv 1 \bmod 3$ και $10^m \equiv 1^m \equiv 1 \bmod 3$ για κάθε ακέραιο m.

Οπότε,

$$n \equiv a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \bmod 3$$
$$\equiv a_k \cdot 1 + a_{k-1} \cdot 1 + \ldots + a_2 \cdot 1 + a_1 \cdot 1 + a_0 \bmod 3$$
$$\equiv a_k + a_{k-1} + \ldots + a_2 + a_1 + a_0 \bmod 3$$

Άρα το υπόλοιπο που παίρνουμε όταν ο n διαιρείται με το 3 είναι το ίδιο με το υπόλοιπο που παίρνουμε όταν το άθροισμα των ψηφίων του το διαιρέσουμε με το 3, οπότε ο n διαιρείται με το 3 αν και μόνο αν το άθροισμα των ψηφίων του διαιρείται με το 3.

Κεφάλαιο 8ο
Γραμμικές Εξισώσεις Ισοτιμίας

Ορισμός 8.1 Μια εξίσωση της μορφής $\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + ... + \alpha_k \cdot x_k \equiv b \bmod m$ με αγνώστους $x_1, x_2, ..., x_k$

Είναι μια **γραμμική εξίσωση ισοτιμίας** με k μεταβλητές.

Μια **λύση** στην παραπάνω εξίσωση είναι ένα σύνολο ακεραίων που ικανοποιούν την παραπάνω εξίσωση.

Παράδειγμα 8.1 $x = 1$, $y = 2$, $z = 3$ είναι μια λύση στην γραμμική εξίσωση ισοτιμίας

$$x + y + z \equiv 6 \bmod 7$$

Παράδειγμα 8.2 Να λυθεί η εξίσωση ισοτιμίας $x + 12 \equiv 5 \bmod 8$.

Λύση

Το κλειδί σε αυτή την εξίσωση είναι να παρατηρήσουμε ότι μπορούμε να αφαιρέσουμε το 12 και από τα 2 μελή της ισοτιμίας (σύμφωνα με το θεώρημα 6.2).

$$x + 12 \equiv 5 \bmod 8$$
$$x \equiv (5 - 12) \bmod 8$$
$$x \equiv -7 \bmod 8$$
$$x \equiv 1 \bmod 8$$

Επομένως κάθε ακέραιος x που είναι ισότιμος με $1 \bmod ulo 8$ ικανοποιεί την παραπάνω ισοτιμία.

Παράδειγμα 8.3 Να λυθεί η ισοτιμία $4 \cdot x \equiv 3 \bmod 19$.

Λύση

Αρχικά, παρατηρούμε ότι **δεν μπορούμε απλά να διαιρέσουμε** και τα 2 μέλη της ισοτιμίας με 4.

Ωστόσο, από το Θεώρημα 6.2 μπορούμε να πολλαπλασιάσουμε και τα δυο μέλη της ισοτιμίας με 5.

Οπότε, $4 \cdot x \equiv 3 \bmod 19$

$20 \cdot x \equiv 15 \bmod 19$

$x \equiv 15 \bmod 19$ αφού $20 \equiv 1 \bmod 19$.

Άρα κάθε ακέραιος x που είναι ισότιμος με το 15 modulo 19 θα ικανοποιεί την ισοτιμία.

Μπορούμε φυσικά να ελέγξουμε την απάντηση μας αντικαθιστώντας το 15 στην αρχική ισοτιμία. Πράγματι $4 \cdot 15 = 60 \equiv 3 \bmod 19$.

Παράδειγμα 8.4 Να λυθεί η παρακάτω εξίσωση ισοτιμίας $x^2 + 2 \cdot x - 1 \equiv 0 \bmod 7$.

Λύση

Η παραπάνω εξίσωση δεν είναι γραμμική αλλά υλοποίει μια βασική αρχή.

Εφόσον δεν είμαστε σίγουροι πώς να προσεγγίσουμε την παραπάνω ισοτιμία, μπορούμε απλά να δοκιμάσουμε συγκεκριμένες τιμές $x = 0, x = 1, x = ..., x = 6$. Στην γενική περίπτωση για να λύσουμε μια εξίσωση ισοτιμίας modulo m, μπορούμε να δοκιμάζουμε τιμές $0, 1, 2, ..., m-1$ για κάθε μεταβλητή.

Για την ισοτιμία $x^2 + 2 \cdot x - 1 \equiv 0 \bmod 7$ βρίσκουμε τις λύσεις $x \equiv 2 \bmod 7$ και $x \equiv 3 \bmod 7$.

Προφανώς υπάρχουν και άλλες λύσεις όπως $x \equiv 9 \bmod 7$, αλλά παρατηρούμε ότι 9 και 2 δεν είναι στην πραγματικότητα διαφορετικές λύσεις καθώς είναι ισότιμες modulo 2.

Όταν μας ρωτάνε να βρούμε όλες τις λύσεις μιας ισοτιμίας, ουσιαστικά μας ζητάνε να βρούμε όλες τις λύσεις που δεν είναι ισότιμες μεταξύ τους.

Παράδειγμα 8.5 Να λυθεί η παρακάτω εξίσωση ισοτιμίας $x^2 \equiv 3 \bmod 4$.

Λύση

$x \bmod ulo 4$	$x^2 \bmod ulo 4$
0	**0**
1	**1**
2	**0**
3	**1**

Επομένως, η ισοτιμία $x^2 \equiv 3 \bmod 4$ δεν έχει λύσεις. Ας θεωρήσουμε την γραμμική εξίσωση ισοτιμίας $a \cdot x \equiv b \bmod m$. Θέλουμε να καθορίσουμε πότε αυτή η ισοτιμία έχει λύση και πότε είναι μοναδική. Όταν υπάρχει μόνο μια λύση modulo m, τότε λέμε ότι η λύση είναι μοναδική. Πριν αναφέρουμε μερικά θεωρήματα ας μελετήσουμε ορισμένα παραδείγματα.

Παράδειγμα 8.6 Να λυθεί η παρακάτω εξίσωση ισοτιμίας $6 \cdot x \equiv 15 \bmod 514$.

Λύση

Αν x είναι μια λύση της παραπάνω ισοτιμίας τότε $514 \mid (6 \cdot x - 15)$.

Ας παρατηρήσουμε ότι ο 514 είναι άρτιος, ο $6 \cdot x$ είναι άρτιος και ο $6 \cdot x - 15$ είναι περιττός.

Τότε ο $6 \cdot x - 15$ δεν μπορεί να διαιρεθεί με το 514, επομένως η παραπάνω ισοτιμία δεν έχει λύσεις. Επιπλέον ας παρατηρήσουμε (για μελλοντική χρήση) ότι $\text{ΜΚΔ}(6, 514) = 2$ και $2 \nmid 15$.

Παράδειγμα 8.7 Να λυθεί η παρακάτω εξίσωση ισοτιμίας $3 \cdot x \equiv 5 \bmod 7$.

Λύση

Αν δοκιμάσουμε τις τιμές $x = 0,1,2,3,4,5,6$ βρίσκουμε ότι $x \equiv 4 \bmod 7$ είναι η μοναδική λύση σε αυτή την ισοτιμία. Ας παρατηρήσουμε (για μελλοντική χρήση) ότι $\text{ΜΚΔ}(3,7) = 1$ και $1 \nmid 5$.

Παράδειγμα 8.8 7 Να λυθεί η παρακάτω εξίσωση ισοτιμίας $9 \cdot x \equiv 15 \bmod 21$.

Λύση

Αν δοκιμάσουμε τις τιμές $x = 0,1,2...,21$ βρίσκουμε ότι $x \equiv 4,11,18 \bmod 21$ είναι τρείς λύσεις στην παραπάνω ισοτιμία. Ας παρατηρήσουμε (για μελλοντική χρήση) ότι $\text{ΜΚΔ}(9,21) = 3$ και $3 | 15$.

Παράδειγμα 8.9 Ας υποθέσουμε ότι θέλουμε να λύσουμε μια αυθαίρετη γραμμική εξίσωση ισοτιμίας της μορφής $a \cdot x \equiv b \bmod m$. Τότε θα πρέπει να βρούμε έναν ακέραιο x τέτοιον ώστε $m | (a \cdot x - b)$.

Ισοδύναμα πρέπει να βρούμε έναν ακέραιο y τέτοιο ώστε $m \cdot y = a \cdot x - b$, δηλαδή $a \cdot x - m \cdot y = b$.

Αυτός ο τύπος της εξίσωσης πρέπει να μας φαίνετε γνωστός αφού τέτοιος τύπος εξίσωσης λύθηκε σε προηγούμενο κεφάλαιο.

Έστω $g = (a,m)$. Γνωρίζουμε ότι κάθε αριθμός της μορφής $a \cdot x - m \cdot y$ είναι πολλαπλάσιο του g (αφού $g | a$ και $g | m$), επομένως αν $g \nmid a$ τότε η εξίσωση $a \cdot x - m \cdot y = b$ δεν έχει λύσεις.

Στη συνέχεια υποθέτουμε ότι $g | b$.

Από το κεφάλαιο 5.1 υπάρχουν ακέραιοι u και v τέτοιοι ώστε $a \cdot u + m \cdot v = g$.

Αφού $g | b$ μπορούμε να πολλαπλασιάσουμε αυτή την εξίσωση με τον ακέραιο b / g οπότε και παίρνουμε την εξίσωση $a \cdot \frac{b \cdot u}{g} - m \cdot \frac{b \cdot v}{g} = b$.

Το παραπάνω όμως δηλώνει ότι $m | a \cdot \frac{b \cdot u}{g} - b$.

Επομένως $a \cdot \frac{b \cdot u}{g} \equiv b \bmod m$.

Δηλαδή το $x_o \equiv \frac{b \cdot u}{g} \bmod m$ είναι μια λύση της ισοτιμίας $a \cdot x \equiv b \bmod m$.

Άρα αποδείξαμε ότι αν $g = (a,m) | b$ τότε το $x_o \equiv \frac{b \cdot u}{g} \bmod m$ είναι λύση της ισοτιμίας.

Σε αυτό το σημείο είναι επακόλουθο να θεωρήσουμε αν το x_o είναι η μοναδική ή όχι λύση της

ισοτιμίας.

Ας υποθέσουμε ότι x_1 είναι μια άλλη λύση της ισοτιμίας $ax \equiv b \bmod m$, τότε $ax_1 \equiv ax_o \bmod m$.

Επομένως, $m \mid (a \cdot x_1 - a \cdot x_o) = a \cdot (x_1 - x_o)$.

Αυτό όμως φανερώνει ότι $\frac{m}{g}$ διαιρεί $\frac{a \cdot (x_1 - x_0)}{g}$. Όμως, $(a, m) = g$ οπότε $\left(\frac{a}{g}, \frac{m}{g}\right) = 1$.

Άρα a / g και m / g και δεν έχουν κοινούς παράγοντες, οπότε m / g πρέπει να διαιρεί $x_1 - x_o$.

Άρα υπάρχει ακέραιος k τέτοιος ώστε $k \cdot \frac{m}{g} = x_1 - x_o$ ή $x_1 = x_o + k \cdot \frac{m}{g}$.

Τέλος υπενθυμίζουμε ότι κάθε 2 λύσεις που διαφέρουν κατά ένα πολλαπλάσιο του m, θεωρούνται ότι είναι οι ίδιες, επομένως υπάρχουν ακριβώς g διαφορετικές λύσεις οι οποίες και προκύπτουν λαμβάνοντας τιμές το $k = 0, 1, ..., g-1$. Ας παρατηρήσουμε ότι αν $g = (a, m) = 1$ τότε θα υπάρχει ακριβώς μια λύση από την ισοτιμία $a \equiv b \bmod m$.

Στη συνέχεια συνοψίζουμε όλα τα παραπάνω στο παρακάτω θεώρημα.

Θεώρημα 8.1 Λύσεις Γραμμικών Εξισώσεων Ισοτιμίας

Ας υποθέσουμε a, b και m είναι ακέραιοι με $m \geq 1$. Έστω $g = (a, m)$.

(α) Αν g ∤ b τότε η ισοτιμία $a \cdot x \equiv b \bmod m$ δεν έχει λύσεις.

(β) Αν $g \mid b$ τότε η ισοτιμία $a \cdot x \equiv b \bmod m$ έχει g μη-ισότιμες λύσεις.

Για να βρεθούν οι λύσεις, πρώτα βρίσκουμε ακέραιους u και v που ικανοποιούν την παρακάτω σχέση $a \cdot u + m \cdot v = g$.

Όπως περιγράψαμε και στο κεφάλαιο 2 ο ευκλείδειος αλγόριθμος μπορεί να χρησιμοποιηθεί για να βρούμε ακεραίους u και v.

Τότε $x_o = \frac{b \cdot u}{g}$ είναι μια λύση της ισοτιμίας $a \cdot x \equiv b \bmod m$.

Οι μη-ισότιμες λύσεις που είναι σε πλήθος g δίνονται από τον παρακάτω τύπο:

$x \equiv x_o + k \cdot \frac{m}{g} \bmod m$ για $k = 0, 1, 2, ..., g-1$.

Παράδειγμα 8.10 Να βρείτε όλες τις λύσεις της παρακάτω ισοτιμίας

$$943 \cdot x \equiv 381 \bmod 2576.$$

Λύση

$g = (943, 2576) = 23 \nmid 381$ οπότε η ισοτιμία δεν έχει λύσεις.

Παράδειγμα 8.11 Να βρείτε όλες τις λύσεις της παρακάτω ισοτιμίας $8 \cdot x \equiv 7 \bmod 13$.

Λύση

$g = (8,13) = 1$ επομένως υπάρχει $g = 1$ λύση της ισοτιμίας. Ας παρατηρήσουμε ότι είμαστε σε θέση να καθορίσουμε το πλήθος των λύσεων χωρίς να υπολογίσουμε τις λύσεις.

Για να βρούμε την λύση αρχικά θα πρέπει να βρούμε ακεραίους u και v τέτοιους ώστε $8 \cdot u + 13 \cdot v = 1$

Χρησιμοποιώντας μεθόδους από το Κεφάλαιο 5, βρίσκουμε τη λύση $u = 5$ και $v = -3$.

Επομένως $x_o = \frac{7 \cdot 5}{1} = 35 \equiv 9 \bmod 13$ είναι η λύση της ισοτιμίας.

Παράδειγμα 8.12 Να βρείτε όλες τις λύσεις της ισοτιμίας $6 \cdot x \equiv 9 \bmod 15$

Λύση

$g = (6,15) = 3 \mid 9$ επομένως υπάρχουν $g = 3$ μη ισότιμες λύσεις της παραπάνω ισοτιμίας.

Ας παρατηρήσουμε ότι είμαστε σε θέση να καθορίσουμε τον αριθμό των λύσεων χωρίς να τις υπολογίσουμε.

Για να βρούμε την λύση αρχικά θα πρέπει να βρούμε ακεραίους u και v τέτοιους ώστε $6 \cdot u + 15 \cdot v = 3$.

Χρησιμοποιώντας μεθόδους από το Κεφάλαιο 3, βρίσκουμε τη λύση $u = -2$ και $v = 1$.

Επομένως, $x_o = \frac{9 \cdot (-2)}{3} = -6 \equiv 9 \bmod 15$ είναι η λύση της ισοτιμίας. Για να υπολογίσουμε όλες τις λύσεις, ξεκινάμε με $x_o = 9$ και προσθέτουμε πολλαπλάσια της ποσότητας $\frac{15}{3} = 5$.

Οπότε οι 3 μη ισότιμες λύσεις είναι 9, 14, 4.

Στην συνέχεια θα θεωρήσουμε ότι έχουμε παραπάνω από μια εξίσωση ισοτιμίας με έναν άγνωστο.

Παράδειγμα 8.13

Να λυθεί το σύστημα των ισοτιμιών

$$x \equiv 2 \bmod 4$$
$$x \equiv 1 \bmod 6$$

Λύση

Δεν υπάρχει καμία κοινή λύση στις δύο παραπάνω ισοτιμίες καθώς η πρώτη ισοτιμία απαιτεί το x να είναι περιττός και η δεύτερη ισοτιμία απαιτεί το x να είναι άρτιος.

Παράδειγμα 8.14

Να λυθεί το σύστημα των ισοτιμιών

$x \equiv 2 \bmod 4$

$x \equiv 3 \bmod 5$

Λύση

Παρατηρούμε ότι $x = 18$ είναι μια κοινή λύση. Για να βρούμε όλες τις λύσεις του συστήματος, προχωράμε όπως παρακάτω.

Η πρώτη ισοτιμία επαληθεύεται από το x αν και μόνο αν $x \mid (x-2)$, δηλαδή $x = 2 + 4 \cdot k$.

Αντικαθιστώντας το x στην δεύτερη ισοτιμία έχουμε $2 + 4 \cdot k \equiv 3 \bmod 5$, δηλαδή $4 \cdot k \equiv 1 \bmod 5$.

Στη συνέχεια παρατηρούμε ότι $k \equiv 1 \bmod 5$ είναι η μόνη λύση της παραπάνω ισοτιμίας.

Επομένως k είναι λύση της $2 + 4 \cdot k \equiv 3 \bmod 5$ αν και μόνο αν το k μπορεί να γραφεί στη μορφή $k = 4 + 5 \cdot j$,

όπου j είναι ένας ακέραιος. Επομένως x ικανοποιεί και τις δυο ισοτιμίες αν και μόνο αν υπάρχει ένας ακέραιος *j* τέτοιος ώστε $x = 2 + 4 \cdot (4 + 5 \cdot j) = 20 \cdot j + 18$.

Επομένως, η μοναδική λύση του συστήματος των ισοτιμιών είναι $x \equiv 18 \bmod 20$.

Αυτά που παρατηρήσαμε σε αυτό το παράδειγμα είναι ένα πιο γενικό παράδειγμα που περιγράφεται στο παρακάτω θεώρημα.

Θεώρημα 8.2

Αν $(m,n) = 1$ τότε οι ισοτιμίες

$x \equiv a \bmod m$

$x \equiv b \bmod n$

έχουν μια μοναδική κοινή λύση modulo $m \cdot n$.

Απόδειξη

Η πρώτη ισοτιμία έχει λύση αν και μόνο αν $x \mid (x-a)$, δηλαδή αν και μόνο αν υπάρχει ένας ακέραιος k τέτοιος ώστε $x = a + m \cdot k$.

Τότε η δεύτερη ισοτιμία γίνεται $m \cdot k = (b-a) \bmod n$.

Αφού $(m,n) = 1$ αυτή η ισοτιμία έχει μοναδική λύση modulo n, με άλλα λόγια $k \equiv c \bmod n$.

Επομένως, το k ικανοποιεί την $m \cdot k \equiv (b-a) \bmod n$ αν και μόνο αν υπάρχει ακέραιος *j* τέτοιος ώστε $k = c + n \cdot j$, όπου j είναι ένας ακέραιος.

Οπότε $x = a + m \cdot k = a + m \cdot (c + n \cdot j) = a + m \cdot c + m \cdot n \cdot k \equiv a + m \cdot c \bmod m \cdot n$.

Όλες οι λύσεις είναι ισότιμες με $(a + m \cdot c) \bmod m \cdot n$, επομένως υπάρχει μια μοναδική λύση modulo $m \cdot n$. Αυτό το αποτέλεσμα είναι μια ειδική περίπτωση ενός πιο γενικού Θεωρήματος.

Ο **Sun Tzu ή Sun Zi** ήτανε ένας κινέζος μαθηματικός και έγινε γνωστός για την συγγραφή του **Sun Tzu's Υπολογισμοί** τον $4^{ο}$ αιώνα όπου περιέχει το Κινέζικο Θεώρημα των Υπολοίπων και με βάση αυτό το θεώρημα επιλύεται το εξής πρόβλημα: Πόσοι στρατιώτες υπάρχουν στην μεραρχία του Han Xing's;

Αν παρατάξουμε τους στρατιώτες σε ομάδες των τριών στρατιωτών η κάθε ομάδα θα περισσεύσουν 2 στρατιώτες. Αν παρατάξουμε τους στρατιώτες σε γραμμές των 5 στρατιωτών η κάθε γραμμή τότε θα περισσεύσουν 3 στρατιώτες. Αν παρατάξουμε τους στρατιώτες σε γραμμές των 7 στρατιωτών η κάθε γραμμή τότε θα περισσεύσουν 2 στρατιώτες.

Θεώρημα 8.3 Κινέζικο Θεώρημα Υπολοίπων

Έστω $m_1, m_2, ..., m_k$ είναι θετικοί ακέραιοι που είναι σχετικά πρώτοι ανά δύο. Τότε οι παρακάτω k ισοτιμίες

$x \equiv a_1 \bmod m_1$
$x \equiv a_2 \bmod m_2$
...
$x \equiv a_k \bmod m_k$

έχουν μοναδική λύση modulo $m_1 \cdot m_2 \cdots m_k$ **.**

Παράδειγμα 8.15

Να βρεθεί αριθμός τέτοιος ώστε όταν διαιρεθεί με το 4 να αφήνει υπόλοιπο 2, όταν διαιρεθεί με το 5 να αφήνει υπόλοιπο 1, ενώ όταν διαιρεθεί με το 7 να αφήνει υπόλοιπο 1.

Λύση

Θέλουμε να βρούμε ένα n τέτοιο ώστε:

$n \equiv 2 \bmod 4$
$n \equiv 1 \bmod 5$
$n \equiv 1 \bmod 7$

Αυτό όμως σημαίνει ότι:

$35 \cdot n \equiv 70 \bmod 140$
$28 \cdot n \equiv 28 \bmod 140$
$20 \cdot n \equiv 20 \bmod 140$

Έχουμε όμως, ότι $n \equiv 3 \cdot (35 \cdot n - 28 \cdot n) - 20 \cdot n \equiv 3 \cdot (70 - 28) - 20 \equiv 106 \bmod 140$ **.**

Επομένως, όλα τα $n \equiv 106 \bmod 140$ ικανοποιούν τις παραπάνω συνθήκες.

Κεφάλαιο 9
Euler's Phi-Συνάρτηση και το Θεώρημα Euler-Fermat

Ορισμός 9.1 Για $n \geq 1$, έστω $\varphi(n)$ είναι το πλήθος των θετικών ακεραίων που είναι μικρότεροι ή ίσοι του n και σχετικά πρώτοι με το n.

Παράδειγμα 9.1 $\varphi(6) = 2$ αφού ο 1 και ο 5 είναι οι μόνοι ακέραιοι που είναι μικρότεροι ή ίσοι με το 6 και είναι σχετικά πρώτοι με το 6.

Παράδειγμα 9.2 Να βρείτε την τιμή του $\varphi(m)$ για κάθε m που εμφανίζετε στον παρακάτω πίνακα.

M	1	2	3	4	5	6	7	8	9	10
ϕ(m)										

Θεώρημα 9.1 Για κάθε πρώτο p ισχύει $\varphi(\mathrm{p}) = \mathrm{p} - 1$ καθώς κάθε θετικός ακέραιος μικρότερος από τον πρώτο p είναι σχετικά πρώτος με το p.

Παράδειγμα 9.3

1. Έστω m = 6. Υπολογίζουμε το $a^{\varphi(m)} \bmod m$ για $a = 1$ και $a = 5$.
2. Έστω m = 9. Υπολογίζουμε το $a^{\varphi(m)} \bmod m$ για $a = 1$, $a = 2, a = 4$, $a = 5, a = 7, a = 8$.
3. Έστω m = 10. Υπολογίζουμε το $a^{\varphi(m)} \bmod m$ για $a = 1$, $a = 3, a = 7, a = 9$.

Βασιζόμενοι στα παραπάνω αριθμητικά αποτελέσματα του παραδείγματος 9.3 καταλήγουμε στο παρακάτω συμπέρασμα:

Θεώρημα 9.1 Euler's-Fermat

Αν $(a, m) = 1$ τότε $a^{\varphi(m)} \equiv 1 \bmod m$.

Απόδειξή

Η απόδειξη του Θεωρήματος Euler's-Fermat είναι παρόμοια απόδειξη με το Μικρό Θεώρημα του Fermat.

Παρατηρούμε ότι το Μικρό Θεώρημα του Fermat είναι ειδική περίπτωση του Θεωρήματος Euler's-Fermat: Αν p είναι πρώτος τότε ϕ(p) = p – 1.

Για να χρησιμοποιήσουμε το Θεώρημα Euler's-Fermat σε προβλήματα και εφαρμογές χρειαζόμαστε μια αποτελεσματική μέθοδο για να υπολογίζουμε το ϕ(m) για τυχαίο ακέραιο m

όχι απαραίτητα πρώτο.

Αν ο m είναι μικρός τότε είναι σχετικά εύκολο να βρούμε όλους τους αριθμούς που είναι μικρότεροι ή ίσοι του m και είναι σχετικά πρώτοι με τον m.

