ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Πρώτοι Αριθμοί και Μέθοδοι Κοσκινοποίησης Αριθμών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΤΣΙΡΙΓΟΥ ΕΜΜΑΝΟΥΗΛ
Α.Μ. 09107119

Επιβλέπων Καθηγητής: Φελλούρης Ανάργυρος
Αναπληρωτής Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2016

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Πρώτοι Αριθμοί και Μέθοδοι Κοσκινοποίησης Αριθμών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΤΣΙΡΙΓΟΥ ΕΜΜΑΝΟΥΗΛ
Α.Μ. 09107119

Επιβλέπων Καθηγητής: Φελλούρης Ανάργυρος
Αναπληρωτής Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την.

(ΥΠΟΓΡΑΦΗ)	(ΥΠΟΓΡΑΦΗ)	(ΥΠΟΓΡΑΦΗ)
……..	……..	……..
Φελλούρης Ανάργυρος Αναπλ. Καθηγητής Ε.Μ.Π.	Ψαρράκος Παναγιώτης Καθηγητής Ε.Μ.Π.	Στεφανέας Πέτρος Επίκουρος Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2016

Περίληψη-Ευχαριστίες

Οι πρώτοι αριθμοί προσέλκυσαν από νωρίς το ενδιαφέρον και αποτέλεσαν ιδιαίτερη θεωρητική ενότητα ήδη από τις απαρχές των Μαθηματικων. Στην παρούσα διπλωματική εργασία επιχειρείται να παρουσιασθούν ιστορικά κομβικά αποτελέσματα της Θεωρίας, από όλη την διαδρομή. Από την μέτρηση στην Παλαιολιθική Εποχή στην Αρχαία Ελλάδα και στην μαθηματική απόδειξη, και από τα θεωρήματα των Fermat, Euler, Bertrand και Gauss στην σύγχρονη εποχή και τους αριθμούς Mersenne και το ασταμάτητο 'κυνήγι' ακόμα μεγαλύτερων πρώτων αριθμών. Έπειτα παρουσιάζονται κάποια βασικά στοιχεία στην θεωρία κοσκίνων και παρουσιάζονται τρία από τα βασικότερα στην εύρεση των πρώτων αριθμών. Στο τελευταίο κεφάλαιο της διπλωματικής παρατίθενται μερικές εφαρμογές των πρώτων αριθμών όπως είναι η κρυπτογραφία και οι πρώτοι αριθμοί του Mersenne.

Θα ήθελα πρώτα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή αυτής της διπλωματικής εργασίας κ.Ανάργυρο Φελλούρη, Αναπληρωτή Καθηγητή του Ε.Μ.Π. κυρίως για την τυφλή εμπιστοσύνη που μου έδειξε κατά την διάρκεια της εκπόνησης της διπλωματικης αλλά και για την υπομονή και τον χρόνο που αφιέρωσε ώστε να πραγματοποιηθεί άρτια η ολοκληρωσή της. Θα ήθελα να ευχαριστήσω και τα άλλα μέλη της τριμελούς εξεταστικής επιτροπής που με τίμησαν με την παρουσία τους : τον κ. Ψαρράκο Παναγιώτη, Καθηγητή του Τομέα Μαθηματικών της Σ.Ε.Μ.Φ.Ε. του Ε.Μ.Π. και τον κ. Στεφανέα Πέτρο, Επίκουρο Καθηγητή του Τομέα Μαθηματικών της Σ.Ε.Μ.Φ.Ε. του Ε.Μ.Π.

Ευχαριστώ ιδιαιτέρα τους φίλους μου και συμφοιτητές μου Ανδρέα Μπάλτα, Αποστόλη Κρυσταλλίδη και Νίκο Στυλιανού για την πολύτιμη στήριξη που μου παρείχαν καθ'όλη την διάρκεια της διπλωματικης.

Το μεγαλύτερο ευχαριστώ όμως το οφείλω στους γονείς μου και στον αδερφό μου για την αμέριστη συμπαράσταση και εμπιστοσύνη που δείχνουν σε μένα, στους στόχους μου και στα ονειρά μου. Ήταν οι άνθρωποι που με την αγάπη τους, την υπομονή τους και την διαρκή υποστήριξή τους έκαναν τις δύσκολες στιγμές να μοιάζουν ευκολότερες.

Την διπλωματική εργασία την αφιερώνω στους γονείς μου Κώστα και Κική και στον αδερφό μου Γιώργο.

Abstract

The subject of this diploma thesis is the prime numbers and sieve methods. We present a brief history of numbers, their main uses and when they first started to concern the mathematicians. Many great mathematicians such as : Fermat, Euler, Bertrand and Gauss studied the prime numbers and some important theorems are referred. Then we present some basic knowledge about sieve theory and more specifically about sieve of Eratosthenes, Sieve of Atkin and Sieve of Sundaram. In the last chapter we present some applications on cryptography and mersenne prime numbers.

Πίνακας περιεχομένων

1 ΚΕΦΑΛΑΙΟ 1^{Ο} - Εισαγωγή

1.1. Εισαγωγικές έννοιες

Ανθρωπολόγοι ανά τον κόσμο έχουν ανακαλύψει ότι όλοι οι πολιτισμοί είχαν αναπτύξει κάποια μορφή αρίθμησης, ακόμη και στους πιο πρώτογονους από αυτούς έχουν παρατηρηθεί στοιχειώδεις αριθμητικές λέξεις. Η χρήση αριθμητικών συμβόλων είναι ένα από τα ολιγάριθμα στοιχεία που παρατηρούνται σε όλους τους πολιτισμούς που εμφανίζονται στην ιστορία. Θα μπορούσαμε να συμπεράνουμε δηλαδή ότι η μέτρηση ήταν πολιτιστική αναγκαιότητα. Η διαδικασία της μέτρησης, έννοια που εμπεριέχει την έννοια του φυσικού αριθμού και του τρόπου συμβολικής αναπαράστασής του, θεωρείται το εγκυρότερο πολιτιστικό στοιχείο.

Είναι σχεδόν βέβαιο ότι η μέτρηση στα πρώτα της βήματα ήταν δυαδική. Χρησιμοποιούνταν, δηλαδή, λέξεις για το ένα και το δύο ενώ δεν υπήρχαν αντίστοιχες για το τρία , το τέσσερα κτλ. Για μεγαλύτερους αριθμούς υπήρχε είτε το ‘πολλά’ είτε το ‘δύο-ένα’ για το τρία ,το ‘δύο-δύο’ για το τέσσερα, το ‘δύο-δύο-ένα’ για το πέντε κοκ. Μια γλωσσολογική μαρτυρία σε αυτή την κατεύθυνση είναι ότι πολλές γλώσσες (Αιγυπτιακή, Αραβική, Εβραική, Σανσκριτική, Ελληνική και Γοτθική) χρησιμοποίησαν για τα ουσιαστικά ενικό αριθμό(για ένα), δυικό αριθμό (για δύο) και πληθυντικό αριθμό (για περισσότερα από δύο). Μπορούμε επίσης να παρατηρήσουμε ότι ακόμα και σήμερα υπάρχουν ειδικοί τύποι λέξεων για το πρώτος (ένα), το δεύτερος (δύο) ενώ συναφείς με το απόλυτο αριθμητικό για το τρίτος (τρία), τέταρτος (τέσσερα), πέμπτος(πέντε) κτλ. Αξιοσημείωτο είναι ακόμα ότι οι λέξεις για το 3 (τρία, trois, drei, tres, tri) έχουν την ίδια ρίζα με το λατινικό trans που σημαίνει ‘πέρα’.

Ως προς τον συμβολισμό τώρα,είναι σχεδόν σίγουρο ότι σε πρώιμο στάδιο περιελάμβανε χάραξη εγκοπών πάνω σε ξύλο. Στην αρχή υπήρχε η αίσθηση της αντιστοίχησης ένα προς ένα. Για το ένα χρησιμοποιήθηκε το I, για το δύο το I I κοκ. Η μέθοδος αυτή

χρησιμοποιήθηκε ήδη από την Παλαιολιθική Εποχή ενώ αλλα ευρήματα δείχνουν δημιουργία κόμπων σε σκοινιά ή σχεδίαση σε πηλό και πάπυρους. Οι πιο διαδεδομένες βάσεις αρίθμησης είναι το πέντε, το δέκα και το είκοσι που είναι βέβαιο ότι υπαγορεύτηκαν από την χρήση του χεριού στην μέτρηση. Η μεγάλη πρόοδος, ωστόσο, στην εξέλιξη του αριθμού συντελέστηκε με την εισαγωγή ιδεογραμμάτων. Η αριθμητική άλλωστε δεν θα μπορούσε να αναπτυχτεί χωρίς αυτά τα σύμβολα.

Διάφοροι πολιτισμοί ανέπτυξαν αριθμητικά συστήματα που έπαιξαν κύριο ρόλο στην διαμόρφωση της εξέλιξης του αριθμού όπως τον αντιλαμβανόμαστε σήμερα. Οι Σουμέριοι χρησιμοποιούσαν σαν βάση του αριθμητικού τους συστήματος το 60, ενώ οι Ακκάδιοι οι κατακτητές τους , το 10. Το σύστημα που προέκυψε είχε στοιχεία και από τα δύο. Οι Βαβυλώνιοι όμως χρησιμοποιούσαν μόνο δύο σύμβολα, ένα για την μονάδα και ένα για την δεκάδα. Οι Αιγύπτιοι χρησιμοποίησαν δεκαδικό σύστημα αρίθμησης ενώ οι Έλληνες χρησιμοποίησαν γράμματα που συμβόλιζαν αριθμούς. Κάθε ένα από αυτά έχει πλεονεκτήματα και μειονεκτήματα και χαρακτηριστικά που, σε πολλές περιπτώσεις,το ένα κληροδότησε στο άλλο.

Ένα χαρακτηριστικό το οποίο δεν χρησιμοποιήθηκε πάντως σε όλους τους πολιτισμούς είναι το σύστημα όπου το ίδιο σύμβολο έχει διαφορετική αξία ανάλογα με τη θέση στην οποία βρίσκεται. Το σύστημα θέσης,όπως ονομάζεται, θεωρείται από τις γονιμότερες στην εξέλιξη των αριθμητικών συστημάτων. Η αξία του έγκειται στην δυνατότητα να εκφραστούν απεριόριστα μεγάλοι ή μικροί αριθμοί χρησιμοποιώντας τα ίδια βασικά ψηφία. Σύστημα θέσης χρησιμοποίησαν τόσο οι Βαβυλώνιοι όσο και οι Μάγια. Αυτός , άλλωστε ήταν ο λόγος που και οι δύο πολιτισμοί ανέπτυξαν την αριθμητική κάνοντας χρήση μόνο δύο συμβόλων. Εντούτοις, μεταγενέστεροι πολιτισμοί όπως ο αιγυπτιακός, ο ελληνικός και ο ρωμαικός δεν το χρησιμοποίησαν. Φαίνεται ότι σε κάποιες περιπτώσεις και ειδικότερα όταν έχουμε να κάνουμε με μικρούς αριθμούς το σύστημα θέσης έχει μειονεκτήματα. Για παράδειγμα, απαιτεί τη χρήση ενός συμβόλου για το 0, κάτι που προβλημάτισε τους πολιτισμούς που το υιοθέτησαν.

Υπάρχει μία διαφοροποίηση σχετικά με το πώς χρησιμοποιούσαν τα Μαθηματικά οι διάφοροι πολιτισμοί. Οι Αιγύπτιοι εκτός από την Γεωμετρία, έκαναν πολλαπλασιασμούς, διαιρέσεις, λογισμούς με κλάσματα και εφαρμοσμένους υπολογισμούς. Οι Βαβυλώνιοι έλυναν γραμμικά ή μη γραμμικά συστήματα με 2 ή 3 αγνώστους και κάποιες μορφές εξισώσεων $3^{ου}$ και $4^{ου}$ βαθμού.Υπήρχε όμως μία σημαντική διαφορά σε σχέση με τους Έλληνες. Σε αυτούς τους λαούς ήταν γνωστές οι γενικές ιδιότητες και οι κανόνες αλλά δεν καταγράφοταν αποτελέσματα σαν γενικές αλήθειες. Γνώριζαν δηλαδή ότι χρησιμοποιώντας γνωστές διαδικασίες θα έφταναν σε συγκεκριμένα αποτελέσματα αλλά δεν διατύπωναν γενικές προτάσεις. Παρέθεταν για κάποιο κανόνα πολλά παραδείγματα, το ένα μετά το άλλο,που οδηγούσε στην αίσθηση ότι θα ισχύει υπό οποιεσδήποτε συνθήκες. Δεν έφτασαν όμως ποτέ στην ελληνική απόδειξη.

Τον $6^{ο}$ αιώνα π.Χ. ιδρύθηκε από τον Πυθαγόρα η ομώνυμος σχολή στον Κρότωνα της σημερινής Νότιας Ιταλίας. Ηδη, από την εποχή των Βαβυλωνίων είχε αρχίσει να ερευνάται η έννοια του αριθμού όπως μαρτυρούν οι αριθμολογικές τους ενασχολήσεις. Στην πυθαγόρεια σχόλη, όμως κυριαρχούσε η ιδέα ότι ‘τα πάντα είναι αριθμοί’. Οι αριθμοί αντιστοιχήθηκαν με αφηρημένες έννοιες όπως αρσενικό, θηλυκό, δικαιοσύνη, γάμος κ.α. Έγιναν μελέτες με βάση την διάκριση των αριθμώνν σε άρτιους και περιττούς ενώ κάποιοι από αυτούς χαρακτηρίστικαν ως φίλοι ή τέλειοι. Αυτός ο αριθμητικός μυστικισμός που αναπτύχτηκε στους πυθαγορείους ήταν καθοριστικός τόσο για την εξέλιξη της έννοιας του αριθμού όσο και για τη σύλληψη αυτού που ονομάζουμε σήμερα Θεωρία Αριθμών. Αργότερα η αριθμολογία και η Θεωρία Αριθμών διαχωρίστηκαν.

1.2 Μαθηματικό υπόβαθρο

Η θεωρία αριθμών ασχολείται με τη μελέτη των ιδιοτήτων του $\mathbb{N} = \{0,1,2, \dots\}$. Με δεδομένο το σύνολο $\mathbb{N}$ και ορίζοντας την πρόσθεση, τον πολλαπλασιασμό καθώς και την διάταξη των φυσικών αριθμών μπορούμε να κατασκευάσουμε το σύνολο $\mathbb{Z}$.

Θεώρημα-Αρχή του Ελαχίστου

Υπάρχει $\alpha \in S$ (όπου S είναι το σύνολο των μη αρνητικών ακεραίων) τέτοιο ώστε : $\alpha \leq b, \forall\, b \in S$.

Αρχιμήδεια Ιδιότητα

Αν $a, b \in \mathbb{N}$ τότε $\exists n \in \mathbb{N}$ τέτοιο ώστε $n \bullet a \geq b$.

Αρχή της μαθηματικής επαγωγής

Έστω S το σύνολο των θετικών ακεραίων με τις ιδιότητες :

i. $1 \in S$
ii. Αν $k \in S$ τότε $k + 1 \in S$,
τότε το $S = \mathbb{N}$.

Θεώρημα

Έστω ακέραιος $m \geq 2$. Κάθε φυσικός αριθμός n μπορεί να αναπαρίσταται μοναδικά με τον εξής τρόπο : $n = a_0 + a_1 m + a_2 m^2 + \cdots + a_k m^k$, όπου k μη αρνητικός ακέραιος για τον οποίο $m^k \leq n < m^{k+1}$ και $a_0, a_1, \dots, a_k$ ακέραιοι για τους οποίους $1 \leq a_k \leq m - 1$ και $0 \leq a_i \leq m - 1$, $\forall i = 0,1, \dots\dots, k - 1$. Αυτή είναι η λεγόμενη m-αδική αναπαράσταση του n. Και γράφουμε, $n = \overline{a_k \bullet \dots \bullet a_1 \bullet a_0}$.

Λήμμα

Έστω m ακέραιος $m \geq 2$, τότε για κάθε $n \in \mathbb{N}$ υπάρχει μοναδικός μη αρνητικός ακέραιος k, τέτοιος ώστε : $m^k \leq n \leq m^{k+1}$.

Παράδειγμα : η δυαδική (2-αδική) αναπαράσταση του 100 είναι :

$$100 = 1 \bullet 2^2 + 1 \bullet 2^5 + 1 \bullet 2^6 = \overline{111_2}$$

Παράδειγμα : η τριαδική (3-αδική) αναπαράσταση του 100 είναι :

$$100 = 1 + 2 \bullet 3^2 + 1 \bullet 3^4 = \overline{121_3}$$

Πρώτοι αριθμοί

Ορισμός:

Έστω $a > 1$ ένας φυσικός αριθμός. Ο a θα ονομάζεται **πρώτος,** αν οι μόνοι του θετικοί διαιρέτες του είναι ο 1 και ο ίδιος ο a. Όταν ο a δεν είναι πρώτος, καλείται **σύνθετος**. Το 1 δεν τον κατατάσσουμε ούτε στη μία ούτε στην άλλη κατηγορία. Επειδή ο ακέραιος αριθμός α είναι πρώτος ακριβώς τότε όταν ο $-\alpha$ είναι πρώτος, από εδώ και πέρα κάθε αναφορά σε πρώτους αριθμούς θα αφορά θετικούς πρώτους.Το σύνολο των πρώτων αριθμών θα το συμβολίζουμε με P.

Κατ’αρχήν αποδεικνύουμε την

Πρόταση

Κάθε φυσικός αριθμός $n, n > 1$, έχει τουλάχιστον έναν πρώτο διαιρέτη.

Απόδειξη

Θεωρούμε το σύνολο

$$M = \{m \in \mathbb{N} \; \omega\sigma\tau\varepsilon \; m|n \; \kappa\alpha\iota \; m > 1\}.$$

Το Μ είναι υποσύνολο του συνόλου $\mathbb{N}$ και είναι διάφορο του κενού,διότι $n \in M$.

Σύμφωνα με την αρχή του ελαχίστου το Μ έχει ένα ελάχιστο στοιχείο,έστω p. Ο p είναι πρώτος διαιρέτης του n.

Πράγματι,αν δεν ήταν πρώτος θα είχε τουλάχιστον μία ανάλυση της μορφής $p = a \bullet b$ με $a, b \in \mathbb{N} \setminus \{1\}$.Αυτό σημαίνει ότι ο $\alpha \in \mathbb{N}, \alpha > 1$ και $\alpha|n$ (αφού $\alpha|p \; \kappa\alpha\iota \; p|n$),δηλαδή ότι α θα ήταν στοιχείο του Μ και ότι $\alpha < p$,άτοπο.

Πρόταση

Αν ο φυσικός αριθμός n είναι σύνθετος,τότε έχει έναν πρώτο παράγοντα $p, p \leq \sqrt{n}$.

Απόδειξη

Αφού ο n είναι σύνθετος,έχει τουλάχιστον μία ανάλυση της μορφής:

$$n = a \bullet b, \text{ με } 1 < \alpha \leq b < n.$$

Ένα τουλάχιστον από τα a, b είναι μικρότερο ή ίσο της $\sqrt{n}$, διότι αν $a > \sqrt{n}$ και $b > \sqrt{n}$ θα είχαμε $n = a \bullet b > \sqrt{n} \bullet \sqrt{n} = n$, άτοπο.Επειδή το $a > 1$ έχει ένα τουλάχιστον πρώτο διαιρέτη p.
Ο πρώτος αυτός είναι διαιρέτης του n και $p \leq a \leq \sqrt{n}$.

Η πρόταση αυτή μας δίνει ένα κριτήριο ελέγχου πρώτων αριθμών.

Παράδειγμα

Ο φυσικός αριθμός $n = 179$ είναι πρώτος.Αν ήταν σύνθετος θα είχε έναν πρώτο διαιρέτη $p \leq 179 < 14$.Οι πρώτοι οι μικρότεροι του 14 είναι οι 2,3,5,7,11 και 13.Κανένας του δεν διαιρεί το 179.Συνεπώς ο 179 δεν είναι σύνθετος,άρα είναι πρώτος.

Φυσικά το κριτήριο δεν είναι εφαρμόσιμο για μεγάλους φυσικούς αριθμούς.

Πρόταση

Αν p_n είναι ο n-οστός πρώτος αριθμός (n ≥ 1), τότε ισχύει $p_n \leq 2^{2^{n-1}}$.

Απόδειξη

Για $n = 1, p_1 = 2 = 2^{2^{1-1}}$, ισχύει.

Υποθέτουμε ότι ισχύει για όλους τους φυσικούς αριθμούς $m, 1 \leq m < n$.Θα αποδείξουμε ότι ισχύει και για n.

Έστω p ένας πρώτος διαιρέτης του αριθμού

$$p_1 p_2 \dots p_{n-1} + 1$$

Επειδή ο $p \neq p_i i = 1,2, \dots, n-1$ έπεται ότι

$$p_n \leq p \leq p_1 p_2 \dots p_{n-1} + 1 \leq 2^{2^{1-1}} 2^{2^{2-1}} \dots 2^{2^{(n-1)-1}} + 1$$
$$= 2 \bullet 2^2 \dots 2^{2^{n-2}} + 1 \leq 2^{2^{n-1}}$$

Αν p πρώτος, $p \neq 2$ τότε ο p θα είναι περιττός.Επομένως ο $(p+1)$ θα είναι άρτιος άρα όχι πρώτος. Άρα η ελάχιστη διαφορά μεταξύ δύο διαδοχικών περιττών πρώτων είναι μεγαλύτερη ή ίση του 2.

