ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Οι Πρώτοι Αριθμοί

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΛΑΡΕΝΤΖΑΚΗ ΕΥΑΓΓΕΛΙΑ

Επιβλέπουσα : Λαμπροπούλου Σοφία
Αν. Καθηγήτρια Ε.Μ.Π.

Αθήνα, Ιούνιος 2012

Η σελίδα αυτή είναι σκόπιμα λευκή.

Υπόδειγμα φύλλου τίτλου (μπροστινή σελίδα) του αντιτύπου που υποβάλλεται στις βιβλιοθήκες (διπλωματική εργασία)

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Οι Πρώτοι Αριθμοί

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΛΑΡΕΝΤΖΑΚΗ ΕΥΑΓΓΕΛΙΑΣ

Επιβλέπουσα : Λαμπροπούλου Σοφία
Αν. Καθηγήτρια Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Σοφία Λαμπροπούλου	Αριστείδης Κοντογεώργης	Αριστείδης Αραγεώργης
Αν. Καθηγήτρια Ε.Μ.Π.	Αν. Καθηγητής Ε.Κ.Π.Α.	Επικ. Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2012

(Υπογραφή)

.....

ΛΑΡΕΝΤΖΑΚΗ ΕΥΑΓΓΕΛΙΑ

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 παρουσιάζονται αναλυτικά οι μεγάλοι μαθηματικοί που μελέτησαν τους πρώτους αριθμούς και παρατίθενται τα σημαντικότερα Θεωρήματα, οι σημαντικότερες αποδείξεις αυτών και οι σημαντικότερες παρατηρήσεις που έχουν γίνει ως προς αυτούς από την αρχαιότητα μέχρι τα νεότερα χρόνια. Συγκεκριμένα αποδεικνύεται ότι οι πρώτοι αριθμοί είναι άπειροι, διατυπώνεται και αποδεικνύεται το Θεμελιώδες Θεώρημα της Αριθμητικής, ορίζονται και μελετώνται οι πρώτοι αριθμοί του Fermat και οι αριθμοί Mersenne.

Στο τρίτο κεφάλαιο μελετάται η προσπάθεια εύρεσης ενός τύπου που να μπορεί να παράγει όλους τους πρώτους αριθμούς. Μέσα από την προσπάθεια αυτή υπήρξαν σημαντικές ανακαλύψεις και συμπεράσματα τα οποία και καταγράφονται.

Στο τέταρτο κεφάλαιο αναφέρονται κάποια προβλήματα σχετικά με τους πρώτους αριθμούς, τα οποία είναι άλυτα ως τις μέρες μας. Ιδιαίτερη έμφαση δίνεται σε δύο από αυτά που έχουν απασχολήσει περισσότερο τους μαθηματικούς.

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

Κλείνοντας θα ήθελα να ευχαριστήσω ιδιαίτερα την επιβλέπουσα αυτής της διπλωματικής εργασίας κ. Σοφία Λαμπροπούλου, Αναπληρώτρια Καθηγήτρια του Ε.Μ.Π., για την καθοδήγηση, τις συμβουλές, την υπομονή και το χρόνο που μου προσέφερε και να τονίσω πως χωρίς την συμβολή της δεν θα ήταν δυνατή η άρτια ολοκλήρωση αυτής της εργασίας. Επίσης θέλω να ευχαριστήσω και τα μέλη της τριμελούς εξεταστικής επιτροπής: την κ. Λαμπροπούλου Σ., τον κ. Κοντογεώργη Αρ. Αναπληρωτή Καθηγητή Τμήματος Μαθηματικών Ε.Κ.Π.Α. και τον κ. Αραγεώργη Αρ. Επίκουρο Καθηγητή του Τομέα ΑΚΕΔ της Σ.Ε.Μ.Φ.Ε. του Ε.Μ.Π.

Η σελίδα αυτή είναι σκόπιμα λευκή.

Abstract

The subject of this diploma thesis is prime numbers. Specifically, in the first chapter we present a brief history in which we study the definition of prime numbers, which are the numbers that can only be divided by one and themselves, their main uses, when they started to concern the mathematicians and why they are so interesting.

In the second chapter, we present all the great mathematicians who studied the prime numbers and we refer to the most important Theorems, the most important proofs and the most important observations made, from antiquity to modern times. Analytically, it is shown that the prime numbers are infinite, the Fundamental Theorem of Arithmetic is stated and proved and Fermat numbers and Mersenne numbers are defined and studied.

In the third chapter, we study the attempt of the mathematicians to find a formula that produces all prime numbers. Through this effort there have been significant discoveries and conclusions which are recorded.

In the fourth chapter, some problems about prime numbers, which are unsolved until today, are presented. Particular emphasis is given to two of them which have occupied most mathematicians.

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

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1

Εισαγωγή

1.1 Οι πρώτοι αριθμοί μέσα στην Ιστορία

Υπάρχουν πολλοί άνθρωποι που αφιέρωσαν όλη τους την ζωή μελετώντας Μαθηματικά. Σε κάποιους αυτό φαίνεται περίεργο όμως αυτοί οι άνθρωποι δεν διαφέρουν σε τίποτα από κάποιους άλλους που αφιέρωσαν όλη τους την ζωή στο να συνθέτουν μουσική. Τα Μαθηματικά κρύβουν μία μαγεία μεγάλη, που όμως δεν γίνεται αισθητή στους περισσότερους. Ένας μαθηματικός προσπαθεί να λύσει ένα πρόβλημα και μέσα από αυτή την διεργασία προκύπτουν και άλλα προβλήματα και ερωτήματα που πρέπει να λυθούν και να απαντηθούν. Αυτό το αιώνιο παιχνίδι είναι που προκαλεί το μυαλό των Μαθηματικών. Είναι η δίψα για να βρουν την λύση καθώς και η δίψα για την δόξα που θα αποκτήσουν, μιας και το όνομά τους θα χαραχτεί στην ιστορία αν καταφέρουν να απαντήσουν σε ένα από τα πολλά αναπάντητα προβλήματα που υπάρχουν μέσα στους αιώνες.

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...

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

Το κόσκινο του Ερατοσθένη είναι ακόμη και σήμερα ένας από τους πιο αποδοτικούς τρόπους 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. Σε λίγο χρόνο αναμένεται να δούμε τον πρώτο πρώτο αριθμό με δέκα εκατομμύρια ψηφία.

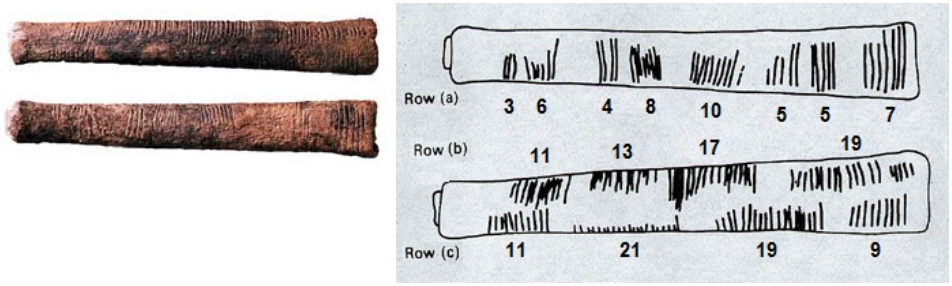
2

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

Δεν είναι σαφές πότε ακριβώς οι άνθρωποι πρωτοξεκίνησαν να μελετάνε τα μυστήρια των πρώτων αριθμών. Το *οστό Ishango*, το οποίο βρέθηκε στο ομώνυμο χωριό στα σύνορα Ουγκάντας και Ζαΐρ το 1960, φυλάσσεται στο Βασιλικό Ινστιτούτο Φυσικών Επιστημών στις Βρυξέλλες και χρονολογείται στην Παλαιολιθική Εποχή, πριν από το 10000 π.Χ., δείχνει ότι οι άνθρωποι ίσως γνώριζαν τους πρώτους αριθμούς χιλιάδες χρόνια πριν. Είναι ένα οστό που φέρει χαραγμένους στην μία του πλευρά μόνο πρώτους αριθμούς (11, 13, 17, 19), (βλ. Εικόνα 1). Δεν είναι γνωστή η χρησιμότητα αυτού αλλά και παρόμοιων οστών που έχουν ανακαλυφτεί. Πολλοί το θεωρούν απλά μια σύμπτωση καθώς αυτοί οι αριθμοί θα μπορούσαν να είναι οι ακέραιοι περιττοί προσθετέοι του συνόλου 60.



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

Είναι οι αρχαίοι Έλληνες όμως που παίρνουν τα εύσημα ότι εκείνοι πρώτοι ασχολήθηκαν με τους πρώτους αριθμούς όπως αυτοί πραγματικά είναι. Οι μαθηματικοί της σχολής του Πυθαγόρα (500-300 π.Χ.) ενδιαφέρθηκαν για τις μυστικιστικές και αριθμητικές ιδιότητες των αριθμών. Καταλάβαιναν την ιδέα των πρώτων και ενδιαφέρονταν για τους *τέλειους* και τους *φιλικούς αριθμούς*.
Ορισμός 2:*Τέλειος αριθμός* ονομάζεται ο αριθμός που το άθροισμα των διαιρετών του ισούται με τον ίδιο τον αριθμό. Για παράδειγμα ο αριθμός 6 έχει διαιρέτες του τους 1,2,3 και 1+2+3=6. Όμοια το 28 έχει διαιρέτες 1,2,4,7,14 και 1+2+4+7+14=28.
Ορισμός 3: Ένα *ζεύγος φιλικών αριθμών* είναι ένα ζεύγος αριθμών που οι διαιρέτες του ενός έχουν ως άθροισμα τον άλλο και αντίστροφα (όπως οι 220 και 284). Έως ότου γραφούν τα «Στοιχεία» του Ευκλείδη στα 300 π.Χ, αρκετά σημαντικά αποτελέσματα για τους πρώτους είχαν ήδη αποδειχτεί.

2.3.1 Ευκλείδης

Το πιο σημαντικό έργο στην ιστορία των ελληνικών μαθηματικών είναι αναμφίβολα τα «Στοιχεία» του Ευκλείδη. Παρά τη μεγάλη του φήμη, ελάχιστα είναι γνωστά για την ζωή του Ευκλείδη, ούτε καν ο τόπος γέννησής του. Τα Στοιχεία αποτελούνται από 13 βιβλία και καλύπτουν την Στοιχειώδη Επιπεδομετρία, την Θεωρία Αριθμών, την Θεωρία των Ασύμμετρων και την Στερεομετρία. Στο βιβλίο IX των Στοιχείων βρίσκουμε την περίφημη απόδειξη, η οποία, με σύγχρονη ορολογία δηλώνει ότι υπάρχουν άπειροι πρώτοι αριθμοί. Στην πραγματικότητα, ο Ευκλείδης σκόπιμα αποφεύγει την αναφορά στο άπειρο. Δηλώνει ότι «οι πρώτοι αριθμοί είναι περισσότεροι από οποιοδήποτε δεδομένο πλήθος πρώτων αριθμών» και προχωρεί στην απόδειξη αυτού του θεωρήματος για μόνο τρεις δεδομένους πρώτους. Η απαραίτητη επέκταση στους υπόλοιπους πρώτους αριθμούς θεωρείται αυτονόητη. Στο ίδιο βιβλίο ο Ευκλείδης φτάνει πολύ κοντά και στην απόδειξη του Θεμελιώδους Θεωρήματος της Αριθμητικής. Τα Στοιχεία υπήρξαν το πιο σημαντικό εγχειρίδιο όλων των εποχών. Αντιγράφτηκε και ξαναντιγράφτηκε με σχόλια πάνω σε προηγούμενα σχόλια, μεταφράστηκε και προσαρμόστηκε στις ανάγκες και στην κουλτούρα διάφορων πολιτισμών. Είναι σχεδόν αδύνατον να ανασυστήσει κανείς το αρχικό έργο του Ευκλείδη, καθώς ολοκληρωμένα αντίγραφα έχουμε μόνο μετά τον 9^{ο} αιώνα μ.Χ.

Εικόνα 2: Ευκλείδης

Θεώρημα 1 (Ευκλείδης 400 π.Χ.)**:** *Το σύνολο των πρώτων αριθμών είναι άπειρο.*

1^{η} Απόδειξη (Ευκλείδης)**:** Για κάθε πεπερασμένο σύνολο $\{p_1, \dots, p_r\}$ πρώτων αριθμών θεωρούμε τον αριθμό $n = p_1 p_2 \dots p_r + 1$. Αυτός ο αριθμός n έχει έναν πρώτο διαιρέτη p. Αλλά ο p δεν είναι κανένας από τους p_i, αλλιώς ο p θα ήταν διαιρέτης του n και του γινομένου $p_1 p_2 \dots p_r$, και έτσι επίσης της διαφοράς $n -$

$p_1 p_2 \dots p_r$=1, το οποίο είναι αδύνατον. Έτσι, το πεπερασμένο σύνολο $\{p_1, \dots, p_r\}$ δεν μπορεί να είναι η συλλογή όλων των πρώτων αριθμών. □

Μέχρι σήμερα έχουν βρεθεί και άλλες πέντε αποδείξεις για το Θεώρημα 1, οι οποίες είναι οι παρακάτω. [Martin Aigner, Günter M. Ziegler: *Proofs from the book.* Εκδόσεις: Springer, Third Edition, p. 3, 2000.] Στο 3ο κεφάλαιο παραθέτουμε μία ακόμη απόδειξη του θεωρήματος αυτού από τον Euler (παρόμοια με την 3η απόδειξη εδώ από τον ίδιο) και η οποία μας βοηθάει να προχωρήσουμε σε κάποια συμπεράσματα.

Ορισμός 4: Οι αριθμοί της μορφής $F_n = 2^{2^n} + 1$ όπου $n = 0,1,2, \dots$ ονομάζονται *αριθμοί του Fermat*.

2η Απόδειξη (Christian Goldbach, 1730, σε γράμμα του προς τον Leonhard Euler)**:** Θα δείξουμε ότι οποιοιδήποτε δύο αριθμοί του Fermat είναι πρώτοι προς αλλήλους, ως εκ τούτου θα πρέπει να υπάρχουν άπειροι πρώτοι αριθμοί. Για τον σκοπό αυτό επαληθεύουμε τον αναδρομικό τύπο

$$\prod_{k=0}^{n-1} F_k = F_n - 2 \quad (n \geq 1),$$

από τον οποίο ο ισχυρισμός μας προκύπτει άμεσα. Πράγματι, αν ο m είναι διαιρέτης των F_k και F_n $(για\ κάποιο\ k < n)$, τότε ο m διαιρεί το 2, και γι' αυτό m=1 ή 2. Αλλά είναι αδύνατον m=2 αφού όλοι οι αριθμοί του Fermat είναι περιττοί. Για να αποδείξουμε τον αναδρομικό τύπο χρησιμοποιούμε επαγωγή στο n. Για $n = 1$ έχουμε $F_0 = 3$ και $F_1 - 2 = 3$. Με επαγωγή καταλήγουμε

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) F_n = (F_n - 2)F_n = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) = 2^{2^n} - 1 = F_{n+1} - 2.$$

□

Ορισμός 5: Ορίζουμε την συνάρτηση $\pi: \mathbb{R} \to \mathbb{N}$ ως: $\pi(x) \coloneqq \#\{p \leq x : p \in \mathbb{P}\}$ τον αριθμό των πρώτων αριθμών που είναι μικρότεροι ή ίσοι από τον πραγματικό αριθμό x.

