



Ακαδημία Εμπορικού Ναυτικού Ασπροπύργου
Σχολή Μηχανικών

Πτυχιακή εργασία
Οι πρώτοι αριθμοί

PRIME NUMBERS									
A prime is a number whose only factors are 1 and the number itself. 0 and 1 are not prime, and 2 is the only even prime number. All numbers that are not prime are called composite.									
not prime	1x2	1x3	2x2 1x4	1x5	2x3 1x6	1x7	2x4 1x8	3x3 1x9	2x5 1x10
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Σπουδαστής: Κολοβός Φώτιος (ΑΜ 7884)

Επιβλέπων Καθηγητής: Στέφανος Ι. Καρναβάς, Μαθηματικός (Μ.Εδ.),
Επικουρος Καθηγητής

Ακαδημαϊκό έτος: 2019 – 2020

Ημερομηνία ανάθεσης: **10.06.2019**
 Ημερομηνία κατάθεσης: **....09.2019**
 Ημερομηνία εξέτασης: **.....09.2019**

A/A	Ονοματεπώνυμο	Χαρακτηρισμός	Υπογραφή
1	Στέφανος Ι. Καρναβάς Μαθηματικός (Μ.Εδ.) Επίκουρος Καθηγητής	Ιδιαίτερα ικανοποιητική	
2	Αντωνάτος Χαράλαμπος Ναυπηγός Μηχανολόγος Μηχανικός Καθηγητής		
3	Φραγκιαδάκης Νικόλαος Δρ. Ναυπηγός Μηχανολόγος Μηχανικός Αναπληρωτής Καθηγητής		
Τελικός χαρακτηρισμός			

Περιεχόμενα

1. Τί σημαίνει πρώτος αριθμός;	4
2. Πως ανακαλύπτουμε τους πρώτους αριθμούς	4
3. Οι πρώτοι αριθμοί, εφεύρεση ή ανακάλυψη;.....	5
4. Το κόσκινο του Ερατοσθένη.....	7
5. Πόσοι πρώτοι αριθμοί υπάρχουν;	7
6. Μεγάλα κενά.....	9
7. Δίδυμοι πρώτοι	10
8. Οι αριθμοί του Mersenne	12
9. Το μικρό θεώρημα του Fermat	12
10. Οι αριθμοί του Fermat	14
11. Η εικασία του Goldbach	14
12. Η πρώτη εικασία	15
13. Σε τι χρησιμεύουν οι πρώτοι αριθμοί;	18
14. Οι πρώτοι αριθμοί στην κρυπτογραφία	18
15. Μέγιστη ασφάλεια	20
16. Κατασκευή των πρώτων αριθμών	20
17. Πώς γνωρίζουμε αν ένας αριθμός είναι πρώτος;	22
Βιβλιογραφία	22

1. Τί σημαίνει πρώτος αριθμός;

Έστω ένας τυχαίος αριθμός, π.χ. το 12. Γνωρίζουμε ότι αυτός ο αριθμός μπορεί να εκφραστεί με διαφορετικούς τρόπους ως γινόμενο άλλων αριθμών π.χ. $12 = 2 \cdot 6$, $12 = 3 \cdot 4$, $12 = 2 \cdot 2 \cdot 4$. Στο εξής θα αναφερόμαστε σε αυτούς τους αριθμούς ως «παράγοντες» ή «γινόμενο». Έτσι, θα λέμε ότι το 3 είναι ένας παράγοντας του 12, όπως και ότι το 3 είναι διαιρέτης του 12. Διαιρέτης, είναι αυτός που διαιρεί, έτσι το 3 διαιρεί το 12. Κατά τον ίδιο τρόπο λέμε ότι το 5 είναι διαιρέτης του 20, διότι το 5 διαιρεί το 20. Λέγοντας ότι διαιρεί, θέλουμε να πούμε ότι αν κάνουμε την διαίρεση 20 δια 5, προκύπτει ένας φυσικός αριθμός, σε αυτήν την περίπτωση το 4, είναι ένα μηδενικό υπόλοιπο. Η λέξη παράγοντας, έχει σαφή σημασία. Προέρχεται από το ρήμα παράγω. Στην έκφραση $12 = 3 \cdot 4$, ο αριθμός 3 είναι παράγοντας διότι είναι ο αριθμός που επιτρέπει να «παραχθεί» ο αριθμός 12. Έτσι, όταν ρωτάμε ποιοι είναι οι διαιρέτες του 12 μπορούμε να απαντήσουμε ότι το 2, το 3, το 4 και το 6 είναι διαιρέτες του 12, καθώς το 12 όταν διαιρεθεί με οποιονδήποτε από αυτούς δίνει έναν ακριβή αριθμό.

Μεταξύ όλων των διαιρετών ενός αριθμού, πρέπει να συμπεριλαμβάνεται και το 1, επειδή όλοι οι αριθμοί διαιρούνται με την μονάδα και τον εαυτό τους. Για παράδειγμα, αν μας ρωτήσουν με ποιους αριθμούς διαιρείται το 18, θα απαντήσουμε ότι το 18 μπορεί να διαιρεθεί με το 1, το 2, το 3, το 6, το 9 και το 18. Ας υποθέσουμε ότι μας κάνουν την ίδια ερώτηση για τον αριθμό 7. Αν αναζητήσουμε πιθανούς διαιρέτες του 7 θα βρούμε ότι οι μόνοι αριθμοί με τους οποίους μπορεί να διαιρεθεί είναι το 1 και το ίδιο το 7. Κάτι παρόμοιο συμβαίνει και με αριθμούς όπως το 2, το 3, το 5, το 11 ή το 13. Αυτό συμβαίνει γιατί οι εν λόγω αριθμοί είναι «πρώτοι». Τώρα είμαστε σε θέση να δώσουμε έναν ακριβή ορισμό του τί σημαίνει «πρώτος αριθμός».

Πρώτος αριθμός είναι ένας αριθμός του οποίου οι μόνοι διαιρέτες είναι το 1 και ο εαυτός του. Σε αυτήν την μελέτη των φυσικών αριθμών, υπεισέλθαν οι πράξεις του πολλαπλασιασμού και της διαίρεσης ανάμεσά τους. Οδηγηθήκαμε στο συμπέρασμα ότι υπάρχουν κάποιοι ειδικοί αριθμοί και περιγράφοντάς τους όλους με έναν ορισμό, λειτουργήσαμε αφαιρετικά. Αφού απέκτησαν όνομα και μια χαρακτηριστική ιδιότητα, αποτελούν πλέον αντικείμενο μελέτης.

2. Πως ανακαλύπτουμε τους πρώτους αριθμούς

Για να κάνουμε ανάλυση των πρώτων παραγόντων, η μέθοδος που πρέπει να ακολουθήσουμε συνίσταται στο να τοποθετήσουμε τον υπό εξέταση αριθμό στα αριστερά μιας κάθετης γραμμής. Στη συνέχεια, εξετάζουμε αν ο αριθμός διαιρείται με 2, 3, 5, κλπ. δηλαδή, με πρώτους αριθμούς, αρχίζοντας από τον μικρότερο. Στην περίπτωση που είναι διαιρετός, τοποθετούμε το αποτέλεσμα της διαίρεσης στο αριστερό μέρος και αρχίζουμε ξανά με αυτόν τον αριθμό. Συνεχίζουμε την διαδικασία, μέχρι ο αριθμός στα αριστερά να είναι μονάδα. Τότε, στην στήλη στα δεξιά, εμφανίζονται οι πρώτοι αριθμοί που παραγοντοποιούν τον δοθέντα αριθμό.

120	2
60	2
30	2
15	3
5	5
1	

3. Οι πρώτοι αριθμοί, εφεύρεση ή ανακάλυψη;

Έχοντας ήδη εδραιώσει ένα σύστημα αρίθμησης, φαίνεται λογικό πως η πρώτη ιδιότητα που θα ανιχνευόταν σε έναν αριθμό θα ήταν αυτή του να είναι περιττός ή άρτιος, έννοια άμεση και ενστικτώδης. Το επόμενο βήμα, ήταν να εξεταστεί η παραγοντοποίηση αριθμών, κάτι που οδηγεί στη θέσπιση των κριτηρίων διαιρετότητας που διδάσκονται στα σχολεία στις μικρές ηλικίες. Με αυτό τον τρόπο, ένας πολιτισμός που έχει ορίσει το δικό του σύστημα αρίθμησης, διαθέτει μια συλλογή αριθμών που ελέγχονται από λίγες εύκολα προσδιορίσιμες ιδιότητες. Στους εν λόγω αριθμούς, δεν περιλαμβάνονται οι πρώτοι. Το μόνο που ήταν γνωστό για αυτούς με απόλυτη βεβαιότητα, είναι ότι δεν μπορούν να είναι άρτιοι, αφού σε μια τέτοια περίπτωση θα μπορούσαν να διαιρεθούν δια του δύο. Ούτε πρέπει να τους δούμε ως κάτι σπάνιο, καθώς ο **Ευκλείδης είχε αποδείξει ότι ήταν άπειροι**.

Επίσης δε γίνεται να υποτιμήσουμε την σπουδαιότητά τους, εφόσον το θεμελιώδες θεώρημα της Αριθμητικής τους έχει τοποθετήσει σε περίοπτη θέση στην πινακοθήκη των μαθηματικών. Συνεπώς, είχαν αποτελέσει από νωρίς αντικείμενο μελέτης. Όταν στις πειραματικές επιστήμες γίνεται λόγος για κάποιο αντικείμενο μελέτης, είναι σαφές ότι το εν λόγω αντικείμενο βρίσκεται κάπου εκεί έξω. Μπορεί να το έχουμε ανακαλύψει ή όχι και στη συνέχεια, να το εξερευνήσουμε ή να το αγνοήσουμε, πάντως σε κάθε περίπτωση, εξακολουθεί να βρίσκεται εκεί, ανεξάρτητα από τι σκεπτόμαστε ή τι κάνουμε για αυτό. Από κάποιο σημείο και μετά, τα βακτήρια αποτέλεσαν αντικείμενο μελέτης για τους βιολόγους.

Κανείς δεν αμφιβάλλει ότι ενυπήρχαν στους ζωντανούς οργανισμούς και πριν από την ύπαρξη των βιολόγων, ακόμα και πριν από την ύπαρξη του ανθρώπινου είδους. Αυτό δεν αμφισβητείται σε κανένα επιστημονικό πεδίο. Ωστόσο, στα μαθηματικά είναι ένα θέμα που απαιτεί διαφορετική προσέγγιση. Οι πρώτοι αριθμοί είναι εφεύρεση ή ανακάλυψη; Θα υπήρχαν οι πρώτοι αριθμοί αν δεν υπήρχαν ανθρώπινα όντα; Αυτή η συζήτηση έχει προκαλέσει και συνεχίζει να προκαλεί μεγάλη συζήτηση, θερμή για κάποιους, επουσιώδη για άλλους. Το πιθανότερο είναι να πρόκειται για ένα ερώτημα δίχως απάντηση ενώπιον του οποίου μπορούμε μόνο να τοποθετηθούμε προσεκτικά. Αυτό που είναι πραγματικά σημαντικό για τη φύση της μαθηματικής σκέψης, είναι ότι ο δημιουργός λειτουργεί ως εξερευνητής που πηγαίνει σε ξένα μέρη, σαν να μην είχε καμία σχέση με τα μαθηματικά. Αυτή η αίσθηση της περιπέτειας αποτελεί μέρος της ίδιας ουσίας της μαθηματικής έρευνας και είναι εκείνο που της δίνει το χαρακτήρα της τέχνης.

Ο Γερμανός φυσικός **Heinrich Rudolf Hertz** (1857–1894) ρωτήθηκε σχετικά *«Μπορεί άραγε κανείς να αποφύγει την σκέψη ότι αυτοί οι μαθηματικοί τύποι έχουν ανεξάρτητη ύπαρξη και δική τους νοήμοσύνη σοφότερη από την δική μας και ότι καταλήγουμε να παίρνουμε από αυτούς περισσότερα από όσα είχαμε αρχικά επενδύσει σε αυτούς;»*. Το φιλοσοφικό ρεύμα, ή μάλλον, το επιστημολογικό, που δέχεται το γεγονός ότι τα αντικείμενα (συμπεριλαμβανομένων των μαθηματικών αληθειών) υπάρχουν για λογαριασμό τους, λαμβάνει την ετικέτα του «πλατωνισμού», που συνοπτικά δηλώνει ότι μπορούμε να έχουμε μια αντικειμενική στάση μόνο όσο βρισκόμαστε παρουσία των αντικειμένων. Οι ιστορικοί των μαθηματικών, συνηθίζουν να γέρνουν τη ζυγαριά προς τον πλατωνισμό βασιζόμενοι στον αναντίρρητο γεγονός της παγκοσμιότητάς του, καθώς σε πολύ απομακρυσμένους στο χώρο και στο χρόνο πολιτισμούς, οι μαθηματικοί συλλογισμοί καταλήγουν στα ίδια συμπεράσματα, στις ίδιες μαθηματικές αλήθειες.

