Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

**Μεταπτυχιακή Διατριβή**

| | |
|---|---|
| Τίτλος Διατριβής | **ΕΠΩΝΥΜΟΙ ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ ΙΙ** |
| Ονοματεπώνυμο Φοιτητή | **ΒΑΡΛΑΜΟΥ ΜΑΡΙΑ** |
| Πατρώνυμο | **ΚΩΝΣΤΑΝΤΙΝΟΣ** |
| Αριθμός Μητρώου | **ΜΠΠΛ/ 07058** |
| Επιβλέπων | **Γεωργιακώδης Φώτιος, Καθηγητής** |

Ημερομηνία Παράδοσης **Μάιος 2011**

**Τριμελής Εξεταστική Επιτροπή**

| | | |
|---|---|---|
| (υπογραφή) | (υπογραφή) | (υπογραφή) |
| Γεωργιακώδης Φ.<br>Καθηγητής | Σαπουνακης Α.<br>Καθηγητής | Τσικούρας Π.<br>Καθηγητής |

## ΠΕΡΙΛΗΨΗ

Οι πρώτοι αριθμοί αποτελούν το βασικό αντικείμενο μελέτης της Θεωρίας Αριθμών και της Κρυπτογραφίας. Από την εποχή του Ευκλείδη μέχρι σήμερα πολλοί διακεκριμένοι επιστήμονες έχουν εργασθεί σε προβλήματα που σχετίζονται άμεσα ή έμμεσα με τους πρώτους αριθμούς.

Στην εργασία αυτή παρουσιάζονται αποτελέσματα που σχετίζονται με τα επόμενα ερωτήματα: Υπάρχει κάποιος τύπος για την κατασκευή όλων των πρώτων αριθμών; Υπάρχει κάποια κανονικότητα στην εμφάνιση των πρώτων αριθμών; Πώς μπορούμε να κατασκευάσουμε μεγάλους πρώτους αριθμούς; Ποια η σύνδεση των πρώτων αριθμών με προβλήματα γεωμετρικών κατασκευών;

Τέλος, σε κάθε ενότητα περιλαμβάνονται βιβλιογραφικές πηγές που περιέχουν μεγαλύτερη ανάλυση κάθε προβλήματος.

## ABSTRACT

Prime numbers lie in the heart of current research in Number Theory and Cryptography. Since the time of Euclid many distinguished scientists have worked on problems related directly or indirectly to prime numbers.

In this work, we present some results related with the following questions: Is there a formula for the construction of all prime numbers? Is there any sort of normality in the appearance of prime numbers? How can we construct large prime numbers? What is the connection of prime number to geometric construction problems?

Every section contains references to sources that have more detailed analysis for each question.

# ΠΕΡΙΕΧΟΜΕΝΑ

# 1. ΕΙΣΑΓΩΓΗ

Ένας φυσικός αριθμός p ονομάζεται **πρώτος αριθμός** αν διαιρείται μόνο από το p και την μονάδα, διαφορετικά ονομάζεται **σύνθετος αριθμός**. Για παράδειγμα, υπάρχουν 25 πρώτοι αριθμοί που είναι μικρότεροι από το 100, οι εξής:

| | | | | |
|---|---|---|---|---|
| 2 | 3 | 5 | 7 | 11 |
| 13 | 17 | 19 | 23 | 29 |
| 31 | 37 | 41 | 43 | 47 |
| 53 | 59 | 61 | 67 | 71 |
| 73 | 79 | 83 | 89 | 97 |

Ο αριθμός 1, ενώ αρχικά θεωρούνταν πρώτος αριθμός, σήμερα δεν θεωρείται ότι ανήκει στους πρώτους αριθμούς αλλά ούτε και στους σύνθετους. Ο λόγος είναι ότι κάθε φυσικός αριθμός γράφεται ως γινόμενο ενός ή περισσοτέρων αριθμών. Για παράδειγμα ο αριθμός 120 γράφεται ως γινόμενο με τον εξής τρόπο:

$$120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3^1 \cdot 5^1$$

Αν ομαδοποιήσουμε όλους τους κοινούς πρώτους παράγοντες, τότε η προηγούμενη έκφραση είναι μοναδική για κάθε αριθμό, δηλαδή κάθε φυσικός αριθμός γράφεται κατά μοναδικό τρόπο υπό τη μορφή

$$n = \mathrm{p}_1^{\mathrm{a}_1} \cdot \mathrm{p}_2^{\mathrm{a}_1} \cdots \mathrm{p}_\mathrm{k}^{\mathrm{a}_\mathrm{k}}$$

όπου $p_{1,}p_{2,,} \dots, p_{k,}$ είναι πρώτοι αριθμοί και $a_{1,}a \dots, a_{k,}$είναι φυσικοί αριθμοί.

Αν θεωρήσουμε και τον αριθμό 1 ως πρώτο αριθμό τότε η ανάλυση αυτή παύει να είναι μονοσήμαντη, αφού για παράδειγμα, ισχύει ότι

$$120 = 1^1 \cdot 2^3 \cdot 3^1 \cdot 5^1 = 1^{120} \cdot 2^3 \cdot 3^1 \cdot 5^1 = 1^{2011} \cdot 2^3 \cdot 3^1 \cdot 5^1$$

δηλαδή ο αριθμός 1 συμμετέχει στην ανάλυση υψωμένος σε οποιαδήποτε δύναμη. Ένας επιπλέον λόγος, για να μην συμπεριλάβουμε το 1 στους πρώτους αριθμούς είναι ότι το 1 έχει μόνο ένα διαιρέτη, τον εαυτό του, και όχι δύο όπως όλοι οι υπόλοιποι πρώτοι αριθμοί.

Οι πρώτοι αριθμοί μελετήθηκαν για πρώτη φορά στην αρχαία Ελλάδα.

Ο Ευκλείδης, στο έργο του Στοιχεία απέδειξε ότι το πλήθος των πρώτων αριθμών είναι άπειρο.

Στη συνέχεια, ο Ερατοσθένης ο Κυρηναίος, επινόησε μια απλή μέθοδο για την εύρεση των πρώτων αριθμών που είναι μικρότεροι από κάποιον φυσικό αριθμό. Η μέθοδός του διασώθηκε από τον Νικόμαχο τον Γερασηνό, στο έργο του Αριθμητική Εισαγωγή, και ονομάστηκε **κόσκινο του Ερατοσθένη**.

Για παράδειγμα, η μέθοδος του Ερατοσθένη για την εύρεση των 25 πρώτων αριθμών που είναι μικρότεροι από το 100 είναι η εξής: Αρχικά τοποθετούμε σε ένα πλέγμα όλους τους αριθμούς από το 1 έως το 100. Σβήνουμε όλα τα πολλαπλάσια του 2 (εκτός από το 2), στην συνέχεια βρίσκουμε τον πρώτο αριθμό που δεν έχουμε σβήσει (δηλαδή το 3) και σβήνουμε όλα τα πολλαπλάσια του 3 (εκτός από 3). Ο επόμενος αριθμός που δεν έχουμε σβήσει είναι το 5. Σβήνουμε όλα τα πολλαπλάσια του 5 (εκτός από το 5). Ο επόμενος αριθμός που απομένει είναι το 7. Σβήνουμε όλα τα πολλαπλάσια του 7 (εκτός από το 7). Ο επόμενος αριθμός που δεν έχουμε σβήσει είναι το 11, το οποίο είναι μεγαλύτερο από την τετραγωνική ρίζα του 100, δηλαδή το 10. Επομένως, η διαδικασία έχει ολοκληρωθεί. Οι αριθμοί που απομένουν είναι όλοι οι πρώτοι αριθμοί που είναι μικρότεροι από το 100.

Γενικότερα, για να βρούμε τους πρώτους αριθμούς που είναι μικρότεροι ή ίσοι από το n σβήνουμε με τον ίδιο τρόπο όλα τα πολλαπλάσια αριθμών που είναι μικρότεροι από την τετραγωνική ρίζα του n. [58]

•Αυτό είναι ένα κενό κόσκινο.

01, 02, 03, 04, 05, 06, 07, 08, 09, 10,<br>
11, 12, 13, 14, 15, 16, 17, 18, 19, 20,<br>
21, 22, 23, 24, 25, 26, 27, 28, 29, 30,<br>
31, 32, 33, 34, 35, 36, 37, 38, 39, 40,<br>
41, 42, 43, 44, 45, 46, 47, 48, 49, 50,<br>
51, 52, 53, 54, 55, 56, 57, 58, 59, 60,<br>
61, 62, 63, 64, 65, 66, 67, 68, 69, 70,<br>
71, 72, 73, 74, 75, 76, 77, 78, 79, 80,<br>
81, 82, 83, 84, 85, 86, 87, 88, 89, 90,<br>
91, 92, 93, 94, 95, 96, 97, 98, 99, 100

•Αυτό είναι ένα κόσκινο πρώτων αριθμών με διαγραμμένα τα πολλαπλάσια 2-10 Αυτά που έχουν μείνει είναι πρώτοι αριθμοί.

~~01,~~ 02, 03, ~~04~~, 05, 06, 07, ~~08~~, ~~09~~, ~~10~~,<br>
11, ~~12~~, 13, ~~14, 15, 16~~, 17, 18, ~~19~~, ~~20~~,<br>
~~21~~, ~~22~~, 23, ~~24, 25, 26, 27, 28~~, 29, ~~30~~,<br>
31, ~~32, 33, 34, 35, 36~~, 37, ~~38, 39, 40,~~<br>
41, ~~42~~, 43, ~~44, 45, 46~~, 47, ~~48, 49, 50~~,<br>
~~51~~, ~~52~~, 53, ~~54, 55, 56, 57, 58, 59, 60,~~<br>
61, ~~62, 63, 64, 65, 66~~, 67, ~~68, 69, 70~~,<br>
71, ~~72~~, 73, ~~74, 75, 76, 77, 78~~, 79, ~~80~~,<br>
~~81~~, ~~82~~, 83, ~~84, 85, 86, 87, 88~~, 89, ~~90~~,<br>
~~91, 92, 93, 94, 95, 96~~, 97, ~~98, 99, 100~~

Μετά τους αρχαίους Έλληνες, τους πρώτους αριθμούς μελέτησαν οι Άραβες, όπως για παράδειγμα ο Thabit Ibn Qurra Ibn Marwan Al-Sabi Al-Harrani. Επίσης, με τους πρώτους αριθμούς ασχολήθηκαν μεγάλοι μαθηματικοί όπως οι Gauss, Euler και Lagrange, αλλά και πολλοί άλλοι ερασιτέχνες μαθηματικοί, όπως για παράδειγμα ο Fermat.. Σήμερα, οι πρώτοι αριθμοί βρίσκονται στην καρδιά της έρευνας του κλάδου των μαθηματικών που ονομάζεται Θεωρία Αριθμών αλλά και της Κρυπτογραφίας.

