ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Ανοικτά Προβλήματα Πρώτων Αριθμών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΠΑΓΕΩΡΓΙΟΥ ΑΛΕΞΑΝΔΡΟΥ

Επιβλέπων Καθηγητής : Φελλούρης Ανάργυρος

Αναπλ. Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2014

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Ανοικτά Προβλήματα Πρώτων Αριθμών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΠΑΓΕΩΡΓΙΟΥ ΑΛΕΞΑΝΔΡΟΥ

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

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την.

(ΥΠΟΓΡΑΦΗ)	(ΥΠΟΓΡΑΦΗ)	(ΥΠΟΓΡΑΦΗ)
……..	……..	……..
Φελλούρης Ανάργυρος Αναπλ. Καθηγητής Ε.Μ.Π.	Κανελλόπουλος Βασίλειος Επίκ. Καθηγητής Ε.Μ.Π.	Στεφανέας Πέτρος Λέκτορας Ε.Μ.Π.

Αθήνα, Ιούλιος 2014

(Υπογραφή)

.....

ΠΑΠΑΓΕΩΡΓΙΟΥ ΑΛΕΞΑΝΔΡΟΣ

Διπλωματούχος Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών Ε.Μ.Π.

Περίληψη-Ευχαριστίες

Στην παρούσα διπλωματική εργασία μελετώνται οι πρώτοι αριθμοί. Πιο συγκεκριμένα, στο πρώτο κεφάλαιο γίνεται μια μικρή ιστορική αναδρομή, στην οποία φαίνεται ο ορισμός των πρώτων αριθμών, ως τους αριθμούς που έχουν μοναδικούς διαιρέτες την μονάδα και τον εαυτό τους, οι κυριότερες χρήσεις τους καθώς και το πότε ξεκίνησε η ενασχόληση των μαθηματικών με αυτούς και γιατί παρουσιάζουν τόσο ενδιαφέρον.

Στο δεύτερο κεφάλαιο γίνεται μια αναλυτικότερη ιστορική αναδρομή και παρουσιάζονται οι μεγάλοι μαθηματικοί που μελέτησαν τους πρώτους αριθμούς όπως: Ευκλείδης, Ερατοσθένης, Pierre de Fermat, Marin Mersenne, Leonhard Euler. Παρατίθενται κάποια σημαντικά θεωρήματα και οι σημαντικότερες παρατηρήσεις που έχουν γίνει ως προς τους πρώτους αριθμούς από την αρχαιότητα μέχρι τα νεότερα χρόνια.

Στο τρίτο κεφάλαιο μελετώνται αναλυτικά κάποιες από τις βασικές ιδέες και θεωρήματα που αποτελούν την Θεωρία των Πρώτων Αριθμών. Συγκεκριμένα, διατυπώνεται και αποδεικνύεται το Θεμελιώδες Θεώρημα της Αριθμητικής, αποδεικνύεται ότι οι πρώτοι αριθμοί είναι άπειροι (6 αποδείξεις), ορίζεται και μελετάται η συνάρτηση π(x), καθώς και τα θεωρήματα των Bertrand, Fermat, Euler και Wilson.

Στο τέταρτο κεφάλαιο αναφέρονται κάποια προβλήματα σχετικά με τους πρώτους αριθμούς, τα οποία είναι άλυτα ως τις μέρες μας. Ιδιαίτερη έμφαση δίνεται σε τρία από αυτά που έχουν απασχολήσει περισσότερο τους μαθηματικούς, στην Υπόθεση του Riemann, την Εικασία του Goldbach και το θέμα της απειρίας των δίδυμων πρώτων αριθμών.

Στο πέμπτο κεφάλαιο παρουσιάζονται μερικές εφαρμογές των πρώτων αριθμών. Συγκεκριμένα παρουσιάζονται οι εφαρμογές τους σε άλλους τομείς των μαθηματικών, στην κρυπτογραφία, τις γεννήτριες ψευδοτυχαίων αριθμών και στη φύση.

Τέλος, στο έκτο κεφάλαιο, περιγράφεται σύντομα η ομορφιά που διέπει την Θεωρία Αριθμών, η οποία είναι και ο λόγος που οι επιστήμονες ασχολήθηκαν και θα συνεχίσουν να ασχολούνται με την μελέτη της.

Κλείνοντας θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα αυτής της διπλωματικής εργασίας κ. Ανάργυρο Φελλούρη, Αναπληρωτή Καθηγητή του Ε.Μ.Π., για την καθοδήγηση, τις συμβουλές, την υπομονή και το χρόνο που μου προσέφερε και να τονίσω πως χωρίς την συμβολή του δεν θα ήταν δυνατή η άρτια ολοκλήρωση αυτής της εργασίας. Επίσης θέλω να ευχαριστήσω και τα άλλα μέλη της τριμελούς εξεταστικής επιτροπής: τον κ. Κανελλόπουλο Βασίλειο, Επίκουρο Καθηγητή του Τομέα Μαθηματικών της Σ.Ε.Μ.Φ.Ε. του Ε.Μ.Π. και τον κ. Στεφανέα Πέτρο, Λέκτορα του Τομέα Μαθηματικών της Σ.Ε.Μ.Φ.Ε. του Ε.Μ.Π.

Abstract

The subject of this diploma thesis is the prime numbers. Specifically, in the first chapter we present a brief history, in which appears the definition of prime numbers, their main uses, when they started to concern the mathematicians, and why they are so interesting.

In the second chapter we present a more thorough history and all the great mathematicians who studied the prime numbers, such as: Euclid, Eratosthenes, Pierre de Fermat, Marin Mersenne and Leonhard Euler. We then refer some important theorems and the most important observations made, from antiquity to modern times.

In the third chapter we thoroughly study some of the basic ideas and theorems consisting the Theory of Prime Numbers. More precisely, the Fundamental Theorem of Arithmetics is stated and proved, it is shown that the prime numbers are infinite (6 proofs), the π-function is defined and proved, as long as the theorems of Bertrand, Fermat, Euler and Wilson.

In the fourth chapter some problems about prime numbers, which are unsolved until today, are presented. Particular emphasis is given to three of them which have occupied many mathematicians: the Riemann Hypothesis, the Goldbach Conjecture and the infinity of twin prime numbers.

In the fifth chapter we present some applications of prime numbers. Specifically, we present their applications on other fields of mathematics, on cryptography, on pseudorandom number generators and in nature.

Finally, in the sixth chapter we briefly describe the beauty of number theory which is why mathematicians have studied it in the past and will continue to study forever.

'...ο 317 είναι πρώτος όχι επειδή το πιστεύουμε ή επειδή τα μυαλά μας είναι διαμορφωμένα με τον ένα ή τον άλλο τρόπο, αλλά γιατί έτσι είναι, γιατί η μαθηματική πραγματικότητα είναι δομημένη με αυτόν τον τρόπο'

G.H.Hardy

'Απολογία ενός μαθηματικού'

Πίνακας περιεχομένων

1

Εισαγωγή

Μία μεγάλη Μαθηματική ενότητα που απασχολεί τους Μαθηματικούς και που έχει δημιουργήσει πολλά ερωτηματικά σχεδόν από την απαρχή της Ιστορίας των Μαθηματικών είναι αυτή των πρώτων αριθμών.

> *''... ο μοναδικός σκοπός της επιστήμης είναι η δόξα του ανθρωπίνου πνεύματος, και, κατ' αυτή την έννοια, ένα πρόβλημα της Θεωρίας Αριθμών έχει την ίδια αξία με ένα ερώτημα σχετικά με το σύστημα του κόσμου.''*
>
> Jacobi
> Επιστολή προς τον Legendre, 2 Ιουλίου 1830
> Collected Works of Jacobi, τόμ. 1, σελ. 454

(εμπνευσμένο από το ''Η γοητεία των Μαθηματικών'', Serge Lang, πανεπιστήμιο Yale, εκδόσεις Κάτοπτρο)

Ορισμός 1:

Ένας ακέραιος αριθμός μεγαλύτερος του ένα λέγεται *πρώτος αριθμός*, αν οι μόνοι θετικοί διαιρέτες του (παράγοντες) είναι το ένα και ο ίδιος ο αριθμός.

Για παράδειγμα, οι πρώτοι πρώτοι αριθμοί είναι οι 2, 3, 5, 7, 11, 13... Για τις ανάγκες της παρούσας εργασίας ορίζουμε και το σύνολο τον πρώτων αριθμών:

Ορισμός 2:

Ορίζεται σύνολο P ως εξής: $P = \{ p \in \mathbb{N} : p \ \textit{πρώτος} \}$.

Το Θεμελιώδες Θεώρημα της Αριθμητικής δείχνει ότι οι πρώτοι αριθμοί είναι οι

δομικοί λίθοι των θετικών ακεραίων: κάθε θετικός ακέραιος μπορεί να αναλυθεί κατά μοναδικό τρόπο ως γινόμενο πρώτων παραγόντων. Ο αριθμός 1 είναι μία ειδική περίπτωση γιατί δεν θεωρείται ούτε πρώτος ούτε σύνθετος [Wells 1986, p. 31]. Παρόλο που ο αριθμός 1 συνηθιζόταν να θεωρείται πρώτος [Goldbach 1742; Lehmer 1909, 1914; Hardy and Wright 1979, p. 11; Gardner 1984, pp. 86-87; Sloane and Plouffe 1995, p. 33; Hardy 1999, p. 46], χρειάζεται ειδική μεταχείριση σε τόσους πολλούς ορισμούς και εφαρμογές που αφορούν τους πρώτους αριθμούς μεγαλύτερους ή ίσους από το 2, που συνήθως τοποθετείται σε μια κατηγορία από μόνος του. Ένας καλός λόγος για να μην καλούμε το 1 πρώτο αριθμό είναι γιατί αν ο 1 ήταν πρώτος τότε το Θεμελιώδες Θεώρημα της Αριθμητικής θα έπρεπε να τροποποιηθεί γιατί η φράση 'κατά μοναδικό τρόπο' θα ήταν λάθος αφού για κάθε αριθμό: $n = 1n$. Ένας άλλος λόγος ελαφρώς λιγότερο διαφωτιστικός αλλά μαθηματικά ορθός σημειώνεται από τον Tietze [Tietze, 1965, p. 2], ο οποίος δηλώνει: «*Γιατί ο αριθμός 1 να αποτελεί εξαίρεση; Αυτό είναι ένα ερώτημα το οποίο συχνά θέτουν τα σχολιαρόπαιδα, αφού όμως είναι θέμα ορισμού δεν είναι αμφισβητήσιμο.*» Όπως πιο απλά επισημαίνει ο Derbyshire [Derbyshire, 2004, p. 33], «*Το 2 πληρεί τις προϋποθέσεις του (ως πρώτος) με ισορροπία. Το 1 όχι.*»

Οι πρώτοι αριθμοί έχουν πολλαπλές χρήσεις. Μελετήθηκαν για πρώτη φορά επειδή πολλές από τις ιδιότητες των αριθμών είναι στενά συνδεδεμένες με την ανάλυσή τους σε γινόμενο πρώτων παραγόντων. Εκτός από την απλή εσωτερική τους ομορφιά, οι πρώτοι αριθμοί είναι πλέον κλειδί για την επανάσταση του Internet, επειδή χρησιμοποιούνται για μια μεγάλη ποικιλία μεθόδων κρυπτογράφησης που είναι χρήσιμες για την ασφάλεια των συναλλαγών μέσω αυτού. Οι επιστήμονες της NASA μάλιστα αποφάσισαν πως είναι ένα καλό σημάδι της νοημοσύνης μας και έχουν συμπεριλάβει μια σύντομη λίστα των πρώτων αριθμών στις 'πλάκες' που έστειλαν στο διάστημα με το διαστημόπλοιο Voyager.

Το ενδιαφέρον για τους πρώτους αριθμούς όμως ξεκινάει από την αρχαιότητα. Πριν πάνω από 200 χρόνια.

Οι αρχαίοι Έλληνες απέδειξαν (περίπου το 300 π. Χ.) ότι υπάρχουν 'άπειρα πολλοί' πρώτοι και ότι έχουν ακανόνιστα διαστήματα (μπορούν να υπάρξουν αυθαίρετα μεγάλα κενά μεταξύ των διαδοχικών πρώτων αριθμών). Από την άλλη μεριά, τον $19^{ο}$ αιώνα δείχτηκε ότι ο αριθμός των πρώτων μικρότερων ή ίσων με n τείνει στο $\frac{n}{\ln n}$

$\log n$

(καθώς το n γίνεται πολύ μεγάλο). Έτσι μια πρόχειρη εκτίμηση για τον n-οστό πρώτο είναι $n \ln n$.

Το κόσκινο του Ερατοσθένη είναι ακόμη και σήμερα ένας από τους πιο αποδοτικούς τρόπους εύρεσης όλων των μικρών πρώτων αριθμών (για παράδειγμα, αυτών που είναι μικρότεροι του 1.000.000.000.000). Ωστόσο οι περισσότεροι από τους μεγαλύτερους πρώτους βρίσκονται χρησιμοποιώντας ειδικές περιπτώσεις του Θεωρήματος Lagrange από την θεωρία ομάδων.

Ένας από τους μεγαλύτερους μαθηματικούς όλων των εποχών, ο Carl Friedrich Gauss έγραψε:

> «*Το πρόβλημα του να διαχωρίσεις τους πρώτους αριθμούς από τους σύνθετους, καθώς και να αναλύσεις τους τελευταίους σε γινόμενο πρώτων παραγόντων είναι γνωστό ως το πιο σημαντικό και χρήσιμο στην Θεωρία Αριθμών. Έχει απασχολήσει την δημιουργία και την σοφία πολλών αρχαίων και σύγχρονων γεωμετρών σε τέτοιο βαθμό που θα ήταν περιττό να συζητήσω το θέμα εις βάθος… Επιπλέον η αξιοπρέπεια της ίδιας της επιστήμης φαίνεται να απαιτεί να εξερευνηθεί κάθε πιθανό μέσο για την επίλυση ενός προβλήματος τόσο κομψού και τόσο φημισμένου.*»
>
> [Carl Friedrich Gauss, Disquisitiones Arithmeticae, 1801]

Το 1984 ο Samuel Yates όρισε ως *τιτανικό πρώτο* κάθε πρώτο με τουλάχιστον 1000 ψηφία. Όταν εισήγαγε αυτόν τον όρο υπήρχαν γνωστοί μόνο 110 τέτοιοι πρώτοι. Σήμερα υπάρχουν πάνω από 1000 φορές περισσότεροι. Και καθώς οι υπολογιστές και η κρυπτογραφία δίνουν συνεχώς νέα έμφαση στην αναζήτηση για ακόμα μεγαλύτερους πρώτους, αυτός ο αριθμός θα συνεχίσει να μεγαλώνει.

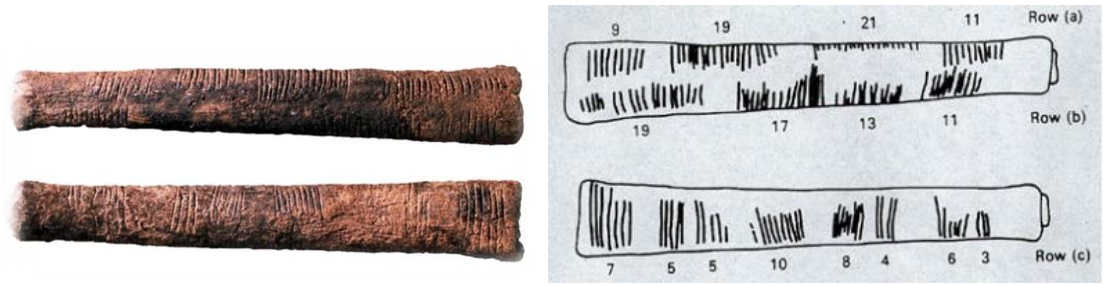
2

Αναλυτική Ιστορική Αναδρομή

Στο κεφάλαιο αυτό θα μελετήσουμε αναλυτικά πότε ξεκίνησε η ενασχόληση του ανθρώπου με τους πρώτους αριθμούς και πώς εξελίχτηκε μέσα στους αιώνες.

2.1 Παλαιολιθική Εποχή

Οι πρώτες ενδείξεις που έχουμε για τη σύλληψη της έννοιας των πρώτων αριθμών χρονολογούνται πολλές χιλιάδες χρόνια προ Χριστού. Το οστό Ishango ανακαλύφθηκε στο ομώνυμο χωριό στα σύνορα Ουγκάντας και Ζαΐρ το 1960 και φυλάσσεται σήμερα στο Βασιλικό Ινστιτούτο Φυσικών Επιστημών στις Βρυξέλλες. Σύμφωνα με τις πρώτες εκτιμήσεις χρονολογούνταν το 6500 π.Χ. αλλά μεταγενέστερες μελέτες το κατατάσσουν στην Παλαιολιθική Εποχή και τουλάχιστον πριν το 10000 π.Χ. Είναι ένα κόκκαλο περίπου 10 εκατοστών που φέρει τρεις σειρές από χαρακιές στην σχεδόν κυλινδρική επιφάνεια του. Αντίστοιχης ή μεγαλύτερης ηλικίας οστά έχουν βρεθεί στις γύρω ή και σε άλλες περιοχές, εντούτοις, είναι το πρώτο που στη μία του πλευρά είναι χαραγμένοι μόνο πρώτοι αριθμοί και συγκεκριμένα οι 11,13,17 και 19. Το άθροισμα αυτής της σειράς είναι 60 και το ίδιο ισχύει και για την δεύτερη, ενώ η τρίτη έχει άθροισμα 48, δυσκολεύοντας την ερμηνεία του μαθηματικού υποβάθρου και τη χρήση αυτού του οστού. Έχουν προταθεί διάφορες χρήσεις, όπως σεληνιακό ημερολόγιο ή ενδείξεις αριθμητικού συστήματος με βάση το 3 και το 4. Κανείς δεν μπορεί να βεβαιώσει αν οι χαρακιές ήταν τυχαίες ή οι χρήστες είχαν συλλάβει την έννοια των πρώτων αριθμών. Αν το είχαν κάνει πάντως θα ήταν οι πρώτοι.



Εικόνα 1: Οστό Ishango

2.2 Αιγύπτιοι-Βαβυλώνιοι

Τα στοιχεία είναι πιο πειστικά για τους αρχαίους Αιγύπτιους με την ιδιαίτερη έμφασή τους στα μοναδιαία κλάσματα (ή αλλιώς Αιγυπτιακά κλάσματα). Ο μαθηματικός πάπυρος του Rhynd, που χρονολογείται 4000 χρόνια πριν, ασχολείται με το να

εκφράσει τον αριθμό n (όπου n περιττός ακέραιος και $4 < n < 102$) ως άθροισμα μοναδιαίων κλασμάτων. Είναι πολύ πιο δύσκολο να φτιάξουμε αυτό το άθροισμα αν ο n είναι πρώτος.

Ενώ είναι οι Αιγύπτιοι αυτοί που παίρνουν τα εύσημα του πρώτου συστήματος αριθμών (το οποίο χρησιμοποιήθηκε και ήταν λειτουργικό) και των βασικών μαθηματικών, σίγουρα ένα μεγάλο ποσοστό για τα σύγχρονα μαθηματικά πρέπει να αποδοθεί στους αρχαίους λαούς της περιοχής της Μεσοποταμίας (που βρίσκεται περίπου όπου το σημερινό Ιράκ, δηλαδή τους Βαβυλώνιους). Ξεκινώντας ήδη από την περίοδο των Σουμέριων (3000-2400 π.Χ.) , η οποία φαίνεται να είναι παράλληλη με την περίοδο εισαγωγής των μαθηματικών στο παλιό βασίλειο της Αιγύπτου, υπάρχουν ενδείξεις ότι αυτοί οι πρώιμοι αρχαίοι πολιτισμοί της Μεσοποταμίας είχαν αναπτύξει ένα σύστημα 60-δικό (δηλαδή ένα σύστημα αρίθμησης με βάση το 60, που ακόμα χρησιμοποιείται στην μέτρηση του χρόνου αλλά και στην γεωμετρία του κύκλου). Ενώ τα αποδεικτικά στοιχεία για πραγματικά μαθηματικά έργα στην αρχαία Αίγυπτο είναι σπάνια, είναι αξιοσημείωτο το γεγονός ότι τα παραδείγματα των Βαβυλώνιων μαθηματικών είναι πάρα πολλά. Υπάρχουν εκατοντάδες πήλινα δισκία, ειδικά από την παλαιά περίοδο (2100-1600 π.Χ.), όπου οι αρχαιολόγοι έχουν βρει παραδείγματα κάποιων αρκετά προηγμένων μαθηματικών. Δισκία από αυτήν την περίοδο περιλαμβάνουν παραδείγματα πινάκων πολλαπλασιασμού, συστημάτων μέτρησης, πρώτων αριθμών, τετραγωνικών τύπων, γεωμετρίας, τριγωνομετρίας και πολλών άλλων. Είχαν ακόμη και πίνακες με Πυθαγόρειες τριάδες, δηλαδή τριάδες αριθμών που ικανοποιούν το Πυθαγόρειο Θεώρημα. Το σύστημα των μαθηματικών που αναπτύχθηκε από τους Βαβυλώνιους ήταν και διαφορετικό και πολύ κοντά στην πραγματικότητα, και ήταν βασισμένο σχεδόν αποκλειστικά σε ένα σύστημα κλασμάτων.

2.3 Αρχαίοι Έλληνες

Οι πρώτοι αριθμοί και οι ιδιότητες τους μελετήθηκαν για πρώτη φορά εκτενώς από τους αρχαίους Έλληνες. Οι μαθηματικοί της σχολής του Πυθαγόρα (500-300 π.Χ.) ενδιαφέρθηκαν για τις μυστικιστικές και αριθμολογικές ιδιότητες των αριθμών.

Αντιλαμβάνονταν την ιδέα των πρώτων και ενδιαφέρονταν για τους *τέλειους* και τους *φιλικούς* αριθμούς.

Ορισμός 3:
Τέλειος αριθμός λέγεται ο φυσικός αριθμός που το άθροισμα των διαιρετών του, πλην του ιδίου του αριθμού, ισούται με τον ίδιο τον αριθμό.

Ο μικρότερος τέλειος αριθμός είναι το 6. Οι διαιρέτες του 6 είναι οι 1,2,3 και το άθροισμα αυτών είναι ίσο με 6 (1+2+3=6). Άλλοι τέλειοι αριθμοί είναι οι 28=1+2+4+7+14, 496=1+2+4+8+16+31+62+124+248 και ο 8128. Αυτοί είναι και οι μόνοι γνωστοί τέλειοι κατά την αρχαιότητα.

Ορισμός 4:
Φιλικοί αριθμοί λέγεται ένα ζεύγος αριθμών όταν το άθροισμα των διαιρετών του ενός ισούται με τον άλλο και αντίστροφα.

Για παράδειγμα, το μικρότερο ζεύγος φιλικών αριθμών είναι οι 220 και 284.
Έως ότου γραφούν τα «Στοιχεία» του Ευκλείδη στα 300 π.Χ., αρκετά σημαντικά αποτελέσματα για τους πρώτους είχαν ήδη αποδειχθεί.

2.3.1 Ευκλείδης

Ο Ευκλείδης συνέλεξε τα σημαντικότερα Μαθηματικά μέχρι την εποχή του στο μνημειώδες έργο του «Στοιχεία». Τα «Στοιχεία» γράφτηκαν περί το 300 π.Χ. στην Αλεξάνδρεια και αποτελούν ίσως το σημαντικότερο μαθηματικό σύγγραμμα όλων των εποχών. Εκτόπισαν γρήγορα και ολοκληρωτικά όλες τις προγενέστερες εργασίες ανάλογου περιεχομένου με αποτέλεσμα να γνωρίζουμε για την ύπαρξη τους μόνο από μεταγενέστερους συγγραφείς. Με το 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 απόδειξη. Τα «Στοιχεία» αποτελούνται από 13 βιβλία και καλύπτουν την Στοιχειώδη Επιπεδομετρία, την Θεωρία Αριθμών, την Θεωρία των Ασύμμετρων και την Στερεομετρία. Τα βιβλία *VII*,

VIII, *IX* θεωρούνται σήμερα τα αρχαιότερα βιβλία Θεωρίας Αριθμών. Σε αυτά αναλύονται τα δύο σπουδαία συμπεράσματα στα οποία έφτασαν οι Αρχαίοι Έλληνες μαθηματικοί σχετικά με τους πρώτους αριθμούς.

Εικόνα 2: Ευκλείδης

Α) 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
Οἱ πρῶτοι ἀριθμοὶ πλείους εἰσὶ παντὸς τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν.
Οι πρώτοι αριθμοί είναι περισσότεροι από κάθε δεδομένο σύνολο πρώτων αριθμών.

1η Απόδειξη (Ευκλείδης)**:**
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 διαιρείται με τους α, β, γ). Προσθέτουμε στον ε την μονάδα μ. Προκύπτει ο αριθμός $\delta = \varepsilon + \mu$. Αν ο δ είναι πρώτος τότε η πρόταση αποδείχτηκε. Αν δεν είναι πρώτος τότε διαιρείται από έναν άλλο πρώτο 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, δηλαδή την μονάδα μ. Άτοπο.
Σε σύγχρονη μορφή θα λέγαμε ότι αποδείχτηκε το εξής Θεώρημα:
Έστω n δοσμένοι πρώτοι αριθμοί $p_1, p_2, ..., p_n$ τότε ο αριθμός $p_1 p_2 ... p_n + 1$ είναι πρώτος.