Ωστόσο αν ο m είναι μεγάλος αριθμός δεν θέλουμε να γράψουμε όλους τους ακεραίους που είναι μικρότεροι ή ίσοι του m και να καθορίσουμε ποιος είναι σχετικά πρώτος με τον m και ποιος δεν είναι.

Στην συνέχεια θα περιγράψουμε την μέθοδο για να υπολογίζουμε το φ(m) χωρίς να γράφουμε όλους τους ακεραίους που είναι μικρότεροι ή ίσοι του m και να καθορίσουμε ποιος είναι σχετικά πρώτος με τον m και ποιος δεν είναι.

Αρχικά θα θεωρήσουμε δυνάμεις πρώτων αριθμών.

Θεώρημα 9.3 Αν p είναι πρώτος αριθμός τότε:

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k \cdot \left(1 - \frac{1}{p}\right).$$

Απόδειξη

Από τον τρόπο που ορίσαμε την συνάρτηση φ έχουμε ότι $\varphi(p^k)$ είναι το πλήθος των ακεραίων που είναι μικρότεροι ή ίσοι με τον p^k και είναι σχετικά πρώτοι με τον p^k.

Υπάρχουν p^k ακέραιοι που είναι μικρότεροι ή ίσοι με τον p^k. Επομένως,

$\varphi(p^k) = p^k -$ (αριθμός των ακεραίων $\le p^k$ που δεν είναι σχετικά πρώτοι με τον p^k).

Οι ακέραιοι που είναι μικρότεροι ή ίσοι με τον p^k και δεν είναι σχετικά πρώτοι με τον p^k είναι ακριβώς οι ακέραιοι που διαιρούνται με το p.

Υπάρχουν p^{k-1} τέτοιοι ακέραιοι: $1 \cdot p, 2 \cdot p, 3 \cdot p, ..., p \cdot p^{k-1}$.

Οπότε, $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k \cdot \left(1 - \frac{1}{p}\right)$.

Παράδειγμα 9.4

1. Να υπολογίσετε τις τιμές $\varphi(6), \varphi(2)$ και $\varphi(3)$. Με ποιο τρόπο σχετίζονται μεταξύ τους οι τιμές $\varphi(6), \varphi(2)$ και $\varphi(3)$;
2. Να υπολογίσετε τις τιμές $\varphi(10), \varphi(2)$ και $\varphi(5)$. Με ποιο τρόπο σχετίζονται μεταξύ τους οι τιμές $\varphi(10), \varphi(2)$ και $\varphi(5)$;
3. Να υπολογίσετε τις τιμές $\varphi(30), \varphi(5)$ και $\varphi(6)$. Με ποιο τρόπο σχετίζονται μεταξύ τους οι τιμές $\varphi(30), \varphi(5)$ και $\varphi(6)$;
4. Να υπολογίσετε τις τιμές $\varphi(72), \varphi(8)$ και $\varphi(9)$. Με ποιο τρόπο σχετίζονται μεταξύ τους οι

τιμές $\varphi(72), \varphi(8)$ και $\varphi(9)$;

Θεώρημα 9.4

Αν $(a,b)=1$ τότε $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$.

Απόδειξη

Έστω n είναι ένας φυσικός αριθμός τέτοιος ώστε $n=a\cdot b$ με $(a,b)=1$. Αλλάζουμε τους ab ακεραίους $1,2,...,ab$ όπως φαίνετε παρακάτω:

1	2	3	$...$	k	$...$	a
$a+1$	$a+2$	$a+3$	$...$	$a+k$	$...$	$2a$
$2a+1$	$2a+2$	$2a+3$	$...$	$2a+k$	$...$	$3a$
$...$	$...$	$...$	$...$	$...$	$...$	$...$
$(b-1)a+1$	$(b-1)a+2$	$(b-1)a+3$	$...$	$(b-1)a+k$	$...$	ba

Ένας ακέραιος r είναι σχετικά πρώτος με το m αν και μόνο αν είναι σχετικά πρώτος με τα a και b.

Στη συνέχεια θα καθορίσουμε τον αριθμό των ακεραίων στον παραπάνω πίνακα που είναι σχετικά πρώτοι με τον a και θα βρούμε πόσοι από αυτούς είναι σχετικά πρώτοι με το b.

Υπάρχουν $\varphi(a)$ ακέραιοι σχετικά πρώτοι με τον a στην πρώτη γραμμή του παραπάνω πίνακα.

Ας θεωρήσουμε την $k-οστή$ στήλη με $1\le k\le a$. Κάθε ακέραιος σε αυτή την στήλη είναι της μορφής $m\cdot a+k$ με $0\le m\le b-1$. Αφού $k\equiv m\cdot a+k \bmod a$ ο k έχει κοινό παράγοντα με τον a αν και μόνο αν έχει κοινό παράγοντα ο $m\cdot a+k$. Αυτό σημαίνει ότι υπάρχουν ακριβώς $\varphi(\alpha)$ στήλες ακεραίων που είναι σχετικά πρώτοι με τον a. Πρέπει να καθορίσουμε πόσοι από αυτούς τους ακεραίους είναι σχετικά πρώτοι με τον b.

Ισχυριζόμαστε ότι από την $k-οστή$ στήλη με τους ακεραίους $k, a+k, 2a+k, ..., (b-1)a+k$ δεν έχουμε 2 ακεραίους που είναι ισότιμοι modulo b.

Έστω ότι $(ia+k)\equiv(ja+k) \bmod b$ τότε $a(i-j)\equiv 0 \bmod b$.

Επομένως, $b\mid a(i-j)$ οπότε $b\mid a$ ή $b\mid(i-j)$.

Αφού $(a,b)=1$ και $b\nmid a$ τότε $b\mid(i-j)$ δηλαδή $(i-j)\equiv 0 \bmod b$.

Αφού $i,j\in[0,b-1]$ προκύπτει ότι $|i-j|<b$.

Ωστόσο ο μόνος ακέραιος $(i-j)$ τέτοιος ώστε $|i-j|<b$ και $b\mid(i-j)$ είναι ο 0.

Αυτό όμως δηλώνει ότι $i-j=0\Rightarrow i=j$.

Αυτό σημαίνει ότι οι ακέραιοι που είναι b σε πλήθος σε οποιαδήποτε από τις $\varphi(n)$ στήλες είναι ισότιμοι με τους ακεραίους $0,1,...,b-1$.

Αλλά ακριβώς $\varphi(b)$ από αυτούς είναι σχετικά πρώτοι με το b.

Αυτό σημαίνει ότι ακριβώς $\varphi(a)\cdot\varphi(b)$ ακέραιοι στον παραπάνω πίνακα είναι σχετικά πρώτοι με το ab.

Επομένως, $\varphi(n)=\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$.

Παρατήρηση

Ονομάζουμε μια συνάρτηση $f:\mathbb{N}^+\to\mathbb{N}$ **πολλαπλασιαστική** αν $f(m\cdot n)=f(m)f(n)$ για κάθε ζεύγος ακέραιων m,n τέτοιοι ώστε $(m,n)=1$.

Επομένως από το **θεώρημα 9.4** η phi-συνάρτηση του Euler είναι **πολλαπλασιαστική**.

Χρησιμοποιώντας τα Θεωρήματα 9.3 και 9.4 μπορούμε να έχουμε έναν γενικό τύπο για το $\varphi(n)$.

Θεώρημα 9.5

Έστω $n=p_1^{a_1}\cdot p_2^{a_2}\cdots p_m^{a_m}$ είναι το γινόμενο πρώτων παραγόντων του n, όπου $p_1,p_2,\cdots,p_m$ είναι διαφορετικοί μεταξύ τους πρώτοι ακέραιοι και $a_1,a_2,\cdots,a_m$ είναι ακέραιοι μεγαλύτεροι ή ίσοι του 1. Τότε

$$\varphi(n)=\left(p_1^{a_1}-p_1^{a_1-1}\right)\cdot\left(p_2^{a_2}-p_2^{a_2-1}\right)\cdots\left(p_m^{a_m}-p_m^{a_m-1}\right)=$$
$$=n\cdot\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right)$$

Παράδειγμα 9.5

Να βρείτε το $\varphi(100)$.

Λύση

Δεν είναι αναγκαίο να καταγράψουμε τους ακεραίους που είναι μικρότεροι ή ίσοι του 100 και να καθορίσουμε ποίοι από αυτούς είναι σχετικά πρώτοι με το 100. Αντί γι αυτό χρησιμοποιούμε το Θεώρημα 9.5. Η ανάλυση του 100 σε γινόμενο πρώτων παραγόντων είναι $100=2^2\cdot5^2$.

Επομένως $\varphi(100)=100\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{5}\right)=40$.

Παράδειγμα 9.6

Να βρείτε άπειρους ακεραίους n τέτοιους ώστε $10\mid\varphi(n)$.

Λύση

Για $n=11^k$ με $k=1,2,\ldots.$ τότε $\varphi(11^k)=11^k-11^{k-1}=10\cdot11^{k-1}$ οπότε $10\mid\varphi(11^k)$ για $k\geq1$.

Παράδειγμα 9.7

Να βρείτε τα 2 τελευταία ψηφία του 3^{1000}.

Λύση

Για να βρούμε τα 2 τελευταία ψηφία του 3^{1000} χρειάζεται να υπολογίσουμε $3^{1000} \bmod ulo 100$.

Γνωρίζουμε ότι $\varphi(100) = \varphi(2^2)\varphi(5^2) = 40$ οπότε, από το Θεώρημα Fermat- Euler προκύπτει $3^{40} \equiv 1 \bmod 100$.

Άρα $3^{1000} = \left(3^{40}\right)^{25} \equiv 1^{25} = 1 \bmod 100$. Επομένως, τα 2 τελευταία ψηφία του 3^{1000} είναι 01.

Παράδειγμα 9.8

Να βρείτε τα 2 τελευταία ψηφία του $7^{7^{1000}}$.

Λύση

Παρατηρούμε ότι $7^{40} \equiv 1 \bmod 100$

$\varphi(40) = 16$ επομένως, $7^{16} \equiv 1 \bmod 40$

$7^{1000} \equiv \left(7^{16}\right)^{62} \cdot 7^8 1 \bmod 40 \equiv 7^8 \equiv \left(7^4\right)^2 \equiv 1 \bmod 40$

Επομένως, $40 \mid 7^{1000} - 1$ οπότε υπάρχει ακέραιος t τέτοιος ώστε $7^{1000} = 40 \cdot t + 1$. Άρα $7^{7^{1000}} = 7^{40t+1} \equiv 7 \bmod 100$.

Κεφάλαιο 10 Πρωταρχικές Ρίζες

Γνωρίζουμε από το Θεώρημα Euler-Fermat ότι αν $(a,n)=1$ τότε $a^{\varphi(n)} \equiv 1 \bmod n$ και ότι αν ο p είναι πρώτος αριθμός τότε $a^{p-1} \equiv 1 \bmod p$ αφού $\varphi(p)=p-1$.

Ωστόσο $\varphi(p)$ μπορεί να μην είναι ο μικρότερος ακέραιος b τέτοιος ώστε $a^b \equiv 1 \bmod n$.

Για παράδειγμα από το **«Μικρό Θεώρημα του Fermat »** γνωρίζουμε ότι $2^6 \equiv 1 \bmod 7$. Όμως $2^3 \equiv 1 \bmod 7$ είναι η μικρότερη δύναμη του 2 που είναι ισότιμο με $1 \bmod 7$. Μπορεί όμως να υπάρχουν μερικές τιμές του a που απαιτούν την δύναμη p-1. Για παράδειγμα η πρώτη δύναμη του 3 που είναι ισότιμη με 1mod7 είναι 3^6. Ας δούμε μερικά παραδείγματα για να καταλήξουμε σε μερικά συμπεράσματα.

Έστω $a^b \equiv 1 \bmod p$ όπου p είναι πρώτος.

Παράδειγμα 10.1

Να συμπληρώσετε τον παρακάτω πίνακα για $p=5$. Έστω b ο μικρότερος ακέραιος τέτοιος ώστε $a^b \equiv 1 \bmod p$.

Λύση

$\varphi(5)=5-1=4$

α	b τέτοιος ώστε $a^b \equiv 1 \bmod 5$
1	
2	
3	
4	

Άρα

α	b τέτοιος ώστε $a^b \equiv 1 \bmod 5$
1	1
2	4
3	4
4	2

Παράδειγμα 10.2

Να συμπληρώσετε τον παρακάτω πίνακα για $p=7$. Έστω b ο μικρότερος ακέραιος τέτοιος ώστε $a^b \equiv 1 \bmod p$.

Λύση

$\varphi(7)=7-1=6$

α	b τέτοιος ώστε $a^b \equiv 1 \bmod 7$
1	
2	
3	
4	
5	
6	

Άρα

α	b τέτοιος ώστε $a^b \equiv 1 \bmod 7$
1	1
2	3
3	6
4	3
5	6
6	2

Παράδειγμα 10.3

Να συμπληρώσετε τον παρακάτω πίνακα για $p = 11$. Έστω b ο μικρότερος ακέραιος τέτοιος ώστε $a^b \equiv 1 \bmod p$.

Λύση

$\varphi(11) = 11 - 1 = 10$

α	b τέτοιος ώστε $a^b \equiv 1 \bmod 7$
1	1
2	10
3	5
4	5
5	5
6	10
7	10
8	10
9	10
10	10

Βασιζόμενοι στα παραπάνω αριθμητικά αποτελέσματα από τους παραπάνω πίνακες κάνουμε τις εξής διαπιστώσεις:

1. Η μικρότερη δύναμη b τέτοια ώστε $a^b \equiv 1 \bmod p$ φαίνεται ότι διαιρεί το $\varphi(p) = p - 1$.
2. Υπάρχουν πάντα τιμές του a που απαιτούν την $p - 1$ δύναμη.

Ορισμός 10.1

Έστω a είναι ένας θετικός ακέραιος τέτοιος ώστε $(a, p) = 1$.

Η **τάξη** του $a \bmod p$ είναι ο μικρότερος θετικός ακέραιος b τέτοιος ώστε $a^b \equiv 1 \bmod p$ και συμβολίζουμε $b = ord_p(a)$.

Από το **«Μικρό Θεώρημα του Fermat »** γνωρίζουμε ότι $ord_p(a) \le \varphi(p) = p-1$.

Θεώρημα 10.1 Τάξη-Ιδιότητα της Διαίρεσης

Έστω a είναι ένας ακέραιος τέτοιος ώστε $(a, p) = 1$ και έστω $a^n \equiv 1 \bmod p$ τότε $ord_p(a) \mid n$. Πιο συγκεκριμένα $ord_p(a) \mid p-1$.

Απόδειξη

Από τον ορισμό της τάξης προκύπτει ότι $a^{ord_p(a)} \equiv 1 \bmod p$

Ας υποθέσουμε ότι $a^n \equiv 1 \bmod p$. Από το Θεώρημα 5.1 γνωρίζουμε ότι υπάρχουν ακέραιοι u και v τέτοια ώστε $ord_p(a) \cdot u - n \cdot v = g$.

Τότε για κάθε ακέραιο t έχουμε $g = ord_p(a) \cdot \left(u + n \cdot t\right) - n \cdot \left(v + ord_p(a) \cdot t\right)$.

Και επιλέγοντας το t να είναι αρκετά μεγάλος ακέραιος, και ο $u + n \cdot t$ και ο $v + ord_p(a) \cdot t$ θα είναι θετικοί.

Επομένως, υπάρχουν ακέραιοι r και s τέτοιοι ώστε : $g = ord_p(a) \cdot r - n \cdot s$, όπου r και s είναι θετικοί ακέραιοι (θα δούμε στην συνέχεια γιατί χρειαζόμαστε να είναι και οι 2 θετικοί αριθμοί).

Στην συνέχεια υπολογίζουμε την ποσότητα $a^{ord_p(a) \cdot r}$ με δυο διαφορετικούς τρόπους.

$a^{ord_p(a) \cdot r} = \left(a^{ord_p(a) \cdot r}\right)^r \equiv 1^r \equiv 1 \bmod p$

$a^{ord_p(a) \cdot r} = a^{ord_p(a) \cdot r} = a^{g + n \cdot s} = a^g \cdot (a^n)^s \equiv a^g \cdot (1)^s \equiv a^g \bmod p$.

Άρα $a^g \bmod p \equiv 1 \bmod p$. Ας θυμηθούμε ότι $ord_p(a)$ είναι η μικρότερη δύναμη του a που είναι ισότιμο με 1 modulo p. Δηλαδή $ord_p(a) \le g$ Όμως $g = \gcd(ord_p(a), n)$ οπότε $g \mid ord_p(a)$ και $g \mid n$. Πιο συγκεκριμένα $g \le ord_p(a)$.

Καταλήγουμε στο συμπέρασμα ότι $g = ord_p(a)$. Οπότε $ord_p(a) \mid n$.

Τελικά από το **«Μικρό Θεώρημα του Fermat »** έχουμε ότι $a^{p-1} \equiv 1 \bmod p$ επομένως $ord_p(a) \mid p-1$.

Ορισμός 10.2 Αν $ord_p(a) = p-1$ τότε ο α λέγεται **πρωταρχική ρίζα modulo p.**

Παράδειγμα 10.4 Χρησιμοποιώντας τους πίνακες που δημιουργήσαμε για $p = 5, 7, 11$ παρατηρούμε ότι 2 και 3 είναι **πρωταρχικές ρίζες modulo 11 .**

Θεώρημα 10.2 Θεώρημα πρωταρχικών ριζών

Έστω p είναι πρώτος και ας υποθέσουμε ότι $d \mid (p-1)$.

Τότε υπάρχουν ακριβώς $\varphi(d)$ διαφορετικοί ακέραιοι α modulo p τέτοιοι ώστε $ord_p(a) = d$.

Πιο συγκεκριμένα υπάρχουν ακριβώς $\varphi(p-1)$ πρωταρχικές ρίζες του p.

Δεν θα δώσουμε την απόδειξη του Θεωρήματος πρωταρχικών ριζών.

Παράδειγμα 10.5 Το θεώρημα πρωταρχικών ριζών μας λέει ότι υπάρχουν $\varphi(10) = 4$ πρωταρχικές ρίζες modulo 11. Έχουμε βρει ότι πράγματι υπάρχουν 4 πρωταρχικές ρίζες modulo 11 συγκεκριμένα 2, 6, 7 και 8. Ομοίως υπάρχουν $\varphi(36) = 12$ πρωταρχικές ρίζες modulo 37 και $\varphi(9906) = 3024$ πρωταρχικές ρίζες modulo 9907.

Παρακάτω αναφέρουμε μια σημαντική ιδιότητα των πρωταρχικών ριζών.

Θεώρημα 10.3 Έστω g είναι πρωταρχική ρίζα modulo p όπου p είναι πρώτος. Τότε κάθε μη μηδενικός αριθμός modulo p μπορεί να εκφραστεί ως δύναμη του p. Με άλλα λόγια για κάθε αριθμό a με $1 \le a < p$, μπορούμε να διαλέξουμε ακριβώς έναν από τους αριθμούς $g, g^2, g^3, ..., g^{p-3}, g^{p-2}, g^{p-1}$ ως ισότιμοι modulo p.

Απόδειξη

Καθώς g είναι πρωταρχική ρίζα modulo p, θα ισχύει $g^{p-1} \equiv 1 \bmod p$ και $p-1$ ο μικρότερος ακέραιος b τέτοιος ώστε $g^b \equiv 1 \bmod p$.

Στη συνέχεια υποστηρίζουμε ότι οι αριθμοί $g, g^2, g^3, ..., g^{p-3}, g^{p-2}, g^{p-1}$ είναι όλοι διαφορετικοί modulo p.

Αν δεν είναι διαφορετικοί τότε θα υπάρχουν εκθέτες i και j με $1 \le i < j \le p-1$ τέτοιοι ώστε $g^j \equiv g^i \bmod p$.

Τότε $p \mid (g^j - g^i) = g^i(g^{j-i} - 1)$.

Επομένως $p \mid g^i$ ή $p \mid g^{j-i} - 1$.

Γνωρίζουμε ότι $p \nmid g^i$ αφού $\text{ΜΚΔ}(g, p) = 1$. Επομένως, $p \mid g^{j-i} - 1$.

Άρα $g^{j-i} \equiv 1 \bmod p$ και $j - i < p - 1$. Αυτό είναι άτοπο όμως γιατί ο $p-1$ είναι ο μικρότερος ακέραιος b τέτοιος ώστε $g^b \equiv 1 \bmod p$. Τότε οι αριθμοί $g, g^2, g^3, ..., g^{p-3}, g^{p-2}, g^{p-1}$ είναι διαφορετικοί modulo p, οπότε κάθε ακέραιος α τέτοιος ώστε $1 \le a < p$ μπορεί να εκφραστεί ως μια δύναμη του g.

Ας παρατηρήσουμε ότι το θεώρημα των πρωταρχικών ριζών μας λέει ότι υπάρχουν ακριβώς $\varphi(p-1)$ πρωταρχικές ρίζες modulo p. Ωστόσο το θεώρημα δεν μας δίνει καμία πληροφορία για το πώς να βρίσκουμε πρωταρχικές ρίζες ή ποιοι αριθμοί είναι πρωταρχικές ρίζες modulo p.

Μια ερώτηση που προκύπτει είναι ή εξής: Με δεδομένο έναν αριθμό a, για ποιους πρώτους αριθμούς p ο a είναι πρωταρχική ρίζα; Για παράδειγμα βρίσκουμε ότι ο 2 είναι μια πρωταρχική ρίζα για τους πρώτους $p = 3,5,11,13,19,29,37,53,59,61,67,83.$

Η εικασία του Artin: Υπάρχουν άπειροι πρώτοι p τέτοιοι ώστε ο 2 να είναι πρωταρχική ρίζα mod p.

Θεώρημα 10.4 Έστω p είναι ένας πρώτος αριθμός. Η ισοτιμία $x^2+1 \equiv 0 \bmod p$ έχει λύσεις αν $p=2$ ή αν $p \equiv 1 \bmod 4$ αλλά δεν έχει καμία λύση αν $p \equiv 3 \bmod 4$.

Απόδειξη

- Όταν $p=2$, $x=1$ είναι μια λύση αφού $1^1+1 \equiv 0 \bmod 2.$
- Έστω ότι $p \equiv 1 \bmod 4$ τότε $4 \mid (p-1)$ επομένως, από το θεώρημα πρωταρχικών ριζών υπάρχει ένας ακέραιος a τέτοιος ώστε $ord_p(a) = 4$,

οπότε $a^4 \equiv 1 \bmod p$. Άρα $a^4 - 1 \equiv (a^2-1)(a^2+1) \equiv 0 \bmod p$.

Η τελευταία όμως σχέση δηλώνει ότι είτε $(a^2-1) \equiv 0 \bmod p$ είτε $(a^2+1) \equiv 0 \bmod p$.

Παρατηρούμε όμως ότι $a^2 - 1 \not\equiv 0 \bmod p$ αφού $ord_p(a) = 4$.

Οπότε $a^2+1 \equiv 0 \bmod p$ άρα a είναι μια λύση της ισοτιμίας $x^2+1 \equiv 0 \bmod a$.

- Έστω ότι $p \equiv 3 \bmod 4$. Τότε $4 \mid (p-3)$ οπότε $4 \nmid p-1$. Αφού p είναι περιττός τότε και ο $p-1$ είναι άρτιος, οπότε $2 \mid (p-1)$. Δηλαδή $(p-1,4) = 2$.

Ας υποθέσουμε τώρα ότι υπάρχει ένας ακέραιος a τέτοιος ώστε $a^2+1 \equiv 0 \bmod p$ τότε $a^4 \equiv \left(a^2\right)^2 \equiv (-1)^2 \equiv 1 \bmod p$. Από το Μικρό Θεώρημα του Fermat έχουμε ότι $a^{p-1} \equiv 1 \bmod p$.

Αφού $2 = (p-1,4)$ υπάρχουν ακέραιοι u και v τέτοιοι ώστε $2 = (p-1)s + 4t$.

Άρα έχουμε $a^2 \equiv a^{(p-1)s+4t} \equiv (a^{p-1})^s (a^4)t \equiv 1 \bmod p$. Τότε $a^2 \equiv 1 \equiv -1 \bmod p$. Επομένως, $2 \equiv 0 \bmod p$.

Αυτό όμως δηλώνει ότι $p \mid 2$ που είναι άτυπο αφού p είναι περιττός αριθμός. Άρα δεν υπάρχει κανένας ακέραιος a τέτοιος ώστε $a^2+1 \equiv 0 \bmod p$, οπότε η ισοτιμία $x^2+1 \equiv 0 \bmod p$ δεν έχει λύσεις σε αυτή την περίπτωση.