Παρατήρηση

Αν γνωρίζαμε ότι ένας σύνθετος αριθμός n περιέχει l −το πλήθος διαιρέτες,τότε ένας τουλάχιστον θα είναι μικρότερος από την $\sqrt[l]{n}$. Σε διαφορετική περίπτωση,αν δηλαδή και οι l διαιρέτες ήταν γνήσια μεγαλύτεροι του $\sqrt[l]{n}$,τότε το γινόμενο θα ήταν γνήσια μεγαλύτερο του n.

Ορισμός :

Δυο αριθμοί $a, b \in \mathbb{N}$ ονομάζονται σχετικά πρώτοι, αν ο Μ.Κ.Δ. τους ισούται με την μονάδα.

Θεώρημα

Έστω $a, b \in \mathbb{N}$ και p ένας πρώτος αριθμός. Αν $p|a \bullet b$, τότε : είτε $p|a$ είτε $p|b$.

Θεώρημα

Κάθε φυσικός αριθμός $n \geq 2$ αναπαρίσταται μονοσήμαντα στη μορφή $n = p_1^{k_1} \dots \dots . . p_r^{k_r}$ όπου $p_i < \cdots < p_r$ είναι πρώτοι αριθμοί και $k_{1,} \dots, k_r \in \mathbb{N}$. Αυτή είναι η λεγόμεη κανονική αναπαράσταση ενός φυσικού αριθμού n.

Πρόταση-Κινεζικό Θεώρημα Υπολοίπων

Έστω $f: \mathbb{Z} \to \mathbb{Z}$ πολυώνυμο με ακέραιους συντελεστές και έστω $m_1, m_2, \dots \ , m_r$ φυσικοί αριθμοί σχετικά πρώτοι ανά δύο. Αν $m = m_1 \bullet m_2 \bullet \dots \bullet m_r$ τότε κάθε λύση της $f(x) \equiv 0(modm)$ είναι λύση του συστήματος

$$f(x) \equiv 0(modm_1)$$
$$f(x) \equiv 0(modm_2)$$
$$\vdots$$
$$\vdots$$
$$f(x) \equiv 0(modm_r)$$

και αντιστρόφως.

Θεώρημα Lagrange

Έστω $f(x) = c_n \bullet x^n + \cdots + c_1 \bullet x + c_0$ πολυώνυμο με ακέραιους συντελεστές και έστω p ένας πρώτος αριθμός. Υποθέτουμε ότι ο p δεν διαιρεί τον συντελεστή c_n. Τότε η ισοτιμία $f(x) \equiv 0(modp)$ έχει το πολύ n λύσεις.

Θεώρημα

Έστω $f(x) = c_n \bullet x^n + \cdots + c_1 \bullet x + c_0$ πολυώνυμο με ακέραιους συντελεστές και έστω p ένας πρώτος αριθμός. Υποθέτουμε ότι η ισοτιμία $f(x) \equiv 0(modp)$ έχει περισσότερες από n λύσεις. Τότε $p|c_j \; \forall \; j = 0,1, \dots, n$.

2.1 Αρχαίοι Έλληνες

Οι Αρχαίοι Έλληνες ήταν οι πρώτοι που αντιλήφθηκαν τη σημασία των πρώτων αριθμών και τη δυναμική που κρύβουν και έφτασαν σε σπουδαία συμπεράσματα σχετικά με τη φύση τους. Τα συμπεράσματα αυτά εμπλουτίστηκαν με τις ισχυρές μαθηματικές αποδείξεις που πρωτοεμφανίστηκαν στα Αρχαία Ελληνικά Μαθηματικά και αποτελούν ακόμα και στις μέρες μας αριστουργήματα της ανθρώπινης διανόησης.

Ο Ευκλείδης συνέλεξε τα σημαντικότερα Μαθηματικά μέχρι την εποχή του στο μνημειώδες έργο του 'Στοιχεία' και αποτελουν ίσως το σημαντικότερο μαθηματικό σύγγραμα όλων των εποχών. Στο έργο αυτό εισάγεται η 'αξιωματική μέθοδος',ο τρόπος κατασκευής, δηλαδή, μιας επιστημονικής θεωρίας κατά τον οποίο ορισμένες προτάσεις (αξιώματα) λαμβάνονται ως αρχή και από αυτά συνάγονται μία ακολουθία θεωρημάτων με μία ακολουθία συλλογισμών, την αποδείξη. Στα βιβλία *VII,VIII,IX* από τα 'Στοιχεία' του Ευκλείδη θεωρούνται σήμερα τα αρχαιότερα βιβλία Θεωρίας Αριθμών. Σε αυτά αναλύονται τα τρία σπουδαία συμπεράσματα στα οποία εφτάσαν οι Αρχαίοι Έλληνες μαθηματικοί σχετικά με τους πρώτους αριθμούς.

2.1.1 Η απειρία των πρώτων αριθμών

Το πρώτο έχει να κάνει με την ερώτηση 'Πόσοι είναι οι πρώτοι αριθμοί;'. Ο Ευκλείδης αποδεικνύει ότι οι πρώτοι αριθμοί είναι άπειροι στο βιβλίο IX.

Πρόταση IX.20

Οι πρώτοι αριθμοί είναι περισσότεροι από κάθε δεδομένο σύνολο πρώτων

Αριθμών.

Απόδειξη

Έστω τρεις δοσμένοι πρώτοι αριθμοί α, β, γ. Θα αποδείξουμε ότι υπάρχουν περισσότεροι πρώτοι αριθμοί από τους α, β, γ. Έστω ότι ο ε είναι ο ελάχιστος αριθμός ο οποίος μετριέται από τους α, β, γ (ή ισοδύναμα διαρείται με τους α, β, γ). Προσθέτουμε στον ε την μοναδα μ. Προκύπτει ο αριθμός $\delta = \varepsilon + \mu$. Αν ο δ είναι πρώτος η πρόταση αποδείχτηκε. Αν δεν είναι πρώτος τότε διαιρείται από έναν άλλο αριθμό έστω τον ζ. Θα δείξουμε ότι ο ζ δεν είναι ένας από τους α, β, γ. Έστω ότι είναι ένας από αυτούς, τότε θα μετράει τον δ και αφού θα μετράει και τον ε θα μετράει και τη διαφορά τους, δήλαδη την μονάδα μ. Άτοπο.

Σε σύγχρονη μορφή θα λέγαμε ότι αποδείχτηκε το εξής αποδείχτηκε το εξής Θεώρημα:

Έστω n δοσμένοι πρώτοι $p_1, p_2, p_3, \dots, p_n$ τότε ο αριθμός $p_1 \bullet p_2 \bullet p_3 \bullet p_n + 1$ είναι πρώτος. Άρα, οι πρώτοι είναι άπειροι. Η απόδειξη αυτή του Ευκλείδη αποτελεί ένα πραγματικό κόσμημα στην Ιστορία όλων των Μαθηματικών και είναι ένα από τα κλασικά παραδείγματα που αποδεικνύουν ότι τα κριτήρια της ορθότητας και της αισθητικής στα Μαθηματικά συμπίπτουν. Δεν είναι τυχαίο ότι περιλαμβάνεται σχεδόν αυτούσια σε οποιοδήποτε σύγχρονο βιβλίο Θεωρίας Αριθμών πάνω από 2.300 χρόνια μετά τη πρώτη της εμφάνιση.

2.1.2 Οι τέλειοι αριθμοί

Το δεύτερο σπουδαίο συμπέρασμα έχει να κάνει με τους τέλειους αριθμούς. Παραθέτουμε τον ορισμό των 'Στοιχείων'.

Ορισμός VII.23

Τέλειος αριθμός είναι ο ίσος με το άθροισμα των αριθμών που ο καθένας αποτελεί μέρος του.

Σήμερα θα λέγαμε ότι τέλειος είναι ο αριθμός που είναι ίσος με το άθροισμα των γνησίων διαιρετών του. Τέλειοι αριθμοί είναι, για παράδειγμα,οι 6 και 28. Στην πορεία της μελέτης των τέλειων αριθμών ο Ευκλείδης παρουσιάζει την εξής πρόταση.

Πρόταση IX.35

Αν υπάρχουν οσοιδήποτε αριθμοί σε συνεχή αναλογία και αφαιρεθεί από το δεύτερο και τον τελευταίο ο πρώτος αριθμός της συνεχούς αναλογίας, τότε ο λόγος των διαφορών που προκύπτουν είναι ίσος με το λόγο του πρώτου αριθμού της συνεχούς αναλογίας προς το άθροισμα όλων των δοσμένων αριθμών, εκτός του τελευταίου.

Απόδειξη

Έστω ότι έχουμε τέσσερις αριθμούς α, β, γ και δ σε συνεχή αναλογία. Θα δείξουμε ότι ο λόγος της διαφοράς των β, α προς την διαφορα των δ, α είναι ίσος με τον λόγο του α προς το άθροισμα των α, β και γ. Αφού οι αριθμοί βρίσκονται σε συνεχή αναλογία, ισχύει ότι ο λόγος τους α προς τον β είναι ίσος με τον λόγο του β προς τον γ και το λόγο του γ προς τον δ. Με εναλλαγή έχουμε ότι ο λόγος του δ προς τον γ είναι ίσος με το λόγο του γ προς το β και ίσος με το λόγο του β προς το α. Αφαιρώντας τους παρανομαστές από τους αριθμητές των παραπάνω λόγων έχουμε ότι ο λόγος του $\delta - \gamma$ προς τον γ είναι ίσος με το λόγο του $\gamma - \beta$ προς τον β και ίσος με τον λόγο του $\beta - \alpha$ προς τον α. Επείδη ο λόγος του αθροίσματος των αριθμητών προς το άθροισμα των παρανομαστών ισούται με οποιοδήποτε από τους λόγους της προηγούμενης αναλογίας, ο λόγος της διαφοράς των β, α προς τον α θα ισούται με το λόγο της διαφοράς των δ, α προς τον άθροισμα α, β, γ. Αν εναλλάξουμε τους όρους έχουμε το ζητούμενο.

Αλγεβρικά η συλλογιστική της απόδειξη είναι η εξής :

$$\frac{\alpha}{\beta} = \frac{\beta}{\gamma} = \frac{\gamma}{\delta} \Rightarrow \frac{\beta}{\alpha} = \frac{\gamma}{\beta} = \frac{\delta}{\gamma} \Rightarrow \frac{\beta-\alpha}{\alpha} = \frac{\gamma-\beta}{\beta} = \frac{\delta-\gamma}{\gamma} = \frac{\beta-\alpha+\gamma-\beta+\delta-\gamma}{\alpha+\beta+\gamma} = \frac{\delta-\alpha}{\alpha+\beta+\gamma}$$

Εναλλάσοντας τους όρους στον πρώτο και τον τελευταίο λόγο έχουμε $\frac{\beta-\alpha}{\delta-\alpha} = \frac{\alpha}{\alpha+\beta+\gamma}$

Σε σύγχρονη μορφή θα λέγαμε ότι στην πρόταση αυτή εξετάζεται το άθροισμα των ν πρώτων όρων της γεωμετρικής προόδου α,αλ,αλ^2,αλ^3 … αφού εκφράζει ότι

$$\frac{\alpha\lambda-\alpha}{\alpha\lambda^{\nu}-\alpha} = \frac{\alpha}{\alpha+\alpha\lambda+\alpha\lambda^2+\alpha\lambda^3+\cdots+\alpha\lambda^{\nu-1}}$$

$$\text{ή αλλιώς } \alpha + \alpha\lambda + \alpha\lambda^2 + \alpha\lambda^3 \ldots + \alpha\lambda^{\nu-1} = \alpha(\frac{\lambda^{\nu}-1}{\lambda-1})$$

Με βάση τη σύγχρονη αλγεβρική ορολογία η απόδειξη είναι η ακόλουθη.

Αν $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{\nu}, \alpha_{\nu+1}$ είναι όροι γεωμετρικής προόδου με λόγο λ τότε θα έχουμε :

$$\frac{\lambda}{1} = \frac{a_2}{a_1} = \frac{a_3}{a_2} = \frac{a_4}{a_3} = \ldots = \frac{a_{\nu}}{\alpha_{\nu-1}} = \frac{\alpha_{\nu+1}}{\alpha_{\nu}}$$

$$\frac{\lambda-1}{1} = \frac{\alpha_2-\alpha_1}{\alpha_1} = \frac{\alpha_3-\alpha_2}{\alpha_2} = \frac{\alpha_4-\alpha_3}{\alpha_3} = \ldots = \frac{\alpha_{\nu+1}-\alpha_{\nu}}{\alpha_{\nu}} = \frac{\alpha_{\nu+1}-\alpha_1}{\sum_1^{\nu}\alpha_{\nu}}$$

Όπου $\sum_1^{\nu}\alpha_{\nu} = \alpha_1 + \alpha_2 + \alpha_3 + \ldots + \alpha_{\nu}$

Άρα $\sum_1^{\nu}\alpha_{\nu} = \frac{\alpha_{\nu+1}-\alpha_1}{\lambda-1} = \frac{\alpha_1\lambda^{\nu}-\alpha_1}{\lambda-1} = \frac{\alpha_1(\lambda^{\nu}-1)}{\lambda-1}$

Ή συσχέτιση των τέλειων αριθμών με τους πρώτους αριθμούς ερευνήθηκε στην πρόταση IX. 36.

<u>Πρόταση IX.36</u>

Αν το άθροισμα ενός δοσμένου πλήθους αριθμών που βρίσκονται σε συνεχή αναλογία, η οποία ξεκινά από τη μονάδα και έχει λόγο τον 2, είναι πρώτος αριθμός, τότε το γινόμενο του αθροίσματος με τον τελευταίο αριθμό της συνεχούς αναλογίας θα είναι τέλειος αριθμός.

Απόδειξη

Ας θεωρήσουμε ότι για τέσσερις αριθμούς μετά την μονάδα τους α, β, γ και δ έχουμε ότι το αθροισμά τους ε είναι πρώτος αριθμός. Έστω ότι το γινόμενο του ε με τον δ ότι είναι ζ. Θα αποδείξουμε ότι ο ζ είναι τέλειος αριθμός. Ας θεωρήσουμε τέσσερις αριθμούς σε συνεχή αναλογία με λόγο 2, ξεκινώντας από τον ε : $\varepsilon, \theta, \lambda, \kappa$. Τότε ο λόγος του α προς το δ είναι ίσος με το λόγο του ε προς το κ. Άρα το γινόμενο των α, κ είναι ίσο με ζ. Επομένως ο κ μετράει τον ζ κατά α μονάδες. Όμως ο α είναι ο 2, επομένως ο ζ είναι διπλάσιος του κ, οπότε οι $\varepsilon, \theta, \lambda, \kappa, \zeta$ βρίσκονται σε συνεχή αναλογία με λόγο 2. Ας αφαιρέσουμε από το θ (που είναι δεύτερος στη συνεχή αναλογία) και από τον ζ (που είναι τελευταίος) τον ε, οπότε προκύπτουν οι διαφορές $\theta - \varepsilon$ και $\zeta - \varepsilon$, των οποίων ο λόγος είναι ίσος με τον λόγο του πρώτου ε προς το άθροισμα όλων των αριθμών που βρίσκονται σε συνεχή αναλογία εκτός του τελευταίου (δηλαδή των $\varepsilon, \theta, \lambda, \kappa$). Αφού όμως ο $\theta - \varepsilon$ είναι ίσος με τον ε, ο $\zeta - \varepsilon$ θα είναι ίσος με το άθροισμα των $\varepsilon, \theta, \lambda, \kappa$. Επομένως ο ζ θα είναι ίσος με το άθροισμα των $\varepsilon, \theta, \lambda, \kappa, \alpha, \beta, \gamma, \delta$ και της μονάδας και μετριέται από αυτούς. Θα αποδείξουμε ότι ο ζ δεν μετριέται από κανέναν άλλο αριθμό. Έστω ότι ο ζ μετριέται από τον ξ κατά π μονάδες και ότι ο ξ είναι διαφορετικός από τους $\alpha, \beta, \gamma, \delta, \varepsilon, \theta, \lambda, \kappa$. Αφού ο ζ είναι το γινόμενο των ε, δ θα έχουμε ότι ο λόγος του ε προς τον π είναι ίσος με τον λόγο του ξ προς το δ. Όμως ο δ δε μετριέται παρά μόνο από τους α, β, γ. Ο ξ είναι διαφορετικός από τους α, β, γ άρα δεν μετράει το δ. Επομένως, ούτε και ο ε μετράει τον π. Ο ε όμως είναι πρώτος, οπότε οι ε, π θα είναι πρώτοι μεταξύ τους, οπότε ο ε μετρά τον ξ και ο π τον δ. Αφού ο π μετράει τον δ, θα ταυτίζεται με κάποιον από τους α, β, γ. Έστω ότι ο π ταυτίζεται με τον β. Τότε, αφού το γινόμενο των β, λ είναι ίσο με το γινόμενο των δ, ε, το οποίο είναι ίσο με το γινόμενο των π, ξ θα έχουμε ότι ο λόγος του π προς το β, είναι ίσος με το λόγο του λ προς το ξ. Όμως ο π ταυτίζεται με τον β, οπότε ο λ θα είναι ίσος με τον ξ, που είναι άτοπο. Επομένως ,ο ζ μετριέται μόνο από τους αριθμούς $1, \alpha, \beta, \gamma, \delta, \varepsilon, \theta, \lambda, \kappa$ και ισούται με το άθροισμά τους. Άρα είναι τέλειος.

Η απόδειξη σύγχρονη αλγεβρίκη μορφή είναι η εξής.

Έστω οι αριθμοί $1, \alpha = 2,\ \beta = 4,\ \gamma = 8,\ \delta = 16$ και το άθροισμά τους $\varepsilon = 31$. Θα αποδείξουμε ότι το γινόμενο $\varepsilon \bullet \delta = 31 \bullet 16 = 496$ είναι τέλειος. Θεωρούμε τη γεωμετρική πρόοδο $\varepsilon = 31, \theta = 62, \lambda = 124, \kappa = 248$. Έχουμε $\frac{\alpha}{\delta}$ = $\frac{\varepsilon}{\kappa}$($\frac{2}{16}$ = $\frac{31}{248}$),άρα $\alpha\kappa = 496 = \zeta$. Όμως ο $\zeta = 496$ είναι ο επόμενος όρος της προόδου $\varepsilon, \theta, \lambda, \kappa$ οπότε $\frac{\theta-\varepsilon}{\zeta-\varepsilon}$ = $\frac{\varepsilon}{\varepsilon+\theta+\lambda+\kappa}$ όμως $\theta - \varepsilon = \varepsilon$ άρα $\zeta - \varepsilon = \varepsilon + \theta + \lambda + \kappa$ ή $\zeta = \varepsilon + \varepsilon + \theta + \lambda + \kappa = 1 + \alpha + \beta + \gamma + \delta + \varepsilon + \theta + \lambda + \kappa$. Με απαγωγή σε άτοπο αποδεικνύεται ότι ο ζ δε διαιρείται από κανέναν άλλο παρά μόνο από τους $1,\ \alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \theta,\ \lambda,\ \kappa$ άρα είναι τέλειος.

Σήμερα θα λέγαμε 'Αν το άθροισμα των ν πρώτων όρων της γεωμετρικής προόδου $1,2,2^{\nu},\ldots,2^{\nu+1}$,δηλαδή ο $2^{\nu} - 1$, είναι πρώτος αριθμός τότε ο $2^{\nu-1}(2^{\nu} - 1)$ είναι τέλειος'. Η σημασία αυτής της πρότασης είναι τεράστια αφού για πρώτη φορά συνδέονται οι τέλοιοι με τους πρώτους. Όπως θα αναφερθεί στη συνέχεια, η συσχέτιση αυτή θα διαδραματίσει σπουδαίο ρόλο στην εύρεση πρώτων αριθμών.

Όπως ήδη αναφερθήκαμε, οι Αρχαίοι Έλληνες είχαν δώσει μέσω της πρότασης *IX.36* στα 'Στοιχεία'του Ευκλείδη μία μέθοδο εύρεσης τέλειων αριθμών. Οι μαθηματικοί μετά τους Αρχαίους Έλληνες ανέλαβαν το δύσκολο έργο της επέκτασης του πίνακά τους. Φαίνεται όμως ότι δεν ήταν οι μόνοι που ενδιαφέρονταν ιδιαίτερα για αυτούς. Ο Αυγουστίνος (περίπου 400 μ.Χ.) αναφέρει ότι ο Θεός έφταξε τον κόσμο σε έξι μέρες μία και η τελειότητα της εργασίας αυτής σηματοδοτείται από τον αριθμό 6, δρομολογώντας έτσι μία σειρά από θρησκευτικές αναφορές στους τέλειους αριθμούς.