## 1.1. ΧΡΗΣΕΙΣ ΤΩΝ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ

Ως τις αρχές του 20ού αιώνα, οι μαθηματικοί θεωρούσαν ότι οι πρώτοι αριθμοί και η μελέτη τους αποτελούσε τμήμα των λεγόμενων Καθαρών Μαθηματικών και πως τα αποτελέσματά τους είχαν κυρίως θεωρητικό χαρακτήρα και όχι πρακτικό.

Χαρακτηριστική είναι η γνώμη του Άγγλου μαθηματικού G. Hardy, όπως περιγράφεται στο βιβλίο του Η Απολογία ενός Μαθηματικού, ο οποίος νιώθει περήφανος ότι τα αποτελέσματα της έρευνάς του πάνω στην θεωρία αριθμών δεν θα χρησιμοποιηθούν ποτέ για σκοπούς όπως πολεμικούς.

Ο προσανατολισμός και τα κίνητρα της έρευνας για τους πρώτους αριθμούς άλλαξε όταν τον $20^{ο}$ αιώνα βρέθηκε τρόπος να χρησιμοποιηθούν οι πρώτοι αριθμοί σε προβλήματα Κρυπτογραφίας. Ειδικότερα, το 1978, οι Ron Rivest, Adi Shamir και Leonard Adleman, παρουσίασαν μια μέθοδο, η οποία ονομάστηκε **αλγόριθμος RSA**, η οποία επιτρέπει την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων χρησιμοποιώντας μεγάλους πρώτους αριθμούς, η δε ασφάλειά της βασίζεται στην δυσκολία εύρεσης των πρώτων παραγόντων ενός αριθμού.

## 1.2. ΠΡΟΤΥΠΑ ΣΤΟΥΣ ΠΡΩΤΟΥΣ ΑΡΙΘΜΟΥΣ

Η κατανομή των πρώτων αριθμών μοιάζει να μην ακολουθεί κάποιο πρότυπο. Το γεγονός αυτό κάνει την εύρεση των πρώτων αριθμών αρκετά δύσκολη.

Το βασικότερο θεώρημα που περιγράφει την κατανομή των πρώτων αριθμών είναι το λεγόμενο **θεώρημα των πρώτων αριθμών** το οποίο αναφέρεται στο πλήθος των πρώτων αριθμών που είναι μικρότεροι ή ίσοι από κάποιο αριθμό. Η διατύπωσή του είναι η εξής:

**Θεώρημα πρώτων αριθμών**

*Ο αριθμός των πρώτων αριθμών που είναι μικρότεροι ή ίσοι από το n ισούται περίπου με*

$$\frac{n}{\ln n}$$

Για παράδειγμα, υπάρχουν 25 πρώτοι αριθμοί που είναι μικρότεροι ή ίσοι από το 100, ενώ το θεώρημα των πρώτων αριθμών δίνει πλήθος $\frac{100}{\ln 100} \approx 22$.

Μέχρι σήμερα δεν έχει βρεθεί κάποια συνάρτηση που να παράγει όλους τους πρώτους αριθμούς Εν τούτοις, υπάρχουν ακολουθίες που παράγουν πρώτους αριθμούς. Για παράδειγμα, όπως θα δούμε παρακάτω, ο Mills έχει αποδείξει ότι υπάρχει μια σταθερά A για την οποία οι τιμές $A^n$ είναι πρώτοι αριθμοί για κάθε φυσικό αριθμό n.

Μια προσπάθεια για να βρεθούν κανονικότητες στις εμφανίσεις των πρώτων αριθμών, έχει γίνει από τον Ulam, σε επόμενη ενότητα θα αναφερθούμε στη λεγόμενη σπείρα του Ulam.

Φυσικά, υπάρχουν και μεμονωμένα παραδείγματα πρώτων αριθμών οι οποίοι εμφανίζουν έντονη κανονικότητα. Για παράδειγμα, ο αριθμός 12345678901234567891 είναι πρώτος αριθμός Επίσης οι παλινδρομικοί ή καρκινικοί αριθμοί 111191111, 919191919, και 123494321 είναι επίσης πρώτοι αριθμοί.[60]

## 1.3. ΤΑΥΤΟΠΟΙΗΣΗ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ (PRIMALITY TESTS)

Λόγω της μη ύπαρξης κάποιου προτύπου στην κατανομή των πρώτων αριθμών, κάθε φυσικός αριθμός πρέπει να εξεταστεί χωριστά προκειμένου να ελεγχθεί αν είναι πρώτος αριθμός ή όχι, ένα έργο το οποίο, ακόμα και με τους υπολογιστές, είναι πολύ δύσκολο

Ένα **primality test** είναι μια δοκιμή για να καθοριστεί εάν ένας δεδομένος αριθμός είναι πρώτος ή όχι.

Υπάρχουν δύο κατηγορίες από primality tests: ντετερμινιστικά και πιθανοθεωρητικά.

Τα ντετερμινιστικά τεστ καθορίζουν με απόλυτη βεβαιότητα αν ένας αριθμός είναι πρώτος ή όχι. Το πρώτο ντετερμινιστικό τεστ είναι το κόσκινο του Ερατοσθένη, ενώ το πιο πρόσφατο είναι το τεστ AKS (Agrawal-Kayal-Saxena primality test, 2002). Ένα από τα πιο δημοφιλή είναι το τεστ Lucas-Lehmer.

Τα πιθανοθεωρητικά τεστ μπορούν ενδεχομένως να αποτύχουν (αν και με πολύ μικρή πιθανότητα) και να χαρακτηρίσουν έναν σύνθετο αριθμό ως πρώτο. Ωστόσο, είναι γενικά πολύ γρηγορότερα από τα ντετερμινιστικά τεστ.

Οι αριθμοί που έχουν περάσει μια πιθανοθεωρητική δοκιμή πρώτων αριθμών αναφέρονται επομένως ως πιθανοί πρώτοι αριθμοί έως ότου αυτό αποδειχθεί με κάποιο ντετερμινιστικό τεστ. Ένας αριθμός που περνά ένα πιθανοθεωρητικό τεστ αλλά στην πραγματικότητα είναι σύνθετος είναι γνωστός ως **ψευδοπρώτος**. Υπάρχουν πολλοί ειδικοί τύποι ψευδοπρώτων αριθμών, οι πιο γνωστοί είναι οι ψευδοπρώτοι Fermat, τους οποίους θα αναφέρουμε σε επόμενη ενότητα.

Το πιο δημοφιλές πιθανοθεωρητικό τεστ είναι το Rabin-Miller τεστ. Από την έκδοση 2.2 και έπειτα το λογισμικό Mathematica χρησιμοποιεί το λεγόμενο πολλαπλό Rabin-Miller τεστ με βάσεις 2 και 3, το οποίο συνδυάζεται με το Lucas-Lehmer τεστ για τον έλεγχο των πρώτων αριθμών (Η εντολή PrimeQ[n] υλοποιεί τις παραπάνω μεθόδους)

Η υπολογιστική πολυπλοκότητα του προβλήματος ελέγχου για πρώτους αριθμούς θεωρούνταν ότι ήταν πολυωνυμικού χρόνου, σε αντίθεση με την υπολογιστική πολυπλοκότητα του προβλήματος της παραγοντοποίησης ενός αριθμού σε πρώτους παράγοντες, η οποία θεωρείται μη πολυωνυμικού χρόνου. Το γεγονός αυτό αποδείχθηκε πρόσφατα, το 2002, από τους ο Agrawal, Kayal και Saxena, οι οποίοι ανακάλυψαν έναν πολυωνυμικό αλγόριθμο για την ταυτοποίηση πρώτων αριθμών που έχει ασυμπτοτική πολυπλοκότητα της τάξης $O(ln^{12}n)$. [61]

# 2. ΕΠΩΝΥΜΟΙ ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

## 2.1. MILLS

Ο **William H. Mills** (9 Νοεμβρίου 1921 – 7 Μαρτίου 2007) ήταν μαθητής του Emil Artin τη δεκαετία του 40. Τελείωσε υπό την επίβλεψή του τη διατριβή του με θέμα «Prime Power Reciprocity in Algebraic Number-Fields» το 1949. [35] Το 1947 ο Mills απέδειξε το επόμενο θεώρημα [22]:

### Θεώρημα Mills (Σταθερά Mills)

Υπάρχει μια σταθερά A για την οποία η ακολουθία $\left[A^{3^n}\right]$ λαμβάνει τιμές μόνο πρώτους αριθμούς για όλες τις ακέραιες τιμές του n, όπου $[x]$ είναι το ακέραιο μέρος του x.

Αν και μια τέτοια σταθερά A υπάρχει, ο Mills στην εργασία του δεν έδωσε κάποια μέθοδο κατασκευής της. Στην πραγματικότητα, για να υπολογίσουμε το A πρέπει να γνωρίζουμε τους πρώτους αριθμούς και επιπλέον για να λάβουμε ακόμα και μερικούς πρώτους αριθμούς από αυτή την ακολουθία πρέπει να υπολογίσουμε το A σε ένα πολύ μεγάλο αριθμό δεκαδικών θέσεων.[5].