3η Απόδειξη (Leonhard Euler)**:** Αριθμούμε τους πρώτους αριθμούς $\mathbb{P} = \{p_1, p_2, p_3, \dots\}$ σε αύξουσα σειρά. Θεωρούμε τον φυσικό λογάριθμο

$$\log x = \int_1^x \frac{1}{t}\, dt.$$

Τώρα συγκρίνουμε την περιοχή κάτω από την γραφική παράσταση της $f(t) = \frac{1}{t}$ με μία ανώτερη συνάρτηση βαθμίδας (upper step function). Έτσι, για $n \leq x < n+1$ έχουμε

$$\log x \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n} \leq \sum \frac{1}{m},$$

όπου το άθροισμα επεκτείνεται σε όλους τους $m \in \mathbb{N}$ που έχουν μόνο πρώτους διαιρέτες $p \leq x$. Αφού κάθε τέτοιος αριθμός m μπορεί να γραφεί με *μοναδικό τρόπο* ως γινόμενο της μορφής $\prod_{p \leq x} p^{k_p}$, βλέπουμε πως το τελευταίο άθροισμα είναι ίσο με

$$\prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(\sum_{k \geq 0} \frac{1}{p_k} \right).$$

Το εσωτερικό άθροισμα είναι γεωμετρική πρόοδος με λόγο $\frac{1}{p}$, ως εκ τούτου

$$\log x \leq \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{1 - \frac{1}{p}} = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

Προφανώς $p_k \geq k+1$ και έτσι

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

και άρα

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

Η $\log x$ δεν είναι φραγμένη, άρα καταλήγουμε στο 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 Oείναι κενό, ή αν για κάθε $a \in O$ υπάρχει κάποιο $b > 0$ με $N_{a,b} \subseteq O$. Προφανώς η ένωση των 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 $N_{a,b_2} \subseteq O_2$, τότε $a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. 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

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

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

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

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

Τώρα αν το $\mathbb{P}$ ήταν πεπερασμένο, τότε η $\cup_{p\in\mathbb{P}} N_{0,p}$ 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 Erdos, ~1950)**:** Αυτή η απόδειξη δεν δείχνει μόνο ότι υπάρχουν άπειροι πρώτοι αριθμοί, αλλά επίσης ότι η σειρά $\sum_{p\in\mathbb{P}} \frac{1}{p}$ αποκλίνει. Η πρώτη απόδειξη αυτού του σημαντικού αποτελέσματος δόθηκε από τον Euler, αλλά αυτή η απόδειξη από τον Erdos είναι πραγματικά πολύ όμορφη.

Θεωρούμε $p_1, p_2, p_3, \ldots$ την ακολουθία των πρώτων αριθμών σε αύξουσα σειρά και υποθέτουμε ότι η $\sum_{p\in\mathbb{P}} \frac{1}{p}$ συγκλίνει. Τότε θα πρέπει να υπάρχει ένας φυσικός αριθμός k τέτοιος ώστε $\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}$. Καλούμε τους $p_1, \ldots, p_k$ 'μικρούς' πρώτους και τους $p_{k+1}, p_{k+2}, \ldots$ 'μεγάλους' πρώτους. Για έναν αυθαίρετο φυσικό αριθμό N επομένως βρίσκουμε

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

Θεωρούμε N_b τον αριθμό των θετικών ακεραίων $n \leq N$ οι οποίοι διαιρούνται από τουλάχιστον ένα 'μεγάλο' πρώτο, και N_s τον αριθμό των θετικών ακεραίων $n \leq N$ οι

οποίοι έχουν μόνο ‘μικρούς’ πρώτους διαιρέτες. Εξ ορισμού $N_b + N_s$ θα πρέπει να είναι ίσο με N. Πρόκειται να δείξουμε πως για κατάλληλο N

$$N_b + N_s < N,$$

το οποίο θα είναι η επιθυμητή μας αντίφαση. Για να εκτιμήσουμε το N_b σημειώνουμε ότι το ακέραιο μέρος $\left\lfloor \frac{N}{p_i} \right\rfloor$ μετράει τους θετικούς ακεραίους $n \leq N$ που είναι πολλαπλάσια του p_i. Άρα από την (1) βρίσκουμε

$$N_b \leq \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2} \quad (2)$$

Ας δούμε τώρα το N_s. Γράφουμε κάθε $n \leq N$ που έχει μόνο ‘μικρούς’ πρώτους διαιρέτες στην μορφή $n = a_n {b_n}^2$, όπου a_n είναι το ελεύθερο από τετράγωνα μέρος. Κάθε a_n είναι έτσι ένα γινόμενο από *διαφορετικούς* μικρούς πρώτους, και καταλήγουμε στο ότι υπάρχουν ακριβώς 2^k διαφορετικά μέρη ελεύθερα τετραγώνων. Επιπλέον, καθώς $b_n \leq \sqrt{n} \leq \sqrt{N}$, βρίσκουμε ότι υπάρχουν το πολύ $\sqrt{N}$ διαφορετικά κομμάτια στο τετράγωνο, και έτσι

$$N_s \leq 2^k \sqrt{N}.$$

Αφού η (2) ισχύει για κάθε N, μένει να βρούμε έναν αριθμό N με $2^k \sqrt{N} \leq \frac{N}{2}$ ή $2^{k+1} \leq \sqrt{N}$, και γι’ αυτό ο $N = 2^{2k+2}$ είναι κατάλληλος. □

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

Θεώρημα 2 (Θεώρημα Lagrange): *Αν G είναι μία πεπερασμένη ομάδα και U μία υποομάδα του, τότε το $|U|$ διαιρεί το $|G|$.*

6η Απόδειξη (Αγνώστου)**:** Υποθέτουμε ότι το $\mathbb{P}$ είναι πεπερασμένο και ο p είναι ο μεγαλύτερος πρώτος. Θεωρούμε τους αριθμούς $2^p - 1$ (Mersenne αριθμοί, 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 $2^p \equiv 1 (mod\, q)$. 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 $p < q$.

Θεώρημα 3 (Το Θεμελιώδες Θεώρημα της Αριθμητικής): *Κάθε φυσικός αριθμός* $n \neq 0$ *εκφράζεται μονοσήμαντα ως γινόμενο πρώτων αριθμών, όχι κατ' ανάγκη διαφόρων μεταξύ τους. Η σειρά των παραγόντων δεν λαμβάνεται υπόψη.*

Απόδειξη: Για $n = 1$ η πρόταση είναι προφανώς αληθής, αν ορισθεί σαν γινόμενο 0 παραγόντων ο φυσικός αριθμός 1.

Έστω $n > 1$. Υποθέτουμε ότι η πρόταση είναι αληθής για όλους τους φυσικούς αριθμούς τους μικρότερους του n και διάφορους του 0 και θα αποδείξουμε ότι ισχύει και για τον n. Έστω, προς τούτο, p_1 ο *ελάχιστος* πρώτος διαιρέτης του n και έστω $n = p_1 m$. Επειδή είναι $m < n$, από υπόθεση επαγωγής ο m εκφράζεται μονοσήμαντα ως γινόμενο πρώτων αριθμών. Έστω

$$m = p_2 p_3 \dots p_r.$$

Λαμβάνουμε λοιπόν μια ανάλυση:

$$n = p_1 m = p_1 p_2 \dots p_r$$

του n σε γινόμενο πρώτων αριθμών.

Αποδεικνύουμε τώρα ότι η ανάλυση $n = p_1 m = p_1 p_2 \dots p_r$ είναι μονοσήμαντη.

Έστω

$$n = q_1 q_2 \dots q_s$$

μια άλλη ανάλυση του n διαφορετική από την προηγούμενη. Μεταξύ των $q_1, q_2, \dots, q_s$ δεν περιέχεται ο p_1, διότι ισχύει $n = p_1 m$ και η ανάλυση του $m = p_2 p_3 \dots p_r$ είναι μονοσήμαντη. Επειδή ο p_1 είναι ο ελάχιστος πρώτος διαιρέτης του n, προκύπτει $p_1 < q_1$. Θέτουμε:

$$q_2 q_3 \dots q_s = l$$

και θεωρούμε τον αριθμό

$$n_0 = n - p_1 l = \begin{cases} p_1(m - l) \\ (q_1 - p_1) l \end{cases}$$

Προφανώς οι αριθμοί $n_0, m - l, q_1 - p_1, l$ είναι φυσικοί αριθμοί διάφοροι του 0 και μικρότεροι του n. Άρα ισχύει για αυτούς η μονοσήμαντη ανάλυση σε γινόμενο πρώτων αριθμών. Από την σχέση $n_0 = p_1(m - l)$ προκύπτει ότι στην ανάλυση του n_0 παρουσιάζεται ο p_1. Από την σχέση $p_1(m - l) = (q_1 - p_1) l$ προκύπτει ότι ο p_1 θα παρουσιάζεται στην ανάλυση του l ή του $q_1 - p_1$. Επειδή όμως $p_1 \neq q_i, i = 2,3, \dots, s$, προκύπτει ότι ο p_1 δεν παρουσιάζεται στην ανάλυση του l. Άρα θα πρέπει

να ισχύει $p_1 \mid q_1 - p_1$. Συνεπώς και $p_1 \mid q_1 - p_1 + p_1$, άρα $p_1 \mid q_1$, το οποίο είναι άτοπο.

Άρα η ανάλυση του n σε γινόμενο πρώτων παραγόντων είναι μονοσήμαντη. □

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 $\lfloor \sqrt{n} \rfloor$. 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 $\lfloor \sqrt{50} \rfloor = 7$. 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 τη ρωμαϊκή κατάκτηση των Ελλήνων, ένα μεγάλο μέρος της γραπτής ελληνικής γνώσης μεταφράστηκε στα Λατινικά, ή τουλάχιστον διατηρήθηκε. Καθώς οι Έλληνες δίδασκαν στους Ρωμαίους τις γνώσεις τους, διέσωσαν την ελληνική μαθηματική γνώση, αλλά δεν έκαναν καμία περαιτέρω πρόοδο στη μελέτη των καθαρών μαθηματικών, όπως είναι οι πρώτοι αριθμοί.

Οι Άραβες μαθηματικοί του Μεσαίωνα μελέτησαν το έργο των αρχαίων Ελλήνων μαθηματικών, αλλά με το επιπρόσθετο πλεονέκτημα ενός αριθμητικού συστήματος πιο δεκτικού σε υπολογιστική εργασία. Ο Thabit ibn Qurra, για παράδειγμα, απέδειξε τον $10^{ο}$ αιώνα τη σχέση ανάμεσα στους διαδοχικούς πρώτους Thabit αριθμούς (όπως ορίζονται παρακάτω) και τους φιλικούς αριθμούς.

Ορισμός 6: *Πρώτοι Thabit αριθμοί* ονομάζονται οι αριθμοί της μορφής $p_n = 3 \times 2^n - 1$ και 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 γενικεύτηκε από τον Euler [Borho 1972])

Θεώρημα 4 *(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

Οι επόμενες σημαντικές εξελίξεις έγιναν από τον Fermat (1601-1665) στις αρχές του 17ου αιώνα. 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 μπορούσε 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 $2027651281 = 44021 \times 46061$. Απέδειξε αυτό που είναι γνωστό ως το 'μικρό Θεώρημα του Fermat' (για να ξεχωρίζει από αυτό που είναι γνωστό ως το 'μεγάλο Θεώρημα του Fermat').

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 a *ισότιμο του* b πληρεί τις τρεις χαρακτηριστικές ιδιότητες μιας σχέσης ισοδυναμίας.

i. $a \equiv a \bmod m \; \forall a \in \mathbb{Z}$
ii. $a \equiv b \bmod m \Longrightarrow b \equiv a \bmod m$
iii. $a \equiv b \bmod m, b \equiv c \bmod m \Longrightarrow a \equiv c \bmod m$

Θεώρημα 5 (μικρό Θεώρημα του Fermat): *Έστω πρώτος αριθμός. Τότε για κάθε ακέραιο έχουμε .*

Αυτό αποδεικνύει μόνο τη μισή 'Κινέζικη Εικασία' (η οποία χρονολογείται περίπου 2000 χρόνια νωρίτερα), δηλαδή το ότι ένας ακέραιος είναι πρώτος αν και μόνο αν ο αριθμός διαιρείται από τον . Η άλλη μισή εικασία είναι λάθος, αφού για παράδειγμα ο διαιρείται από το 341 παρόλο που ο 341=31×11 είναι σύνθετος. Το 'μικρό Θεώρημα του Fermat' είναι η βάση για πολλά άλλα αποτελέσματα στην Θεωρία Αριθμών και είναι επίσης η βάση μεθόδων για να ελέγχουμε αν ένας αριθμός είναι πρώτος, που χρησιμοποιείται ακόμα και σήμερα στους ηλεκτρονικούς υπολογιστές.

Εικόνα 5: Pierre de Fermat

Πρώτοι Αριθμοί του Fermat

Μελετάμε τώρα τους αριθμούς της μορφής . Για να είναι ο αριθμός πρώτος, πρέπει ο να είναι δύναμη του 2, διότι αν είναι με περιττό, τότε από την σχέση προκύπτει ότι ο δεν είναι πρώτος αριθμός. Οι πρώτοι αριθμοί της μορφής καλούνται *πρώτοι αριθμοί του Fermat*, διότι έχουν μελετηθεί πρώτα από αυτόν. Για λαμβάνουμε αντίστοιχα τους πρώτους αριθμούς 3, 5, 17, 257, 65.537.

Εικασία του Fermat: *Για όλους τους φυσικούς αριθμούς , οι αριθμοί είναι πρώτοι.*

Η εικασία αυτή του Fermat δεν είναι αληθής, όπως διαπιστώνουμε εξετάζοντας την περίπτωση .

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

$$(641 - 2^4) \times 2^{28} = t \times 641 + 1 \Leftrightarrow$$
$$-2^{32} = (t - 2^{28}) \times 641 + 1 = s \times 641 + 1 \Leftrightarrow$$
$$2^{32} + 1 = (-s) \times 641$$

Άρα

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

□

Την παραπάνω απέδειξε ο Euler (1707-1783) καταρρίπτοντας την θεωρία του Fermat.

Επίσης διάφοροι συγγραφείς διαπίστωσαν ότι οι αριθμοί $2^{2^n} + 1$ δεν είναι πρώτοι για $n = 6, 7, 8, 9, 11, 12, 15, 18, 23, 36, 38, 73$. Ακόμη 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. Παραδόξως, οι πρώτοι αριθμοί του Fermat σχετίζονται με την γεωμετρία. Ο διάσημος Γερμανός μαθηματικός Carl Friedrich Gauss απέδειξε ότι:

Θεώρημα 6 (Gauss): *Ένα κανονικό ν-γωνο, όπου ν πρώτος αριθμός, μπορεί να κατασκευαστεί με κανόνα και διαβήτη αν και μόνο αν ο ν είναι πρώτος αριθμός του Fermat!*

Ένα γενικότερο εξαγόμενο είναι το παρακάτω:

Θεώρημα 7: *Ένα κανονικό m-γωνο μπορεί να κατασκευαστεί με κανόνα και διαβήτη αν και μόνο αν* $m = 2^s \times p_1 p_2 \dots p_l$, *όπου* $p_1, p_2, \dots, p_l$ *είναι πρώτοι αριθμοί του Fermat διαφορετικοί μεταξύ τους.*

Ένα άλλο Θεώρημα που διατύπωσε ο Fermat, αλλά δεν απέδειξε και προβλημάτισε τους μετέπειτα μαθηματικούς είναι αυτό πάνω στο άθροισμα δύο τετραγώνων. Ο

G.H.Hardy γράφει ότι αυτό το Θεώρημα του Fermat δίκαια έχει χαρακτηριστεί ως ένα από τα καλύτερα στην Θεωρία Αριθμών.

Θεώρημα 8 (Fermat, 1640)**:***Ένας περιττός πρώτος αριθμός p μπορεί να γραφτεί ως*

$$p = x^2 + y^2$$

όπου x, y ακέραιοι αν και μόνο αν $p \equiv 1 \; mod \; 4$.

Έχουν δημοσιευθεί πάνω από 50 αποδείξεις γι' αυτό το Θεώρημα από πολύ μεγάλους μαθηματικούς όπως: Euler, Lagrange, Dedekind, Heath-Brown, και άλλους. Παραθέτονται παρακάτω οι πιο σημαντικές.

1η Απόδειξη (Euler, 1747-1749)**:**

Αυτή η απόδειξη αποτελείται από 5 βήματα. Τα 4 πρώτα περιλαμβάνονται σε γράμμα του Euler προς τον Goldbach το 1747 ενώ το 5ο σε ένα άλλο γράμμα το 1749 γιατί στο πρώτο γράμμα ήταν ασαφές.

1. Το γινόμενο δύο αριθμών καθένας από τους οποίους είναι άθροισμα δύο τετραγώνων, είναι και αυτός επίσης άθροισμα δύο τετραγώνων. Αυτό είναι απλή αναδιατύπωση της ταυτότητας Brahmagupta-Fibonacci:

$$(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2$$

2. Αν ένας αριθμός ο οποίος είναι άθροισμα δύο τετραγώνων διαιρείται από έναν πρώτο αριθμό που είναι άθροισμα δύο τετραγώνων, τότε το πηλίκο είναι άθροισμα δύο τετραγώνων.