Τελικά βγάζουμε το συμπέρασμα ότι η ιδέα της τάξης και των πρωταρχικών ριζών μπορεί να επεκταθεί σε όλους τους θετικούς ακεραίους όχι απαραίτητα πρώτων αριθμών.

Ορισμός 10.3 Έστω ότι $(a,n)=1$. Η τάξη του a modulo n είναι ο μικρότερος θετικός ακέραιος b τέτοιος ώστε $a^b \equiv 1 \bmod n$.

Από το Θεώρημα του **Euler-Fermat** γνωρίζουμε ότι $a^{\varphi(n)} \equiv 1 \bmod n$.

Επομένως, $ord_n(a) \le \varphi(n)$.

Χρησιμοποιώντας παρόμοιο επιχείρημα που δώσαμε στην απόδειξη του Θεωρήματος 12.1 μπορούμε να αποδείξουμε το επόμενο αποτέλεσμα.

Θεώρημα 10.5 Έστω ότι $(a,n)=1$ και ότι $a^b \equiv 1 \bmod n$ τότε $ord_n(a) \mid b$ και πιο συγκεκριμένα $ord_n(a) \mid \varphi(n)$.

Ορισμός 10.4 Αν $(a,n)=1$ και $ord_n(a)=\varphi(n)$, τότε λέμε ότι ο a είναι μια **πρωταρχική ρίζα** modulo p.

Παράδειγμα 10.6 Το 3 είναι μια πρωταρχική ρίζα modulo 10 αφού $\varphi(10)=4$ και $3^1 \equiv 3 \bmod 10$ $3^2 \equiv 9 \bmod 10$, $3^3 \equiv 7 \bmod 10$, $3^4 \equiv 1 \bmod 10$.

Κεφάλαιο 11
Τετράγωνα modulo p και τετραγωνικά ισοϋπόλοιπα

Μάθαμε σε προηγούμενο κεφάλαιο να λύνουμε γραμμικές εξισώσεις της μορφής $a \cdot x \equiv c \bmod p$.

Στη συνέχεια θεωρούμε τετραγωνικά ισοϋπόλοιπα modulo α με p πρώτο αριθμό.

Παράδειγμα 11.1

Είναι ο 3 ισότιμος με το τετράγωνο κάποιου αριθμού modulo 7;

Μπορούμε να βρούμε έναν αριθμό x τέτοιον ώστε $x^2 \equiv 3 \bmod 7$;

Λύση

$0^2 \equiv 0 \bmod 7$

$1^2 \equiv 1 \bmod 7$

$2^2 \equiv 4 \bmod 7$

$3^2 \equiv 2 \bmod 7$

$4^2 \equiv 2 \bmod 7$

$5^2 \equiv 4 \bmod 7$

$6^2 \equiv 1 \bmod 7$

Επομένως, το 3 δεν είναι ισότιμο με κάποιο τετράγωνο modulo 7.

Παράδειγμα 11.2 Έχει η ισοτιμία $x^2 \equiv -1 \equiv 12 \bmod 13$ λύση;

Λύση

Υπολογίζουμε τα $x^2 \bmod 13$ για $x \equiv 0,1,2,\ldots 12 \bmod 13$ και βρίσκουμε ότι η ισοτιμία έχει 2 λύσεις την $x \equiv 5 \bmod 13$ και $x \equiv 8 \bmod 13$. Για να μελετήσουμε τα τετράγωνα modulo p, υπολογίζουμε τα τετράγωνα modulo p για p = 3, 5, 7, 11.

a	$a^2 \mod 3$
0	0
1	1
2	1

a	$a^2 \mod 5$
0	0
1	1
2	4
3	4
4	1

a	$a^2 \mod 7$
0	0
1	1
2	4
3	2
4	2
5	4
6	1

a	$a^2 \mod 11$
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

Στη συνέχεια κάνουμε τις παρακάτω παρατηρήσεις από τα παρακάτω αριθμητικά δεδομένα.

- Κάθε αριθμός διαφορετικός από 0 που εμφανίζεται ως ένα τετράγωνο modulo p εμφανίζεται ακριβώς 2 φορές.
- Το τετράγωνο ενός αριθμού b και το τετράγωνο του αριθμού p-b είναι ίδια.

Θεώρημα 11.1 Έστω p είναι πρώτος. Τότε $b^2 \equiv (p-b)^2 \bmod p$.

Απόδειξη

$(p-b)^2 = p^2 - 2p \cdot b + b^2 \equiv 0 - 0 + b^2 \equiv b^2 \bmod p$.

Επομένως, εάν επιθυμούμε να βρούμε όλους τους αριθμούς που είναι τετράγωνα modulo p, ουσιαστικά χρειαζόμαστε μόνο να υπολογίσουμε τα μισά από αυτά:

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

Ο στόχος μας είναι να καθορίσουμε ποιοι αριθμοί είναι τετράγωνα modulo p και ποιοι αριθμοί δεν είναι τετράγωνα modulo p. Για να ξεκινήσουμε χρειαζόμαστε κάποια «εδάφια».

Ορισμός 11.1 Ένας μη μηδενικός αριθμός που είναι ισότιμος με ένα τετράγωνο modulo p ονομάζεται τετραγωνικό ισοϋπόλοιπο modulo p.

Παράδειγμα 11.3 Το 3 είναι ένα τετραγωνικό ισοϋπόλοιπο modulo 11 αφού $5^2 \equiv 3 \bmod 11$.
Το σύνολο των τετραγωνικών ισοϋπόλοιπων modulo 11 είναι {1,3,4,5,9}.
Ας παρατηρήσουμε ότι υπάρχουν 5 τετραγωνικά ισοϋπόλοιπα modulo 11.

Ορισμός 11.2 Ένας μη μηδενικός αριθμός που δεν είναι ισότιμος με ένα τετράγωνο modulo p ονομάζεται μη-τετραγωνικό ισοϋπόλοιπο modulo p.

Παράδειγμα 11.4 Το 2 είναι ένα μη-τετράγωνικο ισοϋπόλοιπο modulo 11 αφού δεν υπάρχει ακέραιος x τέτοιος ώστε $x^2 \equiv 2 \bmod 11$.
Το σύνολο των μη-τετραγωνικών ισοϋπόλοιπων είναι {2,6,7,8,10}. Ας παρατηρήσουμε ότι υπάρχουν 5 μη-τετραγωνικά ισοϋπόλοιπα modulo 11.

Θεώρημα 11.2 Έστω p είναι περιττός πρώτος αριθμός. Τότε υπάρχουν ακριβώς $\frac{p-1}{2}$

τετραγωνικά ισοϋπόλοιπα modulo p και $\frac{p-1}{2}$ μη-τετραγωνικά ισοϋπόλοιπα modulo p.

Απόδειξη

Τα τετραγωνικά ισοϋπόλοιπα modulo p είναι απλά τα τετράγωνα modulo p. Επομένως είναι οι αριθμοί:

$1^2 \bmod p \quad 2^2 \bmod p \quad \ldots \quad (p-1)^2 \bmod p$

Ωστόσο αφού έχουμε ήδη αποδείξει ότι $p^2 \equiv (\mathrm{p}-\mathrm{b})^2 \bmod p$, χρειάζεται να εξετάσουμε τα μισά.

Τα τετραγωνικά ισοϋπολοιπα modulo p είναι οι αριθμοί $1^2 \bmod p \quad 2^2 \bmod p \quad \ldots \quad \left(\frac{p-1}{2}\right)^2 \bmod p$.

Ας παρατηρήσουμε ότι η λίστα των παραπάνω αριθμών αποτελείται από $\frac{p-1}{2}$ αριθμούς.

Επομένως, για να αποδείξουμε ότι υπάρχουν ακριβώς $\frac{p-1}{2}$ τετραγωνικά ισοϋπόλοιπα modulo p, χρειαζόμαστε μόνο να ελέγξουμε ότι οι αριθμοί $1^2 \bmod p \quad 2^2 \bmod p \quad \ldots \quad \left(\frac{p-1}{2}\right)^2 \bmod p$ είναι όλοι διαφορετικοί modulo p.

Ας υποθέσουμε ότι b_1 και b_2 είναι δυο αριθμοί μεταξύ 1 και $\frac{p-1}{2}$ τέτοιοι ώστε $b_1^2 \equiv b_2^2 \bmod p$.

Τότε $p \mid (\mathrm{b}_1^2 - \mathrm{b}_2^2) = (\mathrm{b}_1 + \mathrm{b}_2)(\mathrm{b}_1 - \mathrm{b}_2)$.

Το $\mathrm{b}_1 + \mathrm{b}_2$ είναι μεταξύ 2 και $p-1$ επομένως δεν διαιρείται από το p. Άρα $p \mid (b_1 - b_2)$, ωστόσο $|b_1 - b_2| < \frac{p-1}{2}$ οπότε $b_1 - b_2 = 0$.

Άρα $b_1 \equiv b_2$ και καταλήγουμε στο συμπέρασμα ότι οι αριθμοί $1^2 \bmod p \quad 2^2 \bmod p \quad \ldots \quad \left(\frac{p-1}{2}\right)^2 \bmod p$ είναι όλοι διαφορετικοί modulo p, οπότε υπάρχουν ακριβώς $\frac{p-1}{2}$ τετραγωνικά ισοϋπόλοιπα modulo p και $\frac{p-1}{2}$ μη-τετραγωνικά ισοϋπόλοιπα modulo p.

Τι θα συμβεί όταν πολλαπλασιάσουμε τετραγωνικά ισοϋπόλοιπα με μη-τετραγωνικά ισοϋπόλοιπα;

Δοκιμάζοντας μερικά παραδείγματα modulo 11 κάνουμε μια εικασία.

Ας θυμηθούμε ότι τα τετραγωνικά ισοϋπόλοιπα modulo 11 είναι {1,3,4,5,9} και τα μη-τετραγωνικα ισοϋπόλοιπα είναι {2,6,7,8,10}.

Τετραγωνικό ισοϋπόλοιπο · Τετραγωνικό ισοϋπόλοιπο = Τετραγωνικό ισοϋπόλοιπο

Μη-τετραγωνικό ισοϋπόλοιπο · Μη-τετραγωνικό ισοϋπόλοιπο = Τετραγωνικό ισοϋπόλοιπο

Τετραγωνικό ισοϋπόλοιπο · Μη-τετραγωνικό ισοϋπόλοιπο = Μη-Τετραγωνικό ισοϋπόλοιπο

Για να αποδείξουμε ότι τα παραπάνω είναι πράγματι σωστά θα πρέπει να ερευνήσουμε την σχέση μεταξύ των τετραγωνικών ισοϋπόλοιπων και των πρωταρχικών ριζών. Έστω g είναι μια πρωταρχική ρίζα modulo p.

Από το θεώρημα 11.3 γνωρίζουμε ότι οι δυνάμεις του g είναι $g, g^2, g^3, ..., g^{p-3}, g^{p-2}, g^{p-1}$ με δεδομένο ότι όλοι είναι μη μηδενικοί αριθμοί modulo p. Γνωρίζουμε ότι οι μισοί από τους μη μηδενικούς αριθμούς modulo p είναι τετραγωνικά ισοϋπόλοιπα και μισοί είναι μη-τετραγωνικα ισοϋπόλοιπα. Πως γνωρίζουμε όμως ποιοι είναι ποιοι;

Γνωρίζουμε ότι g^2 είναι τετραγωνικό ισοϋπόλοιπο αφού είναι στο τετράγωνο . Όμοια $g^4 = \left(g^2\right)^2$ είναι τετραγωνικό ισοϋπόλοιπο. Γενικά κάθε άρτια δύναμη του g π.χ. g^{2k} είναι ένα τετραγωνικό ισοϋπόλοιπο αφού $g^{2k} = \left(g^k\right)^2$. Αφού υπάρχουν ακριβώς $\frac{p-1}{2}$ τετραγωνικά ισοϋπόλοιπα modulo p καταλήγουμε στο συμπέρασμα ότι τα τετραγωνικά ισοϋπόλοιπα modulo p είναι εκείνοι οι αριθμοί a που μπορούν να εκφραστούν ως άρτιες δυνάμεις του g και μη-τετραγωνικά ισοϋπόλοιπα είναι εκείνοι οι αριθμοί a που μπορούν να εκφραστούν ως περιττές δυνάμεις του g. Χρησιμοποιώντας αυτή την πληροφορία μπορούμε τώρα πλέον να αποδείξουμε το παρακάτω Θεώρημα.

Θεώρημα 11.3 Τετραγωνικός Ισοϋπόλοιπος (1ος κανόνας πολλαπλασιασμού).

Έστω p είναι ένας περιττός πρώτος αριθμός . Έστω a και b είναι τετραγωνικά ισοϋπόλοιπα modulo p και c και d είναι μη-τετραγωνικά ισοϋπόλοιπα modulo p. Τότε,

- $a \cdot b$ είναι ένα τετραγωνικό ισοϋπόλοιπο modulo p. Το γινόμενο 2 τετραγωνικών ισοϋπόλοιπων modulo p είναι ένα τετραγωνικό ισοϋπόλοιπο modulo p .
- $c \cdot d$ είναι ένα τετραγωνικό ισοϋπόλοιπο modulo p. Το γινόμενο 2 μη-τετραγωνικών ισοϋπόλοιπων modulo p είναι ένα τετραγωνικό ισοϋπόλοιπο modulo p.
- $a \cdot c$ είναι ένα μη-τετραγωνικό ισοϋπόλοιπο modulo p. Το γινόμενο ενός τετραγωνικού ισοϋπόλοιπου με ένα μη-τετραγωνικό ισοϋπόλοιπο modulo p είναι ένα μη-τετραγωνικό ισοϋπόλοιπο modulo p .

Απόδειξη

Έστω g είναι μια πρωταρχική ρίζα modulo p . Αφού a και b είναι τετραγωνικά ισοϋπόλοιπα modulo p τότε υπάρχουν ακέραιοι j και k τέτοιοι ώστε $1 \le i$, $\mathrm{j} \le \mathrm{p}-1$ και $a \equiv g^{2k} \bmod p$ και $b \equiv g^{2j} \bmod p$.

Αφού c και d είναι μη-τετραγωνικά ισοϋπόλοιπα modulo p τότε θα υπάρχουν ακέραιοι m και n τέτοιοι ώστε $1 \le m \quad n \le \mathrm{p}-1$ και $c \equiv g^{2m-1} \bmod p$ και $d \equiv g^{2n-1} \bmod p$, τότε $a \cdot b \equiv g^{2(\mathrm{j}+\mathrm{k})}$ είναι μια άρτια δύναμη του g, οπότε $a \cdot b$ είναι ένα τετραγωνικό ισοϋπόλοιπο modulo p.

$c \cdot d \equiv g^{2(\mathrm{m}-\mathrm{n}-1)}$ είναι μια άρτια δύναμη του g, οπότε $a \cdot b$ είναι ένα τετραγωνικό ισοϋπόλοιπο modulo p και

$a \cdot c \equiv g^{2(\mathrm{m}+\mathrm{k})-1} \bmod p$ είναι μια περιττή δύναμη του g, οπότε $a \cdot b$ είναι ένα μη-τετραγωνικό ισοϋπόλοιπο modulo p.

Στη συνέχεια χρησιμοποιούμε τον παρακάτω συμβολισμό για τα τετραγωνικά ισοϋπόλοιπα και τα μη-τετραγωνικά ισοϋπόλοιπα.

Ορισμός 11.3 Ο συμβολισμός του Legendre $\left(\frac{a}{p}\right)$ modulo p ορίζεται ως εξής:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \alpha\nu \quad \alpha \quad \epsilon\acute{\iota}\nu\alpha\iota \quad \tau\epsilon\tau\rho\alpha\gamma\omega\nu\iota\kappa\acute{o}\varsigma\, \iota\sigma\upsilon\pi\acute{o}\lambda\iota\pi\sigma\varsigma \quad \mathrm{mod}\, ulo \quad p \\ -1 & an \quad a \quad \epsilon\acute{\iota}\nu\alpha\iota \quad \mu\eta-\tau\epsilon\tau\rho\alpha\gamma\omega\nu\iota\kappa\acute{o}\varsigma \quad \iota\sigma\upsilon\pi\acute{o}\lambda\iota\pi\sigma\varsigma \quad \mathrm{mod}\, ulo \quad p \end{cases}$$

Θεώρημα 12.4 Τετραγωνικό Ισοϋπόλοιπο (2ος κανόνας πολλαπλασιασμού).

Έστω p είναι ένας περιττός πρώτος αριθμός. Τότε

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

Απόδειξη

Αυτό προκύπτει άμεσα από τον 1ο κανόνα Τετραγωνικού Ισοϋπόλοιπου.

Παράδειγμα 11.5 Είναι ο 75 τετράγωνο modulo 97;

Λύση

Για να καθορίσουμε αν ο 75 ή όχι είναι τετράγωνο modulo 97 χρειάζεται να υπολογίσουμε το $\left(\frac{75}{97}\right)$.

Από τον 1ο κανόνα Τετραγωνικού Ισοϋπόλοιπου γνωρίζουμε ότι

$$\left(\frac{75}{97}\right) = \left(\frac{3 \cdot 5 \cdot 5}{97}\right) = \left(\frac{3}{97}\right) \cdot \left(\frac{5}{97}\right) \cdot \left(\frac{5}{97}\right).$$

Στη συνέχεια παρατηρούμε ότι $\left(\frac{5}{97}\right) = \pm 1$. Επομένως $\left(\frac{5}{97}\right)\cdot\left(\frac{5}{97}\right) = 1$.

Επίσης, $10^2 \equiv 3 \bmod 97$ επομένως $\left(\frac{3}{97}\right) = 1$. Άρα $\left(\frac{75}{97}\right) = 1$, δηλαδή 75 είναι τετράγωνο modulo 97.

Ας παρατηρήσουμε ότι η λύση στο προηγούμενο παράδειγμα εξαρτάτε στο γεγονός ότι $\left(\frac{3}{97}\right) = 1$.

Επομένως, είναι σημαντικό να είμαστε σε θέση να υπολογίζουμε $\left(\frac{a}{p}\right)$ για τυχαίο ακέραιο p.

Αρχικά χρειαζόμαστε το επόμενο αποτέλεσμα:

Θεώρημα 11.5

Ας υποθέσουμε ότι p είναι ένας περιττός αριθμός και α $\not\equiv$ mod p. Τότε $a^{(p-1)/2} \equiv \pm 1 \bmod p$.

Απόδειξη

Έστω $\mathrm{A} = a^{(p-1)/2}$. Από το Μικρό Θεώρημα του Fermat έχουμε $\mathrm{A}^2 = a^{p-1} \equiv 1 \bmod p$.

Επομένως, $p \mid (A^2 - 1) = (A-1)(\mathrm{A}+1)$. Άρα $p \mid (A-1)$ ή $p \mid (A+1)$.

Αν $p \mid (A-1)$ τότε $\mathrm{A} \equiv 1 \bmod p$.

Αν $p \mid (A+1)$ τότε $\mathrm{A} \equiv -1 \bmod p$.

Τότε $\mathrm{A} \equiv a^{(p-1)/2} \equiv \pm 1 \bmod p$.

Παρατηρούμε ότι οι ποσότητες $a^{(p-1)/2}$ και $\left(\frac{a}{p}\right)$ παίρνουν και οι δύο ποσότητες τις ίδιες τιμές ± 1. Μπορούμε να εξετάσουμε κατά πόσον αυτές οι ποσότητες συσχετίζονται μεταξύ τους.

Το αφήνουμε για τον αναγνώστη.

Κεφάλαιο 12
Εισαγωγή στην Τετραγωνική Αντιστροφή

Σε αυτή την ενότητα θα βρούμε ποίοι πρώτοι αριθμοί έχουν $a=-1$ ως τετραγωνικό ισοϋπόλοιπο και ποίοι πρώτοι αριθμοί p έχουν $a=2$ ως τετραγωνικό ισοϋπόλοιπο.

Με άλλα λόγια θα είμαστε σε θέση να απαντήσουμε στις παρακάτω 2 ερωτήσεις:

- Για ποιούς πρώτους αριθμούς p υπάρχει ακέραιος x τέτοιος ώστε:
  $x^2 \equiv -1 \bmod p$;
- Για ποιούς πρώτους αριθμούς p υπάρχει ακέραιος x τέτοιος ώστε:
  $x^2 \equiv 2 \bmod p$;

Θεώρημα 12.1 Κριτήριο του Euler

Έστω p είναι ένας περιττός πρώτος αριθμός. Τότε $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p$.

Απόδειξη

Αρχικά θα θεωρήσουμε την περίπτωση όπου α είναι τετραγωνικό ισοϋπόλοιπο modulo p και πότε το α δεν είναι ισοϋπόλοιπο.

Έστω α είναι τετραγωνικό ισοϋπόλοιπο modulo p . Τότε $\left(\frac{a}{p}\right)=1$. Επομένως, θα πρέπει να αποδείξουμε ότι $a^{(p-1)/2} \equiv 1 \bmod p$. Έστω g είναι μια θετική ρίζα modulo p. Γνωρίζουμε ότι α είναι μια άρτια δύναμη του g οπότε ο α μπορεί να εκφραστεί ως εξής: $a \equiv g^{2k} \bmod p$.

Από το μικρό Θεώρημα του Fermat έχουμε ότι $a^{(p-1)/2} \equiv \left(g^{2k}\right)^{(p-1)/2} \equiv \left(g^{p-1}\right)^k \equiv 1^k \equiv 1 \bmod p$.

Επομένως, αν ο α είναι τετραγωνικό ισοϋπόλοιπο modulo p τότε $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p$.

Θεώρημα 12.2 Τετραγωνική αντιστροφή Μέρος 1^{ο}

Έστω p είναι ένας περιττός πρώτος αριθμός. Τότε ο -1 είναι ένας τετραγωνικός ισοϋπόλοιπος modulo p αν $p=1 \bmod 4$ και ο -1 είναι ένας τετραγωνικός ισοϋπόλοιπος modulo p αν $p=3 \bmod 4$.

Χρησιμοποιώντας τον συμβολισμό του Legendre έχουμε:

$$\left(\frac{-1}{p}\right)=\begin{cases} 1 & \alpha\nu \quad p \equiv 1 \bmod 4 \\ -1 & \alpha\nu \quad p \equiv 3 \bmod 4 \end{cases}$$

Απόδειξη

Χρησιμοποιώντας το κριτήριο του Euler έχουμε ότι $(-1)^{(p-1)/2} \equiv \left(\frac{-1}{p}\right) \bmod p$.

Αρχικά, υποθέτουμε ότι $p \equiv 1 \bmod 4$. Τότε $4 \mid (\mathrm{p}-1)$, οπότε υπάρχει ένας ακέραιος k τέτοιος ώστε $p = 4k+1$. Τότε $(-1)^{(p-1)/2} = (-1)^{(4k+1-1)/2} = (-1)^{2k} = 1$. Επομένως, $1 \equiv \left(\frac{-1}{p}\right) \bmod p$.

Άρα αν $p \equiv 1 \bmod 4$ τότε ο -1 είναι τετραγωνικό ισοϋπόλοιπο modulo4.

Στη συνέχεια, υποθέτουμε ότι $p \equiv 3 \bmod 4$. Τότε $4 \mid (p-3)$, οπότε υπάρχει ακέραιος k τέτοιος ώστε $p = 4k+3$. Τότε $(-1)^{(p-1)/2} = (-1)^{(4k+3-1)/2} = (-1)^{2k+1} = -1$. Επομένως, $-1 \equiv \left(\frac{-1}{p}\right) \bmod p$.

Άρα αν $p \equiv 3 \bmod 4$ τότε ο -1 είναι μη-τετραγωνικό ισοϋπόλοιπο modulo p.

Θεώρημα 12.3 Τετραγωνική αντιστροφή Μέρος 2^{ο}

Έστω p είναι ένας περιττός πρώτος αριθμός. Τότε ο 2 είναι ένας τετραγωνικό ισοϋπόλοιπο modulo p αν $p = 1$ ή $7 \bmod 8$ και ο 2 είναι μη-τετραγωνικό ισοϋπόλοιπο modulo p αν $p = 3$ ή $p = 5 \bmod 8$.

Χρησιμοποιώντας τον συμβολισμό του Legendre έχουμε:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \alpha\nu \quad p \equiv 1 \quad \acute{\eta} \quad p \equiv 7 \bmod 8 \\ -1 & \alpha\nu \quad p \equiv 3 \quad \acute{\eta} \quad p \equiv 5 \bmod 8 \end{cases}$$

Απόδειξη

Η πρώτη μας σκέψη πιθανότατα θα είναι να χρησιμοποιήσουμε το κριτήριο του Euler όπως στο θεώρημα τετραγωνικής αντιστροφής μέρος 1. Παρ'όλ'αυτα δεν υπάρχει ένας προφανής τρόπος για να υπολογίζουμε το $2^{(p-1)/2} \bmod p$. Ας θυμηθούμε ότι όταν αποδείξαμε το Μικρό Θεώρημα του Fermat στο κεφάλαιο 9, αρχικά πολλαπλασιάσαμε τους αριθμούς 1, 2, 3, ..., (p-1) με α, και στη συνέχεια τα πολλαπλασιάσαμε όλα μαζί όπου μας έδωσε παράγοντα της μορφής a^{p-1}.