Άρα, οι πρώτοι είναι άπειροι. Η απόδειξη του Ευκλείδη αποτελεί ένα πραγματικό κόσμημα στην ιστορία όλων των Μαθηματικών και είναι ένα από τα κλασσικά 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 την πρώτη της εμφάνιση.

Β) Το Θεμελιώδες Θεώρημα της Αριθμητικής

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

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

Θεώρημα 1 (Θεμελιώδες Θεώρημα της Αριθμητικής):

Για κάθε φυσικό αριθμό n με $n>1$ υπάρχουν πρώτοι $p_1, p_2, ..., p_k$ και φυσικοί $a_1, a_2, ..., a_k$ τέτοιοι ώστε $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$.

Ο Davis (2007) αναφέρει ότι '*ενδεικτικό της ιδιοφυΐας των Ελλήνων είναι το γεγονός ότι είχαν συνειδητοποιήσει πως η μοναδικότητα της παραγοντοποίησης είναι ένα αποτέλεσμα που χρειαζόταν απόδειξη*'. Ο Ευκλείδης έφτασε πολύ κοντά στην απόδειξη, όπως θα τη διαβάζαμε σήμερα σε ένα βιβλίο Θεωρίας Αριθμών, στο ένατο βιβλίο των «Στοιχείων». Για να φτάσει εκεί βέβαια, χρησιμοποίησε τη θεωρία που είχε αναπτύξει στα βιβλία *VII* και *VIII*. Ας δούμε περιληπτικά πως ο Ευκλείδης φτάνει σε αυτό το μεγαλειώδες αποτέλεσμα.

Στους ορισμούς του βιβλίου *VII* ορίζει, μεταξύ άλλων, τους φυσικούς αριθμούς, τους άρτιους, τους περιττούς, τους πρώτους και σύνθετους αριθμούς, τους πρώτους και σύνθετους μεταξύ τους κ.α. Ας σταθούμε στους ορισμούς 3, 4 και 21.

Ορισμός VII.3
Μέρος ἐστὶν ἀριθμὸς ἀριθμοῦ ὁ ἐλάσσων τοῦ μείζονος, ὅταν καταμετρῇ τὸν μείζονα.
Ένας αριθμός λέγεται μέρος ενός μεγαλύτερου του αριθμού αν μπορούμε να μετρήσουμε τον δεύτερο με μονάδα μέτρησης τον πρώτο.

Ορισμός VII.4
Μέρη δέ, ὅταν μὴ καταμετρῇ.
Ένας αριθμός λέγεται μέρη ενός μεγαλύτερου του αριθμού αν δεν μπορούμε να μετρήσουμε τον δεύτερο με μονάδα μέτρησης τον πρώτο.

Για δύο φυσικούς αριθμούς α, β με $\alpha > \beta$, λοιπόν, αν υπάρχει ένας φυσικός κ τέτοιος ώστε $\alpha = \kappa\beta$ τότε ο β είναι μέρος του α , ενώ αν δεν υπάρχει τέτοιος, τότε ο β λέγεται μέρη του α .

Ορισμός VII.21 (ανάλογοι αριθμοί)**:**
Ἀριθμοὶ ἀνάλογόν εἰσιν, ὅταν ὁ πρῶτος τοῦ δευτέρου καὶ ὁ τρίτος τοῦ τετάρτου ἰσάκις ᾖ πολλαπλάσιος ἢ τὸ αὐτὸ μέρος ἢ τὰ αὐτὰ μέρη ὦσιν.
Ανάλογοι είναι αυτοί που ο πρώτος αποτελεί για τον δεύτερο το ίδιο πολλαπλάσιο ή το ίδιο μέρος ή τα ίδια μέρη, όπως αποτελεί ο τρίτος για τον τέταρτο.

Στο εξής θα συμβολίζουμε την αναλογία των αριθμών $\alpha, \beta, \gamma, \delta$ κατά τον ορισμό 21 με $\alpha : \beta = \gamma : \delta$.
Οι προτάσεις του βιβλίου *VII* ξεκινούν με τον περίφημο αλγόριθμο που πήρε το όνομα του από τον Ευκλείδη και μας δίνει τελικά τον Μέγιστο Κοινό Διαιρέτη (ΜΚΔ) δύο αριθμών (προτάσεις *VII.1* και *VII.2*).

Ο Ευκλείδειος Αλγόριθμος:
Δίνονται οι αριθμοί α, β με $\alpha > \beta$. Ας συμβολίσουμε με (α, β) τον Μέγιστο Κοινό Διαιρέτη των α, β . Αν ο β διαιρεί τον α τότε $(\alpha, \beta) = \beta$. Αν ο β δεν διαιρεί τον α τότε υπάρχουν ακέραιοι π_1, υ_1 τέτοιοι ώστε $\alpha = \beta\pi_1 + \upsilon_1$ με $\upsilon_1 < \beta$. Τότε αποδεικνύεται ότι $(\alpha, \beta) = (\beta, \upsilon_1)$. Αν ο υ_1 διαιρεί τον β τότε $(\alpha, \beta) = (\beta, \upsilon_1) = \upsilon_1$, αν όχι τότε η διαδικασία συνεχίζεται.

Ο Ευκλείδης αποδεικνύει στις προτάσεις *VII.1* και *VII.2* ότι η διαδικασία αυτή οδηγεί στην εύρεση του (α, β). Κατά την απόδειξη φτάνει σε ένα πολύ σημαντικό συμπέρασμα που όμως δεν φαίνεται να τονίζει ιδιαίτερα στην συνέχεια.

Πόρισμα:
Αν ένας αριθμός διαιρεί δύο αριθμούς τότε διαιρεί και τον Μέγιστο Κοινό Διαιρέτη τους.

Στην πρόταση *VII.3* λύνει το πρόβλημα εύρεσης του ΜΚΔ τριών αριθμών και στην πρόταση *VII.4* ουσιαστικά αποδεικνύει τον ορισμό 4. Η πρόταση *VII.6* είναι μια πρόταση κλειδί.

Πρόταση VII.6:
Ἐὰν ἀριθμὸς ἀριθμοῦ μέρη ᾖ, καὶ ἕτερος ἑτέρου τὰ αὐτὰ μέρη ᾖ, καὶ συναμφότερος συναμφοτέρου τὰ αὐτὰ μέρη ἔσται, ὅπερ ὁ εἷς τοῦ ἑνός.
Αν $\alpha : \beta = \gamma : \delta$ τότε $\alpha : \beta = (\alpha + \gamma) : (\beta + \delta)$

Η πρόταση *VII.13* είναι επίσης πολύ σημαντική

Πρόταση VII.13 (εναλλάξ)***:***
Ἐὰν τέσσαρες ἀριθμοὶ ἀνάλογον ὦσιν, καὶ ἐναλλὰξ ἀνάλογον ἔσονται.
Αν $\alpha : \beta = \gamma : \delta$ τότε $\alpha : \gamma = \beta : \delta$

Και βάσει αυτών φτάνουμε στην πρόταση *VII.20*

Πρόταση VII.20:
Οἱ ἐλάχιστοι ἀριθμοὶ τῶν τὸν αὐτὸν λόγον ἐχόντων αὐτοῖς μετροῦσι τοὺς τὸν αὐτὸν λόγον ἔχοντας ἰσάκις ὅ τε μείζων τὸν μείζονα καὶ ὁ ἐλάσσων τὸν ἐλάσσονα.
Αν κ, λ είναι οι μικρότεροι αριθμοί τέτοιοι ώστε $\kappa : \lambda = \gamma : \delta$ τότε ο κ διαιρεί τον γ και ο λ διαιρεί τον δ

η οποία χρησιμοποιείται στην απόδειξη της πρότασης 30, το ευκλείδειο λήμμα.

Πρόταση VII.30 (ευκλείδειο λήμμα)***:***
Ἐὰν δύο ἀριθμοὶ πολλαπλασιάσαντες ἀλλήλους ποιῶσί τινα, τὸν δὲ γενόμενον ἐξ αὐτῶν μετρῇ τις πρῶτος ἀριθμός, καὶ ἕνα τῶν ἐξ ἀρχῆς μετρήσει.
Αν ένας πρώτος διαιρεί ένα γινόμενο αριθμών τότε διαιρεί έναν από τους παράγοντες.

Με τη βοήθεια αυτού του λήμματος ο Ευκλείδης αποδεικνύει την πρόταση *IX.14.*

Πρόταση IX.14:
Ἐὰν ἐλάχιστος ἀριθμὸς ὑπὸ πρώτων ἀριθμῶν μετρῆται, ὑπ' οὐδενὸς ἄλλου πρώτου ἀριθμοῦ μετρηθήσεται παρὲξ τῶν ἐξ ἀρχῆς μετρούντων.
Αν δίνονται κάποιοι πρώτοι αριθμοί τότε ο ελάχιστος που διαιρείται από αυτούς, δεν διαιρείται από κανέναν άλλο πρώτο.

και φτάνει σε μία ισοδύναμη μορφή αυτού που ονομάζουμε σήμερα Θεμελιώδες Θεώρημα της Αριθμητικής.

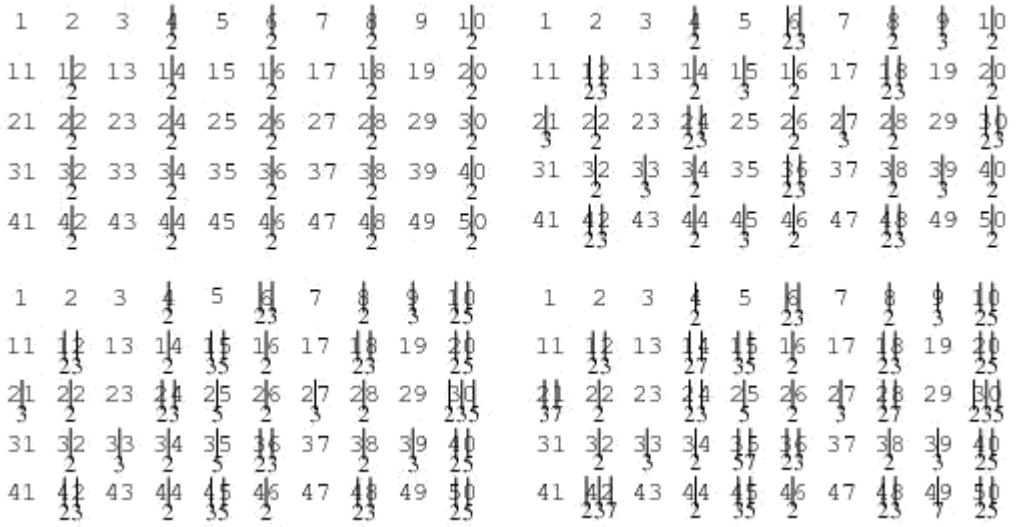
2.3.2 Ερατοσθένης

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 (280-210 π.Χ.) ‘Εισαγωγή στην Αριθμητική’.

Εικόνα 3: Ερατοσθένης

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.



Πίνακας 1: Το κόσκινο του Ερατοσθένη για τους φυσικούς ως το 50.

2.4 Ρωμαίοι – Άραβες

Με την κατάκτηση των Ελλήνων από τους Ρωμαίους, μεγάλο μέρος της γραπτής ελληνικής γνώσης μεταφράστηκε στα Λατινικά, ή τουλάχιστον διατηρήθηκε. Καθώς οι Έλληνες δίδασκαν στους Ρωμαίους τις γνώσεις τους, εκείνοι διέσωσαν την

ελληνική μαθηματική γνώση, δεν έκαναν όμως καμία περαιτέρω πρόοδο στη μελέτη των καθαρών μαθηματικών, όπως οι πρώτοι αριθμοί.

Οι Άραβες μαθηματικοί του Μεσαίωνα μελέτησαν το έργο των αρχαίων Ελλήνων μαθηματικών, με το επιπρόσθετο πλεονέκτημα ενός αριθμητικού συστήματος πιο επιδεκτικού σε υπολογιστική εργασία. Ο Thabit ibn Qurra, για παράδειγμα, απέδειξε τον $10^{ο}$ αιώνα την σχέση μεταξύ διαδοχικών πρώτων Thabit αριθμών και φιλικών αριθμών.

Ορισμός 5:

Πρώτοι Thabit αριθμοί ονομάζονται οι αριθμοί της μορφής $p_n = 3\times 2^n - 1.$

Ονομάστηκαν έτσι από τον Thabit ibn Qurra που ήταν ο πρώτος που τους μελέτησε. (Αργότερα μελετήθηκαν και από τον Fermat το 1636, από τον Descartes το 1638 και τέλος γενικεύτηκαν από τον Euler [Borho 1972])

Θεώρημα 2 (Thabit):

Για $n>1$*, θεωρούμε* $p_n = 3\times 2^n - 1$ *και* $q_n = 9\times 2^{2n-1}$*. Αν* p_{n-1}, p_n *και* q_n *είναι πρώτοι αριθμοί, τότε οι* $a = 2^n p_{n-1} p_n$ *και* $b = 2^n q_n$ *είναι φιλικοί αριθμοί.*

(***Σημείωση:*** Το άθροισμα των διαιρετών του a είναι μεγαλύτερο του a ενώ το άθροισμα των διαιρετών του b είναι μικρότερο του b.)

Εικόνα 4: Thabit ibn Qurra

Υπάρχει έπειτα μεγάλο κενό στην ιστορία των πρώτων αριθμών, ιδιαίτερα στα χρόνια του Μεσαίωνα.

2.5 Νεότερα χρόνια

2.5.1 Pierre de Fermat

Ο Pierre de Fermat γεννήθηκε το 1601 σε μια μικρή πόλη της Νοτιοδυτικής Γαλλίας, την Beaumont-de-Lomagne. Ήταν νομικός και εργαζόταν ως βασιλικός σύμβουλος στο τοπικό κοινοβούλιο. Με τα Μαθηματικά ασχολήθηκε ερασιτεχνικά, αν και η προσφορά του ήταν τεράστια καθορίζοντας σε μεγάλο βαθμό τις γνώσεις της εποχής και χαράσσοντας νέες πορείες σε διάφορους κλάδους όπως ο Διαφορικός Λογισμός, οι Πιθανότητες και η Αναλυτική Γεωμετρία. Διάσημος όμως έγινε χάρη στις εργασίες του στην Θεωρία Αριθμών. Απέδειξε μία εικασία του Albert Girard ότι κάθε πρώτος αριθμός της μορφής $4n+1$ μπορεί να γραφτεί με έναν μοναδικό τρόπο ως το άθροισμα δύο τετραγώνων και μπόρεσε να δείξει πώς κάθε αριθμός μπορεί να γραφτεί ως άθροισμα δύο τετραγώνων. Επινόησε μια νέα μέθοδο παραγοντοποίησης μεγάλων αριθμών την οποία απέδειξε παραγοντοποιώντας τον αριθμό $2027651281 = 44021 \times 46061$. Αν και ισχυριζόταν ότι είχε αποδείξεις για τις μαθηματικές του ανακαλύψεις, πολύ σπάνια τις κοινοποιούσε. Μετά το θάνατο του, το 1665, σε μια λατινική μετάφραση από τα 'Αριθμητικά' του Διόφαντου ανακαλύφθηκε ότι είχε γράψει την πιο διάσημη σημείωση στην ιστορία των Μαθηματικών.

> *'Είναι αδύνατον για έναν κύβο να γραφεί ως άθροισμα δύο κύβων, μια τέταρτη δύναμη ως άθροισμα δύο τέταρτων δυνάμεων ή γενικότερα για κάποιον αριθμό υψωμένο σε δύναμη μεγαλύτερη από το δύο να γραφεί ως άθροισμα δύο όμοιων δυνάμεων. Έχω μία πραγματικά υπέροχη απόδειξη γι' αυτό αλλά το περιθώριο είναι στενό για να την χωρέσει'*

Το αν είχε πράγματι την απόδειξη παραμένει άγνωστο αν και σήμερα θεωρείται εξαιρετικά απίθανο. Η εικασία αυτή, που ονομάστηκε το 'Τελευταίο Θεώρημα του Fermat', αποδείχτηκε μόλις το 1994 από τον Andrew Wiles, δηλαδή πάνω από 350 χρόνια μετά την διατύπωση του.

Θεώρημα 3 (Το Τελευταίο Θεώρημα του Fermat):

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

Εικόνα 5: Pierre de Fermat

Πρώτοι Αριθμοί του Fermat

Μελετάμε τώρα τους αριθμούς της μορφής $2^m+1,\ m\in\mathbb{N}$. Για να είναι ο αριθμός 2^m+1 πρώτος, πρέπει ο m να είναι δύναμη του 2, διότι αν είναι $m=rs$ με $r>1$ περιττό, τότε από την σχέση $2^m+1=\left(2^s+1\right)\left(2^{(r-1)s}-2^{(r-2)s}+\ldots-2^s+1\right)$ προκύπτει ότι ο 2^m+1 δεν είναι πρώτος αριθμός. Οι πρώτοι αριθμοί της μορφής $F_n=2^{2^n}+1,\ n\in\mathbb{N}$ καλούνται πρώτοι αριθμοί του Fermat, διότι έχουν μελετηθεί πρώτα από αυτόν. Για $n=0,1,2,3,4$ λαμβάνουμε τους πρώτους αριθμούς 3, 5, 17, 257, 65.537. Ο Fermat πίστευε ότι οι ομώνυμοι αριθμοί 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 το 1748 ο L.Euler ανακάλυψε ότι $F_5=2^{32}+1=641\cdot 6.700.417$. Αργότερα, το 1801, ο C.F.Gauss βρήκε μια απρόσμενη σχέση ανάμεσα στους πρώτους του Fermat και την κατασκευή κανονικών πολυγώνων με κανόνα και διαβήτη. Πρώτα, σε ηλικία 17 ετών, έδωσε μια 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.

Εικασία του Fermat:

Για όλους τους φυσικούς αριθμούς n, οι αριθμοί $2^{2^n}+1$ είναι πρώτοι.

Απόδειξη κατά της εικασίας του Fermat:

Έχουμε:

$$641 = 5\times 2^7 + 1 \Leftrightarrow 5\times 2^7 = 641-1 \Rightarrow 5^4 \times 2^{28} = (641-1)^4 = t\times 641+1,$$

για κάποιο $t \in \mathbb{Z}$

Επίσης

$$641 = 2^4 + 5^4 \Leftrightarrow 5^4 = 641 - 2^4,$$

Άρα λαμβάνουμε

$$\begin{aligned} \left(641-2^4\right)\times 2^{28} &= t\times 641+1 \Leftrightarrow \\ -2^{32} = \left(t-2^{28}\right)\times 641+1 &= s\times 641+1 \Leftrightarrow \\ 2^{32}+1 &= (-s)\times 641 \end{aligned}$$

Άρα

$$641 \mid 2^{2^5}+1$$

□

Η έρευνα για τους αριθμούς Fermat συνεχίστηκε με αμείωτο ενδιαφέρον. Ωστόσο, το να απαντηθεί αν ο F_6, ένας αριθμός 19 ψηφίων, είναι πρώτος ή σύνθετος ήταν αρκετά δύσκολο εγχείρημα για την εποχή. Ο Ρώσος I.M.Pervushin το 1877-78 έδειξε ότι οι F_{12} και F_{23} δεν είναι πρώτοι. Ο Fermat και όσοι πίστευαν ότι είχαν βρει μέσω των ομώνυμων αριθμών μια μηχανή παραγωγής πρώτων έκαναν λάθος. Λίγο αργότερα ο F.Landry μετά από επίπονη εργασία και σε ηλικία 82 ετών ανακοίνωσε την πλήρη παραγοντοποίηση του F_6. Το 1886 ανακαλύφθηκε ένας παράγοντας του F_{36}, το 1899 ένας του F_{11}, το 1903 του F_9 και του F_{18} και το 1905 του F_7, το 1906 του F_{73}, το 1909 του F_8. Το ερώτημα αν όλοι οι αριθμοί αυτού του είδους είναι πρώτοι είχε απαντηθεί. Ακόμα δεν είναι γνωστό αν υπάρχουν άπειροι αριθμοί Fermat. Επιπλέον, ούτε ένας καινούριος πρώτος αριθμός του Fermat διαφορετικός από αυτούς που έχουν περιγραφεί παραπάνω δεν έχει βρεθεί ακόμη.

2.5.2 Marin Mersenne

Ο Fermat αλληλογραφούσε με άλλους μαθηματικούς της εποχής του και ιδιαίτερα με

τον καλόγερο Marin Mersenne (1588-1648). Ο Mersenne, ο οποίος μόλις το 1647 είχε φτιάξει μια λίστα με όλους τους ακέραιους πρώτους αριθμούς n μικρότερους ή ίσους του 257, πίστευε πως ο τύπος $p=2^n-1$ παράγει πρώτους αριθμούς. Ωστόσο δεν έδωσε καμία απόδειξη και αργότερα η εικασία του αποδείχτηκε εν μέρει εσφαλμένη. Προς τιμήν του όμως οι αριθμοί αυτού του τύπου ονομάζονται *αριθμοί Mersenne* και συμβολίζονται M_n, γιατί πρώτος εκείνος τους μελέτησε.

Προφανώς ο τύπος του Mersenne δεν δίνει πάντα ως αποτέλεσμα πρώτους αριθμούς. Για παράδειγμα, αν ο n είναι σύνθετος τότε $n=kl$, όπου $k>1$ και $l>1$, και ο p διαιρείται από τους 2^k-1 και 2^l-1. Αλλά ακόμα και αν ο n είναι πρώτος αριθμός μπορεί να έχουμε ως αποτέλεσμα σύνθετο αριθμό, για παράδειγμα για $n=11$:

$2^{11}-1=2047=23\times 89$

Εικόνα 6: Marin Mersenne

Αυτό βέβαια δεν παρατηρήθηκε παρά το 1536. Για πολλά χρόνια αριθμοί αυτού του τύπου έδιναν τους πιο μεγάλους πρώτους αριθμούς που γνωρίζουμε. Ο αριθμός $M_{19}=2^{19}-1=524287$ αποδείχτηκε ότι είναι πρώτος από τον Pietro Cataldi (1548-1626) και αυτός ήταν ο πιο μεγάλος γνωστός πρώτος αριθμός για 200 χρόνια ώσπου ο Euler απέδειξε ότι ο M_{31} είναι πρώτος. Αυτό έθεσε ένα καινούριο ρεκόρ για άλλον έναν αιώνα ώσπου ο Édouard Lucas (1842-1891) έδειξε ότι ο M_{127} (που είναι ένας αριθμός με 39 ψηφία) είναι πρώτος και κράτησε το ρεκόρ ως τα χρόνια των ηλεκτρονικών υπολογιστών. Το 1952 οι αριθμοί Mersenne $M_{521}, M_{607}, M_{1279}, M_{2203}$ και M_{2281} αποδείχθηκαν ότι είναι πρώτοι από τον Raphael Mitchel Robinson (1911-1995) με την χρήση ενός πρώιμου υπολογιστή και η ηλεκτρονική εποχή είχε αρχίσει.

Μέχρι το 2005 είχαν βρεθεί 42 πρώτοι αριθμοί Mersenne. Ο μεγαλύτερος ήταν ο $M_{25964951}$ ο οποίος έχει 7.816.230 ψηφία. Ο μεγαλύτερος πρώτος αριθμός έως τις 25 Ιανουαρίου 2013, είναι ο $M_{57885161}$ ο οποίος έχει 17.425.170 ψηφία. (Mersenne Organization 2013)

Εικόνα 7: Pietro Cataldi

Εικόνα 8: Edouard Lucas

Εικόνα 9: Mitchel Robinson

Οι αριθμοί Mersenne έχουν ενδιαφέρον εξ' αιτίας της σχέσης τους με τους τέλειους αριθμούς. Ο ίδιος ο Ευκλείδης, στο βιβλίο του τα «Στοιχεία» που αναφέραμε προηγουμένως, απέδειξε το γεγονός ότι αν ένας πρώτος αριθμός p είναι της μορφής $p = 2^n - 1$, τότε ο αριθμός $\frac{p(p+1)}{2}$ είναι τέλειος.

Για παράδειγμα οι αριθμοί:

$$3 = 2^2 - 1,\ 7 = 2^3 - 1$$

είναι πρώτοι και συνεπώς οι αριθμοί

$$6 = \frac{3 \times 4}{2} = 1 + 2 + 3,$$

$$28 = \frac{7 \times 8}{2} = 1 + 2 + 4 + 7 + 14$$

είναι τέλειοι. Αρκετούς αιώνες αργότερα, ο Leonhard Euler (1707-1783) έδειξε ότι όλοι οι άρτιοι τέλειοι αριθμοί είναι του τύπου που εισήγαγε ο Ευκλείδης. Έτσι το ζήτημα του αν υπάρχουν πεπερασμένοι άρτιοι τέλειοι ακέραιοι μπορεί να περιοριστεί στο ζήτημα του αν υπάρχουν πεπερασμένοι άρτιοι αριθμοί Mersenne. Ακόμη δεν έχει βρεθεί λύση σε αυτό το πρόβλημα.

Παρακάτω παρατίθενται κάποιοι σχετικοί πίνακες και διαγράμματα.