Στην περίπτωση των πρώτων αριθμών, για παράδειγμα, έχουμε ένα ενδιαφέρον στοιχείο, που θα μπορούσαμε να χαρακτηρίσουμε ως μαθηματική αρχαιολογία, το κόκκαλο του Ισάνγκο. Στον εν λόγω οστέινο εργαλείο

από την παλαιολιθική εποχή, διακρίνονται κάποιες εγχοπές σαν μικρά ευθύγραμμα τμήματα. Μια προσεκτικότερη εξέτασή τους οδήγησε στο συμπέρασμα ότι περισσότερο από ένα εργαλείο επρόκειτο για ένα σύστημα αρίθμησης. Σε αυτή την περίπτωση, είναι πιθανό η αιχμή από χαλαζία να χρησίμευε για να σημειώνει κατά κάποιο τρόπο την κατάσταση των λογαριασμών. Με άλλα λόγια, η λαβή του οστού εκτελούσε τις συναρτήσεις ενός πρωτόγονου υπολογιστικού πίνακα. Η διάταξη των εγχοπών σε αυτή την στήλη, φανερώνει πράξεις πρόσθεσης και πολλαπλασιασμού σε ένα σύστημα αρίθμησης με βάση το 12.

Οι αριθμοί στα δεξιά είναι όλοι περιττοί, αλλά το πραγματικά εκπληκτικό είναι ότι όλοι οι αριθμοί στα αριστερά είναι πρώτοι, συγκεκριμένα αυτοί που περιλαμβάνονται μεταξύ 10 και 20. Δεν θα ήταν συνετό να αποδώσουμε τη διάταξη των εγχοπών σε καθαρή τύχη ή σε κάποια άλλη διαδικασία που δεν θα προϋπόθετε κάποιο προχωρημένο αριθμητικό λογισμό. Ας θυμηθούμε ότι η έννοια του πρώτου αριθμού απαιτεί μια διαδικασία αφαίρεσης, που υπερβαίνει τις απλές τεχνικές μέτρησης. Στο ζήτημα σχετικά με το αν οι μαθηματικές αλήθειες υπάρχουν ή όχι στο περιθώριο της ανθρώπινης ύπαρξης, θα μπορούσε να προστεθεί μια τρίτη θέση, μια συμβιβαστική λύση η οποία εξετάζει την πιθανότητα να παραδεχτούμε ότι όντως υπάρχουν αυτά τα μαθηματικά αντικείμενα που πιθανόν να ανακαλυφθούν, αλλά πρόκειται για «νοητικά αντικείμενα» που κληρονομούμε με το γενετικό πακέτο.

Με βάση αυτό τον συλλογισμό, πρέπει να υπήρχε στη φύση κάποια πρωτόγονη μορφή των εν λόγω σχηματισμών. Σε ό,τι αφορά στην ικανότητα αρίθμησης, στο ζωικό βασίλειο υπάρχουν αναρίθμητα παραδείγματα ειδών που μπορούν να «μετρούν» με αρκετή ακρίβεια. **Οι μοναχικές σφήκες**, έχουν την ικανότητα να μετρούν τον αριθμό των ζωντανών καμπίων που αφήνουν για τροφή στις προνύμφες τους, στις κυνέλες όπου εναποθέτουν τα αυγά τους, πάντα είναι **ακριβώς 5, 12 ή 24**.

Ακόμα πιο εκπληκτική είναι η περίπτωση των σφηκών που ανήκουν στο είδος *Eumenes*, **γνωρίζουν αν από το αυγό τους θα βγει αρσενικό ή θηλυκό έντομο**. Αγνοούμε τον μηχανισμό που χρησιμοποιεί για να εξακριβώνει το φύλλο των απογόνων της, εφόσον τα κελιά όπου πραγματοποιεί την εναπόθεση και αφήνει τροφή δεν παρουσιάζουν εμφανή διακριτικά σημάδια. Το θέμα είναι ότι η σφήκα αφήνει **5** κάμπιες για κάθε αυγό που αντιστοιχεί σε αρσενικό απόγονο και **10** αν πρόκειται για θηλυκό. Η ανισότητα αυτή, οφείλεται στο γεγονός ότι οι θηλυκές σφήκες έχουν μεγαλύτερο μέγεθος από αυτό των αρσενικών.

Ακόμη και για μια πιο περίπλοκη έννοια, όπως αυτή του πρώτου αριθμού, συναντάμε ένα περίεργο παράδειγμα σε ορισμένα είδη **τζιτζικιών** *Magiceda septendecim* και *M. tredecim*. Τα επιστημονικά τους ονόματα *septendecim* και *tredecim*, σημαίνουν αντίστοιχα, 17 και 13 και αναφέρονται στους κύκλους της ζωής και των δύο ειδών. Και οι δύο είναι πρώτοι αριθμοί και οι ζωολόγοι έχουν σκεφτεί διαφορετικές θεωρίες για να εξηγήσουν την επιλογή ενός πρώτου αριθμού ετών, για τον κύκλο ζωής αυτών των εντόμων.

Ας πάρουμε σαν παράδειγμα το **Magiceda septendecim**. Αυτό το τζιτζίκι ζει ως νύμφη κάτω από το χώμα και τρέφεται με χυμούς που απομυζά από τις ρίζες των δέντρων. Ζει σε αυτή την κατάσταση για 17 έτη και ύστερα βγαίνει στην επιφάνεια για να μεταμορφωθεί σε ενήλικο έντομο, στάδιο που διαρκεί μόνο λίγες ημέρες, κατά τη διάρκεια των οποίων αναπαράγεται και στο τέλος, πεθαίνει. Η συμπεριφορά αυτή εξηγείται ως εξής: Ανάμεσα στους εχθρούς του τζιτζικιού υπάρχει ένα παράσιτο του οποίου ο κύκλος ζωής είναι δύο χρόνια. Αν ο κύκλος ζωής του τζιτζικιού ήταν πολλαπλάσιο του 2, τότε τα δύο είδη θα συνέπιπταν κάθε 2, 4, 8... χρόνια. Το ίδιο θα συνέβαινε και με άλλα πολλαπλάσια.

Αν όμως ο κύκλος ζωής είναι ένας πρώτος αριθμός ετών αρκούντος υψηλός, όπως είναι η περίπτωση του 17, το παράσιτο και το τζιτζίκι θα μπορούν να συμπέσουν μόνο κάθε 34 έτη, που είναι το πρώτο πολλαπλάσιο του 17. Στην υποθετική περίπτωση που ο κύκλος ζωής του παρασίτου ήταν 16 έτη, η πιθανότητα να συναντηθούν θα ήταν κάθε $16 \cdot 17 = 272$ χρόνια. Είναι πολύ πιθανό, με τον καιρό, η μελέτη της συμπεριφοράς των ζώων να οδηγήσει σε περισσότερα παραδείγματα ειδών που να «ξέρουν να μετρούν». Δεν μπορούμε να παραβλέψουμε την κοινοτοπία αυτής της συλλογιστικής, το σημαντικό όμως είναι ότι αν τα μαθηματικά αντικείμενα, όπως οι πρώτοι αριθμοί, είναι ανθρώπινο δημιούργημα, ο ερευνητής μπορεί να φτάσει να τους ζήσει και να τους νιώσει σαν να ήταν αυθύπαρκτοι.

4. Το κόσκινο του Ερατοσθένη

Η παραγωγή πρώτων αριθμών, υπήρξε και εξακολουθεί να είναι ένα ακανθώδες θέμα. Μια από τις πρώτες γνωστές μεθόδους που εφαρμόστηκαν για αυτό τον σκοπό αποδίδεται στον **Ερατοσθένη τον Κυρηναίο** (273–194 π.Χ.), Έλληνα μαθηματικό, αστρονόμο και γεωγράφο που διετέλεσε διευθυντής της Αλεξανδρινής βιβλιοθήκης. Η εν λόγω μέθοδος, είναι γνωστή ως «**το κόσκινο του Ερατοσθένη**». Ας δούμε πώς πραγματοποιείται το κόσκινο των εκατό πρώτων φυσικών αριθμών.

Πρώτα–πρώτα κατασκευάζουμε έναν πίνακα με όλους τους φυσικούς αριθμούς από το 1 ως το 100. Ξεκινάμε απαλείφοντας τους πολλαπλάσιους του 2, δηλαδή το 4, το 6, το 8, το 10..., ύστερα εκείνους που είναι πολλαπλάσιοι του 3 (αυτό έχει ήδη απαλειφθεί), το 9, το 12, το 15... Θα ακολουθήσουν τα πολλαπλάσια του 5 και ύστερα του επτά. Οι αριθμοί που απέμειναν είναι όλοι τους πρώτοι.

Παρατηρήστε ότι το κόσκινο τελειώνει όταν φτάνουμε στον αριθμό 10, που είναι η τετραγωνική ρίζα του 100. Γενικά για να βρούμε όλους τους πρώτους αριθμούς που είναι μικρότεροι από έναν δοθέντα αριθμό N , αρκεί να χρησιμοποιήσουμε το κόσκινο για αριθμούς μικρότερους ή ίσους με ρίζα N . Έτσι, έχουμε στη διάθεση μας μια μέθοδο εύρεσης πρώτων αριθμών, μικρότερων από έναν άλλον δοθέντα αριθμό. Η εν λόγω μέθοδος, εξακολουθεί να εφαρμόζεται ως τις ημέρες μας, πάνω από 2.000 έτη μετά την εκπόνησή της, προκειμένου να βρίσκουμε μικρούς πρώτους αριθμούς, μικρότερους από τον αριθμό δέκα δισεκατομμύρια.

5. Πόσοι πρώτοι αριθμοί υπάρχουν;

Αν θελήσουμε να αρχίσουμε να εξετάζουμε τη φύση των πρώτων αριθμών προκειμένου να εντοπίσουμε μια θέση ανάμεσά τους ή έναν κανόνα που να μας επιτρέπει να προβλέπουμε πότε θα εμφανιστεί ο επόμενος, κατ' αρχήν πρέπει να έχουμε συλλέξει έναν ικανό αριθμό από αυτούς. Ο παρακάτω κατάλογος, που έχει προκύψει μέσω του κόσκινου του Ερατοσθένη, δείχνει τους πρώτους αριθμούς που βρίσκονται μεταξύ των χιλίων πρώτων φυσικών αριθμών.

2	3	5	7	11	13	17	19
23	29	31	37	41	43	47	53
59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173

179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457
461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569
571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719
727	733	739	743	751	757	761	769
773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881
883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997

Μια προκαταρκτική εξέταση επιτρέπει να διαπιστώσουμε ότι **οι πρώτοι είναι εντελώς απρόβλεπτοι**. Υπάρχουν για παράδειγμα, περισσότεροι πρώτοι μεταξύ του 1 και του 100 από ότι μεταξύ του 101 και του 200. **Μεταξύ των αριθμών 1 και 1.000 υπάρχουν 168 πρώτοι**. Θα μπορούσαμε να σκεφτούμε ότι αν ο πίνακάς ήταν πολύ μεγαλύτερος, θα βλέπαμε το πώς αυξάνει η ποσότητα των πρώτων αριθμών όσο προχωράμε ανά χίλιους αριθμούς. Μόνο που κάτι τέτοιο δεν ισχύει. Πλέον υπάρχουν πίνακες τεραστίων διαστάσεων και γνωρίζουμε ότι, για παράδειγμα, μεταξύ χιλίων αριθμών που πηγαίνουν από 10^{100} και $10^{100} + 1.000$ απαντώνται μόνο 2 πρώτοι αριθμοί. Και μιλάμε για αριθμούς με περισσότερα από 100 ψηφία!