Για να χρησιμοποιήσουμε το κριτήριο του Euler Θέλουμε $\frac{1}{2} \cdot (\mathrm{p}-1)$ παράγοντες του α για να βγάλουμε, οπότε αντί για να ξεκινήσουμε με όλους τους αριθμούς από το 1 έως το p, θα ξεκινήσουμε με τους αριθμούς 1, 2, 3, ..., $\frac{p-1}{2}$ και θα πολλαπλασιάσουμε καθέναν με $a = 2$.

Για να υλοποιήσουμε την παραπάνω ιδέα, θα υπολογίσουμε το $\left(\frac{2}{13}\right)$.

Αρχίζουμε με τους μισούς αριθμούς από το 1 έως το 13-1=12

1, 2, 3, 4, 5, 6 .

Στη συνέχεια πολλαπλασιάσουμε καθέναν από τους παραπάνω αριθμούς με 2 και στη συνέχεια τους πολλαπλασιάζουμε όλους μαζί. Οπότε έχουμε:

$$(2\cdot 1)(2\cdot 2)(2\cdot 3)(2\cdot 4)(2\cdot 5)(2\cdot 6) = 2^6\cdot 6!$$

Παρατηρούμε ότι ο παράγοντας $2^6 = 2^{(13-1)/2}$ είναι αυτός που μας ενδιαφέρει στους υπολογισμούς. Η κεντρική ιδέα τώρα είναι να μειώσουμε κάθε έναν από τους αριθμούς 2, 4, 6, 8, 10, 12 modulo 13 για να πάρουμε έναν αριθμό μεταξύ 6 και -6. Έχουμε:

$$2 \equiv 2 \bmod 13$$
$$4 \equiv 4 \bmod 13$$
$$6 \equiv 6 \bmod 13$$
$$8 \equiv -5 \bmod 13$$
$$10 \equiv -3 \bmod 13$$
$$12 \equiv -1 \bmod 13$$

Πολλαπλασιάζοντας αυτους τους αριθμούς μαζί έχουμε:

$$2\cdot 4\cdot 6\cdot 8\cdot 10\cdot 12 \equiv 2\cdot 4\cdot 6\cdot(-5)\cdot(-3)\cdot(-1) \bmod 13$$
$$\equiv (-1)^3\cdot 6! \bmod 13$$
$$\equiv -6! \bmod 13$$

Οπότε $2^6\cdot 6! \equiv -6! \bmod 13$ που αυτό δηλώνει ότι $2^6 \equiv -1 \bmod 13$.

Από το Κριτήριο του Euler, καταλήγουμε ότι ο 2 είναι ένας τετραγωνικός μη-ισουπόλοιπος modulo 13.

Στη συνέχεια σκεφτόμαστε την παραπάνω ιδέα λίγο πιο γενικά.

Έστω p είναι ένας περιττός αριθμός. Θέλουμε να υπολογίσουμε το $2^{(p-1)/2}$. Ξεκινάμε με τους άρτιους αριθμούς 1, 2, 3, ..., $\frac{p-1}{2}$ και πολλαπλασιάζουμε καθέναν από τους παραπάνω αριθμούς με 2 όπου και παίρνουμε την παρακάτω λίστα αριθμών $2\cdot 1, 2\cdot 2, 2\cdot 3, ..., 2\cdot\frac{p-1}{2}$. Στη συνέχεια πολλαπλασιάζουμε τους αριθμούς μαζί και τους παραγοντοποιούμε με παράγοντα το 2 οπότε και έχουμε:

$$(2\cdot 1)\cdot(2\cdot 2)\cdot(2\cdot 3)\cdot\ldots\cdot 2\cdot\frac{p-1}{2}.$$

Στη συνέχεια πολλαπλασιάζουμε τους παραπάνω αριθμούς και βγάζουμε τον παράγοντα 2 από κάθε αριθμό οπότε και έχουμε:

$$(2\cdot 1)\cdot(2\cdot 2)\cdot(2\cdot 3)\cdot\ldots\cdot 2\cdot\frac{p-1}{2} = 2^{(p-1)/2}\left(\frac{p-1}{2}\right)!$$

Το επόμενο βήμα είναι να μειώσουμε κάθε αριθμό από την λίστα $2, 4, 6, .., p-1$ modulo p

έτσι ώστε να βρίσκονται στο σύνολο τιμών $\left[-\frac{p-1}{2},\frac{p-1}{2}\right]$.

Οι αριθμοί στην αρχή της λίστας δεν θα αλλάξουν, αλλά οποιαδήποτε αριθμός στην λίστα μεγαλύτερος από $\frac{p-1}{2}$ χρειάζεται να αφαιρεθεί p φορές οπότε θα γίνει αρνητικός.

Οι αριθμοί με αρνητικό πρόσημο είναι ακριβώς οι αριθμοί των ακεραίων της λίστας $2,4,6,..,p-1$ που είναι μεγαλύτεροι από $\frac{p-1}{2}$. Οπότε εξισώνοντας τα 2 γινόμενα έχουμε:

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!=2\cdot 4\cdot 6\cdots(p-1)\equiv(-1)^{\text{πλήθος αρνητικών αριθμών}}\cdot\left(\frac{p-1}{2}\right)!\text{modp}.$$

Καταλήγουμε στο συμπέρασμα ότι $2^{\frac{p-1}{2}}\equiv(-1)^{\text{πλήθος αρνητικών αριθμών}}\text{modp}$.

Ας θυμηθούμε ότι το πλήθος των αρνητικών αριθμών είναι ακριβώς το πλήθος των ακεραίων της λίστας $2,4,6,..,p-1$ που είναι μεγαλύτεροι από $\frac{p-1}{2}$.

Χρησιμοποιώντας αυτό το αποτέλεσμα, μπορούμε τώρα να αποδείξουμε το Θεώρημα.

Έστω ότι $p\equiv 3\bmod 8$. Τότε $8\mid(p-3)$, οπότε υπάρχει ένας ακέραιος k τέτοιος ώστε $p=8k+3$.

Χρειάζεται να γράψουμε τους αριθμούς $2,4,6,..,p-1$.

Και να καθορίσουμε πόσοι από αυτούς είναι μεγαλύτεροι από $\frac{p-1}{2}$.

Σε αυτή την περίπτωση

$p-1=8k+2$ και $\frac{p-1}{2}=\frac{8k+2}{2}=4k+1$.

Επομένως, η λίστα είναι $2,4,6,..,4k,4k+2,4k+4,...,8k$.

Υπάρχουν 2k+1 άρτιοι αριθμοί ανάμεσα στους αριθμούς 4k+2 και 8k+2 (μπορούμε να το δοκιμάσουμε για μερικές τιμές του k), οπότε υπάρχουν 2k+1 αριθμοί της λίστας μεγαλύτεροι από $\frac{p-1}{2}$.

Άρα υπάρχουν 2k+1 αρνητικοί αριθμοί, άρα $2^{\frac{p-1}{2}}\equiv(-1)^{2k+1}\equiv-1\bmod p$.

Καταλήγουμε στο συμπέρασμα ότι ο 2 είναι μη-τετραγωνικός ισοϋπόλοιπος modulo p για κάθε πρώτο αριθμό p που είναι ισότιμος με 3 modulo 8.

Οι υπόλοιπες 3 περιπτώσεις μπορούν να αποδεδειχθούν με παρόμοιο τρόπο.

Κεφάλαιο 13
Ο Νόμος της Τετραγωνικής Αντιστροφής

Ο νόμος της τετραγωνικής αντιστροφής πρώτα διατυπώθηκε από τον Euler και Lagrange, αλλά ο Gauss έδωσε την πρώτη απόδειξη το 1801. Ο Gauss ανακάλυψε τον νόμο όταν ήτανε 19 χρονών και κατά την διάρκεια της ζωής του βρήκε άλλες 7 διαφορετικές αποδείξεις. Ο νόμος της τετραγωνικής αντιστροφής είναι ένα «όμορφο» και ευφυή αποτέλεσμα που έχει σημαντικές πρακτικές ισοτιμίες.

Θεώρημα 13.1 Νόμος της Τετραγωνικής Αντιστροφής.

Έστω p και q είναι διαφορετικοί περιττοί πρώτοι ακέραιοι αριθμοί.

$$\left(-\frac{1}{p}\right)=\begin{cases}1 & \alpha\nu \quad p\equiv 1 \mod 4\\ -1 & \alpha\nu \quad p\equiv 3 \mod 4\end{cases}$$

$$\left(\frac{q}{p}\right)=\begin{cases}\left(\frac{p}{q}\right) & \alpha\nu \quad p\equiv 1 \mod 4 \quad \acute{\eta} \quad q\equiv 1 \mod 4\\ -\left(\frac{p}{q}\right) & \alpha\nu \quad p\equiv 3 \mod 4 \quad \kappa\alpha\iota \quad q\equiv 3 \mod 4\end{cases}$$

Έχουμε ήδη απόδειξη το παραπάνω για $\left(-\frac{1}{p}\right)$ και $\left(\frac{2}{p}\right)$ και δεν θα δώσουμε την γενική απόδειξη για $\left(\frac{p}{q}\right)$. Χρησιμοποιώντας τον νόμο της τετραγωνικής αντιστροφής και τον νόμο του τετραγωνικού ισοϋπόλοιπου πολλαπλασιασμού, μπορούμε να υπολογίσουμε το $\left(\frac{a}{p}\right)$ για οποιαδήποτε αριθμό α και για οποιαδήποτε πρώτο αριθμό p. Ο νόμος της τετραγωνικής αντιστροφής μας επιτρέπει να αναστρέφουμε τον συμβολισμό του Legendre $\left(\frac{q}{p}\right)$ και να τον αντικαθιστάμε με $\pm\left(\frac{p}{q}\right)$.

Επομένως μπορούμε να μειώσουμε το p modulo q και να επαναλάβουμε την διαδικασία, και σε κάθε στάδιο να παίρνουμε ένα σύμβολο Legendre με ολοένα και μικρότερες ποσότητες έτσι ώστε να φτάσουμε σε ένα σύμβολο Legendre που να μπορούμε να υπολογίσουμε.

Παράδειγμα 13.1 Να εξετάσετε αν η παρακάτω ισοτιμία $x^2 \equiv 5 \mod 3593$ έχει λύση (ο 3593 είναι πρώτος)**.**

Λύση

Πρέπει να προσδιορίσουμε αν ο 5 είναι τετραγωνικός ισοϋπόλοιπος modulo 3593, οπότε πρέπει να υπολογίσουμε το $\left(\frac{5}{3593}\right)$

$\left(\frac{5}{3593}\right)=\left(\frac{3593}{5}\right)$ επειδή $5\equiv 1 \bmod 4$

$=\left(\frac{3}{5}\right)$ επειδή $3593\equiv 3 \bmod 5$

$=-1$ επειδή 3 είναι ένα μη-τετραγωνικό ισοϋπόλοιπο modulo 5.

Επομένως, το 5 είναι ένα μη-τετραγωνικό ισοϋπόλοιπο modulo 3593, οπότε η ισοτιμία δεν έχει λύση.

Παράδειγμα 13.2 Να εξετάσετε αν η παρακάτω ισοτιμία $x^2\equiv 14 \bmod 137$ έχει λύση (ο 137 είναι πρώτος)**.**

Λύση

Πρέπει να προσδιορίσουμε αν ο 14 είναι τετραγωνικό ισοϋπόλοιπο modulo 137, οπότε πρέπει να υπολογίσουμε το $\left(\frac{14}{137}\right)$.

$\left(\frac{14}{137}\right)=\left(\frac{2}{137}\right)\left(\frac{7}{137}\right)$ με βάση τον πολλαπλασιαστικό νόμο τετραγωνικών ισοϋπολοίπων

$=\left(\frac{7}{137}\right)$ επειδή $137\equiv 1 \bmod 8$

$=\left(\frac{137}{7}\right)$ επειδή $137\equiv 1 \bmod 4$

$=\left(\frac{4}{7}\right)$ επειδή $137\equiv 4 \bmod 7$

$=1$ επειδή $4=2^2$ είναι ένα τετραγωνικό ισοϋπόλοιπο modulo 7.

Επομένως, ο 14 είναι ένα τετραγωνικό ισοϋπόλοιπο modulo 137, οπότε η ισοτιμία έχει λύση.

Παράδειγμα 13.3 Να εξετάσετε αν η παρακάτω ισοτιμία $x^2\equiv 55 \bmod 179$ έχει λύση (ο 179 είναι πρώτος)**.**

Λύση

Πρέπει να προσδιορίσουμε αν ο 55 είναι τετραγωνικό ισοϋπόλοιπο modulo 179, οπότε πρέπει να

υπολογίσουμε το $\left(\frac{55}{179}\right)$.

$\left(\frac{55}{179}\right)=\left(\frac{5}{179}\right)\left(\frac{11}{179}\right)$ με βάση τον πολλαπλασιαστικό νόμο τετραγωνικών ισοϋπόλοιπων

$=\left(\frac{179}{5}\right)\cdot(-1)\cdot\left(\frac{179}{11}\right)$ επειδή $5\equiv 1 \bmod 4$ και $11\equiv 179\equiv 3 \bmod 4$

$=\left(\frac{4}{5}\right)\cdot(-1)\cdot\left(\frac{3}{11}\right)$

$=1\cdot(-1)\cdot(-1)\left(\frac{11}{3}\right)$ αφού $3\equiv 11\equiv 3 \bmod 4$

$=1\cdot(-1)\cdot(-1)\left(\frac{2}{3}\right)$

$=1\cdot(-1)\cdot(-1)(-1)$

$=-1$

Επομένως, ο 55 είναι ένα μη-τετραγωνικό ισοϋπόλοιπο modulo 179, οπότε η ισοτιμία δεν έχει λύση.

Παράδειγμα 13.4

Να βρείτε όλους τους περιττούς ακέραιους p έτσι ώστε ο 3 να είναι τετραγωνικό ισοϋπόλοιπο modulo p.

Λύση

Χρειαζόμαστε να βρούμε όλους τους πρώτους αριθμούς p τέτοιους ώστε $\left(\frac{3}{p}\right)$=1.

$3\equiv 3 \bmod 4$

Γνωρίζουμε ότι $\left(\frac{3}{p}\right)=\begin{cases}\left(\frac{p}{3}\right) & \alpha\nu \quad p\equiv 1 \mod 4\\ -\left(\frac{p}{3}\right) & \alpha\nu \quad p\equiv 3 \mod 4\end{cases}$

Επίσης $\left(\frac{p}{3}\right)=\begin{cases}\left(\frac{1}{3}\right)=1 & \alpha\nu \quad p\equiv 1 \mod 3\\ -\left(\frac{2}{3}\right)=-1 & \alpha\nu \quad p\equiv 2 \mod 3\end{cases}$

Οπότε $\left(\frac{3}{p}\right)=1$ αν p = 1 mod 3 και p = 1 mod 4 ή αν p = 2 mod 3 και $p\equiv 3 \bmod 4$.

Κεφάλαιο 14 Διοφαντικές εξισώσεις

Μια **Διοφαντική εξίσωση** είναι μια πολυωνυμική εξίσωση όπου αναζητάμε ακέραιες λύσεις (ή ίσως και ρητές λύσεις). Δεν υπάρχει μια συγκεκριμένη μέθοδος για να καθορίσουμε εάν μια δοσμένη διοφαντική εξίσωση έχει λύση ή όχι ούτε μέθοδος για να βρίσκουμε όλες τις λύσεις σε περίπτωση που η διοφαντική εξίσωση έχει λύσεις.

Παράδειγμα 14.1 Να βρείτε όλες τις ακέραιες λύσεις της εξίσωσης $x^4+9=y^2$.

Λύση

Ξαναγράφουμε την εξίσωση στην μορφή

$$y^2-x^4=9$$

$$(y-x^2)(y+x^2)=9.$$

Αφού μας ενδιαφέρει μόνο για $y>0$, $x>0$, ο παράγοντας $y+x^2$είναι θετικός. Επομένως, ο άλλος παράγοντας $y-x^2$ πρέπει να είναι θετικός. Υπάρχουν μόνο δύο τρόποι να παραγοντοποιήσουμε το 9 ως γινόμενο 2 θετικών ακεραίων: $9=1\cdot 9$ και $9=3\cdot 3$. Άρα υπάρχουν μόνο τρείς περιπτώσεις:

(α) $y+x^2=1$ και $y-x^2=9$

(β) $y+x^2=3$ και $y-x^2=3$

(γ) $y+x^2=9$ και $y-x^2=1$

Σε κάθε περίπτωση υπάρχουν 2 εξισώσεις με 2 αγνώστους. Στην περίπτωση (α) βρίσκουμε ότι $x=\pm\sqrt{-4}$ που δεν είναι ακέραιος. Στην περίπτωση (β) βρίσκουμε ότι $x=0$ που δεν είναι θετικός ακέραιος.

Στην περίπτωση (γ) βρίσκουμε ότι $y=5$ και $x=\pm 2$. Επομένως η μόνη λύση που είναι θετικοί ακέραιοι είναι $x=2$ και $y=5$.

Θεώρημα 14.1 Το τελευταίο Θεώρημα του Fermat μας λέει ότι αν $n\geq 3$, τότε η εξίσωση $x^n+y^n=z^n$ δεν έχει λύσεις μη μηδενικές. Το 1637 ο Fermat έγραψε στο περιθώριο του βιβλίου του “Arithmetica of Diophantus” ότι είχε μια πραγματικά υπέροχη απόδειξη αυτής της πρότασης που το περιθώριο ήταν περιορισμένο για να την συμπεριλάβει.

Καμία σωστή απόδειξη του τελευταίου Θεωρήματος του Fermat δεν βρέθηκε για 357 χρόνια, μέχρι που μια σωστή απόδειξη δημοσιεύτηκε από τον Andrew Wiles το 1995.

Ας παρατηρήσουμε ότι όταν $n=2$, η εξίσωση $x^2+y^2=z^2$ έχει άπειρες λύσεις τις οποίες μπορούμε να εξερευνήσουμε.

Ο Fermat επίσης είπε ότι η εξίσωση $x^2+2=y^3$ έχει μοναδική λύση που είναι θετικοί ακέραιοι την λύση $x=5$ και $y=3$. Επίσης είπε ότι η εξίσωση $x^2+4=y^3$ έχει μοναδική λύση που είναι θετικοί ακέραιοι την λύση $x=5$ και $y=3$. Αυτές οι προτάσεις έκτοτε έχουν αποδειχθεί χρησιμοποιώντας ιδέες της θεωρίας των δευτεροβάθμιων όπου βέβαια αναπτύχθηκαν 200 χρόνια μετά τις ανακοινώνεις του Fermat.

Είναι πολύ ενδιαφέρον να γνωρίζουμε τις αποδείξεις των προτάσεων του Fermat.

Οι ισοτιμίες συχνά μας παρέχουν έναν εύκολο τρόπο για να αποδεικνύουμε ότι μια συγκεκριμένη διοφαντική εξίσωση δεν έχει λύσεις.

Παράδειγμα 14.2 Να βρείτε όλες τις ακέραιες λύσεις της εξίσωσης $x^2-7\cdot y^2=-1$.

Λύση

Ας θεωρήσουμε την εξίσωση modulo 7 . Αν $x^2-7\cdot y^2=-1$ τότε $x^2-7\cdot y^2\equiv -1 \bmod 7$

$x^2\equiv -1 \bmod 7$.

Ωστόσο $7\equiv 3 \bmod 4$ οπότε -1 είναι ένα δευτεροβάθμιο μη-ισοϋπόλοιπο με modulo 7. Επομένως, δεν υπάρχει κανένας ακέραιος x τέτοιος ώστε $x^2\equiv -1 \bmod 7$. Τα τετράγωνα modulo 7 είναι $1^2\equiv 1 \bmod 7$, $2^2\equiv 4 \bmod 7$, $3^2\equiv 2 \bmod 7$, $5^2\equiv 4 \bmod 7$, $6^2\equiv 1 \bmod 7$. Καταλήγουμε ότι η εξίσωση δεν έχει ακέραιες λύσεις.

Η βασική ιδέα της χρησιμοποίησης των ισοτιμιών για να αποδείξουμε ότι μια Διοφαντική εξίσωση δεν έχει λύσεις είναι ότι μια Διοφαντική εξίσωση δεν έχει λύσεις modulo n, τότε είναι βέβαιο ότι δεν έχει λύσεις.

Θεώρημα 14.2 Ας υποθέσουμε ότι το d διαιρείται από έναν πρώτο $p\equiv 3 mod 4$ ή ότι ο d διαιρείται από το 4. Τότε η εξίσωση $x^2-d\cdot y^2=-1$ δεν έχει λύσεις.

Απόδειξη.

Ας υποθέσουμε ότι (x, y) είναι μια λύση της εξίσωσης. Αρχικά, ας υποθέσουμε ότι $p\equiv 3 mod\ 4$ και ότι p | d. Τότε d ≡ 0 mod p. Επομένως:

$x^2-dy^2\equiv x^2\equiv -1 \bmod p.$ Αλλά αφού p ≡ 3 mod 4, −1 είναι ένα δευτεροβάθμιο μη-ισουπολοιπο modulo p, τότε δεν υπάρχει κανένας τέτοιος ακέραιος x.

Στη συνέχεια ας υποθέσουμε ότι 4 | d. Τότε $x^2-dy^2\equiv x^2\equiv -1\ mod\ 4$

Αλλά τα τετράγωνα modulo 4 είναι $1^2\equiv 1\ mod\ 4, 2^2\equiv 0\ mod\ 4, 3^2\equiv 1\ mod\ 4$, οπότε δεν υπάρχει κανένας ακέραιος x τέτοιος ώστε $x^2\equiv -1\equiv 3 mod 4$. Επομένως η εξίσωση δεν έχει ακέραιες λύσεις.

Παράδειγμα 14.3 Να βρείτε όλες τις ακέραιες λύσεις της εξίσωσης $x^2 - 5 \cdot y^2 = 2$.

Λύση: Ας θεωρήσουμε την εξίσωση modulo 5.

$x^2 - 5 \cdot y^2 \equiv 2 mod 5$

$x^2 \equiv 2 \ mod \ 5$

Ωστόσο, 2 είναι ένα τετράγωνο μη ισοϋπόλοιπο modulo 5, οπότε δεν υπάρχει κανένας τέτοιος ακέραιος x. Τα τετράγωνα modulo 5 είναι $1^2 \equiv 1 mod 5, 2^2 \equiv 4 mod 5, 3^2 \equiv 4 mod 5, 4^2 \equiv 1 mod 5$. Καταλήγουμε στο συμπέρασμα ότι η εξίσωση δεν έχει ακέραιες λύσεις.

Παράδειγμα 14.4 Υπάρχουν ακέραιοι x και y τέτοιοι ώστε $x^2 - 5y^2 = 2$?

Υπόδειξη: Θεωρήστε την εξίσωση modulo 5.

Κεφάλαιο 15 Γραμμική Διοφαντική Εξίσωση

Ας θεωρήσουμε δυο ακεραίους αριθμούς a και b. Γνωρίζουμε ότι υπάρχουν ακέραιοι κ και λ τέτοιοι ώστε $\kappa \cdot a + \lambda \cdot b = (a,b)$

Η αντίστροφη διαδικασία προσδιορισμού του μέγιστου κοινού διαιρέτη των a και b οδηγεί στην εύρεση κατάλληλων κ , λ που ικανοποιούν την προηγούμενη σχέση

Η γενική μορφή μιας τέτοιας εξίσωσης είναι η $a \cdot x + b \cdot y = \gamma$ όπου a και b και γ είναι γνωστοί ακέραιοι αριθμοί και x, y είναι άγνωστοι ακέραιοι.

Η εξίσωση αυτή είναι γνωστή ως γραμμική Διοφαντική εξίσωση.

Για παράδειγμα η εξίσωση $3 \cdot x + 5 \cdot y = 4$ έχει λύση το ζεύγος $(3,-1)$, διότι $3 \cdot 3 + 5 \cdot (-1) = 4$. Αντίθετα η εξίσωση $2 \cdot x + 20 \cdot y = 1$ δεν έχει λύση, γιατί για κάθε επιλογή του ζεύγους (x,y) το αριστερό μέρος της είναι άρτιος ενώ το δεξί μέρος της είναι περιττός.

Ας δούμε λοιπόν πότε η γραμμική Διοφαντική εξίσωση είναι επιλύσιμη.