Πράγματι, υποθέτουμε για παράδειγμα ότι $a^2 + b^2$ διαιρείται από $p^2 + q^2$ που είναι πρώτος αριθμός. Τότε ο $p^2 + q^2$ διαιρεί τον

$$(pb - aq)(pb + aq) = p^2b^2 - a^2q^2 = p^2(a^2 + b^2) - a^2(p^2 + q^2)$$

Αφού ο $p^2 + q^2$ είναι πρώτος, διαιρεί έναν από τους δύο παράγοντες. Υποθέτουμε ότι διαιρεί τον $pb - aq$. Εφόσον

$$(a^2 + b^2)(p^2 + q^2) = (ap + bq)^2 + (aq - bp)^2$$

(ταυτότητα Brahmagupta-Fibonacci) έπεται ότι ο $p^2 + q^2$ πρέπει να διαιρεί τον $(ap + bq)$. Μάλιστα, εφόσον $p^2 + q^2$ πρώτος, έπεται ότι η παραπάνω ισότητα μπορεί να διαιρεθεί από το τετράγωνο του $p^2 + q^2$. Διαιρώντας την έκφραση με τον $(p^2 + q^2)^2$ προκύπτει:

$$\frac{a^2 + b^2}{p^2 + q^2} = \left(\frac{ap + ba}{p^2 + q^2}\right)^2 + \left(\frac{aq - bp}{p^2 + q^2}\right)^2$$

και έτσι εκφράζεται το πηλίκο ως άθροισμα δύο τετραγώνων όπως ισχυριστήκαμε. Αν p^2+q^2 διαιρεί τον $pb+aq$ καταλήγουμε σε ένα παρόμοιο συμπέρασμα χρησιμοποιώντας την ταυτότητα Brahmagupta-Fibonacci:

$$(a^2+b^2)(q^2+p^2)=(aq+bp)^2+(ap-bq)^2$$

3. Αν ένας αριθμός ο οποίος μπορεί να γραφτεί ως άθροισμα δύο τετραγώνων, διαιρείται από έναν αριθμό που δεν είναι άθροισμα δύο τετραγώνων, τότε το πηλίκο έχει έναν παράγοντα ο οποίος δεν είναι άθροισμα δύο τετραγώνων.

Πράγματι, υποθέτουμε ότι ο x διαιρεί τον a^2+b^2 και ότι το πηλίκο αναλυμένο σε γινόμενο πρώτων παραγόντων είναι $p_1p_2\dots p_n$. Τότε $a^2+b^2=xp_1p_2\dots p_n$. Αν όλοι οι παράγοντες p_i μπορούν να γραφτούν ως αθροίσματα δύο τετραγώνων, τότε μπορούμε να διαιρέσουμε τέλεια τον a^2+b^2 με τους $p_1, p_2,$ ... και εφαρμόζοντας το προηγούμενο βήμα διαδοχικά για τους $xp_1p_2\dots p_n$, $xp_1p_2\dots p_{n-1}$, …, xp_1 συμπεραίνουμε ότι κάθε πηλίκο είναι άθροισμα δύο τετραγώνων. Αυτό μέχρι να φτάσουμε στον x, καταλήγοντας ότι ο x θα πρέπει να είναι άθροισμα δύο τετραγώνων, άτοπο. Έτσι, αν ο x δεν είναι άθροισμα δύο τετραγώνων, τότε τουλάχιστον ένας από τους πρώτους p_i δεν είναι άθροισμα δύο τετραγώνων.

4. Αν a και b είναι πρώτοι μεταξύ τους τότε κάθε παράγοντας του a^2+b^2 είναι άθροισμα δύο τετραγώνων.

Πράγματι, θεωρούμε x έναν παράγοντα του a^2+b^2. Μπορούμε να γράψουμε $a=mx\pm c, b=nx\pm d$ όπου c,d είναι το πολύ το μισό του x κατά απόλυτη τιμή. Αυτό δίνει: $a^2+b^2=m^2x^2\pm 2mxc+c^2+n^2x^2\pm 2nxd+d^2=Ax+(c^2+d^2)$. Άρα ο c^2+d^2 πρέπει να διαιρείται από τον x, έστω $c^2+d^2=yx$. Αν c και d δεν είναι πρώτοι μεταξύ τους, τότε ο ΜΚΔ τους δεν διαιρεί τον x (αν το έκανε, τότε θα διαιρούσε τους a και b που έχουμε υποθέσει ότι είναι πρώτοι μεταξύ τους). Οπότε, ο ΜΚΔ στο τετράγωνο διαιρεί τον y (καθώς διαιρεί τον c^2+d^2), δίνοντάς μας μια έκφραση της μορφής $e^2+f^2=zx$ για e και f πρώτους μεταξύ τους, και με z όχι μεγαλύτερο από το μισό του x, εφόσον

$$zx=e^2+f^2\le c^2+d^2\le(\frac{x}{2})^2+(\frac{x}{2})^2=\frac{1}{2}x^2$$

Αν c και d είναι πρώτοι μεταξύ τους, τότε μπορούμε να τους χρησιμοποιήσουμε κατευθείαν αντί να τους μετατρέψουμε σε e και f. Αν ο x δεν είναι άθροισμα δύο τετραγώνων τότε, από το 3^{ο} βήμα, πρέπει να υπάρχει ένας παράγοντας του z ο οποίος

δεν είναι άθροισμα δύο τετραγώνων, έστω w. Αυτό μας δίνει άπειρη κάθοδο, πηγαίνοντας από τον x σε ένα μικρότερο αριθμό w, που και οι δύο δεν είναι αθροίσματα δύο τετραγώνων αλλά διαιρούν ένα άθροισμα δύο τετραγώνων. Αφού η άπειρη κάθοδος είναι αδύνατη, καταλήγουμε ότι ο x μπορεί να εκφραστεί ως άθροισμα δύο τετραγώνων, όπως ισχυριστήκαμε.

5.Κάθε πρώτος της μορφής $4n+1$ είναι άθροισμα δύο τετραγώνων.

Αν $p=4n+1$ τότε $(p,x)=1$ για κάθε $x=1,2,3,\dots,x_n$ και, από το Μικρό Θεώρημα του Fermat, καθένας από τους αριθμούς $1, 2^{4n}, 3^{4n}, \dots, (4n)^{4n}$ είναι ισότιμος με $1 \, mod \, p$. Οι διαφορές $2^{4n}-1, 3^{4n}-2^{4n}, \dots, (4n)^{4n}-(4n-1)^{4n}$ διαιρούνται ως εκ τούτου από τον p. Κάθε μία από αυτές τις διαφορές μπορεί να παραγοντοποιηθεί ως

$$a^{4n}-b^{4n}=(a^{2n}+b^{2n})(a^{2n}-b^{2n})$$

Εφόσον ο p είναι πρώτος, πρέπει να διαιρεί έναν από τους δύο παράγοντες. Αν σε οποιαδήποτε από τις $4n-1$ περιπτώσεις ο p διαιρεί τον πρώτο παράγοντα, τότε από το προηγούμενο βήμα καταλήγουμε ότι ο p είναι ο ίδιος άθροισμα δύο τετραγώνων (εφόσον οι a και b διαφέρουν κατά 1, θα είναι πρώτοι μεταξύ τους). Έτσι είναι αρκετό να δείξουμε ότι ο p δεν μπορεί πάντα να διαιρεί τον δεύτερο παράγοντα. Αν διαιρεί όλες τις $4n-1$ διαφορές, $2^{2n}-1, 3^{2n}-2^{2n}, \dots, (4n)^{2n}-(4n-1)^{2n}$, τότε θα διαιρεί όλες τις $4n-2$ διαφορές των διαδοχικών όρων, όλες τις $4n-3$ διαφορές των διαφορών και ούτω καθεξής. Εφόσον οι k-οστές διαφορές της ακολουθίας $1^k, 2^k, 3^k, \dots$ είναι όλες ίσες με $k!$, οι $2n$-οστές διαφορές θα είναι όλες σταθερές και ίσες με $2n!$, οι οποίες σίγουρα δεν διαιρούνται από τον p. Ως εκ τούτου ο p δεν μπορεί να διαιρέσει όλους τους δεύτερους παράγοντες, το οποίο αποδεικνύει ότι ο p είναι όντως το άθροισμα δύο αριθμών στο τετράγωνο □.

Άλλη μία ενδιαφέρουσα απόδειξη για το ίδιο Θεώρημα του Fermat είναι αυτή του Don Bernard Zagier(1951) που ονομάζεται 'απόδειξη μιας πρότασης' γιατί είναι μικρή μα και στοιχειώδης. Η απόδειξη αυτή είναι η απλούστευση μιας παλαιότερης από τον Heath-Brown, η οποία με την σειρά της ήταν εμπνευσμένη από μία απόδειξη του Liouville.

<u>2η Απόδειξη</u> <u>(Zagier, περίπου το 1990)</u>**<u>:</u>**

Αν $p=4k+1$ είναι πρώτος τότε το σύνολο $S=\{(x,y,z)\in\mathbb{N}^3 : x^2+4yz=p\}$ είναι πεπερασμένο και έχει δύο ενελίξεις (involution), μία προφανή $(x,y,z)\rightarrow$

(x, y, z) της οποίας τα σταθερά σημεία αντιστοιχούν στις αναπαραστάσεις του p ως άθροισμα δύο αριθμών στο τετράγωνο και μία πιο περίπλοκη

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z), & \alpha\nu \quad x < y - z \\ (2y - x, y, x - y + z), & \alpha\nu \; y - z < x < 2y \\ (x - 2y, x - y + z, y), & \alpha\nu \quad x > 2y \end{cases}$$

η οποία έχει ακριβώς ένα σταθερό σημείο, το $(1,1,k)$. Ωστόσο ο αριθμός των σταθερών σημείων μιας ενός πεπερασμένου συνόλου S έχει την ίδια πληθικότητα με τον πληθικό αριθμό του συνόλου S, έτσι αυτός ο αριθμός είναι περιττός και για την πρώτη ενέλιξη επίσης, αποδεικνύοντας ότι ο p είναι άθροισμα δύο αριθμών στο τετράγωνο □.

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 $l > 1$, τότε 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 είναι πρώτος. Αυτό έθεσε ένα καινούριο ρεκόρ για άλλον έναν αιώνα ώσπου ο Édouard Lucas (1842-1891) έδειξε ότι ο (που είναι ένας αριθμός με 39 ψηφία) είναι πρώτος και κράτησε το ρεκόρ ως τα χρόνια των ηλεκτρονικών υπολογιστών. Το 1952 οι 'αριθμοί Mersenne'
και αποδείχθηκαν ότι είναι πρώτοι από την 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 ο οποίος έχει 7816230 ψηφία. Ο μεγαλύτερος πρώτος αριθμός ως τις 15 Σεπτεμβρίου 2008, ήταν ο ο οποίος έχει 12978189 ψηφία. (Mersenne Organization 2008)

Εικόνα 7: Pietro Cataldi

Εικόνα 8: Edouard Lucas

Εικόνα9: Mitchel Robinson

Οι 'αριθμοί Mersenne' έχουν ενδιαφέρον εξ' αιτίας της σχέσης τους με τους τέλειους αριθμούς (βλ. Ορισμό 2). Ο ίδιος ο Ευκλείδης, στο βιβλίο του τα 'Στοιχεία' που αναφέραμε προηγουμένως, απέδειξε το γεγονός ότι αν ένας πρώτος αριθμός είναι του τύπου , τότε ο αριθμός —— είναι τέλειος. Για παράδειγμα οι αριθμοί:

είναι πρώτοι και συνεπώς οι αριθμοί

——

——

είναι τέλειοι. Αρκετούς αιώνες αργότερα, ο Leonhard Euler (1707-1783) 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
$(2^{59}-1)/179951$	13	1867	Landry	δοκιμαστικές διαιρέσεις
$2^{127}-1$	39	1876	Lucas	ακολουθίες Lucas
$(2^{148}+1)/17$	44	1951	Ferrier	Θεώρημα του Proth (1878)

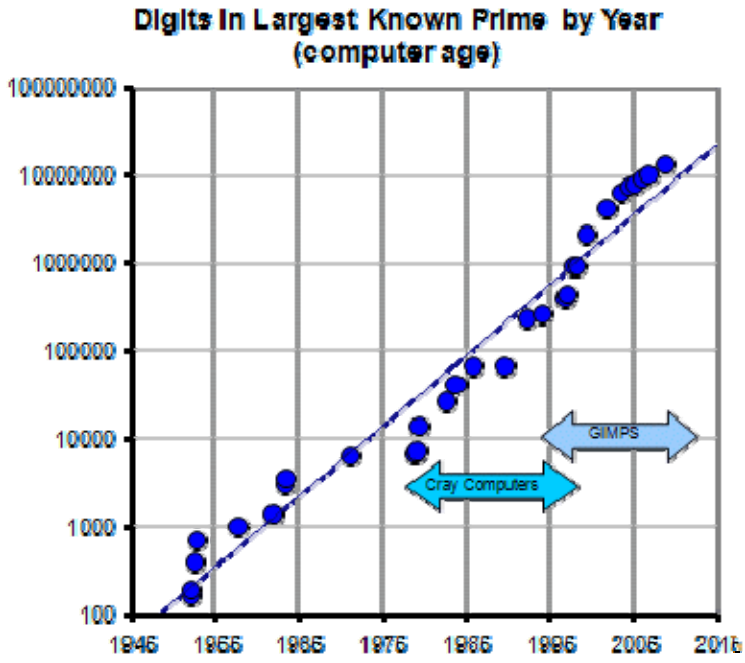
Πίνακας 2

Ρεκόρ πρώτων αριθμών την εποχή των ηλεκτρονικών υπολογιστών				
Αριθμός	**Ψηφία**	**Χρονιά**	**Η/Υ**	**Μαθηματικός**
$180(M_{127})^2+1$	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 (Oct 7)
M_{2281}	687	1952	SWAC	Robinson (Oct 9)

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)	Armengaud,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	AMDT-Bird(800 Mhz)	Cameron,Woltman, Kurowski
$M_{20996011}$	6320430	2003	Pentium (2 GHz)	Shafer,Woltman, Kurowski
$M_{24036583}$	7235733	2004	Pentium4(2.4GHz)	Findley,Woltman,

				Kurowski
$M_{25964951}$	7816230	2005	Pentium4(2.4GHz)	Nowak,Woltman, Kurowski
$M_{30402457}$	9152052	2005	Pentium 4(2GHz upgraded to3GHz)	Cooper,Boone, Woltman, Kurowski
$M_{32582657}$	9808358	2006	Pentium 4 (3 GHz)	Cooper,Boone, Woltman, Kurowski
$M_{43111609}$	12978189	2008	Intel Core 2Duo E6600CPU(2.4GHz)	E_Smith,Woltman, Kurowski

Πίνακας 3



Διάγραμμα 1: οι αριθμοί των ψηφίων γνωστών πρώτων αριθμών μετά την ανακάλυψη του ηλεκτρονικού υπολογιστή

3

Τύποι παραγωγής Πρώτων Αριθμών

Ο Euler έχει δηλώσει: «Οι μαθηματικοί έχουν προσπαθήσει μάταια μέχρι σήμερα να ανακαλύψουν κάποια τάξη στην ακολουθία των πρώτων αριθμών, και έχουμε λόγους να πιστεύουμε πως αυτό είναι ένα μυστήριο στο οποίο ο ανθρώπινος νους δεν πρόκειται να διεισδύσει ποτέ.» [Havil 2003, p. 163]. Σε μία διάλεξη του το 1975 ο D. Zagier σχολίασε: «Υπάρχουν δύο δεδομένα για την κατανομή των πρώτων αριθμών για τα οποία ελπίζω να σας πείσω τόσο πολύ που θα μείνουν για πάντα χαραγμένα στις καρδιές σας. Το πρώτο είναι ότι παρόλο τον απλό ορισμό και ρόλο τους ως δομικοί λίθοι των φυσικών αριθμών, οι πρώτοι αριθμοί μεγαλώνουν σαν τα ζιζάνια μεταξύ των φυσικών αριθμών, δείχνοντας να μην υπακούουν σε κανέναν άλλο νόμο από εκείνον της τύχης, και κανένας δεν μπορεί να προβλέψει που θα βλαστήσει ο επόμενος. Το δεύτερο είναι ακόμα πιο εκπληκτικό, γιατί δηλώνει ακριβώς το αντίθετο: ότι οι πρώτοι αριθμοί παρουσιάζουν εκπληκτική κανονικότητα, ότι υπάρχουν νόμοι που καθορίζουν την συμπεριφορά τους και ότι υπακούουν σε αυτούς τους νόμους σχεδόν με στρατιωτική ακρίβεια.» [Havil 2003, p. 171].