Υπάρχουν πολλές σταθερές A με αυτή την ιδιότητα. Είναι δυνατό να ορισθεί η **σταθερά Mills** ως το μικρότερο $A$ έτσι ώστε: $\left[A^{3^n}\right]$ είναι πρώτος αριθμός για όλες τις ακέραιες τιμές του $n$.

Οι Clawson [10], Delehayer [9] και Ribenboim [12] αναφέρουν ότι η σταθερά A ισούται περίπου με $1.3063778838$ όμως οι Caldwell και Cheng [20] σχολιάζουν ότι ο υπολογισμός της σταθεράς A προϋποθέτει ορισμένες παραδοχές. Οι ίδιοι, υποθέτοντας ότι η υπόθεση του Riemann αληθεύει, αποδεικνύουν ότι για κάθε $x \geq 0.26$ υπάρχει τουλάχιστον ένας πρώτος αριθμός ανάμεσα στους $x^3$ και $(x+1)^3$. Χρησιμοποιώντας αυτήν την πρόταση υπολόγισαν την σταθερά Mills με ακρίβεια 6850 δεκαδικών ψηφίων.

Η σταθερά Mills με τα 600 πρώτα δεκαδικά της ψηφία είναι η εξής:

1.3063778838 6308069046 8614492602 6057129167 8458515671
3644368053 7599664340 5376682659 8821501403 7011973957
0729696093 8103086882 2388614478 1635348688 7133922146
1943534578 7110033188 1405093575 3558319326 4801721383
2361522359 0622186016 1085667905 7215197976 0951619929
5279707992 5631721527 8412371307 6584911245 6317518426
3310565215 3513186684 1550790793 7238592335 2208421842
0405320517 6890260257 9344300869 5290636205 6989687262
1227499787 6664385157 6619143877 2844982077 5905648255
6091500412 3788524793 6260880466 8815406437 4425340131
0736114409 4137650364 3793012676 7211713103 0265228386
6154666880 4874760951 4410790754 0698417260 3473107746

Δεν είναι γνωστό αν η σταθερά Mills είναι αριθμός ρητός ή άρρητος.[23]

Οι τιμές της ακολουθίας $\left[A^{3^n}\right]$ όπου A είναι η σταθερά Mills ονομάζονται (**πρώτοι) αριθμοί του Mills**. Είναι φανερό ότι οι τιμές αυτής της ακολουθίας αυξάνουν ραγδαία, διότι ο εκθέτης της σταθεράς αυξάνει ο ίδιος με εκθετικό ρυθμό, επομένως είναι υπολογιστικά δύσκολος ο προσδιορισμός αυτών των πρώτων αριθμών.

Οι πρώτοι πέντε αριθμοί Mills είναι οι εξής:

2, 11, 1361, 2521008887, 16022236204009818131831320183.

Ο έκτος αριθμός Mills έχει 86 ψηφία. Οι Caldwell και Cheng έχουν προσδιορίσει τους πρώτους δέκα αριθμούς Mills, ο δέκατος αριθμός Mills είναι ο

$((((((((((2^3+3)^3+30)^3+6)^3+80)^3+12)^3+450)^3+894)^3+3636)^3+70756)^3+97220$
ο οποίος έχει 20562 ψηφία [29].

Επιπλέον, οι Caldwell και Cheng έχουν υπολογίσει άλλους δύο αριθμούς, οι οποίοι. πιθανόν να είναι οι επόμενοι δύο αριθμοί Mills. Ο δωδέκατος αριθμός έχει 61684 ψηφία [20][23].

## 2.2. PIERPONT

Ο **James P. Pierpont** (16 Ιουνίου 1866 – 9 Δεκεμβρίου 1938) ξεκίνησε τις σπουδές του στο Worcester Polytechnic Institute ως Μηχανολόγος. Κατά τη διάρκεια όμως των σπουδών του συνειδητοποίησε ότι τα μαθηματικά ήταν αυτά που τον ενδιέφεραν. Αποφοίτησε το 1886 αλλά είχε ήδη σχεδιάσει να σπουδάσει μαθηματικά σε Ευρωπαϊκά Πανεπιστήμια.

Ακολούθησε το Γερμανικό πρότυπο σπουδάζοντας σε διάφορα Πανεπιστήμια, αλλά το μεγαλύτερο μέρος των σπουδών του ήταν στο Πανεπιστήμιο του Βερολίνου. Εκεί διδάχτηκε από κορυφαίους μαθηματικούς όπως τους: Lazarus Fuchs, Karl Weierstrass and Leopold Kronecker. Τα τελευταία χρόνια των σπουδών του τα πέρασε στο Πανεπιστήμιο της Βιέννης. Το 1894 του απενεμήθη το διδακτορικό του για τη διατριβή του «Zur Geschichte der Gleichung fünften Grades bis zum Jahre 1858».

Τον Σεπτέμβριο του 1899 συμμετείχε στη θερινή συνεδρίαση της Γερμανικής Μαθηματικής Κοινότητας στο Μοναχό. Από αυτή τη περίοδο και μετά ασχολήθηκε με τη θεωρία των συναρτήσεων των πραγματικών μεταβλητών και των ολοκληρωμάτων, δημοσιεύοντας τις εργασίες «On multiple integrals» (1905) και «On improper multiple integrals» (1906). Μεταξύ αυτών των δύο δημοσιεύτηκε το πρώτο του βιβλίο, που αποτέλεσε το πρώτο μέρος του μετέπειτα «Lectures on the Theory of Functions of Real Variables» (1905). Το δεύτερο μέρος εκδόθηκε το 1912. Το επόμενο βιβλίο του είχε τίτλο «Functions of a complex variable» (1914).[31]

### Κατασκευές κανονικών πολυγώνων

Τα τρία κλασικά γεωμετρικά προβλήματα της αρχαιότητας είναι το πρόβλημα του διπλασιασμού του κύβου, το πρόβλημα της τριχοτόμησης μιας γωνίας και το πρόβλημα του τετραγωνισμού του κύκλου. Τα προβλήματα αυτά αποδείχθηκε ότι δεν μπορούν να λυθούν χρησιμοποιώντας μόνο κανόνα και διαβήτη. Εκτός από αυτά υπάρχει και το πρόβλημα της κατασκευής ενός κανονικού πολυγώνου με n πλευρές. Στην πραγματικότητα αυτό είναι μια οικογένεια από προβλήματα, ένα για κάθε τιμή του n.

Αποδεικνύεται ότι δεν υπάρχει πάντα λύση, χρησιμοποιώντας μόνο κανόνα και διαβήτη, για όλες τις τιμές του n αλλά για ορισμένες από αυτές. Στην αρχαιότητα ήταν γνωστές οι λύσεις για n = 3, 4, 6, 8, 12. Την τελική λύση όμως στο πρόβλημα αυτό έδωσε ο Carl Gauss, ο οποίος εντυπωσιάστηκε τόσο πολύ από αυτό το πρόβλημα που μετά την λύση του αποφάσισε να αφιερωθεί στα μαθηματικά.

Ο Gauss απέδειξε ότι η κατασκευή, χρησιμοποιώντας μόνο κανόνα και διαβήτη, του κανονικού πολυγώνου με n πλευρές, είναι δυνατή αν και μόνο αν $\varphi(n)$ είναι δύναμη του 2, όπου $\varphi(n)$ είναι η συνάρτηση Euler, δηλαδή $\varphi(n)$ είναι το πλήθος των αριθμών που είναι μικρότεροι από το n και πρώτοι προς αυτό.

Οι τιμές της συνάρτησης $\varphi(n)$ για n∈[3,47] δίνονται στον επόμενο πίνακα:

| n | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|
| $\varphi(n)$ | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 10 |
| n | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| $\varphi(n)$ | 4 | 12 | 6 | 8 | 8 | 16 | 6 | 18 | 8 |
| n | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| $\varphi(n)$ | 12 | 10 | 22 | 8 | 20 | 12 | 24 | 12 | 28 |
| n | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 |
| $\varphi(n)$ | 8 | 30 | 16 | 20 | 16 | 24 | 12 | 36 | 18 |
| n | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 |
| $\varphi(n)$ | 24 | 16 | 40 | 12 | 42 | 20 | 24 | 22 | 46 |

Επομένως, χρησιμοποιώντας μόνο κανόνα και διαβήτη, από τα κανονικά πολύγωνα με το πολύ 47 πλευρές, είναι δυνατή η κατασκευή αυτών που έχουν τους εξής αριθμούς πλευρών:

3,4,5,6,8,10,12,15,16,17,20,24,30,32,34,40.

Μια πιο πλήρη απάντηση στο πρόβλημα της κατασκευής δίνει η επόμενη πρόταση.

**Πρόταση (Κατασκευή κανονικών πολυγώνων με κανόνα και διαβήτη)**

Ένα κανονικό πολύγωνο με n πλευρές μπορεί να κατασκευασθεί με κανόνα και διαβήτη αν και μόνο αν

$$n = 2^r p_1 p_2 \dots p_k$$

όπου $p_1, p_2, \dots, p_k$ είναι διακεκριμένοι **αριθμοί Fermat**.

Οι αριθμοί Fermat, που πήραν το όνομα τους από τον πρώτο μελετητή τους Pierre de Fermat, είναι ακέραιοι αριθμοί της μορφής $F_n = 2^{2^n} + 1$, όπου n είναι ένας θετικός ακέραιος.

Μερικοί από τους πρώτους αριθμούς Fermat είναι οι εξής:

3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, …

Αν επιτρέψουμε την χρήση και άλλων οργάνων εκτός από τον κανόνα και τον διαβήτη τότε επεκτείνονται οι λύσεις του προβλήματος της κατασκευής κανονικών πολυγώνων.

Για παράδειγμα, αν έχουμε ένα όργανο για την τριχοτόμηση της γωνίας (όπως για παράδειγμα την κογχοειδή καμπύλη του Νικομήδη) τότε ισχύει η επόμενη πρόταση.