Θεώρημα 15.1

Η γραμμική Διοφαντική εξίσωση $a \cdot x + b \cdot y = \gamma$ έχει λύση αν και μόνο αν ο $\delta = (\mathrm{a}, \mathrm{b})$ διαιρεί τον ακέραιο γ.

Απόδειξη

Ας υποθέσουμε ότι η εξίσωση $a \cdot x + b \cdot y = \gamma$ έχει λύση (x_o, y_o), δηλαδή ισχύει ότι $a \cdot x_o + b \cdot y_o = \gamma$

Θέτουμε $a = \kappa \cdot \delta$ και $b = \lambda \cdot \delta$, όπου κ, λ ακέραιοι. Έτσι έχουμε ότι $\gamma = a \cdot x_o + b \cdot y_o = \delta(\kappa \cdot x_o + \lambda \cdot y_o)$ όπου ο αριθμός $\kappa \cdot x_o + \lambda \cdot y_o$ είναι ακέραιος , οπότε $\delta \mid \gamma$.

Αντίστροφα ας θεωρήσουμε ότι $\delta \mid \gamma$, οπότε $\gamma = \delta \cdot \mu$, όπου μ ακέραιος.

Από Θεώρημα γνωρίζουμε ότι υπάρχουν ακέραιοι κ , λ τέτοιοι ώστε

$\kappa \cdot a + \lambda \cdot b = (a,b) = \delta$

$a(\kappa \cdot \mu) + b(\lambda \cdot \mu) = \delta\mu = \gamma$

Άρα η εξίσωση $a \cdot x + b \cdot y = \gamma$ έχει λύση $x_o = \kappa\mu, y_o = \lambda\mu$

Μια ιδιότητα της γραμμικής Διοφαντικής εξίσωσης είναι ότι οι λύσεις της, αν υπάρχουν, είναι άπειρες και ανήκουν στην ίδια κλάση ισοϋπόλοιπων ακεραίων.

Θεώρημα 15.2

Αν (x_0, y_0) είναι μία λύση της εξίσωσης $\alpha \cdot x + \beta \cdot y = \gamma$ και $\delta = (\alpha, \beta)$, τότε όλες οι λύσεις της είναι της μορφής:

$x = x_0 + \left(\frac{\beta}{\delta}\right)t$ και $y = y_0 - \left(\frac{\alpha}{\delta}\right)t$, όπου $t \in \mathrm{Z}$.

Απόδειξη

Έστω ότι η εξίσωση $\alpha \cdot x + \beta \cdot y = \gamma$ έχει μία γνωστή λύση (x_0, y_0). Αν υποθέσουμε πως (x, y) είναι μία άλλη λύση, τότε

$\alpha \cdot x_0 + \beta \cdot y_0 = \gamma = \alpha \cdot x' + \beta \cdot y'$,

το οποίο είναι ισοδύναμο με

$\alpha \cdot (x' - x_0) = \beta \cdot (y_0 - y')$,

Διαιρώντας με τον $\delta = (\alpha, \beta)$, παίρνουμε ότι

$\kappa(x' - x_0) = \lambda(y_0 - y')$,

όπου οι $\kappa = \frac{\alpha}{\delta}$ και $\lambda = \frac{\beta}{\delta}$ είναι σχετικά πρώτοι. Επομένως, έχουμε $\kappa \mid \lambda(y_0 - y')$ και $(\kappa, \lambda) = 1$, οπότε από Θεώρημα έχουμε ότι $\kappa \mid (y_0 - y')$. Δηλαδή, υπάρχει ακέραιος t τέτοιος ώστε $y_0 - y' = \kappa t$. Όμοια αποδεικνύεται ότι $x' - x_0 = \lambda t$ και έτσι καταλήγουμε στους τύπους:

$$x' = x_0 + \lambda t = x_0 + \left(\frac{\beta}{\delta}\right)t$$

$$y' = y_0 - \kappa t = y_0 - \left(\frac{\alpha}{\delta}\right)t .$$

Παρατήρηση

Εύκολα μπορεί κανείς να παρατηρήσει ότι αν $(\alpha, \beta) = 1$ και η (x_0, y_0) είναι μία λύση της γραμμικής Διοφαντικής εξίσωσης, τότε όλες οι λύσεις της είναι της μορφής:

$x = x_0 + \beta t$ και $y = y_0 - \alpha t$ για κάθε ακέραιο t.

Η επίλυση μιας γραμμικής Διοφαντικής εξίσωσης ανάγεται στον προσδιορισμό μίας αρχικής της λύσης (x_0, y_0). Η αντίστροφη διαδικασία του αλγόριθμου του Ευκλείδη δίνει τον τρόπο προσδιορισμού μιας τέτοιας λύσης. Αν $\delta = (\alpha, \beta)$, τότε μπορούμε να βρούμε ακεραίους κ, λ ώστε $\kappa\alpha + \lambda\beta = \delta$.

Υποθέτουμε ότι $\delta \mid \gamma$ (για να υπάρχει λύση) δηλαδή $\gamma = \delta\mu$, για κάποιον ακέραιο μ. Άρα $\mu \cdot \kappa \cdot \alpha + \mu \cdot \lambda \cdot \beta = \mu \cdot \delta = \gamma$, δηλαδή μία λύση της αρχικής εξίσωσης είναι η $x_0 = \mu\kappa$, $y_0 = \mu\lambda$, οπότε η γενική λύση είναι η

$$x = \mu\kappa + \left(\frac{\beta}{\delta}\right)t,\ y = \mu\lambda - \left(\frac{\alpha}{\delta}\right)t \text{, όπου } t \in \mathrm{Z}.$$

Εφαρμογές

1. Να υπολογιστεί ο μέγιστος κοινός διαιρέτης των αριθμών 172 και 20. Στη συνέχεια να λυθεί η γραμμική Διοφαντική εξίσωση $172x + 20y = 1000$.

Λύση

Με τη βοήθεια του αλγόριθμου του Ευκλείδη υπολογίζουμε τον (172, 20),

$$172 = 8 \cdot 20 + 12$$
$$20 = 1 \cdot 12 + 8$$
$$12 = 1 \cdot 8 + 4$$
$$8 = 2 \cdot 4.$$

Άρα (172, 20)=4 και προφανώς η εξίσωση $172x + 20y = 1000$ έχει λύση, διότι $4 \mid 1000$.

Ακολουθώντας την αντίστροφη διαδικασία του αλγόριθμου του Ευκλείδη έχουμε:

$$4 = 12 - 8$$
$$4 = 12 - (20 - 12)$$
$$4 = 2 \cdot 12 - 20$$
$$4 = 2(172 - 8 \cdot 20) - 20$$
$$4 = 2 \cdot 172 + (-17) \cdot 20.$$

Άρα $4 = 2 \cdot 172 + (-17) \cdot 20$ και πολλαπλασιάζοντας με 250 προκύπτει ότι $172 \cdot 500 + 20 \cdot (-4250) = 1000$.

Επομένως, μία λύση της Διοφαντικής εξίσωσης είναι $x_0 = 500$, $y_0 = -4250$ και σύμφωνα με το Θεώρημα 15.2, όλες οι λύσεις της είναι της μορφής:

$$x = 500 + \left(\frac{20}{4}\right)t = 500 + 5t$$

$$y = -4250 - \left(\frac{172}{4}\right)t = -4250 - 43t,$$

όπου $t \in \mathrm{Z}$.

2. Να υπολογιστούν οι φυσικοί αριθμοί οι οποίοι διαιρούμενοι με τον 11 αφήνουν υπόλοιπο 6 και διαιρούμενοι με τον 5 αφήνουν υπόλοιπο 2.

Λύση

Έστω ένας φυσικός ν τέτοιος ώστε $\nu = 11\kappa + 6$ και $\nu = 5\lambda + 2$. Τότε

$$11\kappa + 6 = 5\lambda + 2 \text{ ή } 5\lambda - 11\kappa = 4$$

και καταλήγουμε σε μία Διοφαντική εξίσωση η οποία έχει λύση, διότι $(-11,5) = 1$ και $1 \mid 4$. Εκφράζουμε τον μέγιστο κοινό διαιρέτη $(-11,5) = 1$ ως γραμμικό συνδυασμό των -11 και 5, με τη βοήθεια του αλγόριθμου του Ευκλείδη:

$$-11 = (-3)\cdot 5 + 4$$

$$5 = 4\cdot 1 + 1$$

$$4 = 4\cdot 1.$$

Ακολουθώντας την αντίστροφη διαδικασία έχουμε $1 = (-2)\cdot 5 + (-1)(-11)$.

Πολλαπλασιάζοντας επί 4 προκύπτει $5\cdot(-8) - 11\cdot(-4) = 4$ και μία λύση της Διοφαντικής εξίσωσης είναι $\lambda_0 = -8$, $\kappa_0 = -4$. Επομένως, όλες οι λύσεις είναι της μορφής:

$\lambda = -8 + (-11)t = -11t - 8$

$\kappa = -4 - 5t = -5t - 4$,

όπου $t \in Z$ και ο φυσικός ν γράφεται $\nu = -55t - 38$. Επειδή πρέπει $\nu > 0$ έχουμε $-55t - 38 > 0$ ή $t < -\frac{38}{35}$ και επειδή *t* ακέραιος $\nu = -55t - 38$ με $t \le -1$ ή $\nu = 55t - 38$, $t \in Z$, $t \ge 1$.

3. Ένας κουμπαράς περιέχει κέρματα των 50 και 100 δραχμών συνολικού ποσού 1100 δραχμών . Να υπολογίσετε όλους τους δυνατούς συνδυασμούς κερμάτων που μπορούμε να έχουμε.

Λύση

Αν ορίσουμε x το πλήθος των κερμάτων των 50 δραχμών και y το πλήθος των κερμάτων των 100 δραχμών έχουμε τη γραμμική Διοφαντική εξίσωση

$50x + 100y = 1100$.

Προφανώς $(50,100) = 50$ και $50 \mid 1100$, οπότε η εξίσωση έχει λύση. Επιπλέον, παρατηρούμε ότι $50(-1) + 100\cdot 1 = 50$ και πολλαπλασιάζοντας με τον αριθμό 22 έχουμε ότι $50(-22) + 100\cdot 22 = 1100$, οπότε μία λύση της γραμμικής Διοφαντικής εξίσωσης είναι $x_0 = -22$ και $y_0 = 22$. Από το Θεώρημα 15.2, όλες οι λύσεις είναι της μορφής:

$$x = -22 + \left(\frac{100}{50}\right)t = -22 + 2t$$

$$y = 22 - \left(\frac{50}{50}\right)t = 22 - t,$$

όπου $t \in Z$. Επιπλέον οι αριθμοί x και y είναι μη αρνητικοί, οπότε $-22 + 2t \ge 0$ και $22 - t \ge 0$, δηλαδή $22 \ge t \ge 11$. Επομένως, όλοι οι δυνατοί συνδυασμοί είναι

$x = 2t - 22$ και $y = 22 - t$, όπου $t = 11,12,...,22$.

4. Να υπολογισθούν τα κλάσματα, στα οποία αν προσθέσουμε τον αριθμό 3 στον αριθμητή και τον 4 στον παρανομαστή τους γίνονται ίσα με το 6/11.

Λύση

Έστω x/y ένα κλάσμα, τέτοιο ώστε $\frac{x+3}{y+4} = \frac{6}{11}$.

Τότε έχουμε την Διοφαντική εξίσωση $11x - 6y = -9$, η οποία έχει λύση αφού $(11,-6) = 1$ και $1 \mid (-9)$. Με τη βοήθεια του αλγόριθμου του Ευκλείδη γράφουμε τον $(11,-6) = 1$ ως γραμμικό συνδυασμό των 11 και -6:

$$11 = (-1)\cdot(-6) + 5$$
$$-6 = (-2)\cdot 5 + 4$$
$$5 = 1\cdot 4 + 1$$
$$4 = 1\cdot 4.$$

Ακολουθώντας την αντίστροφη διαδικασία έχουμε $1 = (-1)\cdot 11 + (-2)\cdot(-6)$. Πολλαπλασιάζοντας επί (-9) προκύπτει ότι $11\cdot 9 - 6\cdot 18 = -9$ και μία προφανής λύση της Διοφαντικής εξίσωσης είναι η $x_0 = 9$ και $y_0 = 18$. Σύμφωνα με το Θεώρημα 15.2 όλες οι λύσεις είναι της μορφής:

$x = 9 + (-6)\cdot t = 9 - 6t$

$y = 18 - 11\cdot t$,

όπου $t \in Z$. Αν αντικαταστήσουμε τις τιμές αυτές στο κλάσμα έχουμε

$\frac{x+3}{y+4} = \frac{12-6t}{22-11t} = \frac{6(2-t)}{11(2-t)} = \frac{6}{11}$, αν $t \neq 2$.

Για $t = 2$ το κλάσμα είναι το $\frac{x}{y} = \frac{3}{4}$ οπότε έχουμε $\frac{x+3}{y+4} = \frac{6}{8}$. Άρα τα ζητούμενα κλάσματα είναι της μορφής:

$\frac{x}{y} = \frac{9-6t}{18-11t}$, όπου $t \in Z$, $t \neq 2$.

ΜΕΡΟΣ Β

ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ

Κεφάλαιο 16 Εφαρμογή 1η Αριθμοί Fibonacci και Γραμμική Αναδρομικότητα

Ορισμός 16.1 Οι αριθμοί Fibonacci ορίζονται ως εξής:

$F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ για $n \geq 3$.

Παρατηρούμε ότι δεν έχουμε έναν τύπο υπολογισμού του F_n γιατί δεν μπορούμε να υπολογίσουμε τον F_n άμεσα.

Έχουμε όμως έναν κανόνα που μας υποδεικνύει πώς να υπολογίζουμε τον F_n από προηγούμενους όρους.

Στη συνέχεια παρουσιάζουμε ένα παράδειγμα αναδρομής ή αναδρομικής εξίσωσης.

Να φτιαχτεί πίνακας που να περιέχει τους 20 πρώτους όρους Fibonacci.

n	F_n	n	F_n
1	1	11	89
2	1	12	144
3	2	13	233
4	3	14	377
5	5	15	610
6	8	16	987
7	13	17	1597
8	21	18	2584
9	34	19	4181
10	55	20	6765

Παρατηρούμε ότι οι αριθμοί Fibonacci μεγαλώνουν πολύ γρήγορα. Για παράδειγμα αν συνεχίσουμε να υπολογίζουμε όρους της ακολουθίας Fibonacci θα διαπιστώσουμε ότι ο όρος F_{31} είναι μεγαλύτερος από 1 εκατομμύριο $F_{31} = 1.346.269$.

Και ο 45ος Fibonacci αριθμός είναι μεγαλύτερος από 1 δισεκατομμύριο $F_{45} = 1.134.903.170$.

Μας ενδιαφέρει να ανακαλύψουμε θεωρητικά αριθμητικά πρότυπα που προκύπτουν από τους αριθμούς Fibonacci, οπότε ένα ερώτημα που προκύπτει είναι πόσο γρήγορα οι αριθμοί Fibonacci μεγαλώνουν. Μπορούμε να το μετρήσουμε υπολογίζοντας τον λόγο $\frac{F_n}{F_{n-1}}$.

Για το λόγο αυτό φτιάχνουμε έναν πίνακα τιμών των $\frac{F_n}{F_{n-1}}$ για $n \leq 20$.

n	F_n/F_{n-1}	n	F_n/F_{n-1}
2	1.00000	12	1,6179775280
3	2.00000	13	1,6180555555
4	1.5	14	1,6180257510
5	1.6666667	15	1,6180371352
6	1,6	16	1,61803278688
7	1,625	17	1,6180344478
8	1,615384	18	1,6180338134
9	1,6190476	19	1,61803405572
10	1,61764705	20	1,6180339631
11	1,618181818		

Ας παρατηρήσουμε ότι ο λόγος $\frac{F_n}{F_{n-1}}$ φαίνεται να πλησιάζει όλο και περισσότερο τον αριθμό 1,61803.

Ας προσπαθήσουμε να ανακαλύψουμε τι αριθμός είναι ο 1,61803.

Από τον παραπάνω πίνακα προκύπτει ότι ο F_n είναι προσεγγιστικά ίσος με $a \cdot F_{n-1}$ για κάποιον αριθμό α .

$$F_n \approx aF_{n-1}$$
$$F_{n-1} \approx aF_{n-2}$$
$$F_n \approx a^2 F_{n-2}$$

Χρησιμοποιώντας την αναδρομική εξίσωση $F_n = F_{n-1} + F_{n-2}$ έχουμε $a^2 \cdot F_{n-2} \approx a \cdot F_{n-2} + F_{n-2}$.

Διαιρώντας με F_{n-2} παίρνουμε την εξίσωση $a^2 - a - 1 = 0$, όπου αν την λύσουμε θα πάρουμε τις λύσεις

$a = \frac{1 \pm \sqrt{5}}{2}$.

Παρατηρούμε ότι $\frac{1 \pm \sqrt{5}}{2} \approx\sim 1,61803399$.

Γνωρίζουμε ότι και οι 2 τιμές του α ικανοποιούν την εξίσωση $a^2 - a - 1 = 0$.

Επομένως για κάθε αριθμό n και οι 2 τιμές του α ικανοποιούν την εξίσωση $a^n = a^{n-1} + a^{n-2}$,

που μοιάζει με την αναδρομική εξίσωση Fibonacci $F_n = F_{n-1} + F_{n-2}$.

Μπορούμε να επισημοποιήσουμε αυτή την παρατήρηση ως εξής:

Έστω $a_1 = \frac{1+\sqrt{5}}{2}$ και $a_2 = \frac{1-\sqrt{5}}{2}$.

Και επίσης έστω $H_n = c_1 \cdot a_1^{\,n} + c_2 \cdot a_2^{\,n}$ όπου c_1 και c_2 είναι σταθερές .

Τότε $H_n = H_{n-1} + H_{n-2}$.

Οπότε ο H_n ικανοποιεί τον ίδιο αναδρομικό τύπο όπως στην ακολουθία Fibonacci και c_1, c_2 μπορούν να είναι οποιοσδήποτε ακέραιος.

Η ιδέα είναι να επιλέξουμε c_1 και c_2 με τέτοιο τρόπο έτσι ώστε ο H_n και η ακολουθία Fibonacci F_n να ξεκινούν με τις ίδιες δύο αρχικές τιμές . Δηλαδή:

$$H_1 = F_1 = 1 \text{ και } H_2 = F_2 = 1$$

Επομένως λύνουμε το παρακάτω σύστημα:

$$c_1 a_1 + c_2 a_2 = 1 \text{ και } c_1 a_1^2 + c_2 a_2^2 = 1$$

και παίρνουμε ως λύση τα $c_1 = \frac{1}{\sqrt{5}}$ και $c_2 = -\frac{1}{\sqrt{5}}$.

Συνοψίζουμε τα συμπεράσματα μας ως εξής:

Ο τύπος για τον n-οστό όρο της ακολουθίας Fibonacci πήρε το όνομα του μετά τον Binet που το δημοσίευσε το 1843 (παρ'όλο που ήταν γνωστό στους Euler και Daniel Bernulli τουλάχιστον 100 χρόνια νωρίτερα).

Θεώρημα 16.1 Τύπος του Binet.

Η ακολουθία Fibonacci F_n περιγράφεται από την αναδρομή:

$F_1 = F_2 = 1$ και $F_n = F_{n-1} + F_{n-2}$ για $n \geq 3$.

Τότε ο n-οστός όρος της ακολουθίας Fibonacci δίνεται από τον παρακάτω τύπο:

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

Απόδειξη

Για κάθε θετικό ακέραιο $n \geq 1$ έστω $H_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$.

Θα αποδείξουμε ότι $H_n = F_n$ για όλους τους ακεραίους $n \geq 1$ με την βοήθεια της μαθηματικής επαγωγής.

(i) Βάση Επαγωγής : Αρχικά ελέγχουμε αν ισχύει $H_1 = F_1$ και $H_2 = F_2$:

Πράγματι $H_1 = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1\right] = \frac{1}{\sqrt{5}} \cdot \sqrt{5} = 1 = F_1$

$$H_2 = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right] = \frac{1}{\sqrt{5}} \cdot \frac{4\sqrt{5}}{4} = 1 = F_2.$$

(ii) Επαγωγική υπόθεση. Έστω ότι $H_k = F_k$ για όλα τα $k \leq n$. Τότε

$$H_{n+1} = H_n + H_{n-1}$$
$$= F_n + F_{n-1}$$
$$= F_{n+1}$$

Επομένως $H_n = F_n$ για κάθε ακέραιο $n \geq 1$.

Ορισμός 16.2 Ο αριθμός $\varphi = \frac{1+\sqrt{5}}{2}$ είναι γνωστός ως **χρυσή τομή**.

Ο τύπος του Binet μας λέει ότι $F_n = \frac{\varphi^n - (1-\varphi)^n}{\sqrt{5}}$.

Η χρυσή τομή έχει συναρπάσει Δυτικούς Διανοούμενους εδώ και 2400 χρόνια και έχει εμφανιστεί σε εξαιρετικά ποικίλους και μερικές φορές εκπληκτικούς τομείς:

- **Αρχιτεκτονική** (Ακρόπολη, Παρθενώνας, Πυραμίδες της Γκίζας, Μεγάλο Τζαμί της Καϊρουάν, Naqsh-e Jahan πλατεία)
- **Ζωγραφική** (Mona Lisa, *De Divina proportione, ο Μυστικός Δείπνος του Dalli)*
- **Σχεδιασμό βιβλίων**
- **Μουσική**
- **Φύση (**σπείρες Fibonacci στα φυτά, διευθετήσεις φύλλων, διάταξη των φύλλων σε ένα φυτό, σπείρες από τα ηλιοτρόπια, σπείρες από τα κουκουνάρια)
- **Ανθρώπινο Σώμα**

Θεώρημα 16.2 Το Θεώρημα του Zeckendorf

Κάθε θετικός ακέραιος μπορεί να εκφραστεί με μοναδικό τρόπο ως άθροισμα ενός ή περισσότερων διαφορετικών Fibonacci αριθμών με τέτοιο τρόπο ώστε το άθροισμα να μην περιέχει 2 διαδοχικούς Fibonacci αριθμούς.

Παράδειγμα 16.1

$100 = F_{11} + F_6 + F_4 = 89 + 8 + 3$ είναι η αντιπροσώπευση του **Zeckendorf** του ακεραίου 100.

Ας παρατηρήσουμε ότι μπορούμε να εκφράσουμε το 100 ως $100 = F_{11} + F_6 + F_4 = 89 + 8 + 2 + 1 = 55 + 34 + 8 + 3$ αλλά αυτές οι αντιπροσωπεύσεις περιέχουν διαδοχικούς Fibonacci αριθμούς.

Για κάθε θετικό ακέραιο αριθμό μπορούμε να βρούμε μια αντιπροσώπευση που ικανοποιεί τις συνθήκες του Θεωρήματος του **Zeckendorf** χρησιμοποιώντας έναν «άπληστο αλγόριθμο » σε κάθε στάδιο, επιλέγει τον μεγαλύτερο δυνατό αριθμό Fibonacci.

Ένας άπληστος αλγόριθμος θα μπορούσε να είναι ο εξής:

Ξεκινάμε με τον μεγαλύτερο Fibonacci αριθμό που είναι μικρότερος από τον αριθμό στόχο.

Στη συνέχεια επιλέγουμε τον μεγαλύτερο Fibonacci αριθμό που είναι μικρότερος από το υπόλοιπο που μένει αφού αφαιρέσουμε τον πρώτο αριθμό. Συνεχίζοντας τη διαδικασία σταματάμε όταν το υπόλοιπο είναι ένας Fibonacci αριθμός.

Κεφάλαιο 17 Οι πρώτοι αριθμοί του Mersenne και οι τέλειοι αριθμοί

Σε αυτή την παράγραφο θεωρούμε τους πρώτους αριθμούς που μπορούν να γραφούν στην μορφή $a^n - 1$ με $n \geq 2$.

Για παράδειγμα ο 31 είναι πράγματι **πρώτος αριθμός Mersenne** αφού $31 = 2^5 - 1$.

Στην συνέχεια ας παρατηρήσουμε τα παρακάτω παραδείγματα:

	$n=2$	$n=3$	$n=4$	$n=5$
$a=2$	3	7	$15=3\cdot 5$	31
$a=3$	8	26	80	243
$a=4$	15	63	255	1023
$a=5$	24	124	625	3124

Κάνουμε τις εξής παρατηρήσεις:

1. Αν ο a είναι περιττός, τότε ο $a-1$ είναι άρτιος, επομένως δεν μπορεί να είναι πρώτος.

2. Ο $a_n - 1$ πάντα διαιρείται από το $a-1$.