Οι πρώτοι αριθμοί λοιπόν είναι διάσπαρτοι άτακτα ανάμεσα στους ακεραίους και έτσι δεν είναι προς έκπληξη που μέσα από τους αιώνες οι μαθηματικοί έχουν προσπαθήσει σκληρά να βρουν μία ‘φόρμουλα πρώτων αριθμών’, δηλαδή μία μέθοδο που θα παράγει όλους τους πρώτους αριθμούς. Κάποιος μπορεί να επινοήσει μια τέτοια φόρμουλα με πολλούς διαφορετικούς τρόπους. Ως εκ τούτου, είναι πολύ σημαντικό να διευκρινίσουμε τι είναι πραγματικά επιθυμητό.

Προφανώς, μια πολύ απλή φόρμουλα πρώτων αριθμών είναι της μορφής

$$p = p_n \ (1)$$

όπου p_n δηλώνει τον n-οστό πρώτο αριθμό. Γιατί δεν μας ικανοποιεί όμως μια τέτοια φόρμουλα; Η δυσκολία του ζητήματος είναι ότι ο υπολογισμός του δεξιού μέλους της (1) είναι, εν γένει, πολύ δύσκολος, για παράδειγμα αν προσπαθήσουμε να βρούμε μόνοι μας τον p_{1975}! Αλλά θα θέλαμε να βρούμε μία παρόμοια φόρμουλα που να χαρακτηρίζεται από την πιο απλή μέθοδο υπολογισμού του δεξιού μέλους της (παρόλα αυτά, όπως θα διαπιστώσουμε και παρακάτω, η απλότητα υπολογισμού δεν είναι καθόλου προφανής έννοια).

Κατ' αρχάς μπορούμε να απαλλαγούμε από την ανάγκη της ρητής εξάρτησης του δεξιού μέλους από το n και να προσπαθήσουμε να βρούμε φόρμουλες που δίνουν πρώτους αριθμούς όχι απαραίτητα με αύξουσα σειρά μεγέθους. Μπορούμε να περιοριστούμε επιπλέον σε μία φόρμουλα που αποδίδει άπειρο αριθμό πρώτων αριθμών και όχι όλους τους πρώτους. Τέλος, μπορεί να δεχτούμε πως μια τέτοια φόρμουλα ίσως αποδώσει και μερικούς σύνθετους αριθμούς επίσης. Επισημαίνουμε ότι φαινομενικά απλές φόρμουλες μπορεί να αποδειχθούν ότι δεν είναι καλύτερες από την (1).

Οι πρώτοι αριθμοί μπορούν να παραχθούν με την διαδικασία του κοσκινίσματος όπως είδαμε με το κόσκινο του Ερατοσθένη. Το κόσκινο του Ερατοσθένη μπορεί να χρησιμοποιηθεί στην δημιουργία συνάρτησης υπολογισμού των πρώτων αριθμών:

$$\pi(x) = \pi\left(\sqrt{x}\right) + 1 + x - \left\lfloor \frac{1}{2}x \right\rfloor - \left\lfloor \frac{1}{3}x \right\rfloor - \left\lfloor \frac{1}{5}x \right\rfloor - \cdots + \left\lfloor \frac{x}{2 \times 3} \right\rfloor + \left\lfloor \frac{x}{2 \times 5} \right\rfloor + \left\lfloor \frac{x}{3 \ldots 5} \right\rfloor + \cdots - \left\lfloor \frac{x}{2 \times 3 \times 5} \right\rfloor + \cdots$$

η οποία είναι ουσιαστικά μια εφαρμογή της 'αρχής ένταξης-αποκλεισμού'. [Havil 2003, pp. 171-172].

Παρόλο που υπάρχουν πολλές και θαυμάσιες φόρμουλες υπολογισμού πρώτων αριθμών (π.χ. φόρμουλες που είτε παράγουν πρώτους αριθμούς για κάθε τιμή μιας μεταβλητής ή δίνουν τον $n^{\text{ο}}$ πρώτο αριθμό ως συνάρτηση του n), έχουν αναλυθεί σε τέτοιο βαθμό που έχουν ελάχιστη πρακτική αξία.

3.1 Η συνάρτηση $\pi(x)$

Η συνάρτηση που δίνει το πλήθος των πρώτων αριθμών των μικρότερων ή ίσων ενός αριθμού x συμβολίζεται $\pi(x)$. Έχουμε λοιπόν την συνάρτηση $\mathbb{R}^+ \ni x \to \pi(x) \in \mathbb{N}$, όπου $\mathbb{R}^+$ παριστάνει το σύνολο των θετικών πραγματικών αριθμών. Έτσι π.χ. $\pi(1) = 0, \pi(2) = 1, \pi(3) = 2, \pi(20) = 8, \pi(p_n) = n$, όπου p_n παριστάνει τον n-οστό πρώτο αριθμό. Έχουμε ήδη δει έξι διαφορετικές αποδείξεις ότι υπάρχουν άπειροι πρώτοι αριθμοί (Θεώρημα 1) δηλαδή ότι ισχύει $\lim_{x\to+\infty} \pi(x) = +\infty$. Θα παραθέσουμε εδώ άλλη μία απόδειξη του θεωρήματος αυτού από τον Euler από την οποία προκύπτουν όμως σημαντικά συμπεράσματα για τους πρώτους αριθμούς και την συνάρτηση $\pi(x)$.

<u>7η Απόδειξη (Θεωρήματος 1)</u><u>(Leonhard Euler)</u>**<u>:</u>**

Υποθέτουμε ότι το σύνολο P των πρώτων αριθμών είναι πεπερασμένο και θα οδηγηθούμε σε άτοπο. Έστω

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

Για κάθε πρώτο αριθμό p ισχύει:

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

Έχουμε συνεπώς:

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

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

Στο τελευταίο άθροισμα το n διατρέχει όλους τους φυσικούς αριθμούς, οι οποίοι εκφράζονται σαν γινόμενα των πρώτων αριθμών $p_1, p_2, \dots, p_s$, και καθένα ακριβώς μία φορά. Επειδή δε κάθε φυσικός αριθμός, διάφορος του 0, έχει μία 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 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 9: *Ισχύει:*

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

Απόδειξη: Έστω $p_1,p_2,\dots,p_s$ οι s πρώτοι πρώτοι αριθμοί. Θεωρούμε έναν θετικό πραγματικό αριθμό x και το σύνολο

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

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 $p_1,p_2,\dots,p_s$, οπότε θα μείνουν ο 1, οι πρώτοι αριθμοί $p_{s+1},p_{s+2},\dots$ και τα γινόμενα δυνάμεων αυτών. Το πλήθος των πολλαπλάσιων του p_i στο A είναι $\left[\frac{x}{p_i}\right]$, διότι από την σχέση

$$x=p_iy+r,0\leqq r<p_i$$

προκύπτει $\left[\frac{x}{p_i}\right] = y$. Επίσης το πλήθος των πολλαπλάσιων 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 $p_1, p_2, \dots, p_s$ θα μένουν στο σύνολο A:

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

αριθμοί. Συνεπώς προκύπτει

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

Το $\leqq$ εξηγείται από το γεγονός ότι στο A εκτός των πρώτων αριθμών $p_{s+1}, p_{s+2}, \dots$ 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

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

Άρα λαμβάνουμε

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

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

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 $s \geqq s_0$ να ισχύει

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

Εκλέγουμε ένα x_0, για το οποίο να ισχύει

$$s_0 + 2^{s_0} \leqq \varepsilon x_0,$$

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 10: *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

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

προκύπτει ότι για $x \geqq 1$

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

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 $\pi(x)$ εν συγκρίσει με την $\frac{x}{\log(x)}$, όπου $\log(x)$ ο φυσικός λογάριθμος του x.

x	$\pi(x)$	$\frac{x}{\log(x)}$	$\pi(x)/\frac{x}{\log(x)}$
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

3.2 Το Θεώρημα Πρώτων Αριθμών

Ο Adrien-Marie Legendre (1752-1833) αλλά και ο Carl Friedrich Gauss (1777-1855) ήταν οι πρώτοι που έκαναν εκτενείς υπολογισμούς της πυκνότητας των πρώτων αριθμών. Ο Gauss (ο οποίος ήταν μια 'μανιώδης αριθμομηχανή') είχε πει σε έναν φίλο του ότι όποτε είχε 15 λεπτά ελεύθερου χρόνου θα τα σπαταλούσε στο να υπολογίζει πρώτους αριθμούς ανά χιλιάδα. Μέχρι το τέλος της ζωής του εκτιμάται ότι είχε υπολογίσει όλους τους πρώτους αριθμούς ως το 3.000.000!

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 $\frac{x}{\log(x)}$. Ο Legendre έδωσε και μια εκτίμηση για το $\pi(x)$:

$$\pi(x) = \frac{x}{(\log(x) - 1{,}08366)},$$

ενώ η εκτίμηση του Gauss είναι από την άποψη του λογαριθμικού ολοκληρώματος:

$$\pi(x) = \int_2^x (1 - \log(t))\, dt.$$

Η πρόταση ότι η πυκνότητα των πρώτων αριθμών είναι $\frac{x}{\log(x)}$ είναι γνωστή ως **θεώρημα των πρώτων αριθμών**. Πριν όμως το διατυπώσουμε με βάση τα σημερινά δεδομένα αναφέρουμε τον παρακάτω ορισμό.

Ορισμός 8: Δύο συναρτήσεις $f(x), g(x)$ καλούνται ασυμπτωτικά ίσες και συμβολίζεται αυτό $f(x) \sim g(x)$ αν ισχύει

$$\lim_{x \to +\infty} \frac{f(x)}{g(x)} = 1.$$

Θεώρημα 11(Θεώρημα των πρώτων αριθμών): *Ισχύει ότι:*

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

Το θεώρημα πρώτων αριθμών είναι ισοδύναμο με το παρακάτω θεώρημα

Θεώρημα 12: *Ισχύει ότι:*

$$p_n \sim n\, log(n),$$

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 1851 έκανε ένα σημαντικό βήμα αποδεικνύοντας ότι αν η αναλογία $\pi(x) \Big/ \frac{x}{\log(x)}$ έτεινε σε όριο, τότε αυτό το όριο πρέπει να ήταν το 1. Ωστόσο δεν κατάφερε να αποδείξει ότι η αναλογία τείνει σε όριο. Ο τελευταίος 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 αναπόδειχτο. 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 και έτσι ο Riemann δεν κατάφερε να διευθετήσει τελείως το πρόβλημα πριν από τον θάνατό του.

Εικόνα 11:Pafnuty Chebyshev Εικόνα 12: Bernhard Riemann

Τελικά το θεώρημα των πρώτων αριθμών αποδείχτηκε από τους μαθηματικούς J.Hadamard (1865-1963) και De 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). 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 Vallee Poussin Εικόνα 15: P.Erdos Εικόνα 16: A.Selberg

3.3 Θεώρημα Bertrand

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

$$N+2, N+3, N+4, \dots, N+k, N+(k+1)$$

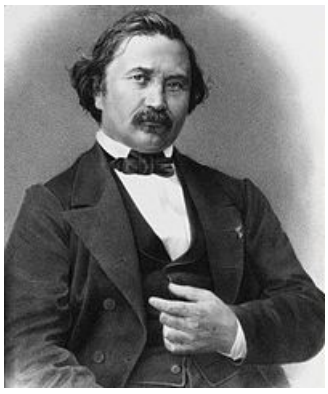
δεν είναι πρώτος, εφόσον για $2 \leq i \leq k+1$ γνωρίζουμε πως ο i έχει πρώτο παράγοντα ο οποίος είναι μικρότερος από $k+2$, και αυτός ο παράγοντας επίσης διαιρεί τον N, άρα επίσης διαιρεί τον $N+i$. Με αυτή την συνταγή, βρίσκουμε για παράδειγμα, ότι για $k=10$ $(N = 2 \times 3 \times 5 \times 7 \times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

$$2312, 2313, 2314, \dots, 2321$$

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 έρευνά 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 Ramanujan (1887-1920) χρησιμοποιώντας ιδιότητες της *Γ-συνάρτησης* $\Gamma(n) = (n-1)!$, n *θετικός ακέραιος* για να δώσει μία πιο απλή απόδειξη. Τέλος ο P.Erdos το 1932, όταν ήταν μόλις 19 χρονών, δημοσίευσε μία ακόμα πιο απλή απόδειξη χρησιμοποιώντας την συνάρτηση-θ-Chebyshev $\theta(x) = \sum_{p=2}^{x} \ln(p)$, όπου $p \leq x$, πρώτος αριθμός και διωνυμικούς συντελεστές.

Θεώρημα 13 (Θεώρημα Bertrand): *Για κάθε* $n \geq 1$, *υπάρχει κάποιος πρώτος αριθμός* p *με* $n < p \leq 2n$.



Εικόνα 17: Joseph Bertrand

3.4 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. Αντίθετα με το 'μικρό Θεώρημα του Fermat', το 'Θεώρημα Wilson' είναι αναγκαίο και ικανό για να δείξει ότι ένας αριθμός είναι πρώτος.

Θεώρημα 14 (Θεώρημα Wilson) (John Wilson,1770): *Ένας φυσικός αριθμός* $p > 1$ *είναι πρώτος αριθμός αν και μόνο αν*

$$(p-1)! \equiv -1 mod\ p.$$

1^{η} Απόδειξη: Το αποτέλεσμα είναι τετριμμένο για $p = 2$, οπότε υποθέτουμε ότι ο p είναι περιττός πρώτος. Δεδομένου ότι οι κλάσεις υπολοίπων $(mod\ p)$ αποτελούν ένα σώμα, κάθε μη μηδενική κλάση a έχει μοναδικό πολλαπλασιαστικό αντίστροφο a^{-1}. Από το Θεώρημα Lagrange συνεπάγεται ότι οι μόνες τιμές του a για τις οποίες $a \equiv a^{-1} mod\ p$ είναι οι $a \equiv \pm 1 mod\ p$ (επειδή ο p είναι πρώτος και η εξίσωση $a^2 \equiv 1$ μπορεί να έχει το πολύ δύο ρίζες $mod\ p$). Ως εκ τούτου με την εξαίρεση του ± 1 οι παράγοντες του $(p-1)!$ μπορούν να οργανωθούν σε άνισα ζευγάρια, που το γινόμενο κάθε ζευγαριού είναι $\equiv 1 mod\ p$. □

Για παράδειγμα για $p = 11$:

$$10! = 1(10)(2 \times 6)(3 \times 4)(5 \times 9)(7 \times 8) \equiv -1 mod\ 11$$

2^{η} Απόδειξη: Το αποτέλεσμα είναι τετριμμένο για $p = 2$, οπότε υποθέτουμε ότι ο p είναι περιττός πρώτος. Θεωρούμε το πολυώνυμο

$$g(x) = (x-1)(x-2) \dots \big(x-(p-1)\big).$$

όπου ο βαθμός του είναι $p-1$, ο πρώτος του όρος είναι ο $x^{(p-1)}$ και ο σταθερός του όρος ο $(p-1)!$. Οι $p-1$ ρίζες του είναι οι $1,2, \dots, p-1$.

Τώρα θεωρούμε το πολυώνυμο

$$h(x) = x^{(p-1)} - 1$$

όπου το h έχει επίσης βαθμό $p-1$ και πρώτο όρο $x^{(p-1)}$. Επίσης το 'Μικρό Θεώρημα του Fermat' , μας λέει ότι το $h(x)$ έχει επίσης τις ίδιες $p-1$ ρίζες $1,2,\dots,p-1$.