Φαίνεται ξεκάθαρο ότι για να μπορέσουμε να βρούμε έναν κανόνα, το καλύτερο θα ήταν να διαθέτουμε έναν πίνακα που θα περιλάμβανε όλους τους πρώτους αριθμούς. Και αν είναι πάρα πολλοί; Δεν έχει σημασία με τα μέσα που διαθέτουμε σήμερα έχουμε την δυνατότητα να τους εντάξουμε σε κάθε είδος κόσκινου και τεστ που θα μας επιτρέψουν να βρούμε τον κανόνα. Διότι είναι σαφές ότι όταν πρόκειται για πεπερασμένα σύνολα, όσο μεγάλα και αν είναι, μπορεί να ανακαλύψουμε έναν κανόνα, ή τουλάχιστον, να εφεύρουμε κάποιον που να ταιριάζει. Εντούτοις, το πράγμα αλλάζει, και πολύ μάλιστα, όταν πρόκειται για άπειρα σύνολα. Συνεπώς, πρέπει να αποφασίσουμε αν υπάρχουν ή δεν υπάρχουν άπειροι πρώτοι αριθμοί. Αυτό είναι ένα ζήτημα που έθεσε και ο Ευκλείδης. Ο τρόπος επίλυσής του είναι τόσο ευρηματικός και από μαθηματικής άποψης τόσο απλός που αξίζει να τον μελετήσουμε με κάθε λεπτομέρεια.

Ας ξεκινήσουμε από μια μικρή λίστα πρώτων διαδοχικών αριθμών, για παράδειγμα 2, 3, 5. Στη συνέχεια, ας εξάγουμε το γινόμενο τους $2 \cdot 3 \cdot 5 = 30$. Τώρα ας αθροίσουμε μια μονάδα στο αποτέλεσμα $2 \cdot 3 \cdot 5 + 1 = 31$. Είναι σαφές ότι αν

το 31 διαιρεθεί με οποιονδήποτε από τους πρώτους αριθμούς της λίστας 2, 3, 5 πρέπει να δώσει υπόλοιπο 1.

- $31 \frac{1}{2} = 15$, με υπόλοιπο 1, άρα $15 \cdot 2 + 1 = 31$
- $31 \frac{1}{3} = 10$, με υπόλοιπο 1, άρα $10 \cdot 3 + 1 = 31$
- $31 \frac{1}{5} = 6$, με υπόλοιπο 1, άρα $5 \cdot 6 + 1 = 31$

Αυτό εξασφαλίζει ότι δεν διαιρείται ακριβώς με κανέναν από αυτούς. Είναι κάτι που συμβαίνει πάντα, αν ξεκινήσουμε με μια λίστα πρώτων διαδοχικών αριθμών, όταν τους πολλαπλασιάζουμε μεταξύ τους και προσθέτουμε μια μονάδα στο αποτέλεσμα, ο αριθμός που προκύπτει δεν διαιρείται με κανέναν από τους αριθμούς της λίστας. Αυτός είναι και ο πυρήνας της Ευκλείδειας απόδειξης.

Ο αριθμός 31 είναι ένας πρώτος αριθμός που δεν βρισκόταν στην αρχική λίστα. Ας πάρουμε την λίστα $\{2, 3, 5, 7, 11, 13\}$. Εξάγουμε το γινόμενο τους και προσθέτουμε μια μονάδα $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30.030 + 1 = 30.031$. Αυτός δεν είναι ένας πρώτος αριθμός, αφού μπορεί να προκύψει ως γινόμενο δυο πρώτων αριθμών $30.031 = 59 \cdot 509$. Ο Ευκλείδης, είχε ήδη αποδείξει ότι **κάθε φυσικός αριθμός μπορεί να αναλυθεί με μοναδικό τρόπο ως γινόμενο πρώτων παραγόντων**. Αν εφαρμόσουμε αυτό το αποτέλεσμα στον αριθμό 30.031, που είναι σύνθετος αριθμός, καθίσταται σαφές ότι με τους πρώτους από τη λίστα $\{2, 3, 5, 7, 11, 13\}$ μπορούμε να αναλύσουμε σε παράγοντες και αυτό διότι από την εν λόγω λίστα απουσιάζουν οι πρώτοι αριθμοί 59 και 509. Το συμπέρασμα είναι ότι, όσο μεγάλη και αν είναι η αρχική λίστα των πρώτων αριθμών, **πολλαπλασιάζοντάς τους όλους μεταξύ τους και προσθέτοντας μια μονάδα**, το αποτέλεσμα είναι ένας νέος αριθμός που πληροί μια από τις παρακάτω συνθήκες:

- Είναι ένας πρώτος αριθμός που δεν βρισκόταν στην αρχική λίστα.
- Είναι ένας σύνθετος αριθμός στην ανάλυση του οποίου, ως γινόμενο πρώτων αριθμών, εμφανίζονται αριθμοί που δεν βρίσκονταν στην αρχική λίστα.

Έτσι, η λίστα πάντα είναι ελλιπής, εκτός και αν είναι άπειρη. Δυστυχώς, αυτή δεν είναι μέθοδος εύρεσης πρώτων αριθμών, μολονότι αποτελεί σημαντικότερη αφετηρία, επειδή προσφέρει μια διάσταση του προβλήματος και μια προοπτική χωρίς την οποία θα ήταν αδύνατο να εξεταστεί οποιαδήποτε στρατηγική. Θα μπορούσαμε επίσης να σκεφτούμε ότι δεν αξίζει τον κόπο να αποδείξουμε ότι υπάρχουν άπειροι πρώτοι αριθμοί, καθώς είναι κάτι που υποθέτομε πως ισχύει. Παρά ταύτα, με τους πρώτους αριθμούς πρέπει να είμαστε πολύ προσεχτικοί, επειδή είναι τόσο «παράξενοι» που **θα μπορούσαν από ένα σημείο και μετά να σταματήσουν να εμφανίζονται. Ωστόσο το θεώρημα του Ευκλείδη μας εγγυάται ότι κάτι τέτοιο δεν πρόκειται να συμβεί.**

6. Μεγάλα κενά

Το πρώτο πράγμα που τράβηξε την προσοχή των μαθηματικών της αρχαιότητας, σε σχέση με τους πρώτους αριθμούς, είναι **η απουσία κανόνων αναφορικά με την εμφάνισή τους στην ακολουθία των φυσικών αριθμών**. Επιπλέον, προκύπτει ότι ούτε και η απουσία τους εκδηλώνεται με ξεκάθαρη συμπεριφορά, δηλαδή, δεν υπάρχει συγκεκριμένος τρόπος με τον οποίο σταματούν να εμφανίζονται. Συνεπώς, μπορεί είτε να βρίσκονται σχετικά συγκεντρωμένοι, είτε να απέχουν πολύ ο ένας από τον άλλο. Αν λάβουμε για παράδειγμα, τους πρώτους αριθμούς που απαντώνται μεταξύ των 100 πρώτων φυσικών αριθμών, 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 θα παρατηρήσουμε ότι οι πρώτοι 8

εμφανίζονται σχεδόν συνεχόμενα, υπάρχουν 8 μεταξύ των πρώτων 20 και αντίθετα, δεν υπάρχει κανένας μεταξύ του 89 και του 97. Αν πάρουμε τους πρώτους αριθμούς που περιλαμβάνονται μεταξύ 100 και 200, είναι 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, θα δούμε μεγάλα κενά, όπως τους 9 σύνθετους διαδοχικούς αριθμούς από το 182 μέχρι το 190.

Το ερώτημα που γεννάται τότε είναι, μπορεί να υπάρχουν πολύ μεγάλα κενά, όπως για παράδειγμα, 50.000 συνεχόμενοι αριθμοί και μεταξύ τους να μην υπάρχει κανένας πρώτος αριθμός; Το σύμπαν των πρώτων αριθμών είναι αρκετά μεγάλο ώστε να μπορούμε να εντοπίσουμε στο εσωτερικό του τεράστια κενά, μεγάλες δηλαδή, ακολουθίες αριθμών που δεν περιέχουν πρώτους αριθμούς. Αυτή δεν είναι απλή εικασία, αλλά κάτι που έχει αποδειχθεί. Ας εξετάσουμε το γινόμενο των 4 πρώτων φυσικών αριθμών: $1 \cdot 2 \cdot 3 \cdot 4$. Μπορούμε να διασφαλίσουμε ότι ο αριθμός $1 \cdot 2 \cdot 3 \cdot 4 + 2$ δεν μπορεί να είναι πρώτος διότι είναι διαιρετός με το δυο.

Η επαλήθευση είναι άμεση, επειδή $1 \cdot 2 \cdot 3 \cdot 4 + 2 = 24 + 2 = 26$ και διαιρώντας τον δια του δυο, δίνει 13. Δεν χρειαζόταν να γίνει κάποια πράξη για να μάθουμε αν διαιρείτο δια του δύο, επειδή αν αθροίσουμε και τους δύο περιέχουν τον αριθμό 2. Για τον ίδιο λόγο

$1 \cdot 2 \cdot 3 \cdot 4 + 3$ δεν μπορεί να είναι πρώτος διότι διαιρείται δια του 3.
 $1 \cdot 2 \cdot 3 \cdot 4 + 4$ δεν μπορεί να είναι πρώτος διότι διαιρείται δια του 4.

Με αυτό τον τρόπο μας δόθηκαν 3 διαδοχικοί αριθμοί, 26, 27, 28, που δεν είναι πρώτοι. Αν τώρα θελήσουμε να έχουμε 4 διαδοχικούς αριθμούς που να μην είναι πρώτοι, γράφουμε $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 + 2 = 122$, $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 + 3 = 123$, $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 + 4 = 124$, $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 + 5 = 125$.

Για ευκολία, θα συμβολίσουμε το γινόμενο διαδοχικών αριθμών με ένα θαυμαστικό $1 \cdot 2 \cdot 3 \cdot 4 = 4!$, $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5!$. Στα μαθηματικά αυτού του είδους οι παραστάσεις ονομάζονται «παραγοντικά». Για παράδειγμα το παραγοντικό του 6 είναι $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 6! = 720$. Συνεπώς, είναι πιο βολικό να γράφουμε τις προηγούμενες παραστάσεις με τη μορφή $5! + 2$, $5! + 3$, $5! + 4$, $5! + 5$. Με αυτό τον τρόπο, μπορούμε να γράφουμε σειρές από διαδοχικούς αριθμούς που δεν περιέχουν κανέναν πρώτο αριθμό. Για παράδειγμα, αν θέλουμε να γράφουμε 100 διαδοχικούς αριθμούς κατά τέτοιο τρόπο ώστε, κανένας από αυτούς να μην είναι πρώτος, δεν έχουμε παρά να κάνουμε το εξής $101! + 2$, $101! + 3$, $101! + 4$. Ομοίως μέχρι το $101! + 101$. Αυτό σημαίνει ότι υπάρχουν μεγάλα κενά στα οποία δεν εμφανίζονται πρώτοι αριθμοί. Με την ίδια μέθοδο θα μπορούσαμε να κατασκευάσουμε μια σειρά από πέντε τρισεκατομμύρια διαδοχικούς αριθμούς στην οποία να μην εμφανίζεται κανένας πρώτος αριθμός. Αυτό μας οδηγεί στο συμπέρασμα ότι οι πρώτοι αριθμοί σπανίζουν όλο και περισσότερο όσο προχωράμε στην ακολουθία των φυσικών αριθμών και συνεπώς, όσο απομακρυνόμαστε προς το άπειρο, θα έρθει στιγμή που δεν θα υπάρχει πλέον κανένας. Αυτή η δελεαστική ματιά ανταποκρίνεται σε μια ψευδή διαίσθηση, αφού γνωρίζουμε ότι το θεώρημα του Ευκλείδη εγγυάται πως υπάρχουν άπειροι πρώτοι αριθμοί και ότι, όσο μεγάλη και αν είναι μια σειρά σύνθετων αριθμών, κάποια στιγμή θα επανεμφανιστεί ένας πρώτος αριθμός.

