ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΑΛΓΟΡΙΘΜΟΙ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗΣ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
ΗΛΙΟΠΟΥΛΟΣ ΔΗΜΗΤΡΙΟΣ
Α.Μ. 09104095

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ: Παπαϊωάννου Αλέξανδρος (Επιβλέπων)
Αναπληρωτής Καθηγητής Ε.Μ.Π.
Κουκουβίνος Χρήστος Καθηγητής Ε.Μ.Π.
Στεφανέας Πέτρος Λέκτορας Ε.Μ.Π.

ΑΘΗΝΑ 2013

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΑΛΓΟΡΙΘΜΟΙ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗΣ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΗΛΙΟΠΟΥΛΟΣ ΔΗΜΗΤΡΙΟΣ
Α.Μ. 09104095

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ: Παπαϊωάννου Αλέξανδρος (Επιβλέπων)
Αναπληρωτής Καθηγητής Ε.Μ.Π.
Κουκουβίνος Χρήστος Καθηγητής Ε.Μ.Π.
Στεφανέας Πέτρος Λέκτορας Ε.Μ.Π.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω ιδιαιτέρως τον καθηγητή μου και επιβλέποντα κύριο Αλέξανδρο Παπαϊωάννου, Αναπληρωτή Καθηγητή του Ε.Μ.Π., για την πολύτιμη βοήθεια του και καθοδήγηση κατά την εκπόνηση της διπλωματικής μου εργασίας.

Ευχαριστώ επίσης θερμά τη φίλη μου Πηνελόπη Μανωλά για την εποικοδομητική συμβολή της καθ' όλη τη διάρκεια της διπλωματικής μου εκπόνησης.

ΠΡΟΛΟΓΟΣ

Αντικείμενο της διπλωματικής μου είναι οι Πρώτοι Αριθμοί και οι Αλγόριθμοι Πιστοποίησης και Παραγοντοποίησης αυτών. Πρώτοι λέγονται οι φυσικοί αριθμοί που είναι μεγαλύτεροι της μονάδας και έχουν μόνο δύο φυσικούς διαιρέτες. Το 1 και τον εαυτό τους.

Αρχικά γίνεται μια ιστορική αναδρομή στην εξέλιξη των αριθμών. Από την εμφάνιση των πρώτων αρχαίων αριθμητικών συστημάτων, το κόσκινο του Ερατοσθένη, το τρίγωνο του Pascal, έως την εμφάνιση της μεταβλητής, της αποδοχής του αριθμού μηδέν, τους αρνητικούς αριθμούς, την ιστορία του π και του λογαρίθμου μέχρι να φτάσουμε στους πρώτους Πρώτους Αριθμούς.

Στη συνέχεια περιγράφονται διάφορες κλασσικές μέθοδοι όπως αυτή των διαδοχικών διαιρέσεων, το κόσκινο του Ερατοσθένη εκτενέστερα, η μέθοδος παραγοντοποίησης του Fermat όπως και αυτή του Euler, καθώς και οι ισοδυναμίες του Gauss, η συνάρτηση του Euler και κάποια βασικά θεωρήματα θεωρίας αριθμών, ολοκληρώνοντας με τα σύμβολα των Legendre και Jacobi.

Έπειτα παρουσιάζονται και αναλύονται τα κριτήρια των Fermat, Miller-Rabin και Solovay-Strassen για την πιστοποίηση πρώτου αριθμού και τα κριτήρια του Dixon, p-1 και Rho του J.Pollard για την παραγοντοποίηση ακεραίου.

PROLOGUE

Subject of my thesis is the Prime numbers and their Certification and Factorization Algorithms. Primes are called the natural numbers that are greater than one and have only two physical dividers. 1 and themselves.

Initially in an historic overview of the numbers. From the first appearance of ancient numeration systems, the sieve of Eratosthenes, the triangle of Pascal, to the appearance of the variable, acceptance number zero, negative numbers, history of pi and the logarithm to get the first prime number.

Thereafter described various conventional methods such as successive divisions, the sieve of Heratosthenes in more details, the method of derivatizing of Fermat and as that of Euler, and the equivalent of Gauss, the function of Euler and basic theorems of theory of numbers, completing with the symbols of Legendre and Jacobi.

Then presented and analyzed the criteria of Fermat, Miller-Rabin and Solovay-Strassen for certification Prime number and the criteria of Dixon, p-1 and Rho of J.Pollard for factoring integers.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1 : ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

1.1 Η ΕΞΕΛΙΞΗ ΤΩΝ ΑΡΙΘΜΩΝ

Ο άνθρωπος χρειάστηκε 1.000.000 χρόνια για να οδηγηθεί στην αφηρημένη έννοια των αριθμών. Η παλαιότερη ένδειξη αριθμητικής καταγραφής βρέθηκε στη Σουαζιλάνδη της **Νότιας Αφρικής** και είναι μια περόνη μπαμπουίνου με 29 εμφανείς εγκοπές που χρονολογείται από το 35.000πΧ. Μοιάζει με τα «ημερολογιακά ραβδιά» που ακόμα χρησιμοποιούν στη Ναμίμπια για να καταγράφουν την παρέλευση του χρόνου.

Οι **Σουμέριοι** ζύγιζαν, υπολόγιζαν τη γη σε «σαρ», μετρούσαν τα υγρά σε «κα», χρησιμοποιούσαν κλάσματα και είχαν σύστημα αριθμών με βάση το 60. π.Χ. Το αριθμητικό τους σύστημα είχε ως βάση το 60, ήταν μη ψηφιακό, θεσιακό, χωρίς υποδιαστολή και χωρίς μηδέν. Υποστηρίζεται ότι γνωρίζανε και το δεκαδικό σύστημα.

Το εξηνταδικό σύστημα των Βαβυλωνίων έχει επιβιώσει μέχρι σήμερα στο μέτρημα του χρόνου. Έτσι π.Χ. όταν οι **Βαβυλώνιοι** ήθελαν να εκφράσουν τον αριθμό 75, έλεγαν «1,15», όπως κι εμείς σήμερα τα 75 λεπτά τα εκφράζουμε σαν 1 ώρα και 15 λεπτά. π.Χ. Οι Αιγύπτιοι χρησιμοποιούν σύστημα αριθμών με βάση το 10.

Στο **βαβυλωνιακό**, το **αιγυπτιακό**, το **ρωμαϊκό** και πολλά άλλα αριθμητικά συστήματα της αρχαιότητας το τρία παριστάνεται ως III επειδή κάθε φορά που συμπληρώνονται δέκα μονάδες δημιουργείται μια μονάδα ανωτέρας τάξης. Οι αριθμοί από το 0 μέχρι το 9 είναι μονοψήφιοι. Ο αριθμός 10 γράφεται ως ένα και μηδέν δηλαδή μια μονάδα ανωτέρας τάξης (δεκάδα) και καμιά απλή μονάδα, γιατί η αξία του κάθε ψηφίου καθορίζεται από τη θέση του μέσα στον αριθμό. Έτσι στο 4737 από δεξιά προς τα αριστερά η αξία αυξάνεται. (δέκατα, εκατοστά, χιλιοστά, …) τότε η υποδιαστολή μας δείχνει που σταματούν οι ακέραιες μονάδες και που αρχίζουν οι κλασματικές. Έτσι αυτό που μας επιτρέπει να διαφοροποιήσουμε το 31,2 από το 3,12 είναι η υποδιαστολή. Εξηνταδικό, αφού απαιτούνται 60 απλές μονάδες για να δημιουργήσουν μια μονάδα ανωτέρας τάξεως, μια εξηντάδα. Με εξήντα εξηντάδες (3.600 απλές μονάδες) φτιάχνουμε μια μονάδα ανωτέρας τάξεως, μια τρισχιλιοεξακοσάδα, κ.ο.κ. Έτσι ο αριθμός 125 απαρτίζεται από δύο (δύο εξηντάδεις=120) και το πέντε (πέντε μονάδες), ενώ ο αριθμός 634 απαρτίζεται από το δέκα (δέκα εξηντάδες=600) και το 24 (24 μονάδες).

Ο **Κινέζικος πολιτισμός**, 2852πΧ, χρησιμοποιεί σύστημα αριθμών με βάση το 60. Κάνανε αστρονομικούς υπολογισμούς 1500 χρόνια πριν από τους αρχαίους Έλληνες, και είχαν αόριστες εξισώσεις και αρνητικούς αριθμούς.

Οι **Ίνκας** έφτιαξαν ένα αριθμητικό σύστημα με βάση το 10, για να παρακολουθούν τις καθημερινές δραστηριότητες του μεγάλου πληθυσμού τους (Μέσα σε 200 χρόνια είχαν πληθυσμό 6-12.000.000 άτομα).

Οι **Μάγια** είχαν αριθμητικό σύστημα εικοσαδικό, μη ψηφιακό, θεσμικό και με ειδικό σύμβολο για το μηδέν. Το εικοσαδικό σύστημα οφείλεται ενδεχομένως στη χρήση των δαχτύλων τόσο των χεριών όσο και των ποδιών, για τη στοιχειώδη μέτρηση.

Οι **Ινδοί** έχουν το δεκαδικό σύστημα αρίθμησης, το οποίο χρησιμοποιείται παγκοσμίως και το οποίο διέδωσαν οι Άραβες. Άραβες μαθηματικοί ήταν ο Αλ Χβαρίσμι (780-850 μΧ), πατέρας της Άλγεβρας, τίτλο που διεκδικεί από το δικό μας Διόφαντο και ο Πέρσης ποιητής και αστρονόμος Ομάρ Χαγιάμ (1048-1131 μΧ) (1180-1250 μΧ). Για να τα υιοθετήσουν όμως οι Ευρωπαίοι χρειάστηκαν ακόμα 400 χρόνια.

Τα επιτεύγματα των Ελλήνων, για 1000 χρόνια επισκιάζουν όλα τα πνευματικά επιτεύγματα των επόμενων 1500 ετών. Οι **Έλληνες** όμως στηρίχτηκαν στις παλαιότερες αρχαίες κοινωνίες των Βαβυλωνίων και Αιγυπτίων. 10: το Ηρωδιανό ή Αττικό και το Ιωνικό ή Αλεξανδρινό. Δε χρησιμοποιούσαν τιμές θέσεις όπως έκανα οι Βαβυλώνιοι και όπως γίνεται σήμερα. Επίσης δε χρησιμοποιούσαν το μηδέν και τα κλάσματα.

ΤΟ ΚΟΣΚΙΝΟ ΤΟΥ ΕΡΑΤΟΣΘΕΝΗ

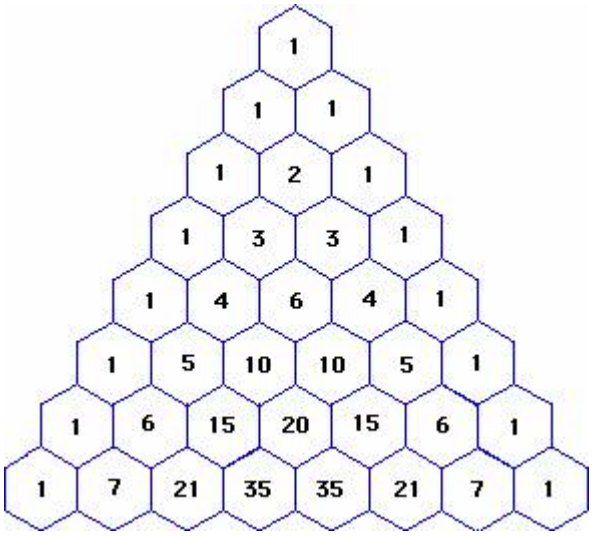
Σε έναν πίνακα γράφουμε όλους τους ακέραιους αριθμούς από το 1 έως π.χ. το 100. Στη συνέχεια αφήνουμε τον αριθμό 2 και διαγράφουμε όλα τα πολλαπλάσια του το 2 , το 4 , το 6 κτλ, επειδή όλοι αυτοί οι αριθμοί ως πολλαπλάσια του 2 δεν είναι πρώτοι. Αμέσως μετά κάνουμε το ίδιο με τον αριθμό 3 που είναι ο επόμενος μικρότερος αριθμός που δεν έχει διαγραφεί. Διαγράφουμε δηλαδή όλα το πολλαπλάσια του 3 που είναι το 6, το 9, το 12 κτλ, επειδή και αυτοί ως πολλαπλάσια του 3 δεν είναι πρώτοι αριθμοί. Συνεχίζουμε με αυτόν τον τρόπο το «κοσκίνισμα» διαγράφοντας όλα τα πολλαπλάσια του μικρότερου αριθμού που δεν έχει διαγραφεί. Τη διαδικασία αυτή, της εύρεσης πρώτων αριθμών την οφείλουμε στον αρχαίο Έλληνα μαθηματικό Ερατοσθένη (έζησε περίπου το 250πΧ) και είναι γνωστή μέχρι σήμερα ως το **«κόσκινο του Ερατοσθένη»**.

Ο αριθμός 1 δεν είναι πρώτος και γι αυτό δεν τον περιλαμβάνουμε στον πίνακα.

	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	16	53	54	55	56	57	58	59	60
61	16	63	64	65	66	67	68	69	70
71	16	73	74	75	76	77	78	79	80
81	16	83	84	85	86	87	88	89	90
91	16	93	94	95	96	97	98	99	100

ΤΟ ΤΡΙΓΩΝΟ ΤΟΥ PASCAL

Για το σχηματισμό του τριγώνου Pascal θέτουμε μία μονάδα (1) στο μέσον της 1ης γραμμής. Στη 2η γραμμή θέτουμε δύο μονάδες μία αριστερά και μία δεξιά της προηγούμενης. Στην επόμενη θέτουμε πάλι δύο (2) μονάδες μία αριστερά της πρώτης και μία δεξιά της τελευταίας της προηγούμενης γραμμής, ενώ ανάμεσα από τις δύο μονάδες θέτουμε το άθροισμά τους. Συνεχίζουμε με αυτό τον τρόπο σχηματίζοντας κάθε φορά μία νέα γραμμή με ένα στοιχείο επιπλέον από την προηγούμενη. Το πρώτο και τελευταίο στοιχείο είναι μονάδες ενώ τα ενδιάμεσα στοιχεία είναι το άθροισμα των δύο στοιχείων της προηγούμενης γραμμής που βρίσκονται αριστερά και δεξιά του. Για παράδειγμα το 15 της έβδομης γραμμής του σχήματος ισούται με το άθροισμα των στοιχείων 5 και 10 της έκτης γραμμής.



1.2 Η ΕΜΦΑΝΙΣΗ ΓΙΑ ΠΡΩΤΗ ΦΟΡΑ ΤΗΣ ΜΕΤΑΒΛΗΤΗΣ

Για πρώτη φορά χρησιμοποιήθηκε γράμμα για να παραστήσει ζητούμενο αριθμό από τον Διόφαντο στα 250πΧ στο έργο του : " Αριθμητικά ". Διατύπωσε και έλυσε ένα πρόβλημα χρησιμοποιώντας το γράμμα (ανάποδος).

Γράφει :

" Τον επιταχθέντα αριθμόν διελείν εις δύο αριθμούς εν υπεροχή τη δοθείσει. Έστω δει ο ρ, η δε υπεροχή Μμ , ευρείν τους αριθμούς...".

Δηλαδή : Δοθέντος αριθμού να διαιρεθεί σε δυο άλλους που έχουν δοθείσα διαφορά. Έστω ότι ο δοθείς αριθμός είναι ο 100 η δε διαφορά 40. Να βρεθούν οι δύο αριθμοί.

Και συνεχίζει :

" Τετάχθω ο ελάσσων ςα ο άρα μείζων έσται ς α Μμ συναμφότεροι άρα γίνονται ςβμμ δέδονται δε Μρ.Μ άρα ρ ίσαι εισιν ςβ Μμ".

Το γράμμα ς που ο Διόφαντος για πρώτη φορά χρησιμοποιεί έχει τελείως διαφορετικό νόημα από τα άλλα γράμματα. Συμβολίζει τον ζητούμενο αριθμό. Έναν συγκεκριμένο αλλά άγνωστο αριθμό. Οι μ, ρ, β συμβολίζουν αριθμούς σύμφωνα με την αρχαιοελληνική γραφή αριθμών.

1.3 ΤΟ ΜΗΔΕΝ ΚΑΙ Η ΑΓΝΟΙΑ

Ήταν ο μεγάλος φιλόσοφος **Λούντβιχ Βιττγκενστάϊν** που είχε γράψει πως τα όρια της γλώσσας είναι και τα όρια της γνώσης μας για τον κόσμο. Το ίδιο ισχύει και για την τελειότερη ίσως γλώσσα που εφηύρε ο άνθρωπος, τα **μαθηματικά**. Τα όρια της φαντασίας μας ήταν και τα όρια της γλώσσας μας. Γι' αυτό και στα αριθμητικά συστήματα των **αρχαίων Ελλήνων** (α, β, γ, δ, στ, ...) και των **Λατίνων** (I,II, III, IV...) δεν υπήρξε ποτέ το στοιχείο **μηδέν**. Για το κυρίαρχο ρεύμα της αρχαιοελληνικής φιλοσοφίας που συνοψίστηκε από τον Αριστοτέλη το κενό δεν μπορούσε να υπάρξει – ή όπως θα μπορούσε να λεχθεί: η μη ύπαρξη απλώς δεν υπήρχε. Η ύπαρξη της ανυπαρξίας ήταν μια τεράστια λογική αντίφαση. Άρα δεν υπήρχε και κανένας λόγος να απεικονιστεί αυτό που δεν υπήρχε. Αντίθετα για τις ανατολικές φιλοσοφίες, που τράβηξαν άλλους δρόμους και η πλήρης ανυπαρξία ήταν ζητούμενο της ανθρώπινης ύπαρξης, το μηδέν υπήρχε και μπορούσε – ή καλύτερα, έπρεπε – να απεικονιστεί. Φαντάζει παράδοξο ίσως πως κοινωνίες ολόκληρες πορεύτηκαν χωρίς την έννοια του μηδενός, μαθηματικά συστήματα στήθηκαν χωρίς αυτό το μαγικό στρογγυλό σύμβολο.