**Πρόταση (Κατασκευή κανονικών πολυγώνων με κανόνα, διαβήτη και τριχοτόμο γωνίας)**

Ένα κανονικό πολύγωνο με n πλευρές μπορεί να κατασκευαστεί από χάρακα, διαβήτη και τριχοτόμο-γωνίας αν και μόνο αν

$$n = 2^r 3^s p_1 p_2 \dots p_k$$

όπου $p_1, p_2, \dots, p_k$ είναι διακεκριμένοι πρώτοι αριθμοί Pierpont και $n > 3$.

Ένας πρώτος αριθμός $p$ ονομάζεται **(πρώτος) αριθμός Pierpont** όταν είναι της μορφής $p = 2^k 3^l + 1$ .

Μερικοί από τους πρώτους αριθμούς Pierpont είναι οι εξής:

2, 3, 5, 7, 13, 17, 19, 37, 73, 97, 109, 163, 193, 257, 433, 487, 577, 769, ...

Το πλήθος των πρώτων αριθμών Pierpont που είναι μικρότεροι από $10^1, 10^2, 10^3, \dots, 10^n$, ... είναι 4, 10, 18, 25, 32, 42, 50, 58, ... αντίστοιχα.

Ενώ, το πλήθος των πρώτων αριθμών Pierpont που είναι μικρότεροι από $10^1, 10^2, 10^4, 10^8, \dots, 10^{2^n}$ ... είναι 4, 10, 25, 58, 125, 250, 505, 1020, 2075, 4227, ..., αντίστοιχα.

Μέχρι σήμερα ο μεγαλύτερος γνωστός πρώτος αριθμός Pierpont είναι ο $3 \cdot 2^{5082306} + 1$ , ο οποίος έχει 1529928 δεκαδικά ψηφία.[24]

Μια επιπλέον εμφάνιση των πρώτων αριθμών Pierpont αναφέρεται στο πρόβλημα της αναζήτησης των πρώτων αριθμών Fermat. Υπάρχουν πρώτοι αριθμοί Pierpont οι οποίοι είναι παράγοντες κάποιων αριθμών Fermat.

Στον επόμενο πίνακα δίνονται οι τιμές των m, k, και n έτσι ώστε ο αριθμός $\alpha = k \cdot 2^n + 1$ $\nu\alpha$ $\delta\iota\alpha\iota\rho\varepsilon\acute{\iota}$ $\tau o\nu$ $\alpha\rho\iota\theta\mu\acute{o}$ $\beta = 2^{2m} + 1$ όπου k είναι δύναμη του 3 και ο αριθμός α είναι πρώτος αριθμός Pierpont και β είναι ένας αριθμός Fermat.[62]

| ***m*** | ***k*** | ***n*** | ***Year*** | ***Discoverer*** |
|---|---|---|---|---|
| 38 | 3 | 41 | 1903 | Cullen, Cunningham & Western |
| 63 | 9 | 67 | 1956 | Robinson |
| 207 | 3 | 209 | 1956 | Robinson |
| 452 | 27 | 455 | 1956 | Robinson |
| 9428 | 9 | 9431 | 1983 | Keller |
| 12185 | 81 | 12189 | 1993 | Dubner |
| 28281 | 81 | 28285 | 1996 | Taura |
| 157167 | 3 | 157169 | 1995 | Young |
| 213319 | 3 | 213321 | 1996 | Young |
| 303088 | 3 | 303093 | 1998 | Young |
| 382447 | 3 | 382449 | 1999 | Cosgrave & Gallot |
| 461076 | 9 | 461081 | 2003 | Nohara,Jobling,Woltman & Gallot |
| 672005 | 27 | 672007 | 2005 | Cooper,Jobling,Woltman & Gallot |
| 2145351 | 3 | 2145353 | 2003 | Cosgrave,Jobling,Woltman & Gallot |
| 2478782 | 3 | 2478785 | 2003 | Cosgrave,Jobling,Woltman & Gallot |

## 2.3. PILLAI

Ο **S. Sivasankaranarayana Pillai** (γνωστός στη Μαθηματική κοινότητα ως **S.S.Pillai**) (5 Απριλίου 1901-31 Αυγούστου 1950) γεννήθηκε στο Vallam του Tamilnadu. Σε ηλικία 9 ετών πήγε στο Γυμνάσιο του Shencottah. Εκεί ο καθηγητής του, Sastriar, βλέποντας την υψηλή διανοητική του ικανότητα, τον στήριξε και τον ενθάρρυνε οικονομικά και ηθικά, όταν έχασε τον πατέρα του, να συνεχίσει τις σπουδές του στο Γυμνάσιο αλλά και να προχωρήσει σε περαιτέρω σπουδές. Ο Pillai συνέχισε τις σπουδές του στο Scott Christian College στο Nargecoil με υποτροφία και έπειτα στο Maharaja's College στο Trivandrum. Το 1927 ο Pillai έλαβε ένα Research Studentship για το University of Madras. Κατόπιν εκλέχθηκε ως λέκτορας στο Annamalai University. Το 1941 πήγε στο University of Calcutta ως λέκτωρ. Για τα επιτεύγματα του κλήθηκε να επισκεφτεί το Institute of Advance Studies στο Princton, ΗΠΑ για ένα χρόνο. Επίσης κλήθηκε να συμμετάσχει στο Διεθνές Συνέδριο Μαθηματικών στο Πανεπιστήμιο του Χάρβαρντ, ως εκπρόσωπος του University of Madras. Έτσι ξεκίνησε για τις ΗΠΑ αεροπορικώς το 1950, αλλά λόγω της συντριβής του αεροσκάφους κοντά στο Κάιρο στις 31 Αυγούστου 1950 η Ινδική Κοινότητα έχασε έναν από τους πιο μεγάλους μαθηματικούς της.[33]

### Πρώτοι Αριθμοί Pillai

Ένας πρώτος αριθμός $p$ ονομάζεται **(πρώτος) αριθμός Pillai** [33], [6] αν υπάρχει ένας αριθμός n ο οποίος ικανοποιεί τις εξής ιδιότητες:

i) Ο n! είναι κατά ένα μικρότερος από κάποιο πολλαπλάσιο του p.
ii) Ο p δεν είναι κατά ένα μεγαλύτερος από κάποιο πολλαπλάσιο του n.

Για παράδειγμα, ο αριθμός 23 είναι αριθμός Pillai διότι, για n=4 έχουμε ότι

i) 4! = 24 = 23 + 1
ii) Τα πολλαπλάσια του 4 είναι 4,8,12,16,20,24 και για κανένα από αυτά δεν είναι το 23 κατά ένα μεγαλύτερο.

Με άλλα λόγια ένας πρώτος αριθμός p ονομάζεται αριθμός Pillai αν υπάρχει αριθμός n για τον οποίο ισχύει ότι

$$n! \equiv -1 (mod\ p) \text{ και } p \not\equiv 1 (mod\ n).$$

Ορισμένοι από τους πρώτους αριθμούς Pillai είναι οι εξής:

*23,29,59,61,67,71,79,83,109,137,139,149,193,227,*
*233,239,251,257,269,271,277,293,307,311,317,359,*
*379,383,389,397,401,419,431,449,461,463,467,479,*
*499,503,521,557,563,569,571,577,593,599,601,607*

## 2.4. PROTH

Ο **François Proth** (1852–1879) ήταν αγρότης και αυτοδίδακτος μαθηματικός. Πέθανε σε ηλικία είκοσι επτά ετών, περνώντας ολόκληρη τη ζωή του στο χωριό Vaux-Devant-Damloup κοντά στη Verdun. [5]

### Πρώτοι αριθμοί Proth

Ένας πρώτος αριθμός p ονομάζεται **(πρώτος) αριθμός Proth**, αν είναι της μορφής

$$\mathrm{p} = k \cdot 2^n + 1$$

όπου $k$ περιττός αριθμός, $n$ ένας θετικός ακέραιος αριθμός και $2^n > k$ .

Για παράδειγμα, το 13 είναι πρώτος αριθμός Proth, διότι

$$13 = 3 \cdot 2^2 + 1$$

και ισχύει ότι

$$2^2 > 3$$

Ομοίως, και το 41 είναι πρώτος αριθμός Proth, διότι

$$41 = 5 \cdot 2^4 + 1$$

και ισχύει ότι

$$2^4 > 5$$

Το 19 δεν είναι πρώτος αριθμός Proth, διότι

$$19 = 9 \cdot 2^1 + 1$$

αλλά δεν ισχύει ότι

$$2^1 > 9$$

Ένα κριτήριο για την εύρεση των πρώτων αριθμών Proth δίδεται στην επόμενη πρόταση.

### Θεώρημα Proth

Ένας αριθμός της μορφής $\mathrm{p} = k \cdot 2^n + 1$ είναι πρώτος αριθμός αν και μόνο αν υπάρχει αριθμός a τέτοιος ώστε

$$a^{(N-1)/2} \equiv -1 \ (mod\ N)$$ . [40]

Μερικοί από τους πρώτους αριθμούς Proth είναι οι εξής:
3, 5, 13, 17, 41, 97, 113, 193, 241, 257, 353, 449, 577, 641, 673, 769, 929, 1153.

Ο μεγαλύτερος γνωστός πρώτος αριθμός Proth, μέχρι σήμερα, είναι ο

$$19249 \cdot 2^{13018586} + 1,$$

ο οποίος βρέθηκε από το λογισμικό Seventeen or Bust. Έχει 3918990 ψηφία και είναι ο μεγαλύτερος γνωστός πρώτος αριθμός που δεν είναι πρώτος αριθμός Mersenne.[40]

Στο επόμενο πίνακα δίδονται μερικές από τις τιμές των n και k έτσι ώστε οι αριθμοί $\mathrm{p} = k \cdot 2^n + 1$ να είναι πρώτοι αριθμοί Proth. [39]

| ***k*** | ***Sloane*** | ***values of n for which $k \cdot 2^n + 1$ is prime*** |
|---|---|---|
| 1 | | 1, 2, 4, 8, 16, ... |
| 3 | A002253 | 1, 2, 5, 6, 8, 12, 18, 30, 36, 41, 66, ... |
| 5 | A002254 | 1, 3, 7, 13, 15, 25, 39, 55, 75, 85, 127, 1947, ... |
| 7 | A032353 | 2, 4, 6, 14, 20, 26, 50, 52, 92, 120, ... |
| 9 | A002256 | 1, 2, 3, 6, 7, 11, 14, 17, 33, 42, 43, 63, ... |

Ένα από τα δημοφιλέστερα προγράμματα εύρεσης πρώτων αριθμών στο διαδίκτυο είναι το πρόγραμμα "Proth.exe" που δημιουργήθηκε από τον Yves Gallot το 1997, για να βρει τους μεγαλύτερους παράγοντες των αριθμών Fermat που είναι της μορφής $k \cdot 2^n + 1$ . Όπως, επίσης και τους αριθμούς της μορφής $k \cdot 2^n - 1$ .