7. Δίδυμοι πρώτοι

Αν δεν είναι δυνατό να καταρτιστεί ένας γενικός νόμος σχηματισμού, τουλάχιστον μπορούμε να προσπαθήσουμε να μελετήσουμε τη συμπεριφορά κάποιων πρώτων αριθμών που παρουσιάζουν ειδικά χαρακτηριστικά. Είναι σαν να κοιτάζουμε έξω από το παράθυρο ένα ατελείωτο πλήθος διαφορετικών ανθρώπων να

πηγαινοέρχεται. Αποτελείται από άντρες και γυναίκες, αλλά δεν μπορούμε να καταλήξουμε σε έναν κανόνα που θα μας επιτρέψει να προβλέπουμε ποια θα είναι η στιγμή κατά την οποία θα περάσει ένας άντρας ή μια γυναίκα. Μία ημέρα όμως, εντελώς ξαφνικά, τραβά την προσοχή μας κάποιο ειδικό χαρακτηριστικό και αντιλαμβανόμαστε ότι, ορισμένες φορές, περνούν άντρες με καπέλο, άτομα με γυαλιά ηλίου ή ομπρέλες. Προσπαθούμε τότε να βρούμε κάποιον κανόνα που να διέπει την εμφάνιση συγκεκριμένων ομάδων ατόμων. Παρατηρούμε για παράδειγμα, αν τα άτομα με καπέλο εμφανίζονται κάθε 100 φορές που περνάει μια γυναίκα, ή αν κάθε φορά που περνάει ένας άντρας, κατόπιν πάντα περνάει μια γυναίκα.

Τέτοιες παρατηρήσεις μας βοηθούν να διατυπώσουμε έναν κανόνα, του οποίου την ισχύ είναι εύκολο να εξετάσουμε. Είναι πιθανό να περάσουν από μπροστά μας τρία εκατομμύρια άνθρωποι επιβεβαιώνοντας τον κανόνα μας, αλλά ο επόμενος να τον καταρρίπτει. Τότε, δεν μπορούμε να κάνουμε τίποτα άλλο απ' το να φωνάξουμε «παρά τρίχα!». Αυτό το «παρά τρίχα» θα μας οδηγήσει να πούμε ότι «τα πράγματα λειτουργούν σχεδόν σαν να...», συνηθής έκφραση στην ιστορία των πρώτων αριθμών. Είναι αλήθεια ότι κατέστη δυνατός ο χαρακτηρισμός κάποιων οικογενειών πρώτων αριθμών (πράγματι υπάρχουν κάποιες δωδεκάδες) που επέτρεψαν σημαντικά βήματα προόδου στο ρου την Ιστορίας. Για παράδειγμα, ας δούμε μερικά μοναδικά ζεύγη πρώτων αριθμών τα χαρακτηριστικά των οποίων θα μας βοηθήσουν να εννοήσουμε κάπως καλύτερα τις μαθηματικές δυσκολίες που εγκυμονούν αυτοί οι «περίεργοι» αριθμοί. Δύο πρώτοι αριθμοί δεν μπορεί να είναι διαδοχικοί, επειδή **κάθε πρώτος αριθμός είναι περιττός** και ο επόμενος αριθμός αναγκαστικά πρέπει να είναι άρτιος, για αυτό και δε θα μπορούσε να είναι πρώτος.

Ως εκ τούτου, η πλησιέστερη απόσταση στην οποία μπορούν να βρίσκονται δύο πρώτοι αριθμοί είναι να χωρίζονται από δύο μονάδες. **Εξαίρεση αποτελούν το 2 και το 3, που είναι διαδοχικοί. Επιπλέον, το 2 είναι ο μοναδικός άρτιος πρώτος αριθμός.** Μεταξύ των πρώτων 100 φυσικών αριθμών βρίσκουμε τα ακόλουθα ζεύγη που χωρίζονται από δύο μονάδες:

(3,5) (5,7) (11,13) (17,19) (29,31) (41,43) (59,61) και (71,73)

Αυτά τα ζεύγη ονομάζονται «**δίδυμοι πρώτοι**» ή, απλώς «**δίδυμοι**». Οι δίδυμοι απαντούν στη δομή $(p, p+2)$ όπου p είναι ένας πρώτος αριθμός. Αυτή είναι η λίστα όλων των δίδυμων πρώτων που συγκαταλέγονται μεταξύ των 1.000 πρώτων αριθμών:

(3,5),	(5,7),	(11,13),	(17,19),	(29,31),
(41,43),	(59,61),	(71,73),	(101,103),	(107,109),
(137,139),	(149,151),	(179,181),	(191,193),	(197,199),
(227,229),	(239,241),	(269,271),	(281,283),	(311,313),
(347,349),	(419,421),	(431,433),	(461,463),	(521,523),
(569,571),	(599,601),	(617,619),	(641,643),	(659,661),
(809,811),	(821,823),	(827,829),	(857,859),	(881,883).

Γνωρίζουμε ότι, οι δίδυμοι πρώτοι αρχίζουν να σπανίζουν όσο προχωράει η σειρά των φυσικών αριθμών. Ωστόσο, γνωρίζουμε, χάρη σε σύγχρονες υπολογιστικές μεθόδους, ότι συναντώνται δίδυμοι πρώτοι ακόμα και σε ασύλληπτα μεγάλους αριθμούς, γεγονός που μας κάνει να **πιστεύουμε ότι υπάρχουν άπειροι δίδυμοι πρώτοι αριθμοί**, εικασία που μέχρι τις ημέρες μας κανείς δεν έχει καταφέρει να αποδείξει. Μια άλλη ομάδα πρώτων αριθμών που τραβάει την προσοχή μας όταν παρατηρούμε τον πίνακα όσων περιέχονται μεταξύ των 100 πρώτων φυσικών

αριθμών, είναι αυτή που αποτελείται από αριθμούς 3, 5, 7. Όταν ο p είναι ένας πρώτος αριθμός, αυτοί οι 3 απαντούν στη δομή $(p, p+2, p+4)$. Είναι μια ομάδα που θα μπορούσε να ονομαστεί «**τρίδυμοι**» ή «**τριπλέτα**». Στην πραγματικότητα, δεν χρειαζόταν να τους δώσουμε κανένα όνομα, καθώς δεν υπάρχουν περισσότεροι από αυτούς τους τρεις. Αυτό το αποτέλεσμα είναι επιβεβαιωμένο. Ευτυχώς, το εν λόγω θέμα έχει κλείσει, αφού σε αντίθετη περίπτωση, οι «τριπλέτες» θα τροφοδοτούσαν περαιτέρω εικασίες που ακόμη θα παρέμεναν αναπάντητες. Οι μεγαλύτεροι δίδυμοι πρώτοι που γνωρίζουμε (μέχρι τον Αύγουστο 2009) είναι αυτοί που σχηματίζονται από τους αριθμούς $65.516.468.355 \cdot 2^{333333} - 1$, $65.516.468.355 \cdot 2^{333333} + 1$ και έχουν έναν επιβλητικό αριθμό εκατό χιλιάδων τριακοσίων πενήντα πέντε ψήφων.

8. Οι αριθμοί του Mersenne

Το μεγάλο επιστημονικό, καθαρά μαθηματικού χαρακτήρα, έργο του Mersenne ήταν το **Cogitata Physico-Mathematica** (1644), στο οποίο περιλαμβάνεται η περίφημη μελέτη του σχετικά με τους πρώτους αριθμούς. Στον πρόλογο του, ο Mersenne δηλώνει ότι μεταξύ όλων των πρώτων αριθμών που υπάρχουν ανάμεσα στο 125 και το 257, ο αριθμός $2^p - 1$ είναι πρώτος μόνον εφόσον η τιμή του p είναι ένας από τους αριθμούς 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257. Όταν παίρνουμε το 2 και το υψώνουμε στον τελευταίο αριθμό της λίστας, το αποτέλεσμα είναι ένας αριθμός 77 ψηφίων. Το πως κατάφερε ο Mersenne με τα υπολογιστικά μέσα της εποχής του να αποφασίσει ότι αυτός ήταν ένας πρώτος αριθμός, αποτελεί πραγματικό μυστήριο που κανένας δεν έχει καταφέρει να διαλευκάνει. Εύκολα αποδεικνύεται ότι αν ο αριθμός $2^p - 1$ είναι πρώτος, τότε το p πρέπει να είναι πρώτος αριθμός (ή παρομοίως ότι αν το p δεν είναι πρώτος αριθμός, τότε το $2^p - 1$ είναι). Αυτό το αποτέλεσμα, που ήταν ήδη γνωστό στην εποχή του Mersenne, τον οδήγησε στο να ερευνήσει τί συνέβαινε όταν σε αυτή την παράσταση εισαγόταν ένας αριθμός p που ήταν πρώτος. Επίσης, ήταν γνωστό ότι το $2^p - 1$ ήταν πρώτος για τις τιμές $p=2, 3, 5, 7, 13, 17, 19$ όχι όμως για $p=11$. Έπρεπε να περάσουν 100 χρόνια για να καταφέρει ο **Euler** να αποδείξει ότι ο αριθμός $2^{31} - 1$ ήταν πρώτος. Το 1947 επιλύθηκε πλήρως η λίστα, έχοντας την μορφή $p=2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$ και 127 με αποτέλεσμα στην αρχική λίστα να περισσεύουν 2 αριθμοί και να λείπουν 3.

Παρόλα αυτά, οι εν λόγω αριθμοί συνεχίζουν να αποκαλούνται «αριθμοί του Mersenne», αριθμοί που σήμερα παίζουν σπουδαίο ρόλο στα αποκαλούμενα «**τεστ ιδιότητας πρώτου αριθμού**», ένα σύνολο αλγορίθμων που εκτελούνται προκειμένου να καθοριστεί αν ένας αριθμός είναι πρώτος ή όχι.

9. Το μικρό θεώρημα του Fermat

Το έτος 1995, ο Andrew Wiles φρόντισε να καταλάβει ο Fermat έναν χώρο στα πρωτοσέλιδα των εφημερίδων αφού είχε καταφέρει να αποδείξει μια από τις πιο διάσημες εικασίες στην ιστορία. Αν n είναι ένας ακέραιος αριθμός μεγαλύτερος του 2 ($n > 2$), τότε δεν υπάρχουν ακέραιοι αριθμοί x, y, z διάφοροι του 0 τέτοιοι που να ικανοποιούν την ισότητα $x^n + y^n = z^n$ εικασία που είναι γνωστή ως το «**τελευταίο θεώρημα του Fermat**». Υπάρχει και άλλο θεώρημα, λιγότερο δημοφιλές, γνωστό ως το μικρό θεώρημα του Fermat, που απέκτησε μεγάλη σπουδαιότητα στη θεωρία των πρώτων αριθμών. Η διατύπωση του εμφανίστηκε για πρώτη φορά σε μια επιστολή που ο Fermat απέστειλε στις **18.10.1640** στον Bernard Frenicle de Bessy (1605–1675), φίλο και επίσης αφοσιωμένο μαθηματικό με τον οποίο ο Fermat μοιραζόταν κάποια από τα αποτελέσματά του (και οι δύο ήταν μέλη του εκλεκτού κύκλου του

Mersenne). Η επιστολή ανέφερε τα εξής «*Κάθε πρώτος αριθμός υπολογίζει μια από τις δυνάμεις μείον έναν, οποιασδήποτε προόδου της οποίας ο εκθέτης είναι πολλαπλάσιο του πρώτου δοθέντος αριθμού μείον ένα (...)* Και αυτή η πρόταση ισχύει γενικά για όλες τις προόδους και όλους τους πρώτους αριθμούς, θα σας έστελνα την απόδειξη αν δεν φοβόμουν πως είναι υπερβολικά μεγάλη».

Όπως το συνήθιζε, ο Fermat παραλείπει την απόδειξη, λέγοντας, όπως και στην περίπτωση του περίφημου τελευταίου θεωρήματός του, πως είναι υπερβολικά μεγάλη. Είναι πολύ πιθανό και οι περισσότεροι σημερινοί ιστορικοί συμπίπτουν σε αυτό, ότι δεν γνώριζε πραγματικά την απόδειξη αυτής και άλλων εικασιών στις οποίες κατέληγε. Οπωσδήποτε, ο Fermat θεωρούσε τον εαυτό του «αφοσιωμένο», πράγμα που του άφηνε κάποιες ελευθερίες. Η διατύπωση στην επιστολή που στάλθηκε στον Bessy αποδεικνύεται κάπως αινιγματική, για αυτό και εδώ εκφράζεται ακολουθώντας τη σύγχρονη ορολογία. Αναφέρεται ότι **δύο αριθμοί είναι μεταξύ τους πρώτοι (ή πρώτοι προς αλλήλους) όταν είναι σχετικά πρώτοι, δηλαδή, δεν έχουν κοινούς παράγοντες**. Για παράδειγμα, το 8 και το 27 είναι μεταξύ τους πρώτοι, επειδή δεν έχουν κοινούς παράγοντες: $8 = 2^3$ και $27 = 3^3$. Αντίθετα, το 12 και το 15 δεν είναι, αφού έχουν το αριθμό 3 ως κοινό παράγοντα $12 = 3 \cdot 4$ και $15 = 3 \cdot 5$.