Οι **Βαβυλώνιοι** ήταν οι πρώτοι που χρησιμοποίησαν τον μηδέν όχι όμως ως αριθμό αλλά ως δείκτη.

Οι **Έλληνες** παρά την πρωτοποριακή θεώρηση που έκαναν στα Μαθηματικά δεν είδαν τον μηδέν ούτε ως αριθμό ούτε ως σύμβολο δείκτη για τη θέση των άλλων. Οι αριθμοί που ήταν αναγκαίο να έχουν όνομα ήταν εκείνοι που χρησιμοποιούσαν οι έμποροι και όχι οι μαθηματικοί. Υπήρχαν όμως και εξαιρέσεις και οι εξαιρέσεις αυτές ήταν οι μαθηματικοί αστρονόμοι. Μπορεί ορισμένοι ιστορικοί να υποστήριξαν ότι οι Έλληνες χρησιμοποίησαν το γράμμα όμικρον – αρχικό της λέξης ΟΥΔΕΝ - ως σύμβολο του μηδενός αλλά ο **Neugebauer** απέρριψε την εικασία υποστηρίζοντας πλην των άλλων ότι οι Έλληνες χρησιμοποιούσαν το όμικρον ως τον αριθμό 70. Πάντως έναν αιώνα μετά Χριστόν, ο **Κλαύδιος Πτολεμαίος** χρησιμοποιεί το βαβυλωνιακό μηδέν ως δείκτη.
Η ιδέα του μηδενός δείκτη θα κάνει την επανεμφάνισή της στην **Ινδία** ενώ το έτος 500 ο **Aryabhata** θα παρουσιάσει ένα σύστημα καταγραφής των αριθμών που θυμίζει το σημερινό αλλά ο μηδέν ως αριθμός δεν υπάρχει.

ΤΟ ΜΗΔΕΝ ΕΡΧΕΤΑΙ ΣΤΗΝ ΕΥΡΩΠΗ

Το 12ο αιώνα μΧ το μηδέν ήρθε και στην Ευρώπη ύστερα από 600 χρόνια καθυστέρησης! Οι Άραβες, επηρεασμένοι από τους Ινδούς, υιοθέτησαν αμέσως το

σύστημά τους και το διέδωσαν στους γύρω λαούς προσθέτοντας μάλιστα σε αυτό το θαυμαστό λογισμό δικές τους ανακαλύψεις ιδιαίτερα σημαντικές. Με την επέκτασή τους στην Ευρωπαϊκή ήπειρο μετέφεραν και αυτές τις μεθόδους τους. Ο **Σαμανίδης Μοχάμεντ Ἰμπν Μουσσά αλ-Χοβαρεσμί** (από το όνομα του οποίου προέκυψε ο όρος αλγόριθμος) έγραψε δύο δοκίμια τα οποία μεταφέρθηκαν στη Δύση. Όμως κάθε εχέφρων και ορθά σκεπτόμενος Ευρωπαίος που ήθελε να χρησιμοποιήσει ή να μεταδώσει την εκπληκτική αυτή γνώση, χρειαζόταν πολύ περισσότερα από αυτά τα δύο βιβλία. Έπρεπε να βρει έναν τρόπο να αντιμετωπίσει τον τρομακτικό συντηρητισμό της δυτικής θρησκείας που έστελνε στη πυρά όποιον τολμούσε να χρησιμοποιήσει τα σύμβολα των «απίστων», δηλαδή τους αριθμούς 1 έως 9. Τα εμπόδια που όρθωσε ο παραλογισμός του θρησκευτικού συντηρητισμού της Ευρώπης διατηρήθηκαν ως το τέλος του Μεσαίωνα και άρχισαν να αίρονται με τις σταυροφορίες από τις οποίες οι Δυτικοί κατακτητές γύρισαν επηρεασμένοι από την παιδεία των Αράβων. Λίγους αιώνες αργότερα τα γαλλικά και τα γερμανικά πανεπιστήμια στα οποία μέχρι τον 14ο και τον 15ο αιώνα μΧ μόλις και μετά βίας διδάσκονταν πρόσθεση και αφαίρεση. Την περίοδο 1804 - 1851 (Αναγέννηση) χρησιμοποιούσαν πλέον σταθερά το ινδικοαραβικό σύστημα αριθμητικής, που τελικά θριάμβευσε.

1.4 ΟΙ ΑΡΝΗΤΙΚΟΙ ΑΡΙΘΜΟΙ

Από την μελέτη της ιστορίας των μαθηματικών μπορούμε να διαπιστώσουμε ότι οι αρνητικοί αριθμοί παρά τη γνώση τους δεν νομιμοποιήθηκαν πριν περάσουν αρκετοί αιώνες! Οι αρχαίοι Αιγύπτιοι δεν αναφέρουν τους αρνητικούς αριθμούς. Αντίθετα, οι Έλληνες τους γνώριζαν, με κύριο εκφραστή το Διόφαντο. Τα ελληνικά γεωμετρικά θεωρήματα περιέχουν κανόνες για αρνητικά μεγέθη. Ο Βραχμαγκούπτα αναφέρει τους κανόνες των προσήμων. Όμως οι αρνητικοί αριθμοί δεν "νομιμοποιήθηκαν" αφού δεν θεωρούνταν λύσεις εξισώσεων. Οι Κινέζοι επίσης δεν αντιμετώπιζαν προβλήματα στους υπολογισμούς θετικών και αρνητικών αφού χρησιμοποιούσαν τον άβακα με δύο ομάδες ράβδων (κόκκινες για τους θετικούς και μαύρες για τους αρνητικούς) (Boyer & Merzbach, 1997).
Η πρώτη εισαγωγή των σημερινών συμβόλων έγινε μόλις το 1489 και στην αρχή χρησιμοποιήθηκαν για να χρεώσουν πλεόνασμα ή έλλειψη των αποθηκών. Η πρώτη συστηματική προσπάθεια εμπέδωσης και μελέτης χρεώνεται στον Cardano Conjectandi στο έργο του Ars. Magna, η δε οριστική τους θεμελίωση επιτεύχθηκε στο 19ο αιώνα με τις συνολοθεωρητικές -αλγεβρικές μεθόδους που γνωρίζουμε (Boyer & Merzbach, 1997).

1.5 Η ΙΣΤΟΡΙΑ ΤΟΥ π

Όταν οι αρχαίοι Βαβυλώνιοι άρχισαν να χτίζουν την πόλη - λέει ο θρύλος- ασχολήθηκαν ιδιαίτερα με τη γεωμετρία. Ήδη από τον 20ό αιώνα πΧ διαπίστωσαν ότι όταν η περιφέρεια οποιουδήποτε κύκλου διαιρείται δια της διαμέτρου του και το αποτέλεσμα είναι πάντοτε περίπου τρία. Υπολόγισαν μάλιστα την τιμή αυτού του λόγου στα 25/8, τα οποία απέχουν μόλις κατά 0,5% της πραγματικής τιμής του. Πολύ λιγότερο ακριβής είναι η άλλη από τις αρχαιότερες τιμές του η, που συναντάμε στη Βίβλο (Βασιλέων Α, 7, 23), σύμφωνα με την οποία η κυκλική λίμνη του οίκου του Σολομώντα είχε διάμετρο δέκα πήχεις και περιφέρεια τριάντα πήχεις, τοποθετώντας την τιμή ακριβώς στο τρία.

Μία από τις αρχαιότερες και ακριβέστερες τιμές είναι αυτή του αιγυπτίου γραφέα Αχμές. Την έχει καταγράψει σε έναν πάπυρο του Μέσου Βασιλείου περίπου το 1650 πΧ, αντιγράφοντας ουσιαστικά έναν ακόμη αρχαιότερο πάπυρο. Ο Αχμές περιέγραψε το π ως το αποτέλεσμα της διαίρεσης του 256 διά του 81, δηλαδή 3,160.

Εκείνος όμως ο οποίος θεωρείται ότι ήταν ο πρώτος που προσέγγισε τον υπολογισμό π σε μια πιο θεωρητική βάση ήταν ο Αρχιμήδης, γι' αυτό και το π είναι γνωστό και ως σταθερά του Αρχιμήδη. Κινέζοι, Ινδοί και Πέρσες σοφοί προσπάθησαν όλοι να υπολογίσουν τη σταθερά αυτή. Ωστόσο, το όνομα με το οποίο τη γνωρίζουμε σήμερα της δόθηκε το 1706, όταν ο ουαλλός μαθηματικός Γουίλιαμ Τζόουνς πρότεινε να ονομαστεί η σταθερά του Αρχιμήδη με το ελληνικό γράμμα π, από τη λέξη "περιφέρεια". Ωστόσο, οι μεγάλες δυσκολίες με το π τότε δεν είχαν ακόμη αρχίσει. Το 1761 ο Γιόχαν Λάμπερτ απέδειξε ότι το π είναι άρρητος αριθμός. Με απλά λόγια αυτό σημαίνει ότι δεν μπορεί να εκφραστεί ως κλάσμα δύο ακέραιων αριθμών. Στο σχολείο τα παιδιά μαθαίνουν ότι το π είναι περίπου 22/7, η τιμή αυτή είναι όμως και πάλι κατά προσέγγιση, γιατί το π βρίσκεται εκτός μαθηματικής λογικής.

Η δεύτερη μεγάλη ανακάλυψη σημειώθηκε το 1882, όταν ο Φέρντιναντ φον Λίντεμαν απέδειξε ότι το π είχε μία ακόμη ασυνήθιστη ιδιότητα: ήταν υπερβατικός αριθμός. Στη μαθηματική ορολογία αυτό σημαίνει ότι δεν αποτελεί τη ρίζα καμιάς αλγεβρικής εξίσωσης με ρητούς συντελεστές.

Στη μη μαθηματική ορολογία αυτό σημαίνει ότι το π αποτελεί την απόδειξη του παλαιού ρητού ότι δεν μπορεί κανείς να τετραγωνίσει τον κύκλο. Δεν μπορεί δηλαδή κανείς, χρησιμοποιώντας μόνο έναν κανόνα και έναν διαβήτη, να φτιάξει ένα τετράγωνο που να έχει ακριβώς το ίδιο εμβαδόν με έναν δεδομένο κύκλο.

Η κομψότητα της φύσης του π συνοψίζεται όμως στις τόσες προσπάθειες που έχουν γίνει και εξακολουθούν να γίνονται για τη συμπλήρωση των αριθμών του. Η επίμονη αναζήτηση ξεκίνησε ίσως με τον γερμανό μαθηματικό Λούντολφ βαν Τσόιλεν, ο οποίος γύρω στο 1600 υπολόγισε τα πρώτα 35 δεκαδικά ψηφία του π. Ήταν τόσο υπερήφανος

γι᾽ αυτό το έργο, στο οποίο αφιέρωσε μεγάλο μέρος της ζωής του, που ζήτησε να γράψουν τα 35 ψηφία στην επιτύμβια στήλη του. Εξίσου επίμονος, ο Γουίλιαμ Σανκς αφιέρωσε από την πλευρά του 20 χρόνια στους υπολογισμούς προχωρώντας το π στα 707 δεκαδικά ψηφία. Δυστυχώς το επίτευγμα του υπέστη τεράστιο πλήγμα όταν οι πρώτο ψηφιακοί υπολογιστές ανακάλυψαν ότι είχε κάνει λάθος στο 528ο δεκαδικό ψηφίο, αχρηστεύοντας όλα τα επόμενα.
Η επέκταση του π στο άπειρο έχει επίσης επανειλημμένως προσελκύσει το ενδιαφέρον των συγγραφέων επιστημονικής φαντασίας. Ο σπουδαίος αμερικανός αστρονόμος Καρλ Σαγκάν στο βιβλίο του "Επαφή" έκρυψε την υπογραφή των εξωγήινων μέσα στα δήθεν τυχαία ψηφία του π, τα οποία στην πραγματικότητα δεν ακολουθούν κάποια συγκεκριμένη διάταξη.
"Ηταν πολύ πονηρό, γιατί αυτό δεν γίνεται" λέει ο καθηγητής Στιούαρτ. "Δεν μπορείς να τακτοποιήσεις το π σε συγκεκριμένη ακολουθία. Ήταν ένα ωραίο απατηλό τέχνασμα εκ μέρους του Σαγκάν. Υπό μίαν έννοιαν ούτε ο ίδιος ο Θεός δεν θα μπορούσε να βρει μια ακολουθία μέσα στο π", προσθέτει.

3.14159265358979323846264338327950288419716939937510582097494459230781640628620899862803482534211706798214808651328230664709384460955058223172535940812848111745028410270193852110555964462294895493038196442881097566593344612847

Αεί ο Θεός ο μέγας γεωμετρεί
το κύκλου μήκος ίνα ορίση διαμέτρω
παρήγαγεν αριθμόν απέραντον
και ον φευ! ουδέποτε όλον θνητοί θα εύρωσι.

Αν γράφουμε τους αριθμούς των γραμμάτων που περιέχει κάθε λέξη του ποιήματος έχουμε τα πρώτα 22 δεκαδικά ψηφία του π.

1.6 Η ΙΣΤΟΡΙΑ ΤΟΥ ΛΟΓΑΡΙΘΜΟΥ

Τον 16ο – 17ο αιώνα παρατηρήθηκε μια σημαντική ανάπτυξη της επιστημονικής γνώσης σε όλους τους κλάδους. Οι ανακαλύψεις των νέων χωρών, ο γύρος του κόσμου από τον Μαγγελάνο και η ανάπτυξη του ναυτικού εμπορίου δημιούργησαν την ανάγκη παραγωγής χαρτών (Gerhard Mercator, 1596). Η εισβολή των μαθηματικών στην αστρονομία και στη φυσική μετά τον Κοπέρνικο, τον Γαλιλαίο και τον Κέπλερ καθώς και το πλήθος των δεδομένων που προέκυψαν προς επεξεργασία στις προαναφερόμενες επιστήμες απαιτούσαν από τους επιστήμονες τη διεκπεραίωση περίπλοκων υπολογισμών. Έπρεπε να επινοηθούν τρόποι που θα τους απάλλασσαν από αυτό το βάρος. Και επειδή είναι ευκολότερο να προσθέτουμε παρά να πολλαπλασιάζουμε, βρέθηκε τρόπος μετατροπής της πρόσθεσης σε πολλαπλασιασμό. Ο λογάριθμος.

Ο **John Napier (1550-1617)**, $8^{ος}$ Λόρδος του Merchistoun στη Σκωτία, γνωστός για τα θρησκευτικού περιεχομένου βιβλία του, ήταν ο πρώτος που δεχόμενος την πρόκληση μετατροπής μιας πράξης σε μια άλλη πιο απλή, παρατήρησε τη σχέση των όρων μιας γεωμετρικής προόδου και των αντίστοιχων εκθετών τους που ακολουθούν αριθμητική πρόοδο.

Ο Napier παίρνοντας ως βάση τον αριθμό $1\text{-}10^{-7}$ υποστήριξε ότι κάθε θετικός αριθμός N μπορεί να γραφεί ως $N=10^7(1\text{-}10^{-7})^L$.

Έτσι έχουμε τον πρώτο ορισμό του Νεπέριου λογάριθμου: L=Nap logN.

Επί 20 χρόνια συμπλήρωνε τους διαδοχικούς όρους της γεωμετρικής προόδου που κατασκεύασε συγκεντρώνοντας τους τελικά στο έργο του Mirifici Logarithmorum Canonis Descriptio.

Παρατήρηση: Εδώ εμφανίζεται και για πρώτη φορά η τιμή της ακολουθίας

$\left(1-\frac{1}{v}\right)^{v}$ όταν το ν είναι πάρα πολύ μεγάλο, ως βάση για λογαρίθμους.

ΤΟ ΧΡΗΜΑ ΕΙΝΑΙ ΜΑΘΗΜΑΤΙΚΑ

Τον 17^{ο} αιώνα κάποιος ανώνυμος έμπορος ή τοκογλύφος παρατήρησε μια παράξενη συμπεριφορά στην αύξηση του τόκου στις τραπεζικές συναλλαγές που στηρίζονται σε ανατοκισμό με ετήσιο επιτόκιο διαιρεμένο σε ν ίσα μέρη, όταν ο αριθμός ν είναι πάρα πολύ μεγάλος. Ας παρακολουθήσουμε το φαινόμενο:

Η συνήθης τραπεζική μέθοδος αύξησης του δανειζόμενου κεφαλαίου είναι ο:

ΑΝΑΤΟΚΙΣΜΟΣ

Έστω ότι καταθέτουμε € Κ σε ένα λογαριασμό που αποδίδει ε% ετήσιο επιτόκιο και ανατοκίζεται κάθε χρόνο.

Τέλος του 1^{ου} έτους: $K_1 = 1 + \frac{\varepsilon}{100}$

Τέλος του Ν^{ου} έτους: $K_N = \left(1 + \frac{\varepsilon}{100}\right)^N$

Άλλη συνήθης τραπεζική συναλλαγή είναι ο:

Ανατοκισμός ν φορές τον χρόνο με ετήσιο επιτόκιο διαιρεμένο σε ν ίσα μέρη

Δηλαδή, αν καταθέσουμε € 100 σε ένα λογαριασμό που αποδίδει 5% και τοκίζεται κάθε χρόνο:

Τέλος του 1^{ου} έτους: € 105,00

Αν καταθέτουμε €100 σε ένα λογαριασμό που αποδίδει 5% τον χρόνο και

ανατοκίζεται κάθε εξάμηνο σε ένα χρόνο ανατοκίζεται δύο (2) φορές με επιτόκιο 2,5%

Τέλος 1^{ου} έτους: 105,06

ανατοκίζεται κάθε τρίμηνο σε ένα χρόνο ανατοκίζεται τέσσερις (4) φορές με επιτόκιο 1,66%

Τέλος 1ου έτους: 105,09 €

ανατοκίζεται κάθε μήνα σε ένα χρόνο ανατοκίζεται δώδεκα (12) φορές με επιτόκιο

0,416%.