Ο Νικόμαχος ο Γερασηνός (περίπου 100 μ.Χ.) αναφέρει τους τέλειους 6,28,496 και 8128.Ο L.Fibonacci μελέτησε τους τέλειους αριθμούς και διατύπωσε την εικασία ότι είναι άπειροι. Σε ένα χειρόγραφο που χρονολογείται στα μέσα του $15^{ου}$ αιώνα δίνεται ο πέμπτος τέλειος αριθμός 33.550.336. Πολλοί ερευνητές της εποχής πίστευαν ότι οι αριθμοί $2^{\nu} - 1$ είναι πρώτοι για κάθε περιττό ν. Οι πρώτοι αυτής της μορφής θα έδιναν σίγουρα έναν τέλειο αριθμό σύμφωνα με το Θεώρημα του Ευκλείδη. Το 1536 όμως ο H.Regius παρατηρεί ότι $2^9 - 1 = 511 = 7 \bullet 73$ και $2^{11} - 1 = 2047 = 23 \bullet 89$. Ο A.Cataldi, ένας μαθηματικός από

τη Μπολόνια απέδειξε ότι ο έκτος τέλειος είναι ο 8.589.869.056 και ο έβδομος ο 137.438.691.328 διαψεύδοντας αρκετούς που πίστευαν ότι τα τελευταία ψηφία των διαδοχικών τέλειων αριθμών εναλλάσσονται μεταξύ 6 και 8. Επίσης, αφού σημείωσε ότι ο $2^{\nu}-1$ είναι σύνθετος αν ο ν είναι σύνθετος, διατύπωσε την εικασία ότι οι αριθμοί αυτής της μορφής είναι πρώτοι για $\nu = 12, 17,\ 19, 23, 29$ και 37. Ο P.Bungus δίνει (1584) έναν πίνακα με 28 τέλειους αριθμούς. Αργότερα ο Fermat δηλώνει τη πίστη του ότι οι τέλειοι αριθμοί είναι πιο σπάνιοι από όσο γενικά πίστευαν οι σύγχρονοι του. Δηλώνει ότι δεν υπάρχουν τέλεοι με 20 ή 21 ψηφία και γενικά δεν υπάρχει ένας τέλειος αριθμός ανάμεσα σε δύο διαδοχικές δυνάμεις του 10 όπως είχε αρχίσει να καθιερώνεται σαν άποψη. Το 1640 στένει ένα γράμμα στον Marin Mersenne, έναν Γάλλο μοναχό που εκτός από τα θρησκευτικά του καθήκοντα ασχολήθηκε ιδιαίτερα με τα Μαθηματικά και τη Μουσική και με τον οποίο αλληλογραφούσε συχνά κοινοποιώντας τις μαθηματικές του ανακαλύψεις. Στο γράμμα αυτό ο Fermat ανέφερε ότι απέδειξε τρεις προτάσεις που αποκάλεσε τη βάση της ανακάλυψης τέλειων αριθμών. Αν ο ν είναι σύνθετος τότε ο $2^{\nu}-1$ είναι σύνθετος, αν ο ν είναι πρώτος,τότε ο $2^{\nu}-2$ διαιρείται από το 2ν και ο $2^{\nu}-1$ διαιρείται μόνο από πρώτους της μορφής $2\kappa\nu+1$. Την ίδια περίοδο δείχνει ότι ο 47 είναι παράγοντας του $2^{23}-1$ και ο 223 του $2^{37}-1$ καταρρίπτοντας την εικασία του A.Cataldi. Ο M.Mersenne ασχολήθηκε επίσης εκτενώς με τους αριθμούς της μορφής $2^{\nu}-1$. Είναι σίγουρα σύνθετοι αν ο ν είναι σύνθετος αλλά αν ο ν είναι πρώτος είναι πιθανό να είναι πρώτοι. Οι πρώτοι αυτής της μορφής είναι μία ειδική κατηγορία πρώτων αριθμών που ονομάζονται σήμερα πρώτοι του Mersenne. Το 1644 ανακοίνωσε ότι μόνο 8 από τους 28 του P.Bungus είναι πράγματι τέλειοι και διατύπωσε την εικασία ότι ο $2^{\nu}-1$ είναι πρώτος αν και μόνο αν ο ν είναι ένας από τους 2,3,5,13,19,31,67,127 και 257.Έκανε λάθος για ν=61,67,89,109 και 257 αλλά η διαιώνιση του ονόματός του εύκολα δικαιολογείται αν αναλογιστούμε ότι σωστά χαρακτήρισε ως πρώτους ή μη τους αριθμούς της μορφής $2^{\nu}-1$ με λιγότερα από 19 ψηφία. Μεγάλη εντύπωση προκαλεί η εικασία του χαρακτηρισμού ως πρώτων για τους αριθμούς $2^{127}-1$ και $2^{257}-1$. Ο πρώτος έχει 39 ψηφία και ο δεύτερος 77. Η επιβεβαίωση για τον πρώτο από τους δύο ήρθε περίπου 250 χρόνια αργότερα ενώ η διάψευση για το δεύτερο πήρε ακόμα περισσοτερο. Για να αναδείξουμε τη σημασία των πρώτων του Mersenne αρκεί να αναφέρουμε ότι σήμερα η εύρεση πρώτων αριθμών περνάει τις περισσότερες φορές μέσα από την εύρεση πρώτων αυτού του είδους.

Σε ένα γράμμα του στον Goldbach το 1752, ο Euler, ανακοινώνει ότι γνωρίζει μόνο εφτά τέλειους αριθμούς της μορφής $2^{\nu-1}(2^{\nu}-1)$,συγκεκριμένα για $\nu = 2,3,5,7,13,17,19$ ενώ δηλώνει αβέβαιος για το $\nu = 31$. Το 1772 όμως,σε ένα γράμμα στον D.Bernoulli δηλώνει πως έχει επαληθεύσει ότι ο $2^{31}-1$ είναι πρώτος δίνοντας ουσιαστικλα τον όγδοο τέλειο. Επιπλέον ο Euler έδωσε τους μικρότερους παράγονες των $2^{\nu}-1$ για $\nu = 37,43,29$ και 73 αποκλείοντας τους από τους πρώτους αριθμούς και γλιτώνοντας από μεγάλο υπολογιστικό κόπο τους μεταγενέστερους μαθηματικούς και ερευνητές. Η πιο σημαντική προσφορά του όμως στο κυνήγι των τέλειων ήταν η απόδειξη της εξής πρότασης:

Οι μόνοι άρτιοι τέλειοι αριθμοί είναι της μορφής $2^{\nu-1}(2^{\nu}-1)$ όπου ο $2^{\nu}-1$ είναι πρώτος.

<u>Απόδειξη</u>

Έστω $\sigma(\nu)$ η συνάρτηση που ορίζεται ως το άθροισμα όλων των διαιρετών του ν συμπεριλαμβανουμένου και του ίδιου. Άρα ο ν θα είναι τέλειος αν και μόνο αν $\sigma(\nu) = 2\nu$. Εύκολα δείχνουμε ότι αν ο p είναι πρώτος τότε $\sigma(p^{a})$=$\frac{p^{a+1}-1}{p-1}$ καθώς επίσης και ότι $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ όπου α, β σχετικά πρώτοι.

Έστω τώρα ν ένας ν άρτιος και τέλειος αριθμός. Τότε ο $\nu = 2^{\alpha}m$ με $\alpha > 0$ και m περιττό, και έτσι $\sigma(\nu) = \sigma(2^{\alpha})\sigma(m)$ =$(2^{\alpha+1}-1)$σ(m). Από την άλλη, αφού ο ν είναι τέλειος θα έχουμε $\sigma(\nu)$=2ν=$2^{\alpha+1}m$. Εξισώνοντας παίρνουμε ότι :

$$(2^{\alpha+1}-1)\sigma(m) = 2^{\alpha+1}m$$

Αυτό σημαίνει ότι ο $2^{\alpha+1}-1$ πρέπει να είναι διαιρέτης του m αφού δεν έχει κοινό παράγοντα με τον $2^{\alpha+1}$. Άρα m=$(2^{\alpha+1}-1)l$ για κάποιον ακέραιο l. Με αντικατάσταση στη παραπάνω σχέση και με απαλοιφή του $2^{\alpha+1}-1$ προκύπτει ότι $\sigma(m) = 2^{\alpha+1}l = l + (2^{\alpha+1}-1)l = l + m$. Επειδή οι l και m είναι και οι δύο διαιρέτες του m και αθροίζονται στο $\sigma(m)$ πρέπει να είναι οι μόνοι διαιρέτες του m. Επειδή όμως και ο 1 είναι διαιρέτης του m πρέπει να έχουμε $l = 1$ και άρα $m = 2^{\alpha+1}-1$ και πρώτος.

Μετά από αυτό το Θεώρημα αν θέλουμε να αναζητήσουμε περιττούς τέλειους πρέπει να ψάχνουμε αποκλειστικά σε αριθμούς της μορφής $2^{\nu-1}(2^{\nu}-1)$ όπου οι ν ,$2^{\nu}-1$ είναι πρώτοι.

Θα πρέπει βέβαια να αναφέρουμε ότι η πρόταση αυτή δεν άλλαξε και πολύ τις μεθόδους αναζήτησης τέλειων αριθμών των σύγχρονων μαθηματικών. Ούτως ή άλλως εκεί στόχευαν όταν τους αναζητούσαν και ήταν πολλοί εκείνοι που είκαζαν την ισχύ της παραπάνω πρότασης. Η απόδεικη, όμως, οριστικοποίησε τη κατάσταση. Επίσης παρατηρούμε ότι με τα παραπάνω καλύπτουμε τους άρτιους τέλειους.Για τους περιττούς; Μέχρι σήμερα δεν έχει βρεθεί περιττός τέλειος και είναι ένα ανοιχτό ερώτημα αν υπάρχει. Αν υπάρχει πάντως πρέπει να έχει τουλάχιστον 11 διακριτούς παράγοντες ενώ θα είναι σίγουρα μεγαλύτερος του 10^{100}.

2.1.3 Το Θεμελιώδες Θεώρημα της Αριθμητικής

Το τρίτο σπουδαίο συμπέρασμα έχει να κάνει με το ρόλο των πρώτων αριθμών στη δομή των φυσικών. Τα αποτελέσματα των Αρχαίων Ελλήνων σε αυτό το τομέα έφτασαν σε αυτό που ονομάζουμε σήμερα Θεμελιώδες Θεώρημα της Αριθμητικής. Και μόνο το όνομά του είναι ικανό για να αντιληφθεί κανείς σε πόσο υψηλό επιπέδο ασχολήθηκαν με τις έννοιες αυτές.

Σύμφωνα με το Θεμελιώδες Θεώρημα της Αριθμητικής, κάθε φυσικός αριθμός γράφεται κατά μοναδικό τρόπο (αν δε λάβουμε υπόψη τη σειρά των παραγόντων) σαν γινόμενο πρώτων αριθμών.

Θεμελιώδες Θεώρημα της Αριθμητικής

Για κάθε φυσικό αριθμό n με n>1

Υπάρχουν πρώτοι $p_1, p_2, \dots, p_k$ *και φυσικοί* $a_1, a_2, \dots, a_k$

τέτοιοι ώστε $n = p_1^{a_1} \bullet p_2^{a_2} \dots p_k^{a_k}$

Οι πρώτοι αριθμοί, δηλαδή, είναι οι δομικοί λίθοι με τους οποίους κατασκεύαζονται όλοι οι αριθμοί. Ο Davis (2007) αναφέρει ότι 'ενδεικτικό της ιδιοφυίας των Ελλήνων είναι το γεγονός ότι είχαν συνειδητοποιήσει όπως η μοναδικότητα της παραγοντοποίησης είναι ένα αποτέλεσμα που χρειάζοταν απόδειξη'. Ο Ευκλείδης έφτασε πολύ κοντά στην απόδειξη, όπως θα την διαβάζαμε σήμερα σε ένα βιβλίο Θεωρίας Αριθμών, στο ένατο βιβλίο των 'Στοιχείων'.

2.1.4. Φίλοι αριθμοί

Δύο αριθμοί λέγονται φίλοι αν ο καθένας είναι ίσος με το άθροισμα των γνήσιων δαιρετών του άλλου. Οι πυθαγόρειοι ήξεραν το ζεύγος 220 και 284. Όταν κάποτε ο Πυθαγόρας ρωτήθηκε 'τι εστί φίλος' απάντησε 'έτερος εγώ' και ανέφερε τους αριθμούς αυτούς. Τον ένατο αιώνα ο Άραβας Thabit ben Korrah έδωσε έναν κανόνα εύρεσης φίλων αριθμών:

Για έναν φυσικό αριθμό n>1 αν οι

$p = 3 \bullet 2^{n-1} - 1, q = 3 \bullet 2^n - 1$ *και* $r = 9 \bullet 2^{2n-1} - 1$

είναι όλοι πρώτοι, τότε το ζευγάρι των αριθμών

$(2^n \bullet p \bullet q, 2^n \bullet r)$ είναι φίλοι.

Για $n = 2$ παίρνουμε τους 220, 284. Παρόλα αυτά, ο ίδιος ο Korrah δεν έδωσε κάποιο καινούργιο ζευγάρι ούτε και κανένας άλλος μετά από αυτόν μέχρι τον Fermat που, κατά δήλωση του Mersenne, βρήκε το δεύτερο ζευγάρι 17.296 και 18.216 και έδωσε έναν γενικό κανόνα εύρεσης φίλων αριθμών. Ο R.Descartes έδωσε την ίδια εποχή έναν ισοδύναμο κανόνα και το τρίτο ζευγάρι 9.363.584 και 9.437.056. Αυτός όμως που και πάλι έδωσε άλλη

ώθηση στο συγκεκριμένο πρόβλημα δεν ήταν άλλος από τον Euler. Κατηγοριοποίησε το πρόβλημα εύρεσης φίλων αριθμών, έδωσε καινούργιους κανόνες και κατέληξε σε 61 καινούργια ζευγάρια. Πολλοί από αυτούς του αριθμούς είχαν πάνω από 10 ψηφία.

Εντούτοις,το 1866 ο N.I.Paganini σε ηλικία μόλις 16 ετών έδωσε το δεύτερο μικρότερο ζευγάρι (1184, 1210) που είχε διαφύγει τόσο στον Euler και σε όλους τους προγενέστερους. Ο ίδιος πάντως δεν εξήγησε τη μέθοδο που ακολούθησε. Οι μεταγενέστεροι μαθηματικοί στηρίχτηκαν στις μεθόδους του Euler και βρήκαν πολλά νέα ζευγάρια. Το αν υπάρχουν άπειροι φίλοι αριθμοί είναι ένα ανοιχτό πρόβλημα.

2.2. Σύγχρονη εποχή

2.2.1.Πίνακες πρώτων

Το πόσο μεγάλα ήταν τα βήματα προόδου σχετικά με τη γνώση μας για τους πρώτους αριθμούς στην Αρχαία Ελλάδα υπερτονίζεται και από τη δυσανάλογη συνέχεια. Εκτός από κάποιες μεμονωμένες προσπάθειες που συνεισφέρουν κυρίως στο πρακτικό μέρος της μελέτης των πρώτων, έπρεπε να φτάσουμε στον 17^{ο} αιώνα για να προχωρήσει η θεωρητική τους μελέτη και να αποκαλυφθούν λίγα περισσότερα από τα μυστικά που κρύβουν. Αυτό βέβαια συνέβη και με πολλές έννοιες και κλάδους των Μαθηματικών, εδώ όμως υπήρχε και ένα επιπλέον λόγος : το πολύπλοκο ρωμαικό σύστημα αρίθμησης που χρησιμοποιήθηκε από τους Ευρωπαίους εώς το 1400 μ.Χ. περίπου.

Οι πρώτοι αριθμοί, λοιπόν, είναι άπειροι αλλά αφού δεν υπάρχει και τρόπος να τους βρίσκουμε ,ποιοι είναι; Στη γενική περίπτωση το ερώτημα δε μπορεί να απαντηθεί άμεσα. Για την ακρίβεια μερικές φορές είναι εξαιρετικά δύσκολο να αποφασίσουμε αν ένας τυχαίος αριθμός είναι πρώτος ή σύνθετος. Για το λόγο αυτό, ήδη από την εποχή των Αρχαίων Ελλήνων, κατασκευάζονταν πίνακες που διαχώριζαν δεδομένους φυσικούς σε πρώτους και σύνθετους. Οι πίνακες αυτοί ονομάζονται πίνακες πρώτων (prime tables) ή

πίνακες παραγόντων (factor tables). Απ'όσο γνωρίζουμε ο πρώτος που εφήυρε μέθοδο κατασκευής πίνακα πρώτων αριθμών ήταν ο Ερατοσθένης (περίπου 275 – 194 π.Χ). Ο Ερατοσθένης ήταν Αλεξανδρινός λόγιος και διατέλεση διευθυντής της μεγάλης βιβλιοθήκης της Αλεξάνδρειας από το 234 π.Χ. και για περίπου 40 χρόνια. Είναι διάσημος για την κατά 99% προσέγγισή του στον υπολογισμό της περιφέρειας της Γης στο έργο του 'Γεωγραφικά'. Είναι ένα γεγονός ιδιαίτερα εντυπωσιακό αν αναλογιστεί κανείς ότι η προσέγγιση αυτή δε βελτιώθηκη για σχεδόν μία χιλιετία ενώ η παγκόσμια κοινή γνώμη δεν είχε αποδεχτεί ότι η Γη δεν είναι επίπεδη για τουλάχιστον δεκαπέντε αιώνες μετά από εκείνον. Μέχρι την εποχή του, αν ήθελε κάποιος να ελέγξει αν ένας φυσικός αριθμός είναι πρώτος ή σύνθετος έπρεπε να κάνει διαιρέσεις με όλους τους προηγούμενούς του. Οι Αρχαίοι Έλληνες όμως είχαν ένα πολύπλοκο συμβολίσμό για τους αριθμούς που καθιστούσε τη διαίρεση αρκετά επίπονη. Η μέθοδος του Ερατοσθένη δεν απαιτεί καμία διαίρεση. Είναι δε σε θέση να δώσει το σύνολο των πρώτων αριθμών (ή αλλιώς να διαχωρίσει τους αριθμούς σε πρώτους και σύνθετους) που είναι μικρότεροι από έναν δοσμένο. Η διαδικασία είναι η ακόλουθη.

Γράφουμε όλους τους φυσικούς αριθμούς που θέλουμε να διαχωρίσουμε σε πρώτους και σύνθετους ξεκινώντας από το 2. Αφήνουμε το 2 ανέπαφα και διαγράφουμε κάθε δεύτερο αριθμό μετά το 2, δηλαδή τα πολλαπλάσιά του. Ο αμέσως επόμενος που μένει μετά από αυτή τη διαδικασία είναι ο 3. Τον αφήνουμε ανέπαφο και διαγράφουμε μετά από αυτόν κάθε τρίτο αριθμό ανεξαρτήτως αν έχει ήδη διαγραφεί ή όχι. Ο αμέσως επόμενος που μένει είναι ο 5. Τον αφήνουμε ανέπαφο και διαγράφουμε κάθε πέμπτο αριθμό μετά από αυτόν ανεξαρτήτως αν έχει ήδη διαγραφεί ή όχι. Συνεχίζοντας τη διαδικασία όσο πάει, οι αριθμοί που θα μείνουν θα είναι πρώτοι. Για την ακρίβεια η διαδικασία ουσιαστικά τελειώνει μόλις φτάσουμε στον πρώτο ακέραιο που είναι μικρότερος από την τετραγωνική ρίζα του μεγαλύτερου αριθμού στον πίνακα, όπως εύκολα μπορεί να αποδειχτεί. Η διαδικασία αυτή ονομάζεται κόσκινο του Ερατοσθένη.

Οι πρώτοι πίνακες πρώτων και παραγόντων φαίνεται ότι κατασκευάστηκαν σαν απαντήσεις σε προβλήματα διοφαντικής ανάλυσης. Η ανάπτυξη της τυπογραφίας βοήθησε στην διάδοση πινάκων πρώτων. Ο Frans van Schooten εξέδωσε το 1657 ένα κατάλογο με τους πρώτους ως το 9979. Το 1668, ο T.Brancker κατασκεύασε ένα κατάλογο με τους

μικρότερους διαιρέτες των αριθμών που δεν διαιρούνται με το 2 ή το 5 έως το 100.000. Ο J.Harris δημοσίευσε το 1685 μία λίστα με λάθη στον πίνακα του Brancker, ολοκληρώνοντας το έργο του. Αυτή τη μορφή είχε η εξέλιξη της αναζήτησης των πρώτων αριθμών. Ο ένας ερευνητής μετά τον άλλο κατασκεύαζαν όλο και μεγαλύτερους πίνακες πρώτων αριθμών ή πίνακες παραγόντων που οι υπόλοιποι έλεγχαν για την ορθότητά τους και τους συμπλήρωναν.