Τέλος θεωρούμε

$$f(x) = g(x) - h(x).$$

Όπου το f έχει βαθμό το πολύ $p-2$, αφού οι πρώτοι όροι διαγράφονται, και $mod\ p$ έχει επίσης τις ίδιες $p-1$ ρίζες $1,2,\dots,p-1$. Αλλά το Θεώρημα Lagrange λέει πως δεν μπορεί να έχει περισσότερες από $p-2$ ρίζες. Έτσι το f πρέπει να είναι ταυτόσημο με $0 mod\ p$, το ίδιο και ο σταθερός του όρος: $(p-1)! + 1 \equiv 0 mod\ p$. □

<u>Απόδειξη του αντιστρόφου:</u> Έστω ότι για τον φυσικό αριθμό $p > 1$ ισχύει

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

και ότι ο p δεν είναι πρώτος αριθμός. Υπάρχει ένας πρώτος διαιρέτης q του p. Επειδή $q < p$, θα ισχύει $q \mid (p-1)!$. Άρα θα πρέπει να ισχύει $q \mid 1$, το οποίο είναι άτοπο. □

Το Θεώρημα Wilson είναι άχρηστο ως έλεγχος πρώτων αριθμών, δεδομένου ότι ο υπολογισμός του $(p-1)!\, mod\ p$ για μεγάλο p είναι δύσκολος και είναι γνωστοί πολύ πιο εύκολοι έλεγχοι πρώτων αριθμών. Ακόμα και αυτός των δοκιμαστικών διαιρέσεων θεωρείται πιο αποδοτικός.

Χρησιμοποιώντας το Θεώρημα Wilson για έναν περιττό πρώτο αριθμό $p = 2m+1$, μπορούμε να αναδιατάξουμε το αριστερό μέλος της ισότητας

$$1 \times 2 \times \dots \times (p-1) \equiv -1 mod\ p$$

και να πάρουμε την ισότητα

$$1(p-1)2(p-2)\dots m(p-m) \equiv 1(-1)2(-2)\dots m(-m) \equiv -1 mod\ p.$$

Αυτή γίνεται

$$\prod_{j=1}^{m} j^2 \equiv (-1)^{m+1} mod\ p.$$

Μπορούμε να χρησιμοποιήσουμε την τελευταία ισότητα για να αποδείξουμε ένα μέρος ενός διάσημου θεωρήματος:

<u>Θεώρημα 15:</u> *Για κάθε πρώτο αριθμό p τέτοιο ώστε $p \equiv 1\ mod\ 4$ ο αριθμός -1 είναι ένα τετραγωνικό υπόλοιπο*

Πράγματι υποθέτοντας ότι $p = 4k + 1$ για κάποιο ακέραιο k, παίρνουμε ότι $m = 2k$ και καταλήγουμε στο συμπέρασμα ότι

$$(\prod_{j=1}^{2k} j)^2 = \prod_{j=1}^{2k} j^2 \equiv (-1)^{2k+1} = -1 mod\ p.$$

Το Θεώρημα Wilson έχει χρησιμοποιηθεί και για την κατασκευή τύπων παραγωγής πρώτων αριθμών, αλλά ήταν πολύ αργοί για να έχουν πρακτική αξία.

Το σημαντικότερο στο Θεώρημα Wilson είναι ότι ισχύει και το αντίστροφό του.

Ένα πόρισμα του Θεωρήματος Wilson λέει ότι: ένας πρώτος αριθμός p είναι της μορφής $4k + 1$ αν και μόνο αν

$$[(2k)!]^2 \equiv -1\ mod\ p.$$

Μερικοί από τους πρώτους πρώτους αριθμούς της μορφής $4k + 1$ είναι $p = 5,13,17,29,37,41$ ... που αντιστοιχούν στο

$$k = 1,3,4,7,9,10,13,15,18,22,24,25,27,28,34,37, \ldots$$

Η γενίκευση του Gauss του 'Θεωρήματος Wilson' θεωρεί $P(n)$ το γινόμενο των ακεραίων που είναι μικρότεροι ή ίσοι και πρώτοι με έναν ακέραιο n. Για $n = 1,2, \ldots$ οι πρώτες μεταβλητές είναι 1,1,2,3,24,5,720,105,2240,189,… Έπειτα ορίζοντας

$$P(n) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n} k$$

δίνει την αντιστοιχία

$$P(n) = \begin{cases} 0\ mod 1\ , & για\ n = 1 \\ -1\ mod n, & για\ n = 4, p^a\ , 2p^a \\ & και\ p\ περιττό\ πρώτο \\ 1\ mod n, & διαφορετικά \end{cases}.$$

Όταν $n = 2$ αυτή μετατρέπεται σε $P(2) = 1 mod 2$ που είναι ισοδύναμη με την $P = -1\ mod 2$. Μερικές πρώτες τιμές της $P(n)\ mod n$ είναι:

0,-1,-1,-1,-1,-1,-1,1,-1,-1,-1,… .

3.5 Πολυώνυμα και πρώτοι αριθμοί

Ο Legendre έδειξε ότι δεν υπάρχει ρητή αλγεβρική συνάρτηση που να δίνει πάντα πρώτους αριθμούς. Το 1752, ο Christian Goldbach (1690-1764) απέδειξε το παρακάτω:

Θεώρημα 16 (Christian Goldbach,1752): *Δεν υπάρχει μη σταθερό πολυώνυμο με ακέραιους συντελεστές που να μπορεί να δώσει πρώτους αριθμούς για όλες τις ακέραιες τιμές της μεταβλητής.*

Απόδειξη: Έστω μη σταθερό πολυώνυμο $P(x)$ με ακέραιους συντελεστές που δίνει πρώτους αριθμούς για κάθε ακέραιη τιμή της μεταβλητής x. Πρέπει να ισχύει

$$P(1) \equiv 0 \, mod \, p$$

όπου p πρώτος αριθμός. Έτσι για κάθε ακέραιο αριθμό k ισχύει:

$$P(1 + kp) \equiv 0 \, mod \, p$$

που αυτό θα σήμαινε ότι ο $P(1 + kp)$ δεν είναι πρώτος γιατί διαιρείται από τον p εκτός εάν για άπειρες τιμές του k, $P(1) = P(1 + kp)$ πράγμα που θα σήμαινε πως το πολυώνυμό μας είναι σταθερό. Άτοπο. □

Το πιο γνωστό πολυώνυμο που παράγει (ενδεχομένως κατά απόλυτη τιμή) μόνο πρώτους αριθμούς είναι το $n^2 + n + 41$ και το βρήκε ο Euler. Αυτό το πολυώνυμο δίνει διακριτούς πρώτους αριθμούς για 40 συνεχόμενους ακεραίους, από $n = 0$ έως $n =$39 (και το πολυώνυμο $n^2 - n + 41$ που βρήκε ο Legendre το 1798, δίνει τους ίδιους 40 πρώτους αριθμούς από $n = 1$ έως $n =$40, και οι αριθμοί αυτοί ονομάστηκαν ‘Euler αριθμοί’ από τους Flannery S. και Flannery D.). Μετατρέποντας το πολυώνυμο αυτό σε

$$n^2 - 79n + 1601 = (n - 40)^2 + (n - 40) + 41$$

λαμβάνονται πρώτοι αριθμοί για 80 συνεχόμενους ακεραίους, που αντιστοιχούν στους 40 πρώτους αριθμούς που λαμβάνουμε από το πολυώνυμο του Euler παίρνοντας δύο φορές τον καθένα. [Hardy and Wright 1979, p. 18] Αν η $p(x)$ παράγει πρώτους αριθμούς για $0 \leq x \leq n$, τότε και η $p(n - x)$ κάνει το ίδιο.

Ο παρακάτω πίνακας δίνει κάποια χαμηλού βαθμού πολυώνυμα που παράγουν μόνο πρώτους αριθμούς για τις πρώτες λίγες μη αρνητικές τιμές της μεταβλητής. [Mollin and Williams 1990]. Πολυώνυμα που έχουν παραχθεί από άλλα με αντικαταστάσεις, όπως πχ αυτά των Legendre και Hardy και Wright δεν συμπεριλαμβάνονται.

πολυώνυμο	**πρώτοι αριθμοί από 0 έως n**	**διαφορετικοί μεταξύ τους πρώτοι αριθμοί**	**αναφορές**
$\frac{1}{4}(n^5 - 133n^4 + 6729n^3 - 158379n^2 + 1720294n - 6823316)$	56	57	Dress and Landreau (2002), Gupta (2006)
$\frac{1}{36}(n^6 - 126n^5 - 153066n^3 + 1987786n^2 - 13055316n + 34747236)$	54	55	Wroblewski and Meyrignac (2006)
$n^4 - 97n^3 + 3294n^2 - 45458n + 213589$	49	49	Beyleveld (2006)
$n^5 - 99n^4 + 3588n^3 - 56822n^2 + 348272n - 286397$	46	47	Wroblewski and Meyrignac (2006)
$-66n^3 + 3845n^2 - 60897n + 251831$	45	46	Kazmenko and Trofimov (2006)
$36n^2 - 810n + 2753$	44	45	Fung and Ruby(A050268)
$3n^3 - 183n^2 + 3318n - 18757$	46	43	S. M. Ruiz (pers. comm., Nov. 20, 2005)
$47n^2 - 1701n + 10181$	42	43	Fung and Ruby(A050267)
$103n^2 - 4707n + 50383$	42	43	Speiser (pers. comm., Jun. 14, 2005)

$n^2 - n + 41$	40	40	Euler(A005846)
$42n^3 + 270n^2 - 26436n + 250703$	39	40	Wroblewski and Meyrignac
$43n^2 - 537n + 2971$	34	35	J. Brox (pers. comm., Mar. 27, 2006)
$8n^2 - 488n + 7243$	61	31	F. Gobbo (pers. comm., Dec. 27, 2005)
$6n^2 - 342n + 4903$	57	29	J. Brox (pers. comm., Mar. 27, 2006)
$2n^2 + 29$	28	29	Legendre (1798) (A007641)
$7n^2 - 371n + 4871$	23	24	F. Gobbo (pers. comm., Dec. 26, 2005)
$n^4 + 29n^2 + 101$	19	20	E. Pegg, Jr. (pers. comm., Jun. 14, 2005)
$3n^2 + 39n + 37$	17	18	A. Bruno (pers. comm., Jun. 12, 2009)
$n^2 + n + 17$	15	16	Legendre(A007635)
$4n^2 + 4n + 59$	13	14	Honaker(A048988)
$2n^2 + 11$	10	11	(A050265)
$n^3 + n^2 + 17$	10	11	(A050266)

Πίνακας 5

Ένα ιδιαίτερα φτωχό πολυώνυμο είναι το $n^6 + 1091$ το οποίο δεν δίνει πρώτους αριθμούς για $n = 1, \dots, 3095$ αλλά δίνει για $n = 3906,4620,5166,5376,5460, \dots$ [Sloane's A066386; Shanks 1971, 1993; Wells 1997, p. 151]. Άλλα πολυώνυμα

τέτοιου τύπου συμπεριλαμβάνουν τα $n^6 + 29450922310244534$, ο οποίο ανακαλύφτηκε από τον Phil Carmody το 2006 (Rivera) και δίνει πρώτους για $n = 63693,64785,70455,90993,100107, \ldots$ και του $x^{12} + 488669$ το οποίο δίνει πρώτους για $x = 616980,764400,933660, \ldots$.

Ο Le Lionnais (1901-1984) το 1983 βάφτισε τους αριθμούς p τέτοιους ώστε το πολυώνυμο Euler:

$$n^2 + n + p$$

να δίνει πρώτους αριθμούς για $n = 0,1, \ldots, p-2$ ως 'τυχερούς αριθμούς Euler'. Ο Rabinowitz το 1913 έδειξε ότι για έναν πρώτο $p > 0$ το πολυώνυμο του Euler παράγει πρώτους για $n \in [0, p-2]$ (αποκλείοντας την ασήμαντη περίπτωση του $p = 3$) αν και μόνο αν το πεδίο $\mathbb{Q}\left(\sqrt{1-4p}\right)$ έχει κλάση $h = 1$ [Rabinowitz 1913, Le Lionnais 1983, Conway and Guy 1996]. Όπως διαπιστώθηκε από τον Stark το 1967 υπάρχουν μόνο 9 αριθμοί $-d$ τέτοια ώστε $h(-d) = 1$ και από αυτά μόνο οι 7,11,19,43,67 και 163 είναι της απαιτούμενης μορφής. Ως εκ τούτου οι μόνοι 'τυχεροί αριθμοί Euler' είναι οι 2,3,5,11,17 και 41 [Le Lionnais 1983, Sloane's A014556] και δεν υπάρχει καλύτερο πολυώνυμο που να παράγει πρώτους αριθμούς από αυτό του Euler. Η σύνδεση μεταξύ των αριθμών 163 και 43 και τα κύρια πολυώνυμα που έχουν αναφερθεί παραπάνω μπορεί να παρατηρηθεί γράφοντας:

$$x^2 + x + 41 = (x + \frac{1}{2})^2 + \frac{163}{4},$$

$$x^2 + x + 11 = (x + \frac{1}{2})^2 + \frac{43}{4},$$

κλπ…

Ο Euler επίσης θεώρησε τετραγωνικά πολυώνυμα της μορφής

$$2x^2 + p$$

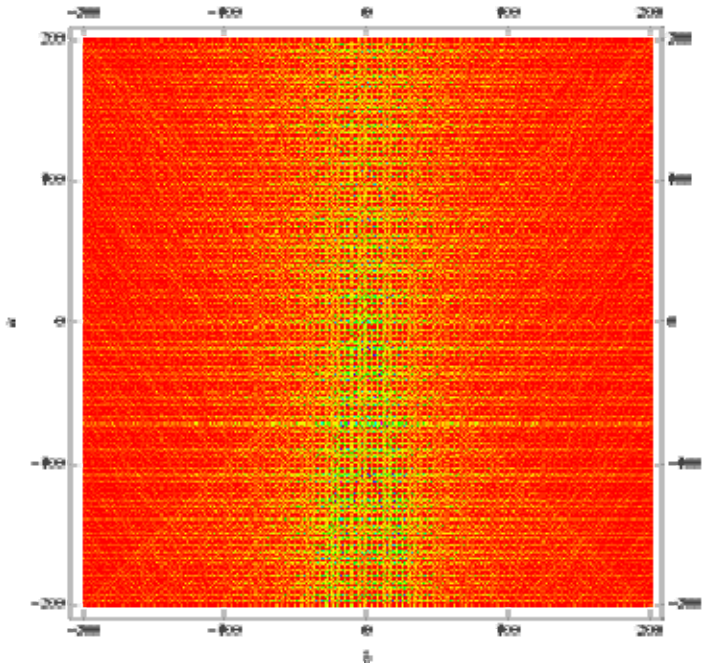
και έδειξε ότι δίνουν πρώτους για $x \in [0, p-1]$ για πρώτο αριθμό $p > 0$ αν και μόνο αν $\mathbb{Q}\left(\sqrt{-2p}\right)$ είναι τάξης 2, που επιτρέπει μόνο τους $p = 3,5,11 \; και \; 29$.

Οι Baker και Stark το 1971 έδειξαν ότι δεν υπάρχουν τέτοια πεδία για $p > 29$. Παρόμοια αποτελέσματα έχουν βρεθεί και για πολυώνυμα της μορφής

$$px^2 + px + n$$

[Hendy 1974].

Το παρακάτω διάγραμμα απεικονίζει τον αριθμό των πρώτων αριθμών που παράγονται από τετραγωνικά πολυώνυμα της μορφής $x^2 + ax + b$ από το -200 ως το 200.



Διάγραμμα 2

3.6 Leonhard Euler

Η δουλειά του Leonhard Euler (1707-1783) είχε μεγάλη επίδραση γενικά στην θεωρία αριθμών και συγκεκριμένα στους πρώτους αριθμούς. Επέκτεινε το 'μικρό Θεώρημα του Fermat' και εισήγαγε την 'φ-συνάρτηση Euler'. Όπως έχουμε αναφέρει παραπάνω παραγοντοποίησε τον $5^{ο}$ αριθμό του Fermat $2^{32} + 1$, βρήκε 60 ζευγάρια φιλικών αριθμών (βλ. Ορισμό 3) και διατύπωσε (αλλά δεν κατάφερε να αποδείξει) αυτό που ονομάζεται 'Law of Quadratic Reciprocity'. Ήταν ο πρώτος που κατάλαβε ότι η θεωρία αριθμών μπορεί να μελετηθεί χρησιμοποιώντας τα εργαλεία της ανάλυσης και εφαρμόζοντάς τα ίδρυσε την Αναλυτική Θεωρία Αριθμών. Απέδειξε ότι δεν είναι μόνο η αρμονική σειρά $\sum \frac{1}{n}$ αποκλίνουσα, αλλά και η σειρά

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{7} + \frac{1}{11} + \cdots$$

που σχηματίζονται από το άθροισμα των αντίστροφων των πρώτων αριθμών είναι αποκλίνουσα.