Τέλος 1ου έτους: 105,12 €

ανατοκίζεται κάθε ημέρα σε ένα χρόνο ανατοκίζεται τριακόσιες εξήντα

πέντε (365) φορές με επιτόκιο 0,0137 %

Τέλος 1ου έτους: 105,19 €

Έστω ότι ο ανατοκισμός γίνεται ν φορές τον χρόνο. Για κάθε περίοδο μετατροπής ως επιτόκιο θεωρείται το ετήσιο επιτόκιο διαιρεμένο με τον ν, δηλαδή $\frac{\varepsilon}{\nu}$ %.

Τέλος 1ου έτους: $K_\nu = K\left(1+\frac{\varepsilon}{\nu 100}\right)^\nu$

Παρατήρηση: Το τελικό κεφάλαιο για περίοδο μετατροπής πάρα πολύ μικρή, π.χ. $\frac{1}{1000000}$ / $\frac{1}{10000000}$, δεν ξεπερνά το 2,72 του αρχικού κεφαλαίου.

Παρατηρούμε ότι ο τύπος $\left(\nu+\frac{1}{\nu}\right)^\nu$ πλησιάζει μια τιμή χωρίς να τη φτάνει και αυτή είναι ο αριθμός e. Τότε λέμε ότι η ακολουθία με τύπο $\left(\nu+\frac{1}{\nu}\right)^\nu$ έχει όριο τον αριθμό e.

ΤΟ e ΩΣ ΟΡΙΟ

Ο αριθμός e, όπως διαπιστώσαμε, είναι όριο της ακολουθίας.

Αλλά, αφού για μεγάλες τιμές του ν η τιμή του $\frac{1}{\nu}$ θα είναι σχεδόν μηδέν,

έχουμε: $(1+\frac{1}{v})^v = 1+1+\frac{1}{2!}+\frac{1}{3!}+\dots$

Συνεπώς $\boxed{e = 2+\frac{1}{2!}+\frac{1}{3!}+\frac{1}{4!}+\dots}$

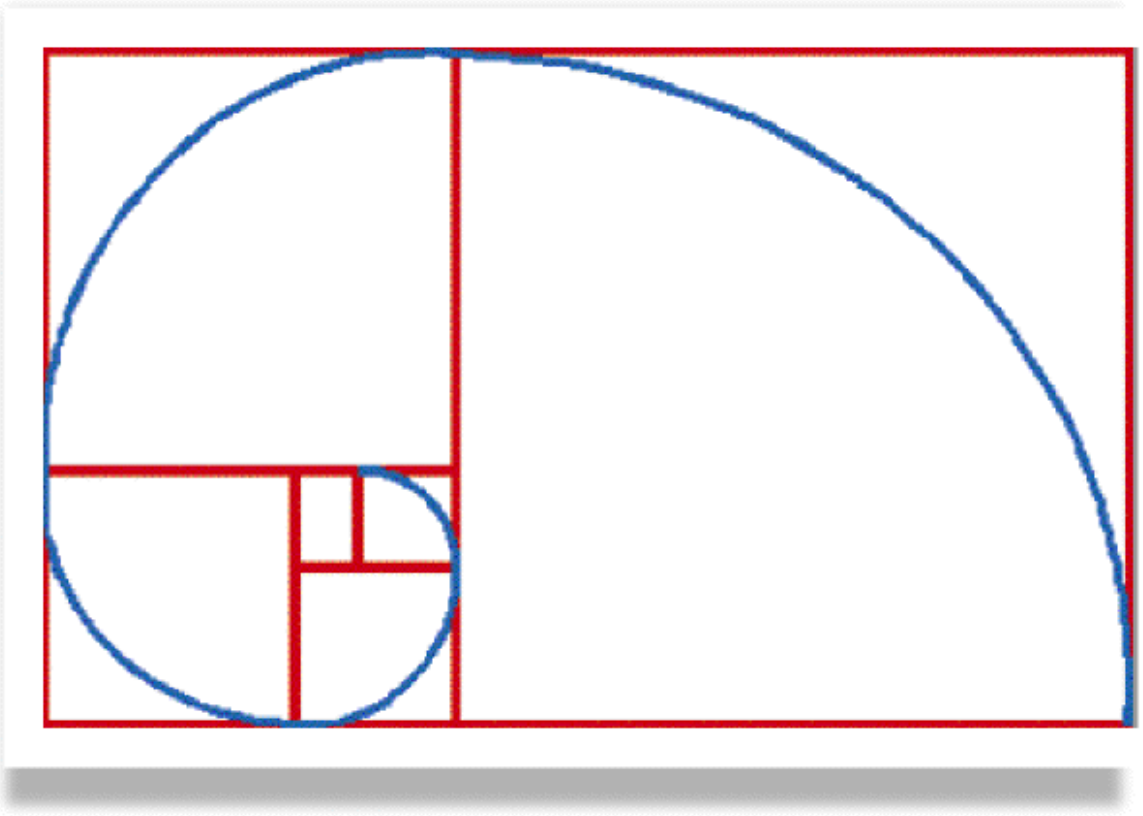
Ο τετραγωνισμός της υπερβολής

Ο Gregorius de Saint-Vincent (1584-1667), στην προσπάθεια τετραγωνισμού της υπερβολής διαπιστώνει ότι αν οι τετμημένες της γραφικής παράστασης της συνάρτησης μεταβάλλονται με γεωμετρική πρόοδο, τότε το εμβαδόν που βρίσκεται μεταξύ του άξονα των τετμημένων και της υπερβολής μεταβάλλεται με αριθμητική πρόοδο.

ΟΤΑΝ ΤΟ e ΣΥΝΑΝΤΑ ΤΟ φ : ΛΟΓΑΡΙΘΜΙΚΗ ΕΛΙΚΑ

Ο **Jacob Bernoulli (1654-1705)** μελέτησε τη λογαριθμική έλικα και την ονόμασε spira mirabilis λόγω των σπανίων μαθηματικών ιδιοτήτων της που την καθιστούν, μετά τον κύκλο, το πιο προσφιλές διακοσμητικό μοτίβο.

Η λογαριθμική έλικα περιγράφεται ως καμπύλη με αφετηρία ένα σημείο (τον πόλο) και ανελίσσεται με τρόπο ώστε η απόσταση των σημείων της από το πόλο να αυξάνει με γεωμετρική πρόοδο εφόσον η γωνία περιστροφής αυξάνει με αριθμητική πρόοδο. Κάθε ευθεία που διέρχεται από τον πόλο τέμνει την έλικα υπό την ίδια γωνία.



ΟΙ ΛΟΓΑΡΙΘΜΟΙ

Η ιδέα των λογαρίθμων γεννήθηκε πιθανόν από τους αστρονόμους οι οποίοι έπρεπε να πολλαπλασιάζουν και να διαιρούν πολύπλοκες τριγωνομετρικές ποσότητες. Στο μεταξύ οι πίνακες με τους αριθμούς και τις δυνάμεις έδειχναν ότι ο πολλαπλασιασμός στον ένα πίνακα αντιστοιχούσε σε πρόσθεση στον άλλο. Στην αυγή του $17^{ου}$ αιώνα ο σκωτσέζος John Napier ή Neper είχε την ιδέα της δημιουργίας ενός πίνακα λογαρίθμων ο οποίος θα διευκόλυνε τους πολλαπλασιασμούς οποιωνδήποτε ποσοτήτων ανάγοντάς τους σε προσθέσεις. Το 1617 δημοσίευσε τον σχετικό πίνακα και το όνομά του δημιούργησε αργότερα τον όρο "νεπέριοι λογάριθμοι".

Σήμερα η έννοια λογάριθμος έχει διαφοροποιηθεί σε σχέση με εκείνη που πρότεινε ο Neper. Ο λογάριθμος ενός αριθμού, όπως λόγου χάρη ο 50, είναι ο ΕΚΘΕΤΗΣ τον οποίο πρέπει να έχει ο αριθμός e (βάση) ώστε να είναι ίσος με 50. $e^{ln50} = 50$.

1.7 Η ΙΣΤΟΡΙΑ ΤΩΝ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ

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

Οι **Αρχαίοι Έλληνες** ήταν οι πρώτοι που αντιλήφθηκαν τη σημασία των πρώτων αριθμών και τη δυναμική που κρύβουν και έφτασαν σε σπουδαία συμπεράσματα σε σχέση με τη φύση τους. Τα στοιχεία του Ευκλείδη (περίπου στο 300 πΧ) περιέχουν σημαντικά θεωρήματα για τους πρώτους αριθμούς, συμπεριλαμβανομένων της απειρίας των πρώτων αριθμών και του θεμελιώδους θεωρήματος της αριθμητικής. Ο Ευκλείδης επίσης απέδειξε πώς μπορούμε να κατασκευάσουμε έναν τέλειο αριθμό από ένα πρώτο Μερσέν αριθμό. Το κόσκινο του Ερατοσθένη, το οποίο αποδίδεται στον Ερατοσθένη, είναι μια απλή μέθοδος να υπολογίσουμε τους πρώτους, παρόλο που οι μεγάλοι πρώτοι δεν υπολογίζονται σήμερα με τους υπολογιστές με αυτό τον τρόπο.

Μετά τους Έλληνες, λίγα πράγματα συνέβησαν με την έρευνα των πρώτων αριθμών μέχρι τον 17ο αιώνα. Το 1640 ο **Πιέρ ντε Φερμά** διατύπωσε (χωρίς απόδειξη) το μικρό θεώρημα του Φερμά (αργότερα αποδείχθηκε από τους Λάιμπνιτς και Όιλερ). Ο Φερμά υπέθεσε ότι όλοι οι αριθμοί της μορφής $2^{2^n} + 1$ είναι πρώτοι (αυτοί οι αριθμοί ονομάζονται αριθμοί Φερμά) και το επαλήθευσε αυτό μέχρι και για n = 4 (ή $2^{16} + 1$). Αλλά ο αμέσως επόμενος αριθμός Φερμά $2^{32} + 1$ είναι σύνθετος (ένας από τους παράγοντες του που είναι πρώτος αριθμός είναι ο 641), όπως ανακάλυψε αργότερα ο Euler και μάλιστα δεν υπάρχουν παραπάνω γνωστοί αριθμοί Φερμά, οι οποίοι είναι πρώτοι. Ο Γάλλος καλόγερος Μερσέν μελέτησε τους πρώτους αριθμούς της μορφής 2^p -

1, όπου p είναι πρώτος. Αυτοί οι αριθμοί ονομάζονται πρώτοι αριθμοί Μερσέν προς τιμή του.

Το έργο του **Όιλερ** στη θεωρία αριθμών περιλαμβάνει πολλά συμπεράσματα για τους πρώτους αριθμούς. Ο Όιλερ απέδειξε ότι η άπειρη σειρά 1/2 + 1/3 + 1/5 + 1/7 + 1/11 + ... αποκλίνει. Το 1747 έδειξε ότι οι άρτιοι τέλειοι αριθμοί είναι ακριβώς οι ακέραιοι της μορφής $2^{p-1}(2^p - 1)$, όπου ο δεύτερος παράγοντας είναι ένας πρώτος Μερσέν αριθμός.

Στις αρχές του 19ου αιώνα, οι **Λεζέντρ και Γκάους** ανεξάρτητα υπέθεσαν ότι καθώς το x τείνει στο άπειρο, το πλήθος των πρώτων αριθμών μέχρι και το x είναι ασύμπτωτο στο κλάσμα x/ln(x), όπου ln(x) είναι ο φυσικός λογάριθμος του x. Στις ιδέες του ο Ρίμαν για τη συνάρτηση ζήτα, τις οποίες εξέδωσε το 1859, σχεδίαζε ένα πρόγραμμα που θα οδηγούσε σε μια απόδειξη του θεωρήματος των πρώτων αριθμών. Αυτό το περίγραμμα ολοκληρώθηκε από τους Χάνταμαρντ και ντε λα Βαλέ Πουσέν, οι οποίοι ανεξάρτητα απέδειξαν το θεώρημα των πρώτων αριθμών το 1896.

Δε γίνεται να αποδείξουμε ότι ένας μεγάλος αριθμός είναι πρώτος με τη δοκιμαστική διαίρεση. Πολλοί μαθηματικοί έχουν εργαστεί στην εύρεση τεχνικών για να αποδειχτεί αν ένας μεγάλος αριθμός είναι πρώτος, αλλά συχνά αυτές οι τεχνικές περιορίζονται σε συγκεκριμένες μορφές αριθμών. Παραδείγματα τέτοιων τεχνικών είναι το τεστ του Πέπιν για τους αριθμούς Φερμά (1877), το θεώρημα του Προθ (γύρω στο 1878), το τεστ των Λούκας-Λέμερ (1856) και το γενικευμένο τεστ πρώτων αριθμών του Λούκας. Πιο πρόσφατοι αλγόριθμοι, όπως οι APRT-CL, ECPP και AKS δουλεύουν για όλους τους αριθμούς, αλλά παραμένουν πολύ πιο αργοί.

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, στην οποία κρυπτογράφηση δημόσιου κλειδιού οι πρώτοι αριθμοί αποτελούσαν τη βάση των πρώτων αλγορίθμων, όπως τον κρυπτογραφικό αλγόριθμο RSA.

Από το 1951 όλοι οι μεγαλύτεροι πρώτοι αριθμοί έχουν βρεθεί από τους ηλεκτρονικούς υπολογιστές. Η έρευνα για όλο και μεγαλύτερους πρώτους αριθμούς έχει προκαλέσει ενδιαφέρον και έξω από τους μαθηματικούς κύκλους. Η μεγάλη διαδικτυακή έρευνα πρώτων Μερσέν αριθμών και άλλες εργασίες σε παράλληλα και κατανεμημένα συστήματα πληροφορικής για την εύρεση μεγάλων πρώτων αριθμών έχουν γίνει διάσημες τα τελευταία δέκα με δεκαπέντε χρόνια, ενώ οι μαθηματικοί συνεχίζουν να παλεύουν με τη θεωρία των πρώτων αριθμών.

ΚΕΦΑΛΑΙΟ 2 : ΚΛΑΣΣΙΚΕΣ ΜΕΘΟΔΟΙ

2.1 Η ΜΕΘΟΔΟΣ ΤΩΝ ΔΙΑΔΟΧΙΚΩΝ ΔΙΑΙΡΕΣΕΩΝ

ΘΕΩΡΗΜΑ Αν ο φυσικός n >1 δεν έχει πρώτο διαιρέτη μικρότερο ή ίσο της $\sqrt{n}$ τότε ο n είναι πρώτος.

Απόδειξη: Έστω ότι ο n είναι σύνθετος και $n=d_1 \cdot d_2$ με d_1, d_2 μεγαλύτερους της μονάδας.

Αν $d_1 > \sqrt{n}$ και $d_2 > \sqrt{n}$ τότε $n = d_1 \cdot d_2 > \sqrt{n} \cdot \sqrt{n} = n$ άτοπο.

Άρα έστω $d_1 \leq \sqrt{n}$, τότε ή ο d_1 είναι πρώτος ή ο d_1 έχει πρώτο διαιρέτη μικρότερο ή ίσο της $\sqrt{n}$.

Φτάσαμε σε άτοπο άρα ο n είναι πρώτος.

Συνεπώς, για να διαπιστώσουμε εάν ο n είναι πρώτος δεν έχουμε παρά να δοκιμάσουμε εάν αυτός διαιρείται από όλους τους πρώτους ≤ $\sqrt{n}$. Η διαδικασία αυτή καλείται μέθοδος των διαδοχικών διαιρέσεων.

Η μέθοδος των διαδοχικών διαιρέσεων όμως δεν είναι αποτελεσματική στην περίπτωση όπου ο n είναι αρκετά μεγάλος. Ο χρόνος που απαιτείται για την μέθοδο αυτή είναι $O(\sqrt{n}(\log n)^2)$.

2.2 ΤΟ ΚΟΣΚΙΝΟ ΤΟΥ ΕΡΑΤΟΣΘΕΝΗ

Ο **Ερατοσθένης** (276πΧ - 194πΧ) από την Κυρήνη, το σημερινό Um Sahad στην Λιβύη, ήταν διευθυντής στην βιβλιοθήκη της Αλεξάνδρειας. Αξίζει να αναφερθεί ότι γνωρίζοντας την απόσταση Συήνης (σημερινό Ασουάν) - Αλεξάνδρειας υπολόγισε πρώτος με μεγάλη ακρίβεια την ακτίνα και το μέγεθος της Γης. Είναι ένα γεγονός ιδιαίτερα εντυπωσιακό αν αναλογιστεί κανείς ότι η προσέγγιση αυτή δεν βελτιώθηκε για σχεδόν μία χιλιετία ενώ η παγκόσμια κοινή γνώμη δεν είχε αποδεχτεί ότι η Γη δεν είναι επίπεδη για τουλάχιστον δεκαπέντε αιώνες μετά από εκείνον. Ο Ερατοσθένης επινόησε την παρακάτω μέθοδο γνωστή σαν το ''κόσκινο του Ερατοσθένη''. Το κόσκινο, το οποίο περιγράφεται στην Εισαγωγή στην Αριθμητική του Νικόμαχου, είναι ένας απλός αλγόριθμος για την εύρεση όλων των πρώτων αριθμών μέχρι ένα συγκεκριμένο ακέραιο. Δυστυχώς κανένα μαθηματικό έργο του Ερατοσθένη δεν έχει διασωθεί.