Οι μέθοδοι παραγοντοποίησης που χρησιμοποιούσαν είχαν αρχίσει να εξελίσσονται. Μία δίασημη μέθοδος που χρονολογείται από το 1643 οφείλεται στον Fermat και φέρει το όνομά του. Σήμερα θα λέγαμε ότι όλη η ιδέα βασίζεται στη σχέση.

$$\nu = \alpha\beta = \left(\frac{\alpha+\beta}{2}\right)^2 - \left(\frac{\alpha-\beta}{2}\right)^2$$

Ας παραγοντοποιήσουμε το 6077. Παρατηρούμε ότι $77 < \sqrt{6077} < 78$ και έτσι αναζητούμε ένα τέλειο τετράγωνο ως εξής

$$78^2 - 6077 = 7$$

$$79^2 - 6077 = 164$$

$$80^2 - 6077 = 323$$

$$81^2 - 6077 = 484 = 22^2$$

Έτσι $6077 = 81^2 - 22^2 = (81 - 22)(81 + 22) = 59 \bullet 103$

Η μέθοδος αυτή δεν έχει πολλά περιθώρια βελτίωσης. Το βασικό της μειονέκτημα είναι ότι ίσως απαιτούνται πολλές δοκιμές μέχρι να βρούμε έναν αριθμό που να είναι τέλειο

τετράγωνο. Θεωρείται καλή μέθοδος μόνο αν γνωρίζουμε ότι ο αριθμός προς παραγοντοποίηση έχει δύο παράγοντες παρομοίου μεγέθους. Ο M.Mersenne πρώτος παρατήρησε ότι αν ένας αριθμός γράφεται σαν άθροισμα τετραγώνων με δύο διαφορετικούς τρόπους τότε είναι σύνθετος.Ο L.Euler απέδειξε ότι αν ένας αριθμός της μορφης $4\nu + 1$ γράφεται σαν άθροισμα τετραγώνων δύο σχετικά πρώτων με έναν μόνο τρόπο τότε είναι πρώτος. Έδωσε για παράδειγμα τον $1.000.009 = 1000^2 + 3^2$. Αργότερα αποδείχθηκε ότι ένας πρώτος δε μπορεί να γραφτεί στη μορφή $mx^2 + ny^2$ με 2 διαφορετικούς τρόπους αν οι m, n είναι σχετικά πρώτοι. Η μέθοδος, όμως, που αναπτύχθηκε και χρησιμοποιήθηκε ευρέως ήταν αυτή των τετραγωνικών υπολοίπων. Οφείλεται στους L.Euler και A.M.Legendre και βασίζεται στο γεγονός ότι όλοι οι αριθμοί με ένα συγκεκριμένο τετραγωνικό υπόλοιπο έχουν πρώτους διαιρέτες που ανήκουν σε μία συγκεκριμένη γραμμική μορφή. Για παράδειγμα αν το -1 είναι το τετραγωνικό υπόλοιπο ενός αριθμού, οι πρώτοι διαιρέτες του θα είναι της μορφης 4ν+1 όπου ο ν είναι φυσικός αριθμός και έτσι αποκλείουμε τους 3 ,7 ,9 ,11 ,19 κτλ. Επίσης αν το 2 είναι τετραγωνικό υπόλοιπό του,τότε έχει τη μορφη $8\kappa \pm 1$.Γενικά, η εξίσωση $x^2 \equiv 2 mod p$ λύνεται αν και μόνο αν $p \equiv \pm 1 mod 8$.

Το 1772,ο A.F. Marci εξέδωσε έναν πίνακα με τους πρώτους αριθμούς ως το 400.000. Τέσσερα χρόνια αργότερα,ο Αυστριακός μαθηματικός A.Felkel εκδίδει έναν πίνακα με όλους τους πρώτους παράγοντες των αριθμών που δεν διαιρούνται με το 2 το 3 ή το 5 μέχρι το 408.000. Ο τελευταίος είχε κατασκευαστεί με τη βοήθεια μιας πρωτότυπης συσκευής αποτελούμενης από ράβδους που υπολόγιζαν μηχανικά τους διαιρέτες. Στο χειρόγραφο ο πίνακας έφτανε μέχρι τα 2.000.000 αλλά και μια δεν υπήρχαν αγοραστές γα το εκδοθέν μέρος, ολόκληρη η έκδοση,εκτός από μερικά αντίτυπα, χρησιμοποιήθηκε στη κατασκευή βλημάτων στο πόλεμο των Αυστριακών κατά των Οθωμανών. Λίγα χρόνια αργότερα, στο πρόλογο της Λατινικής μετάφρασης του έργου του J.H.Lambert ‘ zusatze zu den logarithmischen und trig. Tabellen’, ο Felkel αναφέρει ότι δεν κατάφερε να ανακτήσει το εκτεταμένο του χειρόγραφο και έτσι υπολόγισε το 1785 εκ νέου όλους τους πρώτους παράγοντες των αριθμών από το 408.000 έως το 2.856.000.Στην περίφημη ‘Encyclopedie’ του d’Alembert (1780) υπήρχε, στο τέλος του δευτέρου τόμου, ένας πίνακας παραγόντων μέχρι το 100.000.Οι μηχανικές μέθοδοι του Felkel είχαν πλέον εξελιχτεί. Με τη μέθοδο των

στένσιλ, που βασίζεται σε κάρτες με έτοιμες τρύπες, το 1816 ο J.C. Burckhardt εκδίδει ένα τόμο με τους μικρότερους παράγοντες των αριθμών μέχρι το 3.036.000.

Ο J.P.Kulik αφιέρωσε είκοσι χρόνια στη κατασκευή ενός πίνακα παραγόντων μέχρι το 100.000.000. Το χειρόγραφο βρίσκεται στην βιβλιοθήκη της Βασιλικής Ακαδημίας της Βιέννης από το 1867. Η εργασία του κρίθηκε αρκετά ανακριβής για δημοσίευση και δεν εκδόθηκε ποτέ αφού στον έλεγχο που έγινε το 1909 από τον D.N.Lehmer βρέθηκαν 226 λάθη στη πρώτη δεκάδα εκατομμυρίων των αριθμών. Αργότερα ο δεύτερος τόμος του έργου που περιείχε τους αριθμούς από το 12.642.600 μέχρι τον 22.852.800 χάθηκε. Το συνολικό έργο αποτελούταν από οκτώ τόμους και 4.212 σελίδες.

Ο Z.Dase βασιζόμενος σε ένα γράμμα του C.F.Gauss και στη διαβεβαίωσή του ότι ένα χειρόγραφο με πίνακες παραγόντων για το τέταρτο, το πέμπτο και το έκτο εκατομμύριο αριθμών θα εκδοθεί, αποφάσισε να κατασκευάσει πίνακα παραγόντων για το πρώτο έβδομο εκατομμύριο των αριθμών. Το 1861 πέθανε αφήνοντας ένα εκπληκτικά ακριβές πίνακα παραγόντων για το έβδομο, ένα σχεδόν τελειωμένο για το όγδοο και μεγάλο μέρος για το ένατο και το δέκατο εκατομμύριο αριθμών.

2.2.2.Pierre de Fermat

<u>Το τελευταίο Θεώρημα του Fermat</u>

Αν n είναι φυσικός με $n > 2$ τότε η εξίσωση $\alpha^n + \beta^n = \gamma^n$ δεν έχει θετικές, ακέραιες λύσεις.

Οι αριθμοί Fermat είναι οι $F_n = 2^{2^n} + 1$ όπου n φυσικός αριθμός. Ο Fermat πίστευε ότι είναι όλοι πρώτοι για κάθε n και ότι αυτό θα μπορούσε να αποδειχθεί με επαγωγή αλλά δεν είχε την απόδειξη. Οι M. Mersenne και C. Goldbach είχαν την ίδια άποψη μέχρι που ο L. Euler

το 1748 ανακάλυψε ότι $F_5 = 2^{32} + 1 = 641 \bullet 6.700.417$. Στην ουσία απέδειξε ότι αν οι α και β είναι σχετικά πρώτοι, κάθε παράγοντας του $\alpha^{2n} + \beta^{2n}$ είναι ή 2 ή της μορφής $2^{n+1}k + 1$. Για $k = 10$ στην περίπτωση του F_5 έχουμε το 641. Αργότερα ο C.F.Gauss το 1801 βρήκε μία απρόσμενη σχέση ανάμεσα στους πρωτους του Fermat και τη κατασκευή κανονικών πολυγώνων με κανόνα και διαβήτη. Πρώτα σε ηλικία 17 ετών, έδωσε μία μέθοδο κατασκευής κανονικού δεκαεπταγώνου. Αργότερα, στο περίφημο έργο του 'Disquisitiones Arithmeticae' που εξέδωσε σε ηλικία 24 ετών, απέδειξε ότι ένα κανονικό πολύγωνο με m πλευρές μπορεί να κατασκευαστεί με κανόνα και διαβήτη μόνο αν ο m είναι γινόμενο με παράγοντες δυνάμεις του 2 και διακριτούς πρώτους του Fermat.

Η ενασχόλησή του με τους τέλειους αριθμούς τον οδήγησε στην ανακάλυψη αυτού που ονομάζουμε σήμερα 'μικρό' Θεώρημα του Fermat. Ο χαρακτηρισμός 'μικρό' καθιερώθηκε για να μην υπάρχει σύγχυση με το διάσημο 'τελευταίο' Θεώρημά του.

<u>Το 'μικρό' Θεώρημα του Fermat</u>

Έστω p πρώτος. Για κάθε ακέραιο α ισχύει ότι ο $\alpha^p - \alpha$ διαιρείται από τον p ή αλλιώς $a^p \equiv amodp$.

Ισοδύναμα, αν ο α δεν είναι πολλαπλάσιο του p τότε ο $\alpha^{p-1} - 1$ διαιρείται από τον p ή $\alpha^{p-1} \equiv 1modp$

Διατυπώθηκε από τον Fermat για πρώτη φορά σε ένα από τα γράμματά του στον Mersenne χωρίς, κατά τη προσφιλή του συνήθεια, να αναφέρει την απόδειξη. Σε αντίθεση βέβαια με το 'τελευταίο' ομώνυμο Θεώρημά του, οι μαθηματικοί δεν άργησαν να την βρουν. Ο Euler το 1736 έδωσε μία πρώτη απόδειξη, το 1747 έδωσε μία δεύτερη και το 1757 μία Τρίτη. Από τότε μέχρι σήμερα έχουν προταθεί πολλές διαφορετικές αποδείξεις. Παρουσιάζουμε μία που σχετίζεται με τον Euler.

Απόδειξη

Θα χρησιμοποιήσουμε την αρχή της Μαθηματικής Επαγωγής. Η πρόταση $a^p \equiv amodp$ είναι προφανώς αληθής για α=1. Θα υποθέσουμε ότι ισχύει για α και μετά θα δείξουμε ότι ισχύει για α+1.Έστω λοιπόν ότι ισχύει $a^p \equiv amodp$. Θα δείξουμε ότι ισχύει $(a+1)^p \equiv (a+1)modp$. Όμως:

$$(\alpha+1)^p = \alpha^p + \binom{p}{p-1}\alpha^{p-1} + \binom{p}{p-2}\alpha^{p-2} + \cdots \binom{p}{2}a^2 + \binom{p}{1}\alpha^1 + 1.$$

Από αυτούς τους όρους ο τελευταίος είναι ο 1 και ο πρώτος ο α^pπου είναι εξ υποθέσεως ισότιμος προς τον $amodp$ ενώ όλοι οι ενδιάμεσοι είναι της μορφής $\binom{p}{i}\alpha^i$ όπου i είναι ένας φυσικός ανάμεσα στον 1 και στον p-1. Για κάθε τιμή του i ο συντελεστής είναι πολλαπλάσιο του p, επειδή $\binom{p}{i} = \frac{p!}{i!(p-i)!}$.

Άρα όλοι οι ενδιάμεσοι όροι είναι ισότιμοι προς 0modp. Τελικά

$$(\alpha+1)^p \equiv (\alpha^p + 1) \equiv (\alpha+1)modp.$$

2.2.3. Οι αριθμοί Carmichael

Ορισμός

Ένας μονός σύνθετος αριθμός n λέγεται αριθμός **Carmichael** αν

$$a^{n-1}modn = 1 \; \forall \; a \in \; Z_n^* \; .$$

Παρατηρήσεις

- Ο μικρότερος αριθμός Carmichael είναι ο $561 = 3 \bullet 11 \bullet 17$.

- Το 1994 απεδείχθει ότι υπάρχουν αριθμοί Carmichael και μάλιστα ομοιόμορφα κατανεμημένοι. (Alford-Granville-Pomerance) .
- Ο Richard Pinch του πανεπιστημίου του Cambridge υπολόγισε τους 105.212 αριθμούς Carmichael τους μικρότερους από τον 10^{15} .

Θεώρημα (A.Korselt)

Ένας περιττός σύνθετος ακέραιος $n \geq 3$ είναι αριθμός Carmichael αν και μόνο αν είναι ελεύθερος τετραγώνου (δηλαδή δεν διαιρείται από το τετράγωνο ενός πρώτου) και κάθε πρώτος διαιρέτης p του n είναι τέτοιος ώστε να ισχύει $p-1|n-1$.

Απόδειξη

Ας υποθέσουμε ότι ο ν είναι αριθμός Carmichael και έστω p ένας πρώτος διαιρέτης του n. Έστω p^t η μεγαλύτερη δύναμη του p που διαιρεί τον n και g μια αρχική ρίζα $mod p^t$. Καθώς $\left(p^t, \frac{n}{p^t}\right) = 1$ υπάρχει ακέραιος b με

$$b = g mod p^t \text{ και } b = \frac{1 mod n}{p^t}.$$

Τότε $(b,p) = 1, \left(b, \frac{n}{p^t}\right) = 1$ και επομένως $(b,n) = 1.$ Καθώς ο n είναι αριθμός Carmichael και ο p^t διαιρέτης του θα ισχύει

$$b^{n-1} = 1 mod p^t .$$

Επίσης ο b είναι αρχική ρίζα $modp^t$. Άρα $\varphi(p^t)|n-1$ και επομένως $p^{t-1}(p-1)|n-1$. Συνεπώς έχουμε $t=1$ και $p-1|n-1$.

Αντιστρόφως, υποθέτουμε ότι ο n είναι ελεύθερος τετραγώνου και για κάθε πρώτο διαιρέτη p του n ισχύει $p-1|n-1$. Έστω a ακέραιος με $(a,n)=1$

Αν p πρώτος διαιρέτης του n, τότε

$$a^{p-1}=1modp$$

και καθώς $p-1|n-1$, έχουμε

$$a^{n-1}=1modp\ .$$

Τέλος, επειδή ο n είναι ελεύθερος τετραγώνου ισχύει

$$a^{n-1}=1modn\ .$$

Θεώρημα

Αν ο n είναι αριθμός Carmichael τότε ο n είναι γινόμενο τουλάχιστον τριών διαφορετικών παραγόντων.

Απόδειξη

Έστω n ένας αριθμός Carmichael, τότε ο n είναι σύνθετος.

Ας υποθέσουμε ότι $n = pq$, όπου p, q είναι πρώτοι με $p > q$.

Από το προηγούμενο θεώρημα έχουμε ότι $p - 1|n - 1$.

Καθώς $n - 1 = (p - 1)q + q - 1$, παίρνουμε ότι $p - 1|q - 1$ και επομένως $p \leq q$ που είναι άτοπο.

Άρα ο n έχει τουλάχιστον τρείς πρώτους παράγοντες.

Κατασκευή(J.chernick 1939)

Αν t ακέραιος τέτοιος ώστε $6t + 1$,$12t + 1$ και $18t + 1$ να είναι πρώτοι, τότε ο ακέραιος $n = (6t + 1)(12t + 1)(18t + 1)$ είναι αριθμός Carmichael.

2.2.4 Το κριτήριο Solovay -Strassen

Το 1977 περίπου οι Solovay και Strassen δημοσίευσαν έναν πιθανοτικό αλγόριθμο που στηρίζεται στο Κριτήριο του Euler. Συγκεκριμένα αν p μόνος πρώτος και $(a, p) = 1$ τότε $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} mod p$. Εάν a είναι τετραγωνικό υπόλοιπο $mod p$ θα ισχύει $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = 1 mod p$ και εάν a δεν είναι τετραγωνικό υπόλοιπο $mod p$ θα έχουμε $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = -1 mod p$. Άρα λοιπόν εάν p μονός πρώτος τότε $a^{\frac{p-1}{2}} \bullet \left(\frac{a}{p}\right) = 1 mod p$ για κάθε $a \in \{1,2, \dots, p - 1\}$. Καταλήγουμε λοιπόν στο ότι εάν $a^{\frac{n-1}{2}} \bullet \left(\frac{a}{n}\right) \neq 1 mod n$ τότε ο n δεν είναι πρώτος, για μονό $n \geq 3$ και $a \in \{2, \dots, n - 2\}$. Η πολυπλοκότητα της διαδικασίας είναι $O((log n)^3)$.

<u>Ορισμός</u> Έστω n μονός σύνθετος αριθμός. Ο a με $1 \leq a \leq n - 1$ λέγεται **Ε-μάρτυρας** του n εάν $a^{\frac{n-1}{2}} \bullet \left(\frac{a}{n}\right) \neq 1 mod n$.

Ορισμός Έστω n μονός σύνθετος αριθμός. Ο a με $1 \leq a \leq n-1$ λέγεται **Ε-ψεύτης** του n εάν $a^{\frac{n-1}{2}} \bullet \left(\frac{a}{n}\right) = 1 mod n.$

Παράδειγμα

Έστω $n = 325 = 13 \bullet 5^2$

- Για $a = 15$ έχουμε $(325,15) = 5$ άρα $\left(\frac{15}{325}\right) = 0.$ Ο 15 είναι Ε-μάρτυρας του 325.
- Για $a = 2,\ 2^{162} = 2^{2\bullet 81} = ((2^9)^9)^2 = (187^9)^2 = ((187^3)^3)^2 = (203^3)^2 = 252^2 = 129 mod 325.$

$$\left(\frac{2}{325}\right) = \left(\frac{2}{13 \bullet 5^2}\right) = \left(\frac{2}{13}\right)\left(\frac{2}{5^2}\right) = \left(\frac{2}{13}\right)\left(\frac{2}{5}\right)^2 = \left(\frac{2}{13}\right) = (-1)^{\frac{13^2-1}{8}} = -1.$$

Άρα ο 2 είναι Ε-μάρτυρας του 325.

- Για $a = 7, 7^{162} = 7^{2\bullet 81} = ((7^9)^9)^2 = (307^9)^2 = ((307^3)^3)^2 = (18^3)^2 = 307^2 = 324 = -1 mod 325.$

$$\left(\frac{7}{325}\right) = \left(\frac{7}{13\bullet 5^2}\right) = \left(\frac{7}{13}\right)\left(\frac{7}{5^2}\right) = \left(\frac{7}{13}\right)\left(\frac{7}{5}\right)^2 = \left(\frac{7}{13}\right) = -1\ .$$

Άρα ο 7 είναι Ε-ψεύτης για τον 325.

Λήμμα

Έστω ο μονός σύνθετος $n \geq 3$ τότε κάθε Ε-ψεύτης του n είναι επίσης και F-ψεύτης του n.

Απόδειξη

Αν α είναι Ε-ψευτης τότε $a^{\frac{n-1}{2}} \bullet \left(\frac{a}{n}\right) mod n = 1$ αλλά τότε $\left(\frac{a}{n}\right) = 1$ ή -1, οπότε τετραγωνίζοντας έχω $\left[a^{\frac{n-1}{2}} \bullet \left(\frac{a}{n}\right)\right]^2 mod n = 1 \Rightarrow a^{n-1} mod n = 1$. Άρα ο α είναι και F-ψεύτης.

2.3.Μηχανές και υπολογιστές

Στον 20ο αιώνα είχαμε μεγάλη πρόοδο στη θεωρία των πρώτων αριθμών. Πολύ μεγαλύτερη πρόοδο όμως είχαμε στην εύρεση καινούργιων πρώτων αριθμών αλλά και στις τεχνικές της συγκεκριμένης έρευνας. Είδαμε ότι από τον 18ο αιώνα ο Felkel είχε καταφύγει στη μηχανική υποστήριξη για τον χαρακτηρισμό αριθμών σε πρώτους ή σύνθετους. Αυτή η ιδέα άρχισε να εξελίσσεται αφού οι απαιτήσεις της εποχής πλέον ήταν μεγάλες. Κανείς δεν μπορούσε χωρίς μηχανική βοήθεια να κάνει τόσο ογκώδεις υπολογισμούς με τόσα πολλά ψηφία για να αποφασίσει αν ένας αριθμός είναι πρώτος ή όχι. Η πρόοδος σε αυτό το τομέα θα ερχόταν είτε από κάποιο σπουδαίο θεωρητικό αποτέλεσμα που θα περιόριζε τον έλεγχο ή από κάποια μηχανή που θα αναλάμβανε τον τεράστιο όγκο εργασίας. Ο συνδυαμός των δύο θα είχε σίγουρα θεαματικά αποτελέσματα.

Οι πρώτες ιδέες για υπολογιστικές μηχανές φαίνεται να ανήκουν στον Άγγλο Charles Babatz τον 19ο αιώνα. Ήδη από το 1823 είχε σχεδιάσει τη κατασκευή μίας μηχανής που θα υπολόγιζε λογάριθμους. Αργότερα εμπνεύστηκε μία άλλη που θα είχε πιο ευρύ φάσμα υπολογισμών αλλά ούτε και αυτή κατάφερε να κατασκευαστεί. Τις ιδέες αυτές αλλά και τις θεωρητικές του γνώσεις εμεταλλεύτηκε για να σχεδιάσει τη δικιά του μηχανή ο Alan Turing γύρω στο 1939. Ο Turing σκέφτηκε να αντιμετωπίσει τα τεράστια υπολογιστικά

προβλήματα που προκύπτουν από τη μελέτη της συνάρτησης ζ με μία μηχανή που θα αποτελούνταν από βίδες και γρανάζια. Δυστυχώς, είχαμε φτάσει στις παραμονές του $2^{ου}$ παγκοσμίου πολέμου. Όλες οι σχετικές επιστημονικές δραστηριότητες έπρεπε να ανασταλούν. Και ενώ πολλοί επιστήμονες μετανάστευσαν από την Ευρώπη στην Αμερική όπου βρήκαν άνεση και στήριξη σχετικά με την ερευνά τους, ο Turing έμεινε στην Αγγλία και έθεσε τον εαυτό του στην υπηρεσία της κατασκοπίας. Μετά τον πόλεμο, πάντως η μηχανή του λειτούργησε και υπολόγισε πάνω από 1000 ρίζες της συνάρτησης ζ επεκτείνοντας έστω και για λίγο τον μέχρι τότε κατάλογο με τις γνωστές ρίζες. Παρόλα αυτά,η μηχανή του δεν απέδωσε περισσότερα. Ο ίδιος ο Turing πέθανε λίγο αργότερα.