Ρεκόρ πρώτων αριθμών πριν την εποχή των ηλεκτρονικών υπολογιστών				
Αριθμός	**Ψηφία**	**Χρονιά**	**Μαθηματικός**	**Μέθοδος**
$2^{17}-1$	6	1588	Cataldi	δοκιμαστικές διαιρέσεις
$2^{19}-1$	6	1588	Cataldi	δοκιμαστικές διαιρέσεις
$2^{31}-1$	10	1772	Euler	δοκιμαστικές διαιρέσεις
$\left(2^{59}-1\right)/179951$	13	1867	Landry	δοκιμαστικές διαιρέσεις
$2^{127}-1$	39	1876	Lucas	Ακολουθίες Lucas
$\left(2^{148}+1\right)/17$	44	1951	Ferrier	Θεώρημα του Proth(1878)

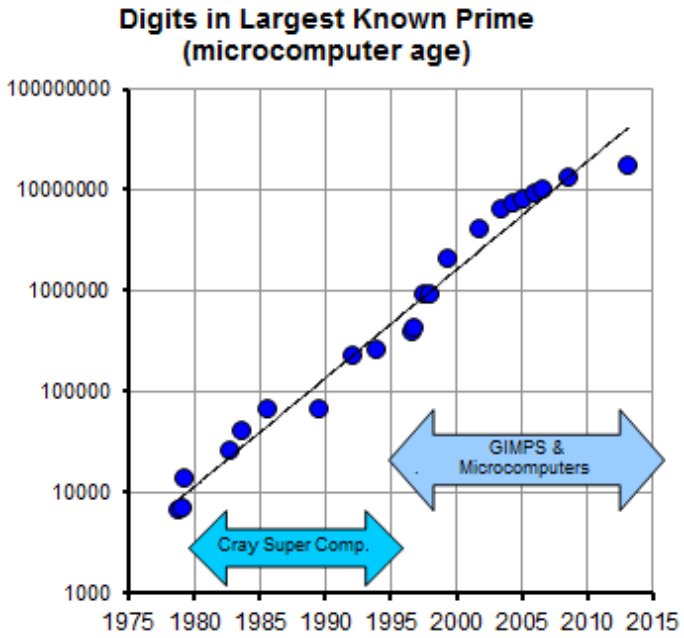
Πίνακας 2

Ρεκόρ πρώτων αριθμών την εποχή των ηλεκτρονικών υπολογιστών				
Αριθμός	**Ψηφία**	**Χρονιά**	**Η/Υ**	**Μαθηματικός**
$180\left(M_{127}\right)^2+1$	79	1951	EDSAC1	Miller & Wheeler
M_{521}	157	1952	SWAC	Robinson(Jan30)
M_{607}	183	1952	SWAC	Robinson(Jan30)
M_{1279}	386	1952	SWAC	Robinson(June25)
M_{2203}	664	1952	SWAC	Robinson(Oct7)
M_{2281}	687	1952	SWAC	Robinson(Oct9)
M_{3217}	969	1957	BESK	Riesel
M_{4423}	1332	1961	IBM7090	Hurwitz
M_{9689}	2917	1963	ILLIAC 2	Gillies
M_{9941}	2993	1963	ILLIAC 2	Gillies
M_{11213}	3376	1963	ILLIAC 2	Gillies

M_{19937}	6002	1971	IBM360/91	Tuckerman
M_{21701}	6533	1978	CDC Cyber 174	Noll & Nickel
M_{23209}	6987	1979	CDC Cyber 174	Noll
M_{44497}	13395	1979	Cray 1	Nelson & Slowinski
M_{86243}	25962	1982	Cray 1	Slowinski
M_{132049}	39751	1983	Cray X-MP	Slowinski
M_{216091}	65050	1985	Cray X-MP/24	Slowinski
$391581\times 2^{216193}-1$	65087	1989	Amdahl 1200	Amdahl Six
M_{756839}	227832	1992	Cray 2	Slowinski & Gage
M_{859433}	258716	1994	Cray C90	Slowinski & Gage
$M_{1257787}$	378632	1996	Cray T94	Slowinski & Gage
$M_{1398269}$	420921	1996	Pentium(90Mhz)	Amengaud,Woltman
$M_{2976221}$	895932	1997	Pentium(100Mhz)	Spence,Woltman
$M_{3021377}$	909526	1998	Pentium(200Mhz)	Clarkson,Woltman, Kurowski
$M_{6972593}$	2098960	1999	Pentium(350Mhz)	Hajratwala,Woltman, Kurowski
$M_{13466917}$	4053946	2001	AMD T-Bird(800Mhz)	Cameron,Woltman, Kurowski
$M_{20996011}$	6320430	2003	Pentium(2Ghz)	Shafer,Woltman, Kurowski
$M_{24036583}$	7235733	2004	Pentium 4(2.4Ghz)	Findley,Woltman, Kurowski
$M_{25964951}$	7816230	2005	Pentium 4(2.4Ghz)	Nowak,Woltman, Kurowski
$M_{30402457}$	9152052	2005	Pentium 4(2Ghz upgraded to 3Ghz)	Cooper,Boone, Woltman,Kurowski
$M_{32582657}$	9808358	2006	Pentium 4(3Ghz)	Cooper,Boone, Woltman,Kurowski

$M_{43111609}$	12978189	2008	Intel Core 2Duo E6600CPU(2.4Ghz)	E. Smith,Woltman, Kurowski
$M_{57885161}$	17425170	2013		Cooper,Woltman, Kurowski

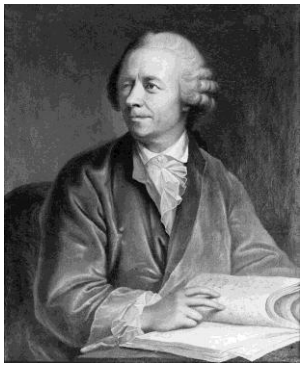
Πίνακας 3



Διάγραμμα 1: ο αριθμός των ψηφίων γνωστών πρώτων αριθμών μετά την ανακάλυψη του ηλεκτρονικού υπολογιστή

2.5.3 Leonhard Euler

Ο Euler γεννήθηκε στην Βασιλεία της Ελβετίας το 1707 αλλά έζησε τα περισσότερα χρόνια του στην Αγία Πετρούπολη και το Βερολίνο. Τα τελευταία δεκαεπτά χρόνια της ζωής του ήταν τυφλός αλλά αυτό δεν επηρέασε καθόλου την παραγωγικότητα του. Δημοσίευσε πολλές εκατοντάδες εργασίες και βιβλία. Η συνεισφορά του είναι μεγάλη σε πολλούς κλάδους των Μαθηματικών. Πέθανε στην Αγία Πετρούπολη το 1783.



Εικόνα 10: Leonhard Euler

Πολλοί μαθηματικοί της γενιάς των Fermat και Mersenne ασχολήθηκαν με τις ιδιότητες των πρώτων χωρίς όμως οι μέθοδοι τους να ταιριάζουν με την αρχαία ελληνική απόδειξη. Στις περισσότερες των περιπτώσεων οι μαθηματικοί δήλωναν, παρατηρούσαν ή είκαζαν σπάνια όμως αποδείκνυαν αυτά που υποστήριζαν. Αυτό εξηγεί μερικώς γιατί συχνά ο Fermat δεν έδινε λεπτομέρειες για τις αποδείξεις που ισχυριζόταν ότι βρήκε. Οι μαθηματικοί αρκούνταν σε περισσότερο πειραματικές προσεγγίσεις των θεμάτων. Ελπίδα προς την αντίθετη κατεύθυνση και αναβάθμιση της σημασίας της απόδειξης έδωσε ο Euler. Ο Euler κατάφερε να αποδείξει πολλές από τις παρατηρήσεις των Fermat και Mersenne και εμπλούτισε τη γνώση σχετικά με την θεωρία των πρώτων και των τέλειων αριθμών. Το πάθος του Euler για την Θεωρία Αριθμών ενεργοποιήθηκε από την αλληλογραφία του με τον ερασιτέχνη Γερμανό μαθηματικό Christian Goldbach. Όπως και ο Mersenne, ο Goldbach, έφτασε σε κάποια συμπεράσματα και έκανε υποθέσεις που όμως δεν κατάφερε να αποδείξει. Σύμφωνα με την πιο διάσημη, αναπόδεικτη έως σήμερα, εικασία που πήρε και το όνομα του '*κάθε άρτιος μπορεί να γραφτεί σαν άθροισμα δύο πρώτων*'.

Παρόλα αυτά σε καμία περίπτωση ο Euler δεν θα χαρακτηριζόταν ως φορμαλιστής. Βαθιά μέσα του ήταν πειραματικός μαθηματικός. Του άρεσε να κάνει υπολογισμούς και το μεγάλο του πάθος ήταν οι πρώτοι αριθμοί. Προσπάθησε να βρει όσο περισσότερους γίνεται και έκανε αξιοσημείωτες απόπειρες να ανακαλύψει τον πολυπόθητο κανόνα-τύπο που θα παρήγαγε πρώτους. Στην προσπάθεια του αυτή, ανακάλυψε ότι το πολυώνυμο $x^2 - x + 41$ δίνει πρώτους για $x = 1, 2, ..., 39$ όχι όμως και για $x = 40$. Μελέτησε τα παραπάνω πολυώνυμα και για άλλους πρώτους στην θέση του 41 και έβγαλε παρόμοια συμπεράσματα. Προσπάθησε να εκμεταλλευτεί αυτές τις ανακαλύψεις και να παράγει έστω και με περιορισμούς έναν απλό τύπο που

θα ‘γεννούσε’ πρώτους. Αυτό όμως φαίνεται ότι ήταν πάνω από τις δυνατότητες ακόμα και του ταλέντου του Euler. Πολλοί μεταγενέστεροι του προσπάθησαν να συνεχίσουν το έργο του, δούλεψαν πάνω στις στέρεες βάσεις που καθιέρωσε εκείνος, ανακαλύπτοντας εκ νέου την αξία της απόδειξης.

3

Στοιχεία Θεωρίας Πρώτων Αριθμών

Στο κεφάλαιο αυτό θα μελετηθούν κάποιες από τις βασικές ιδέες και θεωρήματα που αποτελούν τη σύγχρονη Θεωρία των Πρώτων Αριθμών. Στο πέρας των χρόνων τα αποτελέσματα και οι θεωρίες που έχουν δημοσιευτεί σε αυτόν τον κλάδο των μαθηματικών είναι αναρίθμητα. Η πλήρης καταγραφή τους, εκτός από πρακτικά αδύνατη, ξεφεύγει και από τους σκοπούς της παρούσας διπλωματικής εργασίας. Στο κεφάλαιο αυτό δίνονται τα βασικά αποτελέσματα που χρειάζεται ο αναγνώστης για να κατανοήσει τον θαυμαστό κόσμο των πρώτων αριθμών.

3.1 Θεμελιώδες Θεώρημα της Αριθμητικής

Όπως αναφέραμε και νωρίτερα, η πρώτη αναφορά στο Θεμελιώδες Θεώρημα της Αριθμητικής γίνεται από τον Ευκλείδη στα 'Στοιχεία'. Συγκεκριμένα στο βιβλίο *VII* βρίσκουμε τις εξής προτάσεις:

Πρόταση VII.30 *(ευκλείδειο λήμμα)**:***
Ἐὰν δύο ἀριθμοὶ πολλαπλασιάσαντες ἀλλήλους ποιῶσί τινα, τὸν δὲ γενόμενον ἐξ αὐτῶν μετρῇ τις πρῶτος ἀριθμός, καὶ ἕνα τῶν ἐξ ἀρχῆς μετρήσει.
Αν ένας πρώτος διαιρεί ένα γινόμενο αριθμών, τότε διαιρεί έναν από τους παράγοντες.

Πρόταση VII.32:
Ἅπας ἀριθμὸς ἤτοι πρῶτός ἐστιν ἢ ὑπὸ πρώτου τινὸς ἀριθμοῦ μετρεῖται.
Κάθε αριθμός είτε είναι πρώτος ή διαιρείται από κάποιον πρώτο.

Στην σύγχρονη μορφή του, το θεώρημα συναντάται για πρώτη φορά στο Άρθρο 16 του μνημειώδους έργου του Gauss 'Disquisitiones Arithmeticae'. Παρατίθεται η σύγχρονη διατύπωση του θεωρήματος καθώς και η απόδειξη του.

Θεώρημα 4 (Θεμελιώδες Θεώρημα της Αριθμητικής):
Κάθε φυσικός αριθμός $n>1$ *αναπαρίσταται σαν γινόμενο πρώτων αριθμών. Η αναπαράσταση αυτή είναι μοναδική αν αγνοήσουμε την διάταξη των παραγόντων του γινομένου.*

Σημείωση: Κάθε πρώτος θεωρείται γινόμενο πρώτων με έναν όρο. Ένας βασικός λόγος που δεν θεωρούμε ότι ο 1 είναι πρώτος είναι για να εξασφαλίσουμε την μοναδικότητα σε αυτό το Θεώρημα. Αλλιώς θα είχαμε για παράδειγμα $6=2\cdot 3=1\cdot 2\cdot 3$.
Πριν προχωρήσουμε στην απόδειξη του Θεμελιώδους Θεωρήματος της Αριθμητικής, θα δώσουμε την απόδειξη του Ευκλείδειου Λήμματος, το οποίο είναι απαραίτητο για την απόδειξη της μοναδικότητας.

Απόδειξη Ευκλείδειου Λήμματος:

Ως γνωστόν αν για τους φυσικούς a,b ισχύει $\text{ΜΚΔ}(a,b)=1$ τότε $\text{ΕΚΠ}(a,b)=ab$.

Έστω πρώτος p και $a,b\in\mathbb{N}$ τέτοιοι ώστε $p\mid ab$.

Υποθέτουμε ότι ο p δεν διαιρεί τον a. Θα δείξουμε ότι ο p διαιρεί τον b.

Έστω $m=\text{ΕΚΠ}(p,a)$. Αφού $\text{ΜΚΔ}(p,a)=1$ άρα $m=pa$.

Αφού $p\mid ab$ και $a\mid ab$, ο ab είναι κοινό πολλαπλάσιο των p και a.

Οπότε $m\mid ab\Leftrightarrow pa\mid ab\Leftrightarrow p\mid b$.

□

Μπορούμε τώρα να περάσουμε στην απόδειξη του Θεμελιώδους Θεωρήματος της Αριθμητικής.

Απόδειξη Θεμελιώδους Θεωρήματος της Αριθμητικής:

Δείχνουμε πρώτα με επαγωγή ως προς n ότι κάθε ακέραιος $n\geq 2$ γράφεται σαν γινόμενο πρώτων. Ο 2 είναι προφανώς γινόμενο πρώτων. Η επαγωγική υπόθεση είναι ότι κάθε $m\in\mathbb{N}$ με $2\leq m<n$ γράφεται σαν γινόμενο πρώτων. Αν ο n είναι πρώτος, δεν έχουμε τίποτα να δείξουμε. Αν ο n είναι σύνθετος, υπάρχουν $n_1,n_2\in\mathbb{N}$ με $2\leq n_1,n_2<n$ τέτοιοι ώστε $n=n_1n_2$. Από την επαγωγική υπόθεση, καθένας από τους n_1,n_2 αναπαρίσταται σαν γινόμενο πρώτων, οπότε το ίδιο ισχύει και για τον $n=n_1n_2$.

Δείχνουμε τώρα την μοναδικότητα. Ας υποθέσουμε ότι

$$n=p_1\ldots p_r=q_1\ldots q_s,$$

όπου οι $p_1\leq\ldots\leq p_r$ και $q_1\leq\ldots\leq q_s$ είναι πρώτοι. Αφού $p_1\mid q_1\ldots q_s$ το Ευκλείδειο Λήμμα δείχνει ότι υπάρχει $j\leq s$ τέτοιος ώστε $p_1\mid q_j$. Αφού οι p_1 και q_j είναι πρώτοι, αναγκαστικά έχουμε $p_1=q_j$. Ομοίως, αφού $q_1\mid p_1\ldots p_r$ υπάρχει $i\leq r$ τέτοιος ώστε $q_1\mid p_i$, απ' όπου παίρνουμε $q_1=p_i$. Παρατηρούμε ότι

$$p_1=q_j\geq q_1=p_i\geq p_1,$$

Άρα $p_1=q_1$. Τώρα η ισότητα των δύο αναπαραστάσεων παίρνει την μορφή

$$p_2\ldots p_r=q_2\ldots q_r.$$

Επαναλαμβάνοντας την ίδια διαδικασία πεπερασμένες το πλήθος φορές, συμπεραίνουμε ότι $r=s$ και $p_i=q_i$ για κάθε $i=1,\ldots,r$.

□

Ένας ενδιαφέρον εναλλακτικός τρόπος για να αποδείξουμε την μοναδικότητα της αναπαράστασης ως γινόμενο πρώτων παραγόντων, χωρίς να χρησιμοποιήσουμε το Λήμμα του Ευκλείδη είναι ο εξής:

Έστω $s>1$ ο ελάχιστος θετικός ακέραιος ο οποίος αναπαρίσταται από δύο διαφορετικά γινόμενα πρώτων. Αν ο s ήταν πρώτος αριθμός τότε η παραγοντοποίηση του θα ήταν μοναδική, με μοναδικό όρο τον εαυτό του. Άρα πρέπει να υπάρχουν τουλάχιστον δύο πρώτοι σε κάθε παραγοντοποίηση του s:

$$s = p_1 p_2 ... p_m = q_1 q_2 ... q_n .$$

Αν για κάποια $i \le m,\ j \le n$ ισχύει $p_i = q_j$, τότε ο $\frac{s}{p_i} = \frac{s}{q_j}$ θα ήταν θετικός ακέραιος μεγαλύτερος του 1 με δύο διαφορετικές αναπαραστάσεις ως γινόμενο πρώτων.

Αλλά $\frac{s}{p_i} < s$, που σημαίνει ότι ο s δεν είναι ο μικρότερος ακέραιος με δύο διαφορετικές αναπαραστάσεις ως γινόμενο πρώτων, όπως υποθέσαμε. Άρα κάθε p_i πρέπει να είναι διαφορετικό από κάθε q_j.

Χωρίς βλάβη της γενικότητας, υποθέτουμε $p_1 < q_1$. Θεωρούμε τον αριθμό

$$t = (q_1 - p_1)(q_2 ... q_n),$$

Και παρατηρούμε ότι $1 < q_2 \le t < s$. Άρα ο t έχει μοναδική αναπαράσταση. Έχουμε

$$t = q_1 (q_2 ... q_n) - p_1 (q_2 ... q_n) = s - p_1 (q_2 ... q_n) = p_1 \left((p_2 ... p_m) - (q_2 ... q_n) \right).$$

Εδώ ο $u = \left((p_2 ... p_m) - (q_2 ... q_n) \right)$ είναι θετικός, γιατί αν ήταν αρνητικός ή μηδέν τότε το ίδιο θα ήταν και το γινόμενο του με τον p_1, το οποίο όμως ισούται με t που είναι θετικός. Άρα ο u είτε ισούται με 1 ή αναπαρίσταται ως γινόμενο πρώτων. Σε κάθε περίπτωση, η ισότητα $t = p_1 u$ είναι μια αναπαράσταση του t, που ξέρουμε ότι είναι μοναδική, άρα ο p_1 εμφανίζεται στην αναπαράσταση του t.

Αν $(q_1 - p_1) = 1$ τότε η αναπαράσταση του t αποτελείται μόνο από q_j κάτι που αποκλείει την εμφάνιση του p_1. Άρα $(q_1 - p_1) \ne 1$ αλλά είναι θετικός, άρα

παραγοντοποιείται σε πρώτους: $(q_1 - p_1) = (r_1 ... r_l)$. Αυτό παράγει μια αναπαράσταση $t = (r_1 ... r_l)(q_2 ... q_n)$, η οποία ξέρουμε ότι είναι μοναδική.

Τώρα, το p_1 εμφανίζεται στην αναπαράσταση του t και δεν ισούται με κανένα q_j, άρα πρέπει να ισούται με κάποιο από τα r_i. Αλλά τότε $p_1 \mid r_1 ... r_l = (q_1 - p_1)$ και υπάρχει θετικός ακέραιος k τέτοιος ώστε $p_1 k = (q_1 - p_1) \Leftrightarrow p_1 (k+1) = q_1$ άτοπο, γιατί ο q_1 είναι πρώτος αριθμός. Άρα η υπόθεση ότι ο s έχει δύο διαφορετικές αναπαραστάσεις ως γινόμενο πρώτων αριθμών είναι λανθασμένη.

□

Το Θεμελιώδες Θεώρημα της Αριθμητικής καθιερώνει την σημασία των πρώτων αριθμών. Οι πρώτοι αριθμοί είναι οι δομικοί λίθοι με τους οποίους κατασκευάζονται όλοι οι αριθμοί, αφού κάθε αριθμός μπορεί να κατασκευαστεί από ένα γινόμενο πρώτων με μοναδικό τρόπο. Στη Θεωρία Αριθμών η μελέτη της δομής των αριθμών αποτελεί κεντρικό ζήτημα. Εξάλλου, ξέροντας την αναπαράσταση ενός αριθμού ως γινόμενο πρώτων, μπορούμε να παράγουμε όλους τους διαιρέτες του, πρώτους και σύνθετους. Το Θεμελιώδες Θεώρημα της Αριθμητικής έγινε η βάση για την διατύπωση αλλά και την απόδειξη πολλών άλλων θεωρημάτων στην διάρκεια των χρόνων.

3.2 Απειρία Πρώτων Αριθμών

Όπως είδαμε στο Κεφάλαιο 2, ο Ευκλείδης ήταν ο πρώτος που απέδειξε την απειρία των πρώτων αριθμών. Η απόδειξη του διακρίνεται για την απλότητα και την κομψότητα της. Παρ' όλα αυτά μέχρι σήμερα έχουν βρεθεί άλλες πέντε αποδείξεις για την απειρία των πρώτων, οι οποίες μας δίνουν και κάποιες επιπλέον πληροφορίες για την άπειρη ακολουθία των πρώτων αριθμών. Οι αποδείξεις αυτές είναι οι παρακάτω. [Martin Aigner, Günter M. Ziegler: *Proofs from the book.* Εκδόσεις: Springer, Third Edition, p. 3, 2000.]

2η Απόδειξη (Christian Goldbach, 1730, σε γράμμα του προς τον Leonhard Euler)**:**

Για τους αριθμούς του Fermat ισχύει ότι αφού $F_n \geq 2$ για κάθε $n \geq 2$, κάθε F_n έχει τουλάχιστον έναν πρώτο διαιρέτη q_n. Θα δείξουμε ότι

$$n \neq m \Rightarrow (F_n, F_m) = 1 \quad (1)$$

και ως εκ τούτου

$$n \neq m \Rightarrow q_n \neq q_m \quad (2)$$

Έπεται ότι οι q_n, $n \geq 0$, είναι διακεκριμένοι πρώτοι, το οποίο δείχνει την απειρία των πρώτων αριθμών.

Για την απόδειξη της (1) δείχνουμε πρώτα με επαγωγή το εξής: αν $n \geq 1$, τότε

$$\prod_{j=0}^{n-1} F_j = F_n - 2 \quad (3)$$

Η (3) ισχύει για $n = 1$: $F_0 = 3 = 5 - 2 = F_1 - 2$. Αν δεχτούμε ότι ισχύει για $n = k$, τότε

$$\begin{aligned} \prod_{j=0}^{k} F_j &= \left(\prod_{j=0}^{k-1} F_j \right) \cdot F_k = (F_k - 2) \cdot F_k \\ &= \left(2^{2^k} - 1\right)\left(2^{2^k} + 1\right) = 2^{2^{k+1}} - 1 \\ &= F_{k+1} - 2 \end{aligned}$$

Δηλαδή η (3) ισχύει για $n = k + 1$.

Έστω τώρα $0 \leq m < n$ και έστω d ένας κοινός θετικός διαιρέτης των F_m και F_n. Τότε,

$$d \mid F_m \mid \prod_{j=0}^{n-1} F_j = F_n - 2$$

Άρα $d \mid F_n$ και $d \mid F_n - 2$. Έπεται ότι $d \mid 2$, άρα $d = 1$ ή $d = 2$. Αφού όλοι οι αριθμοί του Fermat είναι περιττοί, ο d δεν μπορεί να ισούται με 2. Άρα, $(F_n, F_m) = 1$.

□

Ορισμός 6:

Ορίζουμε την συνάρτηση $\pi : \mathbb{R} \to \mathbb{N}$ ως: $\pi(x) := \#\{p \leq x : p \in P\}$ το πλήθος των πρώτων αριθμών που είναι μικρότεροι ή ίσοι από τον πραγματικό αριθμό x.

3η Απόδειξη **(**Leonhard Euler**):**

Θεωρούμε την (ενδεχομένως πεπερασμένη) ακολουθία των πρώτων αριθμών σε

αύξουσα διάταξη: $p_1 < p_2 < ... < p_k < ....$ Αν $f(t) = \frac{1}{t}$, τότε για κάθε $n \geq 2$ και για κάθε $n \leq x < n+1$ έχουμε

$$\ln x = \int_1^x \frac{1}{t} dt \leq \int_1^2 \frac{1}{t} dt + \int_2^3 \frac{1}{t} dt + ... + \int_n^{n+1} \frac{1}{t} dt \leq 1 + \frac{1}{2} + ... + \frac{1}{n} \leq \sum_{m \in A(x)} \frac{1}{m}$$

όπου $A(x)$ είναι το σύνολο όλων των φυσικών αριθμών που όλοι οι πρώτοι διαιρέτες τους είναι μικρότεροι ή ίσοι από x. Το σύνολο $A(x)$ περιγράφεται με την βοήθεια του θεμελιώδους θεωρήματος της αριθμητικής:

$$A(x) = \left\{ n = \prod_{k=1}^{\pi(x)} p_k^{\,r_k} : r_k \geq 0 \right\}$$

Χρησιμοποιώντας την επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση ελέγχουμε ότι

$$\sum_{m \in A(x)} \frac{1}{m} = \prod_{k=1}^{\pi(x)} \left(\sum_{s=0}^{\infty} \frac{1}{p_k^{\,s}} \right)$$

Στην παρένθεση έχουμε μια γεωμετρική σειρά με λόγο $\frac{1}{p_k}$, άρα

$$\sum_{s=0}^{\infty} \frac{1}{p_k^{\,s}} = \frac{1}{1 - \frac{1}{p_k}} = \frac{p_k}{p_k - 1}$$

Έπεται ότι

$$\ln x \leq \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}$$

Από την προφανή ανισότητα $p_k \geq k+1$ βλέπουμε ότι

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k}$$

Επιστρέφοντας στην προηγούμενη ανισότητα παίρνουμε

$$\ln x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1$$

Η $\ln x$ δεν είναι φραγμένη, άρα καταλήγουμε ότι ούτε η $\pi(x)$ είναι φραγμένη, και έτσι συμπεραίνουμε ότι υπάρχουν άπειροι πρώτοι αριθμοί.