Το Κόσκινο του Ερατοσθένη :

1. Γράφουμε διαδοχικά τους φυσικούς αριθμούς από τον 2 έως τον n

2. Διαλέγουμε διαδοχικά τους πρώτους αριθμούς ξεκινώντας από τον 2, τους μαρκάρουμε σαν πρώτους αριθμούς και ύστερα διαγράφουμε όλα τα πολλαπλάσιά τους (2p, 3p, 4p, 5p ,.....) έως τον ακέραιο p που είναι μικρότερος ή ίσος από τον $\sqrt{n}$.

Οι ακέραιοι που μένουν είναι σαφώς πρώτοι και εάν ο αριθμός n δεν έχει διαγραφεί είναι πρώτος.

Είναι φανερό ότι πρόκειται για μια εξαντλητική μέθοδο, υπολογιστικά καθόλου αποτελεσματική. Παρόλο που οι διαιρέτες οποιουδήποτε υποψήφιου πρώτου αρκεί να αναζητηθούν μέχρι και την τετραγωνική τους ρίζα, η πολυπλοκότητα της παραπάνω μεθόδου αγγίζει την πολυωνυμική ως προς το μέγεθος της εισόδου και άρα την εκθετική ως προς την αναπαράστασή του. Ο γρηγορότερος υπολογιστής θα χρειαστεί 41 χρόνια για να κάνει όλους τους ελέγχους και να αποδείξει ότι ο αριθμός Mersenne 2^{127}-1 είναι πράγματι πρώτος.

Παράδειγμα

Θα βρούμε όλους τους πρώτους αριθμούς μέχρι τον αριθμό 97 και θα αποφανθούμε για το αν ο 97 είναι πρώτος.

$\sqrt{97}$ =9,85 άρα ο μεγαλύτερος πρώτος που θα χρειαστεί να μαρκάρουμε και να διαγράψουμε τα πολλαπλάσιά του, είναι ο αριθμός 9.

	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	16	53	54	55	56	57	58	59	60
61	16	63	64	65	66	67	68	69	70
71	16	73	74	75	76	77	78	79	80
81	16	83	84	85	86	87	88	89	90
91	16	93	94	95	96	97	98	99	100

2.3 Η ΜΕΘΟΔΟΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΤΟΥ FERMAT

Ο **Pierre de Fermat** (1601-1665), ένας δικηγόρος από την Toulouse και μεγάλος ερασιτέχνης μαθηματικός της Αναγέννησης επινόησε την παρακάτω μέθοδο παραγοντοποίησης. Ο Fermat σπάνια δημοσίευε τα αποτελέσματά του, οπότε η μέθοδος έγινε γνωστή από την αλληλογραφία του με τον Αββά Marin Mersenne, έναν Φραγκισκανό καλόγερο και ενθουσιώδη αριθμοθεωρητικό.

Η μέθοδος παραγοντοποίησης του Fermat στηρίζεται στο να εκφράσει τον αριθμό σαν διαφορά δύο τέλειων τετραγώνων, αν αυτό είναι εφικτό, οπότε η παραγοντοποίηση γίνεται στοιχειωδώς. Ο προς παραγοντοποίηση αριθμός είναι προφανώς μονός οπότε και οι δύο παράγοντες εάν προκύψουν θα είναι επίσης μονοί αριθμοί.

$n=x^2 - y^2=(x+y)(x-y)=u\cdot v$ άρα $\begin{cases} u = x + y \\ v = x - y \end{cases}$ οπότε $x = \frac{u+v}{2}$ και $y = \frac{u-v}{2}$

Ο Fermat ονόμασε k τον μικρότερο φυσικό για τον οποίο $k^2 > n$ και κατασκεύασε την ακολουθία

k^2-n

$(k + 1)^2-n$

$(k + 2)^2-n$

.....

$(k + m)^2-n$

έως ότου το αποτέλεσμα να είναι τέλειο τετράγωνο (για πολλούς αριθμούς αυτό δεν συμβαίνει ποτέ).

Τότε $(k + m)^2-n = y^2$ άρα $y=\sqrt{(k + m)^2 - n}$ και $x= k + m$

οπότε $n=(x+y)(x-y)$.

Αν οι ακέραιοι u,v βρίσκονται πολύ κοντά, τότε ο y είναι είναι πολύ μικρός και επομένως ο x θα είναι λίγο μεγαλύτερος από τον $\sqrt{n}$. Σε αυτήν την περίπτωση, η μέθοδος θα μας δώσει την παραγοντοποίηση του n μετά από ένα μικρό πλήθος δοκιμών για τον x.

<u>Παράδειγμα</u>

Θα παραγοντοποιήσουμε τον αριθμό n=670.661.

$\sqrt{670.661} = 818{,}94$ άρα $k = 819$

$819^2 - 670.661 = 100 = 10^2$

$670.661 = (819+10)(819-10) = 829 \cdot 809$ με μία μόνο δοκιμή, το οποίο οφείλεται στο γεγονός ότι οι δύο παράγοντες έχουν μικρή διαφορά μεταξύ τους.

Βελτίωση Μεθόδου Fermat

Έστω $n = u \cdot v$ και οι ακέραιοι u, v βρίσκονται αρκετά μακριά, τότε θα χρειαστούν αρκετές δοκιμές για να βρεθεί το αποτέλεσμα του τέλειου τετραγώνου. Για να επιταχύνουμε την διαδικασία μπορούμε να χρησιμοποιήσουμε την εξής γενίκευση της μεθόδου του Fermat.

Επιλέγουμε ένα μικρό θετικό ακέραιο t, ακέραιο k τέτοιο ώστε $k^2 > tn$ και παίρνουμε διαδοχικά την εξής ακολουθία

$k^2 - tn$

$(k + 1)^2 - tn$

$(k + 2)^2 - tn$

.....

$(k + m)^2 - tn$

έως ότου προκύψει τέλειο τετράγωνο και στη συνέχεια παραγοντοποιούμε

$(k + m)^2 - tn = y^2$ άρα $y = \sqrt{(k + m)^2 - tn}$ και $x = k + m$

οπότε $tn = (x + y)(x - y)$.

Καθώς οι x και y βρίσκονται αρκετά μακριά και ο t είναι μικρός έπεται ότι

$t < x - y < x + y < n$ άρα $1 < MK\Delta(x \pm y, n) < n$ και κατά συνέπεια οι

ακέραιοι ΜΚΔ$(x \pm y, n)$ είναι γνήσιοι παράγοντες του n.

ΒΑΣΙΚΟ ΚΡΙΤΗΡΙΟ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ

Γενικότερα , αν βρούμε ακεραίους x, y με

$$x^2 = y^2 (\mathrm{mod} n) \quad \text{και} \quad x \neq \pm y (\mathrm{mod} n)$$

τότε οι ακέραιοι ΜΚΔ$(x \pm y, n)$ δίνουν μη τετριμμένους παράγοντες του n.

Παράδειγμα

Θα παραγοντοποιήσουμε τον αριθμό $n=329.345$

Θεωρώ $t=3$ $\sqrt{3 \cdot 329.345} = 993,9$ άρα $k=994$

$994^2 - 3 \cdot 329.345 = 1$

$3 \cdot 329.345 = (994+1)(994-1) = 995 \cdot 993$

$329.345 = 995 \cdot 331$

ΜΚΔ(329.345 , 995) = 995

ΜΚΔ(329.345 , 993) = 331

Με την κλασσική μέθοδο του Fermat θα χρειαζόταν να δοκιμάσουμε πολύ περισσότερες τιμές για το k ώστε να φτάσουμε στην παραγοντοποίηση.

2.4 Η ΜΕΘΟΔΟΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΤΟΥ EULER

Ο **Leonhard Euler** (1707-1783) ήταν πρωτοπόρος Ελβετός μαθηματικός και φυσικός. Σε αυτόν οφείλεται, ανάμεσα σε άλλα, και η καθιέρωση του συμβόλου $f(x)$ για τις συναρτήσεις. Τα τελευταία 17 χρόνια της ζωής του ήταν σχεδόν τυφλός, περίοδος στην οποία παρήγαγε το μισό από το συνολικό του έργο, το οποίο υπολογίζεται σε 75 τόμους, 45.000 σελίδες μαθηματικών. Ο Euler θεωρείται "πατέρας" του Sudoku, αφού ο ίδιος διατύπωσε πρώτος τους κανόνες του.

Ο Frenicle το 1641 ρώτησε τον Fermat αν μπορούσε να παραγοντοποιήσει έναν φυσικό αριθμό που γράφεται με δυο διαφορετικούς τρόπους σαν άθροισμα δύο τετραγώνων. Δεν γνωρίζουμε αν ο Fermat απάντησε αλλά έναν αιώνα αργότερα ο Euler (1745) έδειξε ότι :

εάν $n = a^2 + b^2 = c^2 + d^2$ τότε

$$n = \frac{[(a-c)^2+(b-d)^2][(a+c)^2+(b-d)^2]}{4(b-d)^2}$$

Μία γενίκευση της μεθόδου είναι :

εάν $N = a^2 + k\,b^2 = c^2 + k\,d^2$ τότε $N = \frac{(k\,m^2 + n^2)(k\,r^2 + s^2)}{4}$

όπου ισχύουν οι παρακάτω σχέσεις:

$a+c = kmr$

$a-c = ns$

$d+b = ms$

$d-b = nr$

ΚΕΦΑΛΑΙΟ 3 : ΕΙΣΑΓΩΓΙΚΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

3.1 ΙΣΟΔΥΝΑΜΙΕΣ Ή ΙΣΟΤΙΜΙΕΣ

Οι ισοδυναμίες οφείλονται στον **Gauss**(1777-1855). Ο Gauss ήταν Γερμανός μαθηματικός που συνεισέφερε σε πολλά ερευνητικά πεδία της επιστήμης. Αποκλήθηκε ο <<πρίγκιπας>> των μαθηματικών και ο μεγαλύτερος μαθηματικός μετά τον Αρχιμίδη και τον Ευκλείδη. Σε ηλικία 21 ετών είχε ολοκληρώσει το κύριο έργο του στα καθαρά μαθηματικά. Αυτό το έργο διαδραμάτισε θεμελιώδη ρόλο στην εδραίωση της Θεωρίας Αριθμών ως αυτοδύναμου κλάδου των μαθηματικών.

Η σχέση $a=b \bmod m$ λέγεται **ισοδυναμία**.

Λέμε ότι:

- ο a είναι ισοδύναμος του b κατά μέτρο m
- ο b είναι ισοϋπόλοιπος του a modm
- η διαφορά a-b είναι ακέραιο πολλαπλάσιο του m
- ο m διαιρεί την διαφορά a-b και συμβολίζουμε m|a-b

Ιδιότητες:

1. αν $c\neq 0$ $a=a \bmod c$ (αυτοπαθής)
2. αν $a=b \bmod c$ τότε $b=a \bmod c$ (συμμετρική)
3. αν $a=b \bmod c$ και $b=d \bmod c$ τότε $a=d \bmod c$ (μεταβατική)
4. αν $a=a' \bmod c$ και $b=b' \bmod c$ τότε $a\pm b=a'\pm b' \bmod c$ και $ab=a'b' \bmod c$
5. αν $bd=bd' \bmod c$ και ΜΚΔ(b,c)=1 τότε $d=d' \bmod c$

Η πρόσθεση και ο πολλαπλασιασμός ισοδυναμιών επεκτείνονται και σε περισσότερες από δύο ισοδυναμίες.

3.2 ΣΥΝΟΛΑ ΥΠΟΛΟΙΠΩΝ ΚΑΙ Η ΣΥΝΑΡΤΗΣΗ ΤΟΥ EULER

ΟΡΙΣΜΟΣ Το σύνολο των ακεραίων $\{r_1, r_2, \dots \dots r_s\}$ ονομάζεται **πλήρες σύνολο υπολοίπων** modm εάν:

1. $r_i \neq r_j \text{mod} m$ για $i \neq j$
2. σε κάθε ακέραιο αντιστοιχεί ένας r_i , $n = r_i \text{mod} m$

ΟΡΙΣΜΟΣ Το σύνολο των ακεραίων $\{r_1, r_2, \dots \dots r_s\}$ ονομάζεται **περιορισμένο σύνολο υπολοίπων** modm εάν:

1. $r_i \neq r_j \text{mod} m$ για $i \neq j$
2. ΜΚΔ$(r_i, m)=1$ για κάθε i
3. σε κάθε ακέραιο n με ΜΚΔ$(n,m)=1$ αντιστοιχεί ένας r_i , $n = r_i \text{mod} m$

Παράδειγμα

Το σύνολο {0,1,2,3,4,5} είναι ένα πλήρες σύνολο υπολοίπων mod6 και το {1,5} είναι ένα περιορισμένο σύνολο υπολοίπων mod6.

Εν γένει μπορούμε να πάρουμε ένα περιορισμένο σύνολο υπολοίπων modm από ένα πλήρες αφαιρώντας τα στοιχεία του πλήρους που δεν είναι σχετικά πρώτα προς τον m.

Παρατήρηση

Εάν ο p είναι πρώτος τότε :

$\{0,1,2, \dots, p-1\} \rightarrow$ ΠΛΗΡΕΣ ΣΥΝΟΛΟ ΥΠΟΛΟΙΠΩΝ modp ή $\mathbb{Z}_p$

$\{1,2, \dots, p-1\} \rightarrow$ ΠΕΡΙΟΡΙΣΜΕΝΟ ΣΥΝΟΛΟ ΥΠΟΛΟΙΠΩΝ modp

Εάν m είναι φυσικός τότε :

$\{0,1,2, \dots, m-1\} \rightarrow$ ΠΛΗΡΕΣ ΣΥΝΟΛΟ ΥΠΟΛΟΙΠΩΝ modm ή $\mathbb{Z}_m$

Κάθε πλήρες σύνολο υπολοίπων modm αποτελείται από m στοιχεία και κάθε περιορισμένο σύνολο υπολοίπων modm αποτελείται από στοιχεία του πλήρους τα οποία είναι σχετικά πρώτα προς τον m.

ΣΥΝΑΡΤΗΣΗ ΤΟΥ EULER

Η συνάρτηση φ(n) του Euler είναι μια αριθμητική συνάρτηση (δηλαδή έχει πεδίο ορισμού το $\mathbb{N}$) η οποία μας δίνει το πλήθος των θετικών ακεραίων των μικρότερων (ή μικρότερων και ίσων) του n που είναι σχετικά πρώτοι προς τον n.
Δηλαδή μας δίνει το πλήθος των στοιχείων του περιορισμένου συνόλου υπολοίπων modn.

Ισχύουν τα παρακάτω:

1. ορίζουμε φ(1) = 1
2. εάν p πρώτος τότε φ(p) = p − 1
3. $\sum_{d|n}$ φ(d) = n (η άθροιση γίνεται πάνω σε όλους τους διαιρέτες του n)
4. η συνάρτηση $\varphi(n)$ είναι πολλαπλασιαστική δηλ. φ(m · n) = φ(m) · φ(n)
5. εάν p πρώτος και κ>0 τότε φ(p^k) = p^k-p^{k-1}
6. εάν n>1 και n=$p_1^{k_1}p_2^{k_2}$... $p_r^{k_r}$ τότε φ(n) = n(1 - $\frac{1}{p_1}$) (1 - $\frac{1}{p_2}$)... (1 - $\frac{1}{p_r}$)

3.3 ΒΑΣΙΚΑ ΘΕΩΡΗΜΑΤΑ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ

ΘΕΩΡΗΜΑ ΤΟΥ EULER Αν ο ΜΚΔ(a,m)=1 τότε $a^{\varphi(m)}=1$ modm.

Απόδειξη: Έστω $r_1, r_2, \ldots\ldots, r_{\varphi(m)}$ ένα περιορισμένο σύνολο υπολοίπων modm. Εφόσον ΜΚΔ(a,m)=1 έχουμε ότι και οι αριθμοί $ar_1, ar_2, \ldots\ldots, ar_{\varphi(m)}$ θα είναι όλοι πρώτοι προς τον m. Επίσης είναι όλοι μη ισοδύναμοι μεταξύ τους διότι αν $ar_i = ar_j$modm τότε αφού ΜΚΔ(a,m)=1, από τον κανόνα της απλοποίησης θα είχαμε $r_i = r_j$modm, το οποίο είναι άτοπο διότι οι αριθμοί r ανήκουν σε περιορισμένο σύνολο υπολοίπων.

Μπορούμε λοιπόν να αντιστοιχίσουμε κάθε αριθμό ar_i με κάποιον r_j έτσι ώστε $ar_i = r_j$modm και μάλιστα ο κάθε r_j ορίζεται μοναδικά για κάθε ar_i.

Αλλά και ο κάθε r_j αντιστοιχεί με κάποιον ar_i διότι έχουμε φ(m) το πλήθος r_j και φ(m) το πλήθος ar_i.

Άρα $r_1 \cdot r_2 \ldots r_{\varphi(m)} = ar_1 \cdot ar_2 \ldots ar_{\varphi(m)}$modm.

Θέτουμε $R = r_1 \cdot r_2 \ldots r_{\varphi(m)}$ και η προηγούμενη σχέση γίνεται

$$R = a^{\varphi(m)} \cdot R \text{ modm}$$

Αλλά ο ΜΚΔ(R,m)=1 διότι ο R είναι ένα γινόμενο φ(m) το πλήθος αριθμών όπου κάθε παράγοντας είναι πρώτος προς τον m, οπότε και ο R θα είναι πρώτος προς τον m.