Τη σκυτάλη πήραν οι Αμερικανοί Derrick Norman Lehmer και ο γιός του Derrick Henry Lehmer που κατασκεύασαν μία μηχανή που υπολόγισε πάνω από 25.000 ρίζες της συνάρτησης ζ του Riemann. Παράλληλα κατεύθυνε τις πιο σύγχρονες πλέον, υπολογιστικές μηχανές του και στην εύρεση πρώτων. Και αφού τύπος που να δίνει τους πρώτους δεν ανακαλύφθηκε ποτέ, έπρεπε η μηχανή του απλά να κάνει δοκιμές. Στα τέλη του $2^{ου}$ παγκοσμίου πολέμου ο μεγαλύτερος γνωστός πρώτος ήταν ο $2^{127} - 1$ με το ρεκόρ να κρατάει από το 1876. Ο αριθμός αυτός είχε 39 ψηφία. Οποιος θα προσπαθούσε να σπάσει το ρεκόρ έπρεπε η μηχανή του να ελέγξει πολύ μεγάλους αριθμούς που φυσικά σημαίνει πάρα πολλούς υπολογισμούς. Οι υπολογισμοί γίνονται σαφώς πιο εύκολα από μία μηχανή, αλλά αν ο όγκος είναι τεράστιος,τότε ούτε αυτή θα έχει γρήγορα αποτελέσματα. Έπρεπε οι δοκιμές να περιοριστούν. Ο Lehmer που είχε συνειδητοποιήσει σχετικά γρήγορα τα παραπάνω, στράφηκε πρώτα στα αποτελέσματα της Θεωρίας Αριθμών πριν στρέψει τις μηχανές του σε τυφλή αναζήτηση. Ο Γάλλος μαθηματικός Edouard Lucas είχε επινόησει μία μέθοδο που απλοποιεί το πρόβλημα της απόφασης του αν ένας αριθμός της μορφής $2^n - 1$ είναι πρώτος. Το τεστ χρησιμοποιήθηκε για να αποκαλυφθεί ότι ο $2^{127} - 1$ είναι πρώτος. Ο επόμενος πιθανός πρώτος από την εικασία του Mersenne ήταν ο $2^{257} - 1$. Ο Lucas δεν κατάφερε να απαντήσει. Η μέθοδος του περιόριζε κατά πολύ τις αναγκαίες δοκιμές αλλά οι εμπλεκόμενοι αριθμοί είχαν πάρα πολλά ψηφία και ο όγκος των υπολογισμών ήταν τεράστιος ακόμα και για τις περιορισμένες δοκιμές. Χρειαζόταν μία βελτίωση. Αυτή ήρθε το 1930 από τον D.H.Lehmer κι έτσι το διάσημο τέστ που προέκυψε πήρε το όνομα Lucas-Lehmer.

Τέστ Lucas – Lehmer

Έστω p ένας πρώτος αριθμός και $M_p = 2^p - 1$ ο p-οστός πρώτος του Mersenne. Ορίζουμε αναδρομικά μία ακολουθία ακεραίων θέτοντας $r_1 = 4$ και για k φυσικό με k≥ 2 ως εξής:

$$r_k = (r_{k-1}^2 - 2) mod M_{p,0} \leq r_k \leq M_p$$

Τότε ο M_p είναι πρώτος αν και μόνο αν $r_{p-1} = 0 mod M_p$

Ας θεωρήσουμε για παράδειγμα τον $M_5 = 2^5 - 1$=31.Τότε $r_1 = 4$.

$$r_2 = (r_1^2 - 2) mod M_5 = (4^2 - 2) mod 31 = 14 mod 31$$

$$r_3 = (r_2^2 - 2) mod M_5 = (14^2 - 2) mod 31 = 194 mod 31 = 8 mod 31$$

$r_4 = (r_3^2 - 2) mod M_5 = (8^2 - 2) mod 31 = 62 mod 31 = 0 mod 31$ άρα ο M_5 είναι πρώτος.

ΚΕΦΑΛΑΙΟ 3ο

3.1. Εικασία του Goldbach

Ο Christian Goldbach (1690-1764) ,ήταν ένας ερασιτέχνης Γερμανός μαθηματικός ο οποίος ζούσε στη Μόσχα και εργαζόταν στο Υπουργείο Εξωτερικών.Αλληλογραφούσε με τον Leonard Euler, ο οποίος την περίοδο εκείνη ήταν μέλος της Ακαδημίας Επιστημών στην Αγία Πετρούπολη.Την 7η Ιουνίου του 1742 έστειλε επιστολή στον Euler στην οποία του εμπιστεύθηκε την εικασία του ότι

«Κάθε ακέραιος μεγαλύτερος του 2 γράφεται ως άθροισμα τριών πρώτων αριθμών»

Ο Goldbach θεωρούσε και το 1 πρώτο αριθμό. Σήμερα η εικασία του Goldbach θα έπρεπε να διατυπωθεί ως εξής :

«Κάθε φυσικός αριθμός μεγαλύτερος του 5 γράφεται ως άθροισμα τρίων πρώτων»

Ο Euler έδειξε ενδιαφέρον για το πρόβλημα και απάντησε στον Goldbach ότι το πρόβλημα ήταν ισοδύναμο με την εικασία ότι, «κάθε άρτιος μεγαλύτερος του γράφεται ως άθροισμα δύο πρώτων». Η τελευταία εικασία λέγεται ισχυρή εικασία του Goldbach.

Η εικασία, ότι όλοι οι περιττοί ακέραιοι οι μεγαλύτεροι του 9 γράφονται ως άθροισμα τριών περιττών πρώτων, ονομάζεται ασθενής εικασία του Goldbach.

Στην συνέχεια θα εξετάσουμε υποσύνολα του συνόλου των φυσικών αριθμών $\mathbb{N}$ και θα ελέγξουμε το πλήθος των πρώτων που υπάρχουν σε αυτά.

Κάθε ακέραιος α γράφεται σε μία από τις μορφές :

$$4l, 4l+1, 4l+2, 4l+3 | l \in \mathbb{Z}.$$

Δεν υπάρχει πρώτος αριθμός της μορφής $4l$, αφού όλοι διαιρούνται με 4. Ο 2 είναι ο μόνος πρώτος της μορφής $4l+2$ (για $l=0$), αφού όλοι είναι άρτιοι.

Υπάρχουν πρώτοι αριθμοί της μορφής

$$4l+1, \text{π.χ. } 5,13,17,\ldots$$

Επίσης υπάρχουν πρώτοι αριθμοί της μορφής $4l+3$, π.χ. 3,7,11,19,…

Το ερώτημα είναι πόσοι πρώτοι υπάρχουν σε κάθε κλάση.

Πρόταση

Υπάρχουν άπειροι πρώτοι αριθμοί της μορφής $4l+3$

Απόδειξη

Θα υποθέσουμε ότι υπάρχουν πεπερασμένου πλήθους πρώτοι αριθμοί της μορφής $4l+3$ και θα καταλήξουμε σε άτοπο.

Έστω λοιπόν ότι όλοι οι πρώτοι της μορφής $4l+3$ είναι οι $q_1, q_2, \dots, q_5$. Ο φυσικός αριθμός $N: 4q_1q_2 \dots q_5 - 1 > 0$ έχει έναν τουλάχιστον πρώτο διαιρέτη της μορφής $4l+3$.(Αν όλοι οι πρώτοι διαιρέτες ήταν της μορφής $4l+1$, τότε και το γινόμενό τους θα ήταν της ίδιας μορφής,δηλαδή και ο *N).*

Πρόταση

Υπάρχουν άπειροι πρώτοι της μορφής $4l+1$

Θεώρημα (Θεώρημα του Dirichlet για αριθμητικές προόδους)

Υπάρχουν άπειροι πρώτοι της μορφής $ml+a$ όπου $l \in \mathbb{Z}$.

Το θεώρημα αποδείχτηκε το 1837 από τον L.J.Dirichlet.Η ειδική περίπτωση για $\alpha = 1$ διατυπώθηκε ως εικασία το 1775 από τον Euler.Ο Legendre διατύπωσε την εικασία γενικά,για κάθε α,το 1785.Προσπάθησε να το αποδείξει αλλά χωρίς πλήρη επιτυχία.

Παράδειγμα

Σύμφωνα με το Θεώρημα το σύνολο $A \coloneqq \{77,177,277, \dots\}$
περιέχει άπειρο πλήθος πρώτων.

Παρατήρηση

Κάθε κλάση ακέραιων της μορφής $ml+a$ όπου $l \in \mathbb{Z}$,περιέχει και άπειρο πλήθος σύνθετων ακέραιων.

Πράγματι, αν $a + m \bullet lo = p \in P$ για κάποιο ακέραιο $l_0 \in \mathbb{Z}$, θεωρούμε την ακολουθία

$$l_k = l_0 + k \bullet p \text{ όπου } k = 1,2,3, \dots$$

Για κάθε $k \geq 1$ ισχύει

$$m \bullet l_k + a = m(l_0 + k \bullet p) + a =$$
$$= (mlo + a) + p(km) =$$
$$= p(km + 1).$$

δηλαδή οι $m \bullet l_k + a | k = 1,2, \dots$ είναι σύνθετοι. Αυτό σημαίνει ότι δεν υπάρχει αριθμητική πρόοδος της οποίας όλοι οι όροι να είναι πρώτοι αριθμοί.

3.2. Δίδυμοι πρώτοι αριθμοί

Ορισμός

Δυο διαδοχικοί περιττοί αριθμοί οι οποίοι είναι πρώτοι, θα λέγονται δίδυμοι.

Το ερώτημα είναι πόσα ζευγάρια δίδυμων υπάρχουν.

Η εικασία των διδύμων πρώτων είναι ότι υπάρχουν άπειροι πρώτοι αριθμοί p τέτοιοι ώστε και ο $p + 2$ να είναι πρώτος. Η εικασία είναι ανοιχτή μέχρι σήμερα.

Σταχυολογούμε μερικά σχετικά αποτελέσματα.Είναι γνωστό σε όλους ότι η σειρα

$$\sum_{n=1}^{\infty} \frac{1}{n} \text{ αποκλίνει.}$$

Στα 1737 απέδειξε ο Euler κάτι πολύ ισχυρότερο, ότι και η σειρά

$$\sum_{p \in P} \frac{1}{p} \text{ επίσης αποκλίνει.}$$

Το αποτέλεσμα του Euler αποτελεί μια ακόμη απόδειξη ότι υπάρχουν άπειροι πρώτοι αριθμοί (Αν ήταν πεπερασμένοι, η σειρά θα συνέκλινε!).

Στα 1849 ο A.Prince de Polignac διατύπωσε την εικασία ότι για κάθε άρτιο φυσικό n υπάρχουν άπειροι πρώτοι αριθμοί p τέτοιοι, ώστε και ο $p+n$ να είναι πρώτος.Η εικασία του Polignac για $n=2$ είναη η εικασία των διδύμων πρώτων.

Στα 1919 ο Viggo Brun απέδειξε ότι, όταν το p διατρέχει όλους τους δίδυμους πρώτους, τότε η σειρά

$$\sum_{p,δίδυμος\ πρώτος} \frac{1}{p}$$ συγκλίνει.

Αυτό βέβαια σημαίνει ότι υπάρχουν «πολύ λιγότεροι» δίδυμοι πρώτοι από ότι πρώτοι αριθμοί.Δεν μπορούμε να συμπεράνουμε ότι το πλήθος τους είναι πεπερασμένο!

Ο P.Clement μας έδωσε στα 1949, ένα κριτήριο ελέγχου των διδύμων πρώτων.

Το ζευγάρι $(n, n+2)$ είναι ζευγάρι διδύμων πρώτων, τότε και μόνο τότε, όταν ο $n+2$ διαιρεί τον

$$\big[4\big((n-1)!+1\big)+n\big].$$

Διάσημοι μαθηματικοί, όπως οι Hardy και Wright ήταν πεπεισμένοι για την ύπαρξη άπειρου πλήθους διδύμων πρώτων. Σημείωναν όμως με έμφαση «is at present beyond the resources of mathematics».Κατά τον Daniel Shanks ‘’the evidence is overwhelming’’.

3.3. Carl Friedrich Gauss

Ο Gauss γεννήθηκε το 1777 στο Μπράουνσβαϊγκ της Γερμανίας. Χαρακτηρίστκε από μικρός ως παιδί θαύμα. Σπούδασε στο Gottingen όπου και διορίστηκε διευθυντής του τοπικού αστεροσκοπείου, μία θέση που κράτησε ως το θάνατό του το 1855. Θεωρείται από τους μεγαλύτερους μαθηματικούς όλων των εποχών. Ασχολήθηκε με πολλούς τομείς των Μαθηματικων και της Φυσικής διαμορφώνοντας ριζικά αρκετους από αυτούς.

Την εποχή του Gauss οι λογάριθμοι ήταν ένα πολύ χρήσιμο υπολογιστικό εργαλείο. Τραπεζίτες, έμποροι, θαλασσοπόροι και όχι μόνο τους χρησιμοποιούσαν για να μετατρέψουν τους δύσκολους πολλαπλασιασμούς σε προσθέσεις με βάση τον κανόνα $\log_b(x+y) = \log_b x + \log_b y$ και τη βοήθεια εκτενών πινάκων που επέτρεπαν, έστω και

προσεγγιστικά, να βρεί κάποιος το λογάριθμο ενός αριθμού και αντίστροφα να βρει τον αριθμό αν γνωρίζει τον λογάριθμό του. Ένα καθαρα τεχνικό τέτοιο βιβλίο γεμάτο με λογαριθμικούς πίνακες έπεσε στα χέρια του δεκαπεντάχρονου Gauss. Τα στοιχεία των πινάκων αυτών ήταν τελείως προβλέψιμα σε αντίθεση με αυτά των πινάκων πρώτων που φαίνονταν τελείως τυχαία. Για την ακρίβεια φαίνονταν σε όλους τελείως τυχαία εκτός από εκείνον. Το κρίσιμο βήμα στην ανακάλυψή του ήταν ότι έθεσε ένα τελείως διαφορετικό ερώτημα σχετικά με την εμφάνιση των πρώτων. Δεν προσπάθησε να προβλέψει σε ποια θέση θα εμφανιστεί ο επόμενος πρώτος αλλά εξέτασε αν υπήρχε τρόπος να προβλέψει πόσοι πρώτοι υπάρχουν μικρότεροι από ένα δεδομένο αριθμό. Γενικότερα αν θεωρήσουμε ένα φυσικό αριθμό Ν, αναρωτήθηκε αν υπάρχει τρόπος να εκτιμλήσουμε πόσοι πρώτοι υπάρχουν μεταξύ των 1 και Ν. Να σημειώσουμε ότι την εποχή εκείνη κατασκευάζοταν τεράστιοι πίνακες με πρώτους αριθμούς που δεν παρουσίαζαν μεγάλο ενδιαφέρον, όχι μόνο γιατι συχνά περιείχαν λάθη αλλά γιατί η χρησιμότητά τους ήταν περιορισμένη. Το ταλέντο και η μεγάλη του αγάπη για τους αριθμούς ήταν αυτά που τον οδήγησαν στην παρατήρηση ότι η κατανομή των πρώτων μπορεί να ακολουθεί κάποιους περιορισμούς. Παρατήρησε, λοιπόν, ότι στους πρώτους δέκα φυσικούς υπάρχουν 4 πρώτοι, στους πρώτους εκατό υπάρχουν 25 πρώτοι, στους πρώτους χίλιους 168 και στους πρώτους δέκα χιλιάδες 1229. Έτσι, η μέση απόσταση ανάμεσα σε δύο πρώτους αριθμούς στη πρώτη δεκάδα ηταν 2,5 στη πρώτη εκατοντάδα ήταν 4 και όπως φαίνεται στον παρακάτω πίνακα η μέση απόσταση ανάμεσα σε δύο πρώτους αυξάνεται προοδευτικά κατά έναν συντελεστή περίπου ίσο με 2,3 για τις διάφορες δυνάμεις του 10.

Πίνακας 1

N	Πλήθος πρώτων από το 1 ως το N	Μέση απόσταση ανάμεσα σε δύο πρώτους
10	4	2,5
100	25	4
1000	168	6
10000	1229	8,1
100000	8592	10,4
1000000	78498	12,7
10000000	664579	15

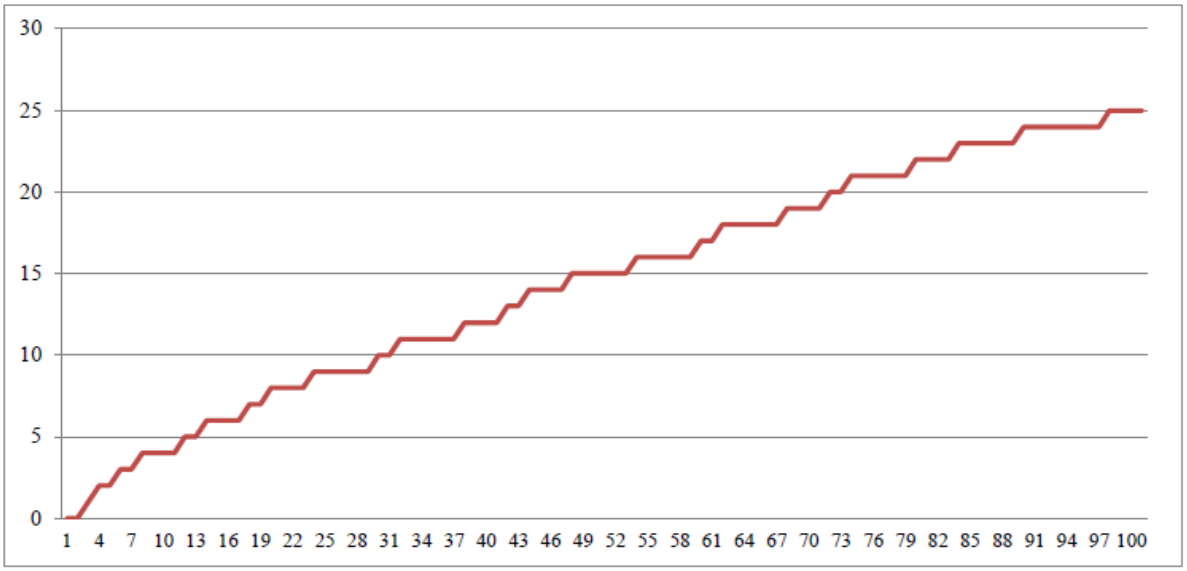
Ο Gauss υπέθεσε ότι ο αριθμός αυτός είναι ο $ln10$ δίνοντας μία αισθητικά τέλεια μορφή στην εικασία του. Αν συμβολίσουμε με $\pi(N)$ το πλήθος των πρώτων αριθμών από το 1 εως το N τότε

$$\pi(N) \sim \frac{N}{lnN}$$

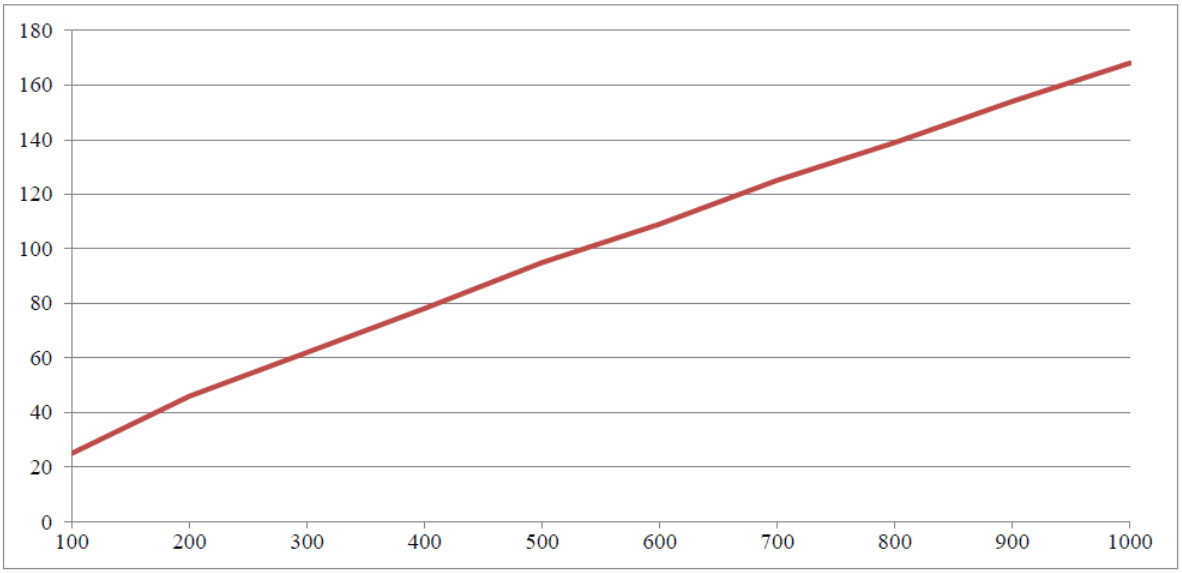
Το σύμβολο $\sim$ δηλώνει ότι η συνάρτηση $\pi(N)$ είναι προσεγγιστικά ίση με $\frac{N}{lnN}$. Η προσέγγιση αυτή φαινόταν πολύ καλή εκείνη την εποχή ειδικά αφού το δείγμα των γνωστών πρώτων δεν ήταν και ιδιαίτερα μεγάλο. Ο ίδιος δεν ισχυρίστηκε ότι ανακάλυψε τον τύπο που έδινε το πλήθος των πρώτων αριθμών αλλά μία καλή προσέγγιση. Η εικασία αυτή είναι γνωστή πλέον ως 'Θεώρημα των Πρώτων Αριθμών.' Και μόνο το όνομά του είναι αντιπροσωπευτικό του πόσο σημαντικό είναι σε αυτό το κλάδο των Μαθηματικών. Το Θεώρημα αυτό, ακόμα και σήμερα, φαίνεται απρόβλεπτο αφού συσχετίζει δύο φαινομενικά ασύνδετες έννοιες των Μαθηματικών, τους πρώτους αριθμούς και τους λογάριθμους. Η ανακάλυψη ότι η αύξηση του πλήθους των πρώτων σε σχέση με το πλήθος των φυσικών μοιάζει να είναι τόσο ομαλή αν και εκείνοι εμφανίζονται τόσο τυχαία συγκαταλέγεται στα θαύματα των Μαθηματικών και αποτελεί ένα από τα πιο κρίσιμα σημεία στην ιστορία της θεωρίας των πρώτων. Η ομαλότητα αυτή φαίνεται στα παρακάτω

διαγράμματα. Για τους πρώτους 100 φυσικούς στο πρώτο, για τους πρώτους 1.000 στο δεύτερο και για τους πρώτους 10.000 στο τρίτο.