□

4η Απόδειξη (Harry Furstenberg, 1955)**:**

Θεωρούμε την ακόλουθη τοπολογία στο σύνολο $\mathbb{Z}$ των ακεραίων αριθμών. Για $a,b\in\mathbb{Z},\ b>0$, θέτουμε

$$N_{a,b}=\{a+nb:n\in\mathbb{Z}\}$$

Κάθε σύνολο $N_{a,b}$, είναι μια άπειρη αριθμητική πρόοδος που εκτείνεται και στους θετικούς και στους αρνητικούς αριθμούς. Καλούμε ένα σύνολο $O\subseteq\mathbb{Z}$ ανοικτό αν είτε το O είναι κενό, ή αν για κάθε $a\in O$ υπάρχει κάποιο $b>0$ με $N_{a,b}\subseteq O$. Προφανώς η ένωση ανοικτών συνόλων είναι ανοικτό σύνολο. Αν O_1,O_2 είναι ανοικτά και $a\in O_1\cap O_2$ με $N_{a,b_1}\subseteq O_1$ και $N_{\alpha,b_2}\subseteq O_2$, τότε $a\in N_{a,b_1b_2}\subseteq O_1\cap O_2$. Έτσι καταλήγουμε ότι κάθε πεπερασμένη τομή ανοικτών συνόλων είναι ανοικτή. Έτσι αυτή η οικογένεια ανοικτών συνόλων επάγει μια καλώς ορισμένη τοπολογία στο $\mathbb{Z}$.

Εδώ σημειώνουμε δύο δεδομένα:

(A) Ένα μη κενό ανοικτό σύνολο είναι άπειρο.

(B) Κάθε σύνολο $N_{a,b}$ είναι κλειστό.

Πράγματι, το (A) έπεται από τον ορισμό. Για το (B) παρατηρούμε ότι

$$N_{a,b}=\mathbb{Z}\setminus\bigcup_{i=1}^{b-1}N_{a+i,b}$$

το οποίο αποδεικνύει ότι το $N_{a,b}$ είναι συμπλήρωμα ενός ανοικτού συνόλου και άρα κλειστό.

Αφού τώρα, κάθε αριθμός $n\neq1,-1$ έχει έναν πρώτο διαιρέτη p και άρα περιέχεται στο $N_{0,p}$, καταλήγουμε ότι

$$\mathbb{Z}\setminus\{1,-1\}=\bigcup_{p\in P}N_{0,p}$$

Τώρα αν το P ήταν πεπερασμένο, τότε η $\bigcup_{p\in P}N_{0,p}$ θα ήταν μία πεπερασμένη ένωση κλειστών συνόλων (από το (B)) και άρα κλειστό. Συνεπώς, το σύνολο $\{1,-1\}$ θα ήταν ανοικτό κατά παράβαση του (A).

□

5η Απόδειξη (Paul Erdős, ~1950)**:**

Αυτή η απόδειξη δεν δείχνει μόνο ότι υπάρχουν άπειροι πρώτοι αριθμοί, αλλά επίσης ότι η σειρά $\sum_{p\in P}\frac{1}{p}$ αποκλίνει. Η πρώτη απόδειξη αυτού του σημαντικού αποτελέσματος δόθηκε από τον Euler, αλλά αυτή η απόδειξη από τον Erdős είναι πραγματικά πολύ όμορφη.

Έστω $P=\{p_1,p_2,...\}$ το σύνολο των πρώτων αριθμών, τους οποίους θεωρούμε σε αύξουσα διάταξη. Ας υποθέσουμε ότι η σειρά $\sum_{i\geq 1}\frac{1}{p_i}$ συγκλίνει. Τότε, υπάρχει φυσικός αριθμός k με την ιδιότητα

$$\sum_{i\geq k+1}\frac{1}{p_i}<\frac{1}{2}$$

Θα λέμε ότι οι $p_1,...,p_k$ είναι οι 'μικροί' πρώτοι, ενώ οι $p_{k+1},...$ είναι οι 'μεγάλοι' πρώτοι. Για κάθε φυσικό αριθμό N έχουμε

$$\sum_{i\geq k+1}\frac{N}{p_i}<\frac{N}{2}$$

Γράφουμε N_b για το πλήθος των φυσικών $n\leq N$ που έχουν τουλάχιστον έναν μεγάλο πρώτο διαιρέτη, και N_s για το πλήθος των φυσικών $n\leq N$ που όλοι οι πρώτοι διαιρέτες τους είναι μικροί. Από τον ορισμό των N_b και N_s έχουμε

$N_b+N_s=N$

Παρατηρούμε ότι το πλήθος των φυσικών $n\leq N$ που είναι πολλαπλάσια κάποιου πρώτου p_i ισούται με το ακέραιο μέρος $\left[\frac{N}{p_i}\right]$. Άρα χρησιμοποιώντας και την

$$\sum_{i\geq k+1}\frac{1}{p_i}<\frac{1}{2}$$

παίρνουμε

$$N_b\leq\sum_{i\geq k+1}\left[\frac{N}{p_i}\right]\leq\sum_{i\geq k+1}\frac{N}{p_i}<\frac{N}{2}$$

Ας δούμε τώρα πώς μπορεί κανείς να φράξει τον N_s. Κάθε φυσικός $n\leq N$ που έχει μόνο μικρούς πρώτους διαιρέτες, γράφεται στην μορφή $n=a_nb_n^{\,2}$, όπου ο a_n είναι γινόμενο διακεκριμένων πρώτων. Αφού αυτοί οι πρώτοι είναι κάποιοι από τους

$p_1,...,p_k$, έχουμε το πολύ 2^k επιλογές για τον a_n. Επιπλέον, $b_n^2 \le n \le N$ άρα $b_n \le \sqrt{N}$. Δηλαδή, έχουμε το πολύ $\sqrt{N}$ επιλογές για τον b_n. Έπεται ότι

$$N_s \le 2^k \sqrt{N}$$

Από τις προηγούμενες τρεις σχέσεις παίρνουμε

$$N = N_b + N_s \le \frac{N}{2} + 2^k \sqrt{N}$$

δηλαδή,

$$\sqrt{N} \le 2^{k+1}$$

Αυτό όμως δεν μπορεί να ισχύει για κάθε φυσικό αριθμό N: τότε το $\mathbb{N}$ θα ήταν άνω φραγμένο. Καταλήξαμε σε άτοπο, άρα η σειρά $\sum_{i\ge1} \frac{1}{p_i}$ αποκλίνει. Ειδικότερα, υπάρχουν άπειροι πρώτοι.

□

Για την 6η απόδειξη χρειαζόμαστε το Θεώρημα Lagrange και γι' αυτό το διατυπώνουμε εδώ.

Θεώρημα 5 (Θεώρημα Lagrange):
Αν G είναι μια πεπερασμένη ομάδα και U μία υποομάδα του, τότε το $|U|$ διαιρεί το $|G|$.

6η Απόδειξη (Αγνώστου)**:**
Υποθέτουμε ότι το P είναι πεπερασμένο και ο p είναι ο μεγαλύτερος πρώτος. Θεωρούμε τους αριθμούς $2^p - 1$ (Αριθμοί Mersenne, βλ. §2.5.2) και θα δείξουμε ότι κάθε πρώτος διαιρέτης q των $2^p - 1$ είναι μεγαλύτερος του p, το οποίο παράγει το επιθυμητό μας αποτέλεσμα. Άρα έχουμε ότι $2^p \equiv 1 (\mathrm{mod}\, q)$. Αφού ο p είναι πρώτος, το στοιχείο 2 είναι τάξης p στην πολλαπλασιαστική ομάδα $\mathbb{Z}_q \setminus \{0\}$ του σώματος $\mathbb{Z}_q$. Αυτή η ομάδα έχει $q-1$ στοιχεία. Από το Θεώρημα Lagrange έχουμε ότι η τάξη κάθε στοιχείου διαιρεί την τάξη της ομάδας και έτσι εδώ $p \mid q-1$ άρα $p < q$.

□

3.3 Η συνάρτηση π(x) και το Θεώρημα των Πρώτων Αριθμών

Κοιτάζοντας καλύτερα την απόδειξη του Christian Goldbach για την απειρία των πρώτων αριθμών παρατηρούμε το εξής: αν $p_1 < p_2 < ... < p_n < p_{n+1} < ...$ είναι η άπειρη ακολουθία των πρώτων αριθμών, τότε:

$$p_n \le F_{n-1} = 2^{2^{n-1}} + 1$$

για κάθε $n \in \mathbb{N}$. Πράγματι, οι $F_0, F_1, ..., F_{n-1}$ έχουν n διακεκριμένους πρώτους διαιρέτες $p_{k_1}, ..., p_{k_n}$, άρα

$$p_n \le \max\left\{p_{k_1}, ..., p_{k_n}\right\} \le \max\left\{F_0, F_1, ..., F_{n-1}\right\} = F_{n-1}$$

Η παρατήρηση αυτή μας οδηγεί στον ορισμό μιας συνάρτησης $\pi : \mathbb{R} \to \mathbb{R}$, με $\pi(x) =$ το πλήθος των πρώτων αριθμών $p \le x$.

Η π είναι αύξουσα, και βέβαια $\pi(x) = 0$ αν $x < 2$. Παρατηρούμε ότι: αν $x \ge 2$ και αν $n = n(x)$ είναι ο μεγαλύτερος μη αρνητικός ακέραιος για τον οποίο $2^{2^n} + 1 \le x$, τότε

$$\pi(x) \ge \pi\left(2^{2^n} + 1\right) \ge n + 1$$

Από την άλλη πλευρά, $2^{2^{n+1}} \ge x$ άρα $\log_2\left(\log_2 x\right) \le n + 1$. Έχουμε λοιπόν το εξής κάτω φράγμα για την $\pi(x)$.

<u>Πρόταση 1:</u>
Για κάθε πραγματικό αριθμό $x \ge 2$ ισχύει η ανισότητα

$$\pi(x) \ge \log_2\left(\log_2 x\right)$$

(Ειδικότερα, $\pi(x) \to +\infty$ καθώς το $x \to +\infty$, άρα υπάρχουν άπειροι πρώτοι αριθμοί.)

Με άλλα λόγια η δεύτερη απόδειξη μας δίνει επιπλέον πληροφορίες για το πλήθος των πρώτων αριθμών σε ένα διάστημα της μορφής $[0, x]$, όπου x είναι ένας «μεγάλος» θετικός πραγματικός αριθμός.

Στην τρίτη απόδειξη, του Leonhard Euler, βρίσκουμε ένα ακόμα καλύτερο κάτω φράγμα για την συνάρτηση $\pi(x)$:

Πρόταση 2:
Για κάθε πραγματικό αριθμό $x \geq 2$ ισχύει η ανισότητα

$$\pi(x) \geq \ln x - 1$$

(Ειδικότερα, $\pi(x) \to +\infty$ καθώς το $x \to +\infty$, άρα υπάρχουν άπειροι πρώτοι αριθμοί.)

Το πρόβλημα της ασυμπτωτικής συμπεριφοράς της συνάρτησης $\pi(x)$ καθώς το $x \to +\infty$ απασχόλησε έντονα τους μαθηματικούς κατά τον $19^{ο}$ αιώνα. Θα παραθέσουμε εδώ άλλη μια απόδειξη του θεωρήματος της απειρίας των πρώτων αριθμών από τον Euler από την οποία προκύπτουν σημαντικά συμπεράσματα γι αυτή την συμπεριφορά της συνάρτησης $\pi(x)$.

7η Απόδειξη (Leonhard Euler)**:**
Υποθέτουμε ότι το σύνολο P των πρώτων αριθμών είναι πεπερασμένο και θα καταλήξουμε σε άτοπο. Έστω

$$P = \{p_1, p_2, ..., p_s\}$$

Για κάθε πρώτο αριθμό p ισχύει:

$$\frac{1}{1-\frac{1}{p}} = \sum_{n=0}^{\infty} \frac{1}{p^n}$$

Έχουμε συνεπώς:

$$\frac{1}{1-\frac{1}{p_1}} \times \frac{1}{1-\frac{1}{p_2}} \times ... \times \frac{1}{1-\frac{1}{p_s}} = \left(\sum_{n=0}^{\infty} \frac{1}{{p_1}^n}\right)\left(\sum_{n=0}^{\infty} \frac{1}{{p_2}^n}\right)...\left(\sum_{n=0}^{\infty} \frac{1}{{p_s}^n}\right)$$

$$= \sum_{n_1, n_2, ..., n_s = 0}^{\infty} \frac{1}{{p_1}^{n_1} {p_2}^{n_2} ... {p_s}^{n_s}} = \sum \frac{1}{n}$$

Στο τελευταίο άθροισμα το n διατρέχει όλους τους φυσικούς αριθμούς, οι οποίοι εκφράζονται ως γινόμενα των πρώτων αριθμών $p_1, p_2, ..., p_s$ και καθένα ακριβώς μία φορά. Επειδή δε κάθε φυσικός αριθμός, διάφορος του 0, έχει μια μονοσήμαντη ανάλυση σε γινόμενο πρώτων αριθμών, προκύπτει ότι στο άθροισμα

$$\sum \frac{1}{n}$$

το n διατρέχει όλους τους διάφορους από το 0 φυσικούς αριθμούς, ήτοι

$$\prod_{i=1}^{s} \frac{1}{p_i} = \sum_{n=1}^{\infty} \frac{1}{n} = +\infty$$

το οποίο είναι άτοπο, δεδομένου ότι ο πραγματικός αριθμός

$$\prod_{i=1}^{s} \frac{1}{p_i}$$

είναι διάφορος του $+\infty$.

□

Από την απόδειξη αυτή του Euler προκύπτει

$$\prod_{p} \frac{1}{1-\frac{1}{p}} = +\infty \Rightarrow \prod_{p} \left(1-\frac{1}{p}\right) = 0$$

Επίσης ισχύει ότι

$$\sum_{p} \frac{1}{p} = +\infty$$

Με την βοήθεια των σχέσεων αυτών αποδεικνύεται το παρακάτω θεώρημα.

Θεώρημα 6:
Ισχύει

$$\lim_{x \to +\infty} \frac{\pi(x)}{x} = 0$$

Απόδειξη:
Έστω $p_1, p_2, ..., \mathrm{p}_s$ οι s πρώτοι αριθμοί. Θεωρούμε έναν θετικό πραγματικό αριθμό x και το σύνολο

$$A = \{1, 2, ..., [x]\}$$

Όπου $[x]$ παριστάνει το ακέραιο μέρος του x, δηλαδή τον μέγιστο ακέραιο αριθμό, ο οποίος είναι μικρότερος ή ίσος του x. Στο σύνολο A διαγράφουμε τα πολλαπλάσια των $p_1, p_2, ..., p_s$, οπότε θα μείνουν ο 1, οι πρώτοι αριθμοί $p_{s+1}, p_{s+2}, ...$ και τα

γινόμενα δυνάμεων αυτών. Το πλήθος των πολλαπλασίων του p_i στο A είναι $\left[\frac{x}{p_i}\right]$, διότι από την σχέση

$$x = p_i y + r, 0 \le r < p_i$$

Προκύπτει $\left[\frac{x}{p_i}\right] = y$. Επίσης το πλήθος των πολλαπλασίων του $p_i p_j$ στο A είναι $\left[\frac{x}{p_i p_j}\right]$, του $p_i p_j p_k$ είναι $\left[\frac{x}{p_i p_j p_k}\right]$ κ.ο.κ. Μετά τη διαγραφή των πολλαπλασίων των $p_1, p_2, ..., p_s$ θα μένουν στο σύνολο A:

$$[x] - \sum_{1\le i\le s}\left[\frac{x}{p_i}\right] + \sum_{1\le i<j\le s}\left[\frac{x}{p_i p_j}\right] - ... + (-1)^s\left[\frac{x}{p_1 p_2 \cdots p_s}\right]$$

αριθμοί. Συνεπώς προκύπτει

$$\pi(x) \le s - 1 + [x] - \sum_{1\le i\le s}\left[\frac{x}{p_i}\right] + ... + (-1)^s\left[\frac{x}{p_1 p_2 \cdots p_s}\right]$$

Το $\le$ εξηγείται από το γεγονός ότι στο A εκτός των πρώτων αριθμών $p_{s+1}, p_{s+2}, ...$ υπάρχουν και τα γινόμενα δυνάμεων αυτών.

Αν στην παραπάνω σχέση απαλείψουμε τις τετραγωνικές αγκύλες, δηλαδή αν τα ακέραια μέρη των αριθμών τα αντικαταστήσουμε με τους ίδιους τους αριθμούς, το συνολικό σφάλμα θα είναι μικρότερο ή το πολύ ίσο με τον αριθμό

$$1 + \binom{s}{1} + ... + \binom{s}{s} = (1+1)^s = 2^s$$

Άρα λαμβάνουμε

$$\pi(x) < s + 2^s + x - \sum_{1\le i\le s}\frac{x}{p_i} + \sum_{1\le i\le j\le s}\frac{x}{p_i p_j} - ... + (-1)^s\frac{x}{p_1 p_2 \cdots p_s}$$

$$= s + 2^s + x\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_s}\right)$$

Επειδή ισχύει

$$\prod_p\left(1 - \frac{1}{p}\right) = 0$$

Προκύπτει ότι για κάθε $\varepsilon > 0$ υπάρχει φυσικός αριθμός $s_0 = s_0(\varepsilon)$, τέτοιος ώστε για

κάθε $s \geq s_0$ να ισχύει

$$\pi(x) < s + 2^s + x\varepsilon$$

Εκλέγουμε ένα x_0, για το οποίο να ισχύει

$$s_0 + 2^{s_0} \leq \varepsilon x_0$$

οπότε για κάθε $x > x_0$ θα έχουμε

$$\pi(x) < s_0 + 2^{s_0} + x\varepsilon < 2x\varepsilon$$

δηλαδή

$$\frac{\pi(x)}{x} < 2\varepsilon \quad \forall \varepsilon > 0$$

Άρα προκύπτει

$$\lim_{x \to +\infty} \frac{\pi(x)}{x} = 0$$

□

Τώρα μπορούμε να αποδείξουμε και το παρακάτω θεώρημα.

Θεώρημα 7:

Η πιθανότητα να είναι ένας φυσικός αριθμός πρώτος υπάρχει και είναι ίση με το μηδέν.

Απόδειξη:

Αρκεί να αποδείξουμε ότι

$$\lim_{x \to +\infty} \frac{\pi(x)}{[x]} = 0$$

Από την σχέση

$$[x] \leq x < [x] + 1$$

προκύπτει για $x \geq 1$

$$1 \leq \frac{x}{[x]} < 1 + \frac{1}{[x]}$$

και από την σχέση αυτή φαίνεται αμέσως ότι

$$\lim_{x \to +\infty} \frac{x}{[x]} = 1$$

Από τις σχέσεις

$$\lim_{x\to+\infty}\frac{\pi(x)}{x}=0,\ \lim_{x\to+\infty}\frac{x}{[x]}=1$$

λαμβάνουμε

$$\lim_{x\to+\infty}\frac{\pi(x)}{[x]}=0$$

□

Παρατίθεται παρακάτω ένας συνοπτικός πίνακας της συνάρτησης $\pi(x)$ συγκριτικά με την $\frac{x}{\log(x)}$, όπου $\log(x)$ ο φυσικός λογάριθμος του x.

x	$\pi(x)$	$\frac{x}{\log(x)}$	$\pi(x)\Big/\frac{x}{\log(x)}$
10	4	4,3	0,93
10^2	25	21,7	1,15
10^3	168	144,8	1,16
10^4	1229	1086	1,13
10^5	9592	8686	1,10
10^6	78498	72382	1,08
10^7	664579	620420	1,07
10^8	5761455	5428681	1,06
10^9	50847534	48254942	1,05
10^{10}	455052511	434294482	1,048

Πίνακας 4

Ο Adrien-Marie Legendre (1752-1833) και ο Carl Friedrich Gauss (1777-1855) ήταν οι πρώτοι που έκαναν εκτενείς υπολογισμούς της πυκνότητας των πρώτων αριθμών.

Εικόνα 10: Carl Friedrich Gauss

Και ο Legendre και ο Gauss μελετώντας πίνακες σαν τον παραπάνω κατέληξαν στο συμπέρασμα ότι για μεγάλο x, η πυκνότητα των πρώτων αριθμών κοντά στο x είναι περίπου ίση με $\frac{x}{\ln x}$. Ο Legendre, το 1798, έκανε την εικασία ότι:

$$\pi(x) \simeq \frac{x}{\ln x - A}$$

όπου $A \simeq 1.08366$, ενώ ο Gauss πρότεινε την προσέγγιση από την άποψη του λογαριθμικού ολοκληρώματος:

$$\pi(x) \simeq \int_2^x \frac{1}{\ln t} dt$$

Στην προσέγγιση αυτή παρατηρούμε ότι το ολοκλήρωμα στο δεξιό μέλος είναι ουσιαστικά ίσο με $\frac{x}{\ln x}$ για μεγάλα x, από το οποίο προκύπτει

$$\lim_{x \to +\infty} \frac{\pi(x) \ln x}{x} = 1$$

Η πρόταση ότι η πυκνότητα των πρώτων αριθμών είναι $\frac{x}{\ln x}$ είναι γνωστή ως *θεώρημα των πρώτων αριθμών*.

<u>Θεώρημα 8 (Θεώρημα των πρώτων αριθμών):</u>
Ισχύει ότι:

$$\pi(x) \sim \frac{x}{\ln x}.$$

Το θεώρημα των πρώτων αριθμών είναι ισοδύναμο με το παρακάτω θεώρημα

Θεώρημα 9:
Ισχύει ότι:

$$p_n \sim n \ln n$$

Όπου p_n παριστάνει τον n-οστό πρώτο αριθμό.

Προσπάθειες για να αποδειχθεί αυτό το θεώρημα έγιναν καθ' όλη την διάρκεια του 19ου αιώνα με αξιοσημείωτη πρόοδο αυτή των Pafnuty Chebyshev (1821-1894) και Bernhard Riemann (1826-1866). Ο Chebyshev το 1848 έκανε ένα σημαντικό βήμα αποδεικνύοντας ότι αν το $\lim_{x \to +\infty} \frac{\pi(x) \ln x}{x}$ υπάρχει, τότε θα είναι υποχρεωτικά ίσο με 1. Λίγο αργότερα, το 1950, έδειξε ότι υπάρχουν δύο θετικές σταθερές c_1 και c_2 τέτοιες ώστε

$$c_1 \frac{x}{\ln x} \le \pi(x) \le c_2 \frac{x}{\ln x}$$

για κάθε $x \ge 2$. Δηλαδή, η σωστή τάξη μεγέθους του $\pi(x)$ είναι $\frac{x}{\ln x}$. Ωστόσο δεν κατάφερε να αποδείξει την ύπαρξη του παραπάνω ορίου. Ο Riemann συνέδεσε το θεώρημα με κάτι που είναι γνωστό ως 'η Υπόθεση του Riemann': ένα αποτέλεσμα για τα μηδενικά στο μιγαδικό επίπεδο της 'Riemann-ζήτα-συνάρτησης': $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ όπου $s > 1$ και $s \in \mathbb{R}$, και που είναι ως τις μέρες μας αναπόδεικτο. Ο Riemann θεώρησε μιγαδική την μεταβλητή s και περιέγραψε μια έξυπνη μέθοδο για να συνδέσει την κατανομή των πρώτων αριθμών με τις ιδιότητες της συνάρτησης $\zeta(s)$. Τα μαθηματικά που χρειαζόντουσαν όμως δεν είχαν αναπτυχθεί ακόμα κι έτσι ο Riemann δεν κατάφερε να διευθετήσει τελείως το ζήτημα πριν από τον θάνατο του.

Εικόνα 11: Pafnuty Chabyshev

Εικόνα 12: Bernhard Riemann

Τελικά το θεώρημα των πρώτων αριθμών αποδείχτηκε από τους μαθηματικούς J.Hadamard (1865-1963) και De La Vallee Poussin (1866-1962) που το απέδειξαν ανεξάρτητα ο ένας από τον άλλον, αλλά σχεδόν ταυτόχρονα το 1896 χρησιμοποιώντας μέσα της μιγαδικής ανάλυσης (τα οποία εισήγαγε ο Riemann). Από την δουλειά του De La Vallee Poussin έπεται ότι το ολοκλήρωμα που πρότεινε ο Gauss δίνει καλύτερη προσέγγιση για την τιμή του $\pi(x)$ από την προσέγγιση του Legendre, όποια τιμή κι αν δοκιμάσει κανείς για την σταθερά A. Αργότερα, το 1948, οι μαθηματικοί P.Erdos (1913-1996) και A.Selberg (1917-2007) κατόρθωσαν να αποδείξουν το θεώρημα αυτό με στοιχειώδη μέσα, δηλαδή χωρίς μέσα της μιγαδικής ανάλυσης.