Έτσι από τον κανόνα της απλοποίησης έχουμε :

$$a^{\varphi(m)} = 1 \text{ modm}$$

Τον 17ο αιώνα ο Fermat έκανε ένα σημαντικό βήμα στην ιστορία της πιστοποίησης πρώτου αριθμού με το θεώρημα που παρουσίασε, γνωστό και ως το μικρό θεώρημα του Fermat. Το θεώρημά του βασίστηκε στο θεώρημα του Euler γι' αυτό θεωρείται πόρισμά του.

ΜΙΚΡΟ ΘΕΩΡΗΜΑ ΤΟΥ FERMAT Εάν p πρώτος και (a,p)=1 τότε $a^{p-1} = 1 \bmod p$.

Απόδειξη: Αφού ο p είναι πρώτος τότε φ(p)=p-1 και από το προηγούμενο θεώρημα παίρνουμε το ζητούμενο.

ΟΡΙΣΜΟΣ Λέμε ότι ο $\bar{a}$ είναι ο **αντίστροφος** του a modn εάν $a\,\bar{a} = 1 \bmod n$.

ΠΟΡΙΣΜΑ Εάν ΜΚΔ(a,n)=1 τότε ο a έχει αντίστροφο και είναι μοναδικός modn.

Το επόμενο θεώρημα αποδίδεται στον Sir John Wilson (1741-1793), φαίνεται όμως ότι ο G.Leibniz το είχε ανακαλύψει πριν από το 1683.

ΘΕΩΡΗΜΑ ΤΟΥ WILSON Η ισοδυναμία $(m-1)! \equiv -1 \bmod m$ ισχύει αν και μόνο αν ο m είναι πρώτος.

Απόδειξη: Υποθέτουμε ότι ο m είναι πρώτος και θεωρούμε τους m-1 ακέραιους 1,2,…,m-1.

Αν a κάποιος από τους αριθμούς αυτούς τότε υπάρχει ο αντίστροφος $\bar{a}$ αυτού με $1 \le \bar{a} \le m-1$ και $a\,\bar{a} = 1 \bmod m$.

Πιθανόν $a=\bar{a}$ δηλαδή $a^2 \equiv 1 \bmod m$ δηλαδή ο a να συμπίπτει με τον αντίστροφό του. Όμως στην περίπτωση αυτή $a^2-1=km \Rightarrow (a+1)(a-1)=km \Rightarrow m|(a+1)(a-1)$

και αφού ο m είναι πρώτος θα ισχύει: $m|a+1$ ή $m|a-1$ άρα $a \equiv \pm 1 \bmod m$.

Στο γινόμενο $(m-2)(m-3)\ldots 3\cdot 2=(m-2)!$ αντιστοιχούμε σε κάθε αριθμό τον αντίστροφό του modm.

Έχουμε λοιπόν $(m-1)!=(m-1)(m-2)!=(m-1)1\cdot 1 \ldots 1 \equiv -1 \bmod m$.

Αντίστροφα Έστω ότι ο m δεν είναι πρώτος. Τότε υπάρχει a τέτοιο ώστε $1<a<m$ με $a|m$. Προφανώς $a|(m-1)!$ αφού ο παράγων a υπάρχει μέσα στο (m-1)!. Αν λοιπόν $(m-1)! \equiv -1 \bmod m$ τότε υπάρχει ακέραιος k με $(m-1)!+1=km$. Αφού $a|m$ και $a|(m-1)!$, ο a θα διαιρεί και την διαφορά τους άρα $a|1$ αδύνατο διότι υπετέθη $a>1$. Άρα όταν ο m δεν είναι πρώτος η ισοδυναμία $(m-1)! \equiv -1 \bmod m$ δεν μπορεί να ισχύει.

3.4 ΠΡΩΤΑΡΧΙΚΕΣ ΡΙΖΕΣ ΚΑΙ ΤΕΤΡΑΓΩΝΙΚΑ ΥΠΟΛΟΙΠΑ

ΟΡΙΣΜΟΣ Αν ο h είναι ο μικρότερος θετικός ακέραιος τέτοιος ώστε $a^h=1 \bmod m$ τότε λέμε ότι ο a **ανήκει στον εκθέτη** h modm.

ΘΕΩΡΗΜΑ Μια ικανή και αναγκαία συνθήκη για να ισχύει $a^b=1 \bmod m$ για κάποιον ακέραιο b είναι ΜΚΔ(a,m)=1.

Απόδειξη: Έστω ΜΚΔ(a,m)=d. Τότε d|a και d|m. Άρα ο d θα διαιρεί την διαφορά τους και έτσι θα διαιρεί και την διαφορά a^b-πολ.m. Όμως $a^b=1 \bmod m$ άρα d|1 και για να συμβαίνει αυτό πρέπει d=1. Άρα ΜΚΔ(a,m)=1.

Αντίστροφα Αν ΜΚΔ(a,m)=1 τότε $a^{\varphi(m)}=1 \bmod m$ από το θεώρημα του Euler οπότε $b=\varphi(m)$.

ΘΕΩΡΗΜΑ Αν ο a ανήκει στον εκθέτη h modm και $a^r=1 \bmod m$ τότε h|r.

Απόδειξη: Από τον αλγόριθμο του Ευκλείδη $r=kh+s$, $0 \leq s \leq h$.
Άρα $a^r=a^{kh+s}=(a^h)^k \cdot a^s=a^s \bmod m$ (διότι ο a ανήκει στον εκθέτη h modm).
Όμως $a^r=1 \bmod m$ άρα $a^s=1 \bmod m$. Αλλά ο h είναι ο μικρότερος εκθέτης για τον οποίο ισχύει $a^h=1 \bmod m$ οπότε s=0. Άρα r=kh δηλαδή h|r.

ΟΡΙΣΜΟΣ Αν ο ακέραιος g ανήκει στον εκθέτη φ(m) modm τότε ο g ονομάζεται **αρχική ή πρωταρχική ρίζα** modm (ΜΚΔ(g,m)=1).

ΘΕΩΡΗΜΑ Αν ο g είναι πρωταρχική ρίζα modm τότε οι δυνάμεις του g δηλαδή $g, g^2, \ldots, g^{\varphi(m)}$ είναι όλες μη ισοδύναμες modm και αποτελούν ένα περιορισμένο σύνολο υπολοίπων modm (ο g ονομάζεται και γεννήτορας).

Απόδειξη: Έστω $1 \leq s < r < \varphi(m)$ και $g^r=g^s \bmod m$ (δηλαδή υπάρχουν δύο ισοδύναμες δυνάμεις του g). Τότε όμως $g^r-g^s=km$ δηλαδή $m|g^r-g^s \Rightarrow m|g^s(g^{r-s}-1)$ και αφού $m \dagger g^s$ (ΜΚΔ(g,m)=1) έπεται ότι $m|g^{r-s}-1$ δηλαδή $g^{r-s}=1 \bmod m$.
Ο g όμως ανήκει στον εκθέτη φ(m) modm δηλαδή $g^{\varphi(m)}=1 \bmod m$ και ο φ(m) είναι ο μικρότερος τέτοιος εκθέτης. Άτοπο διότι $r-s < \varphi(m)$ και οι δυνάμεις του g είναι μη ισοδύναμες και αποτελούν περιορισμένο σύνολο υπολοίπων modm.

Ισχύουν τα παρακάτω:

1. Αν ο a ανήκει στον εκθέτη h modm και ΜΚΔ(k,h)=d τότε ο a^k ανήκει στον εκθέτη h/d modm.
2. Αν g μία πρωταρχική ρίζα modm τότε η g^r είναι επίσης μία πρωταρχική ρίζα modm αν και μόνο αν ΜΚΔ(r, φ(m))=1.
3. Αν υπάρχει κάποια πρωταρχική ρίζα modm τότε το πλήθος των αμοιβαία μη ισοδύναμων ριζών modm είναι φ(φ(m)).
4. Για κάθε πρώτο p, υπάρχουν φ(p-1) πρωταρχικές ρίζες modp.

Παράδειγμα

Έστω p=5 και {1,2,3,4} είναι ένα περιορισμένο σύνολο υπολοίπων mod5.

Από την 4 υπάρχουν πρωταρχικές ρίζες mod5 και το πλήθος των αμοιβαία μη ισοδύναμων θα είναι φ(4)=2.

Έχουμε $2^1=2 \bmod 5$ $3^1=3 \bmod 5$ $4^1=4 \bmod 5$

$2^2=4 \bmod 5$ $3^2=4 \bmod 5$ $4^2=1 \bmod 5$

$2^3=3 \bmod 5$ $3^3=2 \bmod 5$ $4^3=4 \bmod 5$

$2^4=1 \bmod 5$ $3^4=1 \bmod 5$ $4^4=1 \bmod 5$

Άρα οι 2,3 είναι πρωταρχικές ρίζες mod5.

ΟΡΙΣΜΟΣ Ο αριθμός a είναι **τετραγωνικό υπόλοιπο** modp εάν η εξίσωση $x^2 = a \bmod p$ έχει λύση, όπου p πρώτος αριθμός και ΜΚΔ(a,p)=1.

Συντομογραφίες: QR → Τετραγωνικό υπόλοιπο
QNR → Μη τετραγωνικό υπόλοιπο

ΘΕΩΡΗΜΑ(Κριτήριο του Euler) Ο αριθμός a είναι τετραγωνικό υπόλοιπο modp αν και μόνο αν $a^{\frac{p-1}{2}} = 1 \bmod p$.

Απόδειξη: Έστω ότι ο a είναι τετραγωνικό υπόλοιπο modp και έστω x ακέραιος με $x^2=a \bmod p$.

Αφού p†a ⇒ p†x δηλαδή ΜΚΔ(p,x)=1 , άρα

$$a^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1 \bmod p$$ (μικρό θεώρημα Fermat).

Αντίστροφα Έστω $a^{\frac{p-1}{2}}=1 \bmod p$ και g μία πρωταρχική ρίζα modp .
Υπάρχει ακέραιος r με $g^r=a \bmod p$,
οπότε $g^{\frac{r(p-1)}{2}} = a^{\frac{p-1}{2}} = 1 \bmod p$ και επειδή g πρωταρχική ρίζα θα ισχύει $g^{\varphi(p)}=g^{p-1}=1 \bmod p$, άρα $p-1 \mid \frac{r(p-1)}{2}$.
Άρα $\frac{r}{2}$ είναι ακέραιος και έστω $r=2s$ με s ακέραιο.
Θέτω $x=g^s$ οπότε έχουμε $x^2=g^{2s}=g^r=a \bmod p$. Άρα a τετραγωνικό υπόλοιπο modp.

<u>ΠΟΡΙΣΜΑ</u> Έστω g μία πρωταρχική ρίζα modp και έστω ΜΚΔ(a,p)=1. Έστω r ακέραιος με $g^r=a \bmod p$. Τότε ο r είναι ζυγός αν και μόνο αν το a είναι τετραγωνικό υπόλοιπο modp.

<u>ΘΕΩΡΗΜΑ</u> Αν p πρώτος αριθμός υπάρχουν $\frac{p-1}{2}$ ακριβώς μη ισοδύναμα τετραγωνικά υπόλοιπα του p που δίνονται από τη σχέση $1^2,2^2,\ldots,\left(\frac{p-1}{2}\right)^2 \bmod p$.

Απόδειξη: Έστω p μονός πρώτος. Θα προσδιορίσω τα a με $1 \le a \le p-1$ που είναι λύσεις της ισοδυναμίας $x^2=a \bmod p$.
Αλλά $x^2 = (p-x)^2 \bmod p$,διότι $x^2 - (p-x)^2 = \text{πολ.}p$.
Τα τετράγωνα των αριθμών στα σύνολα $\left\{1,2,\ldots,\frac{p-1}{2}\right\}$, $\left\{\frac{p+1}{2},\frac{p+1}{2}+1,\ldots,p-1\right\}$
είναι ισοδύναμα κατά ζεύγη (όχι με τη σειρά που αναγράφονται).
Άρα εξετάζω μόνο για τις τιμές του x με $1 \le x \le \frac{p-1}{2}$.
Αλλά τα τετράγωνα των αριθμών στο σύνολο $\left\{1,2,\ldots,\frac{p-1}{2}\right\}$ είναι όλα μη ισοδύναμα modp διότι αλλιώς η $x^2=a \bmod p$ θα είχε 4 μη ισοδύναμες λύσεις modp πράγμα που αντίκειται στο θεώρημα του Lagrange :

<<Το πλήθος των μη ισοδύναμων λύσεων της ισοδυναμίας $f(x)=0 \bmod p$ ποτέ δεν υπερβαίνει τον βαθμό του f(x)>>.

Άρα τα $\frac{p-1}{2}$ QR modp είναι ακριβώς οι αριθμοί $1^2,2^2,\ldots,\left(\frac{p-1}{2}\right)^2 \bmod p$.

ΛΗΜΜΑ Αν p πρώτος και (a,p)=1 τότε είτε $a^{\frac{p-1}{2}} = 1 \bmod p$ είτε $a^{\frac{p-1}{2}} = -1 \bmod p$.

Απόδειξη: Αφού ο p είναι πρώτος και (a,p)=1 από το Θεώρημα Fermat $a^{p-1}=1 \bmod p \Rightarrow a^{p-1}-1=$πολ.p $\Rightarrow$

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \bmod p$$, οπότε έχουμε το ζητούμενο.

Παράδειγμα

Τα QR του 11 είναι 5 αριθμοί.

$1^2=1 \bmod 11=10^2$ Άρα QR:{*1*,*3*,*4*,*5*,*9*}
$2^2=4 \bmod 11=9^2$ QNR:{*2*,*6*,*7*,*8*,*10*}
$3^2=9 \bmod 11=8^2$
$4^2=5 \bmod 11=7^2$
$5^2=3 \bmod 11=6^2$

3.5 ΣΥΜΒΟΛΟ LEGENDRE ΚΑΙ ΣΥΜΒΟΛΟ JACOBI

ΟΡΙΣΜΟΣ Το **σύμβολο Legendre** των α και p, όπου p≥ *3* πρώτος και α ακέραιος ορίζεται ως εξής:

(a/p)={■(1 $\alpha\nu\ \alpha \in QR\ mod p$@ -1 $\alpha\nu\ \alpha \notin QR\ mod p$ @ 0 $\alpha\nu$ α = $\pi o\lambda.p$)┤

Ιδιότητες:

1. $(a/p)=(b/p)$ αν α=bmodp
2. a^(($p-1$)/2) = (a/p) modp (α,p)=1 (Κριτήριο Euler)
3. $(ab/p)=(a/p)(b/p)$
4. $((-1)/p)=(-1)^{\frac{-1}{2}}$ (= {■(1 $\alpha\nu$ p = 1$mod4$@ -1 $\alpha\nu$ p = 3$mod4$)┤)
5. $(2/p)=(-1)^{\frac{2-1}{8}}$ (= { ■(1 $\alpha\nu$ p = ±1$mod8$ @ -1 $\alpha\nu$ p = ±3$mod8$)┤)
6. $(p/q)(q/p)=(-1)^{\frac{-1}{2}\cdot\frac{-1}{2}}$ p,q πρώτοι, **Τετραγωνικός νόμος αντιστροφής** (QRL του Gauss)

ΛΗΜΜΑ ΤΟΥ GAUSS Αν p πρώτος και (α,p)=1 τότε (a/p)= $〚(-1)〛$ ^s όπου s το πλήθος των στοιχείων του συνόλου $\{\alpha, 2\alpha, 3\alpha, \dots, (p-1)/2\ a\}$ που είναι μεγαλύτερα του $p/2$.

ΟΡΙΣΜΟΣ Το **σύμβολο Jacobi** για ζεύγη α,n με n≥3 και α ακέραιος είναι μία γενίκευση του συμβόλου του Legendre όπου ο n δεν είναι πρώτος αριθμός. Αναλυτικά από το ΘΘΑ έστω n=p_1^(k_1) p_2^(k_2) … p_r^(k_r), το σύμβολο Jacobi θα είναι :

(a/n) =(a/p_1)^(k_1) (a/p_2)^(k_2)… (a/p_r)^(k_r), όπου (a/p_i) το σύμβολο του Legendre.

Παρατήρηση:Το σύμβολο του Jacobi δεν δίνει πληροφορία αν το α είναι τετραγωνικό υπόλοιπο ή όχι.

Ιδιότητες:

1. $(a/n)=(b/n)$ αν α=bmodn
2. $(ab/n)=(a/n)(b/n)$
3. $(a/mn)=(a/m)(a/n)$
4. $((-1)/n)=〚(-1)〛$^$((n-1)/2)$
5. $(2/n)=〚(-1)〛$^$((n^2-1)/8)$

<u>Παράδειγμα</u>

Θα υπολογίσουμε το σύμβολο Jacobi $\left(\frac{1050}{1573}\right)$.

$1573=11^2\cdot 13$, $1050=2\cdot 3\cdot 5^2\cdot 7$

$\left(\frac{1050}{1573}\right)=\left(\frac{1050}{11\cdot 11\cdot 13}\right)=\left(\frac{1050}{11}\right)\left(\frac{1050}{11}\right)\left(\frac{1050}{13}\right)=\left(\frac{1050}{11}\right)^2\left(\frac{1050}{13}\right)=1\cdot\left(\frac{1050}{13}\right)=\left(\frac{1050}{13}\right)=\left(\frac{1050}{13}\right)=\left(\frac{10}{13}\right)=\left(\frac{2\cdot 5}{13}\right)=\left(\frac{2}{13}\right)\left(\frac{5}{13}\right)$

$\left(\frac{2}{13}\right)=(-1)^{\frac{13^2-1}{8}}=(-1)^{21}$=-1

13=3mod5 και 5=2mod3

$\left(\frac{5}{13}\right)\left(\frac{13}{5}\right)=(-1)^{12}$=1(QRL)

$\left(\frac{3}{5}\right)\left(\frac{5}{3}\right)=(-1)^2$=1(QRL)

Άρα $\left(\frac{5}{13}\right)=\left(\frac{13}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=(-1)^1$=-1

$\left(\frac{1050}{1573}\right)$=(-1)(-1)=1

Διαφορετικά θα μπορούσαμε να υπολογίσουμε τα τετραγωνικά υπόλοιπα mod13, ο 13 είναι πρώτος αριθμός οπότε έχει 6 μη ισοδύναμα τετραγωνικά υπόλοιπα και υπολογίζονται ως εξής :

1^2=1mod13 4^2=3mod13 QRmod13:{*1*,*3*,*4*,*9*,*10*,*12*}

2^2=4mod13 5^2=12mod13

3^2=9mod13 6^2=10mod13

Άρα $\left(\frac{2}{13}\right)=\left(\frac{5}{13}\right)$=-1 (διότι 2, 5 δεν είναι τετραγωνικά υπόλοιπα mod13).