Το θεώρημα δηλώνει τότε ότι αν p είναι ένας πρώτος αριθμός και a ένας άλλος οποιοσδήποτε αριθμός, έτσι ώστε a και p να είναι μεταξύ τους πρώτοι, τότε το $a^p - 1$ διαιρείται με το p . Για παράδειγμα ας πάρουμε τον πρώτο αριθμό 3 και τον αριθμό 8 που είναι πρώτος με αυτόν, τότε $8^3 - 8 = 512 - 8 = 504$ διαιρείται με το 3. Πράγματι διαπιστώνουμε ότι $504/3 = 168$.

Μπορούμε να πούμε ότι το μικρό θεώρημα του Fermat είναι μικρό, αλλά δυνατό (το επίθετο «μικρό» χρησιμοποιήθηκε για πρώτη φορά το **1913** από τον Γερμανό μαθηματικό **Kurt Hensel**), καθώς είναι ένα από τα θεώρηματα στα οποία ανατρέχει κανείς περισσότερο όταν πρόκειται να διενεργήσει έλεγχο πρώτων αριθμών, ώστε να αποφασίσει αν ένας πολύ μεγάλος αριθμός είναι ή όχι πρώτος.

Πράγματι, ο Fermat αναγκάστηκε να το χρησιμοποιήσει ως μαθηματικό εργαλείο για να αναλύσει κάποιους μεγάλους πρώτους αριθμούς σε γινόμενο παραγόντων. Γνωρίζουμε ότι κατάφερε να βρει τον αριθμό 100.895.598.169 ως γινόμενο των αριθμών 898.423 και 112.303, πρώτοι και οι δύο, σε απάντηση αιτήματος του Mersenne, που ήθελε να μάθει αν ο εν λόγω αριθμός ήταν πρώτος. Ακόμη και έτσι, είναι δύσκολο να μάθουμε πώς ο Fermat μπόρεσε να χειριστεί τόσο μεγάλους αριθμούς. Το θεώρημα αποδείχτηκε για πρώτη φορά από τον **Euler** το **1736** (η απόδειξη του Leibniz ήταν παρόμοια, αλλά τότε δεν την δημοσίευσε). Και ο **Gauss** παρουσίασε μια άλλη απόδειξη στο περίφημο σύγγραμμά του *Disquisitiones arithmeticae*, που δημοσιεύθηκε το **1801**. Ο Euler, θα έδινε εκ των υστέρων ακόμη δύο αποδείξεις. Από όλες αυτές, η απλούστερη ήταν η πρώτη του Euler και μπορεί να γίνει κατανοητή με βασικές γνώσεις Μαθηματικών. Το μικρό θεώρημα του Fermat, αποτελεί μια μέθοδο για να μάθουμε αν ένας αριθμός δεν είναι πρώτος χωρίς να χρειάζεται να βρούμε κάποιον παράγοντά του.

Ας δούμε ένα απλό παράδειγμα. Έστω ότι $p=9$ και $a=2$. Τότε έχουμε ότι $2^9 - 2 = 510$ που δεν διαιρείται με το 9, οπότε συνάγεται ότι το 9 δεν είναι πρώτος αριθμός, κάτι που ήδη γνωρίζαμε. Η συμβολή της μεθόδου συνίσταται στη δυνατότητα να την εφαρμόζουμε σε πολύ μεγάλους αριθμούς. Πρέπει να προσέξουμε το γεγονός ότι, το μικρό θεώρημα του Fermat θέτει μια αναγκαία αλλά όχι ικανή προϋπόθεση, ωστόσο το γεγονός ότι ικανοποιείται δεν σημαίνει ότι ο p είναι πρώτος. Για παράδειγμα, αν $p=10$ και $a=3$, έχουμε $3^{10} - 3 = 59.046$ που δεν είναι πρώτος αριθμός, αφού διαιρείται με το 3.

10. Οι αριθμοί του Fermat

Ένας «αριθμός του Fermat» είναι ένας φυσικός αριθμός με τη μορφή $2^{2^n} + 1$. Συνήθως συμβολίζουμε με το γράμμα F (του Fermat) και με έναν δείκτη (n) που δείχνει τον αριθμό για τον οποίο πρόκειται, έτσι F_0 είναι ο πρώτος αριθμός του Fermat, ο F_1 ο δεύτερος κ.ο.κ. Θα υπολογίσουμε την τιμή των 5 πρώτων αριθμών του Fermat. Ας θυμηθούμε ότι οποιοσδήποτε αριθμός που υψώνεται στο 0 έχει τιμή 1, άρα $2^0=1$, $2^1=2$, $2^2=4$, $2^3=8$. Αντικαθιστώντας τον προηγούμενο τύπο έχουμε ότι:

$$F_0 = 2^1 + 1 = 3,$$

$$F_1 = 2^2 + 1 = 4 + 1 = 5,$$

$$F_2 = 2^4 + 1 = 16 + 1 = 17,$$

$$F_3 = 2^8 + 1 = 256 + 1 = 257,$$

$$F_4 = 2^{16} + 1 = 65.536 + 1 = 65.537.$$

Ο Fermat, υπέθεσε ότι όλοι οι αριθμοί που προκύπτανε κατ' αυτόν τον τρόπο ήταν πρώτοι. Οι πέντε πρώτοι 3, 5, 7, 257, 65.537, είναι όντως. Όταν $n=5$ ο αριθμός που προκύπτει είναι $F_5 = 2^{32} + 1 = 4.294.967.296 + 1 = 4.294.967.297$. Ο Fermat δεν διέθετε τα μέσα για να μάθει αν ένας αριθμός μεγαλύτερος του τέσσερις χιλιάδες εκατομμύρια, ήταν ή όχι πρώτος. Εντούτοις, δε συνέβαινε το ίδιο με τον **Euler** ο οποίος το **1732** βρήκε μια παραγοντοποίηση αυτού του αριθμού, ως γινόμενο άλλων δύο $4.294.967.297 = 641 \cdot 6.700.417$. Ο Euler είχε εντοπίσει την ψευδή εικασία στην επιχειρηματολογία του Fermat. Ήταν η πρώτη φορά που συνέβαινε κάτι τέτοιο.

Παρόλο που η εικασία ήταν ψευδής, η συμβολή των αριθμών του Fermat υπήρξε καθοριστική, όχι μόνο γιατί έδωσαν το έναυσμα για καινούρια ερωτήματα και νέες εικασίες, αλλά γιατί αποδείχθηκαν χρήσιμοι κατά την εκτέλεση ενός τεστ ιδιότητας πρώτου αριθμού. Για την ώρα, γνωρίζουμε ότι **μόνο οι 5 πρώτοι αριθμοί του Fermat είναι πρώτοι**, το οποίο δεν αποκλείει ότι υπάρχουν και περισσότεροι, ή ακόμη και άπειροι. Η πλήρης παραγοντοποίηση, είναι γνωστή μόνο μέχρι $n=11$. Και το να παραγοντοποιήσει κανείς έναν αριθμό ως γινόμενο πρώτων αριθμών δεν είναι εύκολη δουλειά.

11. Η εικασία του Goldbach

Ο Christian Goldbach (1690–1764) ήταν Πρώσος μαθηματικός που διατηρούσε συχνότατη αλληλογραφία με τον Euler. Στις **17.11.1752** του έστειλε μια επιστολή όπου διατύπωνε την ακόλουθη πρόταση «**Κάθε άρτιος αριθμός μεγαλύτερος του 2 μπορεί να γραφτεί ως άθροισμα δύο πρώτων αριθμών**». Στην έκφραση «άθροισμα δύο πρώτων» συμπεριλαμβάνεται η περίπτωση επανάληψης ενός πρώτου αριθμού δύο φορές. Για παράδειγμα

$$4 = 2 + 2,$$

$$6 = 3 + 3,$$

$$8 = 3 + 5,$$

$$10 = 3 + 7,$$

$$12 = 5 + 7,$$

$$14 = 3 + 11.$$

Στις **16.12.1752**, ο Euler του απάντησε ότι είχε επαληθεύσει την εικασία μέχρι τον αριθμό 1.000 και σε άλλη του επιστολή με ημερομηνία **03.04.1753**, ότι είχε επαληθεύσει πως το αποτέλεσμα ίσχυε μέχρι τον αριθμό 2.500. Σήμερα, η εικασία έχει επαληθευτεί με μεθόδους υπολογιστών για όλους τους άρτιους αριθμούς που είναι μικρότεροι από δύο χιλιάδες εκατομμύρια. Εντούτοις, δεν έχει ακόμα αποδειχτεί

και θεωρείται από τη μαθηματική κοινότητα ως ένα από τα δυσκολότερα προβλήματα στην ιστορία της επιστήμης.

12. Η πρώτη εικασία

Στο σημειωματάριο που διατηρούσε ο Gauss όταν ήταν 14 ετών, διαβάζουμε τη σημείωση «**Πρώτοι αριθμοί μικρότεροι του $a(=\infty)$ a/la** ». Ο Gauss, είχε επικεντρωθεί στη μελέτη της μεγάλης λίστας των πρώτων αριθμών που εμφανίζονταν στο τέλος του λογαριθμικού πίνακα και ήταν αναπόφευκτο να μαγευτεί από τη χαώδη σειρά. Είχε όμως ήδη αποφασίσει ότι οι προσπάθειές του δε θα προσανατολιζόνταν στην εύρεση ενός τύπου που θα του επέτρεπε να μάθει πώς ήταν και πού βρισκόταν «ο επόμενος πρώτος αριθμός». Αναμφίβολα, προαισθανόταν ότι αυτός ο δρόμος θα τον οδηγούσε στην αποτυχία. Αντ' αυτού, υπολόγισε πόσοι πρώτοι αριθμοί υπήρχαν μεταξύ 2 δοθέντων αριθμών ή, ακριβέστερα, πόσοι πρώτοι αριθμοί υπήρχαν μεταξύ των 10, των 100, των 1.000, των 10.000 πρώτων αριθμών, επειδή με αυτόν τον τρόπο θα μπορούσε να εκτιμήσει τη συχνότητα εμφάνισης των πρώτων αριθμών στη σειρά των φυσικών αριθμών. Γνωρίζουμε ότι **μεταξύ των 10 πρώτων φυσικών αριθμών έχουμε μόνο 4 πρώτους αριθμούς (2, 3, 5, 7). Μεταξύ 10 και 100 εμφανίζονται 21.**

Για να το αποδώσει αυτό, ο Gauss όρισε μια συνάρτηση την οποία ονόμασε $\pi(x)$ και η οποία ορίζεται ως εξής $\pi(x) =$ το πλήθος των πρώτων αριθμών που είναι μικρότεροι του x . Σύμφωνα με αυτό, $\pi(10)=4$. Για παράδειγμα, για να υπολογίσουμε το $\pi(15)$, θα έπρεπε να μετρήσουμε τους πρώτους αριθμούς που είναι μικρότεροι του 15, που είναι 2, 3, 5, 7, 11, 13, οπότε $\pi(15) = 6$. Το σύμβολο π που εμφανίζεται στον τύπο είναι ο γνωστός αριθμός π , αλλά σε αυτήν την περίπτωση στερείται μαθηματικής σημασίας, επειδή η συνάρτηση θα μπορούσε να οριστεί με τον ίδιο τρόπο αν βάζαμε οποιοδήποτε άλλο σύμβολο, όπως το $C(x)$. Η επιλογή του π δεν ήταν τόσο τυχαία εκ μέρους του Gauss και είναι πιθανό να χρησιμοποίησε το πρώτο που του ήρθε στο μυαλό. Λέμε ότι δεν ήταν πολύ τυχαίο γιατί η παρουσία του $\pi(x)$ υποδηλώνει αυτόματα όλους τους τύπους μαθηματικών σχέσεων που σχετίζονται με την περιφέρεια του κύκλου, οι οποίες, σε αυτή την περίπτωση, είναι εντελώς άσχετες με τους πρώτους αριθμούς.