Απόδειξη

$a_n - 1 = (a-1)(a_{n-1} + a_{n-2} + ... + a_2 + a + 1)$

Επομένως ο $a_n - 1$ είναι σύνθετος εκτός και αν $a - 1 = 1 \Rightarrow a = 2$.

Στη συνέχεια φτιάχνουμε έναν πίνακα τιμών του $2^n - 1$:

n	2	3	4	5	6	7	8	9	10
$2^n - 1$	3	7	15	31	63	127	255	511	1023

Θεώρημα 17.1 Αν n διαιρείται με το m τότε ο $2^n - 1$ διαιρείται από το $2^m - 1$.

Απόδειξη

Έστω ότι $m \mid n$. Τότε υπάρχει ακέραιος k τέτοιος ώστε $n = m \cdot k$. Τότε $2^n = \left(2^m\right)^k$

και $2^n - 1 = \left(2^m\right)^k - 1 = \left(2^m - 1\right) \cdot \left(\left(2^m\right)^{k-1} + \left(2^m\right)^{k-2} + ... + \left(2^m\right)^2 + \left(2^m\right) + 1\right)$

Επομένως, αν n είναι σύνθετος, τότε ο $2^n - 1$ είναι σύνθετος και μπορούμε να συμπεράνουμε το παρακάτω αποτέλεσμα:

Θεώρημα 17.2

Αν ο $a^n - 1$ είναι πρώτος για κάποιους ακεραίους $a \geq 2$ και $n \geq 2$ τότε $a = 2$ και ο n είναι πρώτος.

Ορισμός 17.1 Πρώτοι αριθμοί της μορφής $2^p - 1$ καλούνται **πρώτοι αριθμοί του Mersenne.**

Μερικά παραδείγματα απο τους αριθμούς Mersenne είναι:

$2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$, $2^{13} - 1 = 8191$.

Παρατηρούμε ότι κάθε αριθμός της μορφής $2^p - 1$ δεν είναι απαραίτητα πρώτος.

Για παράδειγμα ο $2^{11} - 1 = 2047 = 23 \cdot 89$ δεν είναι πρώτος όπως και ο $2^{29} - 1 = 233 \cdot 1103 \cdot 2089$ δεν είναι πρώτος.

Δεν είναι γνωστό αν είναι άπειροι σε πλήθος οι πρώτοι αριθμοί του Mersenne. Ο μεγαλύτερος γνωστός αριθμός Mersenne είναι ο $2^{57885161} - 1$ που ανακαλύφθηκε το 2009 από τον Dr. Curtis Cooper.

Αυτός ο πρώτος έχει 17425170 ψηφία με τα σημερινά δεδομένα. (http://www.mersenne.org/default.php)

17.1 Εικασία των Πρώτων του Mersenne

Έστω p είναι ένας περιττός φυσικός αριθμός. Αν 2 απο τις παρακάτω προτάσεις είναι αληθινές τότε θα είναι και η τρίτη πρόταση αληθής.

1. $p = 2^k \pm 1$ ή $p = 4k \pm 3$
2. $2^p - 1$ είναι πρώτος
3. $\frac{2^p \pm 1}{3}$ είναι πρώτος

Συμπληρώνουμε τον παρακάτω πίνακα στην περίπτωση που η παραπάνω εικασία είναι αληθής.

p	Is $p = 2^k \pm 1$ or $p = 4k \pm 3$?	Is $2^p - 1$ a prime?	Is $\frac{2^p + 1}{3}$ prime?
3	✓	✓	
5	✓	✓	
7	✓	✓	
9	✓	✓	
11	✓	✓	
13		✓	✓

Ο ακέραιος 6 έχει την ιδιότητα οτι το άθροισμα των ορθών διαιρετων του 6 (ορθοί διαιρέτες του 6 είναι όλοι οι διαιρέτες του 6 εκτος απο το 6) είναι ίσο με 6: 1+2+3 = 6.

Οι αριθμοί με την παραπάνω ιδιότητα καλούνται **τέλειοι αριθμοί**. Έχει βρεθεί μέθοδος που βρίσκει τέλειους αριθμούς που είναι στενά συνεδεμένοι με τους πρώτους αριθμούς Merenne.

Θεώρημα 17.3 Τύπος του Euclid των τέλειων αριθμών

Αν 2^p-1 είναι πρώτος αριθμός τότε ο $2^{p-1}\left(2^p-1\right)$ είναι τέλειος αριθμός.

Οι αρχικοί 2 πρώτοι του Mersenne είναι $2^2-1=3$ και $2^3-1=7$. Αν εφαρμόσουμε τον τύπο του Euclid των τέλειων αριθμών στους 2 αυτούς πρώτους του Mersenne παίρνουμε τις 2 τέλειους αριθμούς 6 και 28.

Ο επόμενος πρώτος του Mersenne είναι ο $2^5-1=31$.

Ο τύπος του Euclid μας δίνει τον τέλειο αριθμό 496. Για να ελέγξουμε οτι ο 496 είναι τέλειος αριθμός πρέπει να προσθέσουμε τους ορθούς διαιρέτες του 496.

Παραγοντοποιούμε το 496 οπότε και έχουμε $496=2^4\cdot 31$, επομένως οι ορθοί διαιρέτες είναι:

$1,2,2^2,2^3,2^4,31,2\cdot 31,2^2\cdot 31,2^3\cdot 31$.

Για να υλοποιήσουμε την γενική μέθοδο που θα χρησιμοποιήσουμε για να αποδείξουμε τον τύπο του Euclid θα προσθέσουμε τους ορθούς διαιρέτες σε δύο στάδια.

Αρχικά $1+2+2^2+2^3+2^4=31$ και στη συνέχεια $31+2\cdot 31+2^2\cdot 31+2^3\cdot 31=31\cdot 15$.

Οπότε $31+31\cdot 15=496$.

Άρα ο 496 είναι πράγματι τέλειος αριθμός. Μπορούμε να χρησιμοποιήσουμε μια παρόμοια ιδέα για να αποδείξουμε τον τύπο του Euclid.

Απόδειξη

΄Εστω ότι ο 2^p-1 είναι πρώτος . Τότε οι ορθοί διαιρέτες του $2^{p-1}(2^p-1)$ είναι:

$1,2,2^2,2^3,...,2^{p-1}$ και $2^p-1,2\cdot(2^p-1),2^2\cdot(2^p-1),..,2^{p-2}\cdot(2^p-1)$.

Προσθέτουμε τους παραπάνω διαιρέτες οπότε και έχουμε:

$$1+2+2^2+2^3+...+2^{p-1}=\frac{2^p-1}{2-1}=2^p-1.$$

$$(2^p-1)+2(2^p-1)+2^2(2^p-1)+...+2^{p-2}(2^p-1)=(2^p-1)(1+2+2^2+...+2^{p-2})$$

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

$$=(2^p-1)(2^{p-1}-1)$$

Τότε το άθροισμα των ορθών διαιρετών του $(2^{p-1})(2^p-1)$ είναι

$$(2^p-1)+(2^p-1)(2^{p-1}-1)=2^{p-1}(2^p-1).$$

Επομένως, ο $(2^{p-1})(2^p-1)$ είναι πράγματι πρώτος αριθμός.

Μια ερώτηση που προκύπτει στη συνέχεια είναι αν ο τύπος του Euclid πράγματι περιγράφει

όλους τους τέλειους αριθμούς. Έχει κάθε τέλειος αριθμός την μορφή $(2^{p-1})(2^p-1)$ με 2^p-1 πρώτο ή υπάρχουν και άλλοι τέλειοι αριθμοί;

Οι απαντήσεις στα παραπάνω ερωτήματα ήρθαν 2000 χρόνια μετά τον θάνατο του Euclid, από τον Euler που απέδειξε οτι ο τύπος του Euclid δίνει όλους τους άρτιους τέλειους αριθμούς.

Κεφάλαιο 18ο

Δυνάμεις ισοϋπόλοιπων m και ακόλουθα τετράγωνα

Πώς θα υπολογίσουμε το $5^{100000000000000} \bmod 12830603$;

Αν ο 12830603 ήταν πρώτος αριθμός θα χρησιμοποιούσαμε το Μικρό Θεώρημα του Fermat. Εναλλακτικά αν δεν ήταν πρώτος αριθμός το Θεώρημα των Euler – Fermat. Παρ'όλ'αυτά θα θέλαμε να υπολογίσουμε το $5^{100000000000000} \bmod 12830603$ χωρίς να παραγοντοποιήσουμε το 12830603. Αυτό που πραγματικά θέλουμε να πετύχουμε είναι να είμαστε σε θέση να υπολογίσουμε ισοϋπόλοιπα της μορφής $a^k \bmod m$ για αριθμούς *α*, *k*, *m* που έχουν εκατοντάδες ψηφία, έτσι ώστε σίγουρα να μη χρειάζεται να παραγοντοποιήσουμε πρώτα το m. Αυτοί οι υπολογισμοί είναι σημαντικοί στη μελέτη της RSA Public Key Cryptography.

Η μέθοδος που θα χρησιμοποιήσουμε για να υπολογίσουμε το $a^k \bmod m$ καλείται *διαδοχικός τετραγωνισμός* (*successive squaring*). Θα παρουσιάσουμε την ιδέα με ένα παράδειγμα.

Παράδειγμα 18.1 Υπολογίστε το $7^{327} \bmod 853$.

Παρατηρούμε ότι:

$$327 = 256 + 64 + 4 + 2 + 1.$$

και

$$7^{327} = 7^{256} \cdot 7^{64} \cdot 7^4 \cdot 7^2 \cdot 7^1.$$

Μπορούμε να υπολογίσουμε τις 2^k δυνάμεις του 7 mod 853 με διαδοχικό τετραγωνισμό (*successive squaring*) όπως παρουσιάζεται παρακάτω:

$$7^1 = 7 \bmod 853$$

$$7^2 = 49 \bmod 853$$

$$7^4 = (49)^2 \equiv 695 \bmod 853$$

$$7^8 = (695)^2 \equiv 227 \bmod 853$$

$$7^{16} = (227)^2 \equiv 349 \bmod 853$$

$$7^{32} = (349)^2 \equiv 675 \bmod 853$$

$$7^{64} = (675)^2 \equiv 123 \bmod 853$$

$$7^{128} = (123)^2 \equiv 628 \bmod 853$$

$$7^{256} = (628)^2 \equiv 298 \bmod 853$$

και

$$7^{327} = 7^{256} \cdot 7^{64} \cdot 7^4 \cdot 7^2 \cdot 7^1$$

$$\equiv 298 \cdot 123 \cdot 695 \cdot 49 \cdot 7 \bmod 853$$

$$\equiv 828 \cdot 695 \cdot 49 \cdot 7 \bmod 853$$

$$\equiv 538 \cdot 49 \cdot 7 \bmod 853$$

$$\equiv 727 \cdot 7 \bmod 853$$

$$\equiv 286 \bmod 853 .$$

Παράδειγμα 18.2 Χρησιμοποιώντας τη μέθοδο διαδοχικού τετραγωνισμού, δείξτε ότι

$$2^{283976710803262} \equiv 280196559097287 \bmod 283976710803263 .$$

Ο αριθμός 283976710803263 είναι πρώτος ή σύνθετος;

Λύση:

Αν ο αριθμός 283976710803263 ήταν πρώτος τότε ο αριθμός $2^{283976710803262}$ θα ήταν ισότιμος με το $1 \bmod 283976710803263$. Άρα ο 283976710803263 είναι σύνθετος. Σημειώνεται ότι προσδιορίστηκε ότι ο αριθμός 283976710803263 είναι σύνθετος χωρίς να υπολογιστεί κάποιος παράγοντας.

Κεφάλαιο 19^{ο} Υπολογισμός ριζών *k*-τάξης modulo m

Μάθαμε πώς να επιλύουμε γραμμικές ισοτιμίες της μορφής $ax \equiv b \bmod m$ και γραμμικές ισοτιμίες της μορφής $x^2 \equiv b \bmod m$. Σε αυτή την ενότητα θα αναπτύξουμε τεχνικές για να επιλύσουμε ισοτιμίες της μορφής

$$x^k \equiv b \bmod m,$$

όπου $k \geq 3$. Αυτές οι μέθοδοι είναι σημαντικές στη μελέτη της RSA Public Key Cryptography.

Παράδειγμα 19.1 Επιλύστε την ισοτιμία

$x^{131} \equiv 758 \bmod 1073$.

Λύση:

Αρχικά υπολογίζουμε το $\phi(1073)$. Αφού $1073 = 29 \cdot 37$,

$\phi(1073) = \phi(29) \cdot \phi(37) = 28 \cdot 36 = 1008$.

Στη συνέχεια παρατηρούμε ότι $\gcd(131, 1008) = 1$, επομένως υπάρχουν ακέραιοι u και v έτσι ώστε $131u + 1008v = 1$.

Στη συνέχεια χρησιμοποιώντας τη μέθοδο που παρουσιάστηκε στο κεφάλαιο 4, βρίσκουμε $u = 731$ και $v = -95$. Επομένως, $131 \cdot 731 - 1008 \cdot 95 = 1$. Χρησιμοποιώντας αυτή την ισότητα έχουμε:

$\left(x^{131}\right)^{731} = x^{131 \cdot 731} = x^{1+1008 \cdot 95} = x \cdot \left(x^{1008}\right)^{95}$.

Από το Θεώρημα των Euler – Fermat έχουμε,

$x^{1008} \equiv 1 \bmod 1073$.

Επομένως,

$\left(x^{131}\right) \equiv x \bmod 1073$,

Συνεπώς οι αρχικές ισοτιμίες γίνονται

$x \equiv \left(x^{131}\right)^{731} \equiv 758^{731} \bmod 1073$.

Άρα για να βρούμε τη λύση της αρχικής ισοτιμίας, πρέπει να υπολογίσουμε $758^{731} \bmod 1073$. Αυτό το πετυχαίνουμε χρησιμοποιώντας τη μέθοδο του διαδοχικού τετραγωνισμού (*successive squaring*). Αρχικά παρατηρούμε ότι:

$731 = 512 + 128 + 64 + 16 + 8 + 2 + 1$

$758^{731} = 758^{512} \cdot 758^{128} \cdot 758^{64} \cdot 758^{16} \cdot 758^{8} \cdot 758^{2} \cdot 758^{1}$.

Υπολογίζοντας τις δυνάμεις του $758 \bmod 1073$, παίρνουμε:

$$758 \equiv 758 \bmod 1073$$

$$758^2 \equiv 509 \bmod 1073$$

$$758^4 \equiv 488 \bmod 1073$$

$$758^8 \equiv 1011 \bmod 1073$$

$$758^{16} \equiv 625 \bmod 1073$$

$$758^{32} \equiv 53 \bmod 1073$$

$$758^{64} \equiv 663 \bmod 1073$$

$$758^{128} \equiv 712 \bmod 1073$$

$$758^{256} \equiv 488 \bmod 1073$$

$$758^{512} \equiv 1011 \bmod 1073 .$$

Επομένως,

$$\begin{aligned} 758^{731} &= 758^{512} \cdot 758^{128} \cdot 758^{64} \cdot 758^{16} \cdot 758^{8} \cdot 758^{2} \cdot 758^{1} \\ &\equiv 1011 \cdot 712 \cdot 663 \cdot 625 \cdot 1011 \cdot 509 \cdot 758 \bmod 1073 \\ &\equiv 922 \cdot 197 \cdot 632 \cdot 758 \bmod 1073 \\ &\equiv 297 \cdot 498 \bmod 1073 \\ &\equiv 905 \bmod 1073 . \end{aligned}$$

Τέλος, μπορούμε να χρησιμοποιήσουμε τη μέθοδο του διαδοχικού τετραγωνισμού (*successive squaring*) για να ελέγξουμε ότι $905^{131} \equiv 758 \bmod 1073$.

Η γενική μέθοδος για να υπολογίσουμε ρίζες *k*-τάξης modulo m περιγράφεται με τον ακόλουθο αλγόριθμο.

Αλγόριθμος 19.1 Υπολογισμός ριζών *k*-τάξης modulo m. Έστω *b*, *k* και *m* ακέραιοι τέτοιοι ώστε $\gcd(b, m) = 1$ και $\gcd(k, \phi(m)) = 1$.

Τότε τα ακόλουθα βήματα επιλύουν την ισοτιμία $x^k \equiv b \bmod m$:

1. Υπολόγισε το $\phi(m)$.
2. Χρησιμοποίησε τον Ευκλείδειο Αλγόριθμο για να βρεις δύο ακεραίους που ικανοποιούν την εξίσωση $ku + \phi(m)v = 1$.
3. Υπολόγισε το $b^u \bmod m$ με τη μέθοδο του διαδοχικού τετραγωνισμού. Η τιμή που λαμβάνεται αποτελεί τη λύση x.

Απόδειξη:

Πρέπει να αποδείξουμε ότι η $x = b^u$ είναι μία λύση της ισοτιμίας $x^k \equiv b \bmod m$.

$$x^k = \left(b^u\right)^k = b^{uk} = b^{1-\phi(m)u} = b \cdot \left(b^{\phi(m)}\right)^{-u} \equiv b \bmod m .$$

Κεφάλαιο 20 RSA Public Key - Κρυπτογραφία

Σε αυτή την παράγραφο περιγράφουμε μια τεχνική για να κωδικοποιούμε και αποκωδικοποιούμε μηνύματα.

1. Το πρώτο βήμα για να κωδικοποιήσουμε ένα μήνυμα είναι να το μετατρέψουμε σε ακολουθία αριθμών.

   Μια απλή μέθοδος για να το επιτύχουμε αυτό είναι να θέσουμε $A=11, B=12, C=13..., Z=36$.

   Στον παρακάτω πίνακα φαίνονται οι παραπάνω αντιστοιχήσεις:

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

   Ας παρατηρήσουμε οτι έχουμε αγνοήσει τα κενά και άλλα σημεία στίξης.

2. Στη συνέχεια επιλέγουμε 2 μεγάλους πρώτους p και q και αφού τους πολλαπλασιάσουμε προκύπτει ένα ισουπόλοιπο $m = p \cdot q$. Επιπλέον υπολογίζουμε το $\varphi(\mathrm{m}) = \varphi(p \cdot q) = (\mathrm{p}-1)\cdot(\mathrm{q}-1)$.

3. Στη συνέχεια επιλέγουμε έναν αριθμό k τέτοιο ώστε $\mathrm{MK\Delta}(\mathrm{k}, \varphi(m)) = 1$.

4. Στη συνέχεια δημοσιεύουμε τους αριθμούς k και m στο κοινό και κρατάμε τους αριθμούς p και q μυστικούς.

5. Κάποιος που θέλει να κωδικοποιήσει ένα μήνυμα και να μας το στείλει μπορεί να χρησιμοποιήσει τους αριθμούς k και m για να κωδικοποιήσει το μήνυμα με τον παρακάτω τρόπο:

   (a) Αρχικά μετατρέπουν το μήνυμα τους σε μια ακολουθία από αριθμούς όπως περιγράψαμε παραπάνω.

   (b) Στη συνέχεια, παρατηρούμε τον αριθμό m και σπάμε τα αντίστοιχα ψηφία του σε αριθμούς που είναι μικρότεροι από το m έτσι ώστε το μήνυμα να είναι μια λίστα αριθμών $a_1, a_2, ..., a_r$.

   (c) Στη συνέχεια χρησιμοποιώντας την μέθοδο διαδοχικού τετραγωνισμού (successive squaring) υπολογίζουμε τις δυνάμεις $a_1^{\,k} \bmod m$, $a_2^{\,k} \bmod m$, $..., a_r^{\,k} \bmod m$.

   Αυτές οι τιμές δημιουργούν μια νέα λίστα τιμών $b_1, b_2, .., b_r$.

   Αυτή η λίστα είναι το κωδικοποιημένο μήνυμα.

6. Για να αποκωδικοποιήσουμε το μήνυμα αφού το λάβουμε κωδικοποιημένο χρησιμοποιούμε την παρακάτω μέθοδο.

(a) Έχουμε λάβει την λίστα των αριθμών $b_1, b_2, .., b_r$ και θέλουμε να ανακτήσουμε τους αριθμούς $a_1, a_2, ..., a_r$.

(b) Υπενθυμίζουμε ότι κάθε b_i είναι ισότιμο με $a_i^k \bmod m$, οπότε για να βρούμε κάθε a_i πρέπει να λύσουμε την ισοτιμία: $x^k \equiv b_i \bmod m$.

Χρησιμοποιούμε τον Αλγόριθμο για τον υπολογισμό ριζών κ τάξης modulo m (όπως περιγράφετε σε προηγούμενο κεφάλαιο) και αυτό μπορούμε να το κάνουμε αν γνωρίζουμε το $\varphi(m)$.

(c) Αφού γνωρίζουμε τις τιμές των αριθμών p και q με $m = p \cdot q$.

Γνωρίζουμε ότι $\varphi(m) = \varphi(p \cdot q) = (p-1)(q-1) = pq - p - q + 1 = m - p - q + 1$.

(d) Τέλος εφαρμόζουμε τον Αλγόριθμο για τον υπολογισμό ριζών κ τάξης modulo m για να λύσουμε καθεμία από τις ισοτιμίες $x^k \equiv b_i \bmod m$. Οι λύσεις είναι οι αριθμοί $a_1, a_2, ..., a_r$. Στη συνέχεια χρησιμοποιούμε αυτή την ακολουθία των ψηφίων για να ανακτήσουμε το αρχικό μήνυμα.

Για παράδειγμα ο αλγόριθμος υπολογισμού ριζών κ τάξης modulo m είναι ο εξής:

Έστω b, k και m είναι ακέραιοι τέτοιοι ώστε $\text{ΜΚΔ}(b, m) = 1$ και $\text{ΜΚΔ}(k, \varphi(m)) = 1$.

Τότε τα επόμενα βήματα δίνουν μια λύση στην ισοτιμία $x^k \equiv b \bmod m$.

i) Υπολόγισε το $\varphi(m)$.

ii) Χρησιμοποίησε τον Ευκλείδειο Αλγόριθμο για να βρεις ακεραίους u και v που ικανοποιούν την σχέση $ku + \varphi(m)v = 1$.

iii) Υπολόγισε το $b^u \bmod m$ με την μέθοδο του διαδοχικού τετραγωνισμού. Η τιμή που λαμβάνετε αποτελεί την λύση x.

Παράδειγμα 20.1 Κωδικοποιήσε το μήνυμα 'STANFORD' χρησιμοποιώντας το δημόσιο κλειδί $m = 143$ και $k = 23$.

Λύση

Αρχικά μετατρέπουμε το κείμενο 'STANFORD' σε μια ακολουθία απο αριθμούς: 2930111416252814.

Ο αριθμός m έχει 3 ψηφία, οπότε χωρίζουμε το μήνυμα 2930111416252814 σαν να είναι μια ακολουθία αριθμών με 2 ψηφία το καθένα: 29, 30, 11, 24, 16, 25, 28, 14

Στη συνέχεια χρησιμοποιούμε τη μέθοδο του διαδοχικού τετραγωνισμού για να υπολογίσουμε την $23^{η}$ δύναμη απο κάθε αριθμό modulo 143.

Άρχικά υπολογίζουμε το $29^{23} \bmod 143$ οπότε και έχουμε:

$29^{23} \equiv 29^{16}29^{4}29^{2}29^{1}$

$29 \equiv 29 \bmod 143$

$29^{2} \equiv 126 \bmod 143$

$29^{4} \equiv 3 \bmod 143$

$29^{8} \equiv 9 \bmod 143$

$29^{16} \equiv 81 \bmod 143$

Άρα $29^{23} \equiv 81 \cdot 3 \cdot 126 \cdot 29 \equiv 35 \bmod 143$.

Έπειτα χρησιμοποιούμε τη μέθοδο του διαδοχικού τετραγωνισμού για να υπολογίσουμε την 23η δύναμη απο κάθε αριθμό που απομένει modulo 143:

$29^{23} \equiv 35 \bmod 143$

$30^{23} \equiv 127 \bmod 143$

$11^{23} \equiv 110 \bmod 143$

$24^{23} \equiv 19 \bmod 143$

$16^{23} \equiv 48 \bmod 143$

$25^{23} \equiv 38 \bmod 143$

$28^{23} \equiv 7 \bmod 143$

$14^{23} \equiv 27 \bmod 143$

Παράδειγμα 20.2 Να αποκωδικοποιήσετε το μήνυμα 20, 130, 62, 107 χρησιμοποιώντας τους πρώτους αριθμούς p = 11 και q = 13 και k = 23.

Λύση

Πρέπει να λύσουμε τις παρακάτω ισοτιμίες modulo 143.