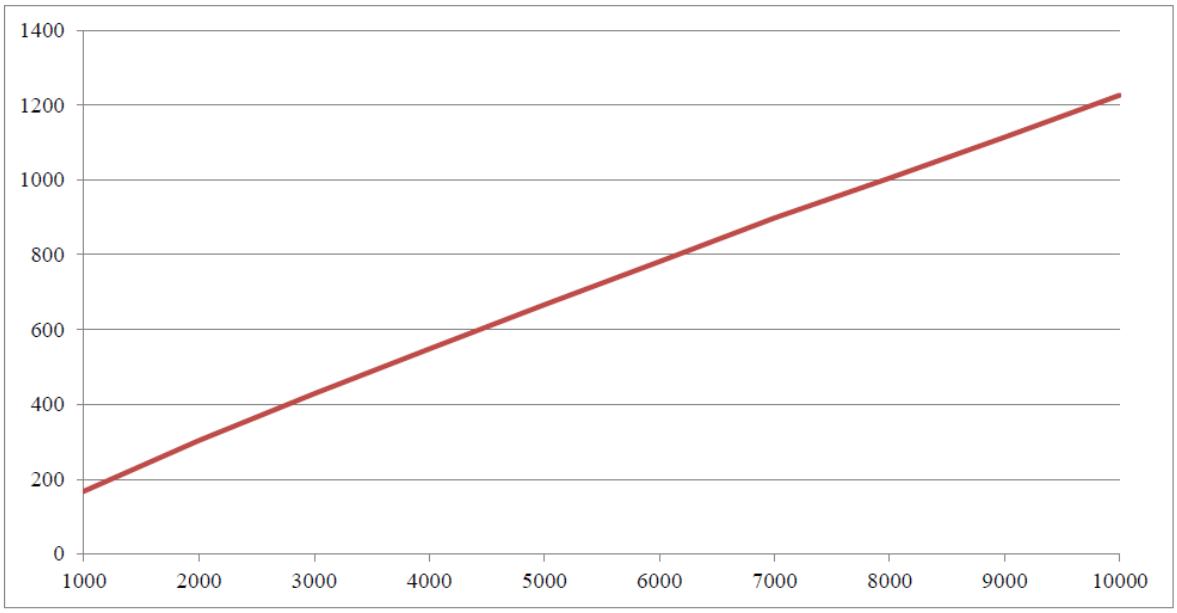
Διάγραμμα αθροιστικής συχνότητας πρώτων στους φυσικούς 1-100



Διάγραμμα αθροιστικής συχνότητας πρώτων στους φυσικούς 1-1.000



Διάγραμμα αθροιστικής συχνότητας πρώτων στους φυσικούς 1-10.000



Ο Gauss δεν ενημέρωσε κανέναν γι αυτή του την ανακάλυψη για λόγους που ακόμαι και σήμερα αποτελούν μυστήριο. Βέβαια, δεν είχει βρεί παρά μόνο ενδείξεις για την ισχύ των παρατηρήσεών του, δεν είχει απόδειξη για τους ισχυρισμούς του ούτε κάποια εξήγηση γιατί συνέβαινε αυτό. Αποδείξεις όμως, δεν είχαν και πολλοί συναδελφοί του που, αντίθετα από εκείνον, δημοσιοποιούσαν αβίαστα τις παρατηρήσεις τους και οδηγούσαν σε συλλογικές θεωρήσεις των ιδεών τους. Ο Gauss δεν λειτούργησε έτσι μόνο σε αυτή την περίπτωση. Γενικά κοινοποιούσε μόνο αποδεδειγμένα αποτελέσματα γεγονός που, κατά πολλούς, έπαιξε σημαντικό ρόλο στην ιστορία των Μαθηματικών. Η προσωπική του σφραγίδα ήταν διακοσμημένη με το ρητό ‘Pauca Sed Matura’(λίγα αλλά ώριμα) και παρίστανε ένα δέντρο με ελάχιστους καρπούς στα κλαδιά του, αντιπροσωπεύοντας απόλυτα τη φιλοσοφία του σχετικά με τη παραγωγή των Μαθηματικών. Αν κάποιο αποτέλεσμα δεν έφτανε στο επίπεδο ωριμότητας που εκείνος θεωρούσε ικανό προς δημοσίευση, αρκούνταν σε μία σημείωση στο περίφημο Notizenjournal (ημερολόγιο σημειώσεων), ένα προσωπικό ημερολόγιο με τις μαθηματικές του ανακαλύψεις. Πολλές φορές μάλιστα, ακόμα και αυτές οι σημειώσεις ήταν κωδικοποιημένες, γεγονός που δυσκολεύει ακόμα και σήμερα την ερμηνεία κάποιων από τα μαθηματικά του αποτελέσματα.

Το 1798, έξι χρόνια μετά την μυστική ανακάλυψη του Gauss, ο Adrian Marie Legendre ανακοινώνει τη πειραματική ανακάλυψη της σχέσης ανάμεσα στους πρώτους και τους λογάριθμους. Η διχογνωμία σχετικά με την πατρότητα της πρώτης ανακάλυψης της σχέσης μεταξύ πρώτων και λογάριθμων οδήγησε σε μία οξύτατη αντιπαράθεση. Ο Legendre πάντως ήταν αυτός που δημοσίευσε πρώτος τις παρατηρήσεις του το 1808 στο 'Theories des Nombres'.

Σύμφωνα με τον Legendre έχουμε

$$\pi(N) \sim \frac{N}{lnN - 1{,}08366}$$

Ο τύπος του Legendre φαινόταν ότι έδινε καλύτερη προσέγγιση του πλήθους των πρώτων.Θα λέγαμε ότι είναι μία ελαφρώς τροποποιημένη εκδοχή του τύπου του Gauss που ταίριαζε καλύτερα στα ευρήματα της εποχής σχετικά με τους πρώτους αριθμούς. Σε μία επιστολή του προς τον Johan Encke που έχει ημερομηνία 24 Δεκεμβρίου 1849, υπάρχουν όλες οι ενδείξεις ότι η σχετική ανακάλυψη του Gauss είχε προηγηθεί χρονικά του Legendre. Σε αυτή την επιστολή, ο Gauss εξετάζει κριτικά τον αριθμό 1,08366 του Legendre για τον οποίο γράφει ότι πράγματι προσδίδει μεγαλύτερη ακρίβεια στη δική του προσέγγιση για το πλήθος των πρώτων για σχετικά μικρές τιμές του N. Εντούτοις, εκφράζει το φόβο ότι πιθανώς να μη συμβαίνει το ίδιο για μεγαλύτερες τιμές. Θα πρέπει να αναφέρουμε ότι ο Gauss δεν εμπιστευόταν τα έτοιμα αποτελέσματα που έδιναν οι τότε γνωστοί πίνακες πρώτων αλλά έφτιαχνε τους δικούς του. Στην ίδια επιστολή αναφέρει ότι συχνά αφιέρνωνε ένα τέταρτο της ώρας για να βρεί τους πρώτους σε μία χιλιάδα αριθμών ενώ δίνει και διορθώσεις στους πίνακες του Lambert.

Με την πάροδο των χρόνων κατασκευάστηκαν καλύτεροι πίνακες πρώτων οπότε οι τύποι των Gauss και Legendre μπορούσαν να συναγωνιστούν σε μεγαλύτερο δείγμα πρώτων. Ο τύπος του Gauss κέρδισε. Ο αντιαισθητικός αριθμός $1{,}08366$ του Legendre καταρρίφθηκε. Ήταν βαλμένος για να διορθώνει το σφάλμα στην εκτίμηση του Gauss για μικρά σχετικά N αλλά έκανε τα πράγματα πολύ χειρότερα στη συνέχεια σε μεγαλύτερα N. Η θεωρητική

ανάλυση αλλά και η διαίσθηση του Gauss είχε νικήσει την προσπάθεια του Legendre να τροποποιήσει τον τύπο ώστε να ταιριάζει στα διαθέσιμα στοιχεία. Ο Gauss όμως δεν σταμάτησε εκεί. Βασιζόμενος σε νέες παρατηρήσεις όρισε μία καινούργια συνάρτηση που αν και στερείται της εξαιρετικής απλότητας της πρώτης του προσπάθειας, είναι ακριβέστερη. Η νέα αυτή συνάρτηση ονομάστηκε λογαριθμικό ολοκλήρωμα του x:

$$Li(x) = \int_0^x \frac{1}{lnt}\,dt$$

Το πόσο εμπνευσμένη ήταν και αυτή η εκτιμησή του φαίνεται στον παρακάτω πίνακα.

Πίνακας 2

N	π(N)	N/lnN-π(N)	Li(N)-π(N)
100	25	3	5
1000	168	23	10
10.000	1229	140	17
100.000	9592	1.036	38
1.000.000	78498	6.034	130
10.000.000	664.579	43.461	339
100.000.000	5.761.455	−332.774	754
1.000.000.000	50.847.534	−2.592.592	1.701
10.000.000.000	455.052.511	−20.758.030	3.104
100.000.000.000	4.118.054.813	−169.923.160	11.588
1.000.000.000.000	37.607.912.018	−1.416.706.193	38.263

Το μόνο που έμενε πλέον ήταν να δοθεί μία απόδειξη για την εικασία αυτή ώστε να μπορέσει να βαφτιστεί Θεώρημα. Αυτό όμως θα γινόταν αρκετά χρόνια αργότερα.

3.4 Bernhard Riemann

Ο Bernhard Riemann γεννήθηκε στο Αννόβερο το 1826. Αρχικά βιοποριστικοί λόγοι τον οδήγησαν να επιλέξει θεολογικές σπουδές. Τελικά όμως, επικράτησε το πάθος του για τα Μαθηματικά. Σπούδασε στο Βερολίνο και το Gottingen όπου δίδασκε ο Gauss. Η προσφορά του στην Ανάλυση, στη Διαφορική Γεωμετρία, στη Θεωρία Αριθμών ακόμα και

στην μεταγενέστερη Θεωρία της Σχετικότητας θεωρείται κομβική. Πέθανε από φυματίωση σε ηλικία 39 χρονών στην Ιταλία.

Το 1859 ο Riemann διορίστηκε αντεπιστέλλον μέλος της ακαδημίας του Βερολίνου που ήταν μία πολύ μεγάλη τιμή για έναν μαθηματικό. Κάθε τέτοιος διορισμός συνοδεύοταν από μία πρωτότυπη εργασία του νέου μέλους. Ο Riemann υπέβαλε μία εργασία του με τίτλο 'Der die Anzahl der Primzahlen unter einer gegebenen Grosse' (' Σχετικά με το πλήθος των αριθμών που είναι μικρότεροι από κάποιον δεδομένο αριθμό.'). Η εργασία αυτή ήταν το επόμενο μεγάλο βήμα στην κατανόηση της κατανομής των πρώτων αριθμών. Παραδόξως ήταν η μοναδική του εργασία στη Θεωρία Αριθμών. Κομβικό ρόλο στη μελέτη του Riemann έπαιξε η συνάρτηση ζ. Η συνάρτηση αυτή ορίζεται ως εξής

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

ή συνεπτυγμένα

$$\zeta(s) = \sum_n n^{-s}$$

όπου $n \in \mathbb{N}$ και $s \in C$. Ο ρόλος του s στη θέση της ανεξάρτητης μεταβλητής καθώς και η ονομασία της συνάρτησης ως ζ είναι μία επιλογή του ίδιου και έχει υιοθετηθεί από όλους τους μεταγενέστερους μαθηματικούς.

Γεγονός είναι, πάντως, ότι ο Riemann δεν ήταν ο πρώτος που ασχολήθηκε με αθροίσματα αυτού του είδους. Το 'Πρόβλημα της Βασιλείας' πήρε το όνομά του από τη πόλη στην οποία διατέλεση καθηγητής Μαθηματικών ο Jacob Bernoulli (1654-1705). Αν και δεν διατυπώθηκε αρχικά από εκείνον ήταν αυτός που το διέδωσε σε ευρύ ακρωατήριο

Το πρόβλημα της Βασιλείας

Να υπολογιστεί το άθροισμα

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + ..$$

Λίγη ώρα επεξεργασίας του αθροίσματος είναι αρκετή για να υποθέσει κανείς ότι η σειρά συγκλίνει και μαλιστά σε έναν αριθμό περίπου ίσο με 1,645 αλλά ποιον; Το πρόβλημα τελικά προσεγγίστηκε από τον Euler το 1735, περίπου 45 χρόνια μετά τη διατύπωσή του.

Η συλλογιστική του ήταν η εξής

$$\eta\mu x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + ..$$

διαιρώντας με το x έχουμε

$$\eta\mu x = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \cdots$$

Όπου φυσικά $\eta\mu x = 0$ αν $x = \pm\pi, \pm 2\pi, \pm 3\pi, \ldots$. Ο Euler υπέθεσε ότι μπορεί να εκφράσει ένα άπειρο άθροισμα σαν γινόμενο παραγόντων που ορίζονται από τις λύσεις του όπως ακριβώς κάνουμε για τα πεπερασμένα πολυώνυμα.

$$1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \cdots = \left(1 - \frac{x}{\pi}\right)\left(1 + \frac{x}{\pi}\right)\left(1 - \frac{x}{2\pi}\right)\left(1 + \frac{x}{2\pi}\right)\left(1 - \frac{x}{3\pi}\right)\left(1 + \frac{x}{3\pi}\right)\ldots$$

Ισοδύναμα μπορούμε να γράψουμε

$$1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \cdots = \left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{4\pi^2}\right)\left(1 - \frac{x^2}{9\pi^2}\right)\ldots$$

Αν τώρα πολλαπλασιάσουμε όλους τους όρους στο δεύτερο μέλος θα παρατηρήσουμε ότι ο συντελεστής του x^2 είναι ο $-\left(\frac{1}{\pi^2} + \frac{1}{\pi^4} + \frac{1}{\pi^6} + \cdots\right) = -\frac{1}{\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2}$. Στην αρχική μορφή όμως ο συντελεστής του x^2 είναι ο $\frac{1}{3!} = -\frac{1}{6}$ άρα έχουμε $-\frac{1}{\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2} = -\frac{1}{6}$ ή αλλιώς $\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$.

Η απάντηση λοιπόν είναι $\frac{\pi^2}{6}$. Η απάντηση αυτή ειδικά εκείνη την εποχή ήταν τελείως απρόσμενη. Δε φαινόταν πως σχετίζεται ο αριθμός π, ο λόγος περιφέρεις προς διάμετρο κύκλου, με ένα άπειρο άθροισμα. Το αποτέλεσμα όμως ήταν ακριβές και η μέθοδος που εφάρμοσε ο Euler για να το λύσει ήταν αρκετά γενική έτσι ώστε κατάφερε να υπολογίσει και άλλα αθροίσματα αυτής της μορφής όπως για παράδειγμα $1+\frac{1}{2^4}+\frac{1}{3^4}+\frac{1}{4^4}+\frac{1}{5^4}+..$ με την απάντηση να είναι $\frac{\pi^4}{90}$ ή $1+\frac{1}{2^6}+\frac{1}{3^6}+\frac{1}{4^6}+\frac{1}{5^6}+..$ που είναι ίσο με $\frac{\pi^6}{945}$. Για την ακρίβεια η μέθοδος αυτή μπορεί να δώσει την απάντηση για κάθε σειρά της μορφής $1+\frac{1}{2^\nu}+\frac{1}{3^\nu}+\frac{1}{4^\nu}+\frac{1}{5^\nu}+..$ όπου ν άρτιος. Δυστυχώς δεν υπάρχει καμία γνωστή μέθοδος για ν περιττό μεγαλύτερο του 1. (Για ν=1 το άθροισμα είναι η αρμονική σειρά που αποκλίνει). Ο ίδιος ο Euler υπολόγισε μέχρι και για $\nu = 26$.

Είναι σαφές ότι στο πρόβλημα της Βασιλείας ζητείται η τιμή της συνάρτησης ζ για $s=2$ και έτσι έχουμε $\zeta(2)=\frac{\pi^2}{6}$. Με βάση τη συνάρτηση ζ ο Riemann διατύπωσε ίσως τη πιο διασήμη εικασία όλων των εποχών μετά από το 'τελευταίο' Θεώρημα του Fermat, υστερώντας μόνο σε απλότητα διατύπωσης. Η 'υπόθεση Riemann', όπως έχει καθιερωθεί, είναι σαφώς πιο σημαντική και αν αποδειχθεί θα έχει τεράστιες συνέπειες στη Θεωρία Αριθμών. Σύμφωνα με την υπόθεση Riemann, οι μη τετριμμένες ρίζες της μιγαδικής συνάρτησης ζ έχουν πραγματικό μέρος ίσο με $\frac{1}{2}$. Μετά και την απόδειξη του 'τελευταίου' Θεωρήματος του Fermat το 1994, μπορούμε να πούμε με σιγουριά ότι αυτό είναι το ιερό δισκοπότηρο των Μαθηματικών.

Ας δούμε όμως πως σχετίζεται η συνάρτηση ζ του Riemann με τους πρώτους. Έχουμε

$$\zeta(s)=1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\frac{1}{6^s}+\cdots$$

αν πολλαπλασιάσουμε και τα δύο μέλη με $\frac{1}{2^s}$ θα έχουμε

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} + \cdots$$

αφαιρώντας τώρα κατά μέλη

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \cdots$$

Αν πολλαπλασιάσουμε τώρα με $\frac{1}{3^s}$ και αφαιρέσουμε από την παραπάνω σχέση παίρνουμε

$$\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \frac{1}{17^s} + \cdots$$

Συνεχίζοντας πολλαπλασιάζουμε με $\frac{1}{5^s}$ και αφαιρούμε από τη παραπάνω σχέση, μετά με $\frac{1}{7^s}$ κοκ.

Στο πρώτο βήμα απαλείψαμε όλα τα κλάσματα που είχαν για παρανομαστή δύναμη με βάση τις δυνάμεις τους 2, στο δεύτερο τα αντίστοιχα με 3, μετα με 5 κοκ. Η όλη διαδικασία είναι προφανώς ένα επικαιροποιημένο κόσκινο του Ερατοσθένη. Αν η διαδικασία συνεχιστεί για όλους τους πρώτους τελικά προκύπτει η ισότητα.

$$\ldots\left(1 - \frac{1}{7^s}\right)\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1$$

η πιο συνεπτυγμένα

$$\prod_p (1 - p^{-s}) \bullet \zeta(s) = 1$$

Τελικά

$$\zeta(s) = \sum_n n^{-s} = \prod_p (1 - p^{-s})^{-1}$$

όπου ο n είναι φυσικός αριθμός και ο p είναι πρώτος.

Η συνάρτηση ζ λοιπόν είναι ίση με ένα γινόμενο που εμπλέκονται μόνο οι πρώτοι αριθμοί. Στη πραγματικότητα η σχέση αυτή είναι άλλη μία απόδειξη ότι οι πρώτοι αριθμοί είναι άπειροι. Πράγματι, αν θέσουμε $s = 1$ το αριστερό μέλος είναι η αρμονική σειρά που αποκλίνει άρα και το δεξί μέλος είναι άπειρο που συμβαίνει μόνο αν οι παράγοντας του δεξιού γινομένου είναι άπειροι. Άρα οι πρώτοι είναι άπειροι. Η ανακάλυψη αυτή αλλά και η κομψή απόδειξη είναι του Euler.

Ο Riemann σε αυτή τη μνημειώδη εργασία του, έδωσε έναν τύπο που δίνει με πολύ καλύτερη προσέγγιση το πλήθος των πρώτων αριθμών από το 1 ως το N αλλά επίσης και ένα τρόπο, μέσω των ριζών της συνάρτησης ζ, να απαλλαγούμε από οποιοδήποτε σφάλμα και να το υπολογίζουμε ακριβώς. Ουσιαστικά, ο Riemann κατάφερε να σχεδιάσει έναν τύπο που δίνει ακριβώς το πλήθος των πρώτων μεταξύ 1 και N. Το πυκνογραμμένο κείμενο των σελίδων, παραδόξως έδινε μία οριστική απάντηση στο πρόβλημα που είχε διατυπώσει ο Gauss, όμως δεν έδινε καν την απόδειξη του Θεωρήματος των Πρώτων Αριθμών.