Εικόνα 13: J.Hadamard

Εικόνα 14: De La Vallee Poussin

Εικόνα 15: P.Erdos **Εικόνα 16: A.Selberg**

3.4 Θεώρημα Bertrand

Έχουμε δει ότι η ακολουθία των πρώτων είναι άπειρη. Για να δείξουμε ότι το μέγεθος των κενών μεταξύ δύο πρώτων αριθμών δεν είναι φραγμένο, θέτουμε $N := 2\times 3\times 5\times ...\times p$ το γινόμενο όλων των πρώτων αριθμών που είναι μικρότεροι ενός $k+2$ και σημειώνουμε ότι κανένας από τους k αριθμούς,

$$N+2, N+3, N+4, ..., N+k, N+(k+1)$$

δεν είναι πρώτος, εφόσον για $2\le i\le k+1$ γνωρίζουμε πως ο i έχει πρώτο παράγοντα ο οποίος είναι μικρότερος από $k+2$, και αυτός ο παράγοντας επίσης διαιρεί τον N, άρα επίσης διαιρεί τον $N+i$. Με αυτόν τον τρόπο, βρίσκουμε για παράδειγμα, ότι για $k=10$ $(N=2\times 3\times 5\times 7\times 11=2310)$, κανένας από τους δέκα αριθμούς

$$2312, 2313, 2314, ..., 2321$$

δεν είναι πρώτος.

Υπάρχουν όμως και μεγαλύτερα φράγματα στα κενά μεταξύ των πρώτων αριθμών. Διάσημη είναι η δήλωση ότι: «*Το κενό μέχρι τον επόμενο πρώτο αριθμό δεν μπορεί να είναι μεγαλύτερο από τον αριθμό με τον οποίο ξεκινάμε την έρευνα μας*». Αυτό είναι γνωστό ως Θεώρημα Bertrand, αφού εικάστηκε και επαληθεύτηκε εμπειρικά για $n<3000000$ από τον Γάλλο μαθηματικό Joseph Bertrand (1822-1900). Το θεώρημα αυτό αποδείχτηκε για κάθε n, πρώτη φορά από τον Pafnuty Chebyshev το 1850 και έτσι καλείται επίσης και Θεώρημα Bertrand-Chebyshev. Ο ιδιοφυής Ινδός μαθηματικός Srinivasa Ramanujan (1887-1920) χρησιμοποίησε ιδιότητες της Γ-

συνάρτησης $\Gamma(n)=(n-1)!$, n θετικός ακέραιος, για να δώσει μια πιο απλή απόδειξη [Ramanujan, 1919]. Τέλος ο P.Erdos το 1932, όταν ήταν μόλις 19 χρονών, δημοσίευσε μια ακόμα πιο απλή απόδειξη χρησιμοποιώντας την συνάρτηση θ-Chebyshev $\theta(x)=\sum_{p=2}^{x}\ln p$, όπου $p\le x$ πρώτος αριθμός, και διωνυμικούς συντελεστές [Erdos, 1930–1932].

Θεώρημα 10 (Θεώρημα Bertrand):
Για κάθε $n\ge 1$, υπάρχει κάποιος πρώτος αριθμός p με $n<p\le 2n$.

Εικόνα 17: Joseph Bertrand

3.5 Θεωρήματα των Fermat και Euler

Η ενασχόληση του Fermat 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’ Θεώρημα του.

Ορισμός 7:
Έστω ένας φυσικός αριθμός m. Ορίζουμε στο σύνολο $\mathbb{Z}$ των ακέραιων αριθμών τη σχέση

$$a\equiv b(\bmod m)\Leftrightarrow m\mid a-b$$

Η σχέση αυτή την οποία διαβάζουμε *ισότιμο του* πληρεί τις τρεις χαρακτηριστικές ιδιότητες μιας σχέσης ισοδυναμίας.

i. $a \equiv a \pmod m \ \ \forall a \in \mathbb{Z}$

ii. $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$

iii. $a \equiv b \pmod m, b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

Θεώρημα 11 (μικρό Θεώρημα του Fermat):

Έστω p πρώτος αριθμός. Τότε για κάθε ακέραιο a έχουμε $a^p \equiv a \pmod p$.

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

Απόδειξη:

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

Θα δείξουμε ότι ισχύει $(a+1)^p \equiv (a+1) \pmod p$. Όμως

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

Από αυτούς τους όρους ο τελευταίος είναι ο 1 και ο πρώτος ο a^p που είναι εξ υποθέσεως ισότιμος προς τον $a \pmod p$ ενώ όλοι οι ενδιάμεσοι είναι της μορφής $\binom{p}{i} a^i$ όπου i είναι ένας φυσικός ανάμεσα στον 1 και τον $p-1$. 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 $0 \pmod p$.

Τελικά $(a+1)^p \equiv (a^p + 1) \equiv (a+1) \pmod p$.

□

Λίγο αργότερα ο Euler παρουσίασε και την γενίκευση

Θεώρημα 12 (Θεώρημα Euler):

Έστω $\varphi(n)$ το πλήθος των φυσικών αριθμών που δεν ξεπερνάνε το n και είναι σχετικά πρώτοι προς αυτό, m ένας φυσικός αριθμός και a ακέραιος εκτός από το 0, τέτοιοι ώστε $(a,m)=1$. Τότε $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.

Προφανώς αν ο m είναι πρώτος τότε ισχύει $\varphi(m)=m-1$ και προκύπτει το 'μικρό' Θεώρημα του Fermat.

Το 'μικρό' Θεώρημα του Fermat είναι μεταξύ άλλων ένα κριτήριο για το αν ένας αριθμός είναι σύνθετος. Για παράδειγμα ο 63 δεν είναι πρώτος αφού $2^{63}=2^{60}\cdot 2^3=\left(2^6\right)^{10}\cdot 2^3=64^{10}\cdot 2^3\equiv 2^3\equiv 8(\mathrm{mod}\,63)$ και όχι $2(\mathrm{mod}\,63)$.

Θα ήταν ίσως ακόμα πιο χρήσιμο αν μπορούσαμε να δείξουμε, με την βοήθεια του, ότι ένας αριθμός είναι πρώτος. Οι Αρχαίοι Κινέζοι ήξεραν ότι αν ο p είναι πρώτος τότε διαιρεί τον 2^p-2. Πίστευαν όμως ότι αν ο 2^n-2 διαιρείται από τον n τότε αυτός είναι πρώτος. Δυστυχώς το αντίστροφο του Θεωρήματος δεν ισχύει, όπως δείχνει το παρακάτω παράδειγμα. Οι Κινέζοι έπρεπε να φτάσουν στον $n=341$ για να διαπιστώσουν ότι έκαναν λάθος.

Έστω $n=341=11\cdot 31$. Από το 'μικρό' Θεώρημα του Fermat έχουμε ότι $2^{10}\equiv 1(\mathrm{mod}11)$. Έτσι $2^{340}=\left(2^{10}\right)^{34}\equiv 1(\mathrm{mod}11)$. Επίσης $2^{340}=\left(2^5\right)^{68}=32^{68}\equiv 1(\mathrm{mod}\,31)$. Κι έτσι θα έχουμε ότι $2^{340}\equiv 1(\mathrm{mod}\,341)$ και πολλαπλασιάζοντας με 2 έχουμε $2^{341}\equiv 2(\mathrm{mod}\,341)$ αν και ο 341 δεν είναι πρώτος.

Υπάρχουν, δηλαδή, φυσικοί αριθμοί που ικανοποιούν την συνθήκη του Θεωρήματος για κάποιο a αλλά δεν είναι πρώτοι. Γενικά αν για έναν σύνθετο αριθμό n ισχύει $b^{n-1}\equiv 1 \mathrm{mod}\, n$ για κάποιον αριθμό b που είναι πρώτος προς τον n, τότε ο n λέγεται ψευδοπρώτος ως προς την βάση b. Συγκεκριμένα ο 341 του παραδείγματος είναι ψευδοπρώτος ως προς την βάση 2. Το ότι είναι ψευδοπρώτος ως προς την βάση 2 βέβαια, δεν σημαίνει ότι θα ισχύει το ίδιο και για άλλες βάσεις. Μήπως αν για έναν

αριθμό n βρίσκαμε μια βάση b για την οποία δεν θα ίσχυε το κριτήριο $b^{n-1} \equiv 1 \bmod n$ θα σήμαινε ότι ο αριθμός n δεν είναι πρώτος; Αν η προηγούμενη πρόταση ήταν αληθής θα είχαμε ένα πολύ απλό και γρήγορο κριτήριο για να ελέγξουμε αν ένας αριθμός είναι πρώτος. Δυστυχώς υπάρχουν σύνθετοι αριθμοί n που ικανοποιούν το παραπάνω κριτήριο για οποιαδήποτε βάση b, όπου b σχετικά πρώτος προς τον n. Αυτοί οι αριθμοί λέγονται αριθμοί Carmichael. Ο μικρότερος από αυτούς είναι ο 561. Πράγματι $561 = 3 \cdot 11 \cdot 17$. Αν $(b, 561) = 1$ τότε $(b, 3) = (b, 11) = (b, 17) = 1$. Από το 'μικρό' Θεώρημα του Fermat έχουμε $b^2 \equiv 1 \bmod 3$, $b^{10} \equiv 1 \bmod 11$, $b^{16} \equiv 1 \bmod 17$. Επομένως, $b^{560} = \left(b^2\right)^{280} \equiv 1 \bmod 3$, $b^{560} = \left(b^{10}\right)^{56} \equiv 1 \bmod 11$, $b^{560} = \left(b^{16}\right)^{35} \equiv 1 \bmod 17$. Άρα $b^{560} \equiv 1 \bmod 561$ για κάθε βάση b με $(b, 561) = 1$. Ο αριθμός 1729, ο μικρότερος που μπορεί να γραφτεί σαν άθροισμα δύο κύβων με δύο διαφορετικούς τρόπους ($1729 = 10^3 + 9^3 = 1^3 + 12^3$), είναι αριθμός Carmichael. Οι αριθμοί αυτοί είναι πολύ σπάνιοι. Μέχρι το 1.000.000.000 υπάρχουν μόνο 646. Παρ' όλα αυτά αποδείχτηκε, μόλις το 1992, ότι οι αριθμοί Carmichael είναι άπειροι.

Με την βοήθεια του 'μικρού' θεωρήματος του Fermat αποδεικνύεται μία πολύ σπουδαία πρόταση.

Πρόταση 3:

Ο $2^p - 1$ όπου ο p είναι πρώτος με $p \neq 2$ διαιρείται μόνο από τους αριθμούς της μορφής $2kp + 1$ για κάποιον ακέραιο k

Απόδειξη:

Αρκεί να δείξουμε ότι οι πρώτοι διαιρέτες του $2^p - 1$ είναι της μορφής $2kp + 1$. Έστω q ένας τέτοιος.

Ισχυρισμός: ο p διαιρεί τον $q - 1$.

Πράγματι, αν ο p δεν διαιρεί τον $q - 1$ τότε αφού ο p είναι πρώτος θα είναι πρώτοι μεταξύ τους, άρα θα υπάρχουν m, n τέτοιοι ώστε $mp + n(q-1) = 1$.

Τότε ή ο m ή ο n είναι αρνητικός, έστω ο m, άρα ο $-m$ είναι θετικός.

Από την υπόθεση έχουμε ότι $2^p \equiv 1 \bmod q$ άρα $2^{-mp} \equiv 1 \bmod q$ και επομένως

$\left[2^{q-1}\right]^n \equiv 1 \bmod q$.

Τελικά, $2 = 2^1 = 2^{mp+n(q-1)} \equiv 2^{n(q-1)} \bmod q \equiv 1 \bmod q$ που είναι άτοπο.

Άρα ο p διαιρεί τον $q-1$.

Επίσης, ο q είναι περιττός αφού διαιρεί τον $2^p - 1$, άρα ο $q-1$ είναι άρτιος κι έτσι ο 2 είναι διαιρέτης του $q-1$.

Τελικά ο $2p$ είναι διαιρέτης του $q-1$. Δηλαδή $q-1 = 2pk$ ή $q = 2kp+1$ για κάποιον ακέραιο k.

□

Η πρόταση αυτή γλύτωσε τους μαθηματικούς από πολλούς υπολογισμούς την εποχή που αυτοί συναγωνίζονταν για την εύρεση του μεγαλύτερου πρώτου ή ενός τέλειου αριθμού. Με αυτή την πρόταση, για παράδειγμα, εύκολα αποδεικνύεται πως ο $2^{17} - 1$ είναι πρώτος. Πράγματι, έχουμε ότι $2^{17} - 1 = 131.071$. Επειδή $\sqrt{131071} \approx 362,03$ αρκεί να εξετάσουμε αν ο 131.071 δεν έχει πρώτους διαιρέτες μικρότερους του 362. Σύμφωνα με τα παραπάνω οι μόνοι δυνατοί διαιρέτες του $2^{17} - 1$ είναι της μορφής $34k+1$. Οι δέκα αριθμοί αυτής της μορφής είναι οι 36,69,103,137,171,205,239,273,307 και 341. Από αυτούς πρώτοι είναι οι 103,137,239 και 307 και με έναν απλό έλεγχο επαληθεύεται ότι κανείς από αυτούς δεν διαιρεί τον 131.071. Άρα ο $2^{17} - 1$ είναι πρώτος κι έτσι οδηγούμαστε στον έκτο τέλειο αριθμό.

3.6 Θεώρημα Wilson

Εκείνη την εποχή (τον 18^{ο} αιώνα) ανακοινώθηκε ένα άλλο πολύ σημαντικό θεώρημα που είναι γνωστό ως ‘Θεώρημα Wilson’. Ονομάστηκε έτσι από τον Άγγλο μαθηματικό John Wilson, ο οποίος ήταν ο πρώτος που το δημοσίευσε μαζί με τον καθηγητή του Edward Waring το 1770 αλλά δεν μπορούσε και να το αποδείξει. Ο πρώτος που το απέδειξε ήταν ο Joseph Louis Lagrange (1736-1813) το 1771. Υπάρχουν ενδείξεις ότι το θεώρημα αυτό ήταν γνωστό και στον Gottfried Wilhelm Leibniz (1646-1716) έναν αιώνα νωρίτερα, αλλά ποτέ δεν το δημοσίευσε.

<u>Θεώρημα 13 (Θεώρημα Wilson)</u> *(John Wilson, 1770)**:***
Ένας φυσικός αριθμός $p>1$ *είναι πρώτος αν και μόνο αν* $(p-1)!\equiv -1(\mathrm{mod}\ p)$.

Το σημαντικότερο στο Θεώρημα Wilson είναι ότι, αντίθετα με το 'μικρό Θεώρημα του Fermat', ισχύει και το αντίστροφο του. Για παράδειγμα $(12-1)!=11!=39.916.800\equiv 0(\mathrm{mod}12)$ άρα ο 12 είναι σύνθετος ενώ $(13-1)!=12!=479.001.600=-1(\mathrm{mod}13)$,δηλαδή ο 13 είναι πρώτος. Έτσι το Θεώρημα Wilson μας δίνει και ένα κριτήριο για το αν ένας αριθμός είναι πρώτος ή όχι. Παρ' όλα αυτά δεν χρησιμοποιείται ως τέτοιο, λόγω του ότι ο υπολογισμός του $(p-1)!\mathrm{mod}\ p$ για μεγάλο p είναι δύσκολος και είναι γνωστοί πολύ πιο εύκολοι έλεγχοι πρώτων αριθμών. Ακόμα και αυτός των δοκιμαστικών διαιρέσεων θεωρείται πιο αποδοτικός.

4

Άλυτα προβλήματα πρώτων αριθμών

Υπάρχουν ακόμα πολλά αναπάντητα ερωτήματα (μερικά από τα οποία χρονολογούνται εκατοντάδες χρόνια πριν) σχετικά με τους πρώτους αριθμούς. Μερικά άλυτα προβλήματα παρατίθενται παρακάτω:

1. Έχουν όλες οι μη τετριμμένες λύσεις της συνάρτησης ζήτα του Riemann πραγματικό μέρος ίσο με $\frac{1}{2}$; (Υπόθεση Riemann)
2. Υπάρχει ζυγός αριθμός >2 που να μην εκφράζεται ως άθροισμα δύο περιττών πρώτων αριθμών; (Εικασία του Goldbach)
3. Υπάρχουν άπειροι δίδυμοι πρώτοι αριθμοί; (δύο πρώτοι αριθμοί p, q καλούνται δίδυμοι πρώτοι αν $q = p + 2$)
4. Υπάρχει ζυγός αριθμός >2 που να μην εκφράζεται ως διαφορά δύο πρώτων αριθμών;
5. Υπάρχουν άπειροι ‘πρώτοι αριθμοί του Mersenne’;
6. Υπάρχουν άπειροι ‘πρώτοι αριθμοί του Fermat’;
7. Υπάρχουν άπειροι πρώτοι αριθμοί της μορφής $x^2 + 1$, όπου x ακέραιος; (είναι γνωστό ότι υπάρχουν άπειροι πρώτοι της μορφής $x^2 + y^2 + 1$ και της μορφής $x^2 + y^2 + z^2 + 1$)
8. Υπάρχουν άπειροι πρώτοι της μορφής $x^2 + k$ (k γνωστό);
9. Υπάρχει πάντα τουλάχιστον ένας πρώτος αριθμός μεταξύ των n^2 και $(n+1)^2$ για κάθε ακέραιο $n \geq 1$; (το γεγονός ότι υπάρχει πάντα πρώτος αριθμός μεταξύ των n και $2n$ είναι η Εικασία του Bertrand που έχει αποδειχτεί από τον

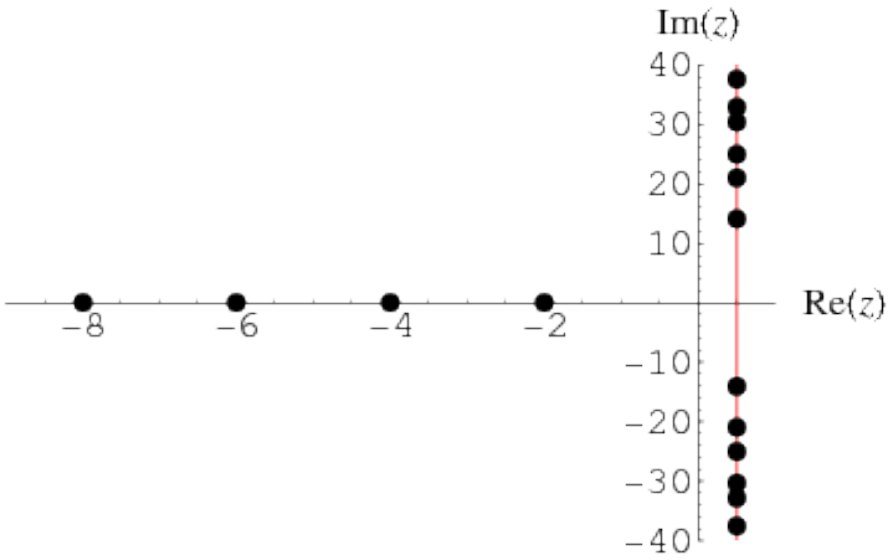
Chebyshev).

10. Υπάρχει πάντα τουλάχιστον ένας πρώτος αριθμός μεταξύ των n^2 και n^2+n για κάθε ακέραιο $n>1$;
11. Υπάρχουν άπειροι πρώτοι των οποίων όλα τα ψηφία να είναι 1; (για παράδειγμα δύο τέτοιοι πρώτοι είναι οι 11 και 11.111.111.111.111.111.111.111).
12. Υπάρχουν άπειροι πρώτοι της μορφής $n\#+1$ και $n\#-1$; (όπου $n\#$ το γινόμενο όλων των πρώτων αριθμών $\le n$).
13. Υπάρχουν άπειροι πρώτοι αριθμοί της μορφής $n!+1$ και $n!-1$;
14. Περιέχει η ακολουθία Fibonacci (της οποίας κάθε όρος προκύπτει από το άθροισμα των δύο προηγούμενων: 1,1,2,3,5,8,13,…) άπειρους πρώτους αριθμούς;
15. Υπάρχει αριθμητική πρόοδος με διαδοχικούς πρώτους αριθμούς για κάθε πεπερασμένο μήκος αυτής; (για παράδειγμα η ακολουθία: 251,257,263,269 έχει μήκος 4 και το μεγαλύτερο γνωστό παράδειγμα έχει μήκος 10).
16. Υπάρχουν άπειρα σύνολα τριών διαδοχικών πρώτων αριθμών σε αριθμητική πρόοδο; (ισχύει για μη διαδοχικούς πρώτους αριθμούς).
17. Το πολυώνυμο n^2-n+41 δίνει πρώτους για $0\le n\le 40$. Υπάρχουν άπειροι τέτοιοι πρώτοι αριθμοί; Το ίδιο ερώτημα ισχύει και για το $n^2-79n+1601$ που δίνει πρώτους για $0\le n\le 79$.

Στη συνέχεια θα εξετάσουμε διεξοδικότερα κάποια από τα παραπάνω προβλήματα, καθώς και την πρόοδο που έχει γίνει προς την επίλυση τους.

4.1 Υπόθεση Riemann

Το 1859, ο μεγάλος Γερμανός μαθηματικός Bernhard Riemann έγραψε το διάσημο έργο του 'Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse' (Για τον Αριθμό των Πρώτων μικρότερων από ένα δοσμένο Μέγεθος), το οποίο περιέχει μία από τις πιο θαυμαστές εικασίες των μαθηματικών. Ο Riemann μελετούσε μια συγκεκριμένη συνάρτηση μιγαδικής μεταβλητής, την $\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$. Απέδειξε ότι αυτή η συνάρτηση, όπου s είναι μιγαδικός αριθμός ($s=x+yi,\ x,y\in\mathbb{R}$), μπορεί να εκφραστεί ως μια αναλυτική συνάρτηση σε όλο το επίπεδο των μιγαδικών (με εξαίρεση το $s=1$). Η συνάρτηση $\zeta(s)$ είναι γνωστή ως 'συνάρτηση ζ του Riemann'. Στο έργο του ο Riemann παρατήρησε ότι η $\zeta(s)=0$ έχει λύση για κάθε αρνητικό άρτιο ακέραιο. Αυτές λέγονται 'τετριμμένες' λύσεις της συνάρτησης ζ. κάθε άλλη λύση εκτός από αυτές λέγεται 'μη τετριμμένη' λύση. Υπάρχουν άπειρες μη τετριμμένες λύσεις και ο Riemann έκανε την εκπληκτική εικασία ότι όλες οι μη τετριμμένες λύσεις είναι της μορφής $\frac{1}{2}+yi$ για κάποιον πραγματικό αριθμό y. Με άλλα λόγια όλες οι μη τετριμμένες λύσεις βρίσκονται πάνω στην ευθεία $x=\frac{1}{2}$ που είναι γνωστή ως 'κρίσιμη ευθεία'.



Διάγραμμα 2: Η κρίσιμη ευθεία (κόκκινη γραμμή) και οι λύσεις (μαύρες τελείες) της συνάρτησης ζ

Γιατί όμως είναι αυτή η εικασία σημαντική για τους πρώτους αριθμούς; Ο Riemann κατάφερε να συνδέσει τις μη τετριμμένες λύσεις της συνάρτησης ζ με την κατανομή των πρώτων αριθμών. Υποθέτοντας ότι η εικασία του είναι σωστή, βρήκε μια ακόμα καλύτερη εκτίμηση για το πλήθος των πρώτων που είναι μικρότεροι από έναν δοσμένο αριθμό. Στην πραγματικότητα, βρήκε έναν τρόπο να υπολογίσει τον ακριβή αριθμό των πρώτων χωρίς καθόλου σφάλμα. Δεν κατάφερε όμως να αποδείξει την εικασία του, λέγοντας

'*Φυσικά, θα ήταν επιθυμητό να έχουμε μια αυστηρή απόδειξη της εικασίας. Στο μεταξύ, μετά από μερικές επιπόλαιες μάταιες προσπάθειες, αφήνω προσωρινά στην άκρη την αναζήτηση απόδειξης, καθώς δεν φαίνεται απαραίτητη για τον επόμενο στόχο της αναζήτησης μου.*' [Devlin, 2003]

Η εικασία του ότι όλες οι μη τετριμμένες λύσεις της $\zeta(s)$ βρίσκονται στην ευθεία $\Re(s)=\frac{1}{2}$, είναι γνωστή ως 'Υπόθεση Riemann', και θεωρείται ένα από τα σημαντικότερα άλυτα προβλήματα των μαθηματικών για πάνω από έναν αιώνα.

Έχουν γίνει αρκετές αποτυχημένες προσπάθειες απόδειξης της υπόθεσης Riemann, μερικές από τις οποίες ανακοινώθηκαν δημοσίως. Το 1885, ο Ολλανδός μαθηματικός T.J.Stieltjes ισχυρίστηκε ότι είχε αποδείξει την 'εικασία του Mertens', η οποία συνεπάγεται την υπόθεση Riemann. Δυστυχώς πέθανε πριν προλάβει να δημοσιεύσει την απόδειξη του. Η απόδειξη του Stieltjes όμως ήταν σίγουρα λανθασμένη, καθώς το 1985 οι A.Odlyzko και H.te Riele έδειξαν ότι η 'εικασία του Mertens' δεν ισχύει. [Borwein et al., 2008].