Το 1997, ο Carlos Rivera χρησιμοποίησε αυτό το πρόγραμμα για να βρει τον μεγαλύτερο γνωστό μη-Meresenne πρώτο αριθμό:

$$9183 \cdot 2^{262112} + 1.$$

Επίσης, το 1998, ο Chip Kerchner βρήκε, με τη βοήθεια αυτού του προγράμματος, τον τότε μεγαλύτερο γνωστό «Sophie Germain πρώτο αριθμό»

$$92305 \cdot 2^{16998} + 1.$$ [5]

## 2.5. STERN

Ο **Moritz Abraham Stern** (29 Ιουνίου 1807 – 30 Ιανουαρίου 1894) ήταν ο πρώτος εβραίος τακτικός καθηγητής (Ordinarius) σε Γερμανικό Πανεπιστήμιο.

Ο Stern μαζί με τον Gauss είχαν μαθητή τον Bernhard Riemann. Ο Stern βοήθησε επίσης τον Ferdinand Eisenstein στη διατύπωση μιας απόδειξης του θεωρήματος της τετραγωνικής αντιστροφής. Ο Stern ασχολήθηκε με προβλήματα που αφορούσαν την αναπαράσταση αριθμών – πρώτων ή μη - με τη μορφή αθροισμάτων που έχουν συγκεκριμένες ιδιότητες.

Είναι γνωστός για τη ακολουθία

$$1, 2, 1, 3, 2, 3, 1, 4, \dots ,$$

η οποία ονομάζεται διατομική ακολουθία του Stern και μετρά το πλήθος των διαφορετικών τρόπων που είναι δυνατόν να εκφραστεί ένας αριθμός ως άθροισμα δυνάμεων του δύο, χωρίς μια δύναμη να έχει χρησιμοποιηθεί πάνω από δύο φορές.

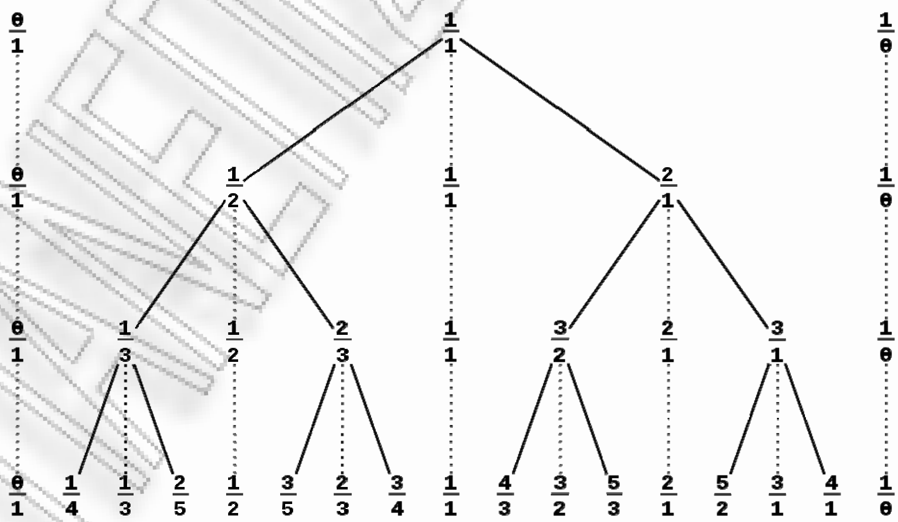
Για παράδειγμα, ο αριθμός 6 γράφεται ως άθροισμα αυτής της μορφής με τους εξής τρεις τρόπους:

$$6 = 2^2 + 2^1$$
$$6 = 2^2 + 2^0 + 2^0$$
$$6 = 2^1 + 2^1 + 2^0 + 2^0$$

ενώ ο αριθμός 7 γράφεται ως άθροισμα κατά μοναδικό τρόπο:

$$7 = 2^2 + 2^1 + 2^0.$$

Ο Stern είναι επίσης γνωστός για το δέντρο Stern–Brocot




του οποίου τα φύλλα αναπαριστούν όλους τους θετικούς ρητούς αριθμούς.[41]

## Πρώτοι αριθμοί Stern

Ένας πρώτος αριθμός p ονομάζεται **(πρώτος) αριθμός Stern** αν δεν γράφεται στη μορφή $q + 2a^2$ όπου $q$ είναι πρώτος αριθμός και $a > 0$, με άλλα λόγια ένας πρώτος αριθμός p είναι αριθμός Stern όταν η διαφορά $p - 2a^2$ δεν είναι πρώτος αριθμός για όλα τα $a > 0$ όπου $p > 2a^2$.[5]

Για παράδειγμα, ο πρώτος αριθμός 137 είναι αριθμός Stern διότι για κάθε α από 1 έως 8 έχουμε ότι

$137 - 2 \cdot 1^2 = 135$, το οποίο δεν είναι πρώτος αριθμός
$137 - 2 \cdot 2^2 = 129$, το οποίο δεν είναι πρώτος αριθμός
$137 - 2 \cdot 3^2 = 119$, το οποίο δεν είναι πρώτος αριθμός
$137 - 2 \cdot 4^2 = 105$, το οποίο δεν είναι πρώτος αριθμός
$137 - 2 \cdot 5^2 = 87$, το οποίο δεν είναι πρώτος αριθμός
$137 - 2 \cdot 6^2 = 65$, το οποίο δεν είναι πρώτος αριθμός
$137 - 2 \cdot 7^2 = 39$, το οποίο δεν είναι πρώτος αριθμός
$137 - 2 \cdot 8^2 = 9$, το οποίο δεν είναι πρώτος αριθμός

Αντίθετα, το 79 δεν είναι πρώτος αριθμός Stern διότι ενώ για α=1 το 79 ικανοποιεί την ιδιότητα των αριθμών Stern αφού

$79 - 2 \cdot 1^2 = 77$, το οποίο δεν είναι πρώτος αριθμός

για α=2 έχουμε ότι

$79 - 2 \cdot 2^2 = 71$, το οποίο είναι πρώτος αριθμός

Οι μόνοι γνωστοί πρώτοι αριθμοί Stern είναι οι εξής:

2, 3, 17, 137, 227, 977, 1187, 1493.

Ο Jud McCranie έχει επιβεβαιώσει ότι αυτοί είναι οι μόνοι πρώτοι αριθμοί Stern ανάμεσα στους πρώτους 100000 πρώτους αριθμούς. Πιθανόν, να μην υπάρχουν άλλοι αριθμοί Stern.

Ο λόγος είναι ότι οι πρώτοι αριθμοί έχουν συνήθως περισσότερους από ένα τρόπους να γραφούν στην μορφή $q + 2a^2$, όπου q πρώτος αριθμός και $a > 0$.

Για παράδειγμα ο πρώτος αριθμός 79, που δεν είναι αριθμός Stern, γράφεται ως εξής:

$$79 = 71 + 2 \cdot 2^2$$
$$79 = 61 + 2 \cdot 3^2$$
$$79 = 47 + 2 \cdot 4^2$$
$$79 = 29 + 2 \cdot 5^2$$
$$79 = 7 + 2 \cdot 6^2$$

Ο Leonhard Euler παρατήρησε πως όσο οι πρώτοι αριθμοί μεγαλώνουν τόσο αυξάνει το πλήθος των τρόπων που μπορούν να γραφούν στην μορφή $q + 2a^2$. Επιπλέον, ο Christian Goldbach εικάζει σε μια επιστολή προς τον Leonhard Euler ότι κάθε περιττός ακέραιος αριθμός είναι της μορφής $q + 2a^2$ με το $a \geq 0$. Επιπρόσθετα, ο Laurent Hodges θεωρεί ότι ίσως ο Stern έδειξε ενδιαφέρον στο πρόβλημα αφού διάβασε ένα μέρος της αλληλογραφίας του Goldbach και εκείνη την περίοδο το 1 εθεωρείτο πρώτος αριθμός, οπότε το 3 δεν θεωρούνταν πρώτος αριθμός Stern διότι μπορεί να εκφραστεί με τη μορφή $1 + 2 \cdot 1^2$.[42]

## 2.6. THABIT

Ο **Thabit Ibn Qurra Ibn Marwan Al-Sabi Al-Harrani** (836 – 18 Φεβρουαρίου 901) γεννήθηκε στη Harran (η οποία βρίσκεται στην σημερινή Τουρκία). Όπως δείχνει και το όνομά του ήταν βασικά μέλος της αίρεσης Sabian, αλλά ο μεγάλος Μουσουλμάνος μαθηματικός Muhammad Ibn Musa Ibn Shakir, εντυπωσιάστηκε από την γλωσσομάθειά του (γνώριζε τα Συριακά, ως μητρική γλώσσα, άπταιστα Ελληνικά και Αραβικά) και συνειδητοποιώντας τις προοπτικές του για μια επιστημονική σταδιοδρομία, τον επέλεξε να γίνει μέλος της επιστημονικής ομάδας στη Βαγδάτη, την οποία χρηματοδοτούσαν οι Χαλίφηδες Abbasid. Εκεί σπούδασε, υπό την επίβλεψη των διάσημων αδερφών Banu Musa. Ο Thabit συνείσφερε σε διάφορους κλάδους της επιστήμης, ιδιαίτερα στα μαθηματικά, την αστρονομία και τη μηχανική. Επιπλέον, μετέφρασε ένα μεγάλο αριθμό έργων από τα Ελληνικά στα Αραβικά.[43]