ΚΕΦΑΛΑΙΟ 4 : ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΩΤΟΥ

4.1 ΑΠΕΙΡΙΑ ΚΑΙ ΘΕΩΡΗΜΑ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ

Το επόμενο θεώρημα οφείλεται στον **Ευκλείδη** (βιβλίο 9 των Στοιχείων). Ο Ευκλείδης από την Αλεξάνδρεια ήταν Έλληνας μαθηματικός που δίδαξε και πέθανε στην Αλεξάνδρεια της Αιγύπτου. Δεν ξέρουμε ακριβείς ημερομηνίες γέννησης και θανάτου του. Γεννήθηκε περίπου το 325πΧ και πέθανε το 265πΧ αν και υπάρχουν αμφιβολίες λέγεται ότι μαθήτευσε στην ακαδημία του Πλάτωνα. Το όνομά του είναι συνώνυμο με την γεωμετρία καθώς η γεωμετρία που περιέγραψε στα Στοιχεία (13 βιβλία) ονομάστηκε Ευκλείδεια και έχει χρησιμοποιηθεί σαν βάση για την γεωμετρική εκπαίδευση όλης της Δύσης τα τελευταία 2000 χρόνια.

ΘΕΩΡΗΜΑ Υπάρχουν άπειροι πρώτοι αριθμοί.

Απόδειξη: Γράφουμε τους πρώτους κατά την φυσική τους διάταξη και έστω p_n ο τελευταίος πρώτος με $1<p_1<p_2<\ldots<p_n$.

Θεωρώ τον φυσικό αριθμό $P= p_1.p_2\ldots p_n+1$ όπου προφανώς P όχι πρώτος αφού $P>p_n$. Θα υπάρχει λοιπόν πρώτος p_k με $p_k|P$ όπου $1\leq\kappa\leq n$.

Αλλά τότε θα ισχύουν οι σχέσεις:

$p_k| p_1.p_2\ldots p_n$, αφού ο p_k είναι ένας παράγοντας του γινομένου

$p_k|P \Rightarrow p_k| P- p_1.p_2\ldots p_n \Rightarrow p_k|1$ άτοπο αφού $p_k>1$.

Το άτοπο προέκυψε διότι δεχτήκαμε την ύπαρξη του τελευταίου πρώτου αριθμού άρα υπάρχουν άπειροι πρώτοι αριθμοί.

Το παρακάτω θεώρημα γνωστό ως το θεώρημα των πρώτων αριθμών (PNT, Prime Number Theorem) περιγράφει την κατανομή των πρώτων αριθμών και δηλώνει ότι αν διαλέξουμε τυχαία έναν αριθμό μικρότερο ή ίσο του x τότε η πιθανότητα να είναι πρώτος είναι περίπου $1/lnx$.

ΘΕΩΡΗΜΑ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ

Έστω π(x) το πλήθος των πρώτων που δεν ξεπερνούν το x, τότε

$$\lim_{\top}(x \to \infty) \quad [\![(\pi(x))/(x/lnx)]\!] \quad = 1 \quad \text{ή} \quad \pi(x) \sim x/lnx \ .$$

Άρα εάν επιλέξουμε τυχαία έναν αριθμό και θέλουμε να αποφανθούμε για το εάν είναι πρώτος μπορούμε να υπολογίσουμε πόσους αριθμούς κατά μέσο όρο θα εξετάσουμε χρησιμοποιώντας κριτήρια πιστοποίησης πρώτων για να καταλήξουμε στο αποτέλεσμα.

Στη συνέχεια θα παρουσιάσουμε τα κριτήρια πιστοποίησης πρώτων αριθμών των Fermat, Miller-Rabin και Solovay-Strassen τα οποία είναι πιθανοθεωρητικά τεστ, δηλαδή μπορούν να δώσουν και λάθος απάντηση, με μικρή πιθανότητα κάποιες φορές.

4.2 ΤΟ ΚΡΙΤΗΡΙΟ ΤΟΥ FERMAT

Το μικρό θεώρημα του Fermat λέει ότι εάν ο n είναι πρώτος αριθμός και $1 \leq \alpha < n$ με (α,n)=1 τότε $\alpha^{n-1}=1 \bmod n$. Συνεπώς εάν βρούμε ένα α για το οποίο δεν ισχύει η τελευταία ισότητα δηλαδή $\alpha^{n-1} \neq 1 \bmod n$ τότε ο n θα είναι σύνθετος. Στην περίπτωση που βρούμε α για το οποίο $\alpha^{n-1}=1 \bmod n$ δεν μπορούμε να αποφανθούμε αν ο n είναι πρώτος ή σύνθετος. Το αντίστροφο του θεωρήματος του Fermat δεν ισχύει. Το θεώρημα αυτό είναι ένα αρνητικό κριτήριο για την πιστοποίηση πρώτων αριθμών και η πολυπλοκότητα της διαδικασίας είναι $O((logn)$^3).

ΟΡΙΣΜΟΣ Ο α , $1 \leq \alpha < n$, ονομάζεται **F-μάρτυρας** για τον n αν $\alpha^{n-1} \neq 1 \bmod n$.

ΟΡΙΣΜΟΣ Ο α , $1 \leq \alpha < n$, ονομάζεται **F-ψεύτης** για τον σύνθετο μονό n αν $\alpha^{n-1}=1 \bmod n$. Τότε ο n λέγεται ψευδοπρώτος με βάση το α.

ΠΑΡΑΤΗΡΗΣΗ: Για κάθε μονό σύνθετο αριθμό n, τετριμμένα έχουμε ότι οι 1,n-1 είναι F-ψεύτες αφού $1^{n-1}=1 \bmod n$ και $(n-1)^{n-1}=(-1)^{n-1}=1 \bmod n$ (αφού ο n είναι ζυγός).

Το κριτήριο του Fermat λειτουργεί με α=2 για όλους τους σύνθετους αριθμούς n≤340 όμως :

$2^{340}=(2^{10})^{34}=(1)^{34}=1 \bmod 341$, ο 2 είναι F-ψεύτης για τον 341 ή ο 341 είναι ψευδοπρώτος ως προς τη βάση 2.

Παράδειγμα

$n=91=7 \cdot 13$

$2^{90}=(2^{10})^{9}=(23)^{9}=(23^{3})^{3}=64^{3}=64 \bmod 91$, οπότε ο 91 είναι σύνθετος.

$3^{90}=(3^{6})^{15}=1^{15}=1 \bmod 91$, το κριτήριο δεν δίνει αποτέλεσμα.

ΑΛΓΟΡΙΘΜΟΣ 1 (FERMAT TEST)

Είσοδος: Μονός φυσικός n≥3.

Μέθοδος: 1. Επιλέγω τυχαία α ∈ {2,3, … , $n-2$}

2. εάν $a^{n-1} \neq 1 \bmod n$

3. τότε επιστροφή 1

4. αλλιώς επιστροφή 0

Αν ο αλγόριθμος δώσει 1 σημαίνει ότι έχει βρει έναν F-μάρτυρα α για τον n άρα ο n είναι σύνθετος. Εάν όμως δώσει 0 δεν μπορούμε να αποφανθούμε για τον n καθώς υπάρχουν α που είναι F-ψεύτες. Όμως για πολλούς σύνθετους n υπάρχει αφθονία F-μαρτύρων οπότε το κριτήριο πετυχαίνει με σταθερή πιθανότητα.

Η χρονική διάρκεια του αλγορίθμου είναι:

Η γρήγορη εκθετοποίηση $a^{n-1} \bmod n$ είναι $O(logn)$ αριθμητικές πράξεις και $O((logn)^3)$ πράξεις bit.

ΘΕΩΡΗΜΑ Αν n≥3 ένας μονός σύνθετος αριθμός που έχει τουλάχιστον έναν F-μάρτυρα α, τότε το τεστ του Fermat αν εφαρμοστεί στον n δίνει απάντηση 1 με πιθανότητα μεγαλύτερη του 1/2.

Απόδειξη: Το σύνολο $L_n^F=\{a| 1 \leq a < n \ με \ a^(n-1) \ mod n = 1\}$ των F-ψευτών για το n είναι προφανώς υποσύνολο του $\mathbb{Z}_n^*$. Θα δείξουμε ότι είναι και υποομάδα της $\mathbb{Z}_n^*$. Αφού η $\mathbb{Z}_n^*$ είναι πεπερασμένη ομάδα (με $|\mathbb{Z}_n^*|=\varphi(n)$) αρκεί να δείξουμε ότι:

1) $1 \in L_n^F$ που ισχύει διότι $1^{n-1}=1 \bmod n$ τετριμμένα.

2) Η L_n^F είναι κλειστή ως προς την πράξη πολλαπλασιασμός modn διότι

$a^{n-1} \bmod n=1$ και $b^{n-1} \bmod n=1$ συνεπάγεται $(ab)^{n-1}=a^{n-1}b^{n-1}=1 \cdot 1=1 \bmod n$.

Αφού το $\mathbb{Z}\_n\hat{}*$ έχει τουλάχιστον ένα στοιχείο, το $L\_n\hat{}F$ είναι γνήσια υποομάδα του $\mathbb{Z}\_n\hat{}*$. Από το θεώρημα του Lagrange λοιπόν η τάξη του θα είναι γνήσιος διαιρέτης του $\varphi(n)$, όπου $\varphi(n)$<*n-1* (διότι ο n είναι σύνθετος), άρα $|L\_n\hat{}F| \leq (n-2)/2$. Άρα η πιθανότητα μία τυχαία επιλογή από το $\{2,3,\dots,n-2\}$ να ανήκει στο $L\_n\hat{}F$-$\{1,n-1\}$ είναι το πολύ $((n-2)/2-2)/(n-3) = (n-6)/(2(n-3)) < \frac{1}{2}$.

Ένας αλγόριθμος όμως που δίνει πιθανότητα λάθους < 1/2 φυσικά δεν είναι αρκετά έμπιστος. Οπότε θα είχαμε καλύτερα αποτελέσματα μετά από επαναλήψεις του τεστ του Fermat και ο αλγόριθμος που περιγράφει την διαδικασία είναι ο παρακάτω :

ΑΛΓΟΡΙΘΜΟΣ 2 (ITERATED FERMAT TEST)

Είσοδος: Μονός φυσικός n≥3 και φυσικός $\ell \geq 1$.

Μέθοδος: 1. Επαναλαμβάνω ℓ φορές

2. επιλέγω τυχαία $a \in \{2,3,\dots,n-2\}$

3. εάν $a^{n-1} \neq 1 \bmod n$ επιστροφή 1

4. αλλιώς επιστροφή 0

Επίσης στον αλγόριθμο 2 εάν η έξοδος είναι 1 ο αλγόριθμος έχει βρει έναν F-μάρτυρα άρα ο n σύνθετος.

Αν ο n είναι σύνθετος και υπάρχει τουλάχιστον ένας F-μάρτυρας a με (a,n)=1 η πιθανότητα να επιλέξουμε F-ψεύτη μετά από ℓ δοκιμές γίνεται μικρότερη από $\left(\frac{1}{2}\right)^{\ell}$. Άρα για μεγάλα ℓ η πιθανότητα λάθους γίνεται αρκετά μικρή.

Υπάρχουν όμως κάποιοι σπάνιοι αριθμοί που ονομάζονται αριθμοί Carmichael που δεν ικανοποιούν το τεστ του Fermat διότι όλα τα στοιχεία του $\mathbb{Z}\_n\hat{}*$ είναι F-ψεύτες. Οι αριθμοί αυτοί είναι άπειροι.

4.3 ΟΙ ΑΡΙΘΜΟΙ CARMICHAEL

ΟΡΙΣΜΟΣ Ένας μονός σύνθετος αριθμός n λέγεται **αριθμός Carmichael** αν

$$a^{n-1} \bmod n = 1 \quad \forall\, a \in \mathbb{Z}\_n\text{^}*.$$

ΠΑΡΑΤΗΡΗΣΕΙΣ

- Ο μικρότερος αριθμός Carmichael είναι ο $561 = 3 \cdot 11 \cdot 17$.
- Το 1994 απεδείχθει ότι υπάρχουν άπειροι αριθμοί Carmichael και μάλιστα ομοιόμορφα κατανεμημένοι.(Alford-Granville-Pomerance)
- Ο Richard Pinch του πανεπιστημίου του Cambridge υπολόγισε τους 105.212 αριθμούς Carmichael τους μικρότερους από τον 10^{15}.

ΘΕΩΡΗΜΑ (**Alwin Korselt**) Ένας περιττός σύνθετος ακέραιος $n \geq 3$ είναι αριθμός Carmichael αν και μόνο αν είναι ελεύθερος τετραγώνου (δηλαδή δεν διαιρείται από το τετράγωνο ενός πρώτου) και κάθε πρώτος διαιρέτης p του n είναι τέτοιος ώστε να ισχύει $p-1 | n-1$.

Απόδειξη: Ας υποθέσουμε ότι ο n είναι αριθμός Carmichael και έστω p ένας πρώτος διαιρέτης του n. Έστω p^t η μεγαλύτερη δύναμη του p που διαιρεί τον n και g μία αρχική ρίζα $\bmod p^t$. Καθώς $(p^t, n/p^t)=1$ υπάρχει ακέραιος b με

$$b = g \bmod p^t \quad \text{και} \quad b = 1 \bmod n/p^t.$$

Τότε $(b,p)=1$, $(b, n/p^t)=1$ και επομένως $(b,n)=1$. Καθώς ο n είναι αριθμός Carmichael και ο p^t διαιρέτης του θα ισχύει

$$b^{n-1} = 1 \bmod p^t.$$

Επίσης ο b είναι αρχική ρίζα $\bmod p^t$. Άρα $\varphi(p^t) | n-1$ και επομένως $p^{t-1}(p-1) | n-1$. Συνεπώς έχουμε $t=1$ και $p-1 | n-1$.

Αντιστρόφως, υποθέτουμε ότι ο n είναι ελεύθερος τετραγώνου και για κάθε πρώτο διαιρέτη p του n ισχύει p-1|n-1. Έστω a ακέραιος με (a,n)=1.

Αν p πρώτος διαιρέτης του n, τότε

$$a^{p-1}=1 \bmod p$$

και καθώς p-1|n-1, έχουμε

$$a^{n-1}=1 \bmod p$$

Τέλος, επειδή ο n είναι ελεύθερος τετραγώνου ισχύει

$$a^{n-1}=1 \bmod n$$

ΘΕΩΡΗΜΑ Αν ο n είναι αριθμός Carmichael τότε ο n είναι γινόμενο τουλάχιστον τριών διαφορετικών παραγόντων.

Απόδειξη: Έστω n ένας αριθμός Carmichael, τότε ο n είναι σύνθετος.

Ας υποθέσουμε ότι n=pq, όπου p,q είναι πρώτοι με p>q.

Από το προηγούμενο θεώρημα έχουμε ότι p-1|n-1

Καθώς n-1=(p-1)q+q-1, παίρνουμε ότι p-1|q-1 και επομένως $p \leq q$ που είναι άτοπο.

Άρα ο n έχει τουλάχιστον τρείς πρώτους παράγοντες.

ΚΑΤΑΣΚΕΥΗ (Jack Chernick 1939) Αν t ακέραιος τέτοιος ώστε 6t+1, 12t+1 και 18t+1 να είναι πρώτοι, τότε ο ακέραιος n = (6t+1)(12t+1)(18t+1) είναι αριθμός Carmichael.

4.4 ΤΟ ΚΡΙΤΗΡΙΟ SOLOVAY-STRASSEN

Το 1977 περίπου οι Solovay και Strassen δημοσίευσαν έναν πιθανοτικό αλγόριθμο που στηρίζεται στο Κριτήριο του Euler. Συγκεκριμένα αν p μονός πρώτος και (a,p)=1 τότε $\left(\frac{a}{p}\right)= a^{\frac{p-1}{2}}$ modp. Εάν a είναι τετραγωνικό υπόλοιπο modp θα ισχύει $\left(\frac{a}{p}\right)= a^{\frac{p-1}{2}}$ =1modp και εάν a δεν είναι τετραγωνικό υπόλοιπο modp θα έχουμε $\left(\frac{a}{p}\right)= a^{\frac{p-1}{2}}$ = -1modp. Άρα λοιπόν εάν p μονός πρώτος τότε $a^{\frac{p-1}{2}} \cdot \left(\frac{a}{p}\right)=$ 1modp για κάθε $a\in \{1,2,\dots,p-1\}$. Καταλήγουμε λοιπόν στο ότι εάν $a^{\frac{n-1}{2}} \cdot \left(\frac{a}{n}\right) \neq 1$modn τότε ο n δεν είναι πρώτος, για μονό $n\geq 3$ και $a\in \{2,\dots,n-2\}$. Η πολυπλοκότητα της διαδικασίας είναι $O((logn)^3)$.