Προς αυτή τη κατεύθυνση δούλεψαν πολλοί μαθηματικοί όπως ο Ρώσος P.Chebyshev που έδειξε ότι αν

$$\pi(N) \sim \frac{CN}{lnN}$$

όπου C ένας σταθερός αριθμός τότε αναγκαστικά C=1 ενώ λίγο αργότερα κατάφερε να βρεί κάποια όρια στο λόγο $\frac{N}{lnN}$. Η εργασία του αυτή, μάλιστα, ήταν πολύ σημαντική γιατί πιθανό να ενέπνευσε τη χρήση της συνάρτησης ζ από τον Riemann. Το 1896 και ενώ οι συνθήκες είχαν ωριμάσει μετά από την εργασία του Riemann αλλά και τη γνώση από τους πληρέστερους πλέον πίνακες πρώτων, ο Γάλλος Jacques Hadamard και ο Βέλγος Jean de la Vallee Poussin δημοσίευσαν σχεδόν ταυτόχρονα αλλά ανεξάρτητα ο ένας από τον άλλον την απόδειξη του Θεωρήματος των Πρώτων Αριθμών.

3.5. Πρώτοι αριθμοί ως διαδοχικοί όροι αριθμητικής προόδου

Στη συνέχεια θα ασχοληθούμε με το ερώτημα της ύπαρξης πρώτων αριθμών ως διαδοχικών όρων αριθμητικής προόδου. Δίνεται ένα φυσικός αριθμός $n > 2$. Υπάρχει πρώτος αριθμός p και φυσικός αριθμός d τέτοιοι ώστε οι n διαδοχικοί όροι της αριθμητικής ακολουθίας

$$p, p + d, \dots, p + (n - 1)d$$

να είναι όλοι τους πρώτοι αριθμοι;

Έστω $n = 3$. Αν $d = 2$ τότε η μοναδική τριάδα είναι η 3,5,7.Κάθε άλλη τριάδα της μορφής $p, p + 2, p + 4$ έχει έναν όρο διαιρετό με το 3 και διάφορο του 3. Φυσικά και υπάρχουν τριάδες για άλλα d. Έτσι έχουμε μια τριάδα για d=6 την $p = 47,53,59$. Το ερώτημα είναι πόσες αριθμητικές πρόδοι φυσικών αριθμών υπάρχουν οι οποίες να περιέχουν διαδοχικές τριάδες πρώτων αριθμών.Η απάντηση είναι άπειρες. Το αποτέλσμα αυτό αποδείχτηκε από τον van der Copurt,S.Chowla και ως πόρισμα γενικότερης θεωρίας από τον Heath-Brown.

Η πιο μικρή τετράδα πρώτων αριθμών η οποία να αποτελεί διαδοχικούς όρους αριθμητικής προόδου φυσικών αριθμών είναι αυτή με p=5 και d=6, δηλαδή η 5,11,17,23.

Θεώρημα (Διαδοχικοί πρώτοι σε αριθμητικές προόδους). Για κάθε $n \geq 4$ υπάρχουν άπειρες αριθμητικές πρόοδοι οι οποίες να περιέχουν ως διαδοχικούς όρους n πρώτους αριθμούς.

<u>Πρόταση</u>

Έστω $d \geq 2$ και $a, a + d, a + (n - 1)d$ για $n \geq 2$ πρώτοι αριθμοί, διαδοχικοί όροι αριθμητικής προόδου και q ο μεγαλύτερος πρώτος με $q \leq n$.Τότε ο φυσικός αριθμός

$\left(\prod_{p \leq q} p\right)$ διαιρεί τον d

ή $p = q$ και $\left(\prod_{p \le q} p\right)$ διαιρεί τον d.

Εικασία

($(N^2 + 1)$-εικασία).Υπάρχουν άπειροι πρώτοι αριθμοί της μορφής $(N^2 + 1)$.

Η εικασία μέχρι σήμερα είναι ανοιχτή.Το καλύτερο γνωστό σχετικό αποτέλεσμα είναι του Hendrik Iwaniec, από το 1978:

«Υπάρχουν άπειρες τιμές του N για τις οποίες ο $N^2 + 1$ είναι πρώτος ή γινόμενο δύο πρώτων».

Εάν επιθυμούμε να μελετήσουμε το ανάλογο πρόβλημα και για άλλα πολυώνυμα δευτέρου ή ανώτερου βαθμού, θα πρέπει κατ' αρχήν να περιοριστούμε σε πολυώνυμα με ακέραιους συντελεστές με τον περιορισμό ότι δεν υπάρχει πρώτος, αριθμός p τέτοιος ώστε να διαιρεί όλες τις τιμες $f(n)$ όπου $n \in \mathbb{Z}$.

Πρόταση

Υπάρχουν διαστήματα φυσικών αριθμών οσοδήποτε μεγάλα τα οποία δεν περιέχουν κανέναν πρώτο αριθμό.

Απόδειξη

Έστω $n \in \mathbb{N}$. Κανένας από τους διαδοχικούς φυσικούς αριθμούς $(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + (n+1)$ δεν είναι πρώτος, διότι ο $(n+1)! + m$,διαιρείται με m για κάθε $m = 2,3, \dots, (n+1)$.

Παρατήρηση

Για να αποδείξουμε την παραπάνω πρόταση χρειάστηκε να πάμε «αρκετά μακριά» από σύνολο των φυσικών π.χ. για $n = 100$, οι αριθμοί $n! + 2, ..$ είναι πολύ μεγάλοι.

Υπάρχουν όμως διαστήματα στα οποία να εξασφαλίζεται η ύπαρξη πρώτων αριθμών;

Πρόταση (Αξίωμα του Bertrand)

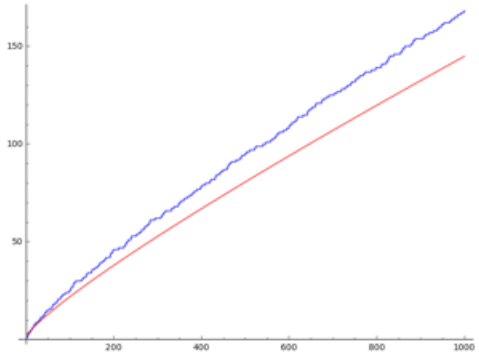
Για κάθε φυσικό ακέραιο $n > 1$ υπάρχει τουλάχιστο ένας πρώτος p.

$$n < p < 2n$$

Θεώρημα

(Θεώρημα των πρώτων αριθμών), Για μεγάλο x η συνάρτηση $\pi(x)$ προσεγγίζει την $x/logx$, δηλαδή

$$\lim_{x\to\infty} \frac{\pi(x)}{x/logx} = 1$$



Γραφική παράσταση της $\pi(x)(\mu\pi\lambda\acute{\epsilon})$ και της $x/\log(x)$ (κόκκινο) μέχρι το 1000.

Θεώρημα

Έστω a,b∈ℕ kai p ένας πρώτος αριθμός.Αν p| ab, τότε είτε p | a ή p | b.

Απόδειξη

Έστω ότι ο p δεν διαιρεί τον a.Αφού οι μόνοι διαιρέτες του p είναι ο 1 και ο p,έχουμε (a,p)=1.Απο γνωστό Θεώρημα υπάρχουν x,y∈ℤ τέτοιοι ώστε $1 = ax + py$.Άρα,

$$b = abx + pby$$

Αφού p | ab ,έπεται ότι p | b.

Με επαγωγή ως προς k παίρνουμε την εξής γενίκευση.

Θεώρημα

Έστω $a_1, \dots, a_k \in \mathbb{N}$ και p ένας πρώτος αριθμός.Αν $p \mid a_1, \dots, a_k$ τότε p | a_j για τουλάχιστον ένα $j \in \{1, \dots, k\}$.

ΚΕΦΑΛΑΙΟ 4^{Ο} - ΜΕΘΟΔΟΙ ΚΟΣΚΙΝΟΠΟΙΗΣΗΣ

4.1. Θεωρία κοσκίνων

Η θεωρία κοσκίνων είναι ένα σύμπλεγμα γενικών τεχνικών στην θεωρία αριθμών, σχεδιασμένο για να μετρά ή πιο ρεαλιστικά να εκτιμά το μέγεθος των κοσκινισμένων συνόλων ακεραίων. Το αρχικό παράδειγμα ενός κοσκινισμένου συνόλου είναι το σύνολο των πρώτων αριθμών μέχρι κάποιο ορισμένο όριο Χ.

Αντίστοιχα, το πρωταρχικό παράδειγμα ενός κοσκίνου είναι το κόσκινο του Ερατοσθένη, ή το πιο γενικό Κοσκινο του Legendre. Η άμεση επίθεση στους πρώτους αριθμούς χρησιμοποιώντας αυτές τις μεθόδους φτάνει σύντομα ανυπέρβλητα εμπόδια, με τον τρόπο της συσσώρευσης των όρων σφάλματος. Σε μια απο τις σημαντικότερες θέσεις της θεωρίας αριθμών του εικοστού αιώνα, βρέθηκαν τρόποι για να αποφευχθούν μερικές δυσκολίες μίας μετωπικής επίθεσης με μια αφελής ιδέα για το τι πρέπει να είναι το κοσκίνισμα.

Μια επιτυχής αντιμετώπιση είναι να προσεγγίσουμε ένα συγκεκριμένο κοσκινισμένο σύνολο αριθμών(για παράδειγμα το σύνολο των πρώτων αριθμών) με ένα άλλο, πιο απλό σύνολο το οποίο είναι τυπικά κάπως μεγαλύτερο από το αρχικό σύνολο, και επομένως ευκολότερο να αναλυθεί.

<u>Τύποι κοσκινίσματος</u>

Στα μοντέρνα κόσκινα συμπεριλαμβάνονται το κόσκινο του Brun, το κόσκινο του Selberg, το κόσκινο του Turan, το ‘’large sieve’’ και το ‘’larger sieve’’. Ένας από τους πρωταρχικούς σκοπούς της θεωρίας κοσκινίσματος ήταν να προσπαθήσει να αποδείξει εικασίες στην θεωρία αριθμών όπως είναι η εικασία των πρώτων διδύμων. Ενώ οι πρωταρχικοί στόχοι της θεωρίας κοσκινίσματος ακόμα δεν έχουν επιτευχθεί σε μεγάλο βαθμό, υπάρχουν εν μέρη επιτυχίες σε συνδυασμό με άλλα θεωρητικά αριθμητικά εργαλεία.

Κάποιες επιτυχίες είναι :

1. Το θεώρημα του Brun το οποίο ισχυρίζεται ότι το άθροισμα των αντιστρόφων των διδύμων πρώτων συγλίνει.(ενώ το άθροισμα των αντιστρόφων των πρώτων αποκλίνει)
2. Το θεώρημα του Chen το οποίο μας αποδεικνύει ότι υπάρχουν τόσοι άπειροι πρώτοι p τέτοιοι ώστε $p+2$ να είναι είτε πρώτος είτε ‘’semiprime’’.
3. Το θεώρημα των Friedlander-Iwaniec, το οποίο ισχυρίζεται ότι υπαρχουν άπειροι πρώτοι της μορφής a^2+b^4.
4. Το θεώρημα του Zhang το οποίο ισχυρίζεται ότι υπάρχουν άπειρα ζευγάρια πρώτων με προκαθορισμένη απόσταση.

4.2 Το κόσκινο του Ερατοσθένη

Ο Ερατοσθένης (Κυρήνη 276 π.Χ. – Αλεξάνδρεια 194 π.Χ.) ήταν αρχαίος Έλληνας μαθηματικός, γεωγράφος, αστρονόμος, γεωδαίτης, ιστορικός και φιλόλογος. Θεωρείται ο πρώτος που υπολόγισε το μέγεθος της Γης και κατασκεύασε ένα σύστημα συντεταγμένων με παράλληλους και μεσημβρινούς. Ακόμα κατασκεύασε ένα χάρτη του κόσμου όπως τον θεωρούσε. Το 200 π.Χ. περίπου ο Έλληνας Ερατοσθένης, γεννημένος στην Λιβύη, επινόησε έναν αλγόριθμο για τον υπολογισμό των πρώτων αριθμών που ονομάζεται ‘κόσκινο του Ερατοσθένη’. Το ‘κόσκινο του Ερατοσθένη’, σε τροποποιημένη μορφή, είναι χρήσιμο ακόμα και σήμερα στην έρευνα της Θεωρίας Αριθμών. Το κόσκινο εμφανίζεται στο βιβλίο του Νικομήδη ‘Εισαγωγή στην Αριθμητική’.

Σύμφωνα με τον αλγόριθμο αυτό,γράφουμε διαδοχικά τους ακέραιους αριθμούς από το 2 ως τον μεγαλύτερο αριθμό n που επιθυμούμε να συμπεριλάβουμε στον πίνακα. Διαγράφουμε όλους τους αριθμούς τους μεγαλύτερους από 2 που διαιρούνται με το 2 (δηλαδή κάθε δεύτερο αριθμό). Βρίσκουμε τον μικρότερο εναπομείναντα αριθμό μεγαλύτερο του 2, δηλαδή τον 3. Διαγράφουμε όλους τους αριθμούς τους μεγαλύτερους από 3 που διαιρούνται με το 3 (δηλαδή κάθε τρίτο αριθμό). Βρίσκουμε τον μικρότερο εναπομείναντα αριθμό μεγαλύτερο του 3, δηλαδή τον 5. Διαγράφουμε όλους τους αριθμούς τους μεγαλύτερους από 5 που διαιρούνται με το 5 (δηλαδή κάθε πέμπτο

αριθμό). Συνεχίζουμε μέχρι να έχουμε διαγράψει όλους τους αριθμούς που διαιρούνται με $\left[\sqrt{n}\right]$. Οι αριθμοί που απέμειναν είναι πρώτοι. Αυτή η διαδικασία παρουσιάζεται στον παρακάτω πίνακα που περιέχει τους φυσικούς ως το 50, και ως εκ τούτου διαγράφει τους σύνθετους αριθμούς που διαιρούνται ως το $\left[\sqrt{50}\right] = 7$. Αν η διαδικασία συνεχιστεί ως τον n , τότε ο αριθμός των διαγραφέντων δίνει τον αριθμό των διακριτών πρώτων παραγόντων του κάθε αριθμού.

Σχηματικά θα δούμε ένα παράδειγμα μέχρι το 300.

Κρατάμε τον πρώτο αριθμό 2 και διαγράφουμε όλα τα πολλαπλάσιά του.

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220
221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260
261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280
281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300

στη συνέχεια κρατάμε τον επόμενο πρώτο αριθμό (3) και διαγράφουμε όλα τα πολλαπλάσια του,

	2	3		5		7		9		11		13		15		17		19	
21		23		25		27		29		31		33		35		37		39	
41		43		45		47		49		51		53		55		57		59	
61		63		65		67		69		71		73		75		77		79	
81		83		85		87		89		91		93		95		97		99	
101		103		105		107		109		111		113		115		117		119	
121		123		125		127		129		131		133		135		137		139	
141		143		145		147		149		151		153		155		157		159	

161		163		165		167		169		171		173		175		177		179	
181		183		185		187		189		191		193		195		197		199	
201		203		205		207		209		211		213		215		217		219	
221		223		225		227		229		231		233		235		237		239	
241		243		245		247		249		251		253		255		257		259	
261		263		265		267		269		271		273		275		277		279	
281		283		285		287		289		291		293		295		297		299	

Συνεχίζουμε την διαδικασια για 5,7,11… και καταλήγουμε

οι πρώτοι αριθμοί μέχρι το 300 είναι:

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
73	79	83	89	97															
101	103	107	109	113	127	131	137	139	149	151	157	163	167	173	179	181	191	193	197
199																			
211	223	227	229	233	239	241	251	257	263	269	271	277	281	283	293				

Το κόσκινο του Euler

Ο Euler , στην απόδειξή του για το γινόμενο Euler της ζ-συνάρτησης του Riemann, χρησιμοποίησε μια έκδοση του κόσκινου του Ερατοσθένη, η οποία ήταν καλύτερη γιατί κάθε αριθμός απαλειφόταν ακριβώς μια φορά. Σε αντίθεση με το κόσκινο του Ερατοσθένη που διαγράφει πολλαπλάσια των πρώτων αριθμών που βρίσκει από την ίδια ακολουθία, το κόσκινο του Όιλερ χρησιμοποιεί ακολουθίες που έχουν δημιουργηθεί διαδοχικά από πολλαπλάσια των προηγούμενων πρώτων αριθμών:

Α) Αρχίζουμε με όλους τους φυσικούς αριθμούς εκτός από το '1' που δεν είναι πρώτος αριθμός:

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27…

Β) Ο αριθμός στα αριστερά είναι πρώτος. Πολλαπλασιάζουμε κάθε αριθμό στη λίστα με αυτόν και αγνοούμε τα γινόμενα

(4 6 8 10 12 14 16 18 20 22 24 26 …)

Διαγράφονται:

4 6 8 10 12 14 16 18 20 22 24 26

Παραμένουν:

2 **3** 5 7 9 11 13 15 17 19 21 23 25 ...

Γ) Ο αριθμός πριν τον προηγούμενο πρώτο είναι επίσης πρώτος. Πολλαπλασιάζουμε με αυτόν κάθε αριθμό στη λίστα αρχίζοντας από αυτόν τον πρώτο και αγνοούμε τα γινόμενα

(9 15 21 27 33 39 45 51 57 63 69 75 …)

Αφαιρούνται:

9 15 21 27

Παραμένουν :

2 3 **5** 7 11 13 17 19 23 25 29 …

Επαναλαμβάνουμε το Γ) επ' άπειρον. Σε κάθε επανάληψη εντοπίζουμε έναν νέο πρώτο αριθμό (που μαρκάρεται με έντονη γραμματοσειρά) μέχρι να βρεθούν όλοι οι πρώτοι στην αρχική λίστα. Οι αριθμοί που απορρίπτονται εξακολουθούν να χρησιμοποιούνται για την κατασκευή του τρέχοντος κόσκινου, δηλ. όταν κατασκευάζουμε ένα κόσκινο για το 3 κάνουμε τις πράξεις $3 * 3 = 9,\ 3 * 5 = 15,\ 3 * 7 = 21, \ldots 3 * 15 = 45, \ldots$ Το 15 που απορρίπτεται χρησιμοποιείται για την κατασκευή του κόσκινου και μετά οι αριθμοί αφαιρούνται από τη λίστα.

Το κόσκινο του Euler είναι μια καλή λύση για την παραγωγή άπειρων ακολουθιών πρώτων αριθμών και το κόσκινο του Turner είναι μια κοντινή εκδοχή του.

4.3. Το κόσκινο του Sundaram

Στα Μαθηματικά, το κόσκινο του Sundaram είναι ένας απλός ντετερμινιστικός αλγόριθμος που χρησιμοποιείται για την εύρεση όλων των πρώτων αριθμών μεχρι ένα συγκεκριμένο ακέραιο. Ανακαλύφθηκε από τον Ινδό Μαθηματικό S.P. Sundaram το 1934.

Αλγόριθμος

Ξεκινάμε με μία λίστα από τους ακέραιος από το 1 μέχρι το n. Από αυτή την λίστα, αφαιρούμε όλους τους αριθμούς που έχουν την μορφή

$i + j + 2ij$

- $i, j \in \mathbb{N}, 1 \leq i \leq j$
- $i + j + 2ij \leq n$

Οι υπόλοιποι αριθμοί διπλασιάζονται και αυξάνονται κατά 1, δίνοντας μία λίστα περιττών πρώτων αριθμών(το οποίο είναι όλοι οι πρώτοι εκτός του 2) μικρότεροι από $2n + 2$.

Το κόσκινο του Sundaram επιλέγει τους σύνθετους αριθμούς έτσι ακριβώς από το κόσκινο του Ερατοσθένη, αλλά οι άρτιοι δεν λαμβάνονται υπόψιν. Η διαδικασία διαγραφής των πολλαπλάσιων του 2 γίνεται από το τελικό βήμα διπλασιασμού και αύξησης. Ενώ η μέθοδος του Ερατοσθένη θα διέγραφε κ διαφορετικά πολλαπλάσια ενός πρώτου $2i + 1$, η μέθοδος του Sundaram διαγράφει $i + j(2i + 1)$ for $1 \leq j \leq \left\lfloor \frac{k}{2} \right\rfloor$.

Εάν ξεκινήσουμε με ακέραιους από το 1 μέχρι το n, η τελική λίστα περιέχει μόνο περιττούς ακέραιους από το 3 μέχρι το $2n + 1$. Από αυτή την τελική λίστα, κάποιοι περιττοί ακέραιοι έχουν εξαιρεθεί: πρέπει να δείξουμε ότι αυτοί οι συγκεκριμένοι σύνθετοι περιττοί ακέραιοι είναι μικρότεροι του $2n + 2$.