Η πιο περίεργη από αυτές τις λανθασμένες αποδείξεις παρουσιάστηκε το 1959, όταν ο διάσημος μαθηματικός John Nash έδωσε μια διάλεξη στο πανεπιστήμιο της Κολούμπια, διοργανωμένη από την Αμερικάνικη Μαθηματική Εταιρία. Ο Nash παρουσίασε την απόδειξη του στην υπόθεση Riemann σε 250 συμμετέχοντες οι οποίοι είχαν υψηλές προσδοκίες. Δυστυχώς όμως η διάλεξη του δεν έβγαζε απολύτως κανένα νόημα. Το συμβάν αργότερα αποδόθηκε στην μάχη του με την σχιζοφρένεια [Sabbagh, 2004].

Έχουν παρουσιαστεί επίσης και αποδείξεις που δείχνουν ότι η υπόθεση Riemann είναι λανθασμένη. Στις αρχές του 1943 ο εκδότης του περιοδικού της Αμερικάνικης

Μαθηματικής Εταιρίας έλαβε ένα τηλεγράφημα από τον γραμματέα της Εταιρίας, που του ζητούσε να καθυστερήσει την έκδοση του περιοδικού, για μια εργασία που αποδείκνυε λανθασμένη την υπόθεση Riemann. Ο συγγραφέας της εργασίας H.Rademacher έστειλε ένα γράμμα που ανέφερε ότι οι υπολογισμοί του είχαν ελεγχθεί και επιβεβαιωθεί από τον Γερμανό μαθηματικό C.Siegel, ειδικό στην θεωρία αριθμών. Ωστόσο, την τελευταία στιγμή, ο Rademacher έστειλε ένα τηλεγράφημα στον εκδότη, λέγοντας ότι ο Siegel είχε βρει ένα λάθος στην συλλογιστική του. Ο Rademacher θεώρησε λανθασμένα ότι ο λογάριθμος ενός μιγαδικού αριθμού έχει μοναδική τιμή, ενώ στην πραγματικότητα οι μιγαδικοί λογάριθμοι λαμβάνουν άπειρες το πλήθος τιμές. Η απόδειξη του δεν μπορούσε να διορθωθεί [Sabbagh, 2004].

Παρ' όλες τις προσπάθειες των μαθηματικών να αποδείξουν την υπόθεση Riemann τα τελευταία 150 χρόνια, ελάχιστη πρόοδος έχει γίνει. Είναι λογική λοιπόν η ερώτηση, 'Υπάρχει λόγος να πιστεύουμε ότι η υπόθεση Riemann είναι αληθής;'. Η απάντηση είναι ναι. Υπάρχει ένας τεράστιος όγκος εμπειρικών στοιχείων που δείχνουν ότι η υπόθεση Riemann είναι σωστή. Από την εποχή που ο Riemann διατύπωσε για πρώτη φορά την υπόθεση του, οι μαθηματικοί υπολογίζουν τις λύσεις της $\zeta(s)$ και έχουν βρει ότι όλες βρίσκονται στην κρίσιμη ευθεία. Ο ίδιος ο Riemann υπολόγισε τις πρώτες μερικές λύσεις πριν καν παρουσιάσει την εργασία του. Οι υπολογισμοί του Riemann δεν δημοσιεύτηκαν ποτέ κι έτσι η μέθοδος του δεν ήταν γνωστή μέχρι που ο Siegel την ανακάλυψε μελετώντας τις σημειώσεις του Riemann. Την δεκαετία του '30 ο Siegel δημοσίευσε την μέθοδο που χρησιμοποιούσε ο Riemann, η οποία έγινε γνωστή ως 'μέθοδος Riemann-Siegel'. Μέχρι σήμερα όλοι οι υπολογισμοί της $\zeta(s)$ βασίζονται σε αυτή την μέθοδο. Έως το 2004, οι πρώτες 10^{13} λύσεις έχουν υπολογιστεί και βρίσκονται όλες στην κρίσιμη ευθεία, αυτό όμως στα μαθηματικά δεν αποτελεί απόδειξη. Ο παρακάτω πίνακας αποτυπώνει την πορεία αυτών των υπολογισμών που παρέχουν στοιχεία για την ορθότητα της υπόθεσης.

Έτος	**Αριθμός λύσεων**	**Υπολογίστηκαν από**
1859 (περίπου)	1	B.Riemann
1903	15	J.P.Gram
1914	79	R.J.Backlund

1925	138	J.I.Hutchinson
1935	1.041	E.C.Titchmarsh
1953	1.104	A.M.Turing
1956	15.000	D.H.Lehmer
1956	25.000	D.H.Lehmer
1958	35.337	N.A.Meller
1966	250.000	R.S.Lehman
1968	3.500.000	J.B.Rosser, et al.
1977	40.000.000	R.P.Brent
1979	81.000.001	R.P.Brent
1982	200.000.001	R.P.Brent, et al.
1983	300.000.001	J.van de Lune, H.J.J.te Riele
1986	1.500.000.001	J.van de Lune, et al.
2001	10.000.000.000	J.van de Lune (αδημοσίευτη)
2004	900.000.000.000	S.Wedeniwski
2004	10.000.000.000.000	X.Gourdon

Πίνακας 5: Υπολογισμός λύσεων της συνάρτησης ζ του Riemann

Κάποιοι μαθηματικοί έχουν καταφέρει μικρά βήματα προόδου και στην θεωρητική πλευρά του ζητήματος. Το 1896, ο Γάλλος μαθηματικός Jacques Salomon Hadamard και ο Βέλγος Charles Jean de la Vallee-Poussin απέδειξαν ανεξάρτητα ότι δεν μπορεί να υπάρχει λύση πάνω στην ευθεία $x=1$. Έδειξαν επίσης ότι όλες οι μη τετριμμένες λύσεις πρέπει να βρίσκονται στο εσωτερικό της περιοχής $0<x<1$, γνωστή ως 'κρίσιμη λωρίδα'. Η ανακάλυψη αυτή αποτέλεσε κομβικό βήμα για την απόδειξη του Θεωρήματος των Πρώτων Αριθμών.

Τον $20^{ο}$ αιώνα, οι μαθηματικοί συνέχισαν να περιορίζουν την περιοχή των μη τετριμμένων λύσεων. Το 1914, ο G.H.Hardy απέδειξε μια απαραίτητη συνθήκη για την υπόθεση Riemann. Απέδειξε ότι υπάρχουν άπειρες το πλήθος λύσεις πάνω στην κρίσιμη ευθεία $x=\frac{1}{2}$. Οι μαθηματικοί συνέχισαν να προσεγγίζουν την υπόθεση Riemann με αυτόν τον τρόπο, αποδεικνύοντας ισχυρότερα αποτελέσματα σχετικά με το πόσες λύσεις βρίσκονται στην κρίσιμη ευθεία. Το 1942, ο Atle Selberg απέδειξε ότι τουλάχιστον ένα μικρό ποσοστό λύσεων βρίσκεται στην κρίσιμη ευθεία. Το 1974,

ο Norman Levinson βελτίωσε αυτό το αποτέλεσμα δείχνοντας ότι το ένα τρίτο των λύσεων βρίσκεται στην κρίσιμη ευθεία. Το καλύτερο και πιο πρόσφατο αποτέλεσμα αποδείχτηκε από τον Brian Conrey ο οποίος βελτίωσε το ποσοστό σε δύο πέμπτα το 1989.

Πολλές φορές η μαθηματικοί δεν προσεγγίζουν μια πρόταση σαν την υπόθεση Riemann ευθέως, αλλά προσπαθούν να βρουν και να αποδείξουν άλλες ισοδύναμες προτάσεις. Υπάρχουν πολλές διαφορετικές προτάσεις που είναι ισοδύναμες με την υπόθεση Riemann. Μερικές από αυτές παρουσιάζονται παρακάτω.

Μια αριθμοθεωρητική πρόταση ισοδύναμη με την υπόθεση Riemann είναι η εξής:

'Το πλήθος των ακεραίων με άρτιο αριθμό πρώτων παραγόντων είναι ίσο με το πλήθος των ακεραίων με περιττό αριθμό πρώτων παραγόντων'

Η πρόταση αυτή μπορεί να γίνει ακριβής με τη χρήση της συνάρτησης Liouville, η οποία δίνει το πλήθος των πρώτων παραγόντων ενός θετικού ακεραίου. Η συνάρτηση Liouville ορίζεται ως:

$$\lambda(n) = (-1)^{\omega(n)}$$

Όπου $\omega(n)$ είναι το πλήθος, όχι απαραίτητα διακριτών, πρώτων παραγόντων του n.

Η υπόθεση Riemann είναι ισοδύναμη με την πρόταση ότι για κάθε δοσμένο $\varepsilon > 0$,

$$\lim_{n\to\infty} \frac{\lambda(1)+\lambda(2)+\ldots+\lambda(n)}{n^{\frac{1}{2}+\varepsilon}} = 0.$$

Ένας άλλος τρόπος να εκφράσουμε το παραπάνω είναι ότι η υπόθεση Riemann είναι ισοδύναμη με την πρόταση ότι ένας ακέραιος έχει ίση πιθανότητα να έχει άρτιο ή περιττό πλήθος διακριτών πρώτων παραγόντων.

Η υπόθεση Riemann είναι από τη φύση της μια πολύ αναλυτική έκφραση. Είναι λοιπόν επόμενο ότι θα έχει αρκετές αναλυτικές ισοδυναμίες. Οι Hardy και Littlewood έδειξαν ότι η υπόθεση Riemann ισχύει αν και μόνο αν

$$\sum_{k=1}^{\infty} \frac{(-x)^k}{k!\zeta(2k+1)} = O\left(x^{-\frac{1}{4}}\right),$$

καθώς $x \to \infty$.

Υπάρχουν πολύ περισσότερες προτάσεις ισοδύναμες με την υπόθεση Riemann από τις τρεις που αναφέρθηκαν παραπάνω. Όσο περισσότερες ισοδυναμίες αναπτυχθούν, τόσο περισσότερους τρόπους θα έχουν οι μαθηματικοί για να προσεγγίσουν την

υπόθεση Riemann. Αυτό φέρνει νέες ιδέες από διάφορους μαθηματικούς αλλά και κλάδους των μαθηματικών και βοηθά στην επίλυση του προβλήματος.

Η απόδειξη της υπόθεσης Riemann θα ήταν ένα θαυμαστό επίτευγμα που θα είχε τεράστιο αντίκτυπο σε όλους τους τομείς των μαθηματικών. Υπάρχουν αμέτρητες προτάσεις στην μαθηματική βιβλιογραφία που ξεκινούν με την φράση 'υποθέτοντας την υπόθεση Riemann' και συνεχίζουν αποδεικνύοντας κάποιο αποτέλεσμα. Έτσι, όποιος αποδείξει την υπόθεση Riemann θα αποδείξει ταυτόχρονα εκατοντάδες άλλα θεωρήματα.

Το 1742, ο C.Goldbach είκασε ότι κάθε φυσικός αριθμός $n \geq 5$ μπορεί να γραφεί ως άθροισμα τριών πρώτων αριθμών. Ο Euler ανασκεύασε αυτή την εικασία λέγοντας ότι κάθε άρτιος αριθμός $n \geq 3$ είναι άθροισμα δύο πρώτων. Η πρόταση αυτή είναι γνωστή ως 'εικασία του Goldbach' και είναι ένα από τα παλαιότερα άλυτα προβλήματα της θεωρίας αριθμών. Μια ασθενέστερη μορφή αυτής της πρότασης είναι ότι κάθε περιττός αριθμός $n \geq 7$ είναι άθροισμα τριών περιττών πρώτων. Οι Hardy και Littlewood απέδειξαν ότι η γενικευμένη υπόθεση Riemann συνεπάγεται την ασθενή εικασία του Goldbach για 'αρκούντως μεγάλα' n. Το 1997 οι μαθηματικοί Deshouillers, Effinger, te Riele και Zinoviev έδειξαν ότι η γενικευμένη υπόθεση Riemann συνεπάγεται την εικασία του Goldbach.

Η απόδοση πολλών αλγορίθμων ελέγχου πρώτων, όπως για παράδειγμα τα τεστ πρώτων Miller-Rabin και Solovay-Strassen, εξαρτάται από την ορθότητα της γενικευμένης υπόθεσης Riemann.

Υπάρχουν εκατοντάδες άλλες προτάσεις και εικασίες που οι μαθηματικοί έχουν αποδείξει υποθέτοντας την υπόθεση Riemann. Αν ποτέ αποδειχθεί, τότε ένας τεράστιος αριθμός θεωρημάτων θα προστεθεί αυτόματα στη θεωρία των μαθηματικών. Αυτό βέβαια δημιουργεί ένα επιπλέον κίνητρο και ενδιαφέρον για το συγκεκριμένο πρόβλημα. Δεν είναι ξεκάθαρο αν θα βρεθεί ποτέ η απόδειξη της υπόθεσης Riemann. Ωστόσο, τα στοιχεία δείχνουν ότι είναι αληθής. Η υπόθεση Riemann συνδέεται βαθιά με την κατανομή των πρώτων αριθμών και είναι ίσως το πιο σημαντικό άλυτο πρόβλημα σήμερα. Τόσο σημαντικό που συμπεριελήφθη στην λίστα των 23 άλυτων προβλημάτων που παρουσίασε ο David Hilbert στο Διεθνές Συνέδριο Μαθηματικών στο Παρίσι το 1900, και επελέγη από το Clay Mathematics Institute το 2000 στη λίστα των επτά 'Millennium Prize Problems', με έπαθλο για τη

λύση τους 1.000.000 δολάρια. Η υπόθεση Riemann θα είναι σίγουρα στο επίκεντρο της έρευνας των μαθηματικών για πολλά χρόνια.

4.2 Η Εικασία του Goldbach

Ένα από τα παλαιότερα αλλά και δημοφιλέστερα άλυτα προβλήματα της θεωρίας αριθμών είναι αυτό που είναι γνωστό ως η 'Εικασία του Goldbach'. Ο Christian Goldbach (1690-1764) ήταν ένας μεγάλος Γερμανός μαθηματικός που συχνά αλληλογραφούσε με άλλους μαθηματικούς της εποχής του για τις μαθηματικές του ανησυχίες. Στις 7 Ιουνίου 1742, έγραψε ένα γράμμα στον Leonhard Euler στο οποίο διατύπωσε την εξής εικασία:

«*Κάθε ακέραιος που μπορεί να γραφτεί ως το άθροισμα δύο πρώτων αριθμών, μπορεί να γραφτεί επίσης ως άθροισμα όσων πρώτων αριθμών θέλει κανείς, έως ότου όλοι οι όροι να είναι μονάδες.*»

Πρότεινε έπειτα μια δεύτερη εικασία στο περιθώριο της επιστολής του:

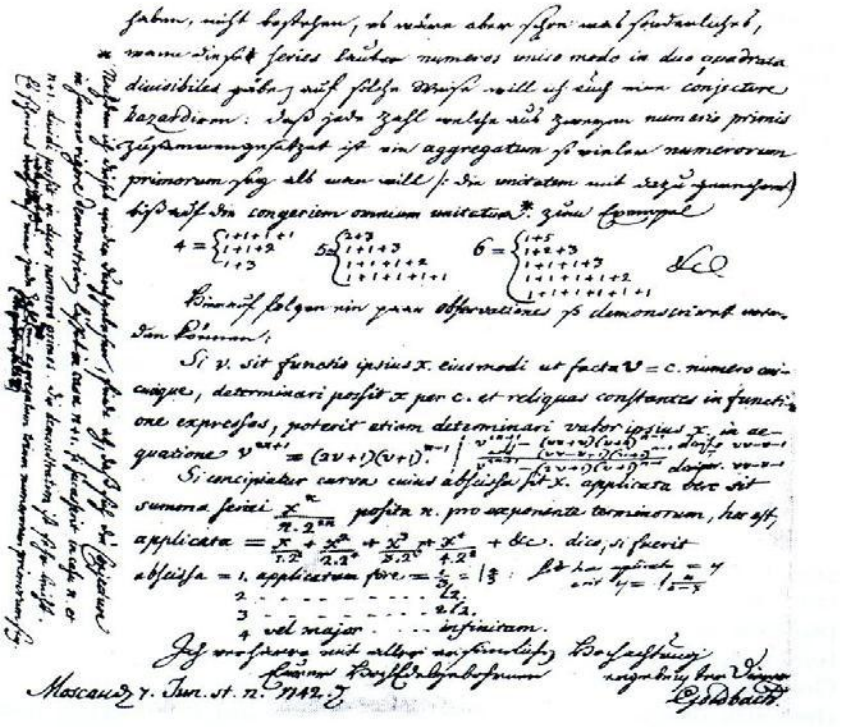
«*Κάθε ακέραιος μεγαλύτερος του 2 μπορεί να γραφτεί ως άθροισμα τριών πρώτων αριθμών.*»

Θεώρησε βέβαια το 1 ως πρώτο αριθμό, μια παραδοχή που αργότερα εγκαταλείφθηκε. Οι δύο αυτές εικασίες πλέον θεωρούνται ισοδύναμες, αλλά αυτό δεν φαίνεται να ήταν ζήτημα τότε. Ο Euler απάντησε με γράμμα του στις 30 Ιουνίου 1742 και θύμισε στον Goldbach μια παλαιότερη συζήτησή τους στην οποία ο Goldbach είχε θέσει την αρχική εικασία του:

«*Κάθε άρτιος ακέραιος μεγαλύτερος του 2 μπορεί να γραφτεί ως άθροισμα δύο πρώτων αριθμών.*»

Στο ίδιο γράμμα ο Euler δήλωσε ότι:

«*Κάθε άρτιος ακέραιος είναι άθροισμα δύο πρώτων. Το θεωρώ ένα απόλυτα σίγουρο και ολοκληρωμένο θεώρημα αν και δεν μπορώ να το αποδείξω.*»



Εικόνα 18: Το γράμμα από τον Goldbach προς τον Euler

Η σημερινή διατύπωση της ‘εικασίας του Goldbach’ είναι η εξής:

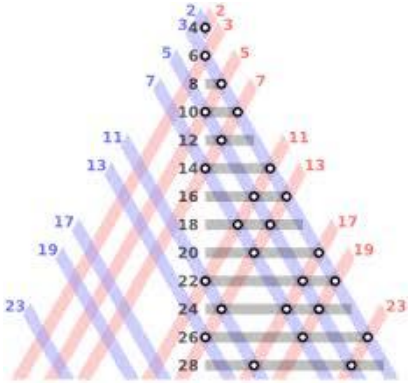
Εικασία του Goldbach:

Κάθε άρτιος ακέραιος μεγαλύτερος του 2 μπορεί να εκφραστεί ως το άθροισμα δύο πρώτων αριθμών.

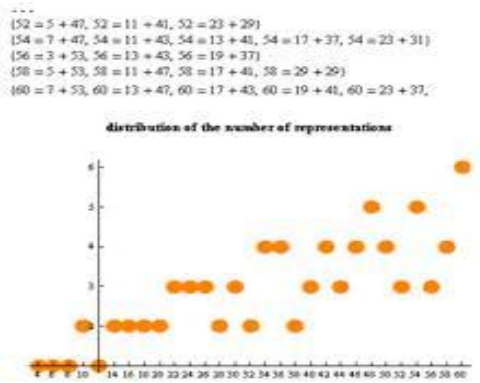
Και σε αναλυτική μορφή:

$$\forall n \in \mathbb{N}, \left((n>2) \wedge (n\ \acute{\alpha}\rho\tau\iota o\varsigma)\right) \Rightarrow \exists\, p,q \in P : n = p+q$$

Για μικρούς άρτιους αριθμούς επαληθεύεται εύκολα η ισχύς της εικασίας του Goldbach, για παράδειγμα 6=3+3, 8=5+3, 10=7+3=5+5, 12=7+5, 14=11+3=7+7, … Δεν είναι όμως γνωστό αν η εικασία ισχύει για όλους τους άρτιους αριθμούς τους μεγαλύτερους του 4.



Διάγραμμα 3: Πώς γράφονται οι αριθμοί 4-28 ως άθροισμα δύο πρώτων αριθμών.



Διάγραμμα 4: Ο αριθμός των τρόπων που ένας άρτιος μπορεί να παρασταθεί ως το άθροισμα 2 πρώτων.

Στην θεωρία αριθμών όμως ακόμα και η επαλήθευση μερικών χιλιάδων περιπτώσεων δεν είναι αρκετή απόδειξη για να πείσει τους μαθηματικούς πως κάτι πιθανόν είναι αληθινό. Με υπολογισμούς η εικασία του Goldbach έχει επαληθευτεί για έως και πολύ μεγάλους αριθμούς. Το 1938 ο Nils Pipping επαλήθευσε την εικασία με κόπο για $n \le 10^5$. Με την έλευση των υπολογιστών πολύ περισσότεροι αριθμοί έχουν ελεγχθεί. Ο T. Oliveira e Silva εκτελεί μια κατανεμημένη έρευνα που έχει επαληθεύσει την εικασία για $n \le 4\times10^{18}$.

Οι υπολογισμοί φαίνονται αναλυτικότερα στον παρακάτω πίνακα και τα παρακάτω διαγράμματα:

έλεγχος για $n \le \ldots$	πηγή
1×10^4	Desboves 1885
1×10^5	Pipping 1938
1×10^8	Stein and Stein 1965
2×10^{10}	Granville et al. 1989
4×10^{11}	Sinisalo 1993
1×10^{14}	Deshouillers et al. 1998
4×10^{14}	Richstein 1999, 2001
2×10^{16}	Oliveira e Silva (Mar. 24, 2003)
6×10^{16}	Oliveira e Silva (Oct. 3, 2003)
2×10^{17}	Oliveira e Silva (Feb. 5, 2005)

3×10^{17}	Oliveira e Silva (Dec. 30, 2005)
12×10^{17}	Oliveira e Silva (Jul. 14, 2008)

Πίνακας 6: Ακέραιοι μέχρι τους οποίους έχει ελεγχθεί η εικασία του Goldbach

Επειδή λοιπόν οι υπολογισμοί δεν αποτελούν απόδειξη, οι μαθηματικοί χρησιμοποιούν και έναν άλλο τρόπο για να συλλέξουν στοιχεία για την αλήθεια μιας εικασίας. Αυτό γίνεται αποδεικνύοντας άλλα θεωρήματα παρόμοια με την εικασία. Για παράδειγμα το 1930 ο Ρώσος μαθηματικός Schnirelmann (1905-1938) έδειξε ότι υπάρχει αριθμός M τέτοιος ώστε κάθε αριθμός n από κάποιο σημείο και έπειτα ισούται με το άθροισμα M ή λιγότερων πρώτων αριθμών.

$$n = p_1 + p_2 + ... + p_M$$

(για αρκούντως μεγάλο n).

Αν γνωρίζαμε πως $M = 2$ για όλους τους άρτιους n, αυτό θα αποδείκνυε την εικασία του Goldbach για όλους τους μεγάλους n. Το 1956 ο Κινέζος μαθηματικός Yin Wen-Lin απέδειξε ότι $M \le 18$. Αυτό σημαίνει πως κάθε αριθμός n από κάποιο σημείο και έπειτα ισούται με το άθροισμα 18 ή λιγότερων πρώτων αριθμών. Το πιο γνωστό και πιο πρόσφατο αποτέλεσμα, βασισμένο στο θεώρημα του Schnirelmann οφείλεται στον Ramaré Olivier, ο οποίος το 1995 έδειξε ότι κάθε ζυγός αριθμός $n \ge 4$ είναι άθροισμα το πολύ 6 πρώτων αριθμών. Η απόδειξη του Schnirelmann θεωρείται ένα γιγάντιο βήμα προς την απόδειξη της εικασίας του Goldbach. Ήταν η μοναδική πραγματική πρόοδος που έγινε για 200 χρόνια.

Μία πολύ κοντινότερη προσέγγιση προς την λύση της εικασίας του Goldbach έγινε το 1937 από έναν άλλο Ρώσο μαθηματικό I. M. Vinogradoff (1891-1983) που απέδειξε ότι από κάποιο σημείο και έπειτα κάθε περιττός αριθμός ισούται με το άθροισμα τριών πρώτων αριθμών:

$$n = p_1 + p_2 + p_3, \text{ (} n \text{ περιττός, αρκούντως μεγάλος)}$$

Μέχρι και σήμερα αυτό είναι το πιο δυνατό στοιχείο υπέρ της εικασίας του Goldbach. Είναι εύκολο να αποδείξουμε ότι το θεώρημα του Vinogradoff είναι συνέπεια της εικασίας του Goldbach. Δηλαδή αν η εικασία του Goldbach είναι αληθής είναι εύκολο να συμπεράνουμε το θεώρημα του Vinogradoff. Το μεγάλο κατόρθωμα του Vinogradoff ήταν ότι κατάφερε να αποδείξει το θεώρημά του χωρίς να

χρησιμοποιήσει την εικασία του Goldbach. Δυστυχώς κανένας δεν έχει καταφέρει να το δουλέψει από την άλλη μεριά και να αποδείξει την εικασία του Goldbach από το θεώρημα του Vinogradoff. Χρησιμοποιώντας τη μέθοδο του Vinogradoff, οι μαθηματικοί Chudakov (1904-1986), Van der Corput (1890-1975), και Estermann (1902-1991) έδειξαν ότι σχεδόν όλοι οι άρτιοι αριθμοί μπορούν να γραφούν ως το άθροισμα δύο πρώτων αριθμών.