Ο Γερμανός μαθηματικός κατήρτισε τότε έναν πρώτο πίνακα με δύο στήλες: στην 1^η έβαλε τις δυνάμεις του 10 και στη 2^η, την τιμή που έπαιρνε η $\pi(x)$. Ο 2^{ος} πίνακας έχει υπολογιστεί για τα πρώτα δέκα δισεκατομμύρια. Προφανώς, στην εποχή του Gauss τα υπολογιστικά εργαλεία ήταν πολύ πιο ελλιπή και δεν διέθεταν τέτοιο εύρος τιμών.

x	$\pi(x)$
10	4
100	25
1.000	168
10.000	1.229
100.000	9.592
1.000.000	78.498
10.000.000	664.579
100.000.000	5.761.455
1.000.000.000	50.847.534
10.000.000.000	455.052.512

Λογικά, η $\pi(x)$ είναι ένας αριθμός που αυξάνεται, όμως ο τρόπος αύξησής της δε λέει και πολλά πράγματα. Θα προσθέσουμε και άλλη στήλη που δίνει

την αναλογία των πρώτων αριθμών οι οποίοι είναι μικρότεροι από άλλον δεδομένο αριθμό. Για αυτό υπολογίζουμε τον λόγο $\pi(x)/x$. Γνωρίζουμε ότι υπάρχουν 168 πρώτοι αριθμοί μικρότεροι του 1.000. $\pi(x)/x = \pi(1.000)/1.000 = 168/1.000 = 0,168$.

Η πληροφορία που μας προσφέρει αυτός ο αριθμός είναι ότι το 16,8 % των αριθμών μεταξύ 1 και 1.000 είναι πρώτοι. Το υπόλοιπο 83,2 % αποτελείται από σύνθετους αριθμούς.

x	$\pi(x)$	$\pi(x)/x$
10	4	0,40000000
100	25	0,25000000
1.000	168	0,16800000
10.000	1.229	0,12290000
100.000	9.592	0,09592000
1.000.000	78.498	0,07849800
10.000.000	664.579	0,06645790
100.000.000	5.761.455	0,05761455
1.000.000.000	50.847.534	0,05084753
10.000.000.000	455.052.512	0,04550525

Προσθέτοντας αυτή την 3^η στήλη στον πίνακα, μπορούμε να παρατηρήσουμε ότι η αναλογία των πρώτων αριθμών, ελαττώνεται όσο ακολουθούμε μεγαλύτερους αριθμούς. Επρόκειτο για ένα μάλλον προβλέψιμο δεδομένο. **Για να είναι ένας αριθμός πρώτος, δεν πρέπει να διαιρείται με κανέναν από αυτούς που προηγούνται αυτού.** Για παράδειγμα, για να είναι το 13 πρώτος, δεν πρέπει να διαιρείται με τα 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12. Όσο μεγαλύτερος είναι ο αριθμός, τόσο μεγαλύτερη είναι η απαίτηση να μην διαιρείται και ως εκ τούτου, είναι λογικό οι πρώτοι αριθμοί να φθίνουν όλο και περισσότερο. Ο Gauss, ήξερε ήδη ότι αυτό δεν σήμαινε πως θα ερχόταν η στιγμή που θα τελείωναν οι διαθέσιμοι πρώτοι αριθμοί, καθώς γνώριζε την ύπαρξη του θεμελιώδους θεωρήματος της αριθμητικής, με το οποίο ο Ευκλείδης είχε αποδείξει το άπειρο πλήθος των πρώτων αριθμών. Η 3^η στήλη που εισήγαγε ο Gauss στον πίνακα δεν ήταν αυτή που είχε πετύχει κάνοντας το λόγο $\pi(x)/x$, αλλά το αντίστροφο $x/\pi(x)$.

x	$\pi(x)$	$x/\pi(x)$
10	4	2,5
100	25	4
1.000	168	6
10.000	1.229	8,1
100.000	9.592	10,4
1.000.000	78.498	12,7
10.000.000	664.579	15
100.000.000	5.761.455	17,4
1.000.000.000	50.847.534	19,7
10.000.000.000	455.052.512	22

Αυτός ο πίνακας, δείχνει ότι **μεταξύ των 100 πρώτων αριθμών, ένας κάθε 4 είναι πρώτος.** Ότι **μεταξύ των 1.000 πρώτων αριθμών, περίπου ένας κάθε 6 είναι πρώτος**, και ούτω καθεξής. Αυτή είναι απλά μια εκτίμηση. Ο πίνακας δεν δηλώνει ότι μεταξύ των πρώτων 100 αριθμών εμφανίζεται ένας πρώτος αριθμός κάθε 4

αριθμούς, το οποίο μπορούμε να επαληθεύσουμε με σύντομο τρόπο από το κόσκινο του Ερατοσθένη, για τους πρώτους 100 αριθμούς. Έτσι, ο προηγούμενος πίνακας μάλλον πρέπει να ερμηνεύεται ως μια πιθανή απόσταση μεταξύ πρώτων αριθμών. Ο Gauss, παρατήρησε ότι η 1^η στήλη αυξανόταν περίπου κατά δύο μονάδες κάθε φορά που προχωρούσε μια γραμμή. Έτσι, η κατάσταση είχε ως εξής, αν πολλαπλασιάζε επί 10 την 1^η σειρά, έπρεπε να προσθέσει 2 στη 2^η σειρά. Αυτή η σχέση μεταξύ γινομένου και αθροίσματος, ήταν εγγενής των λογαρίθμων. Ο Gauss, είχε στα χέρια του έναν πίνακα λογαρίθμων και έναν πίνακα πρώτων αριθμών στον ίδιο τόμο. Αυτό, του έδωσε την ιδέα να χρησιμοποιήσει ένα διαφορετικό εργαλείο, ένα νέο μέσο παρατήρησης. Οι λογάριθμοι, θα γίνονταν ο νέος φακός που ο Gauss θα προσάρμοζε στο τηλεσκόπιο του. Όταν η βάση των λογαρίθμων είναι το 10, κάθε φορά που πολλαπλασιάζουμε επί 10, οι δεκαδικοί λογάριθμοι αυξάνονται ένας-ένας, για αυτό και η βάση αυτή δεν λειτουργούσε καλά στο σχήμα του Gauss και αποφάσισε να πάρει λογάριθμους με βάση e , έναν αριθμό με παρόμοια χαρακτηριστικά με εκείνα του αριθμού π . Η τιμή του κατά προσέγγιση είναι $e = 2,7\ 1828\ 1828\ 4590452354...$

Πρόκειται για μια έκφραση με άπειρα δεκαδικά ψηφία και εμφανίζεται στα μαθηματικά με την ίδια ή μεγαλύτερη συχνότητα του αριθμού π , για αυτό όταν λαμβάνεται ένας λογάριθμος με βάση e λέμε ότι έχουμε να κάνουμε με «φυσικούς λογάριθμους». Κατά συνέπεια, θα έπρεπε να γράφουμε **log**, για να συμβολίσουμε τους φυσικούς λογάριθμους. Ωστόσο, γράφονται συντομογραφικά ως **«ln»**. Στις επιστημονικές υπολογιστικές μηχανές υπάρχει ένα πλήκτρο «log», για δεκαδικό λογάριθμο και ένα «ln», για λογάριθμο με βάση e .

Η εικασία που έκανε ο Gauss, με αφετηρία το συγκεκριμένο σημείο, ήταν η ακόλουθη **«Για μεγάλες τιμές του x , η τιμή $\pi(x)/x$ προσεγγίζει τον λόγο $1/\ln x$ »** το οποίο αν αποδιδόταν διαφορετικά θα είχε την μορφή $\pi(x)/x \approx 1/\ln x$ (για μεγάλες τιμές του x). Αυτό το αποτέλεσμα, δίνει μια εκτίμηση της συχνότητας με την οποία εμφανίζονται οι πρώτοι αριθμοί στην ακολουθία των φυσικών αριθμών. Έστω ότι $P(N)$ είναι ο αριθμός των πρώτων που είναι μικρότεροι του N . Ο τύπος, δηλώνει ότι όσο αυξάνει το N , ο λόγος $N/P(N)$ πλησιάζει όλο και περισσότερο προς τον φυσικό λογάριθμο N . Υπάρχει ένας απλός τρόπος να εφαρμόσουμε πρακτικά τον τύπο του Gauss, όταν θέλουμε να μάθουμε πόσοι πρώτοι αριθμοί είναι μικρότεροι ενός δεδομένου αριθμού. Για παράδειγμα, ας υποθέσουμε ότι κάποιος μας κάνει την εξής ερώτηση: **Πόσοι αριθμοί νομίζεις ότι υπάρχουν μεταξύ των πρώτων 1.000 αριθμών;** Παίρνουμε μια αριθμομηχανή τσέπης και κάνουμε τα εξής βήματα:

- Εισάγουμε τον αριθμό 1.000,
- Πατάμε το πλήκτρο $\ln$,
- Ύστερα πατάμε το πλήκτρο $1/x$
- Πολλαπλασιάζουμε το αποτέλεσμα επί 1.000 και εμφανίζεται ο αριθμός 144,76482730108394255037630630554, που μας επιτρέπει να απαντήσουμε καταφατικά στην ερώτηση **«Υπάρχουν άραγε περίπου 145 πρώτοι αριθμοί μεταξύ του 1 και του 1.000;»** Η προσέγγιση δεν είναι θαυμαστό γεγονός γιατί, στην πραγματικότητα, υπάρχουν **168**. Αλλά ας μην ξεχνάμε ότι το θεώρημα τελειοποιείται όσο ο αριθμός N μεγαλώνει και μας επιτρέπει να δηλώσουμε με σιγουριά, για παράδειγμα, ότι μόνο το 3,6% του 1^{ου} δισεκατομμυρίου των αριθμών είναι πρώτοι.

Τώρα πλέον μπορούμε να αποκωδικοποιήσουμε αυτό που ο Gauss ήθελε να πει όταν έγραψε **«Πρώτοι αριθμοί μικρότεροι του a ($=\infty$) a/la »** στο σημειωματάριό του «πρώτοι αριθμοί μικρότεροι του a » σημαίνει το ίδιο με $\pi(a)$. Το « la » είναι αυτό που βάλαμε ως $\ln a$. Το « $=\infty$ » σημαίνει ότι η ισότητα είναι έγκυρη για τιμές πολύ μεγαλύτερες του a (όταν ο a τείνει στο άπειρο). Σήμερα, αυτό το αποτέλεσμα είναι γνωστό ως **θεώρημα των πρώτων αριθμών** και είναι ένα από τα σημαντικότερα

στην ιστορία των μαθηματικών. Ο Gauss δεν γνωστοποίησε αυτό το αποτέλεσμα. Όχι εξαιτίας κάποιας μικροπρεπούς επιφύλαξης, όπως συνηθιζόταν σε πολλούς τομείς της επιστήμης, ούτε και της άποψης του Fermat, που είχε αναφέρει ότι δεν θα περιελάμβανε στην απόδειξη λόγω του ότι ήταν μακροσκελής, ο Gauss διέθετε αρκετό χαρτί για να περιλάβει οποιανδήποτε απόδειξη, όσο μακροσκελής και αν ήταν. **Δεν γνωστοποίησε αυτό το θεώρημα ακριβώς γιατί δεν είχε κανένα τρόπο να το αποδείξει.** Τα μαθηματικά, είχαν κάνει μια στροφή με την υποστήριξη του Euler. Η μαθηματική θεωρία, έπρεπε να διαρθρώνεται αναντίρρητα εντός ενός λογικού πλαισίου, που είχε αρχίσει να παραμερίζει αμφιλεγόμενες τεχνικές και αμφίβολους πραγματισμούς.

Η διαίσθηση, ραχοκοκαλιά κάθε ανακάλυψης, έπρεπε να στηρίζεται σε στερεές θεωρητικές βάσεις. Η απόδειξη ενός θεωρήματος, είχε μετατραπεί σε αντικειμενική επιχειρηματολογία η οποία, χάρη σε μια κοινή γλώσσα, αποκτούσε υπόσταση αλήθειας. Η εικασία του Gauss, δεν θα μετατρεπόταν σε θεώρημα παρά μόνο 100 έτη αργότερα, το **1896** ο **Jacques Hadamard** (1865–1963) και ο **Vallee Poussin** (1866–1962) απέδειξαν το θεώρημα ταυτόχρονα, αλλά χωριστά, οπότε η αναγνώριση αξίζει και στους δύο. Μεταξύ των πολλών θεωρημάτων που διατυπώθηκαν γύρω από τους πρώτους αριθμούς, αυτό που ξεκίνησε με την εικασία του Gauss κατέχει τιμητική θέση στην ιστορία των μαθηματικών για την τεράστια σημασία του στη μετέπειτα ανάπτυξη της έρευνας των πρώτων αριθμών.