$a_1^{23} \equiv 20 \bmod 143$

$a_2^{23} \equiv 130 \bmod 143$

$a_3^{23} \equiv 62 \bmod 143$

$a_4^{23} \equiv 107 \bmod 143$

Μπορούμε να λύσουμε τις παραπάνω ισοτιμίες χρησιμοποιώντας τον αλγόριθμο υπολογισμού ριζών κ τάξης modulo m. Αφού γνωρίζουμε οτι p = 11 και q = 13 μπορουμε να υπολογίσουμε το $\varphi(\mathrm{m}) = \varphi(11) \cdot \varphi(13) = 10 \cdot 12 = 120$.

Στη συνέχεια βρίσκουμε ακεραίους u και v τέτοιους ώστε $23 \cdot u + 120 \cdot v = 1$.

Χρησιμοποιώντας τον Ευκλείδειο Αλγόριθμο θα λάβουμε $u = 47$ και $v = -9$.

Οπότε είμαστε σε θέση να λύσουμε κάθε ισοτιμία. Για να λύσουμε την 1η ισοτιμία modulo 143 υπολογίζουμε το $20^u \equiv 20^{47}$ modulo 143 με τη μέθοδο του διαδοχικού τετραγωνισμού.

Άρα έχουμε:

$20^{47} \equiv 20^{32}20^{8}20^{4}20^{2}20^{1}$

$20^{1} \equiv 20 \bmod 143$

$20^{2} \equiv 114 \bmod 143$

$20^{4} \equiv 126 \bmod 143$

$20^{8} \equiv 3 \bmod 143$

$20^{16} \equiv 9 \bmod 143$

$20^{32} \equiv 81 \bmod 143$

Οπότε $20^{47} \equiv 20 \cdot 114 \cdot 126 \cdot 3 \cdot 81 \equiv 15 \bmod 143$.

Συνεπώς, ο πρώτος αριθμός του μηνύματος είναι ο 15 που αντιστοιχεί στο γράμμα Ε. Με τον ίδιο τρόπο λύνονται οι 3 ισοτιμίες που απέμειναν ώστε να καταφέρουμε να αποκωδικοποιήσουμε το μήνυμα.

Παράδειγμα 20.3 Να κωδικοποιήσετε το μήνυμα 'To be or not to be' χρησιμοποιώντας τους πρώτους p = 12553 και q = 13007.

Λύση

Αρχικά υπολογίζουμε το $m = p \cdot q = 12553 \cdot 13007 = 163276871$ και το $\varphi(m) = 163251312$.

Χρειαζόμαστε να επιλέξουμε ένα k που είναι σχετικά πρώτοι με το $\varphi(m)$. Επιλέγουμε $k = 79921$.

Το μήνυμα 'TOBEORNOTTOBE' γίνεται ακολουθία ψηφίων με βάση τον αρχικό πίνακα που περί 302512152528242530302512 15.

Η ισοτιμία modulo m με m = 163276871 έχει 9 ψηφία οπότε το σπάμε σε 8ψήφιους αριθμούς : 30251215, 25282425, 30302512, 15.

Στη συνέχεια χρησιμοποιούμε τη μέθοδο του διαδοχικού τετραγωνισμού για να υψώσουμε καθε έναν απο τους αριθμούς στην κ-οστή δύναμη modulo m:

$30251215^{79921} \equiv 149419241 \bmod 163276871$

$25282425^{79921} \equiv 62721998 \bmod 163276871$

$30302512^{79921} \equiv 118084566 \bmod 163276871$

$15^{79921} \equiv 40481382 \bmod 163276871$

Άρα το κωδικοποιημένο μήνυμα είναι η λίστα αριθμών 149419241, 62721998, 118084566, 40481382.

Είναι επακόλουθο να αναρωτηθεί κάποιος πόσο ασφαλές είναι το συγκεκριμένο κρυπτοσύστημα. Ας υποθέσουμε οτι το μύνημα υποκλάπτεται απο τρίτους. Αφού το m και το k είναι δημόσια τότε ο υποκλοπέας μπορεί να αποκωδικοποίησει το μήνυμα αν μπορεί να βρεί την τιμή του $\varphi(m) = \varphi(p) \cdot \varphi(q)$.

Άρα για να αποκωδικοποιήσεις το μήνυμα, ο υποκλοπέας πρέπει να παραγοντοποιήσει το m για να βρει το p και το q. Αν το m έχει από 5 έως 10 ψηφία τότε ένας υπολογιστής μπορεί να βρει τους παράγοντες του m σχεδόν ακαριαία. Χρησιμοποιώντας εξειδικευμένες μέθοδοι από την θεωρία αριθμών, οι μαθηματικοί έχουν κατασκευάσει τεχνικές για να παραγοντοποιούν αριθμούς με 50 έως 100 ψηφία.

Επομένως, αν οι πρώτοι p και q έχουν 100 ψηφία ο καθένας τότε δεν υπάρχουν γνωστές τεχνικές για τον υποκλοπέα να καθορίσει τους p και q από τον $m = p \cdot q$.

Η ιδέα που βασίζεται η παραπάνω τεχνική είναι πως παρόλο που είναι εύκολο να πολλαπλασιάσουμε 2 μεγάλους αριθμούς, είναι πολύ δύσκολο να παραγοντοποιήσουμε έναν μεγάλο αριθμό.

Η κρυπτογραφική μέθοδος που παρουσιάστηκε παραπάνω καλείται **κρυπτοσύστημα δημοσίου κλειδιού** γιατί το κλειδί της κωδικοποίησης αποτελείται από το m και τον εκθέτη k που μπρορούν να διανεμηθούν στο κοινό ενώ η μέθοδος της αποκωδικοποίησης παραμένει ασφαλής. Αυτό το συγκεκριμένο κρυπτοσύστημα καλείται RSA **κρυπτοσύστημα δημοσίου κλειδιού** και ονομάστηκε απο τους εφευρέτες του Ron Rivest, Adi Shamir και Leonard Adleman που το ανακάλυψαν το 1977.

Κεφάλαιο 21 Πυθαγόρειες τριάδες

Ορισμός: Μια **πυθαγόρεια τριάδα** είναι μια τριάδα (a,b,c) ακεραίων τέτοια ώστε $a^2+b^2=c^2$.

Η μελέτη των πυθαγορείων τριάδων ξεκίνησε πολύ πριν από τους Πυθαγόρειους. Στην πραγματικότητα υπήρχαν βαβυλώνιες πλάκες (αβάκια) που χρονολογούνται το 1800 π.χ. και περιείχαν λίστες με τέτοιες τριπλέτες αρκετά μεγάλες, το οποίο φανερώνει ότι οι Βαβυλώνιοι πιθανότατα είχαν μια συστηματική μέθοδο για να παράγουν τις πυθαγόρειες τριάδες.

- Αποδεικνύεται ότι υπάρχουν άπειρες πυθαγόρειες τριάδες .Η ιδέα της απόδειξης είναι να θεωρήσουμε ότι αν (a,b,c) είναι μια πυθαγόρεια τριάδα και να αποδειχθεί ότι και η τριάδα $(a\cdot d,b\cdot d,c\cdot d)$ είναι επίσης πυθαγόρεια τριάδα για κάθε ακέραιο d.
- Μια **πρωταρχική Πυθαγόρεια Τριάδα** είναι μια τριάδα αριθμών (a,b,c) που δεν έχει κανένας από τους a,b,c κοινό παράγοντα και ικανοποιούν την σχέση $a^2+b^2=c^2$.
- Αποδεικνύεται ότι αν (a,b,c) είναι μια πρωταρχική πυθαγόρεια τριάδα τότε ή ο a είναι περιττός και ο b άρτιος ή ο a είναι άρτιος και ο b περιττός. Σε οποιαδήποτε περίπτωση αποδεικνύεται ότι ο c είναι πάντα περιττός.
- Παρατηρούμε ότι αν (a,b,c) είναι μια πρωταρχική πυθαγόρεια τριάδα τότε $a^2=c^2-b^2=(c-b)(c+b)$.

Για παράδειγμα:

$3^2=5^2-4^2=(5-4)(5+4)=1\cdot 9$

$8^2=17^2-15^2=(17-15)(17+15)=2\cdot 32=64$

$33^2=65^2-56^2=(65-56)(65+56)=9\cdot 121=1089$

$20^2=29^2-21^2=(29-21)(29+21)=8\cdot 50=400$

$16^2=65^2-63^2=(65-63)(65+63)=2\cdot 128=256$

Κεφάλαιο 22ο Ποιοι πρώτοι αριθμοί είναι άθροισμα δύο τετραγώνων;

Σε αυτή την ενότητα θα απαντήσουμε στο ακόλουθο ερώτημα: ποιοι πρώτοι αριθμοί μπορούν να γραφτούν ως άθροισμα δύο τετραγώνων; Για παράδειγμα ο αριθμός 5 είναι άθροισμα δύο τετραγώνων, δεδομένου ότι $5 = 1^2 + 2^2$.

Από την άλλη το 19 δεν μπορεί να γραφτεί ως άθροισμα δύο τετραγώνων. Για να ελέγξουμε αυτό, αρκεί να παρατηρήσουμε ότι καμία από τις διαφορές:

$19 - 1^2 = 18$, $19 - 2^2 = 15$, $19 - 3^2 = 10$, $19 - 4^2 = 3$ δεν είναι τετράγωνο κάποιου άλλου αριθμού. Γενικά, για να ελέγξουμε αν ένας αριθμός *m* είναι άθροισμα δύο τετραγώνων ελέγχουμε τους αριθμούς

$m - 0^2$, $m - 1^2$, $m - 2^2$, ...

μέχρι να λάβουμε έναν τετράγωνο αριθμό ή μέχρι οι αριθμοί να γίνουν αρνητικοί.

a) i. Δημιούργησε μία λίστα πρώτων αριθμών *p*, $5 \le p \le 229$ που μπορούν να γραφτούν ως άθροισμα δύο τετραγώνων. (Αγνόησε τον αριθμό 2)

   ii. Δημιούργησε μία λίστα πρώτων αριθμών *p*, $3 \le p \le 227$ που δεν μπορούν να γραφτούν ως άθροισμα δύο τετραγώνων.

   iii. Παρατηρείς κάποιο μοτίβο? Θεώρησε τους πρώτους αριθμούς modulo 4. Αν $p \equiv 1 \bmod 4$ ο *p* είναι πάντα ή κάποιες φορές ή και καμία φορά άθροισμα δύο τετραγώνων; Αν $p \equiv 3 \bmod 4$ ο *p* είναι πάντα ή κάποιες φορές ή και καμία φορά άθροισμα δύο τετραγώνων;

b) Απέδειξε ότι αν ο πρώτος *p* μπορεί να γραφτεί ως άθροισμα δύο τετραγώνων τότε $p \equiv 1 \bmod 4$.

c) Στο επόμενο πρόβλημα θα αποδείξουμε ότι αν ο *p* είναι ένας πρώτος αριθμός που είναι ισότιμος με το 1 modulo 4, τότε ο *p* μπορεί να γραφτεί ως άθροισμα δύο τετραγώνων. Σε αυτό το πρόβλημα θα εργαστούμε μέσω της αποδεικτικής μεθόδου που είναι γνωστή ως Διαδικασία Υποβιβασμού του Fermat (*Fermat's Descent Procedure*), για ένα συγκεκριμένο *p* = 881.

   I. Επαλήθευσε ότι $387^2 + 1^2 = 170 \cdot 881$. Επομένως, έχουμε ένα πολλαπλάσιο του p ως άθροισμα δύο τετραγώνων.

   II. Διαπίστωσε ότι $u = 47$ και $v = 1$ ικανοποιούν: $u = 387 \bmod 170$, $v = 1 \bmod 170$, $-\frac{170}{2} \le u, v \le \frac{170}{2}$.

   III. Διαπίστωσε ότι $47^2 + 1^2 = 170 \cdot 13$ και $387^2 + 1^2 = 170 \cdot 881$.

   IV. Πολλαπλασίασε τις εξισώσεις του προηγούμενου βήματος και δείξε ότι

$\left(47^2+1^2\right)\cdot\left(387^2+1^2\right)=170^2\cdot 13\cdot 881$.

V. Χρησιμοποίησε την ταυτότητα $\left(u^2+v^2\right)\cdot\left(A^2+B^2\right)=\left(uA+vB\right)^2+\left(vA-uB\right)^2$ για να δείξεις ότι $18190^2+340^2=170^2\cdot 13\cdot 881$.

VI. Διαίρεσε με 1702 για να δείξεις ότι $107^2+2^2=13\cdot 881$.

VII. Παρατήρησε ότι ένα μικρότερο πολλαπλάσιο του 881 έχει γραφτεί ως άθροισμα δύο τετραγώνων και ότι μπορείς να επαναλάβεις τη διαδικασία μέχρι το ίδιο το p να γραφτεί ως άθροισμα δύο τετραγώνων.

d) Σε αυτό το πρόβλημα θα χρησιμοποιήσουμε τη Διαδικασία Υποβιβασμού του Fermat (*Fermat's Descent Procedure*) για να αποδείξουμε ότι αν $p\equiv 1 \bmod 4$, τότε το *p* μπορεί να γραφτεί ως άθροισμα δύο τετραγώνων. Συνεπώς, ας υποθέσουμε ότι το *p* είναι ένας πρώτος ισότιμος με το 1 modulo 4.

I. Δείξε ότι υπάρχει ένας ακέραιος A τέτοιος ώστε $p\mid\left(A^2+1\right)$. Υπόδειξη: Χρησιμοποίησε το τετραγωνικό ισοϋπόλοιπο. Επομένως, υπέθεσε ότι υπάρχει ένας ακέραιος A τέτοιος ώστε A $p\mid\left(A^2+1\right)$. Ισχύει ότι αν $p\equiv 1 \bmod 4$ υπάρχει ένας ακέραιος A τέτοιος ώστε A $p\mid\left(A^2+1\right)$.

II. Δείξε ότι υπάρχουν ακέραιοι B (B = 1) και M τέτοιοι ώστε $A^2+B^2=Mp$. Δείξε ότι M < p.

III. Παρατήρησε ότι αν $M=1$ αποδείχθηκε το ζητούμενο, διαφορετικά υπέθεσε ότι $M\geq 2$. Επέλεξε αριθμούς u, v για τους οποίους να ισχύει:

$u\equiv A \bmod M$, $v\equiv B \bmod M$, $-\frac{1}{2}M\leq u,v\leq\frac{1}{2}M$.

IV. Δείξε ότι υπάρχει ένας ακέραιος r τέτοιος ώστε $u^2+v^2=Mr$.

V. Δείξε ότι $\left(u^2+v^2\right)\left(A^2+B^2\right)=M^2rp$.

VI. Δείξε ότι $r\geq 1$.

VII. Δείξε ότι $r<M$.

VIII. Δείξε ότι $M\mid\left(uA+vB\right)$. Υπόδειξη: Χρησιμοποίησε την ταυτότητα $\left(u^2+v^2\right)\cdot\left(A^2+B^2\right)=\left(uA+vB\right)^2+\left(vA-uB\right)^2$.

IX. Δείξε ότι $M\mid\left(vA-uB\right)$. Υπόδειξη: Χρησιμοποίησε την ταυτότητα $\left(u^2+v^2\right)\cdot\left(A^2+B^2\right)=\left(uA+vB\right)^2+\left(vA-uB\right)^2$.

X. Κατέληξε στη σχέση:

$\left(\frac{uA+vB}{M}\right)^2+\left(\frac{vA-uB}{M}\right)^2=rp$.

Αυτό σημαίνει ότι ένα μικρότερο πολλαπλάσιο του p έχει γραφτεί ως άθροισμα δύο τετραγώνων.

XI. Παρατήρησε ότι αυτή η διαδικασία μπορεί να επαναληφθεί προκειμένου να γράψουμε ένα ακόμη μικρότερο πολλαπλάσιο του p ως άθροισμα δύο τετραγώνων. Επαναλαμβάνοντας τη διαδικασία συνεχώς, θα καταλήξουμε στο να έχουμε γράψει το ίδιο το p ως άθροισμα δύο τετραγώνων.

e) Δημιούργησε μία λίστα με όλους τους πρώτους $p < 50$ που μπορούν να γραφτούν στη μορφή $p = a^2 + ab + b^2$. Π.χ. $p = 7$ έχει αυτή τη μορφή με $a = 2$ και $b = 1$, ενώ το $p = 11$ δεν μπορεί να γραφτεί σε αυτή τη μορφή. Προσπάθησε να βρεις ένα μοτίβο, να εικάσεις ποιοι ακριβώς πρώτοι αριθμοί έχουν αυτή τη μορφή και προσπάθησε σε κάθε περίπτωση να αποδείξεις την εικασία σου.

f) Δημιούργησε μία λίστα με όλους τους πρώτους $p < 50$ που μπορούν να γραφτούν στη μορφή $p = a^2 + 2b^2$. Προσπάθησε να βρεις ένα μοτίβο, να εικάσεις ποιοι ακριβώς πρώτοι αριθμοί έχουν αυτή τη μορφή και προσπάθησε σε κάθε περίπτωση να αποδείξεις την εικασία σου.

g) Υπέθεσε ότι το p είναι ένας πρώτος όχι ίσος με 5. Αν το 5 μπορεί να γραφτεί στη μορφή $p = a + 5b^2$, δείξε ότι $p \equiv 1 \text{ or } 9 \bmod 20$.

h) Χρησιμοποίησε τη Διαδικασία Υποβιβασμού 2 φορές, ξεκινώντας από την εξίσωση $557^2 + 55^2 = 26 \cdot 12049$ για να γράψεις τον πρώτο αριθμό 12049 ως άθροισμα δύο τετραγώνων.

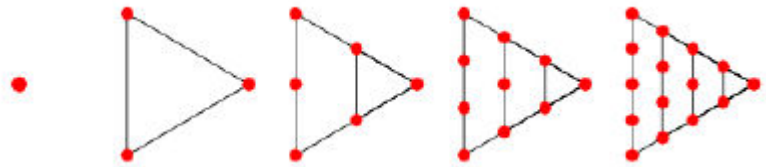
i) Χρησιμοποίησε τη Διαδικασία Υποβιβασμού, ξεκινώντας από την εξίσωση $259^2 + 1^2 = 34 \cdot 1973$ για να γράψεις τον πρώτο αριθμό 1973 ως άθροισμα δύο τετραγώνων.

j) Ποιος πρώτος αριθμός $p < 100$ μπορεί να γραφτεί ως άθροισμα τριών τετραγώνων $p = a^2 + b^2 + c^2$;

k) Βασισμένοι στα δεδομένα που συλλέξατε, προσπαθήστε να εικάσετε ποιοι πρώτοι αριθμοί μπορούν να γραφτούν ως άθροισμα τριών τετραγώνων.

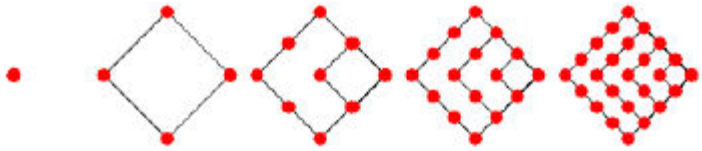
Κεφάλαιο 23 Γεωμετρικοί Αριθμοί

Τριγωνικοί αριθμοί είναι οι αριθμοί που μπορούν να τοποθετηθούν σε τριγωνικό σχήμα. Ας φανταστούμε κάθε τρίγωνο να βρίσκεται μέσα στο επόμενο τρίγωνο. Ο n-οστός τριγωνικός αριθμός T_n σχηματίζεται χρησιμοποιώντας ένα εξωτερικό τρίγωνο στο οποίο οι πλευρές του έχουνε n τελείες.



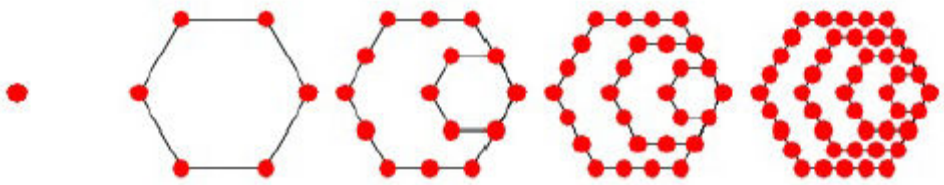
Οι πρώτοι τριγωνικοί αριθμοί είναι οι 1,3,6,10,15. Ας παρατηρήσουμε ότι ο n-οστός τριγωνικός αριθμός που θα συμβολίζεται ως T_n είναι $T_n = 1+2+3+...+n = \frac{n(n+1)}{2}$.

Τετράγωνοι αριθμοί είναι οι αριθμοί που μπορούν να τοποθετηθούν σε σχήμα τετραγώνου.



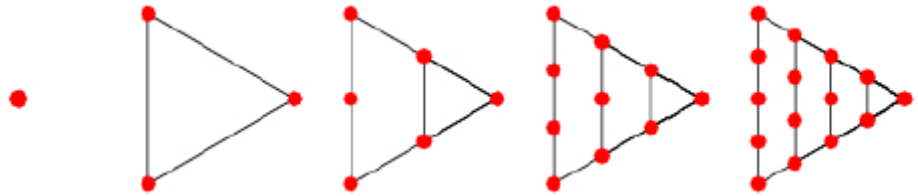
Ας φανταστούμε κάθε τετράγωνο να είναι τοποθετημένο μέσα σε επόμενο τετράγωνο. Ο n-οστός τετράγωνος αριθμός σχηματίζεται χρησιμοποιώντας ένα εξωτερικό τετράγωνο όπου οι πλευρές του έχουν n τελείες. Ο n-οστός τετράγωνος αριθμός είναι Ψ. Ένας πενταγωνικός αριθμός είναι ένας αριθμός που μπορεί να τοποθετηθεί σε σχήμα πενταγώνου.

Οι πρώτοι 4 πενταγωνικοί αριθμοί είναι ο 1, 5,12, 22. Ας φανταστούμε κάθε πεντάγωνο να είναι τοποθετημένο μέσα σε επόμενο πεντάγωνο. Ο n-οστός πενταγωνικός αριθμός σχηματίζεται χρησιμοποιώντας ένα εξωτερικό πεντάγωνο όπου οι πλευρές του έχουν n τελείες. Εξαγωνικοί αριθμοί ορίζονται με όμοιο τρόπο.

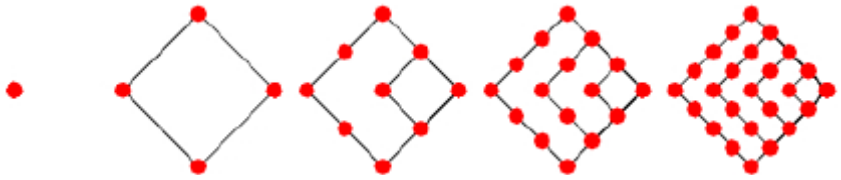


Κεφάλαιο 24 Τετράγωνοι-Τρίγωνικοι Αριθμοί και η εξίσωση του Pell

Ας υπενθυμίσουμε από το προηγούμενο κεφάλαιο ότι οι τριγωνικοί αριθμοί είναι αριθμοί της μορφής $T_m = \frac{m(m+1)}{2}$. Γεωμετρικά είναι αριθμοί που μπορούν να τοποθετηθούν σε ένα σχήμα ενός τριγώνου:



Ο n-οστός τριγωνικός αριθμός μοντελοποιείται γεωμετρικά χρησιμοποιώντας ένα εξωτερικό τρίγωνο όπου οι πλευρές τους έχουν n τελείες. Όμοια, οι τετράγωνοι αριθμοί είναι αριθμοί που μπορούν να τοποθετηθούν σε ένα σχήμα ενός τετραγώνου.



Ο n-οστός τετράγωνος αριθμός μοντελοποιείται γεωμετρικά χρησιμοποιώντας ένα εξωτερικό τετράγωνο όπου οι πλευρές τους έχουν n τελείες . Ο n-οστός τετράγωνος αριθμός είναι $S_n = n^2$.

Παράδειγμα 24.1

Δημιουργήστε μια λίστα από τους πρώτους 10 τριγωνικούς αριθμούς και μια λίστα από τετράγωνους αριθμούς.

Υπάρχουν αριθμοί που βρίσκονται ταυτόχρονα και στις 2 λίστες;

Σε αυτό το κεφάλαιο θα κατασκευάσουμε μια μέθοδο εύρεσης όλους τους τετράγωνους-τριγωνικούς αριθμούς (δηλαδή αριθμοί που είναι ταυτόχρονα και τετράγωνοι και τριγωνικοί).

Μια από τις βασικές ερωτήσεις που μας ενδιαφέρει να απαντήσουμε είναι αν υπάρχουν ή όχι άπειροι τετράγωνοι-τριγωνικοι αριθμοί. Αφού οι τριγωνικοί αριθμοί είναι της μορφής: $T_m = \frac{m(m+1)}{2}$ και οι τετράγωνοι αριθμοί είναι της μορφής $S_n = n^2$ τότε οι τετράγωνοι-τριγωνικοί αριθμοί θα είναι οι ακέραιες λύσεις της εξίσωσης: $\frac{m(m+1)}{2} = n^2$.