Έστω q περιττός ακέραιος της μορφής $2k + 1$. Τότε ο q εξαιρείται αν και μόνο αν είναι της μορφής $i + j + 2ij$, δηλαδή $q = 2(i + j + 2ij) + 1$. Τότε έχουμε

$$q = 2(i + j + 2ij) + 1$$
$$= 2i + 2j + 4ij + 1$$
$$= (2i + 1)(2j + 1)$$

Συνεπώς ένας περιττός ακέραιος αριθμός εξαιρείται της τελικής λίστας αν και μόνο αν έχει παραγοντοποιημένη μορφή $(2i + 1)(2j + 1)$ η οποία μας δείχνει ότι ο q είναι γινόμενο περιττών. Επομένως η λίστα πρεπεί να αποτελείται από περιττους που είναι πρώτοι και είναι μικρότεροι η ίσοι από το $2n + 2$.

4.4. Το κόσκινο του Atkin

Στα μαθημάτικα το κόσκινο του Atkin είναι ένας μοντέρνος αλγόριθμος για την εύρεση όλων των πρώτων αριθμών μέχρι ένα συγκεκριμένο ακέραιο. Σε σύγκριση με το κόσκινο του Ερατοσθένη, το οποίο διαγράφει τα πολλαπλάσια των πρώτων, αυτό κάνει μια προκαταρκτική εργασία και έπειτα διαγράφει τα πολλαπλάσια των τετραγώνων των πρώτων. Δημιουργήθηκε το 2003, από τον A. O. L. Atkin και από τον Daniel J. Bernstein.

Αλγόριθμος

Στον αλγόριθμο

- Όλα τα υπόλοιπα είναι $mod60$
- Όλοι οι αριθμοί, μαζι με το x, y, είναι θετικοί ακέραιοι.
- Αλλάζοντας μία καταχώρηση στην λίστα κοσκινίσματος σημαίνει αλλαγή χαρακτηρισμού από πρώτο σε μη-πρώτο.

Ο αλγόριθμος

1. Δημιουργεί μία λίστα αποτελεσμάτων, συμπληρωμένη με το 2 το 3 και το 5.
2. Δημιουργεί μία λίστα κοσκινίσματος με μία καταχώρηση για κάθε θετικό ακέραιο, όλες οι καταχωρήσεις σε αυτή τη λίστα θα πρεπει να είναι αρχικά χαρακτηρισμένες ως μη-πρώτοι(σύνθετοι).
3. Για κάθε καταχώρηση αριθμού n στην λίστα κοσκινίσματος, με $mod60$ υπόλοιπο r
   i) Εάν το $r = 1, 13, 17, 29, 37, 41, 49$ ή 53 αλλάζουμε την καταχώρηση για κάθε πιθανή λύση της $4x^2 + y^2 = n$.
   ii) Εάν το $r = 7,19,31$ ή 43 αλλάζουμε την καταχώρηση για κάθε πιθανή λύση $3x^2 + y^2 = n$.
   iii) Εάν το $r = 11, 23, 47$ ή 59 αλλάζουμε την καταχώρηση για κάθε πιθανή λύση $3x^2 - y^2 = n$ για $x > y$.
   iv) Εάν το r είναι κάτι διαφορετικό το αγνοούμε εντελώς.
4. Αρχίζουμε με την μικρότερο αριθμό στην λίστα κοσκινίσματος
5. Παίρνουμε τον επόμενο αριθμό στην λίστα κοσκινίσματος που είναι ακόμα χαρακτηρισμένος πρώτος.

6. Συμπεριλαμβάνουμε τον αριθμό στην λίστα αποτελεσμάτων
7. Υψώνουμε στο τετράγωνο τον αριθμό και χαρακτηρίζουμε όλα τα πολλαπλάσια του τετραγώνου σαν μη-πρώτα.
8. Επαναλμβάνουμε τα βήματα 4 μέχρι 7.

ΚΕΦΑΛΑΙΟ $5^{Ο}$ – Μερικές εφαρμογές των πρώτων αριθμών

5.1. Οι πρώτοι αριθμοί του Mersenne και οι τέλειοι αριθμοί

Θεωρούμε τους πρώτους αριθμούς που μπορούν να γραφτουν 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	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 α είναι περιττός, τότε ο $\alpha - 1$ είναι άρτιος, επομένως δεν μπορεί να είναι πρώτος.
2. Ο $\alpha_n - 1$ διαιρείται πάντα από το $a - 1$.

<u>Απόδειξη</u>

$$\alpha_n - 1 = (a-1)(a_{n-1} + a_{n-2} + \cdots + a_2 + a + 1$$

Επομένως ο $\alpha_n - 1$ είναι σύνθετος εκτός και αν $\alpha - 1 = 1 \Rightarrow \alpha = 2$

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

<u>Ορισμός</u>

Πρώτοι αριθμοί της μορφής $2^p - 1$ καλούνται πρώτοι αριθμοί του Mersenne

Μερικά παραδείγματα από τους αριθμούς του Mersenne είναι :

$$2^2 - 1 = 3, 2^5 - 1 = 31, 2^{13} - 1 = 8191.$$

Παρατηρούμε ότι κάθε αριθμός της μορφής $2^p - 1$ δεν είναι απαραίτητα πρώτος.
Για παράδειγμα ο $2^{11} - 1$=2047=23•89 δεν είναι πρώτος .
Δεν είναι γνωστό αν είναι άπειροι σε πλήθος οι πρώτοι αριθμοί του Mersenne. Ο μεγαλύτερος γνωστός αριθμος 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.

<u>Τύπος του Euclid των τέλειων αριθμών</u>

Αν $2^p - 1$ είναι πρώτος αριθμός τότε ο $2^{p-1}(2^p - 1)$ 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 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 ότι ο 496 είναι τέλειος αριθμός πρέπει να προσθέσουμε τους ορθούς διαιρέτες του 496.
Παραγοντοποιούμε το 496 οπότε και έχουμε $496 = 2^4 \bullet 31$, επομένως οι ορθοί διαιρέτες είναι :

$$1,2, 2^2, 2^3, 2^4, 31,2 \bullet 31, 2^2 \bullet 31, 2^3 \bullet 31$$

Για να υλοποιήσουμε την γενική μέθοδο που θα χρησιμοποιήσουμε για να αποδείξουμε τον τύπο του Euclid θα προσθέσουμε τους ορθούς διαιρέτες σε 2 στάδια.
Αρχικα $1 + 2 + 2^2 + 2^3 + 2^4 = 31$ και στην συνέχεια $31 + 2 \bullet 31 + 2^2 \bullet 31 + 2^3 \bullet 31 = 31 \bullet 15$. Οπότε $31 + 31 \bullet 15 = 496$..

Άρα ο 496 είναι πράγματι τέλειος αριθμός.

5.2. RSA Public Key – Κρυπτογραφία

Αυτή είναι μία τεχνική για να κωδικοποιούμε και αποκωδικοποιούμε μηνύματα.

1. Το πρώτο βήμα για να κωδικοιήσουμε ένα μήνυμα είναι να το μετατρέψουμε σε ακολουθία αριθμών. Μια απλή μέθοδος για να το επιτύχουμε 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 ότι 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 $m = p \bullet q$. Επιπλέον υπολογίζουμε το $\varphi(m) = \varphi(p \bullet q) = (p-1) \bullet (q-1)$.
3. Στη συνέχεια επιλέγουμε έναν αριθμό k τέτοιο ώστε ΜΚΔ$(k, \varphi(m)) = 1$.
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 μπορει να χρησιμοποιήσει τους αριθμούς k και m για να κωδικοποιήσει το μήνυμα με τον παρακάτω τρόπο:
   i) Αρχικά μετατρέπουν το μήνυμα τους σε μία ακολουθία από αριθμούς όπως περιγράψαμε παραπάνω.
   ii) 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 μία λίστα αριθμών $a_1, a_2, \dots, a_r$.
   iii) Στη συνέχεια, χρησιμοποιώντας την μέθοδο διαδοχικού τετραγωνισμού(successive squaring) υπολογίζουμε τις δυνάμεις

$a_1^k mod m, a_2^k mod m, \dots, a_r^k mod m$. Αυτές οι τιμές δημιουργούν μία νέα λίστα τιμών $b_1, b_2, \dots, b_r$.

6. Για να αποκωδικοποιήσουμε το μήνυμα αφού το λάβαμε κωδικοποιημένο χρησιμοποιούμε την παρακάτω μέθοδο
   i) Έχουμε λάβει την λίστα των αριθμών $b_1, b_2, \dots, b_r$ και θέλουμε να ανακτήσουμε τους αριθμούς $a_1, a_2, \dots, a_r$.
   ii) Υπενθυμίζουμε ότι κάθε b_i είναι ισότιμο με $a_i^k mod m$, οπότε για να βρούμε κάθε a_i πρέπει να λύσουμε την ισοτιμία: $x^k \equiv b_i mod m$.
   iii) Αφού γνωρίζουμε τις τιμές των αριθμών p και q με $m = p \bullet q$. Γνωρίζουμε ότι $\varphi(m) = \varphi(p \bullet q) = (p-1)(q-1) = pq - p - q + 1 = m - p + q + 1$.
   iv) Τέλος εφαρμόζουμε τον Αλγόριθμο για τον υπολογισμό ριζών k τάξης modulo m για να λύσουμε καθεμία από τις ισοτιμίες $x^k \equiv b_i mod m$. Οι λύσεις είναι οι αριθμοί $a_1, a_2, \dots, a_r$. Στη συνέχεια χρησιμοποιούμε αυτή την ακολουθία των ψηφίων για να ανακτήσουμε το αρχικό μήνυμα.

Για παράδειγμα ο αλγόριθμος υπολογισμού ριζών k τάξης modulo m είναι ο εξής:

Έστω b,k και m είναι ακέραιοι τέτοιοι ώστε ΜΚΔ$(b, m) = 1$ και ΜΚΔ $k, \varphi(m)) = 1$.

Τότε τα επόμενα βήματα δίνουν μία λύση στην ισοτιμία $x^k \equiv b mod m$.

i. Υπολόγισε το $\varphi(m)$.
ii. Χρησιμοποίησε τον Ευκλείδιο Αλγόριθμο για να βρείς ακέραιους u και v που ικανοποιούν την σχέση $ku + \varphi(m)v = 1$.
iii. Υπολόγισε το $b^u mod\ m$ με την μέθοδο του διαδοχικού τετραγωνισμού. Η τιμη που λαμβάνετε αποτελει την λύση x.

Παράδειγμα

Κωδικοποιήσε το μήνυμα 'STANFORD' χρησιμοποιώντας το δημόσιο κλειδί $m = 143$ και $k = 23$.

Λύση

Αρχικά μετατρέπουμε το κείμενο ‘STANFORD’ σε μία ακολουθία από αριθμούς : 2930111416252814.

Ο αριθμός m έχει 3 ψηφία, οπότε χωρίζουμε το μήνυμα 2930111416252814 σαν να είναι μία ακολουθία αριθμών με το ψηφία το καθένα: 29,30,11,24,16,25,28,14.

Στη συνέχεια χρησιμοποιούμε τη μέθοδο του διαδοχικού τετραγωνισμού για να υπολογίσουμε την 23η δύναμη από κάθε αριθμό modulo 143.

Αρχικά υπολογίζουμε το $29^{23} mod 143$ οπότε και έχουμε :

$$29^{23} \equiv 29^{16}29^{4}29^{2}29^{1}$$

$$29 \equiv 29 mod 143$$

$$29^{2} \equiv 126 mod 143$$

$$29^{4} \equiv 3 mod 143$$

$$29^{8} = 9 mod 143$$

$$29^{16} \equiv 81 mod 143$$

Άρα $29^{23} \equiv 81 \bullet 3 \bullet 126 \bullet 29 \equiv 35 mod 143$.

Έπειτα χρησιμοποιούμε τη μέθοδο του διαδοχικού τετραγωνισμού για να υπολογίσουμε την 23η δύναμη από κάθε αριθμό που απομένει modulo 143:

$$29^{23} \equiv 35 mod 143$$

$$30^{23} \equiv 127 mod 143$$

$$11^{23} \equiv 110 mod 143$$

$$24^{23} \equiv 19 mod 143$$

$$16^{23} \equiv 48 mod 143$$

$$25^{23} \equiv 38 mod 143$$

$$28^{23} \equiv 7 mod 143$$

$$14^{23} \equiv 27 mod 143$$

<u>Παράδειγμα</u>

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 modulo143

$$a_1^{23} \equiv 20 mod 143$$
$$a_2^{23} \equiv 130 mod 143$$
$$a_3^{23} \equiv 62 mod 143$$
$$a_r^{23} \equiv 107 mod 143$$

Μπορούμε να λύσουμε τις παραπάνω ισοτιμίες χρησιμοποιώντας τον αλγόριθμο υπολογισμού ριζών k τάξης modulo m. Αφού γνωρίζουμε ότι $p = 11$ και $q = 13$ μπορούμε να υπολογίσουμε το $\varphi(m) = \varphi(11) \bullet \varphi(13) = 10 \bullet 12 = 120$

Στη συνέχεια βρίσκουμε ακεραίους u και v τέτοιους ώστε $23u + 120v = 1$

Χρησιμοποιώντας τον Ευκλείδιο αλγόριθμο θα λάβουμε $u = 47$και $v = -9$.

Οπότε είμαστε σε θέση να λύσουμε κάθε ισοτιμία. Για να λύσουμε την $1^{η}$ ισοτιμία modulo143 υπολογίζουμε το $20^u \equiv 20^{47} modulo\ 143$ με την μέθοδο του διαδοχικού τετραγωνισμού. Άρα έχουμε:

$$20^{47} \equiv 20^{32}20^8 20^4 20^2 20^1$$
$$20^1 \equiv 20 mod 143$$
$$20^2 \equiv 114 mod 143$$
$$20^4 \equiv 126 mod 143$$
$$20^8 \equiv 3 mod 143$$
$$20^{16} \equiv 9 mod 143$$
$$20^{32} \equiv 81 mod 143$$

Οπότε $20^{47} \equiv 20 \bullet 114 \bullet 126 \bullet 3 \bullet 81 \equiv 15 mod 143$.

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

Να κωδικοποιήσετε το μήνυμα ' To be or not to be ' χρησιμοποιώντας τους πρώτους $p = 12553$ και $q = 13007$.

Λύση

Αρχικά υπολογίζουμε το $m = pq = 12553 \bullet 13007 = 163276871$ 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 30251215252824253030251215.

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 κάθε έναν από τους αριθμούς στην κ-οστη δύναμη modulo m:

$$30251215^{79921} \equiv 149419241 mod 163276871$$

$$25282425^{79921} \equiv 62721998 mod 163276871$$

$$30302512^{79921} \equiv 118084566 mod 163276871$$

$$15^{79921} \equiv 40481382 mod 163276871$$

Άρα το κωδικοποιημένο μήνυμα είναη η λίστα αριθμών 149419241, 62721998, 118084566, 40481382.

Είναι επακόλουθο να αναρωτηθεί κάποιος πόσο ασφαλές είναι το συγκεκριμένο κρυπτοσύστημα. Ας υποθέσουμε ότι το μήνυμα υποκλάπτεται από τρίτους. Αφού το m και το k είναι δημόσια τότε ο υποκλοπέας μπορεί να αποκωδικοποιήσει το μήνυμα αν μπορεί να βρεί την τιμή του $\varphi(m) = \varphi(p)\varphi(q)$.

Άρα για να αποκωδικοποιήσεις το μήνυμα, ο υποκλοπέας πρέπει να παραγοντοποιήσει το m για να βρεί το p και το q. Αν το m έχει από 5 εώς 10 ψηφία τότε ένας υπολογιστής μπορεί να βρεί τους παράγοντες του m σχεδόν ακαριαία. Χρησιμοποιώντας εξειδικευμένες

μεθόδους 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 τότε δεν υπάρχουν γνωστές τεχνικές για τον υποκλοπέα να καθορίσει τους p και q από τον $m = pq$.

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 μπορούν να διανεμηθούν στο κοινό ενώ η μέθοδος της αποκωδικοποίησης παραμένει ασφαλής. Αυτό το συγκεκριμένο κρυπτοσύστημα καλείται RSA **κρυπτοσύστημα δημοσίου κλειδιού** και ονομάστηκε από τους εφευρέτες του Ron Rivest, Adi Shamir και Leonard Adleman που το ανακάλυψαν το 1977.

5.3. Πρώτοι αριθμοί στην φύση

Αναπόφευκτα, κάποιοι από τους αριθμούς που απαντώνται στη φύση είναι πρώτοι. Υπάρχουν ωστόσο σχετικά λίγα παραδείγματα αριθμών που εμφανίζονται *επειδή* είναι πρώτοι. Ένα παράδειγμα της χρήσης των πρώτων αριθμών στη φύση είναι μια εξελικτική στρατηγική που χρησιμοποιείται από τα τζιτζίκια του γένους Magicicada. Τα έντομα αυτά περνούν το μεγαλύτερο μέρος της ζωής τους κάτω από τη γη σαν κάμπιες. Μεταμορφώνονται και βγαίνουν από το έδαφος μόνο μετά από 7, 13 ή 17 χρόνια, οπότε πετούν, αναπαράγονται και πεθαίνουν έπειτα από το πολύ μερικές εβδομάδες. Γεννάται λοιπόν το ερώτημα, γιατί τα τζιτζίκια έχουν εξελιχθεί ώστε να χρησιμοποιούν τα συγκεκριμένα χρονικά διαστήματα; Ο γνωστός εξελικτικός οικολόγος Steven Jay Gould ήταν από τους πρώτους που παρατήρησαν αυτή την συμπεριφορά και υπέθεσε ότι τα διαστήματα πρώτων αριθμών μεταξύ των εμφανίσεων δυσκολεύουν την εξέλιξη θηρευτών που θα εξειδικεύονται στα τζιτζίκια. Αν τα τζιτζίκια εμφανίζονταν σε μη-πρώτα διαστήματα,

ας πούμε κάθε 12 χρόνια, τότε οι θηρευτές που εμφανίζονται κάθε 2, 3, 4, 6 ή 12 χρόνια θα τα συναντούσαν σίγουρα. Έχει βρεθεί ότι σε μια περίοδο 200 ετών, ο μέσος πληθυσμός θηρευτών αν τα τζιτζίκια εμφανίζονταν κάθε 14 ή 15 χρόνια θα ήταν 2% μεγαλύτερος από ότι αν τα τζιτζίκια εμφανίζονται κάθε 13 ή 17 χρόνια. Αν και μικρό, αυτό το πλεονέκτημα δείχνει να είναι αρκετό ώστε να οδηγήσει την φυσική επιλογή υπέρ του κύκλου ζωής με διάρκεια πρώτων αριθμών γι αυτά τα έντομα. Ωστόσο αυτή είναι απλά μια υπόθεση που ακόμα αμφισβητείται, αφού δεν εξηγεί γιατί τα τζιτζίκια κατέληξαν να έχουν κύκλο ζωής 13 και 17 ετών και όχι 11 ή 19 ή κάποιον άλλο πρώτο αριθμό.

Βιβλιογραφία

1. Γιαννόπουλος, Α.(2003). *Σημειώσεις Θεωρίας Αριθμών.* Ηράκλειο Κρήτης: Πανεπιστήμιο Κρήτης Τμήμα Μαθηματικών
2. Νεγρεπόντης Σ., (2009), *Σημειώσεις του μαθήματος 'Ιστορία των Αρχαίων Ελληνικών Μαθηματικών-Στοιχεία Ευκλείδη*'.
3. Παπαιωάννου, Α.(2006). *Θεωρία Γραφημάτων*. Αθήνα : Εκδόσεις Ε.Μ.Π.
4. Παπαιωάννου, Α. & Ρασσιάς, Μ.(2009). *Εισαγωγή στην Θεωρία Αριθμών*. Αθήνα : Εκδόσεις Συμεών
5. Chen, J. R. (1973). *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*. Sci. Sinica 16:157-176
6. Davis,M.D., (2007), *Η φύση και η δύναμη των Μαθηματικών*, απόδοση στα ελληνικά: Καραγιαννίδης Δ., Μαγειρόπουλος Μ., Πανεπιστημιακές εκδόσεις Κρήτης.
7. Dickson L.E., (2005), *History of the theory of numbers*, Vol. 1 : Divisibility and Primality, Dover.
8. Gauss, Carl Friedrich; Clarke, Arthur a. (translator into English)(1986), *Disquisitiones Arithemeticae*(Second, corrected edition), New York : Springer, ISBN 0-387-9524-9.
9. Greaves, G.R.H., (1997), *Sieve methods, Exponential Sums, and their Applications in Number Theory,* Cambridge University Press.
10. Hardy, G. H. and Wright, E. M. *An introduction to the Theory of Numbers*, 5th ed. Oxford, England : Clarendon Press; 1979.
11. Heath, T. L., (1921), *A history of Greek Mathematics*, Oxford University.
12. H.Fustenberg : *On the infinitude of primes*, Amer. Math. Monthly 62(1955), 353.
13. Mollin, R.A., (2008) *Fundamental Number Theory with Applications*, Chapman & Hall/CRC.
14. Ribenboim, P., (1996), *The New Book of Prime Number Records*. New York: Springer – Verlag, pp. 20-21,
15. Rosen, K.H., (1986), *Elementary number theory and its applications*, Addison-Wesley.
16. Schroeder, M.R. Schroeder,(2009), *Number Theory in Science and Communication*, Springer-Verlag Berlin Heidelberg.
17. https://en.wikipedia.org/wiki/Sieve_theory
18. https://en.wikipedia.org/wiki/Sieve_of_Eratosthenes
19. https://en.wikipedia.org/wiki/Sieve_of_Sundaram
20. https://en.wikipedia.org/wiki/Sieve_of_Atkin