Ο Thabit γενίκευσε το Πυθαγόρειο θεώρημα σε ένα αυθαίρετο τρίγωνο (όπως έκανε και ο Πάππος). Ασχολήθηκε επίσης με τις παραβολές, την τριχοτόμηση γωνίας και τα μαγικά τετράγωνα. Επίσης, υπολόγισε το ολοκλήρωμα $\sqrt{x}$ φράσσοντας, όπως και ο Αρχιμήδης, μεταξύ δύο αθροισμάτων και ακολουθώντας την μέθοδο της εξάντλησης..[44]

Επιπρόσθετα, συνέχισε τη δουλειά των αδερφών Baru Musa και αργότερα ο γιος του και ο εγγονός του συνέχισαν την παράδοση ως μέλη της ομάδας. Τα πρώτα του βιβλία καθώς επίσης και οι μεταφράσεις τους, που ολοκληρώθηκαν στον 9ο αιώνα, άσκησαν μια θετική επιρροή στην ανάπτυξη της μετέπειτα επιστημονικής έρευνας.[43]

### Πρώτοι αριθμοί Thabit

Ένας πρώτος αριθμός p ονομάζεται **(πρώτος) αριθμός Thabit** (μερικές φορές αναφέρεται και ως **321 πρώτος αριθμός**) αν είναι της μορφής

$$p = 3 \cdot 2^n - 1.$$

Για παράδειγμα, ο πρώτος αριθμός 47 είναι αριθμός Thabit, αφού γράφεται στη μορφή

$$47 = 3 \cdot 2^4 - 1$$

Μερικοί από τους πρώτους αριθμούς Thabit είναι οι εξής:

2, 5, 11, 23, 47,191, 383, 6143, 786431, 51539607551, 824633720831..

Είναι φανερό ότι η ακολουθία των αριθμών Thabit αυξάνει ραγδαία. Υπάρχει ένα κατανεμημένο πρόγραμμα, το λεγόμενο 321 project, το οποίο είναι αφιερωμένο στην αναζήτηση μεγάλων πρώτων αριθμών Thabit. Ο μεγαλύτερος γνωστός αριθμός Thabit είναι ο αριθμός

$$3 \cdot 2^{4235414} - 1$$

ο οποίος έχει 1274988 ψηφία.

Παρακάτω δίδονται όλες οι γνωστές τιμές του εκθέτη n για τους οποίους ο αριθμός $3 \cdot 2^n - 1$ είναι αριθμός Thabit:

0, 1, 2, 3, 4, 6, 7, 11, 18, 34, 38, 43, 55, 64, 76, 94, 103, 143, 206, 216, 306, 324, 391, 458, 470, 827, 1274, 3276, 4204, 5134, 7559, 12676, 14898, 18123, 18819, 25690, 26459, 41628, 51387, 71783, 80330, 85687, 88171, 97063, 123630, 155930, 164987, 234760, 414840, 584995, 702038, 727699, 992700, 1201046, 1232255, 2312734, 3136255, 4235414. [45]

Δύο αριθμοί α και β ονομάζονται **φίλοι** ή **φιλικοί** αριθμοί αν το άθροισμα των γνήσιων διαιρετών του α ισούται με β και το άθροισμα των διαιρετών του β ισούται με α.

Για παράδειγμα, οι αριθμοί 220 και 284 είναι φίλοι αριθμοί, διότι οι γνήσιοι διαιρέτες του 220 είναι οι:

1,2,4,5,10,11,20,22,44,55,110

και ισχύει ότι

1+2+4+5+10+11+20+22+44+55+110=284

ενώ, οι γνήσιοι διαιρέτες του 284 είναι οι

1,2,4,71,142

και ισχύει ότι

1+2+4+71+142=220.

Οι αριθμοί 220 και 284 είναι οι μικρότεροι φίλοι αριθμοί.

Τα ζεύγη των φίλων αριθμών τα οποία έχουν στοιχεία μικρότερα από το 10000 είναι τα εξής:

(220,284), (1184,1210), (2620,2924), (5020,5564), (6232,6368)

Ο Thabit βρήκε ένα κανόνα, ο οποίος ονομάζεται **κανόνας του Thabit**, για την κατασκευή ζευγών φίλων αριθμών.

Έστω ότι για κάποιο αριθμό $n \geq 2$ ισχύει ότι οι αριθμοί

$$h = 3 \cdot 2^n - 1$$
$$t = 3 \cdot 2^{n-1} - 1$$
$$s = 9 \cdot 2^{2n-1} - 1$$

είναι όλοι πρώτοι αριθμοί. Τότε το ζεύγος

$$(2^n ht, 2^n s)$$

είναι φίλοι αριθμοί

Οι γνωστές τιμές του n για τις οποίες εφαρμόζεται, ο κανόνας του Thabit είναι για n=2,4 και 7.

Πράγματι, για n=2, έχουμε ότι οι αριθμοί

$$h = 3 \cdot 2^2 - 1 = 11$$
$$t = 3 \cdot 2^{2-1} - 1 = 5$$
$$s = 9 \cdot 2^{2 \cdot 2-1} - 1 = 71$$

είναι όλοι πρώτοι αριθμοί, οπότε από τον κανόνα του Thabit, προκύπτει ότι το ζεύγος των φίλων αριθμών

$$(2^2 \cdot 11 \cdot 5, 2^2 \cdot 71) = (220{,}284)$$

Ομοίως, για n=4, προκύπτει το ζεύγος των φίλων αριθμών

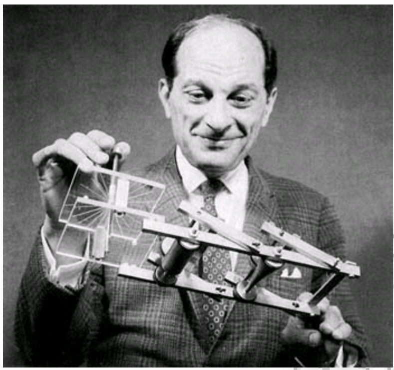
$$(2^4 \cdot 47 \cdot 23, 2^4 \cdot 1151) = (17296{,}18416)$$

Τέλος, για n=7, προκύπτει το ζεύγος των φίλων αριθμών

$$(2^7 \cdot 383 \cdot 191, 2^7 \cdot 73727) = (9363584{,}9437056)$$

Ο κανόνας του Thabit, ανακαλύφθηκε εκ νέου, από τον Fermat το 1636 και από τον Descartes το 1638, και γενικεύθηκε από τον Euler.[46]

## 2.7. ULAM



Ο **Stanislaw Marcin Ulam** (13 Απριλίου 1909 – 13 Μαΐου 1984) γεννήθηκε στο Lemberg της Πολωνίας. Ήταν παιδί-θαύμα. Μόλις δώδεκα χρονών ξεκίνησε να διαβάζει την θεωρία της σχετικότητας του Einstein. Αυτό όμως απαιτούσε την κατανόηση ανώτερων μαθηματικών από αυτά που διδασκόταν στο σχολείο, έτσι σύντομα άρχισε να μελετά μαθηματικά από βιβλία που ξεπερνούσαν τα σχολικά μαθηματικά. Το 1927 γράφτηκε στο Polytechnic Institute στην Lvov.

Στο πρώτο έτος είχε δάσκαλο τον νεοδιορισμένο Kazimir Kuratowski, υπό την επίβλεψη του οποίου, το 1933, ολοκλήρωσε την διδακτορική του διατριβή, Το θέμα της διατριβής του αφορούσε ένα πρόβλημα της θεωρίας μέτρου το οποίο έθεσε ο Lebesgue. Επίσης, την ίδια περίοδο ο Ulam συνεργάστηκε με Stephen Banach, τον οποίο θεωρούσε και μέντορά του.

Το 1940 ο Ulam διορίστηκε ως βοηθός καθηγητής στο Πανεπιστήμιο του Wisconsin. Εκείνο το έτος ο von Neumann τον προσκάλεσε για να αναλάβει κάποια πολύ σημαντική πολεμική εργασία. Εργάστηκε πάνω στη βόμβα υδρογόνου στο εθνικό εργαστήριο του Los Alamos στο Νέο Μεξικό. Ο Ulam, μαζί με τον J.C.Everett, πρότεινε επίσης το «σχέδιο Orion» για την πυρηνική προώθηση των διαστημικών οχημάτων.

Ο Ulam θεωρείται ένας από τους επινοητές της μεθόδου Monte Carlo, η οποία βρίσκει λύσεις σε μαθηματικά προβλήματα χρησιμοποιώντας μια μέθοδο στατιστικής δειγματοληψίας με τυχαίους αριθμούς.

Ο Ulam ενδιαφέρθηκε και για την προβολή των μαθηματικών και στους μη ειδικούς. Χαρακτηριστικά είναι τα βιβλία του A collection of mathematical problems (1960) και η αυτοβιογραφία του Adventures of a Mathematician (1976). [47]

Το 1963, ο Ulam παρατήρησε μια κανονικότητα στην κατανομή κάποιων από τους πρώτους αριθμούς:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | ← | 61 | 60 | 59 | 58 | 57 | |
| | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 56 | |
| | 38 | 17 | 16 | 15 | 14 | 13 | 30 | 55 | |
| | 39 | 18 | 5 | 4 | 3 | 12 | 29 | 54 | |
| | 40 | 19 | 6 | 1 | 2 | 11 | 28 | 53 | |
| | 41 | 20 | 7 | 8 | 9 | 10 | 27 | 52 | |
| | 42 | 21 | 22 | 23 | 24 | 25 | 26 | 51 | |
| | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | |
| | | | | | | | | | |

**Εικόνα 1**

Σχεδιάζοντας, το λεγόμενο **σπιράλ του Ulam**, πρόσεξε ότι κάποιοι πρώτοι αριθμοί περιέχονται σε τετράγωνα που βρίσκονται πάνω σε διαγώνιες γραμμές. Ο λόγος είναι ότι οι αριθμοί που περιέχονται σε τετράγωνα που βρίσκονται πάνω σε ευθείες γραμμές έχουν διαφορές που αυξάνονται γραμμικά. Επομένως, υπάρχουν πολυώνυμα δευτέρου βαθμού των οποίων πολλές από τις τιμές είναι πρώτοι αριθμοί.