Εικόνα 18: Leonhard Euler

Ως το 1772 ο Euler είχε χρησιμοποιήσει έξυπνες αιτιολογίες και δοκιμαστικές διαιρέσεις για να αποδείξει ότι ο $2^{31} - 1 = 2147483647$ είναι πρώτος. Η πραγματική ημερομηνία πρέπει να ήταν μεταξύ της 28ης Οκτωβρίου 1752, όταν ο Euler έστειλε ένα γράμμα στον Goldbach λέγοντας του πως ήταν αβέβαιος γι' αυτό το νούμερο (παρόλο που το είχε νωρίτερα συμπεριλάβει στην λίστα του ως πρώτο αριθμό) και 1772 όταν δημοσιεύτηκε ένα γράμμα από τον Euler στον Bernoulli που έλεγε ότι απέδειξε πως ο $2^{31} - 1$ είναι πρώτος δείχνοντας πως όλοι οι πρώτοι διαιρέτες του πρέπει να είναι είτε της μορφής $248n + 1$ ή της μορφής $248n + 63$ και στην συνέχεια διαιρώντας με όλους αυτούς τους πρώτους που είναι μικρότεροι του 46339. [Dickson19 pp18-19]

3.7 Johann Lejeune Dirichlet και αριθμητικοί πρόοδοι

Όπως είδαμε, μερικά πολυώνυμα αναπαριστούν άπειρους πρώτους αριθμούς. Για παράδειγμα, καθώς το x τρέχει μέσα από τους ακεραίους 0, 1, 2, 3, … το γραμμικό πολυώνυμο $2x + 1$ δίνει όλους τους περιττούς αριθμούς άρα δίνει άπειρους πρώτους. Επίσης καθένα από τα πολυώνυμα $4x + 1$ και $4x + 3$ παράγει άπειρους πρώτους αριθμούς. Σε ένα διάσημο βιβλίο με κάποια απομνημονεύματα που εκδόθηκε το 1837, ο Johann Peter Gustav Lejeune Dirichlet (1805-1859) απέδειξε ότι αν a και b είναι θετικοί ακέραιοι που είναι πρώτοι μεταξύ τους, το πολυώνυμο $ax + b$ δίνει άπειρους πρώτους αριθμούς καθώς το x διατρέχει όλους τους θετικούς ακεραίους. Αυτό το συμπέρασμα είναι πλέον γνωστό ως το Θεώρημα του Dirichlet στην ύπαρξη των πρώτων αριθμών σε μια δεδομένη αριθμητική πρόοδο.

Για να αποδείξει αυτό το θεώρημα ο Dirichlet πήγε έξω από την σφαίρα των ακεραίων αριθμών και εισήγαγε εργαλεία της ανάλυσης όπως το όριο και η συνέχεια. Κάνοντας το αυτό έβαλε τις βάσεις, όπως και ο Euler, για ένα καινούριο κλάδο των μαθηματικών που ονομάζεται Αναλυτική Θεωρία Αριθμών, στην οποία ιδέες και

μέθοδοι της πραγματικής και της μιγαδικής ανάλυσης χρησιμοποιούνται για να αντιμετωπιστούν προβλήματα με τους ακεραίους.

Δεν ήταν γνωστό αν υπάρχει 2ου βαθμού πολυώνυμο $ax^2 + bx + c$ με $a \neq 0$ το οποίο παράγει άπειρους πρώτους αριθμούς. Ωστόσο ο Dirichlet χρησιμοποίησε τις δυνατές αναλυτικές του μεθόδους για να αποδείξει ότι αν οι $a, 2b$ και c είναι πρώτοι μεταξύ τους το πολυώνυμο 2ου βαθμού, δύο μεταβλητών $ax^2 + 2bxy + cy^2$ καθώς τα x, y διατρέχουν τους θετικούς ακεραίους.

Εικόνα 19: Dirichlet

Σημειώνεται τέλος ότι το Θεώρημα του Dirichlet δεν απαιτεί οι πρώτοι αριθμοί σε μια αριθμητική ακολουθία να είναι συνεχόμενοι. Είναι επίσης γνωστό ότι υπάρχουν αυθαίρετα μεγάλες πεπερασμένες αριθμητικές ακολουθίες που αποτελούνται μόνο από πρώτους αριθμούς, κάτι το οποίο αποδείχτηκε το 2004 από τους Ben Green και Terence Tao και είναι γνωστό ως Θεώρημα Green- Tao. Με άλλα λόγια το θεώρημα τους λέει πως υπάρχουν αριθμητικές πρόοδοι πρώτων αριθμών, με k όρους, όπου k μπορεί να είναι οποιοσδήποτε πραγματικός αριθμός. Το θεώρημα αυτό όμως ήταν θεώρημα ύπαρξης και δεν έδειχνε πως βρίσκουμε τέτοιες αριθμητικές προόδους.

Στις 17 Μαΐου 2008, οι Wróblewski και Raanan Chermoni βρήκαν την πρώτη γνωστή αριθμητική πρόοδο 25 πρώτων αριθμών.

$$6.171.054.912.382.631 + 366.384 \times 223.092.870 \times n$$

όπου $n = 0,1, \dots ,24$.

Στις 12 Απριλίου 2010, ο Benoãt Perichon με λογισμικό των Wróblewski και Geoff Reynolds, σε ένα ερευνητικό πρόγραμμα κατανομής των πρώτων αριθμών βρήκε την πρώτη γνωστή αριθμητική πρόοδο 26 πρώτων αριθμών.

$$43.142.746.595.714.191 + 23.681.770 \times 223.092.870 \times n$$

όπου $n = 0,1, \dots ,25$.

3.8 Τύποι παραγωγής πρώτων που χρησιμοποιούν την συνάρτηση 'ακέραιο μέρος' (floor function)

Το 1947 ο William H. Mills δημοσίευσε το παρακάτω αποτέλεσμα:

Θεώρημα 17: *Υπάρχει πραγματικός αριθμός λ τέτοιος ώστε για όλα τα $n = 1,2, \dots$ ο αριθμός*

$$\lfloor \lambda^{3^n} \rfloor$$

είναι πρώτος. (όπου $\lfloor \alpha \rfloor$ το ακέραιο μέρος του α).

Ο λ ονομάζεται σταθερά Mills. Η χρησιμότητά της είναι άγνωστη, αλλά αν ισχύει η υπόθεση Riemann, είναι περίπου 1,3063778838630806904686144926... Οι πρώτοι αριθμοί που παράγονται από αυτή την σταθερά ονομάζονται 'πρώτοι αριθμοί Mills' και αν η υπόθεση Riemann είναι αληθής η ακολουθία ξεκινάει: 2, 11, 1361, 2521008887...

Αν ο $a(i)$ δηλώνει τον i-οστό πρώτο αριθμό της ακολουθίας, τότε ο $a(i)$ μπορεί να υπολογιστεί ως ο μικρότερος πρώτος αριθμός μεγαλύτερος από τον $a(i-1)^3$. Για να εξασφαλίσουμε ότι η στρογγυλοποίηση του λ^{3^n}, για $n = 1,2, \dots$ παράγει την ακολουθία των πρώτων, πρέπει να ισχύει η υπόθεση $a(i) < (a(i-1)+1)^3$. Τα αποτελέσματα των Hoheisel-Ingham (μαθηματικοί που μελέτησαν τα κενά των πρώτων αριθμών γύρω στο 1930) εγγυώνται ότι υπάρχει ένας πρώτος αριθμός μεταξύ δύο οποιωνδήποτε αρκετά μεγάλων αριθμών στον κύβο, το οποίο είναι επαρκές για να αποδείξουμε αυτή την ισότητα αν ξεκινήσουμε από έναν αρκετά μεγάλο πρώτο αριθμό $a(1)$. Η Υπόθεση Riemann συνεπάγεται ότι υπάρχει ένας πρώτος αριθμός ανάμεσα σε οποιουσδήποτε δύο διαδοχικούς αριθμούς στον κύβο, επιτρέποντάς μας να αφαιρέσουμε αυτή την αρκετά μεγάλη προϋπόθεση και η ακολουθία των 'πρώτων αριθμών Mills' να ξεκινάει με $a(1) = 2$.

Μέχρι τώρα ο μεγαλύτερος 'πρώτος αριθμός Mills' (υπό την Υπόθεση Riemann) είναι ο

$$(((((((((2^3+3)^3+30)^3+6)^3+80)^3+12)^3+450)^3+894)^3+3636)^3 + 70756)^3+97220$$

που έχει 20562 ψηφία.

Με τον υπολογισμό της ακολουθίας των ‘πρώτων αριθμών Mills’ μπορεί κανείς να προσεγγίσει την σταθερά Mills ως:

$$\lambda \approx \alpha(n)^{\frac{1}{3^n}}.$$

Οι Caldwell & Cheng [Caldwell & Cheng 2005] χρησιμοποίησαν αυτή την μέθοδο για να υπολογίσουν σχεδόν 7000 ψηφία της σταθεράς Mills με την παραδοχή ότι ισχύει η υπόθεση Riemann.

Ο τύπος αυτός παράγει πρώτους αριθμούς αλλά δεν τους παράγει όλους κι έτσι δεν έχει καμία πρακτική αξία, γιατί γνωρίζουμε πολύ λίγα πράγματα γι’ αυτή την σταθερά (δεν γνωρίζουμε ούτε αν είναι ρητός αριθμός [Finch 2003]) και δεν υπάρχει γνωστός τρόπος υπολογισμού της χωρίς να έχουμε βρει πρώτα πρώτους αριθμούς.

Ακολούθησε μια σειρά από τύπους τέτοιου είδους. Όμως όλα αυτά τα αποτελέσματα κατείχαν μια παρόμοια ιδιότητα: ο ορισμός τους ήταν καλός, αλλά η απόδειξή τους απογοητευτική. Άλλα δύο τέτοια γνωστά θεωρήματα είναι τα παρακάτω:

Θεώρημα 18 (E. M. Wright): *Υπάρχει πραγματικός αριθμός μ τέτοιος ώστε κάθε αριθμός της μορφής*

$$\left\lfloor 2^{2^{\cdot^{\cdot^{2^{\mu}}}}} \right\rfloor$$

είναι πρώτος αριθμός.

Θεώρημα 19 (E. M. Wright 1951, Ribenboim 1996): *Υπάρχει πραγματικός αριθμός $\omega \approx 1{,}9287800$ τέτοιος ώστε για όλα τα $n = 1,2,\ldots$ ο αριθμός*

$$\lfloor 2\omega n \rfloor$$

είναι πρώτος αριθμός.

Τόσο ο αριθμός $\lfloor \lambda^{3^n} \rfloor$ όσο και ο αριθμός $\lfloor 2\omega n \rfloor$ για $n = 4$ μεγαλώνουν τόσο ραγδαία που χρειάζεται να γνωρίζουμε με εξαιρετική ακρίβεια την τιμή των σταθερών λ και ω ώστε να επιτευχθεί το σωστό αποτέλεσμα και τα αποτελέσματα για $n \geq 5$ τα αποτελέσματα είναι ουσιαστικά μη υπολογίσιμα.

Το βασικό μειονέκτημα αυτών των τύπων είναι ότι αποτυγχάνουν να αποδώσουν μία μέθοδο για να παίρνουμε καινούριους πρώτους αριθμούς, αφού για να υπολογίσουμε έναν πρώτο αριθμό πρέπει να γνωρίζουμε τις σταθερές λ, μ και ω με επαρκή ακρίβεια. Εξάλλου αυτοί οι τύποι δεν ρίχνουν καθόλου φως στις ιδιότητες των πρώτων αριθμών.

Άλλος ένας σημαντικός τύπος που επίσης χρησιμοποιεί την συνάρτηση 'ακέραιο μέρος' δημοσιεύτηκε το 1964 από τον Willans και έχει ως εξής:

Έχουμε p_n τον n-οστό πρώτο αριθμό και $\lfloor x \rfloor$ την συνάρτηση ακέραιο μέρος. Από το Θεώρημα Wilson έχουμε: $\frac{(x-1)!+1}{x}$ ακέραιο για $x = 1$ ή $πρώτος\ αριθμός$, αλλά κλάσμα για $x = σύνθετος$. Θεωρούμε την συνάρτηση

$$F(x) = \left\lfloor \cos^2 \pi \frac{(x-1)! + 1}{x} \right\rfloor = \begin{cases} 1, για\ x = 1, ή\ πρώτος \\ 0, \quad για\ x = σύνθετος \end{cases}$$

Έπεται ότι αν $\pi(m)$ δηλώνει τον αριθμό των πρώτων $\leq m$, τότε

$$\pi(m) = -1 + \sum_{x=1}^{m} F(x).$$

Θεωρούμε $A_n(\alpha) = \left\lfloor \sqrt[n]{\frac{n}{1+\alpha}} \right\rfloor$ για $n = 1,2, \ldots$ και $\alpha = 0,1,2, \ldots$. Αυτή η συνάρτηση έχει τις ιδιότητες $A_n(\alpha) = 1, για\ \alpha < n$ και $A_n(\alpha) = 0, για\ \alpha \geq n$ (γιατί αν $\alpha < n$ τότε $1 \leq \frac{n}{1+\alpha} \leq n$ και έτσι $1 \leq \sqrt[n]{\frac{n}{1+\alpha}} \leq \sqrt[n]{n} < 2$ και αν $\alpha \geq n$ τότε $0 < \frac{n}{1+\alpha} < 1$ και έτσι $0 < \sqrt[n]{\frac{n}{1+\alpha}} < 1$).

Ως εκ τούτου παίρνουμε τον τύπο:

$$p_n = 1 + \sum_{m=1}^{N} A_n(\pi(m))$$

όπου N κάθε αρκούντως μεγάλος ακέραιος ($N = 2^n$ αρκεί αφού $p_n \leq 2^n$ για όλα τα n).

Ο τύπος πλήρως γραμμένος είναι:

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \sqrt[n]{n} \left(\sum_{x=1}^{m} \left\lfloor \cos^2 \pi \frac{(x-1)! + 1}{x} \right\rfloor \right)^{-\frac{1}{n}} \right\rfloor$$

Για παράδειγμα

$$\begin{aligned} p_5 &= 1 + A_5(\pi(1)) + A_5(\pi(2)) + \cdots + A_5(\pi(10)) + A_5(\pi(11)) + \cdots + A_5(\pi(32)) \\ &= 1 + A_5(0) + A_5(1) + \cdots + A_5(4) + A_5(5) + \cdots + A_5(11) \\ &= 1 + 1 + 1 + \cdots + 1 + 0 + \cdots + 0 = 11 \end{aligned}$$

[Willans 1964; Havil 2003, pp. 168-169].

Με το πέρασμα των χρόνων πολλοί σπουδαίοι μαθηματικοί βρήκαν αρκετούς τύπους που παράγουν πρώτους αριθμούς. Ενδεικτικά αναφέρουμε τους: Ernvall (1975), Regimbal (1975), Μάκη Παπαδημητρίου(1975), Ruiz (2004), Rowland (2008) που δημοσίευσαν πιο πρόσφατα μερικούς από τους πιο σημαντικούς τύπους. Ωστόσο, θα πρέπει και πάλι να τονιστεί ότι αυτοί οι τύποι είναι εξαιρετικά αναποτελεσματικοί και σε πολλές (αν όχι όλες) τις περιπτώσεις, εκτελώντας απλώς ένα κοσκίνισμα θα παίρναμε πρώτους αριθμούς πολύ πιο γρήγορα και αποτελεσματικά.