ΟΡΙΣΜΟΣ Έστω n μονός σύνθετος αριθμός. Ο a με $1\leq a\leq n-1$ λέγεται **Ε-μάρτυρας** του n εάν $a^{\frac{n-1}{2}} \cdot \left(\frac{a}{n}\right) \neq 1$modn.

ΟΡΙΣΜΟΣ Έστω n μονός σύνθετος αριθμός. Ο a με $1\leq a\leq n-1$ λέγεται **Ε-ψεύτης** για τον n εάν $a^{\frac{n-1}{2}} \cdot \left(\frac{a}{n}\right) =$ 1modn.

Παράδειγμα

Έστω $n=325=13\cdot 5^2$.

- για a=15 έχουμε (325,15)=5 άρα $\left(\frac{15}{325}\right)$=0. Ο 15 είναι Ε- μάρτυρας του 325.
- για a=2, $2^{162}=2^{2\cdot 81}=((2^9)^9)^2=(187^9)^2=((187^3)^3)^2=(203^3)^2=252^2=129$mod325.

$$\left(\frac{2}{325}\right)=\left(\frac{2}{13\cdot 5^2}\right)=\left(\frac{2}{13}\right)\left(\frac{2}{5^2}\right)=\left(\frac{2}{13}\right)\left(\frac{2}{5}\right)^2=\left(\frac{2}{13}\right)=(-1)^{\frac{13^2-1}{8}}=-1.$$

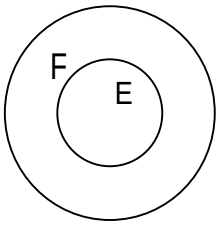
Άρα ο 2 είναι Ε-μάρτυρας του 325.

- για a=7, $7^{162}=((7^9)^9)^2=(307^9)^2=((307^3)^3)^2=(18^3)^2=307^2=324=-1$mod325

$\left(\frac{7}{325}\right)= \left(\frac{7}{13\cdot 5^2}\right)=\left(\frac{7}{13}\right)\left(\frac{7}{5}\right)^2=\left(\frac{7}{13}\right)=$ -1 διότι το $7\notin QR$.

Άρα ο 7 είναι Ε-ψεύτης για τον 325.

ΛΗΜΜΑ Έστω ο μονός σύνθετος n ≥3 τότε κάθε E-ψεύτης του n είναι επίσης και F-ψεύτης του n.



Απόδειξη: Αν α είναι E- ψεύτης τότε $〚\alpha〛$^$((n-1)/2) \cdot (\alpha/n)$modn=1 αλλά τότε (α/n)=1 ή -1, οπότε τετραγωνίζοντας έχω [$〚\alpha〛$^$((n-1)/2) \cdot (\alpha/n)$]^2modn=1⇒ a^{n-1}modn=1. Άρα ο α είναι και F-ψεύτης.

Θα δείξουμε ότι το $\mathbb{Z}\_n$^$*$ περιέχει πάντα έναν E- μάρτυρα και οι E- ψεύτες είναι το πολύ τα μισά στοιχεία του $\mathbb{Z}\_n$^$*$.

ΛΗΜΜΑ Έστω n≥3 ένας μονός σύνθετος. Τότε το σύνολο L_n^E={a| α $είναι$ $E-ψεύτης$ $του$ n } είναι γνήσια υποομάδα του $\mathbb{Z}\_n$^$*$.

Απόδειξη: Γνωρίζουμε ότι το σύνολο των F-ψευτών του n είναι υποσύνολο του $\mathbb{Z}\_n$^$*$ και από το προηγούμενο Λήμμα και το σύνολο των E-ψευτών είναι υποσύνολο του $\mathbb{Z}\_n$^$*$. Θα εφαρμόσουμε το κριτήριο για υποομάδες για να δείξουμε ότι το σύνολο των E-ψευτών είναι υποομάδα του $\mathbb{Z}\_n$^$*$.

Τέλος θα δείξουμε ότι το $\mathbb{Z}\_n$^$*$ περιέχει τουλάχιστον έναν E-μάρτυρα.

Το κριτήριο λέει ότι ένα υποσύνολο του $\mathbb{Z}\_n$^$*$ είναι υποομάδα εάν :

1. το 1 ανήκει στο υποσύνολο,
2. το υποσύνολο είναι κλειστό ως προς την πράξη της υποομάδας .

Προφανώς το 1 είναι E-ψεύτης άρα 1∈ L_n^E. Υποθέτουμε ότι a,b ∈ $\mathbb{Z}\_n$^$*$ είναι

E-ψεύτες για τον n. Τότε

$〚(\alpha \cdot b)〛$^$((n-1)/2) \cdot ((\alpha \cdot b)/n)$modn = $〚\alpha〛$^$((n-1)/2) \cdot (\alpha/n)$modn $\cdot$ $〚b〛$^$((n-1)/2) \cdot (b/n)$modn = 1·1=1

Άρα $L\_n\text{^}E$ είναι υποομάδα. Θα δείξουμε ότι υπάρχει τουλάχιστον ένας E- μάρτυρας στο $\mathbb{Z}\_n\text{^}*$ οπότε το $L\_n\text{^}E$ είναι γνήσια υποομάδα του $\mathbb{Z}\_n\text{^}*$.

Περίπτωση 1η : Έστω $p^2|n$ για κάποιο πρώτο $p\geq 3$. Από το θεώρημα περί αριθμών Carmichael είδαμε πώς κατασκευάζουμε έναν F-μάρτυρα στο $\mathbb{Z}\_n\text{^}*$,ο οποίος από το προηγούμενο Λήμμα θα είναι και E-μάρτυρας.

Περίπτωση 2η: Έστω ότι ο n είναι γινόμενο κάποιων διαφορετικών πρώτων. Τότε θέτουμε $n=p\cdot m$ όπου p μονός πρώτος και $m\geq 3$ μονός με $p\nmid m$.

Έστω $b\in \mathbb{Z}\_p\text{^}*$ κάποιο μη τετραγωνικό υπόλοιπο modp, δηλαδή (b/p)=-1. Από το ΚΘΥ (Κινέζικο Θεώρημα Υπολοίπων) υπάρχει $1\leq a<n$ με :

$$a=b \bmod p \quad (1)$$

$$a=1 \bmod m \quad (2)$$

Ισχυρίζομαι ότι $a\in \mathbb{Z}\_n\text{^}*$ και ο a είναι E-μάρτυρας του n.

Απόδειξη ισχυρισμού: $p\nmid a$ άρα $a\neq$ πολ.p, διότι από (1) a-b=πολ.p και αν a=πολ.p θα είχα b=0 ή b=πολ.p , ενώ (b/p)=-1.

Επίσης από (2) (a,m)=1, διότι a-1=πολ.m άρα $a\in \mathbb{Z}\_n\text{^}*$.

Ακόμα $(\alpha/n)=(\alpha/p)\cdot(\alpha/m)=(b/p)\cdot(1/m)=(b/p)\cdot 1=-1\cdot 1=-1$.

Αν ο a ήταν E-ψεύτης θα είχα $[\![\alpha]\!]\text{^}((n-1)/2)$ =-1modn αφού (α/n)=-1. Όμως n=πολ.m και θα είχα $[\![\alpha]\!]\text{^}((n-1)/2)$ =-1modm, που έρχεται σε αντίθεση με το ότι a=1modm(η σχέση (2)). Άρα ο a είναι E-μάρτυρας για το n.

Συμπέρασμα: Το πλήθος των E-ψευτών του n είναι γνήσιος διαιρέτης του $|\mathbb{Z}\_n\text{^}*|=\varphi(n)$ άρα τουλάχιστον τα μισά στοιχεία του $\mathbb{Z}\_n\text{^}*$ είναι E-μάρτυρες.

ΚΡΙΤΗΡΙΟ SOLOVAY-STRASSEN

Είσοδος: Μονός ακέραιος n≥3

Μέθοδος: 1. Έστω α τυχαία επιλογή από το $\{2, \dots, n-2\}$

2. Αν $〚\alpha〛$^$((n-1)/2) \cdot (\alpha/n)$modn $\neq 1$

3. Επιστροφή 1

4. Αλλιώς επιστροφή 0

Αν στην έξοδο έχω 1 ο n είναι σύνθετος και αν έχω 0 είναι πρώτος.

Η πιθανότητα να πάρω στην έξοδο 0 ενώ ο n είναι σύνθετος είναι μικρότερη της 1/2.

Στη γραμμή 2 η εκθετοποίηση $〚\alpha〛$^$((n-1)/2)$ modn γίνεται με fast exponentiation και ο υπολογισμός του συμβόλου Jacobi γίνεται από τον παρακάτω αλγόριθμο.

4.5 Ο ΑΛΓΟΡΙΘΜΟΣ ΓΙΑ ΤΟ ΣΥΜΒΟΛΟ ΤΟΥ JACOBI

Είσοδος: Ακέραιος a, μονός ακέραιος $n \geq 3$

Μέθοδος: 0. b,c,s ακέραιοι

1. $b \leftarrow a \bmod n$; $c \leftarrow n$;
2. $s \leftarrow 1$
3. while $b \geq 2$ repeat
4. while $4|b$ repeat $b \leftarrow b|4$
5. if $2|b$ then
6. if $c \bmod 8 \in \{3,5\}$ then $s \leftarrow (-s)$
7. $b \leftarrow b|2$
8. if $b=1$ then break
9. if $b \bmod 4 = c \bmod 4 = 3$ then $s \leftarrow (-s)$
10. $(b,c) \leftarrow (c \bmod b, b)$;
11. return $s \cdot b$;

4.6 ΤΟ ΚΡΙΤΗΡΙΟ MILLER-RABIN

Ο Miller περί το 1975 επινόησε έναν ντετερμινιστικό αλγόριθμο που βασιζόταν στην εκτεταμένη υπόθεση του Riemann, η οποία δεν έχει αποδειχθεί μέχρι σήμερα και αποτελεί ένα από τα άλυτα ανοιχτά προβλήματα της Θεωρίας Αριθμών. Λίγο αργότερα, το 1980, ο Rabin τροποποίησε τον αλγόριθμο αυτό σε πιθανοτικό. Ο τελευταίος αλγόριθμος γνωστός ως κριτήριο Miller-Rabin, ελαφρά τροποποιημένος από τον Knuth, χρησιμοποιείται περισσότερο στην πράξη σήμερα. Η πολυπλοκότητα του είναι $O((logn)$^3).

Το κριτήριο βασίζεται στο παρακάτω θεώρημα.

ΘΕΩΡΗΜΑ Έστω n πρώτος και n-1=u·2^k, όπου u είναι μονός ακέραιος και k θετικός ακέραιος. Αν a είναι ακέραιος ο οποίος δεν διαιρείται από τον n, τότε είτε ισχύει :

a^u=1modn

είτε υπάρχει r∈ {0,1, … , $k-1$} με

α^(2^$r \cdot u$) =-1modn

Απόδειξη: Έστω d=$ord_n(a^u)$ δηλαδή $(a^u)^d$=1modn.

Καθώς ο n είναι πρώτος έχουμε $[\![(\alpha$^$u)]\!]$ ^(2^k) =1modn και επομένως ο d διαιρεί τον 2^k.

Αν d=1 τότε a^u =1modn.

Αν d>1 τότε d=2^{ℓ} με 1≤ ℓ ≤k και επομένως $ord_n(a$^(2^($\ell - 1$) $\cdot u$))=2.

Από την άλλη πλευρά, μόνο η κλάση του -1 μέσα στο $\mathbb{Z}\_n$^ $*$ έχει τάξη ίση με 2 και κατά συνέπεια έχουμε:

a^(2^($\ell - 1$) $\cdot u$) = -1 modn

ΟΡΙΣΜΟΣ Έστω n≥3 μονός θετικός ακέραιος και γράφουμε n-1=u·2^k με u μονό και k ≥ *1*. Ο αριθμός a, 1≤a<n ονομάζεται **Α-μάρτυρας** για τον n εάν a^u≠1modn και α^($[\![u \cdot 2]\!]$ ^i) ≠-1 modn για όλα τα i με 0≤ i <k.

ΟΡΙΣΜΟΣ Εάν ο n είναι σύνθετος και ο α δεν είναι Α-μάρτυρας του n, τότε ο α ονομάζεται **Α-ψεύτης** του n.

ΚΡΙΤΗΡΙΟ MILLER-RABIN

Είσοδος: Μονός φυσικός $n\geq 3$.

Μέθοδος: 1. Βρίσκω μονό u και $k\geq 1$ ώστε $n-1=u\cdot 2^k$.

2. Επιλέγω τυχαίο $a\in\{2,\dots,n-2\}$.

3. $b\leftarrow a^u \bmod n$.

4. εάν b=1 ή b=-1 επιστροφή 0.

5. επανάληψη k-1 φορές.

6. $b\leftarrow b^2 \bmod n$.

7. εάν b=-1 επιστροφή 0.

8. εάν b=1 επιστροφή 1.

9. επιστροφή 1.

Επιστροφή 0 σημαίνει ότι ο n είναι πιθανά πρώτος και επιστροφή 1 σημαίνει ότι είναι σύνθετος. Η πιθανότητα να πάρω στην έξοδο 0 ενώ ο n είναι σύνθετος είναι μικρότερη της 1/4.

Το κριτήριο Miller-Rabin αναλυτικά:

- Έστω $n\geq 3$ μονός φυσικός. Θέτω $n-1=u\cdot 2^k$ με u μονό και $k\geq 1$.
- Επιλέγουμε τυχαίο α, $2\leq a\leq n-2$.
- Υπολογίζω τον $b_0=a^u \bmod n$. Αν $b_0=\pm 1$ σταματάμε και ο n είναι πιθανά πρώτος.
- Αλλιώς υπολογίζουμε τον $b_1=b_0^2 \bmod n$.

Αν $b_1=1 \mod n$ τότε ο n είναι σύνθετος και ο ΜΚΔ(b_0-1,n) δίνει μη τετριμμένο παράγοντα του n.
Αν $b_1=-1 \mod n$, ο n είναι πιθανά πρώτος.

- Αλλιώς υπολογίζουμε $b_2=b_1^2 \mod n$.
  Αν $b_2=1 \mod n$ τότε ο n είναι σύνθετος .
  Αν $b_2=-1 \mod n$, ο n πιθανά πρώτος.

- Συνεχίζουμε έως ότου είτε σταματήσουμε είτε φτάσουμε στο b_{k-1}.
  Αν $b_{k-1} \neq -1 \mod n$ τότε ο n είναι σύνθετος.

Παράδειγμα

$n=561 \quad n-1=560=35 \cdot 16=35 \cdot 2^4$, $k=4$,$u=35$

Έστω $a=2$.

Τότε $b_0=2^{35}=263 \mod 561$

$b_1=263^2=166 \mod 561$

$b_2=166^2=67 \mod 561$

$b_3=67^2=1 \mod 561$

Άρα ο 561 είναι σύνθετος και ΜΚΔ(b_2-1,n)=ΜΚΔ(66,561)=33 παράγοντας του 561.

Παρατήρηση : ο 561 είναι αριθμός Carmichael και όπως αναφέραμε παραπάνω το κριτήριο του Fermat δεν μπορεί να αποδείξει την συνθετότητα των αριθμών αυτών. Αντίθετα οι αριθμοί Carmichael δεν αποτελούν πρόβλημα για το κριτήριο Miller-Rabin.

Παρατήρηση : Οι σύνθετοι αριθμοί n οι οποίοι επιτυχαίνουν το τεστ του Fermat και επιπλέον το τεστ του Miller-Rabin ονομάζονται ισχυροί ψευδοπρώτοι για δοσμένη βάση α. Οι ισχυροί ψευδοπρώτοι είναι είναι πάρα πολύ λιγότεροι από τους ψευδοπρώτους.

Τα παραπάνω καθιστούν το τεστ Miller-Rabin καλύτερο και πιο αξιόπιστο από τα υπόλοιπα τεστ, των Fermat και Solovay-Strassen.

ΚΕΦΑΛΑΙΟ 5 : ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΑΚΕΡΑΙΟΥ

Η παραγοντοποίηση ακεραίων και ειδικά αυτών με πολλά ψηφία αποτελεί ένα από τα πλέον δύσκολα υπολογιστικά προβλήματα της κλασσικής Θεωρίας Αριθμών. Η δυσκολία αυτή άλλωστε ενέπνευσε την δημιουργία του κρυπτοσυστήματος RSA, στην οποία και οφείλει την ασφάλεια του. Η στενή σύνδεση της ασφάλειας του RSA με το πρόβλημα αυτό αύξησε το ενδιαφέρον και κατ΄επέκταση την ενασχόληση με αυτό. Παρά το γεγονός ότι τα τελευταία χρόνια έχουν αναπτυχθεί αρκετοί αλγόριθμοι, κανένας δεν έχει επιτύχει να απειλήσει σοβαρά την ασφάλεια του RSA. Πέρα όμως από τη σχέση που έχει η παραγοντοποίηση με την κρυπτογραφία και την ασφάλεια των πρωτοκόλλων, αποτελούσε ιδιαίτερα φλέγον ζήτημα από τα παλαιότερα χρόνια σε αριθμοθεωρητικό επίπεδο. Η πιο παλιά μέθοδος παραγοντοποίησης είναι αυτή των διαδοχικών διαιρέσεων και ύστερα η μέθοδος του Fermat και του Euler όπως αναφέρθηκαν στο 1ο κεφάλαιο. Στη συνέχεια θα εξετάσουμε αλγόριθμους παραγοντοποίησης του Dixon, p-1 Pollard και Rho Pollard.