Άλλο ένα στοιχείο υπέρ της εικασίας του Goldbach βρέθηκε το 1948 από τον Ούγγρο μαθηματικό Alfred Renyi (1921-1970) που απέδειξε ότι υπάρχει αριθμός M τέτοιος ώστε κάθε αρκούντως μεγάλος άρτιος αριθμός n να μπορεί να γραφεί ως άθροισμα ενός πρώτου αριθμού και ενός άλλου αριθμού A που έχει το πολύ M διαφορετικούς πρώτους παράγοντες:

$$n = p + A, \ (n \text{ περιττός, αρκούντως μεγάλος})$$

Αν γνωρίζαμε ότι $M = 1$, τότε η εικασία του Goldbach θα ήταν αληθής για όλους τους αρκούντως μεγάλους n. Το 1965 οι A. A. Buhstab και A. I. Vinogradov απέδειξαν ότι $M \leq 3$ και το 1966 ο Chen Jingrun (1933-1996) απέδειξε χρησιμοποιώντας τις μεθόδους της 'Θεωρίας του κοσκινίσματος' ότι $M \leq 2$. Το 1975 οι Hugh Montgomery και Robert Charles Vaughan έδειξαν ότι οι περισσότεροι άρτιοι εκφράζονται ως το άθροισμα δύο πρώτων αριθμών. Ακριβέστερα, έδειξαν ότι υπάρχουν θετικές σταθερές c και C τέτοιες ώστε για όλους τους αρκούντως μεγάλους αριθμούς n, κάθε άρτιος αριθμός μικρότερος του n είναι άθροισμα δύο πρώτων αριθμών με το πολύ Cn^{1-c} εξαιρέσεις. Συγκεκριμένα το σύνολο των άρτιων ακεραίων που δεν είναι άθροισμα δύο πρώτων αριθμών έχει πυκνότητα 0.

Όπως και με πολλές άλλες διάσημες εικασίες στα μαθηματικά, υπάρχουν μια σειρά από δήθεν αποδείξεις της εικασίας του Goldbach, αλλά καμία δεν είναι αποδεκτή από την μαθηματική κοινότητα.

Από την εικασία του Goldbach συνεπάγεται μια ακόμα εικασία για τους πρώτους αριθμούς, γνωστή ως 'Ασθενής Εικασία του Goldbach' ή 'Περιττή Εικασία του Goldbach':

Ασθενής Εικασία του Goldbach:

Κάθε περιττός αριθμός μεγαλύτερος του 5 μπορεί να γραφτεί ως άθροισμα τριών πρώτων αριθμών.

Αν η εικασία του Goldbach ισχύει τότε, απλά προσθέτοντας 3 σε κάθε ζυγό αριθμό μεγαλύτερο του 2, θα έχουμε όλους τους περιττούς μεγαλύτερους του 5, και η ασθενής εικασία θα ισχύει αυτόματα. Αυτός είναι και ο λόγος που η εικασία αυτή λέγεται ασθενής.

Το 1923 οι Hardy και Littlewood έδειξαν ότι, αν υποθέσουμε την γενικευμένη υπόθεση Riemann, η ασθενής εικασία του Goldbach ισχύει για όλους τους 'αρκούντως μεγάλους' αριθμούς.

Το 1937, ο Vinogradov κατάφερε να παρακάμψει την γενικευμένη υπόθεση Riemann και απέδειξε ευθέως το ίδιο αποτέλεσμα. Η αρχική απόδειξη του Vinogradov δεν έδινε ένα όριο για το 'αρκούντως μεγάλους'. Αργότερα ο μαθητής του K.Borozdin απέδειξε ότι το $3^{3^{15}}$ είναι επαρκές όριο. Ο αριθμός αυτός όμως έχει 6.846.169 ψηφία κι έτσι ο έλεγχος κάθε αριθμού μικρότερου από αυτό το όριο θα ήταν ανέφικτος.

Ο Γάλλος μαθηματικός Olivier Ramare, το 1995, έδειξε ότι κάθε άρτιος αριθμός $n \geq 4$ είναι άθροισμα το πολύ έξι πρώτων, από όπου συνεπάγεται ότι κάθε περιττός $n \geq 5$ είναι άθροισμα το πολύ επτά πρώτων. Στη συνέχεια ο Leszek Kaniecki έδειξε ότι κάθε περιττός ακέραιος είναι άθροισμα το πολύ πέντε πρώτων, υπό την Υπόθεση Riemann, για να έρθει το 2012 ο Αυστραλός Terence Tao να το αποδείξει χωρίς την Υπόθεση Riemann.

Το 1997, οι Deshouillers, Effinger, te Riele και Zinoviev δημοσίευσαν μια εργασία, δείχνοντας ότι η γενικευμένη υπόθεση του Riemann συνεπάγεται την ασθενή εικασία του Goldbach για κάθε αριθμό. Το αποτέλεσμα αυτό συνδυάζει ένα γενικό αποτέλεσμα που ισχύει για τους αριθμούς μεγαλύτερους από 10^{20} με μία εκτεταμένη υπολογιστική έρευνα για τις μικρότερες τιμές.

Το 2002, οι Κινέζοι μαθηματικοί Liu Ming-Chit και Wang Tian-Ze κατέβασαν το όριο που προβλέπεται από τα αποτελέσματα των Hardy, Littlewood και Vinogradov περίπου στο $n > e^{3100} \approx 2 \cdot 10^{1346}$. Ο εκθέτης αυτός είναι ακόμα υπερβολικά μεγάλος για να ελεγχθούν μέσω υπολογιστή όλοι οι μικρότεροι αριθμοί. Οι έρευνες μέσω υπολογιστή έχουν φτάσει έως το 10^{18} για την 'ισχυρή' εικασία του Goldbach και όχι πολύ παραπάνω για την 'ασθενή'.

Τέλος, το 2012 και το 2013, ο Περουβιανός μαθηματικός Harald Helfgott δημοσίευσε δύο εργασίες, όπου χρησιμοποιώντας την 'κυκλική μέθοδο Hardy-Littlewood' κατάφερε να αποδείξει χωρίς περιορισμούς την Ασθενή Εικασία του

Goldbach.

4.3 Δίδυμοι Πρώτοι Αριθμοί

Ορισμός 9:
Δίδυμοι πρώτοι αριθμοί καλούνται τα ζεύγη πρώτων αριθμών της μορφής $(p, p+2)$

Ο όρος 'δίδυμοι πρώτοι' επινοήθηκε από τον Γερμανό μαθηματικό Paul Stäckel (1862-1919) [Tietze 1965, p. 19]. Μερικοί από τους πρώτους δίδυμους πρώτους αριθμούς είναι οι:

$(3,5),(5,7),(11,13),(17,19),(29,31),(41,43),(59,61),(71,73),(101,103),(107,109),...$
[Sloane's A001359, A006512].

Οι δίδυμοι πρώτοι απέχουν όσο το δυνατόν λιγότερο γίνεται να απέχουν οι πρώτοι αριθμοί. Κάθε τρίτος περιττός αριθμός είναι πολλαπλάσιο του 3 και γι' αυτό δεν υπάρχουν τρεις διαδοχικοί περιττοί αριθμοί που να είναι πρώτοι εκτός και αν ο ένας από αυτούς είναι ο 3. Ως εκ τούτου, ο 5 είναι ο μοναδικός πρώτος που βρίσκεται σε δύο ζεύγη δίδυμων πρώτων αριθμών. Εκτός από το πρώτο ζεύγος δίδυμων πρώτων αριθμών, ο αριθμός ανάμεσα σε κάθε ζεύγος δίδυμων πρώτων είναι πολλαπλάσιο του 6. Άρα όλοι οι δίδυμοι πρώτοι αριθμοί εκτός του ζεύγους $(3,5)$ είναι της μορφής:

$$(6n-1, 6n+1).$$

Το ερώτημα αν υπάρχουν άπειροι δίδυμοι πρώτοι αριθμοί υπήρξε ένα ακόμα από τα μεγάλα ανοικτά ζητήματα στην Θεωρία Αριθμών για πολλά χρόνια.

Εικασία των δίδυμων πρώτων:
Υπάρχουν άπειροι πρώτοι αριθμοί p τέτοιοι ώστε ο $p+2$ να είναι επίσης πρώτος αριθμός.

Δεν είναι γνωστό αν υπάρχουν άπειροι τέτοιοι πρώτοι αριθμοί [Wells 1986, p. 41; Shanks 1993], αλλά φαίνεται σχεδόν βέβαιο ότι είναι αλήθεια [Hardy and Wright 1979, p. 5].

Το 1849 ο Γάλλος μαθηματικός Alphonse de Polignac (1817-1890) έκανε την πιο

γενική εικασία ότι για κάθε φυσικό αριθμό k υπάρχουν άπειρα ζευγάρια p και p' τέτοια ώστε $p'-p=2k$. Η περίπτωση $k=1$ είναι η εικασία των δίδυμων πρώτων αριθμών. Μία ισχυρότερη μορφή της εικασίας των δίδυμων πρώτων αριθμών είναι η εικασία των μαθηματικών Hardy και Littlewood που αξιώνει έναν νόμο κατανομής των δίδυμων πρώτων αριθμών παρόμοιο με το θεώρημα των πρώτων αριθμών.
Ένα σημαντικό αποτέλεσμα για τους πρώτους αριθμούς ήταν το παρακάτω που ανακαλύφθηκε το 1915 από τον Νορβηγό μαθηματικό Viggo Brun (1885-1978).

Θεώρημα 14 (Θεώρημα Brun, 1919):
Ο αριθμός που προκύπτει από την πρόσθεση των αντίστροφων των περιττών δίδυμων πρώτων αριθμών,

$$B=\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)+\ldots,$$

συγκλίνει σε έναν συγκεκριμένο αριθμό.

Ο αριθμός αυτός που έχει ονομαστεί *σταθερά του Brun* εκφράζει την σπανιότητα των δίδυμων πρώτων, ακόμα και αν υπάρχουν άπειροι από αυτούς [Ribenboim 1996, p. 201]. Το διάσημο αυτό αποτέλεσμα ήταν το πρώτο αποτέλεσμα του ‘κόσκινου του Brun’, και βοήθησε στην εξέλιξη της μοντέρνας ‘θεωρίας κόσκινου’. Η μοντέρνα εκδοχή του θεωρήματος του Brun μπορεί να χρησιμοποιηθεί για να δείξουμε ότι το πλήθος των δίδυμων πρώτων μικρότερων από N δεν ξεπερνάει το $\frac{CN}{\left(\ln N\right)^2}$ για κάποια σταθερά $C>0$.

Θεωρούμε $\pi_2(n)$ τον αριθμό των ζευγών δίδυμων πρώτων p και $p+2$ τέτοιο ώστε $p\le n$.

Ο Brun απέδειξε ότι υπάρχει υπολογίσιμη σταθερά x_o τέτοια ώστε αν $x\ge x_o$, τότε

$\pi_2(x)<\frac{100x}{\left(\ln x\right)^2}$ [Ribenboim 1996, p. 261].

Έχει δειχτεί ότι:

$$\pi_2(x)<c\prod_{p>2}\left[1-\frac{1}{(p-1)^2}\right]\frac{x}{(\ln x)^2}\left[1+O\left(\frac{\ln\ln x}{\ln x}\right)\right]$$

το οποίο γράφεται πιο συνοπτικά:

$$\pi_2(x) < c\Pi_2 \frac{x}{(\ln x)^2}\left[1+O\left(\frac{\ln\ln x}{\ln x}\right)\right]$$

Όπου Π_2 σταθερά, γνωστή ως *σταθερά των δίδυμων πρώτων αριθμών* και c μια άλλη σταθερά. Οι Hardy και Littlewood (1923) έδειξαν ότι $c=2$ [Ribenboim 1996, p. 262] και ότι $\pi_2(x) \sim 2\Pi_2 \int_2^x \frac{dx}{\ln x}$. Αυτή η εικασία λέγεται *δυνατή εικασία των δίδυμων πρώτων*.

Το 1940, ο Paul Erdos έδειξε ότι υπάρχει σταθερά $c<1$ και άπειρο πλήθος πρώτων p τέτοιοι ώστε $(p'-p)<(c\ln p)$, όπου p' είναι ο επόμενος πρώτος μετά τον p. Αυτό το αποτέλεσμα στη συνέχεια βελτιώθηκε. Το 1986, ο Γερμανός Helmut Maier έδειξε ότι μπορεί να χρησιμοποιηθεί μια σταθερά $c<0.25$. Το 2004, οι Daniel Goldston και Cem Yildirim βελτίωσαν κι άλλο την σταθερά δείχνοντας ότι $c=0.085786...$. Τέλος, το 2005, οι Goldston, Janos Pintz και Yildirim κατέληξαν ότι η σταθερά c μπορεί να επιλεγεί οσοδήποτε μικρή.

Πράγματι υιοθετώντας την 'εικασία Elliot-Halberstam', ή μια ελαφρώς ασθενέστερη εκδοχή, μπόρεσαν να δείξουν ότι υπάρχουν άπειροι το πλήθος n τέτοιοι ώστε τουλάχιστον δύο εκ των $n, n+2, n+6, n+8, n+12, n+18$ και $n+20$ να είναι πρώτοι. Χρησιμοποιώντας μια ισχυρότερη υπόθεση έδειξαν επίσης ότι για άπειρους το πλήθος n, τουλάχιστον δύο εκ των $n, n+2, n+4$ και $n+6$ είναι πρώτοι.

Το 1966, ο Chen Jingrun έδειξε ότι υπάρχουν άπειροι πρώτοι p τέτοιοι ώστε ο $p+2$ να είναι είτε πρώτος είτε ένας 'ημι-πρώτος' (το γινόμενο δύο πρώτων). Η προσέγγιση που έκανε ενέπλεξε την 'θεωρία κόσκινου', και κατάφερε να αντιμετωπίσει την εικασία των δίδυμων πρώτων και την εικασία του Goldbach με παρόμοιο τρόπο.

Στην προσπάθεια τους να καθορίσουν ότι 'πρώτος Chen' είναι ένας πρώτος p τέτοιος ώστε ο $p+2$ είναι είτε πρώτος είτε 'ημι-πρώτος', ο Αυστραλός μαθηματικός Terence Tao και ο Βρετανός Ben Green απέδειξαν, το 2005, ότι υπάρχουν άπειρες τριάδες ακολουθιών από πρώτους του Chen

Επιστρέφοντας στην υπόθεση του de Polignac, στις 17 Απριλίου 2013, ο Κινεζοαμερικάνος μαθηματικός Yitang Zhang εξέπληξε την μαθηματική κοινότητα με μια σπουδαία ανακάλυψη. Απέδειξε ότι υπάρχουν άπειρα το πλήθος ζευγάρια

πρώτων που διαφέρουν κατά N, με $N < 7 \cdot 10^7$. Στη συνέχεια ο Terence Tao πρότεινε μια συλλογική προσπάθεια βελτίωσης του ορίου του Zhang. Έως τις 14 Απριλίου 2014, μόλις έναν χρόνο μετά την αρχική ανακάλυψη του Zhang, το όριο είχε μειωθεί στο $N < 246$. Επιπλέον, υποθέτοντας την 'εικασία Elliott-Halberstam' και την γενικευμένη μορφή της, το όριο μειώνεται σε $N < 12$ και $N < 6$ αντίστοιχα.

Στις 15 Ιανουαρίου 2007 δύο διαφορετικά υπολογιστικά προγράμματα, το Twin Prime Search και το PrimeGrid, βρήκαν το μεγαλύτερο γνωστό ζεύγος δίδυμων πρώτων αριθμών: $2003663613 \cdot 2^{195000} \pm 1$ με 58711 ψηφία ο καθένας. Ανακαλύφθηκαν από τον Γάλλο Eric Vautier. Στις 6 Αυγούστου 2009 τα δύο αυτά προγράμματα ανακοίνωσαν ότι ένα νέο ρεκόρ δίδυμων πρώτων αριθμών είχε βρεθεί: $65516468355 \cdot 2^{333333} \pm 1$ με 100355 ψηφία. Στις 25 Δεκέμβρη του 2011 το πρόγραμμα PrimeGrid ανακοίνωσε ότι ένα ακόμη ρεκόρ δίδυμων πρώτων είχε βρεθεί: $3756801695685 \cdot 2^{666669} \pm 1$ με 200700 ψηφία ο καθένας.

Μια εμπειρική ανάλυση όλων των ζευγαριών δίδυμων πρώτων έως το $4.35 \cdot 10^{15}$ δείχνει ότι αν το πλήθος τέτοιων ζευγαριών μικρότερων του x είναι $\frac{f(x) \cdot x}{(\ln x)^2}$ τότε η $f(x)$ είναι περίπου 1.7 για μικρά x, ενώ τείνει στο 1.3 καθώς το x τείνει στο άπειρο.

Υπάρχουν 808.675.888.577.436 ζευγάρια δίδυμων πρώτων έως το 10^{18}.

Η οριακή τιμή της $f(x)$ εικάζεται ότι είναι διπλάσια της σταθεράς των δίδυμων πρώτων, $2 \cdot \prod_{\substack{p \text{ prime} \\ p>3}} \left(1 - \frac{1}{(p-1)^2}\right) = 1.3203236\ldots$. Η εικασία αυτή συνεπάγεται την εικασία των δίδυμων πρώτων, παραμένει όμως κι αυτή αναπόδεικτη.

5

Μερικές εφαρμογές των πρώτων αριθμών

Για πολλά χρόνια, η Θεωρία Αριθμών και ειδικότερα η μελέτη των πρώτων αριθμών, αντιμετωπιζόταν ως το τυπικό παράδειγμα ‘καθαρών’ μαθηματικών, χωρίς εφαρμογές πέρα από το ενδιαφέρον της μελέτης του ίδιου του αντικειμένου. Συγκεκριμένα αρκετοί αριθμοθεωρητικοί, όπως ο Βρετανός G.H.Hardy, ήταν υπερήφανοι που το αντικείμενο τους δεν είχε κανένα στρατιωτικό ενδιαφέρον. Το όραμα αυτό ωστόσο διαλύθηκε την δεκαετία του ’70 όταν εμφανίστηκαν οι πρώτες εφαρμογές των πρώτων αριθμών.

5.1 Μαθηματικές εφαρμογές των πρώτων αριθμών

Η modular αριθμητική τροποποιεί τη συνήθη αριθμητική χρησιμοποιώντας μόνο τους αριθμούς $\{0,1,2,...,n-1\}$, όπου ο n είναι ένας σταθερός φυσικός αριθμός που ονομάζεται modulus. Ο υπολογισμός των αθροισμάτων, των διαφορών και των γινομένων γίνεται ως συνήθως, αλλά όποτε συναντούμε έναν αρνητικό αριθμό ή έναν αριθμό μεγαλύτερο του $n-1$, αυτός αντικαθίσταται από το υπόλοιπο μετά την διαίρεση από τον n. Για παράδειγμα, για $n=7$, το άθροισμα 3+5 ισούται με 1 αντί για 8, αφού όταν το 8 διαιρείται με το 7 αφήνει υπόλοιπο 1. Για να αναφερθούμε σε αυτό λέμε ότι '3+5 είναι ισοδύναμο με 1 modulo 7' και γράφουμε $3+5\equiv 1(\mathrm{mod}\,7)$. Ομοίως, $6+1\equiv 0(\mathrm{mod}\,7)$, $2-5\equiv 4(\mathrm{mod}\,7)$, αφού $-3+7=4$ και $3\cdot 4\equiv 5(\mathrm{mod}\,7)$, καθώς το 12 αφήνει υπόλοιπο 5. Οι βασικές ιδιότητες της πρόσθεσης και του πολλαπλασιασμού γνωστές από τους ακεραίους ισχύουν και στην modular αριθμητική. Στον τομέα της αφηρημένης άλγεβρας, το παραπάνω σύνολο ακεραίων, το οποίο συμβολίζεται με $\mathbb{Z}/n\mathbb{Z}$, είναι επομένως ένας αντιμεταθετικός δακτύλιος για κάθε n. Η διαίρεση όμως, δεν είναι γενικά δυνατή σε αυτή την κατάσταση. Για παράδειγμα, για $n=6$, στην εξίσωση $3\cdot x\equiv 2(\mathrm{mod}\,6)$, μια λύση του x, η οποία θα ήταν ανάλογη του $2/3$, δεν μπορεί να βρεθεί, όπως μπορεί να διαπιστώσει κανείς υπολογίζοντας το $3\cdot 0,3\cdot 1,...,3\cdot 5(\mathrm{mod}\,6)$.

Το ιδιαίτερο χαρακτηριστικό των πρώτων αριθμών είναι το εξής: η διαίρεση είναι δυνατή στην modular αριθμητική αν και μόνο αν ο n είναι πρώτος αριθμός. Ισοδύναμα, ο n είναι πρώτος αριθμός αν και μόνο αν όλοι οι ακέραιοι m που ικανοποιούν την ανισότητα $2\le m\le n-1$ είναι σχετικά πρώτοι με τον n, δηλαδή ο μόνος κοινός διαιρέτης τους είναι το 1. Πράγματι, για $n=7$, η εξίσωση $3\cdot x\equiv 2(\mathrm{mod}\,7)$, έχει μοναδική λύση, την $x=3$. Εξαιτίας αυτού, για κάθε πρώτο αριθμό p, το $\mathbb{Z}/p\mathbb{Z}$ (μερικές φορές σημειώνεται ως F_p) ονομάζεται *σώμα* ή πιο συγκεκριμένα *πεπερασμένο σώμα*, αφού περιέχει πεπερασμένα το πλήθος, συγκεκριμένα p, στοιχεία. Ένα πλήθος θεωρημάτων μπορεί να εξαχθεί από τη μελέτη του F_p με αυτόν τον αφηρημένο τρόπο. Για παράδειγμα το 'μικρό θεώρημα του Fermat' το οποίο, όπως αναφέρεται και νωρίτερα, λέει ότι $a^{p-1}\equiv 1(\mathrm{mod}\,p)$ για

κάθε ακέραιο αριθμό a που δεν διαιρείται από τον p, μπορεί να αποδειχθεί χρησιμοποιώντας αυτές τις έννοιες. Αυτό συνεπάγεται ότι

$$\sum_{a=1}^{p-1} a^{p-1} \equiv (p-1)\cdot 1 \equiv -1 (\mathrm{mod}\ p).$$

Η 'εικασία του Giuga' λέει ότι αυτή η εξίσωση είναι επίσης μια επαρκής συνθήκη για να πούμε ότι ο p είναι πρώτος αριθμός. Μια άλλη συνέπεια του 'μικρού θεωρήματος του Fermat' είναι η εξής: αν ο p είναι ένας πρώτος αριθμός διάφορος του 2 και του 5, ο $1/p$ είναι πάντα ένας περιοδικός αριθμός, με περίοδο $p-1$ ή έναν διαιρέτη του $p-1$. Ομοίως, το κλάσμα $1/p$ εκφρασμένο στη βάση q (αντί στη βάση 10) έχει παρόμοιο αποτέλεσμα, υπό τον όρο ο p να μην είναι πρώτος παράγοντας του q. Το θεώρημα του Wilson αναφέρει ότι ένας ακέραιος $p>1$ είναι πρώτος αν και μόνο αν το παραγοντικό $(p-1)!+1$ διαιρείται από τον p. Επιπλέον, ένας ακέραιος αριθμός $n>4$ είναι σύνθετος αν και μόνο αν το $(n-1)!$ διαιρείται από τον n.

Υπάρχουν και άλλοι τομείς των μαθηματικών που χρησιμοποιούν πολύ τους πρώτους αριθμούς. Ένα παράδειγμα από τη θεωρία των πεπερασμένων σωμάτων είναι τα θεωρήματα του Sylow: αν G είναι ένα πεπερασμένο σώμα και p^n είναι η μεγαλύτερη δύναμη του πρώτου αριθμού p που διαιρεί την τάξη της G, τότε η G έχει μια υποομάδα τάξης p^n. Επίσης, κάθε ομάδα της οποίας η τάξη είναι πρώτος αριθμός είναι κυκλική (θεώρημα Lagrange).

5.2 Οι πρώτοι αριθμοί στην κρυπτογραφία

Την δεκαετία του '70, τεχνικές από την θεωρία αριθμών άλλαξαν τον κόσμο για πάντα, προσφέροντας για πρώτη φορά έναν τρόπο να ανταλλάσουν δύο άνθρωποι μυστικά μηνύματα υποθέτοντας ότι σε όλη την συνομιλία παρεμβάλλεται ένας 'αντίπαλος'. Η ιδέα αυτή άντεξε στον χρόνο. Στην πραγματικότητα, κάθε φορά που, για παράδειγμα, αγοράζουμε κάτι μέσω του διαδικτύου χρησιμοποιούμε αυτό το σύστημα, το οποίο δουλεύει πάνω στον δακτύλιο των ακεραίων modulo n.

Το σύστημα αυτό λέγεται *Κρυπτογράφηση Δημοσίου Κλειδιού* (Public Key Cryptography) και επινοήθηκε στα τέλη της δεκαετίας του '70 από τους Whitfield

Diffie και Martin Hellman. Παρέχει ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης από την προγενέστερη κρυπτογράφηση συμμετρικού κλειδιού. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες. Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται *ιδιωτικό κλειδί* (private key) και το άλλο *δημόσιο κλειδί* (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη την διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες.