4

Μερικά ακόμη 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. Υπάρχει ζυγός αριθμός >2 που να μην εκφράζεται ως άθροισμα δύο περιττών πρώτων αριθμών; (εικασία του Goldbach)
2. Υπάρχουν άπειροι δίδυμοι πρώτοι αριθμοί; (δύο πρώτοι αριθμοί p, q καλούνται δίδυμοι πρώτοι αν $q = p + 2$)
3. Υπάρχει ζυγός αριθμός >2 που να μην εκφράζεται ως διαφορά δύο πρώτων αριθμών;
4. Υπάρχουν άπειροι πρώτοι 'αριθμοί Mersenne';
5. Υπάρχουν άπειροι 'πρώτοι αριθμοί του Fermat';
6. 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 $x^2 + y^2 + z^2 + 1$)
7. Υπάρχουν άπειροι πρώτοι της μορφής $x^2 + k$ (k γνωστό);
8. 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 $2n$ καλείται εικασία του Bertrand και έχει αποδειχτεί από τον Chebyshev)

9. Υπάρχει πάντα τουλάχιστον ένας πρώτος αριθμός μεταξύ των n^2 και $n^2 + n$ για κάθε ακέραιο $n > 1$;
10. 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)
11. Υπάρχουν άπειροι πρώτοι της μορφής $n\# + 1$ και $n\# - 1$; (όπου $n\#$ το γινόμενο όλων των πρώτων αριθμών $\leq n$)
12. Υπάρχουν άπειροι πρώτοι αριθμοί της μορφής $n! + 1$ και $n! - 1$;
13. 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;
14. Υπάρχει αριθμητική πρόοδος με διαδοχικούς πρώτους αριθμούς για κάθε πεπερασμένο μήκος αυτής; (για παράδειγμα η: 251,257,263,269 έχει μήκος 4 και το μεγαλύτερο γνωστό παράδειγμα έχει μήκος 10)
15. Υπάρχουν άπειρα σύνολα τριών διαδοχικών πρώτων αριθμών σε αριθμητική πρόοδο; (ισχύει για μη διαδοχικούς πρώτους αριθμούς)
16. Το πολυώνυμο $n^2 - n + 41$ δίνει πρώτους για $0 \leq n \leq 40$. Υπάρχουν άπειροι τέτοιοι πρώτοι αριθμοί; Το ίδιο ερώτημα ισχύει και για $n^2 - 79n + 1601$ που δίνει πρώτους για $0 \leq n \leq 79$.

4.1 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.»

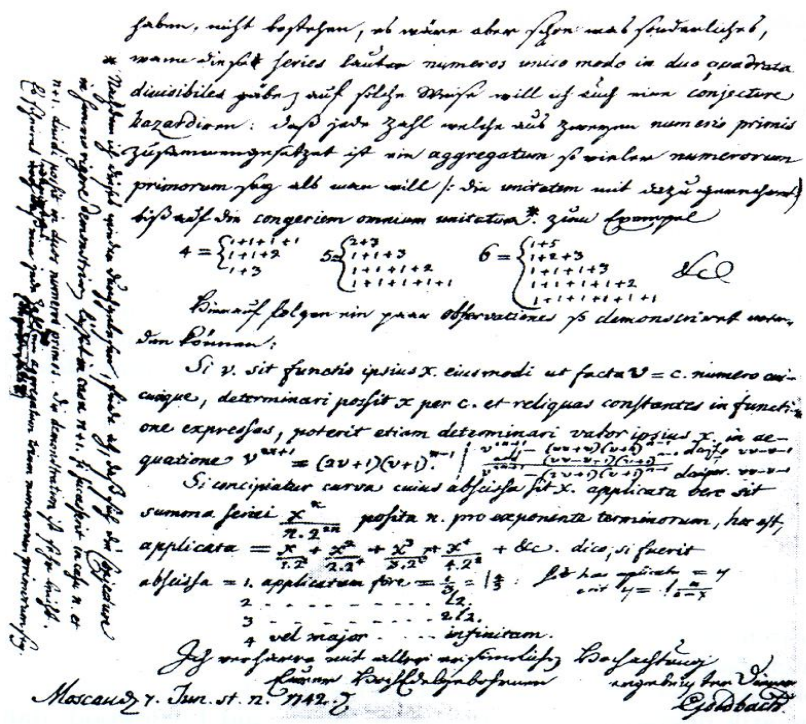
Πρότεινε έπειτα μια δεύτερη υπόθεση στο περιθώριο της επιστολής του:

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

Θεώρησε βέβαια το 1 ως πρώτο αριθμό, μια παραδοχή που αργότερα εγκαταλείφτηκε. 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 συζήτηση τους στην οποία ο Goldbach είχε θέσει την αρχική εικασία του που ήταν:

«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 μπορω να το αποδείξω.»



Το γράμμα από τον Goldbach προς τον Euler

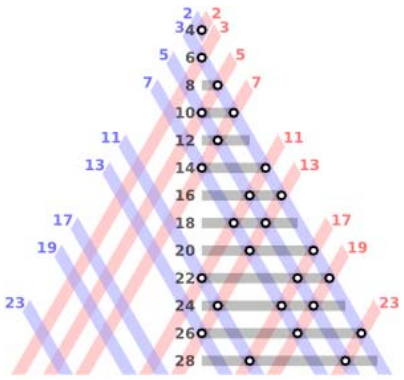
Η σημερινή διατύπωση της ‘εικασίας του Goldbach’ είναι η εξής:

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

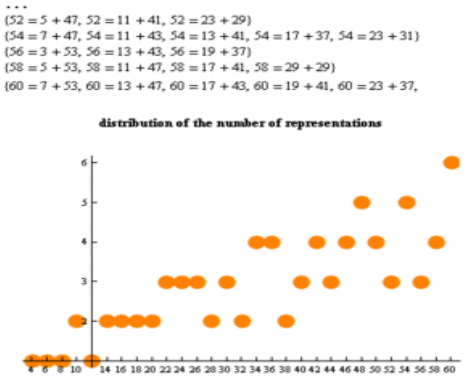
Και σε αναλυτική μορφή:

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

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



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



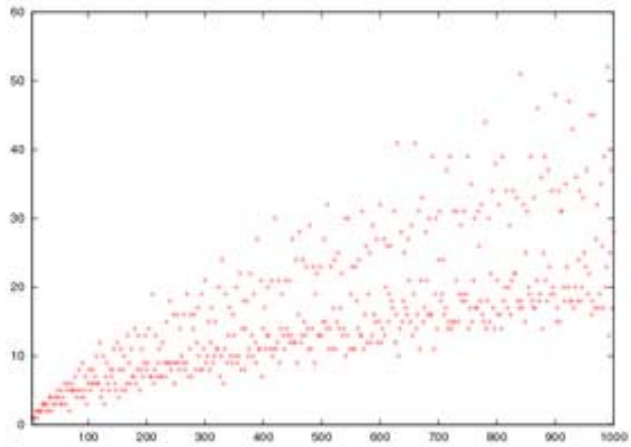
Ο αριθμός των τρόπων που ένας άρτιος αριθμός μπορεί να παρασταθεί ως το άθροισμα 2 πρώτων.

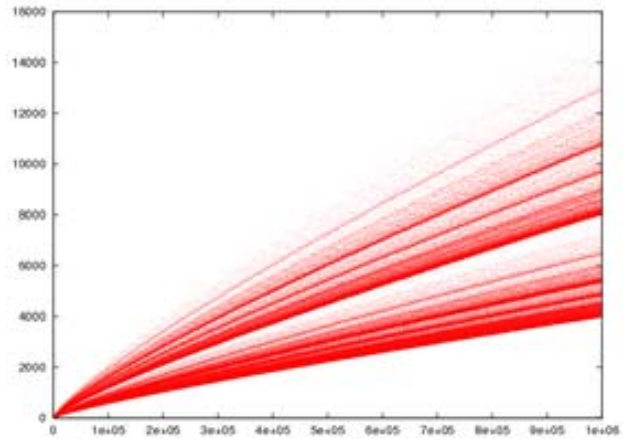
Στην θεωρία αριθμών όμως ακόμα και η επαλήθευση μερικών χιλιάδων περιπτώσεων δεν είναι αρκετή απόδειξη για να πείσει τους μαθηματικούς πως κάτι πιθανόν είναι αληθινό. Για παράδειγμα, όλοι οι περιττοί πρώτοι αριθμοί χωρίζονται σε δύο κατηγορίες, αυτούς της μορφής και αυτούς της μορφής . Θέτουμε όλους τους πρώτους της μορφής και της μορφής . Είναι γνωστό ότι υπάρχουν άπειροι πρώτοι αριθμοί και των δύο τύπων. Από υπολογισμούς βρέθηκε ότι για όλα τα . Όμως το 1957 ο βρετανός μαθηματικός J.Leech(1926-1992) βρήκε ότι για έχουμε και , άρα εδώ η ανίσωση ισχύει αντίστροφα. Το 1914 ο επίσης Βρετανός μαθηματικός J.Littlewood (1885-1977) είχε αποδείξει πως η ανίσωση αυτή αντιστρέφεται δεξιά-αριστερά απείρως συχνά. Αυτό σημαίνει ότι υπάρχουν άπειρα για τα οποία καθώς επίσης και άπειρα για τα οποία . Οι εικασίες για τους πρώτους αριθμούς λοιπόν μπορεί να είναι εσφαλμένες ακόμα και αν επαληθεύονται υπολογιστικά για χιλιάδες περιπτώσεις!

Με υπολογισμούς η εικασία του Goldbach έχει επαληθευτεί για ως και πολύ μεγάλους αριθμούς. Το 1938 ο Nils Pipping επαλήθευσε την εικασία με κόπο για Με την έλευση των υπολογιστών πολλοί περισσότεροι αριθμοί έχουν ελεγχθεί. Ο T. Oliveira e Silva εκτελεί μια κατανεμημένη έρευνα που έχει επαληθεύσει την εικασία για .

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

έλεγχος για $n \leq \cdots$	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)





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 τέτοιος ώστε κάθε αριθμός από κάποιο σημείο και έπειτα ισούται με το άθροισμα ή λιγότερων πρώτων αριθμών.

(για αρκούντως μεγάλο).

Αν γνωρίζαμε πως για όλους τους άρτιους , αυτό θα αποδείκνυε την εικασία του Goldbach για όλους τους μεγάλους . Το 1956 ο κινέζος μαθηματικός Yin Wen-Lin απέδειξε ότι . Αυτό σημαίνει πως κάθε αριθμός από κάποιο σημείο και έπειτα ισούται με το άθροισμα 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 είναι στην πραγματικότητα το άθροισμα των κατά πολύ έξι 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 της λύσης 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.

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

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 γραφτούν 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 μπορεί να γραφτεί ως άθροισμα ενός πρώτου αριθμού και ενός άλλου αριθμού που έχει το πολύ M διαφορετικούς πρώτους παράγοντες.

$$n = p + A,$$

$$A\ έχει\ το\ πολυ\ διαφορετικούς\ πρώτους\ παράγοντες, n\ περιττός, n\ αρκούντως\ μεγάλος.$$

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.

4.2 Δίδυμοι πρώτοι αριθμοί

Ορισμός 9: *Δίδυμοι πρώτοι αριθμοί* καλούνται οι πρώτοι αριθμοί 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:

$(3,5), (5,7), (11,13), (17,19), (29,31), (41,43), (59,61), (71,73), (101,103), (107,109), \ldots$

[Sloane's A001359, A006512].

Οι δίδυμοι πρώτοι απέχουν όσο το δυνατών 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 $6n \pm 1$.

Το ερώτημα αν υπάρχουν άπειροι δίδυμοι πρώτοι αριθμοί υπήρξε ένα ακόμα από τα μεγάλα ανοικτά ζητήματα στην θεωρία αριθμών για πολλά χρόνια. Η εικασία των δίδυμων πρώτων αριθμών λέει ότι: Υπάρχουν άπειροι πρώτοι αριθμοί p τέτοιοι ώστε ο $p+2$ να είναι επίσης πρώτος αριθμός. 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 που $k = 1$ είναι η εικασία των δίδυμων πρώτων αριθμών. Μία δυνατότερη μορφή της εικασίας των δίδυμων πρώτων αριθμών είναι η εικασία των μαθηματικών Hardy–

Littlewood που απαιτεί έναν νόμο κατανομής των δίδυμων πρώτων αριθμών παρόμοιο με το θεώρημα των πρώτων αριθμών.

Ένα σημαντικό αποτέλεσμα για τους πρώτους αριθμούς ήταν το Θεώρημα Brun (1919) από τον Νορβηγό μαθηματικό Viggo Brun (1885-1978).

Θεώρημα 20 (Θεώρημα Brun): Ο αριθμός που προκύπτει από την πρόσθεση των αντίστροφων των περιττών δίδυμων πρώτων αριθμών,

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

συγκλίνει σε έναν συγκεκριμένο αριθμό (ο αριθμός αυτός έχει ονομαστεί σταθερά του Brun) που εκφράζει την σπανιότητα των δίδυμων πρώτων, ακόμα και αν υπάρχουν άπειροι από αυτούς. [Ribenboim 1996, p. 201]

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

Ο Brun απέδειξε ότι υπάρχει υπολογίσιμη σταθερά x_0 τέτοια ώστε αν $x \geq x_0$, τότε $\pi_2(x) < \frac{100x}{(\ln x)^2}$ [Ribenboim 1996, p. 261].

Έχει δειχτεί ότι:

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

το οποίο γράφεται πιο συνοπτικά:

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

όπου Π_2 σταθερά γνωστή ως *σταθερά των δίδυμων πρώτων αριθμών* και c μία άλλη σταθερά.

Οι Hardy και Littlewood (1923) είπαν 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 η *δυνατή εικασία των δίδυμων πρώτων*.

Στις 15 Ιανουαρίου 2007, δύο ξεχωριστά υπολογιστικά προγράμματα, το Twin Prime Search και το PrimeGrid βρήκαν το μεγαλύτερο γνωστό ζεύγος δίδυμων πρώτων αριθμών: $2003663613 \times 2^{195000} \pm 1$ με 58711 ψηφία ο καθένας. Ανακαλύφτηκαν από τον Γάλλο Eric Vautier. Στις 6 Αυγούστου 2009 τα δύο αυτά προγράμματα

ανακοίνωσαν ότι ένα νέο ρεκόρ δίδυμων πρώτων αριθμών είχε βρεθεί: $65516468355 \times 2^{333333} \pm 1$ με 100355 ψηφία. Στις 25 Δεκέμβρη του 2011 το πρόγραμμα PrimeGrid ανακοίνωσε ότι ένα ακόμη ρεκόρ δίδυμων πρώτων είχε βρεθεί: $3756801695685 \times 2^{666669} \pm 1$ με 200700 ψηφία. Και η αναζήτηση συνεχίζεται.

5

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 $x^n + y^n = z^n$ δεν έχει μη τετριμμένη λύση για $n \geq 3$ (εικασία 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 είναι αμφιλεγόμενη, αυτό φαίνεται ασήμαντο εν συγκρίσει με την συντριπτική ποσότητα πολύτιμων μαθηματικών που έχουν δημιουργηθεί ως αποτέλεσμα ερευνών γι' αυτή 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. Όπως ο μαθηματικός Sierpinski (1882-1969) είπε κάποτε: «…η πρόοδος της γνώσης μας ως προς τους αριθμούς εξελίσσεται όχι μόνο από αυτά που ήδη γνωρίζουμε για αυτούς, αλλά από το ότι συνειδητοποιούμε τι ακόμη δεν γνωρίζουμε γι' αυτούς.»

6

Βιβλιογραφία

1. Abel, U. and Siebert, H. *"Sequences with Large Numbers of Prime Values."* *Am. Math. Monthly* **100**, 167-169, 1993.
2. A Granville, Harald Cramér and the distribution of prime numbers, Harald Cramér Symposium, Scand. Actuar. J. (1) (1995), 12-28.
3. A Weil, *Number Theory: An Approach Through History from Hammurapi to Legendre* (1984).
4. B. Artmann: *Euclid-The creation of Mathematics*, Springer-Verlag, New York 1999.
5. B C Berndt, *Ramanujan and the theory of prime numbers*, Number theory Madras 1987 (Berlin, 1989), 122-139.
6. Baker, A. *"Linear Forms in the Logarithms of Algebraic Numbers."* Mathematika 13, 204-216, 1966.
7. Baker, A. *"Imaginary Quadratic Fields with Class Number Two."* Ann. Math. 94, 139-152, 1971.
8. Ball, W. W. R. and Coxeter, *H. S. M. Mathematical Recreations and Essays*, 13th ed. New York: Dover, p. 60, 1987.
9. Borho, W. *"On Thabit ibn Kurrah's Formula for Amicable Numbers."* Math. Comput. 26, 571-578, 1972.
10. Boston, N. and Greenwood, M. L. *"Quadratics Representing Primes."* Amer. Math. Monthly 102, 595-599, 1995.
11. C. F. Gauss, *Disquisitiones Arithmeticae* (English Edition). Transl. by Arthur A. Clarke. Springer-Verlag, 1986.