Η ανακάλυψη αυτής της ιδιότητας, όπως παραδέχονται και οι Ulam, Stein και Wells, στην εργασία τους στο American Mathematical Monthly το 1964, οφείλεται στην οπτική ικανότητα του ανθρώπινου εγκεφάλου να ανακαλύπτει αμέσως τέτοιες γραμμές και να παρατηρεί πολλές άλλες ιδιαιτερότητες της διανομής των σημείων σε δύο διαστάσεις.

Για παράδειγμα, στη σπειροειδή μορφής της Εικόνα 1, στα τετράγωνα της κυρίας διαγωνίου περιέχονται οι τιμές της ακολουθίας

$$n^2 + n + 1.$$

Οι ακολουθίες της μορφής

$$n^2 + n + a.$$

ονομάζονται τετραγωνικές μορφές του Euler.

Στην Εικόνα 2, το σχεδιάγραμμα άρχιζε από το 41 και στα τετράγωνα της κυρίας διαγωνίου περιέχονται οι τιμές της ακολουθίας

$$n^2 + n + 41.$$

Παρατηρούμε ότι και στις δύο περιπτώσεις πολλά από τα τετράγωνα των κύριων διαγωνίων περιέχουν πρώτους αριθμούς. Για παράδειγμα, από τους πρώτοι 2.398 όρους που παράγονται από τη τετράγωνη μορφή $x^2 + x + 41$ οι μισοί είναι πρώτοι αριθμοί.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | 77 | 76 | 75 | 74 | 73 | 72 | **71** | |
| | 78 | 57 | 56 | 55 | 54 | **53** | 70 | |
| | 79 | 58 | 45 | 44 | **43** | 52 | 69 | |
| | 80 | 59 | 46 | **41** | 42 | 51 | 68 | |
| | 81 | 60 | **47** | 48 | 49 | 50 | 67 | |
| | 82 | **61** | 62 | 63 | 64 | 65 | 66 | |
| | **83** | → | | | | | | |

**Εικόνα 2**

Ένα δύσκολο ερώτημα είναι γιατί μερικές τετραγωνικές μορφές παράγουν ένα τέτοιο μεγάλο μέρος πρώτων αριθμών.

Για παράδειγμα, ο Ulam, ελέγχοντας όλους τους όρους της τετράγωνη μορφή $n^2 + n + 41$, για τιμές μικρότερες του 10.000.000 υπολόγισε ότι η αναλογία πρώτων αριθμών προς το συνολικό πλήθος ισούται με 0,475

Επίσης, για τη τετραγωνική μορφή

$$4n^2 + 170n + 1847,$$

η αναλογία πρώτων αριθμών είναι 0.466, ενώ για την τετραγωνική μορφή

$$4n^2 + 4n + 59,$$

είναι 0.437.

Αντίθετα, για την τετραγωνική μορφή

$$2n^2 + 4n + 117$$

μόνο το 5% των όρων της είναι πρώτοι αριθμοί.[5]

## 2.8. WAGSTAFF

O **Samuel Standfield Wagstaff, Jr.** (ssw@cs.purdue.edu) είναι Αμερικανός επιστήμονας που ασχολείται με τα μαθηματικά και την πληροφορικής. Τα ερευνητικά ενδιαφέροντά του ανήκουν στους τομείς των κρυπτογραφικών συστημάτων, του παράλληλου υπολογισμού, και της ανάλυσης των αλγορίθμων. Είναι Καθηγητής της πληροφορικής και των μαθηματικών στο πανεπιστήμιο Purdue.[52]

Μαζί με τον J.W. Smith του Πανεπιστημίου της Γεωργίας έχουν δημιουργήσει έναν ειδικό παράλληλο επεξεργαστή για την παραγοντοποίηση μεγάλων ακεραίων αριθμών.

Έχει συγγράψει πάνω από 50 ερευνητικές εργασίες και 2 βιβλία. Πιο συγκεκριμένα κάποια από τα συγγράμματά του είναι : Factorizations of $b^n \pm 1$, b = 2, 3, 5, 6, 7, 10, 11, 12 up to high powers, Contemporary Mathematics series, v. 22, Third edition, American Mathematical Society, 2002 (με τους John Brillhart, D. H. Lehmer, J. L. Selfridge και Bryant Tuckerman) (http://www.ams.org/online_bks/conm22), Cryptanalysis of Number Theoretic Ciphers, CRC Press, 2002, and Sums of Squares of Integers, CRC Press, 2005 (με τον Carlos Moreno).[51]

### Πρώτοι αριθμοί Wagstaff

Ένας πρώτος αριθμός p ονομάζεται **(πρώτος) αριθμός Wagstaff** αν ο p είναι της μορφής

$$p = (2^q + 1)/3$$

όπου $q$ είναι πρώτος αριθμός.

Μερικοί από τους πρώτους αριθμούς Wagstaff είναι οι εξής:

3, 11, 43, 683, 2731, 43691, 174763, 2796203, 715827883, 2932031007403,

Είναι φανερό ότι η ακολουθία των αριθμών Wagstaff αυξάνει ραγδαία. Όλες οι γνωστές τιμές του q για τις οποίες ο αριθμός $p = (2^q + 1)/3$ είναι αριθμός Wagstaff είναι οι εξής:

3, 5, 7, 11, 13, 17, 19, 23, 31, 43, 61, 79, 101, 127, 167, 191, 199, 313, 347, 701, 1709, 2617, 3539, 5807, 10501, 10691, 11279, 12391, 14479, 42737

Ο μεγαλύτερος γνωστός πρώτος αριθμός Wagstaff , $(2^{42737} + 1)/3$ έχει 12865 ψηφία.

Επίσης εικάζεται ότι και οι επόμενες τιμές του q δίνουν αριθμούς Wagstaf:

83339, 95369, 117239, 127031, 138937, 141079, 267017, 269987, 374321, 986191, 4031399. [50]

## 2.9. WALL – SUN – SUN

-Zhi Hong Sun-

-Zhi Wei Sun-

Ο **Donald Dines Wall (13 Αυγούστου 1921-28 Νοεμβρίου 2000)** γεννήθηκε στη πόλη του Κάνσας το 1921. Το 1938 γράφτηκε στο UCLA (Πανεπιστήμιο της Καλιφόρνια) και αποφοίτησε από αυτό το 1944 με πτυχίο στα Μαθηματικά. Στο ενδιάμεσο διάστημα των σπουδών του, το 1940, υποβλήθηκε σε χειρουργική επέμβαση αφαίρεσης όγκου του εγκεφάλου, η οποία στέφθηκε με επιτυχία.

Το 1946 έλαβε το μεταπτυχιακό τίτλο στη Μαθηματική Στατιστική από το Πανεπιστήμιο UCLA, ενώ το 1947 επιστρέφοντας στο πανεπιστήμιο του Χάρβαρντ άρχισε να μελετά τη Θεωρία Αριθμών. Ακολούθως, το 1949 του απονεμηθεί ο διδακτορικό τίτλος από το Πανεπιστήμιο του Μπέρκλεϋ για τη διατριβή του πάνω στους κανονικούς αριθμούς.

Μετά τις σπουδές του, εργαζόμενος ως διδάκτωρ υπολογιστικών μαθηματικών στην αεροπορική βάση του πολεμικού ναυτικού στο Point Mugu, όπου οι υπολογιστές είχαν αναπτυχθεί ώστε να υπολογίζουν τις συντεταγμένες πυραύλων, προσέλκυσε το ενδιαφέρον της εταιρείας IBM, στην οποία και εργάστηκε ως συντονιστής του εκπαιδευτικού προγράμματος της εταιρείας. Συνέχισε να εργάζεται στην IBM έως τη συνταξιοδότηση του το 1982.

Ορισμένες από τις εργασίες του είναι οι εξής: The accuracy of the root-squaring method for solving equations ( P.G. Hoel and D.D. Wall, 1957), Normal numbers (Wall, Ph.D. thesis, 1949) Univ. California, Berkeley, 1949 D.D. Wall, The order of an iteration formula, Math. Tables Aids Comput. 10 (1956) 167-168. D.D. Wall, Fibonacci series modulo m, Amer. Math. Monthly 67 (1960) 525-532.[53]

Ο **Zhi Hong Sun (16 Οκτωβρίου 1965 - ...)** είναι Κινέζος μαθηματικός με ερευνητικά ενδιαφέροντα που εμπίπτουν στους τομείς της Θεωρίας Αριθμών, Συνδυαστικής ανάλυσης, και στα ακρότατα όρια της θεωρίας γραφικών παραστάσεων, και στις ειδικές συναρτήσεις..

Ορισμένες από τις εργασίες του είναι οι εξής: «Fibonacci numbers and Fermat's last theorem» (Z.H.Sun and Z.W.Sun, Acta Arithmetica 60(1992),no.4, 371-388), «Congruences for Bernoulli numbers and Bernoulli polynomials» (Z.H.Sun, Discrete Mathematics 163(1997),no.1-3,153-163), «Five congruences for primes» (Z.H.Sun, Fibonacci Quart.40(2002),no.4,345-351), «Values of Lucas sequences modulo primes» (Z.H.Sun, Rocky Mountain J. Math. 33(2003),no.3,1123-1145), «Cubic and quartic congruences modulo a prime» (Z.H.Sun, J. Number Theory 102(2003),no.1, 41-89) και «Primality tests for numbers of the form» (Z.H.Sun, Fibonacci Quart. 44(2006), no.2, 121-130).[54]

Ο **Zhi Wei Sun (16 Οκτωβρίου 1965 - ...)** είναι Κινέζος μαθηματικός, δίδυμος αδελφός του Zhi Hong Sun, με ερευνητικά ενδιαφέροντα που εμπίπτουν στους τομείς της Θεωρίας αριθμών, της Συνδυαστικής ανάλυσης και της Μαθηματικής λογικής. Είναι διευθυντής σύνταξης του Journal of Combinatorics and Number Theory.

