

ΑΕΝ Ασπροπύργου
Σχολή Μηχανικών

Πτυχιακή εργασία

Οι πρώτοι αριθμοί

Σπουδαστής: Κολοβός Φώτιος (ΑΜ 7884)

Τί σημαίνει πρώτος αριθμός;

- Στα μαθηματικά, πρώτος αριθμός (ή απλά πρώτος) είναι ένας φυσικός αριθμός **μεγαλύτερος της μονάδας** με την ιδιότητα οι μόνοι φυσικοί διαιρέτες του να είναι η μονάδα και ο εαυτός του.
- Οι πρώτοι αριθμοί είναι ένα από τα αντικείμενα της **θεωρίας αριθμών** και είναι μια πολύ ενεργή ερευνητικά περιοχή των μαθηματικών.
- Χρησιμοποιούνται σε πολλούς τομείς στην τεχνολογία πληροφοριών, όπως το **ηλεκτρονικό ταχυδρομείο**, οι **τραπεζικές συναλλαγές**, οι **πιστωτικές κάρτες** ή οι **επικοινωνίες μέσω κινητής τηλεφωνία**, τα οποία προστατεύονται μέσω μυστικών κλειδιών, που βασίζονται απευθείας στις ιδιότητες των πρώτων αριθμών.

Το κόσκινο του Ερατοσθένη 1/3

- Η παραγωγή πρώτων αριθμών υπήρξε και εξακολουθεί να είναι ένα θέμα πραγματικά ακανθώδες.
- 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 100 πρώτων φυσικών αριθμών.

Το κόσκινο του Ερατοσθένη 2/3

- Πρώτα – πρώτα κατασκευάζουμε έναν πίνακα με όλους τους φυσικούς αριθμούς από το 1 έως το 100.
- Ξεκινάμε απαλείφοντας τους πολλαπλάσιους του δύο, δηλαδή το 4, το 6, το 8, το 10..., ύστερα εκείνους που είναι πολλαπλάσιοι του τρία (αυτό έχει ήδη απαλειφθεί), το 9, το 12, το 15...
- Θα ακολουθήσουν τα πολλαπλάσια του 5 και ύστερα του 7. Οι αριθμοί που απέμειναν είναι όλοι τους πρώτοι.
- Η εν λόγω μέθοδος εξακολουθεί να εφαρμόζεται ως τις ημέρες μας, χιλιάδες χρόνια μετά από την εκπόνησή της, προκειμένου να βρίσκουμε μικρούς πρώτους, μικρότερους από τον αριθμό δέκα δισεκατομμύρια.

Το κόσκινο του Ερατοσθένη

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

Δίδυμοι πρώτοι αριθμοί 1/2

- 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 δεν 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 εκατό 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)

Δίδυμοι πρώτοι αριθμοί 2/2

Αυτά τα ζεύγη ονομάζονται «δίδυμοι πρώτοι» ή, απλώς «δίδυμοι». Γνωρίζουμε ότι, οι δίδυμοι πρώτοι **αρχίζουν να σπανίζουν όσο προχωρά η σειρά των φυσικών αριθμών**.

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.

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 πρόλογό του, ο Mersenne δηλώνει ότι μεταξύ όλων των πρώτων αριθμών που υπάρχουν ανάμεσα στο 1 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.

Οι εν λόγω αριθμοί 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.

Το μικρό θεώρημα του Fermat

- Το θεώρημα δηλώνει ότι αν το p είναι ένας πρώτος αριθμός και είναι a ένας άλλος οποιοσδήποτε αριθμός, έτσι ώστε a, 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 $504/3 = 168$.
- Να τονίσουμε ότι το μικρό θεώρημα του Fermat **αποτελεί μια μέθοδο για να μάθουμε αν ένας αριθμός δεν είναι πρώτος χωρίς να χρειάζεται να βρούμε κάποιον παράγοντα του.**

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 σαν άθροισμα δύο πρώτων αριθμών**».
- Στην έκφραση «άθροισμα δύο πρώτων» συμπεριλαμβάνεται η περίπτωση επανάληψης ενός πρώτου αριθμού δύο φορές. Για παράδειγμα **$4=2+2$, $6=3+3$, $8=3+5$, $10=3+7$, $12=5+7$, $14=3+11$** . 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**.

Οι πρώτοι αριθμοί στην κρυπτογραφία 1/2

- Για ένα μεγάλο χρονικό διάστημα, οι πρώτοι αριθμοί θεωρούνταν ότι είχαν εξαιρετικά περιορισμένη εφαρμογή έξω από τα καθαρά μαθηματικά.
- Αυτό άλλαξε τη **δεκαετία του 1970**, όταν οι έννοιες της κρυπτογραφίας δημοσίου κλειδιού ανακαλύφθηκαν και σε αυτή την κρυπτογράφηση, οι πρώτοι αριθμοί αποτελούσαν τη βάση των πρώτων αλγορίθμων, όπως στον **κρυπτογραφικό αλγόριθμο RSA**.

Οι πρώτοι αριθμοί στην κρυπτογραφία 2/2

- 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 μεγάλων πρώτων αριθμών ήταν δύσκολος, αφού απαιτούσε ένα **πολύ συγκεκριμένο λογισμικό**. Για το λόγο αυτό τους αγόραζαν από ειδικευμένες εταιρίες ή 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, σε σύντομο χρονικό διάστημα η απόκτησή τους έγινε πολύ πιο προσιτή.