13. Σε τι χρησιμεύουν οι πρώτοι αριθμοί;

Η εύρεση μεγάλων πρώτων αριθμών, δεν είναι κάτι απλό διότι δεν έχει κατορθώσει κανείς ακόμα να βρει τον τύπο, τον αλγόριθμο που θα μας επιτρέψει να κατασκευάσουμε πρώτους αριθμούς κατά βούληση. Μπροστά σε αυτή την κατάσταση, κάποιοι μπορεί να αναρωτηθούν «Για ποιόν λόγο θέλουμε να κατασκευάσουμε πρώτους αριθμούς;». Υπάρχουν δύο απαντήσεις. Η 1^η απάντηση είναι επειδή παρουσιάζει θεωρητικό ενδιαφέρον.

Η προσπάθεια, προωθεί τη χρήση ενδιαφερόντων εργαλείων λογισμού, ειδικά πληροφορικού λογισμού. Επιπλέον, το να διαθέτει κανείς τεράστιες λίστες πρώτων αριθμών είναι κάτι που χρειάζεται για την επαλήθευση θεωρημάτων που ακόμη δεν έχουν αποδειχθεί. Αν κάποιος διατυπώσει μια εικασία σχετικά με τους πρώτους αριθμούς και μπορεί να επαληθεύσει ότι υπάρχει ένας πρώτος αριθμός, ακόμη και αν αποτελείται από εκατομμύρια ψηφία, που δεν την ικανοποιεί, το ζήτημα έχει λήξει.

Έτσι, ξεκίνησε μια φρενήρης αναζήτηση πρώτων αριθμών όλων των ομάδων (του Mersenne, διδύμων κλπ.), που σε ορισμένες περιπτώσεις έλαβε χαρακτήρα ανταγωνιστικό, που ανήκει στον κόσμο των ρεκόρ και των μεγάλων επάθλων. Υπάρχει όμως και ένας άλλος, 2^{ος} πρακτικός λόγος, που συνδέεται στενά με τα εμπονομαζόμενα κρυπτογραφικά κλειδιά όπως το **ηλεκτρονικό ταχυδρομείο**, τις **τραπεζικές συναλλαγές**, τις **πιστωτικές κάρτες** ή τις **επικοινωνίες μέσω κινητής τηλεφωνίας** που προστατεύονται μέσω μυστικών κλειδιών τα οποία βασίζονται απευθείας στις ιδιότητες των πρώτων αριθμών.

14. Οι πρώτοι αριθμοί στην κρυπτογραφία

Το **1975**, οι **W. Diffie** και **M. Hellman**, του πανεπιστημίου του Stanford, ανέπτυξαν την ιδέα της **ασύμμετρης κρυπτογράφησης** ή του «δημόσιου κλειδιού», ενός συστήματος βασισμένου σε καθορισμένες μαθηματικές συναρτήσεις, τις αποκαλούμενες «μιας μόνο κατεύθυνσης» ή «συναρτήσεις παγίδας», οι οποίες επιτρέπουν την κωδικοποίηση, αλλά καθιστούν εικονικά αδύνατη την αποκωδικοποίηση αν δεν είναι γνωστό το κλειδί. Η ιδέα είναι κάθε χρήστης να

διαθέτει δύο κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Αν θέλω να στείλω ένα μήνυμα σε κάποιον, κρυπτογραφώ το μήνυμα σύμφωνα με το κλειδί του που είναι δημόσιο, με την έννοια ότι οποιοσδήποτε μπορεί να το γνωρίζει, αλλά μόνο αυτός, με το ιδιωτικό κλειδί του, μπορεί να το αποκρυπτογραφήσει. Ένα από τα πλεονεκτήματα αυτής της μεθόδου είναι ότι **το ιδιωτικό κλειδί δεν κυκλοφορεί ποτέ στα μέσα επικοινωνίας** και, ως εκ τούτου, δεν χρειάζεται διαρκώς ανανέωση.

Δεν πρόκειται για απλό ζήτημα, ωστόσο μπορούμε να προσπαθήσουμε να το καταλάβουμε μέσω μιας αναλογίας. Ας φανταστούμε μια αποθήκη χρωμάτων στην οποία διαθέτουμε εκατοντάδες χιλιάδες κουτιά με διάφορα χρώματα. Παίρνουμε δύο οποιαδήποτε κουτιά και δημιουργούμε ένα μίγμα με διάφορες ποσότητες μπογιάς από κάθε κουτί. Μέχρι εδώ, η διαδικασία είναι απλή. Ωστόσο, αν τώρα δείξουμε το αποτέλεσμα σε κάποιον και του ζητήσουμε να «αποκρυπτογραφήσει» τις ποσότητες από κάθε χρώμα που χρησιμοποιήθηκαν στο τελικό μίγμα, θα του θέσουμε ένα δισεπίλυτο πρόβλημα. Αυτός είναι ο μηχανισμός των μαθηματικών **συναρτήσεων παγίδας ή μιας μόνο κατεύθυνσης**, στις οποίες είναι πολύ εύκολο να «πάμε» αλλά πρακτικά αδύνατο να «γυρίσουμε». Έστω ότι σε μια αποθήκη, αντί για κουτιά με χρώματα, έχουμε πρώτους αριθμούς. Ας πάρουμε δύο στην τύχη, για παράδειγμα, 7 και 13 και ας τους πολλαπλασιάσουμε, διαδικασία ανάλογη με την ανάμειξη των κουτιών με τα χρώματα, με αποτέλεσμα $7 \cdot 13 = 91$. Το ερώτημα που τίθεται είναι «Μπορούμε να μάθουμε ποιοι δύο πρώτοι αριθμοί πολλαπλασιαζόμενοι μεταξύ τους δίνουν 91 ως αποτέλεσμα;» Βασικά, πρέπει να έχουμε μια λίστα πρώτων αριθμών και να συνεχίσουμε να κάνουμε δοκιμές. Το πράγμα φαίνεται απλό, όπως θα ήταν άλλωστε και το να εξακριβώσουμε τα χρώματα που αποτελούν το μίγμα χρωμάτων αν στην αποθήκη δεν υπήρχαν περισσότερα από μια δωδεκάδα βασικά χρώματα. Εντούτοις, κάτι τέτοιο δεν ισχύει, κυρίως στην περίπτωση των πρώτων αριθμών.

Το να επαληθεύσουμε, για παράδειγμα, ότι ο αριθμός 1.409.305.684.859 είναι το αποτέλεσμα πολλαπλασιασμού των δύο πρώτων αριθμών 705.967 και 1.996.277 μπορεί να δοκιμάσει την υπομονή του οποιουδήποτε, προ πάντων αν ληφθεί υπόψη ότι αυτοί οι δύο πρώτοι αριθμοί έχουν εξαχθεί από λίστα στην οποία εμφανίζονται μόνο όλοι όσοι αριθμοί υπάρχουν μεταξύ του 1 και του 2.000.000, που είναι ο επιβλητικός αριθμός 148.933. Παρ' όλα αυτά, όπως επιμένουμε να λέμε, ζούμε στην εποχή της πληροφορικής και αυτό είναι ένα ζήτημα το οποίο, κατ' αρχήν, ένα καλό πρόγραμμα εγκατεστημένο σε έναν δυνατό υπολογιστή μπορεί να το λύσει σε σύντομο χρόνο αλλά μέχρι ένα σημείο, αφού όλα εξαρτώνται από το πόσο μεγάλη είναι η αποθήκη των χρωμάτων και πρέπει να επιμένουμε στο ότι η αποθήκη των πρώτων αριθμών είναι όχι απλώς μεγάλη, αλλά άπειρη.

Το ζεύγος των πρώτων αριθμών του προηγούμενου παραδείγματος είχε λίγα ψηφία. Αν ληφθούν πρώτοι με 100 ψηφία ο καθένας, ο χρόνος αναμονής εκείνου του προγράμματος του υπολογιστή, που στο τέλος-τέλος αναζητά τους αριθμούς «απερίσκεπτα» ή, όπως λέγεται και στην ιδιόλεκτο της κρυπτογραφίας, μέσω μιας επίθεσης «ωμής βίας», μπορεί να ξεπεράσει τον χρόνο ζωής επί της Γης.

Αν ισχύει πως οι πρώτοι αριθμοί έχουν μπει ολοκληρωτικά στην καθημερινή μας ζωή, μέσω της πιστωτικής κάρτας ή του προσωπικού υπολογιστή, τότε πρέπει να υπάρχει απαραίτητα και ζήτηση πρώτων αριθμών, αφού για να κατασκευαστεί ένα μυστικό κλειδί χρειάζονται δύο πρώτοι. Υπάρχει μια «αγορά» πρώτων αριθμών που διαθέτει ευρείας κλίμακας παραγωγή μεγάλων πρώτων αριθμών, αλλά σε αυτά τα ζητήματα είναι τόσο σημαντική η παραγωγή όσο και ο ποιοτικός έλεγχος. **Προκειμένου να αναγνωριστεί ένας πολύ μεγάλος αριθμός ως πρώτος, πρέπει να έχει δοκιμαστεί από κάποιον επίσημα αναγνωρισμένο οργανισμό.** Το σύστημα **RSA** δημοσιεύτηκε το **1978**, αλλά η γενικευμένη του χρήση ως κρυπτογραφικό κλειδί

δεν έλαβε χώρα μέχρι τα τέλη της δεκαετίας του 1990, με την καθιέρωση του διαδικτύου. Ο προσδιορισμός των μεγάλων πρώτων αριθμών ήταν δύσκολος, αφού απαιτούσε ένα πολύ συγκεκριμένο λογισμικό. Για τον λόγο αυτό, τους αγόραζαν από ειδικευμένες εταιρίες ή από πανεπιστημιακά τμήματα τα οποία τους διέθεταν, ως αποτέλεσμα των ερευνών τους. Αλλά η εκθετική αύξηση της υπολογιστικής ικανότητας των υπολογιστών μαζί με τη σταθερή εμφάνιση των πλέον εξελιγμένων αλγορίθμων εφαρμογής, μετέβαλε την αγορά των πρώτων αριθμών οπότε σε σύντομο χρονικό διάστημα, η απόκτησή τους έγινε πολύ πιο προσιτή.

15. Μέγιστη ασφάλεια

Η κυβέρνηση των ΗΠΑ, επιτρέπει την χρησιμοποίηση μόνο συγκεκριμένων κρυπτογραφικών κλειδίων στην επικράτειά της και στον Καναδά. Εκτός των συνόρων δεν επιτρέπει την πώληση, εκτός και αν πρόκειται για χρηματοπιστωτικό ίδρυμα. Η μη εξουσιοδοτημένη εξαγωγή στάνταρ κωδικοποίησης, θεωρείται όπως το λαθρεμπόριο όπλων. Οι επιχειρήσεις που ασχολούνται με την κατασκευή προγραμμάτων κωδικοποίησης, αποθηκεύουν τα μυστικά κλειδιά σε «παστίλιες» που είναι εφοδιασμένες με εξελιγμένα συστήματα ασφαλείας. Όταν ανοίγουν καθώς έρχονται σε επαφή με το οξυγόνο, στερεοποιούνται σε μια άμορφη μάζα. Αν προσπαθήσουμε να τις διαβάσουμε με ακτίνες X, όλα όσα είναι γραμμένα σε αυτές μετατρέπονται σε μηδενικά.

16. Κατασκευή των πρώτων αριθμών

Είναι σύνηθες φαινόμενο κάποιος που δεν έχει μεγάλο μαθηματικό υπόβαθρο, να πανηγυρίζει ότι έχει βρει (σχεδόν πάντα στο διαδίκτυο) ένα σύστημα ή έναν τύπο ώστε να επαληθεύσει ποιος είναι ο επόμενος πρώτος αριθμός, για έναν φυσικό αριθμό n . Αρκεί να σκεφτούμε ότι μια είδηση αυτού του διαμετρήματος δε θα αποτελούσε αντικείμενο αναζήτησης αφού, δεδομένων των επιπτώσεών της, αν κάποιος είχε βρει το μαγικό τύπο και τον είχε γνωστοποιήσει θα κυριαρχούσε στις πρώτες σελίδες των εφημερίδων και των ενημερωτικών φυλλαδίων όλου του κόσμου.