Ορισμένες από τις εργασίες του είναι οι εξής: «A congruence for primes» ( Proc. Amer. Math. Soc., 123(1995), no.5, 1341—1346), «A note on the Erdos-Ginzburg-Ziv theorem» (Sun Z. W. και Liu J. X., Nanjing Univ. J. Natur. Sci., 37(2001), no.4, 473—476), «An extension of Lucas' theorem» (Sun Z. W. και Hu H., Proc. Amer. Math. Soc., 129(2001), no.12, 3471—3478), «Some identities for Bernoulli and Euler polynomials» (Sun Z.W. et al., Fibonacci Quart. 42(2004), no.4, 295—299) και «Mixed sums of primes and other terms, in: Additive Number Theory» (Sun Z.W., Mathematical Sunject Classifications, Springer (2000)). [55]

## Wall-Sun-Sun Πρώτοι Αριθμοί

Ένα από τα διασημότερα προβλήματα της θεωρίας αριθμών είναι το λεγόμενο τελευταίο πρόβλημα του Fermat ή τελευταίο θεώρημα του Fermat.

Ο Fermat ήταν δικηγόρος στο επάγγελμα. Αλλά, όταν έπεσε στα χέρια του το βιβλίο των Αριθμητικών του Διόφαντου εντυπωσιάστηκε τόσο από τα μαθηματικά, ώστε αφιέρωσε μεγάλο χρόνο της ζωής του ως ερασιτέχνης μαθηματικός.

Ο Fermat διάβασε στο βιβλίο των Αριθμητικών για τις πυθαγόρειες τριάδες, δηλαδή για ακέραιους αριθμούς που ικανοποιούν την εξίσωση

$$\alpha^2 + b^2 = c^2$$

όπως για παράδειγμα την τριάδα (3,4,5) για την οποία ισχύει ότι $3^2 + 4^2 = 5^2$.

Αναρωτήθηκε, αν υπάρχουν ακέραιες τριάδες που ικανοποιούν εξισώσεις της μορφής

$$\alpha^n + b^n = c^n$$

όπου $n > 2$. Στο περιθώριο, του αντίτυπου του βιβλίου σημείωσε ότι είχε μια απόδειξη ότι δεν υπάρχουν τέτοιες τριάδες αλλά ήταν πολύ μεγάλη για να χωρέσει εκεί.

Με το πρόβλημα αυτό, που όπως αποδείχθηκε ήταν πολύ δύσκολο, ασχολήθηκαν πολλοί διάσημοι μαθηματικοί και παρέμεινε άλυτο πάνω από 300 χρόνια μέχρις ότου το 1992 ο Andrew Wiles έδωσε την πρώτη απόδειξη ότι δεν υπάρχουν λύσεις.

Πριν από τον Willes, οι Zhi Hong Sun και Zhi Wei Sun, βασιζόμενοι στις εργασίες του D.D.Wall, απέδειξαν μια πρόταση που συνδέει το τελευταίο θεώρημα του Fermat με την ύπαρξη κάποιων πρώτων αριθμών με συγκεκριμένες ιδιότητες.

Ένας πρώτος αριθμός $p > 5$ ονομάζεται **(πρώτος) αριθμός Wall-Sun-Sun** αν ικανοποιεί την εξής ιδιότητα:

$$p^2 \text{ διαιρεί το } u\big(p - (p|5)\big).$$

όπου $u(n)$ είναι ο n-οστός αριθμός Fibonacci και $(a|b)$ είναι το σύμβολο του Legendre (δηλαδή $(a|b) = 0$ αν ο b διαιρεί τον α, $(a|b) = 1$, αν υπάρχει λύση της εξίσωσης $x^2 \equiv a\, mod b$ και b δεν διαιρεί τον a, και τέλος $(a|b) = -1$, αν δεν υπάρχει λύση της εξίσωσης $x^2 \equiv a\, mod b$).

Οι Zhi Hong Sun και Zhi Wei Sun απέδειξαν ότι αν το τελευταίο θεώρημα του Fermat είναι ψευδές τότε ο αριθμός n για τον οποίο δεν ισχύει θα είναι πρώτος αριθμός Wall-Sun-Sun.[56]

# 3. ΒΙΒΛΙΟΓΡΑΦΙΑ

## ΒΙΒΛΙΑ


[1] J. Gudmundsson (ed), *Algorithm Theory – SWAT 2008, 11th Scandinavian Workshop on Algorithm Theory Gothenburg Sweden, July 2008, Proceedings*, Springer-Verlag, Berlin Heidelberg,2008.

[2] J. D. Louck, *Unitary Symmetry and Combinatorics*, World Scientific Publishing CO. PTE.LTD, 2008.

[3] A. Krasinski, *General Relativity and Graviation, (I. M. H. Etherington: A Brief History)*, Springer, Netherland, 2006.

[4] G. W. F. Drake (ed), *Springer Handbook of Atomic, Molecular, and Optical Physics*, Springer, 2006

[5] D. Wells, *Prime Numbers: the most mysterious figures in math,* John Wiley & Sons, 2005.

[6] R. K. Guy, *Problem Books in Mathematics-Unsolved Problems in Number Theory*, 3rd edition, Springer, 2004.

[7] R. Safani-Naini, J. Seberry (eds), *Information Security and Privacy, 8th Australian Conference, ACISP 2003, Wollongong, Australia, July 2003, Proceedings*, Springer-Verlag Heidelberg, New York, 2003.

[8] W. E. Clark, *Elementary Number Theory*, Department of Mathematics, University South Florida, 2003.

[9] J-P.Delehaye,Merveilleux nombres premiers-Voyage au coeur de l'arithmetique,Pour la science,Paris,2000.

[10] C.Clawson,Mathematical Mysteries: the beauty and Mystery of Mathematics, Plenum Press,New York,1996.

[11] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1996.

[12] P. Ribbenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.

[13] R. Crandall, C. Pomerance, *Prime Numbers - A computational Respective*, Springer, 2001.

[14] R. K. Guy, *Unsolved Problems in Number Theory*, 2nd edition, Springer, 1994.

[15] P. Ribenboim, *The Little Book of Big Primes*, Springer, 1991.

[16] P. J. Cameron*, London Mathematical Society – Lecture Note Series 152 – Oligomorphic Permutation Groups*, Cambridge University Press, 1990.

[17] A. Baker, *A Concise Introduction to the theory of Numbers*, Cambridge University Press, 1984.

[18] D. M. Burton, *Elementary Number Theory*, (revised printing), Allyn and Bacon INC, University of New Hampshire, 1980.

[19] G. H. Hardy and E. M. Wright (principal and vice, chancellor of the University of Aberdeen), *An Introduction to the Theory of Numbes*, 4th edition, Claredon Press, Oxford, 1960.


## ΑΡΘΡΑ


[20] C. K. Caldwell and Y. Cheng, Determining Mill's Constant and a Note on Honaker's Problem, *Journal of Integer Sequences*, **8** (2005), Article 05.4.1, 9pp.

[21] Canadian Journal of Mathematics, Vol. XV, No. I, Published for the Canandian Mathematical Congress, by the University of Torondo press, 1963.

[22] W. H. Mills, A prime-representing function, *Bull. Amer. Math. Soc.* **53** (1947), 604.

## ΙΣΤΟΣΕΛΙΔΕΣ

[23] http://mathworld.wolfram.com/MillsConstant.html
[24] http://mathworld.wolfram.com/PierpontPrime.html
[25] http://planetmath.org/
[26] http://primes.utm.edu/
[27] http://www.knowledgerush.com/kr/encyclopedia/Main_Page/
[28] http://www.amazines.com/
[29] http://encyclopedia.thefreedictionary.com/
[30] http://www.prothsearch.net/
[31] http://www.gap-system.org/~history/index.html
[32] http://www.numbertheory.org/ntw/N14.html#biographies
[33] http://www.mri.ernet.in/~thanga/sspillai/PILLAI.html
[34] http://primes.utm.edu/glossary/xpage/PillaiPrime.html
[35] http://genealogy.math.ndsu.nodak.edu
[36] http://www.ams.org/news?class_id=402
[37] http://mathworld.wolfram.com/PerrinPseudoprime.html
[38] http://en.wikipedia.org/wiki/Fran%C3%A7ois_Proth
[39] http://mathworld.wolfram.com/ProthPrime.html
[40] http://encyclopedia.thefreedictionary.com/Proth%27s+theorem
[41] http://en.wikipedia.org/wiki/Moritz_Abraham_Stern
[42] http://en.wikipedia.org/wiki/Stern_prime
[43] http://www.ummah.net/history/scholars/QURRA.html
[44] http://www-groups.dcs.st-and.ac.uk/~history/Printonly/Thabit.html
[45] http://mathworld.wolfram.com/ThabitibnKurrahNumber.html
[46] http://mathworld.wolfram.com/ThabitibnKurrahRule.html
[47] http://www-groups.dcs.st-and.ac.uk/~history/Printonly/Ulam.html
[48] http://mathworld.wolfram.com/UlamSequence.html
[49] http://mathworld.wolfram.com/WagstaffPrime.html
[50] http://primes.utm.edu/top20/page.php?id=67
[51] http://www.cs.purdue.edu/people/faculty/ssw/
[52] http://en.wikipedia.org/wiki/Samuel_S._Wagstaff_Jr.
[53] http://en.allexperts.com/e/d/d/d._d._wall.htm
[54] http://www.hytc.cn/xsjl/szh/
[55] http://math.nju.edu.cn/~zwsun/
[56] http://primes.utm.edu/glossary/page.php?sort=WallSunSunPrime
[57] http://mathworld.wolfram.com/Wall-Sun-SunPrime.html
[58] http://www.odec.ca/projects/2007/fras7j2/History.htm
[59] http://www.odec.ca/projects/2007/fras7j2/uses.htm
[60] http://www.odec.ca/projects/2007/fras7j2/patterns.htm
[61] http://mathworld.wolfram.com/PrimalityTest.html
[62] http://en.wikipedia.org/wiki/Pierpont_prime