12. Caldwell, C. K. and Cheng, Y. *"Determining Mills' Constant and a Note on Honaker's Problem."* J. Integer Sequences 8, Article 05.4.1, 1-9, 2005. http://www.cs.uwaterloo.ca/journals/JIS/VOL8/Caldwell/caldwell78.html.
13. Caldwell, Chris (2008). *"Goldbach's conjecture"*. Retrieved 2008-08-13.
14. 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.
15. Chudakov, Nikolai G. (1937). *"[On the Goldbach problem]"*. Doklady Akademii Nauk SSSR 17: 335–338.
16. Conway, J. H. and Guy, R. K. *The Book of Numbers*. New York: Springer-Verlag, pp. 127-130, 1996.
17. Conway, J. H. and Guy, R. K. *"The Nine Magic Discriminants."* In The Book of Numbers. New York: Springer-Verlag, pp. 224-226, 1996.
18. Courant, R. and Robbins, H. *What Is Mathematics?: An Elementary Approach to Ideas and Methods*, 2nd ed. Oxford, England: Oxford University Press, p. 26, 1996.
19. Derbyshire, J. *Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics*. New York: Penguin, 2004.)
20. 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.
21. Don Zagier, *A one-sentence proof that every prime p ≡ 1 mod 4 is a sum of two squares.* Amer. Math. Monthly 97 (1990), no. 2, 144, doi:10.2307/2323918
22. Dudley, U. *"History of Formula for Primes."* Amer. Math. Monthly 76, 23-28, 1969.
23. D. R. Heath-Brown, *Fermat's two squares theorem*. Invariant, 11 (1984) pp. 3–5.
24. 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]

25. 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.
26. Euler, L. *Nouveaux Mémoires de l'Académie royale des Sciences*. Berlin, p. 36, 1772.
27. Finch, S. R. *"Mills' Constant."* §2.13 in Mathematical Constants. Cambridge, England: Cambridge University Press, pp. 130-133, 2003.
28. Flannery, S. and Flannery, D. In Code: *A Mathematical Journey*. London: Profile Books, p. 47, 2000.
29. Fliegel, Henry F.; Robertson, Douglas S.; *"Goldbach's Comet: the numbers related to Goldbach's Conjecture"*; Journal of Recreational Mathematics, v21(1) 1–7, 1989.
30. Forman, R. *"Sequences with Many Primes."* Amer. Math. Monthly 99, 548-557, 1992.
31. F Ischebeck, *Primzahlfragen und ihre Geschichte*, Math. Semesterber. 40 (2) (1993), 121-132.
32. F Manna, *The Pentathlos of ancient science, Eratosthenes, first and only one of the 'primes'* (Italian), Atti Accad. Pontaniana (N.S.) 35 (1986), 37-44.
33. Gardner, M. *The Sixth Book of Mathematical Games from Scientific American.* Chicago, IL: University of Chicago Press, 1984.
34. Garrison, B. *"Polynomials with Large Numbers of Prime Values."* Amer. Math. Monthly 97, 316-317, 1990.
35. Gauss, Carl Friedrich; Clarke, Arthur A. (translator into English) (1986), *Disquisitiones Arithemeticae* (Second, corrected edition), New York: Springer, ISBN 0-387-96254-9
36. 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
37. 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.
38. *"Goldbach's Conjecture"* by Hector Zenil, Wolfram Demonstrations Project, 2007.

39. Goldman, Jay R. (1998), *The Queen of Mathematics: A historically motivated guide to Number Theory*, A K Peters, ISBN 1-56881-006-7
40. Granville, A.; van der Lune, J.; and te Riele, H. J. J. *"Checking the Goldbach Conjecture on a Vector Computer."* In Number Theory and Applications: Proceedings of the NATO Advanced Study Institute held in Banff, Alberta, April 27-May 5, 1988 (Ed. R. A. Mollin). Dordrecht, Netherlands: Kluwer, pp. 423-433, 1989.
41. Green, Ben; Tao, Terence (2008), *"The primes contain arbitrarily long arithmetic progressions"*, Annals of Mathematics 167 (2): 481–547, arXiv:math.NT/0404188, doi:10.4007/annals.2008.167.481.
42. Hardy, G. H. and Wright, E. M. *An Introduction to the Theory of Numbers*, 5th ed. Oxford, England: Clarendon Press, 1979.
43. Hardy, G. H. Ch. 2 in *Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work*, 3rd ed. New York: Chelsea, 1999.
44. Harold M. Edwards, *Fermat's Last Theorem. A genetic introduction to algebraic number theory*. Graduate Texts in Mathematics no. 50, Springer-Verlag, NY, 1977.
45. Havil, J. Gamma: *Exploring Euler's Constant*. Princeton, NJ: Princeton University Press, p. 167, 2003.
46. Heath-Brown, D. R.; Puchta, J. C. (2002). *"Integers represented as a sum of primes and powers of two"*. Asian Journal of Mathematics 6 (3): 535–565. arXiv:math.NT/0201299.
47. Hendy, M. D. *"Prime Quadratics Associated with Complex Quadratic Fields of Class Number 2."* Proc. Amer. Math. Soc. 43, 253-260, 1974.
48. Hilton, P.; Holton, D.; and Pedersen, J. *Mathematical Reflections in a Room with Many Mirrors*. New York: Springer-Verlag, pp. 41-42, 1997.
49. Hoffman, P. *The Man Who Loved Only Numbers: The Story of Paul Erdős and the Search for Mathematical Truth.* New York: Hyperion, pp. 108-109, 1998.
50. H Cohen, *Les nombres premiers, La recherche* 26 (278) (1995.), 760-765.
51. H. Fürstenberg: *On the infinitude of primes*, Amer. Math. Monthly 62 (1955), 353.
52. H S Uhler, *A brief history of the investigations on Mersenne numbers and the latest immense primes*, Scripta Math. 18 (1952), 122-131.
53. Ingham, AE. *"Popular Lectures"* (PDF). Retrieved 2009-09-23.

54. Jens Kruse Andersen, *Primes in Arithmetic Progression Records*. Retrieved on 2010-04-13
55. John Stillwell, *Introduction to Theory of Algebraic Integers* by Richard Dedekind. Cambridge Mathematical Library, Cambridge University Press, 1996.
56. J Echeverria, *Observations, problems and conjectures in number theory-the history of the prime number theorem, in The space of mathematics* (Berlin, 1992), 230-252.
57. J Pintz*, On Legendre's prime number formula*, Amer. Math. Monthly 87 (9) (1980), 733-735.
58. Κ. Λάκκη, *Θεωρία αριθμών*, Πανεπιστημιακές Εκδόσεις Θεσσαλονίκης 1979.
59. Landau, Edmund (1966), *Elementary Number Theory*, New York: Chelsea
60. Le Lionnais, F. *Les nombres remarquables*. Paris: Hermann, pp. 88 and 144, 1983.
61. 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.
62. L E Dickson, *History of the Theory of Numbers* (3 volumes) (New York, 1919-23, reprinted 1966).
63. L E Mauistrov, *Prime values of the polynomial x2+x+41* (Russian), Istor.-Mat. Issled. 27 (1983), 63-67.
64. L. Euler: *Introductio in Analysin Infintorum*, Tomus Primus, Lausanne 1748; Opera Omnia, Ser. 1, Vol. 8.
65. L J Goldstein, *A history of the prime number theorem*, Amer. Math. Monthly 80 (1973), 599-615.
66. Margenstern, M. (1984). *"Results and conjectures about practical numbers"*. Comptes-Rendus de l'Académie des Sciences Paris 299: 895–898.
67. Martin Aigner, Günter M. Ziegler: *Proofs from the book*. Εκδόσεις: Springer, Third Edition, p. 3, 2000.
68. Mills, W. H. *"A Prime-Representing Function."* Bull. Amer. Math. Soc. 53, 604, 1947.

69. Mollin, R. A. and Williams, H. C. *"Class Number Problems for Real Quadratic Fields." Number Theory and Cryptology*; LMS Lecture Notes Series 154, 1990.
70. Nagell, T. *"General Remarks. The Sieve of Eratosthenes."* §15 in Introduction to Number Theory. New York: Wiley, pp. 51-54, 1951.
71. Nagell, T. *"Primes in Special Arithmetical Progressions."* §44 in Introduction to Number Theory. New York: Wiley, pp. 60 and 153-155, 1951.
72. Nagell, T. *"Wilson's Theorem and Its Generalizations."* Introduction to Number Theory. New York: Wiley, pp. 99-101, 1951.
73. Oliveira e Silva, T. *"New Goldbach Conjecture Verification Limit."* Feb. 5, 2005a. http://listserv.nodak.edu/cgi-bin/wa.exe?A1=ind0502&L=nmbrthry#9.
74. Oliveira e Silva, T. *"Goldbach Conjecture Verification."* Dec. 30, 2005b. http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0512&L=nmbrthry&T=0&P=3233.
75. Ore, Ø. *Number Theory and Its History*. New York: Dover, pp. 259-261, 1988.
76. Pappas, T. The Joy of Mathematics. San Carlos, CA: Wide World Publ./Tetra, pp. 100-101, 1989.
77. Pegg, E. Jr. *"Al Zimmermann's Programming Contests: Prime Generating Polynomials."* Mar. 13, 2006. http://www.recmath.org/contest/description.php.
78. Pegg, E. Jr. *"Math Games: Prime Generating Polynomials."* Jul. 17, 2006. http://www.maa.org/editorial/mathgames/mathgames_07_17_06.html.
79. Pintz, J.; Ruzsa, I. Z. (2003). *"On Linnik's approximation to Goldbach's problem, I"*. Acta Arithmetica 109 (2): 169–194. doi:10.4064/aa109-2-6.
80. Pipping, Nils (1890-1982), *"Die Goldbachsche Vermutung und der Goldbach-Vinogradovsche Satz."* Acta. Acad. Aboensis, Math. Phys. 11, 4–25, 1938.
81. P. A. Cataldi, Trattato de nvmeri perfetti di Pietro Antonio Cataldo, Presso gli Heredi di Giovanni Rossi, Bologna, 1603.
82. P. Erdos : *Über die Reihe* $\sum 1/p$. Mathematica, Zutphen B 7 (1938), 1-2.
83. P Ribenboim, *The little book of big primes* (New York, 1991).
84. P Ribenboim, *The book of prime number records* (New York-Berlin, 1989).
85. Ribenboim, P. *The New Book of Prime Number Records*. New York: Springer-Verlag, pp. 20-21, 1996.

86. Rabinowitz, G. *"Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern."* Proc. Fifth Internat. Congress Math. (Cambridge) 1, 418-421, 1913.
87. Regimbal, Stephen (1975*), "An explicit Formula for the k-th prime number"*, Mathematics Magazine (Mathematical Association of America) 48 (4): 230–232.
88. Rowland, Eric S. (2008), *"A Natural Prime-Generating Recurrence"*, Journal of Integer Sequences 11: 08.2.8.
89. Richard Dedekind, *The theory of algebraic integers*.
90. Richstein, J. *"Verifying the Goldbach Conjecture up to 4•10^(14)."* Math. Comput. 70, 1745-1750, 2001.
91. Rivera, C. *"Highly Composite Polynomials."* http://www.primepuzzles.net/puzzles/puzz_275.htm.
92. Ruiz, S. M. *"The General Term of the Prime Number Sequence and the Smarandache Prime Function."* Smarandache Notions J. 11, 59-61, 2000.
93. R de La Taille, *Nombres premiers : 2000 ans de recherche,* Science et vie 838 (1987), 16-20, 146.
94. Serge Tabachnikov, *"Mathematica World, Volume 15,Kvant Selecta: Algebra and Analysis 2"*.
95. Séroul, R. "*The Sieve of Eratosthenes."* §8.6 in Programming for Mathematicians. Berlin: Springer-Verlag, pp. 169-175, 2000.
96. Séroul, R. *"Wilson's Theorem."* §2.9 in Programming for Mathematicians. Berlin: Springer-Verlag, pp. 16-17, 2000.
97. Shanks, D. *"A Low Density of Primes."* J. Recr. Math. 5, 272-275, 1971.
98. Shanks, D. Ex. 162 in *Solved and Unsolved Problems in Number Theory*, 4th ed. New York: Chelsea, p. 222, 1993.
99. Sinisalo, Matti K. (Oct., 1993*). "Checking the Goldbach Conjecture up to 4 1011"*. Mathematics of Computation 61 (204): 931–934. doi:10.2307/2153264.
100. 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)

101. Stark, H. M. *"A Complete Determination of the Complex Quadratic Fields of Class Number One."* Michigan Math. J. 14, 1-27, 1967.

102. Stark, H. M. *"An Explanation of Some Exotic Continued Fractions Found by Brillhart."* In Computers in Number Theory, Proc. Science Research Council Atlas Symposium No. 2 held at Oxford, from 18-23 August, 1969 (Ed. A. O. L. Atkin and B. J. Birch). London: Academic Press, 1971.

103. Stark, H. M. *"A Transcendence Theorem for Class Number Problems."* Ann. Math. 94, 153-173, 1971.

104. Stein, M. L. and Stein, P. R. *"New Experimental Results on the Goldbach Conjecture."* Math. Mag. 38, 72-80, 1965a.

105. Stein, M. L. and Stein, P. R. *"Experimental Results on Additive 2 Bases."* BIT 38, 427-434, 1965b

106. Szántó, S. *"The Proof of Szántó's Note."* http://www.dkne.hu/Proof.html.

107. S Das Gupta, *The story of prime number*, Ganita Bharati 16 (1-4) (1994), 37-52.

108. Tao, Terence; Ziegler, Tamar (2008), *"The primes contain arbitrarily long polynomial progressions"*, Acta Mathematica 201: 213-305, arXiv:math.NT/0610050.

109. 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.

110. Tom M. Apostol. *"Introduction to Analytic Number Theory"*, Springer.

111. Tomás Oliveira e Silva, [1]. Retrieved 25 April 2008.

112. U Dudley, *Formulas for primes*, Math. Mag. 56 (1) (1983), 17-22.

113. U Dudley, *History of a formula for primes*, Amer. Math. Monthly 76 (1969), 23-28.

114. Van der Corput, J. G. (1938). "*Sur l'hypothèse de Goldbach*". Proc. Akad. Wet. Amsterdam 41: 76–80.

115. V N Chubarikov, *Problems in prime number theory that are related to classical theorems of P L Chebyshev*, Moscow Univ. Math. Bull. 46 (5) (1991), 15-19.

116. Waring, E. *Meditationes Algebraicae*. Cambridge, England: University Press, 1770.

117. Wells, D. *The Penguin Dictionary of Curious and Interesting Numbers*. Middlesex, England: Penguin Books, 1986.

118. Weisstein, Eric W., *"Goldbach Conjecture"* from MathWorld.

119. Weisstein, Eric W., *"Goldbach Number"* from MathWorld.

120. Weisstein, Eric W. *"Prime-Generating Polynomial."* From MathWorld--A Wolfram Web Resource. http://mathworld.wolfram.com/Prime-GeneratingPolynomial.html

121. Willans, C. P. *"A Formula for the nth Prime Number."* Math. Gaz. 48, 413-415, 1964.

122. Wright, E. M. *"A Prime-Representing Function."* Amer. Math. Monthly 58, 616-618, 1951.

123. W Schwarz, *Some remarks on the history of the prime number theorem from 1896 to 1960, in Development of mathematics 1900-1950* (Basel, 1994), 565-616.

124. Wolfram, S. *A New Kind of Science*. Champaign, IL: Wolfram Media, p. 132, 2002.

125. "*News Archive*". PrimeGrid. 6 August 2009. Retrieved 2009-08-07.

126. *"The Prime Database: 65516468355*2^333333-1"*. Prime Pages. 13 August 2009. Retrieved 2009-08-14.

127. *"News Archive"*. PrimeGrid. 25 December 2011. Retrieved 2011-12-25.

128. *"The Prime Database: 3756801695685 • 2666669 - 1"*. Prime Pages. 25 December 2011. Retrieved 2011-12-25.

http://primes.utm.edu/largest.html

http://mathworld.wolfram.com/SieveofEratosthenes.html

http://www.gap-system.org/~history/Biographies/Eratosthenes.html

http://isaacmmcphee.suite101.com/ancient-babylonian-mathematics-a49377

http://www.math.dartmouth.edu/~euler/

http://cseweb.ucsd.edu/~gill/BWLectSite/Resources/C1U2Lo.pdf

http://www.math.dartmouth.edu/~euler/correspondence/letters/OO0765.pdf