Υπάρχουν πολλά γεωμετρικά μοντέλα για να βρίσκουμε πρώτους αριθμούς. Μερικές φορές, μπορούν να παραπλανήσουν τους απρόσεκτους, επειδή παρουσιάζονται ως τύποι που επιτρέπουν την εύρεση όλων των πρώτων αριθμών, όταν στην πραγματικότητα δεν είναι τίποτα περισσότερο από παραλλαγές του κόσκινου του Ερατοσθένη ή διαφορετικοί τρόποι δημιουργίας του κόσκινου μέσω γεωμετρικών μεθόδων. Και η αλήθεια είναι ότι υπάρχουν κάποια πραγματικά ευφυή μοντέλα. Ένα από τα πιο ενδιαφέροντα μοντέλα είναι αυτό που δημιούργησαν οι Ρώσοι μαθηματικοί **Yuri Matiyasevich** (1947–) και **Boris Stechkin** (1920–1995) κάνοντας χρήση μιας παραβολής. Η εν λόγω παραβολή παρουσιάζεται με τους δύο κλάδους της και στον άξονά της γράφεται η ακολουθία των φυσικών αριθμών. Ύστερα υψώνεται μια κάθετος που αντιστοιχεί με το τετράγωνο κάθε αριθμού, δηλαδή, στη θέση όπου βρίσκεται το 4 υψώνεται η κάθετος που αντιστοιχεί, σε καθένα από τους δύο κλάδους της καμπύλης, με τον αριθμό 2. Η γεωμετρική σημασία της καθέτου είναι ότι, βγήκε το γινόμενο του 2 επί τον εαυτό του. Με τον ίδιο τρόπο, θα είχαμε και άλλη κάθετος για να συμβολίσουμε το γινόμενο του 3 επί τον εαυτό του και θα την υψώναμε στο σημείο 9 του άξονα και ούτω καθεξής. Όταν πια έχουμε όλους αυτούς τους αριθμούς που παριστάνονται από σημεία στην παραβολή, ενώνουμε κάθε σημείο ενός κλάδου με όλα τα σημεία του άλλου κλάδου. Ήτοι, το σημείο 2 του άνω κλάδου το ενώνουμε με το 2, 3, 4, 5... του κάτω κλάδου. Κάθε ένα από αυτά τα τμήματα τέμνει τον άξονα στο αντίστοιχο γινόμενο. Αν ολοκληρωθούν όλες οι δυνατές τομές, τα μοναδικά σημεία της παραβολής από τα οποία δεν διέρχεται

κανένα τμήμα είναι ακριβώς πρώτοι αριθμοί. Τα κόσκινα αλγεβρικού τύπου, είναι πιο κατάλληλα σχεδιασμένα για να βρίσκουν γρήγορους υπολογιστικούς αλγόριθμους.

Ένα από αυτά είναι το **κόσκινο του Atkin**, που επινόησαν ο **Atkin** και ο **Daniel J. Bernstein**, το οποίο επιτρέπει την εύρεση όλων των πρώτων αριθμών που είναι μικρότεροι ή ίσοι από δεδομένο φυσικό αριθμό. Από ορισμένες απόψεις, πρόκειται για εξελιγμένη μορφή του κόσκινου του Ερατοσθένη. Όταν λέμε «εξελιγμένη μορφή» αναφερόμαστε μάλλον σε ενημέρωσή του, καθώς το κόσκινο του Atkin, από αριθμητική σκοπιά, παρουσιάζει κάποιες ελλείψεις σε σχέση με εκείνο του Ερατοσθένη, δεδομένου ότι αιτείται μια προηγούμενη προετοιμασία και δεν εξαλείφει τα πολλαπλάσια των πρώτων αριθμών, αλλά μόνο τα πολλαπλάσια των τετραγώνων των πρώτων.

Ήδη γνωρίζουμε ότι το ιδανικό θα ήταν να μπορούσαμε να βρούμε έναν τύπο που να συνδέει κάθε φυσικό αριθμό n τον νιοστό πρώτο αριθμό. Έχουμε δει ότι οι μαθηματικοί αναζητούν πάνω από 3.000 έτη τον εν λόγω τύπο. Εκείνο που σίγουρα υπάρχει, είναι οι συναρτήσεις οι οποίες επιτρέπουν να υπολογίσουμε με πρακτικό τρόπο πρώτους αριθμούς. Για παράδειγμα, αποδεικνύεται (**θεώρημα de Wilson**) ότι ο p είναι ένας πρώτος αριθμός αν και μόνο αν $(p-1)! \equiv -1 \pmod{p}$, όμως, οποιοσδήποτε τύπος που περικλείει παραγοντικά δεν είναι εφικτός τη στιγμή εγκατάστασης ενός αλγόριθμου σε έναν υπολογιστή, λόγω της γρήγορης αύξησης της συνάρτησης η οποία εκτελεί υπερβολικά μεγάλους χρόνους υπολογισμού. Υπάρχουν επίσης πολυώνυμα που «κατασκευάζουν» πρώτους αριθμούς, όπως αυτό που χρησιμοποίησε ο Euler για να υπολογίσει μια λίστα σαράντα πρώτων αριθμών μέσω της συνάρτησης $f(x) = x^2 + x + 41$, η οποία παρέχει πρώτους αριθμούς δίνοντας τιμές στον x . Για παράδειγμα

$$\text{Αν } x=0, \text{ τότε } f(0)=0+0+41=41,$$

$$\text{Αν } x=1, \text{ τότε } f(1)=1+1+41=43,$$

$$\text{Αν } x=2, \text{ τότε } f(2)=4+2+41=47.$$

Ωστόσο, ο τύπος αρχίζει να παρουσιάζει σφάλμα για τιμές του x μεγαλύτερες του 41. Για παράδειγμα, για την τιμή $x=41$, η έκφραση δίνει αποτέλεσμα έναν αριθμό σύνθετο $f(41)=1.681+41+41=1.763$. Ο Euler, συνέχισε τις έρευνες γύρω από το εν λόγω πολυώνυμο και οδηγήθηκε στο συμπέρασμα ότι ένα πιο γενικό πολυώνυμο, όπως το $x^2 - x + q$, θα μπορούσε να δώσει πρώτους αριθμούς για τιμές του x που περιλαμβάνονται μεταξύ 0 και $(q-2)$.

Υπάρχουν πολυώνυμα, όπως αυτό που ανακάλυψαν οι **Jones, Sata, Wada** και **Wiens** το 1976, που έδωσαν μόνο πρώτους αριθμούς όταν δίνει κανείς τιμές στις μεταβλητές τους. Πρόκειται για ένα πολυώνυμο 28 μεταβλητών με κάπως δυσανάλογη περιπλοκότητα. Δεν έχει μεγάλο πρακτικό ενδιαφέρον, όταν η παραγόμενη τιμή είναι θετική, πρόκειται πάντα για έναν πρώτο αριθμό, αλλά τις περισσότερες φορές, για να μην πούμε σχεδόν όλες, το αποτέλεσμα είναι αρνητικός αριθμός. Σήμερα, το μεγαλύτερο μέρος των γνωστών πρώτων αριθμών (σε αυτή την περίπτωση μιλάμε πάντα για μεγάλους πρώτους αριθμούς) είναι οι αποκαλούμενοι πρώτοι του Mersenne. Αυτό οφείλεται στο ότι υπάρχει ένα τεστ ιδιότητας πρώτου αριθμού ή τεστ των **Lucas – Lehmer**, που λειτουργεί πολύ καλά με αυτό το είδος αριθμών. Ένας αριθμός του Mersenne είναι της μορφής $2^n - 1$. Όταν ο n εν λόγω αριθμός είναι πρώτος, τότε μιλάμε για ένα «πρώτο του Mersenne».

Μέχρι τις 10.06.2009 ήταν γνωστοί μόνο 47 πρώτοι αριθμοί του Mersenne. Ο μεγαλύτερος από αυτούς είναι ο $2^{45112000} - 1$, που έχει σχεδόν δεκατρία εκατομμύρια ψηφία.

17. Πώς γνωρίζουμε αν ένας αριθμός είναι πρώτος;

Ο μόνος τρόπος να το μάθουμε με απόλυτη ακρίβεια είναι να τον διαιρέσουμε με όλους τους προηγούμενους του αριθμούς. Αν δεν διαιρείται με κανέναν από αυτούς, τότε είναι πρώτος. Γνωρίζουμε ότι, μπορούμε να σταματήσουμε στην τετραγωνική ρίζα του εν λόγω αριθμού. Για μικρούς αριθμούς και υπολογισμούς που γίνονται στο χέρι, είναι μια καλή μέθοδος. Για παράδειγμα, θα επαληθεύσουμε αν ο αριθμός 101 είναι πρώτος ή σύνθετος. Για αυτό, το να γνωρίζουμε τα κριτήρια διαιρετότητας μπορεί να μας προφυλάξει από κάποιους μη απαραίτητους υπολογισμούς. Ήδη γνωρίζουμε ότι το 101 δεν διαιρείται δια του 2, γιατί θα έπρεπε να λήγει σε 0 ή σε άρτιο ψηφίο. Ούτε και δια του 3 διαιρείται, αφού το άθροισμα των ψηφίων του δεν διαιρείται δια του 3 ($1+0+1=2$). Επίσης δεν διαιρείται δια του 5 διότι θα έπρεπε να λήγει σε 0 ή σε 5. Επίσης, μπορούμε να παραλείψουμε το 4, το 6 και το 9, αφού όλα είναι πολλαπλάσια του 2 ή του 3. Αν δοκιμάσουμε με το 7, μας δίνει πηλίκο 14 και υπόλοιπο 3, οπότε δεν διαιρείται με το 7. Ο επόμενος αριθμός που πρέπει να δοκιμάσουμε είναι το 11 (προφανώς το 101 δεν είναι πολλαπλάσιο του 10). Η διαίρεση δια του 11 δίνει πηλίκο 9 και υπόλοιπο 2.

Εδώ πλέον μπορούμε να σταματήσουμε και να δηλώσουμε ότι το 101 είναι ένας πρώτος αριθμός, καθώς η τετραγωνική ρίζα του 101 είναι περίπου 10, γεγονός που μας εξασφαλίζει με βεβαιότητα ότι δεν θα διαιρείται με κανέναν από τους αριθμούς που υπολείπονται μέχρι το 101. Αυτή η μέθοδος, είναι γνωστή με το όνομα «δοκιμαστική διαίρεση» και είναι η πιο απλή και σίγουρη από όλες. Μόνο που δεν μπορεί να εφαρμοστεί για πολύ μεγάλους αριθμούς, ούτε μέσω των μεθόδων της πληροφορικής. Ας σκεφτούμε ότι ένας αριθμός 50 ψηφίων θα απαιτούσε τον υπολογισμό τουλάχιστον της τάξης των 25 ψηφίων, που θα ήταν αυτός που θα αντιστοιχούσε λίγο ως πολύ στην τετραγωνική του ρίζα. Σε έναν υπολογιστή με ικανότητα εκτέλεσης ενός δισεκατομμυρίου διαιρέσεων ανά δευτερόλεπτο, θα χρειαζόμασταν πολλά περισσότερα από 300.000.000 έτη για να ολοκληρώσουμε τον υπολογισμό και ως τότε το πιθανότερο είναι να εξαφανιστεί το ανθρώπινο γένος.

Εντούτοις, πρέπει να επισημάνουμε ότι η μέθοδος μπορεί να λειτουργήσει αν πρόκειται για έναν σύνθετο αριθμό και έναν από τους παράγοντές του που δεν είναι υπερβολικά μεγάλος. Πρέπει να έχουμε υπόψη μας ότι, δοθέντος ενός οποιουδήποτε αριθμού n , η πιθανότητα ο αριθμός 2 να είναι παράγοντας του είναι 50%, η πιθανότητα ο 3 να είναι παράγοντας του είναι 33% και ούτω καθεξής.

Από την άλλη πλευρά, οι σύγχρονοι υπολογιστές έχουν κερδίσει αρκετά σε ταχύτητα και ικανότητα μνήμης, προκειμένου η αναζήτηση ενός πρώτου αριθμού σε μια μακρά λίστα να καταστεί σε ορισμένες περιπτώσεις αποτελεσματικότερη από την περίπλοκη διαδικασία επαλήθευσης του κατά πόσον ένας δεδομένος αριθμός είναι πρώτος.

Βιβλιογραφία

- Crandall, R. (1961). “Prime numbers: A computational perspective”, Springer
- Gracian, E. (2011). «Οι πρώτοι αριθμοί», Αθήνα, εκδόσεις 4π
- Wells, D. (2005). “Prime numbers: The most mysterious figures in math”, 1st edition, Trade paper press
- Ευκλείδη «Στοιχεία, βιβλίο IX», Αθήνα, ΟΕΔΒ