Στη συνέχεια πολλαπλασιάζουμε και τα 2 μέλη της παραπάνω εξίσωσης με 8 οπότε η παραπάνω εξίσωση γίνεται:

$$4m(m+1) = 8n^2$$

$$4m^2 + \mathrm{m} = 8n^2$$

$$(2m+1)^2 - 1 = 8n^2$$

Οπότε θέτουμε $x = 2m+1, y = 2n$ και προκύπτει η εξίσωση $x^2 - 2y^2 = 1$.

Λύσεις στην παραπάνω εξίσωση παράγει τετράγωνους-τριγωνικούς αριθμούς με $m = \frac{x-1}{2}$ και $n = \frac{y}{2}$.

Με άλλα λόγια αν (x, y) είναι μία λύση της εξίσωσης $x^2 - 2y^2 = 1$ τότε ο $N = n^2 = \left(\frac{y}{2}\right)^2$ είναι ένας τετράγωνος-τριγωνικός αριθμός. Γεωμετρικά το τετράγωνο έχει $\frac{y}{2}$ τελείες σε μια πλευρά του και το τρίγωνο έχει $\frac{x-1}{2}$ τελείες στην βάση του τριγώνου.

Παράδειγμα 24.2 Να αποδειχθεί ότι το ζεύγος $(x, y) = (3, 2)$ και $(x, y) = (17, 12)$ είναι λύσεις της εξίσωσης $x^2 - 2y^2 = 1$. Τότε να βρείτε τις τιμές (m, n) και τους τετράγωνους-τριγωνικούς αριθμούς. Μπορείτε να βρείτε άλλες λύσεις (ίσως χρησιμοποιώντας μια αριθμομηχανή ή έναν υπολογιστή);

Για να βρούμε όλους τους τετράγωνους-τριγωνικούς αριθμούς, πρέπει να βρούμε όλες τις λύσεις της εξίσωσης $x^2 - 2y^2 = 1$. Παρατηρούμε ότι μπορούμε να παραγοντοποιήσουμε την εξίσωση ως εξής:

$x^2 - 2y^2 = (\mathrm{x} + \mathrm{y}\sqrt{2})(\mathrm{x} - \mathrm{y}\sqrt{2})$.

Για παράδειγμα μπορούμε να γράψουμε τη λύση $(x, y) = (3, 2)$ ως $1 = 3^2 - 2 \cdot 2^2 = (3 + 2\sqrt{2})(3 - 2\sqrt{2})$.

Στη συνέχεια υψώνουμε και τα 2 μέλη της εξίσωσης στο τετράγωνο:

$$1 = 1^2 = (3 + 2\sqrt{2})^2 (3 - 2\sqrt{2})^2$$
$$= (17 + 12\sqrt{2})(17 - 12\sqrt{2})$$
$$= 17^2 - 2 \cdot 12^2$$

Επομένως, υψώνοντας στο τετράγωνο τη λύση $(x, y) = (3, 2)$ παράγαμε την επόμενη λύση $(x, y) = (17, 12)$.

Θεώρημα 24.1

Υπάρχουν άπειροι τετράγωνοι-τριγωνικοί αριθμοί.

Απόδειξη

Για κάθε θετικό ακέραιο k $1 = 1^k = (3 + 2\sqrt{2})^k (3 - 2\sqrt{2})^k$.

Υψώνοντας την παράσταση $(3 + 2\sqrt{2})$ σε ολοένα και μεγαλύτερες δυνάμεις βρίσκουμε όλο και περισσότερες λύσεις της εξίσωσης $x^2 - 2y^2 = 1$ και κάθε νέα λύση δίνει έναν νέο τετράγωνο-τριγωνικό

αριθμό.

Συνεπώς, υπάρχουν άπειροι τετράγωνοι-τριγωνικοί αριθμοί και είναι λογικό να προκύπτει το ερώτημα αν η συγκεκριμένη διαδικασία παράγει όλους τους τετράγωνους-τριγωνικούς αριθμούς.

Θεώρημα 24.2 Θεώρημα Τετράγωνων-Τριγωνικών Αριθμών

(α) Κάθε λύση (x_k, y_k) στους θετικούς ακέραιους της εξίσωσης $x^2 - 2y^2 = 1$ είναι της μορφής

$x_k + y_k\sqrt{2} = (3+2\sqrt{2})^k \quad k = 1,2,3,...$

(β) Κάθε τετράγωνος-τριγωνικός αριθμός $n^2 = \frac{1}{2}m(m+1)$ δίνεται από την σχέση $m = \frac{x_k - 1}{2}$ και $n = \frac{y_k}{2}$.

Απόδειξη

Το (β) το έχουμε ήδη αποδείξει. Το μόνο που χρειάζεται είναι να ελέγξουμε αν (u,v) είναι μια οποιαδήποτε λύση της εξίσωσης $x^2 - 2y^2 = 1$ τότε θα είναι της μορφής $u + v\sqrt{2} = (3+2\sqrt{2})^k$ για κάποιο k. Για να το εξετάσουμε θα πρέπει να χρησιμοποιήσουμε την παρακάτω μέθοδο.

Αρχικά παρατηρούμε ότι αν $u \geq 3$ και αν $u = 3$ τότε $v = 2$, οπότε δεν υπάρχει κάτι να ελέγξουμε.

Στη συνέχεια υποθέτουμε ότι $u > 3$ και θα αποδείξουμε ότι υπάρχει άλλη λύση (s,t) στους θετικούς ακεραίους τέτοια ώστε $u + v\sqrt{2} = (3+2\sqrt{2})(s+t\sqrt{2})$ με $s < u$.

Αν $(s,t) = (3,2)$ τότε το αποδείξαμε (δηλαδή (u,v) είναι στην σωστή μορφή). Αν όχι τότε θα πρέπει να βρούμε μια άλλη λύση (q,r) τέτοια ώστε $s + t\sqrt{2} = (3+2\sqrt{2})(q+r\sqrt{2})$ με $q < s$.

Αν μπορούμε να την βρούμε τότε θα ισχύει $u + v\sqrt{2} = (3+2\sqrt{2})^2(q+r\sqrt{2})$.

Επομένως, αν $(q,r) = (3,2)$ τότε το αποδείξαμε. Αν όχι τότε θα εφαρμόσουμε την διαδικασία ξανά.

Ας παρατηρήσουμε ότι αυτή η διαδικασία δεν μπορεί να συνεχίζετε επ' άπειρον, αφού κάθε φορά που παίρνουμε μια νέα λύση, η τιμή του 'x' είναι μικρότερη (δηλαδή $q < s < u$). Αφού αυτές οι τιμές είναι όλες θετικοί ακέραιοι δεν μπορούνε να γίνονται ολοένα και μικρότερες για πάντα, οπότε η διαδικασία πρέπει να σταματήσει σε πεπερασμένο αριθμό βημάτων. Συνεπώς, ενδεχομένως θα πρέπει να φτάσουμε το (3,2) ως λύση, οπότε τελικά θα είμαστε σε θέση να γράφουμε το $u + v\sqrt{2}$ σαν δύναμη του $3 + 2\sqrt{2}$.

Άρα απομένει να αποδείξουμε ότι αν ξεκινήσουμε με μια λύση (u,v) με $u > 3$, τότε μπορούμε να βρούμε μια λύση (s,t) με την ιδιότητα $u + v\sqrt{2} = (3+2\sqrt{2})(s+t\sqrt{2})$ με $s > u$.

Για να γίνει αυτό κάνουμε την επιμεριστική ιδιότητα στο δεύτερο μέλος οπότε και έχουμε:

$u + v\sqrt{2} = (3s+4t) + (2s+3t)\sqrt{2})$.

Συνεπώς χρειάζεται να λύσουμε το σύστημα $u = 3s + 4t$ και $v = 2s + 3t$.

Λύνοντας το σύστημα προκύπτει ότι $s = 3u - 4v$ και $t = -2u + 3v$ για s και t.

Έμειναν 3 πράγματα να ελέγξουμε. Χρειάζεται να βεβαιωθούμε ότι η (s,t) είναι πράγματι λύση της εξίσωσης $x^2-2y^2=1$, ότι ο s και t είναι και οι 2 ακέραιοι θετικοί και ότι $s<u$.

Για το πρώτο απλά ελέγχουμε ότι $s^2-2t^2=1$ (ας θυμηθούμε ότι $u^2-2v^2=1$ αφού (u,v) είναι λύση).

Αφού γνωρίζουμε ότι s και t είναι και οι 2 θετικοί ακέραιοι, μπορούμε να ελέγξουμε ότι $s<u$ όπως φαίνετε στη συνέχεια:

$$s=3u-4v$$
$$=3u-4\left(\frac{1}{3}\mathrm{t}+\frac{2}{3}\mathrm{u}\right)$$
$$=3u-\frac{4}{3}t-\frac{8}{3}u$$
$$=\frac{1}{3}u-\frac{4}{3}t$$

Απομένει να αποδείξουμε ότι ο s και ο t είναι και οι 2 θετικοί. Αρχικά θα ελέγξουμε ότι ο s είναι θετικός:

$$u^2=1+2v^2>2v^2$$
$$u>\sqrt{2}v$$
$$s=3u-4v$$
$$s>3u-4v$$
$$s>3\sqrt{2}v-4v=(3\sqrt{2}-4)v>0$$

Στη συνέχεια θα ελέγξουμε ότι ο t είναι θετικός:

$$u>3$$
$$u^2>9$$
$$9u^2>9+8u^2$$
$$9u^2-9>8u^2$$
$$u^2-1>\frac{8}{9}u^2$$
$$2v^2>\frac{8}{9}u^2$$
$$v>\frac{2}{3}u$$
$$t=-2u+3v>-2u+3\frac{2}{3}u=0$$

Αυτό ολοκληρώνει και την απόδειξη.

Πιο γενικά οποιαδήποτε Διοφαντική Εξίσωση της μορφής $x^2-dy^2=1$ όπου d είναι ένας μη-τετραγωνος θετικός ακέραιος καλείται **Εξίσωση του Pell**. Η εξίσωση του Pell έχει μια ενδιαφέρουσα ιστορία που καταγράφετε στο «Πρόβλημα του Αρχιμήδη με τις αγελάδες » σε ένα γράμμα που έστειλε ο Αρχιμήδης στον Ερατοσθένη. Το 1880 ο A.Amthor ένας Γερμανός μαθηματικός απέδειξε ότι ο συνολικός αριθμός των αγελάδων πρέπει να είναι ένας αριθμός με 206,545 ψηφία ξεκινώντας με 7766. Στα επόμενα 85

χρόνια άλλα 40 ψηφία βρέθηκαν, αλλά δεν ήταν πριν το 1965 στο πανεπιστήμιο του Waterloo που βρέθηκε μια ολοκληρωμένη λύση από έναν υπολογιστή IBM και χρειάστηκε λιγότερο από 7,5 ώρες.

Ωστόσο δεν τύπωσαν την Λύση και το πρόβλημα λύθηκε δεύτερη φορά χρησιμοποιώντας έναν Gray υπολογιστή το 1981.

Επομένως γνωρίζουμε ότι αν μπορούμε να βρούμε μια λύση στην εξίσωση του Pell τότε μπορούμε να βρούμε απείρως πολλές . Αλλά πώς βρίσκουμε την πιο μικρή (δηλαδή την βασική λύση);

Για να απαντήσουμε σε αυτή την ερώτηση θα ερευνήσουμε την σχέση μεταξύ συνεχών κλασμάτων και εξισώσεων Pell.

Παράδειγμα 24.5 Ένα συνεχή κλάσμα είναι μια έκφραση της μορφής $4+\dfrac{1}{2+\dfrac{1}{7+\dfrac{1}{3}}}$.

Αυτό ονομάζεται **συνεχή κλάσμα επέκτασης** για το κλάσμα $\dfrac{210}{47}$. Ας παρατηρήσουμε ότι στο **συνεχή κλάσμα επέκτασης** όλοι οι παρανομαστές είναι ίσοι με 1. Ένας άλλος συμβολισμός για το **συνεχή κλάσμα επέκτασης** είναι $[4,2,7,3]$.

Παράδειγμα 24.6 Ας θεωρήσουμε την δεκαδική αναπαράσταση του π:

$\pi = 3.14159265358979323846264 33...$

Παρατηρούμε ότι μπορούμε να γράψουμε το παραπάνω ως : $\pi = 3 + $κάτι, όπου το «κάτι» είναι ένας αριθμός ανάμεσα στο 0 και 1. Στη συνέχεια παρατηρούμε ότι μπορούμε να το ξαναγράψουμε ως εξής:

$$\pi = 3 + 0.14159265358979323846264 33...$$

$$= 3 + \frac{1}{\dfrac{1}{0.14159265358979323846264 33...}}$$

$$= 3 + \frac{1}{7.06251330593104576930051...}$$

$$= 3 + \frac{1}{7 + 0.06251330593104576930051...}$$

Η τελευταία εξίσωση μας δίνει μια «καλή» προσέγγιση $\dfrac{22}{7}$ για το π. Στη συνέχεια αν επαναλάβουμε την παραπάνω διαδικασία θα έχουμε:

$$0.06251330593104576930051... = \frac{1}{\dfrac{1}{0.06251330593104576930051..}}$$

$$= 15.996594406685719888923060$$

$$= 15 + 0.996594406685719888923060$$

Επομένως, έχουμε την παρακάτω αναπαράσταση για το π

$$\pi = 3 + \frac{1}{7 + \frac{1}{15 + 0.996594406685719888923060}}.$$

Στο παραπάνω κλάσμα έχουμε στον παρανομαστή τον αριθμό 15.996594406685719888923060 που είναι πολύ κοντά στο 16. Αν αντικαταστήσουμε τον παραπάνω αριθμό με το 16 τότε θα λάβουμε έναν ρητό αριθμό πολύ κοντά στον άρρητο αριθμό π . Πράγματι

$$\pi = 3 + \frac{1}{7 + \frac{1}{16}} = \frac{355}{113} = 3.14159292035538823008849557...$$

Το κλάσμα $\frac{355}{113}$ είναι μια προσέγγιση του π με ακρίβεια 6 δεκαδικών ψηφίων. Συνεχίζοντας την παραπάνω διαδικασία όπου σε κάθε στάδιο ρίχνεις το δεκαδικό που έχει απομείνει και στη συνέχεια διαχωρίζεις από το σύνολο το ακέραιο μέρος, για να ληφθεί ένα κλάσμα τεσσάρων στρώσεων όπου θα εκπροσωπήσει το π. Χρησιμοποιώντας την τελική εκπροσώπηση για να πάρουμε μια ρητή προσέγγιση του π μπορούμε να την συγκρίνουμε με την γνωστή δεκαδική προσέγγιση του π για να εξετάσουμε κατά πόσο ακριβή είναι η παραπάνω προσέγγιση μας. Χρησιμοποιώντας συμβολισμό, μπορούμε να εκφράσουμε το συνεχές κλάσμα επέκτασης του π ως

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, ...].$$

Ορισμός 24.1 Ο n-οστός συγκλίνων όρος στο α είναι ο ρητός αριθμός

$$\frac{p_n}{q_n} = [a_o; a_1, a_2, ..., a_n] = \mathrm{a}_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + ... + \frac{1}{a_n}}}}$$

που προκύπτει χρησιμοποιώντας όρους μέχρι το a_n στο συνεχές κλάσμα επέκτασης του α.

Παράδειγμα 24.7 Για το συνεχές κλάσμα επέκτασης του $\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, ...]$.

Οι πρώτοι συγκλίνοντες όροι του π είναι:

$$\frac{p_o}{q_o} = 3$$

$$\frac{p_1}{q_1} = 3 + \frac{1}{7} = \frac{22}{7} = 3.142857143$$

$$\frac{p_2}{q_2} = 1 + \frac{1}{7 + \frac{1}{15}} = \frac{333}{106} = 3.141509434$$

Ας θεωρήσουμε την εξίσωση του Pell με $d = 2$:

$$x^2 - 2y^2 = 1$$

Στη συνέχεια βρίσκουμε το συνεχή κλάσμα επέκτασης του $\sqrt{2}$:

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

Οι πρώτοι συγκλίνοντες όροι του $\sqrt{2}$ είναι:

$$\frac{p_o}{q_o} = 1$$

$$\frac{p_1}{q_1} = 1 + \frac{1}{2} = \frac{3}{2}$$

$$\frac{p_2}{q_2} = 1 + \frac{1}{2 + \frac{1}{2}} = \frac{7}{5}$$

Παρατηρούμε ότι η θεμελιώδης λύση της εξίσωσης $x^2 - 2y^2 = 1$ είναι $(3, 2)$ που είναι στους συγκλίνων όροι του $\sqrt{2}$.

Θεώρημα 24.3 Συνεχή κλάσματα και θεμελιώδης λύσεις των Εξισώσεων Pell

Ας Θεωρήσουμε την εξίσωση του **Pell** $x^2 - d \cdot y^2 = 1$. Έστω $\frac{h_i}{k_i}$ με $i = 0, 1, ...$ είναι η ακολουθία των συγκλινουσών όρων στο συνεχή κλάσμα επέκτασης για το $\sqrt{d}$. Τότε η θεμελιώδης λύση (x_1, y_1) της εξίσωσης του **Pell** ικανοποιεί τις παρακάτω σχέσεις για κάποιο i .

Παράδειγμα 24.8

Ας Θεωρήσουμε την εξίσωση του **Pell** $x^2 - 3 \cdot y^2 = 1$. Να βρεθεί το συνεχή κλάσμα επέκτασης του $\sqrt{3} = 1.7320508075688...$ και στη συνέχεια να χρησιμοποιηθεί για να βρεθεί η θεμελιώδης λύση της εξίσωσης του **Pell.**

Λύση

Έστω $\sqrt{3} = [1; 1, 2, 1, 2, 1, 2, 1, 2...]$

$$\frac{p_0}{q_0} = 1$$

$$\frac{p_1}{q_1} = 1 + \frac{1}{1} = \frac{2}{1}$$

$$\frac{p_2}{q_2} = 1 + \frac{1}{1 + \frac{1}{2}} = \frac{5}{3} = 1.666....$$

Παράδειγμα 24.9

Ας Θεωρήσουμε την εξίσωση του **Pell** $x^2 - 7 \cdot y^2 = 1$. Να βρεθεί το συνεχή κλάσμα επέκτασης του $\sqrt{7} = 2.6457513110645907...$ και στη συνέχεια να χρησιμοποιηθεί για να βρεθεί η θεμελιώδης λύση της εξίσωσης του **Pell.**

Λύση

$$\frac{p_0}{q_0} = 2$$

$$\frac{p_1}{q_1} = 2 + \frac{1}{1} = \frac{3}{1}$$

$$\frac{p_2}{q_2} = 2 + \frac{1}{1 + \frac{1}{1}} = \frac{5}{2} = 2,5$$

$$\frac{p_3}{q_3} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} = \frac{8}{3} = 2.6666...$$

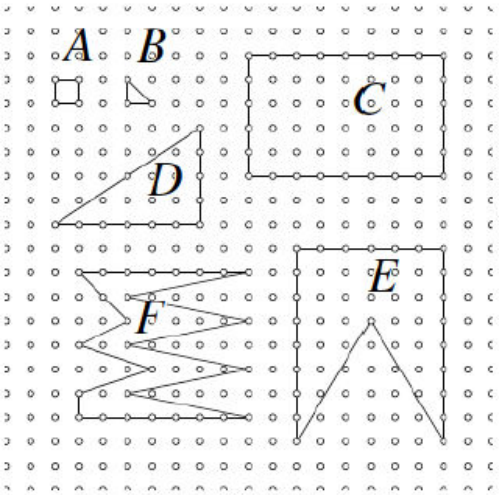
Κεφάλαιο 25 Το θεώρημα του Pick

Το Θεώρημα του Pick είναι ένα υπέροχο αποτέλεσμα που δημιουργεί μια σύνδεση μεταξύ της περιοχής ενός πολυγωνικού πλέγματος και του αριθμού των σημείων του πλέγματος μέσα στην περιοχή του πολυγώνου.

Το πολύγωνο μπορεί να είναι κυρτό ή κοίλο. Οι μόνες απαιτήσεις του Θεωρήματος του RIA είναι οι πλευρές του πολύγωνου να μην τέμνονται. **Σημεία πλέγματος** είναι σημεία με ακέραιες συντεταγμένες στο xy επίπεδο.

Ένα **ευθύγραμμο τμήμα πλέγματος** είναι ένα ευθύγραμμο τμήμα που έχει δύο διαφορετικά σημεία ως τελικά σημεία (αρχή και τέλος ευθύγραμμου τμήματος).

Πολύγωνο πλέγματος είναι ένα πολύγωνο όπου οι πλευρές του έχει ευθύγραμμα τμήματα πλέγματος που αυτό σημαίνει ότι οι κορυφές του πολυγώνου είναι σημεία πλέγματος.



Προφανώς για πολύγωνα με ένα μεγάλο εσωτερικό, η περιοχή προσεγγίζεται χονδρικά από τον αριθμό των σημείων του πλέγματος στο εσωτερικό του πολυγώνου.

Μπορεί να Θεωρηθεί ότι μια καλύτερη προσέγγιση μπορεί να γίνει με την προσθήκη περίπου το μισών από τα σημεία πλέγματος στο σύνορο, δεδομένου ότι είναι ένα δεύτερο είδος μέσα και έξω από το μισό του πολυγώνου. Αλλά ας ρίξουμε μια ματιά σε μερικά παραδείγματα του Σχήματος 1.

Για όλα τα παραδείγματα που ακολουθούν, θεωρούμε τον αριθμό των εσωτερικών κορυφών, και B είναι ο αριθμός των κορυφών του συνόρου. Θα χρησιμοποιήσουμε το συμβολισμό A (P) για να αναφερθούμε στην έκταση του πολύγωνου P (εμβαδό).

A: I = 0, B = 4, A (A) = 1, I + B/2 = 2.

B: I = 0, B = 3, A(B) = 1=2, I + B/2 = 3/2.

C: I = 28, B = 26, A(C) = 40, I + B/2 = 41.

D: I = 7, B = 12. A(D) = 12, I + B/2 = 13.

E: Είναι δυσκολότερο να υπολογιστούν τα εμβαδά των πολυγώνων E και F. Το E μπορεί να διασπαστεί

σε 6 x 3 ορθογώνιο και δύο όμοια τρίγωνα με βάση 3 και ύψος 5, επομένως παίρνουμε I = 22, B = 24 A (E) = 33, I + B / 2 = 34.

F:

Είναι ακόμη πιο δύσκολο να υπολογιστεί το εμβαδό για αυτό το πολύγωνο, αλλά μετά από κάποιο προσθήκη και αφαίρεση περιοχών, έχουμε ότι: I = 9, B = 26, A (F) = 21, I + B / 2 = 22.

Αυτό που είναι εκπληκτικό είναι ότι αν προσέξουμε όλα τα παραπάνω παραδείγματα, η εκτίμηση I + B/ 2 έχει διαφορά από το εμβαδό του πολυγώνου A (E) κατά 1. Φαίνεται ότι για κάθε πολύγωνο πλέγματος P, ισχύει ο παρακάτω τύπος:

$A(P) = I_p + \frac{B_p}{2} - 1,$ όπου I_p είναι ο αριθμός των σημείων πλέγματος «καθαρά» στο εσωτερικό του πολυγώνου P και B_p είναι ο αριθμός των σημείων πλέγματος στο σύνορο του P. Αυτό είναι το **Θεώρημα του Pick**.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] ΔΗΜΗΤΡΙΟΣ ΠΟΥΛΑΚΗΣ Θεωρία Αριθμών Εκδόσεις Ζητή ΘΕΣΣΑΛΟΝΙΚΗ 1997

[2] Α.Παπαιωάννου και Μ.Ρασσιάς, Εισαγωγη στη Θεωρία Αριθμών, Εκδόσεις Συμεών, Αθήνα, 2010

[3] Π.Μ. ΒΛΑΜΜΟΣ, Ε.ΡΑΠΠΟΣ,Π.ΨΑΡΡΑΚΟΣ Θεωρία Αριθμών Ελληνική Μαθηματική Εταιρεία ΑΘΗΝΑ 2000

[4] G.HARDY,E.M. WRIGHT An Introduction to yhe Theory of Numbers OXFORD, 1959

[5] Harold M .Stark, An Introduction to Number Theory, The MIT Press, 1987

[6] Joseph H. Silverman, A Friendly Introduction to Number Theory, Third Edition, Prentice Hall, 2006.

[7] EDMUND LANDAU Elementary Number Theory CHELSEA, 1966

[8] L.Moser, An Introduction to the Theory of Numbers, The Trillia Group, West Lafayette, 2004

[9] G.Everest and T. Ward, An Introduction to Number Theory, Springer – Verlag, New York, 2005