Οι αλγόριθμοι δημοσίου κλειδιού βασίζονται σε μαθηματικά προβλήματα τα οποία μέχρι σήμερα δεν έχουν αποδοτική λύση, όπως για παράδειγμα το πρόβλημα της παραγοντοποίησης ενός ακεραίου σε πρώτους παράγοντες. Είναι υπολογιστικά εύκολο για έναν χρήστη να δημιουργήσει το δικό του ζεύγος δημόσιου και ιδιωτικού κλειδιού και να το χρησιμοποιήσει για κρυπτογράφηση και αποκρυπτογράφηση. Η δύναμη της μεθόδου έγκειται στο γεγονός ότι είναι υπολογιστικά ανέφικτο να προσδιοριστεί ένα σωστά παραγμένο ιδιωτικό κλειδί από το αντίστοιχο δημόσιο κλειδί.

Εικόνα 19: Whitfield Diffie

Εικόνα 20: Martin Hellman

5.2.1 Πρωτόκολλο Diffie-Hellman

Μία από τις πρώτες πρακτικές εφαρμογές της ‘ανταλλαγής κλειδιού’ στην κρυπτογραφία είναι το πρωτόκολλο Diffie-Hellman. Παρουσιάστηκε το 1976 από τους Whitfield Diffie και Martin Hellman. Πριν από τη δημιουργία αυτού κάθε

κρυπτογραφική τεχνική βασιζόταν σε κάποιο προσυμφωνημένο κλειδί. Το συγκεκριμένο πρωτόκολλο είναι το πρώτο που προτάθηκε ώστε να επιτρέπει σε δύο οντότητες, χωρίς προηγούμενη επικοινωνία, να ανταλλάξουν ένα κοινό κλειδί μέσω ενός μη ασφαλούς διαύλου επικοινωνίας. Η ισχύς του πρωτοκόλλου βασίζεται στο γεγονός ότι υπάρχουν αποδοτικοί αλγόριθμοι modular ύψωσης σε δύναμη, ενώ η αντίστροφη διαδικασία, γνωστή ως 'πρόβλημα διακριτού λογαρίθμου', είναι πολύ δύσκολη.

Ακολουθεί η διαδικασία του πρωτοκόλλου Diffie-Hellman με ένα παράδειγμα:

1. Η Alice και ο Bob συμφωνούν στη χρήση ενός πρώτου αριθμού $p = 23$ και μιας βάσης $g = 5$.
2. Η Alice επιλέγει έναν κρυφό ακέραιο $a = 6$ και στέλνει στον Bob το $A = g^a \pmod p$
   - $A = 5^6 \pmod{23} = 8$
3. Ο Bob επιλέγει έναν κρυφό ακέραιο $b = 15$ και στέλνει στην Alice το $B = g^b \pmod p$
   - $B = 5^{15} \pmod{23} = 19$
4. Η Alice υπολογίζει το $s = B^a \pmod p$
   - $s = 19^6 \pmod{23} = 2$
5. Ο Bob υπολογίζει το $s = A^b \pmod p$
   - $s = 8^{15} \pmod{23} = 2$
6. Η Alice και ο Bob μοιράζονται τώρα τον ίδιο μυστικό αριθμό $s = 2$.

Οι δύο πλευρές έφτασαν στο ίδιο αποτέλεσμα διότι τα $\left(g^a\right)^b$ και $\left(g^b\right)^a$ είναι ισοδύναμα $\pmod p$. Παρατηρούμε ότι μόνο τα a, b και $g^{ab} \pmod p = g^{ba} \pmod p$ κρατούνται κρυφά. Όλες οι άλλες τιμές - p, g, $g^a \pmod p$ και $g^b \pmod p$ - αποστέλλονται δημόσια. Αφού οι δύο πλευρές υπολογίσουν τον κοινό μυστικό αριθμό s μπορούν να τον χρησιμοποιήσουν σαν κλειδί κρυπτογράφησης για να στέλνουν μηνύματα στον ίδιο ανοιχτό δίαυλο επικοινωνίας. Φυσικά στην

πραγματικότητα χρησιμοποιούνται πολύ μεγαλύτερες τιμές για τα a, b και p, της τάξεως των 300 ψηφίων για το p και 100 ψηφίων για τα a και b, για λόγους ασφάλειας. Το πρωτόκολλο Diffie-Hellman μπορεί να χρησιμοποιηθεί και σαν μέρος της κρυπτογράφησης δημοσίου κλειδιού. Στην πράξη όμως τις περισσότερες φορές χρησιμοποιείται η μέθοδος RSA.

5.2.2 Μέθοδος RSA

Η μέθοδος RSA είναι ένας από τους πρώτους κρυπταλγορίθμους δημοσίου κλειδιού και χρησιμοποιείται ευρέως για την ασφαλή μετάδοση δεδομένων αλλά και ως ψηφιακή υπογραφή. Το όνομα του RSA προέρχεται από τους δημιουργούς του, Ron **R**ivest, Adi **S**hamir και Len **A**dleman οι οποίοι τον δημοσίευσαν πρώτοι το 1977.

Ο χρήστης της μεθόδου RSA δημιουργεί και έπειτα δημοσιεύει το γινόμενο δύο μεγάλων πρώτων αριθμών. Το γινόμενο αυτό αποτελεί το δημόσιο κλειδί (public key). Οι πρώτοι παράγοντες του γινομένου πρέπει να κρατούνται μυστικοί. Ο καθένας μπορεί να χρησιμοποιήσει το δημόσιο κλειδί για να κρυπτογραφήσει ένα μήνυμα, αλλά με τις υπάρχουσες μεθόδους, αν το δημόσιο κλειδί είναι αρκετά μεγάλο, μόνο κάποιος που γνωρίζει τους πρώτους παράγοντες μπορεί να αποκρυπτογραφήσει το μήνυμα. Το ‘σπάσιμο’ της κρυπτογράφησης RSA είναι γνωστό ως το ‘πρόβλημα RSA’. Η ασφάλεια της μεθόδου βασίζεται στο γεγονός ότι είναι πολύ εύκολο να πολλαπλασιαστούν δύο μεγάλοι πρώτοι αριθμοί p και q, ενώ είναι πολύ δυσκολότερο (πρακτικά αδύνατο) να υπολογιστούν οι πρώτοι παράγοντες p και q από το γινόμενο pq.

Τα βήματα του αλγόριθμου κρυπτογράφησης RSA είναι τα εξής:

1. Επιλέγουμε δύο πρώτους αριθμούς p και q.
    - Για λόγους ασφάλειας, οι ακέραιοι p και q πρέπει να επιλέγονται τυχαία και να είναι παρόμοιου μήκους. Πρώτοι αριθμοί μπορούν να βρεθούν εύκολα χρησιμοποιώντας τα ανάλογα τεστ.
2. Υπολογίζουμε το γινόμενο $n = pq$.
    - Το n χρησιμοποιείται σαν modulo για το δημόσιο και το ιδιωτικό κλειδί. Το μήκος του, εκφρασμένο σε bits, είναι το μήκος του κλειδιού.

3. Υπολογίζουμε το $\varphi(n)=\varphi(p)\varphi(q)=(p-1)(q-1)=n-(p+q-1)$, όπου φ είναι η συνάρτηση Euler.
4. Επιλέγουμε έναν ακέραιο e τέτοιο ώστε $1<e<\varphi(n)$ και $\text{ΜΚΔ}(e,\varphi(n))=1$, δηλαδή ο e και ο $\varphi(n)$ να είναι πρώτοι προς αλλήλους.
   - Το e αποτελεί τον 'δημόσιο εκθέτη'
   - Μια συνήθης επιλογή για το e είναι το $2^{16}+1=65.537$ καθώς είναι αρκετά μικρό και διευκολύνει την κρυπτογράφηση. Ωστόσο μικρότερες τιμές του e οδηγούν σε πολύ αδύναμη ασφάλεια.
5. Υπολογίζουμε το $d\equiv e^{-1}\left(\text{mod}\,\varphi(n)\right)$, δηλαδή το d είναι το αντίστροφο του $e\left(\text{mod}\,\varphi(n)\right)$.
   - Το d αποτελεί τον 'ιδιωτικό εκθέτη'
   - Το d συνήθως υπολογίζεται μέσω του 'εκτεταμένου Ευκλείδιου αλγόριθμου'.

Το δημόσιο κλειδί αποτελείται από το modulo n και τον δημόσιο εκθέτη e. Το ιδιωτικό κλειδί αποτελείται από το modulo n και τον ιδιωτικό εκθέτη d, τα οποία κρατούνται μυστικά. Μυστικά κρατούνται επίσης τα p, q και $\varphi(n)$ καθώς μπορούν να χρησιμοποιηθούν για τον υπολογισμό του d.

5.3 Γεννήτριες ψευδοτυχαίων αριθμών

Γεννήτρια ψευδοτυχαίων αριθμών (pseudorandom number generator – PRNG) ονομάζουμε έναν αλγόριθμο, ο οποίος παράγει μια ακολουθία αριθμών που προσεγγίζει τις ιδιότητες μιας ακολουθίας τυχαίων αριθμών. Στην πραγματικότητα, οι αριθμοί αυτής της ακολουθίας δεν είναι τυχαίοι, με την έννοια ότι καθορίζονται πλήρως από ένα σχετικά μικρό σύνολο αρχικών τιμών, στις οποίες περιλαμβάνεται μια πραγματικά τυχαία τιμή που ονομάζεται 'πηγή'. Χρησιμοποιώντας μια μηχανική γεννήτρια τυχαίων αριθμών μπορούμε να παράγουμε ακολουθίες οι οποίες είναι πολύ πιο κοντά στην πραγματική 'τυχαιότητα'. Ωστόσο, οι ψευδοτυχαίοι αριθμοί είναι πολύ σημαντικοί στην πράξη, λόγω της ταχύτητας παραγωγής τους.

Οι γεννήτριες ψευδοτυχαίων αριθμών έχουν πολλές εφαρμογές σε τυχερά παιχνίδια,

δειγματοληψία για στατιστικές αναλύσεις, προσομοιώσεις, την κρυπτογραφία, τον εντελώς τυχαίο σχεδιασμό και άλλες περιοχές όπου είναι επιθυμητή η παραγωγή ενός απρόβλεπτου αποτελέσματος. Σε γενικές γραμμές, όταν οι απρόβλεπτοι αριθμοί είναι υψίστης σημασίας, όπως σε εφαρμογές ασφάλειας, προτιμούνται οι μηχανικές γεννήτριες τυχαίων αριθμών (όπου αυτό είναι εφικτό).

Οι γεννήτριες ψευδοτυχαίων αριθμών είναι πολύ χρήσιμες στους αλγόριθμους Monte Carlo και τις προσομοιώσεις, διότι η διαδικασία ελέγχου, εντοπισμού και διόρθωσης των σφαλμάτων (debugging) διευκολύνεται από την δυνατότητα των γεννητριών να παράξουν την ίδια ακολουθία τυχαίων αριθμών σε πολλά ‘τρεξίματα’ της ίδιας εφαρμογής. Χρησιμοποιούνται επίσης στην κρυπτογραφία – όταν η ‘πηγή’ είναι μυστική.

Η δημιουργία ψευδοτυχαίων αριθμών είναι μία σημαντική και συχνή εργασία στον προγραμματισμό ηλεκτρονικών υπολογιστών. Ενώ η κρυπτογραφία και ορισμένοι αριθμητικοί αλγόριθμοι απαιτούν πολύ υψηλό βαθμό τυχαιότητας, πολλές λειτουργίες δεν το χρειάζονται. Μερικά απλά παραδείγματα είναι το "τυχαίο απόσπασμα της ημέρας", ή η κίνηση ενός χαρακτήρα σε ένα ηλεκτρονικό παιχνίδι Ηπιότερες μορφές της τυχαιότητας χρησιμοποιούνται σε αλγόριθμους κατακερματισμού και ταξινόμησης.

Ορισμένες εφαρμογές που εκ πρώτης όψεως φαίνεται να είναι κατάλληλες για τυχαιοποίηση δεν είναι στην πραγματικότητα όσο απλές φαίνονται. Για παράδειγμα , ένα σύστημα που επιλέγει «τυχαία» μουσικά κομμάτια για αναπαραγωγή πρέπει απλώς να φαίνεται τυχαίο και μπορεί να έχει ακόμη και έλεγχο στην επιλογή μουσικής: ένα αληθινά τυχαίο σύστημα δεν θα πρέπει να έχει κανένα περιορισμό για το αν το ίδιο αντικείμενο εμφανίζεται δύο ή τρεις φορές διαδοχικά.

Αρκετές από αυτές τις γεννήτριες χρησιμοποιούν τις ιδιότητες των πρώτων αριθμών. Οι πρώτοι αριθμοί του Fermat είναι ιδιαίτερα χρήσιμοι στην παραγωγή ψευδοτυχαίων αριθμών. Υπενθυμίζουμε ότι οι ‘πρώτοι του Fermat’ είναι της μορφής $F_n = 2^{2^n} + 1$ όπου $n \geq 0$. Συγκεκριμένα χρησιμοποιούνται για να παραχθούν ψευδοτυχαίοι αριθμοί στο διάστημα $1,...,N$ όπου ο N είναι δύναμη του 2. Ο πιο συνηθισμένος τρόπος να το πετύχουμε αυτό είναι ο εξής:

1. Επιλέγουμε μια αρχική τιμή V_0 με $1 \leq V_0 \leq P-1$ όπου ο P είναι πρώτος Fermat.
2. Πολλαπλασιάζουμε το V_0 με έναν αριθμό A ο οποίος είναι μεγαλύτερος από την

τετραγωνική ρίζα του P ($A > \sqrt{P}$) και είναι πρώτη ρίζα modulo P

- Ο A είναι πρώτη ρίζα modulo P σημαίνει ότι για κάθε ακέραιο x πρώτο προς τον P, υπάρχει ακέραιος k τέτοιος ώστε $A^k \equiv x \pmod{P}$.

3. Υπολογίζουμε το παραπάνω γινόμενο modulo P. Αυτή είναι η νέα τιμή της γεννήτριας. Δηλαδή, $V_{i+1} = (A \times V_i) \pmod{P}$

Ο αλγόριθμος αυτός είναι ιδιαίτερα χρήσιμος στους υπολογιστές, αφού οι περισσότερες δομές δεδομένων αποτελούνται από στοιχεία με 2^x πιθανές τιμές. Για παράδειγμα, ένα byte έχει 256 (2^8) πιθανές τιμές (0-255). Ως εκ τούτου για να συμπληρώσουμε ένα byte με τυχαίες τιμές, μπορούμε να χρησιμοποιήσουμε μια γεννήτρια που παράγει τιμές από 0 έως 255. Πολύ μεγάλοι αριθμοί του Fermat χρησιμοποιούνται στην κρυπτογράφηση δεδομένων γι αυτό τον λόγο. Η μέθοδος αυτή παράγει μόνο ψευδοτυχαίες τιμές, καθώς έπειτα από $P-1$ επαναλήψεις, η ακολουθία επαναλαμβάνεται.

Ένας ακόμα τύπος πρώτων αριθμών που βρίσκουν εφαρμογή στις γεννήτριες ψευδοτυχαίων αριθμών είναι οι 'πρώτοι του Mersenne'. Υπενθυμίζουμε ότι 'πρώτοι του Mersenne' λέγονται οι πρώτοι αριθμοί της μορφής $M_n = 2^n - 1$.

Ένα παράδειγμα είναι ο αλγόριθμος 'Mersenne twister'. Η Mersenne twister είναι μακράν η πιο συχνά χρησιμοποιούμενη γεννήτρια ψευδοτυχαίων αριθμών. Το όνομα της προέρχεται από το γεγονός ότι η περίοδος της επιλέγεται να είναι πρώτος Mersenne. Ο αλγόριθμος Mersenne twister αναπτύχθηκε το 1997 από τους Γιαπωνέζους Makoto Matsumoto και Takuji Nishimura. Σχεδιάστηκε ειδικά για να διορθώσει τα περισσότερα σφάλματα των παλαιότερων γεννητριών. Ήταν η πρώτη γεννήτρια που πέτυχε γρήγορη παραγωγή ψευδοτυχαίων αριθμών υψηλής ποιότητας.

Η πιο συνηθισμένη έκδοση της γεννήτριας Mersenne twister βασίζεται στον πρώτο Mersenne $2^{19937} - 1$.

Η γεννήτρια Mersenne twister χρησιμοποιείται σε πλήθος εφαρμογών όπως η R, το Matlab, το PHP, η C++, το SPSS και άλλες. Ο ακριβής τρόπος λειτουργίας του αλγορίθμου είναι αρκετά περίπλοκος και ξεφεύγει από τον σκοπό της παρούσας διπλωματικής.

5.4 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.

Εικόνα 21: Το τζιτζίκι Magicicada

6

Επίλογος

Ο επαγγελματίας μαθηματικός έλκεται από την Θεωρία Αριθμών εξαιτίας του τρόπου με τον οποίο μπορούν να χρησιμοποιηθούν όλα τα όπλα των σύγχρονων μαθηματικών για να αντιμετωπιστούν τα προβλήματά της. Στην πραγματικότητα, πολλά σημαντικά παρακλάδια των μαθηματικών έχουν την ρίζα τους στην Θεωρία Αριθμών. Για παράδειγμα οι πρώτες προσπάθειες για να αποδειχτεί το Θεώρημα των πρώτων αριθμών παρακίνησαν την ανάπτυξη της θεωρίας των μιγαδικών συναρτήσεων. Οι προσπάθειες για να αποδειχτεί πως μία Διοφαντική εξίσωση $x^n + y^n + z^n = 0$ δεν έχει μη τετριμμένη λύση για $n \geq 3$ (Τελευταίο Θεώρημα του Fermat), οδήγησαν στην ανάπτυξη της Αλγεβρικής Θεωρίας Αριθμών, μιας από τις πιο ενεργές περιοχές της έρευνας των μοντέρνων μαθηματικών. Παρόλο που η εικασία του Fermat ήταν μέχρι πρότινος αμφισβητούμενη, αυτό φαινόταν ασήμαντο εν συγκρίσει με την συντριπτική ποσότητα πολύτιμων μαθηματικών που είχαν δημιουργηθεί ως αποτέλεσμα ερευνών για αυτήν την εικασία.

Υπάρχουν εκατοντάδες άλυτα προβλήματα στην Θεωρία Αριθμών. Καινούρια προβλήματα προκύπτουν γρηγορότερα απ' ότι λύνονται τα παλιότερα, πολλά από τα οποία μένουν άλυτα για αιώνες. Αρκετά από αυτά δεν ξέρουμε καν αν επιδέχονται επίλυση. Οι προσπάθειες για την λύση τους όμως, όχι μόνο δεν σταματούν, αλλά εντείνονται συνεχώς. Όπως είχε πει και ο μεγάλος Γερμανός μαθηματικός David Hilbert (1862-1943) σε ομιλία του το 1930, φράση που αναγράφεται και στον τάφο του: «*Πρέπει να μάθουμε. Θα μάθουμε.*».

7

Βιβλιογραφία

1. B C Berndt, *Ramanujan and the theory of prime numbers*, Number theory Madras 1987 (Berlin, 1989), 122-139.
2. Borho, W. *"On Thabit ibn Kurrah's Formula for Amicable Numbers."* Math. Comput. 26, 571-578, 1972.
3. Borwein, P., Choi, S., Rooney, B. and Weirathmueller, A. (2008), "*The Riemann Hypothesis*", Canadian Mathematical Society.
4. Caldwell, Chris (2008). *"Goldbach's conjecture"*. Retrieved 2008-08-13.
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. Chudakov, Nikolai G. (1937). *"[On the Goldbach problem]"*. Doklady Akademii Nauk SSSR 17: 335–338.
7. Davis, M.D. (2007), "*Η φύση και η δύναμη των Μαθηματικών",* απόδοση στα ελληνικά: Καραγιαννίδης Δ., Μαγειρόπουλος Μ., Πανεπιστημιακές εκδόσεις Κρήτης.
8. Derbyshire, J. *Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics*. New York: Penguin, 2004.
9. Deshouillers, J.-M.; te Riele, H. J. J.; and Saouter, Y. *"New Experimental Results Concerning The Goldbach Conjecture."* In Algorithmic Number Theory: Proceedings of the 3rd International Symposium (ANTS-III) held at Reed College, Portland, OR, June 21-25, 1998 (Ed. J. P. Buhler). Berlin: Springer-Verlag, pp. 204-215, 1998.
10. Devlin, K. (2003), "*The millennium problems*", Basic Books.

11. D. Shanks, *Solved and unsolved problems in number theory*, Chelsea, New York, NY, 1978. pp. xiii+258, ISBN 0-8284-0297-3. MR 80e:10003 [QA241.S44, ISBN 0-8284-0297-3]
12. Erdos, P., *Beweis eines Satzes von Tschebyschef, Acta Sci. Math. (Szeged)* 5 (1930–1932), 194–198.
13. Estermann, T. (1938). *"On Goldbach's problem: proof that almost all even positive integers are sums of two primes"*. Proc. London Math. Soc.. 2 44: 307–314. doi:10.1112/plms/s2-44.4.307.
14. Gardner, M. *The Sixth Book of Mathematical Games from Scientific American*, Chicago, IL: University of Chicago Press, 1984.
15. Gauss, Carl Friedrich; Clarke, Arthur A. (translator into English) (1986), *Disquisitiones Arithemeticae* (Second, corrected edition), New York: Springer, ISBN 0-387-96254-9
16. Gauss, Carl Friedrich; Maser, H. (translator into German) (1965), *Untersuchungen uber hohere Arithmetik* (Disquisitiones Arithemeticae & other papers on number theory) (Second edition), New York: Chelsea, ISBN 0-8284-0191-8
17. Goldbach, C. Letter to L. Euler, June 7, 1742. http://www.mathstat.dal.ca/~joerg/pic/g-letter.jpg or http://www.informatik.uni-giessen.de/staff/richstein/pic/g-letter-zoomed.jpg.
18. Hardy, G. H. and Wright, E. M. *An Introduction to the Theory of Numbers*, 5th ed. Oxford, England: Clarendon Press, 1979.
19. Hardy, G. H. Ch. 2 in *Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work*, 3rd ed. New York: Chelsea, 1999.
20. Heath, T.L. (1921), "*A history of Greek Mathematics",* Oxford University.
21. H. Fürstenberg: *On the infinitude of primes*, Amer. Math. Monthly 62 (1955), 353.
22. H S Uhler, *A brief history of the investigations on Mersenne numbers and the latest immense primes*, Scripta Math. 18 (1952), 122-131.
23. Lehmer, D. N. *Factor Table for the First Ten Millions, Containing the Smallest Factor of Every Number Not Divisible by 2, 3, 5 or 7 Between the Limits 0 and 10017000*. Washington, DC: Carnegie Institution of Washington,

No. 105, 1909.

24. L E Dickson, *History of the Theory of Numbers* (3 volumes) (New York, 1919-23, reprinted 1966).
25. Martin Aigner, Günter M. Ziegler: *Proofs from the book*. Εκδόσεις: Springer, Third Edition, p. 3, 2000.
26. Pengelley, D. & Richman, F. (2006), "*Did Euclid need the Euclidean algorithm to prove unique factorization?*", The American mathematical monthly, Vol.113, No3, pp196-205.
27. Ramanujan, S. (1919). "*A proof of Bertrand's postulate*". Journal of the Indian Mathematical Society 11: 181–182.
28. Ribenboim, P. *The New Book of Prime Number Records*. New York: Springer-Verlag, pp. 20-21, 1996.
29. Rosen, K.H. (1986), "*Elementary number theory and its applications*", Addison-Wesley.
30. Sabbagh, K. (2004), "*The Riemann hypothesis*", Farrar, Straus and Giroux.
31. Séroul, R. *"Wilson's Theorem."* §2.9 in Programming for Mathematicians. Berlin: Springer-Verlag, pp. 16-17, 2000.
32. Shanks, D. Ex. 162 in *Solved and Unsolved Problems in Number Theory*, 4th ed. New York: Chelsea, p. 222, 1993.
33. Sloane, N. J. A. and Plouffe, S. *The Encyclopedia of Integer Sequences*. San Diego, CA: Academic Press, 1995. (A005846/M5273, A007635, A007641, A014556, A048988, A050265, A050266, A050267, A050268, A066386, A119276, A122131, A001783/M0921, A002144/M3823, A005098, A103131, A112448, A051021, A051254, A086238 and A108739).
34. Tietze, H. *"Prime Numbers and Prime Twins."* Ch. 1 in Famous Problems of Mathematics: Solved and Unsolved Mathematics Problems from Antiquity to Modern Times. New York: Graylock Press, pp. 1-20, 1965.
35. Wells, D. *The Penguin Dictionary of Curious and Interesting Numbers*. Middlesex, England: Penguin Books, 1986.
36. Κέντρο έρευνας επιστήμης και εκπαίδευσης (2001), *Ευκλείδη 'Στοιχεία'.*
37. *http://primes.utm.edu/largest.html*
38. *http://mathworld.wolfram.com/SieveofEratosthenes.html*

39. *http://www.gap-system.org/~history/Biographies/Eratosthenes.html*
40. *http://isaacmmcphee.suite101.com/ancient-babylonian-mathematics-a49377*
41. *http://www.math.dartmouth.edu/~euler/*
42. *http://cseweb.ucsd.edu/~gill/BWLectSite/Resources/C1U2Lo.pdf*
43. *http://www.math.dartmouth.edu/~euler/correspondence/letters/OO0765.pdf*