5.1 Ο ΑΛΓΟΡΙΘΜΟΣ ΤΟΥ DIXON

Ο αλγόριθμος του Dixon το 1981, στηρίζεται στο βασικό κριτήριο παραγοντοποίησης δηλαδή στην εύρεση ακεραίων x, y τέτοιων ώστε να ισχύει:

1. x^2 = y^2 $mod n$
2. $x \neq \pm y mod n$

Οπότε $(x + y)(x - y) = k \cdot n$, δηλαδή ο n παραγοντοποιείται και οι αριθμοί $ΜΚΔ(x - y, n), ΜΚΔ(x + y, n)$ δίνουν μη τετριμμένους παράγοντες του n. Ακόμα η μέθοδος χρησιμοποιεί μια βάση παραγοντοποίησης B και τις έννοιες B-λείος και B-προσαρμοσμένος ως προς τον φυσικό , τις οποίες θα δούμε παρακάτω.

ΟΡΙΣΜΟΙ

1. **Βάση παραγοντοποίησης Β** είναι το σύνολο των διακεκριμένων πρώτων B={$-1, p\_1, p\_2, \dots, p\_h$} όπου -1=n-1 $mod n$.
2. Ένας ακέραιος καλείται **Β-λείος** αν γράφεται σαν γινόμενο στοιχείων του Β.
3. Ένας ακέραιος b λέγεται **Β-προσαρμοσμένος ως προς τον φυσικό n** αν ο ακέραιος c , με $-n/2 \leq c \leq n/2$ και b^2 = $c\, mod n$, είναι Β-λείος.(Παρατηρούμε ότι ο b είναι Β-προσαρμοσμένος ως προς τον φυσικό n εάν το τετράγωνό του αναλύεται σε πρώτους παράγοντες της βάσης Β).

Παράδειγμα

Έστω η βάση B={$-1,2,3,5,7$}. Οι ακέραιοι $40=2^3\cdot 5$ και $63=3^2\cdot 7$ είναι Β-λείοι.

Ο αριθμός 59 είναι Β-προσαρμοσμένος ως προς τον 1147 και ο αριθμός 71 είναι Β-προσαρμοσμένος ως προς τον 2849 διότι:

- 59^2=40mod1147 , -1147/2≤40≤1147/2 και ο 40 είναι Β-λείος
- 71^2=63mod2849 , -2849/2≤63≤2849/2 και ο 71 είναι Β-λείος

Συνοπτική περιγραφή του αλγορίθμου του Dixon: Αρχικά παίρνουμε μια βάση που αποτελείται από μικρούς πρώτους (εξού και παίρνω -1 αντί του n-1) και φτιάχνω τετράγωνα που γράφονται σαν γινόμενα μικρών πρώτων (το προσαρμοσμένος) και στοιχείων της βάσης(το λείος). Κάθε τέτοιο τετράγωνο δίνει μια γραμμή σ'έναν πίνακα στον οποίο καταχωρούνται οι εκθέτες των πρώτων αριθμών της βάσης. Αν πάρουμε περισσότερους τέτοιους αριθμούς από τα στοιχεία της βάσης ο προκύπτων πίνακας θα έχει $mod 2$ γραμμικές εξαρτήσεις μεταξύ των γραμμών. Οι γραμμικά εξαρτημένες γραμμές δίνουν το ζητούμενο x^2 = y^2 $mod n$ (για διάφορα x, y). Αν $x \neq \pm y mod n$ καταλήγουμε κατά τα γνωστά σε μη τετριμμένο παράγοντα του n. Η πολυπλοκότητα του αλγορίθμου, με κατάλληλα μικρή βάση, δίνει χρόνο εκτέλεσης *O*(e^($c\sqrt{(log n \cdot loglog n)}$)) , άρα είναι υποεκθετικού χρόνου.

ΑΛΓΟΡΙΘΜΟΣ ΤΟΥ DIXON

1. Επιλέγω φυσικό y και θεωρώ την βάση Β που σχηματίζουν οι πρώτοι παράγοντες $p\_1,p\_2,\ldots,p\_(\pi(y))$ που είναι μικρότεροι του y.
2. Αν κανένας από τους πρώτους p_i δεν διαιρεί τον n βρίσκουμε ακεραίους b_i με $1\leq b\_i\leq n$ όπου i=1,...,$\pi(y)$+2 που να είναι Β-προσαρμοσμένοι ως προς τον n.
3. Αν b_i^2= $[\![(-1)]\!]$ ^(a_i0) p_1^(a_i1)… $p\_(\pi(y))$^($a\_(i\pi(y))$) mod τότε αντιστοιχώ στο b_i το διάνυσμα u_i των εκθετών : u_i=(u_i0,u_i1,..., $u\_(i\pi(y))$) του $\mathbb{Z}\_2$^($\pi(y)$ + 1) θέτοντας u_ij=0 αν ο α_ij είναι άρτιος και u_ij=1 αν ο α_ij είναι περριτός.(0,1 τα στοιχεία του $\mathbb{Z}\_2$).
4. Υπολογίζω το υποσύνολο I του {1,…,$\pi(y)$ + 2} με $\sum\_(i\in I)\blacksquare u\_i$ =0. (δηλαδή τα γραμμικά εξαρτημένα mod2).
5. Υπολογίζω τα γινόμενα $b=\prod\_(i\in I)\blacksquare b\_i$, $c=p\_1$^(γ_1) p_2^(γ_2)… $p\_(\pi(y))$^($\gamma\_(\pi(y))$) όπου $2\gamma\_j=\sum\_(i\in I)\blacksquare a\_ij$. **Προσοχή:** κάθε πρώτος της βάσης Β πρέπει να χρησιμοποιείται άρτιο πλήθος φορών.
6. Αν $b\neq \pm cmodn$ υπολογίζω τον ΜΚΔ(b + c,n) που δίνει μη τετριμμένο παράγοντα του n. Αν b = $\pm cmodn$ τότε υπολογίζω άλλο $I\subset$ {1,…,$\pi(y)$ + 2} ή άλλον y και επαναλαμβάνω την διαδικασία.

Παρατηρήσεις: Καθώς ο n δεν διαιρείται από τους πρώτους $p\_1,p\_2,\ldots,p\_(\pi(y))$, έχουμε ότι (b,n) = 1. Έτσι εάν ο n έχει 2^r πρώτους παράγοντες ($r\geq 2$) τότε η

πολυωνυμική ισοδυναμία x^2 = b^2 $modn$ θα έχει r λύσεις. Η πιθανότητα λοιπόν να έχω b = $\pm cmodn$ ισούται με 1/2^($r-1$).
Ένας απλός τρόπος εύρεσης των ακεραίων b_i είναι να δοκιμάζουμε ακεραίους της μορφής $\lfloor\sqrt{kn}\rfloor + j$ (j = 0,1,…, k = 1,2,…). Ο μικρότερος κατ' απόλυτη τιμή ακέραιος της κλάσης του τετραγώνου τέτοιων ακεραίων $modn$ είναι αρκετά μικρός και άρα έχουν μεγάλη πιθανότητα να είναι Β-προσαρμοσμένοι ως προς τον n.

Παράδειγμα

Θα παραγοντοποιήσω τον ακέραιο n=93.623.

Θεωρώ την βάση B={$-1,2,3,5,7,11,13$} η οποία έχει 7 στοιχεία, άρα θα προσπαθήσω να βρώ τουλάχιστον 8 B-προσαρμοσμένους ως προς τον n. Παρατηρώ ότι κανένα στοιχείο της βάσης δεν διαιρεί τον 93.623.

Δοκιμάζω ακεραίους της μορφής $\lfloor\sqrt{kn}\rfloor + j$ με k, j=1,2,...,9 και προκύπτουν τα παρακάτω:

$\sqrt{n}$ = 305,9... b_1: $[\![306]\!]$ ^2 = 93.636 = $13 mod n \in B$

$\sqrt{2n}$ = 432,7 ... b_2: $[\![433]\!]$ ^2 = 187.489 = 243 = 3^5 $mod n \in B$

$\sqrt{3n}$ = 529,9 ... b_3: $[\![531]\!]$ ^2 = 281.961 = 1.092 = $2^2 \cdot 3 \cdot 7 \cdot 13 mod n \in B$

b_4: $[\![537]\!]$ ^2 = 288.369 = 7.500 = 2^2 · 3 · 5^4 $mod n \in B$

$\sqrt{4n}$ = 611,9 ... b_5: $[\![612]\!]$ ^2 = 374.544 = 52 = $2^2 \cdot 13 mod n \in B$

$\sqrt{7n}$ = 809,5 ... b_6: $[\![809]\!]$ ^2 = 654.481 = −880 = $[\![-2]\!]^4 \cdot 5 \cdot 11 mod n \in B$

$\sqrt{8n}$ = 865,4 ... b_7: $[\![866]\!]$ ^2 = 749.956 = 972 = $2^2 \cdot 3^5 mod n \in B$

$\sqrt{9n}$ = 917,9 ... b_8: $[\![918]\!]$ ^2 = 842.724 = 117 = $3^2 \cdot 13 mod n \in B$

οπότε παίρνουμε τα παρακάτω 8 διανύσματα στο $\mathbb{Z}\_2^7$:

u_1 = (0,0,0,0,0,0,1)

u_2 = (0,0,1,0,0,0,0)

u_3 = (0,0,1,0,1,0,1)

u_4 = (0,0,1,0,0,0,0)

u_5 = (0,0,0,0,0,0,1)

u_6 = (1,0,0,1,0,1,0)

u_7 = (0,0,1,0,0,0,0)

u_8 = (0,0,0,0,0,0,1)

Θεωρώ το γραμμικό ομογενές σύστημα $x\_1 \cdot u\_1 + x\_2 \cdot u\_2 + \ldots + x\_8 \cdot u\_8 = 0 \ mod 2$ για να βρω μια σχέση γραμμικής εξάρτησης μεταξύ τους.Ισοδύναμα έχουμε :

$$\{\blacksquare(x\_6 = 0@x\_2 + x\_3 + x\_4 + x\_7 = 0@x\_3 = 0@x\_1 + x\_3 + x\_5 + x\_8 = 0)\dashv \quad (mod 2)$$

Μία λύση του συστήματος είναι

$$x\_1 = x\_5 = 1$$

$$x\_2 = x\_3 = x\_4 = x\_6 = x\_7 = x\_8 = 0$$

Άρα $I = \{x\_1, x\_5\}$ και υπολογίζω τα b, c

$$b = \prod\_(i \in I) \ ⟦b\_i = b\_1 \, b\_5 = 306 \cdot 612 = 187.272⟧$$

$$c\text{^}2 = 13 \cdot 2\text{^}2 \cdot 13 \quad \Rightarrow \quad c = 26$$

Όμως $187.272 = 26 \, mod 93.623$ άρα δεν μπορούμε να υπολογίσουμε έναν μη τετριμμένο παράγοντα του 93.623.

Μία άλλη λύση του συστήματος είναι

$$x\_2 = x\_4 = 1$$

$$x\_1 = x\_3 = x\_5 = x\_6 = x\_7 = x\_8 = 0$$

Άρα $b = b\_2 \, b\_4 = 433 \cdot 537 = 232.521$

$$c\text{^}2 = 3\text{^}5 \cdot 2\text{^}2 \cdot 3 \cdot 5\text{^}4 = 3\text{^}6 \cdot 2\text{^}2 \cdot 5\text{^}4 \quad \Rightarrow \quad c = 1350$$

Καθώς $232.521 = 45.275 mod 93.623$ δηλαδή $b \neq \pm c mod n$ μπορώ να προσδιορίσω τετριμμένο παράγοντα του 93.623 υπολογίζοντας

$\text{ΜΚΔ}(b + c, n) = \text{ΜΚΔ}(233.871, 93.623)$

233.871 93.623

46.625 93.623

46.625 373

0 373 Άρα $MK\Delta = 373$ και $93.623 = 373 \cdot 251.$

5.2 Ο ΑΛΓΟΡΙΘΜΟΣ p-1 ΤΟΥ JONATHAN POLLARD

Ο αλγόριθμος p-1 που παρουσίασε ο J.Pollard το 1974 δουλεύει ικανοποιητικά για σύνθετους αριθμούς οι οποίοι έχουν έναν πρώτο παράγοντα p τέτοιον ώστε ο p-1 να έχει μόνο μικρούς πρώτους παράγοντες. Ο αλγόριθμος p-1 όπως και εκείνος του Dixon στηρίζεται σε προκαθορισμένο φράγμα B δηλαδή σε βάση B μικρών πρώτων. Ο αλγόριθμος λοιπόν έχει δύο εισόδους, τον αριθμό n που θέλουμε να παραγοντοποιήσουμε και το προκαθορισμένο φράγμα B.

ΑΛΓΟΡΙΘΜΟΣ p-1 ΤΟΥ JONATHAN POLLARD

1. Υπολογίζω το γινόμενο $\kappa = \prod_{(q \le B)} q^{\lfloor \log_q B \rfloor}$ όπου q διατρέχει το σύνολο των πρώτων $\le B$ και κάθε μέλος του γινομένου δεν ξεπερνά το B.
2. Επιλέγω έναν ακέραιο α με $1 < \alpha < n$ και υπολογίζω $\text{ΜΚΔ}(\alpha, n) = \delta$. (αρχίζω με α=2,α=3 κοκ).
3. Αν δ>1 τότε ο δ είναι μή τετριμμένος παράγοντας του n. Αν δ=1 υπολογίζω τον ΜΚΔ d , $d = \text{ΜΚΔ}(\alpha^{\kappa} - 1, n)$.
4. Αν 1 < d < n , τότε ο d είναι μη τετριμμένος παράγοντας του n. Αν d = 1 ή d = n τότε επιλέγουμε ένα άλλο B και επαναλαμβάνουμε την διαδικασία.

<u>Παράδειγμα Βήμα 1ο</u>

Έστω $B = 19$ τότε $\kappa = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ διότι:

$2^{\log_2 19} = 2^4 < 19$, $3^{\log_3 19} = 3^2 < 19$ και οι υπόλοιποι δίνουν εκθέτη 1.

Αναλυτική περιγραφή του αλγορίθμου p-1: Έστω p είναι πρώτος παράγοντας του n και κάθε δύναμη πρώτου που διαιρεί τον $p-1$ είναι $\le B$. Άρα ο κ που έχει την ίδια μορφή με τον $p-1$ (πιθανότατα με μεγαλύτερους εκθέτες) θα είναι πολλαπλάσιο του $p-1$, δηλαδή $p-1 | k \Rightarrow k = l \cdot (p-1)$. Τότε για κάθε α με $1<\alpha<n$ και $(\alpha, p) = 1$ από το μικρό θεώρημα του Fermat θα έχω :

$\alpha^{\wedge}\kappa = \alpha^{\wedge}(l \cdot (p-1)) = [\![(\alpha^{\wedge}(p-1))]\!]^{\wedge} l = 1 \bmod p \quad \Rightarrow \quad \alpha^{\wedge}\kappa - 1 = \pi o \lambda . p$ $\Rightarrow \quad [\![p \mid \alpha]\!]^{\wedge}\kappa - 1.$

Αν λοιπόν $1<d<n$ τότε ο d είναι μη τετριμμένος παράγοντας του n.

Η πολυπλοκότητα του αλγορίθμου είναι $O(B^{\wedge}2\ [\![(\log\ [\![B]\!]]\!]^{\wedge}2\ [\![(\log\ [\![n]\!]]\!]^{\wedge}2)$ και για $B = O([\![(\log\ [\![n]\!]]\!]^{\wedge}c)$, όπου c θετικός ακέραιος, ο αλγόριθμος είναι πολυωνυμικού χρόνου, όμως μειώνεται αρκετά η πιθανότητα επιτυχίας του. Γρήγορα αποτελέσματα θα έχουμε μόνο στην περίπτωση όπου ο n έχει έναν πρώτο παράγοντα p τέτοιον ώστε ο p-1 να έχει αρκετά μικρούς πρώτους παράγοντες. Στην περίπτωση που αυξήσουμε την βάση B, ο αλγόριθμος έχει μεγαλύτερη πιθανότητα επιτυχίας με σημαντικό όμως μειονέκτημα ότι γίνεται πολύ αργός.

<u>Παράδειγμα</u>

1. n=1.127.041 και παίρνω βάση B=19
   $\kappa=2^4\cdot3^2\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19=232.792.560$
   υπολογίζω ΜΚΔ($2^{232792560}$-1 , 1.127.041)=761
   άρα n=1.127.041=761·1.481 (761 , 1.481 είναι πρώτοι αριθμοί)
   $760=2^3\cdot5\cdot19$ (έχει μικρούς πρώτους παράγοντες $\leq$19)

2. n=1.241.143 και παίρνω βάση B=13
   $\kappa=2^3\cdot3^2\cdot5\cdot7\cdot11\cdot13=360.360$
   υπολογίζω ΜΚΔ(2^{360360}-1 , 1.241.143)=547
   άρα n=1.241.143=547·2.269 (547 , 2.269 είναι πρώτοι αριθμοί)
   $546=2\cdot3\cdot7\cdot13$ (έχει μικρούς πρώτους παράγοντες $\leq$13)

3. n=143 και παίρνω βάση B=5
   $\kappa=2^2\cdot3\cdot5=60$
   υπολογίζω ΜΚΔ(2^{60}-1 , 143)=ΜΚΔ(4.095 , 143)

   4095 143
   91 143
   91 52 Άρα 143=13·11
   39 52 $12=2^2\cdot3$
   39 13
   0 13

5.3 Ο ΑΛΓΟΡΙΘΜΟΣ Rho ΤΟΥ JONATHAN POLLARD

Το 1975 ο J.Pollard εισήγαγε τον αλγόριθμο Rho ο οποίος είναι αρκετά αποδοτικός στο να παραγοντοποιεί αριθμούς με μικρούς πρώτους παράγοντες. Ο αλγόριθμος στηρίζεται στην παρακάτω ιδέα : έστω p ο μικρότερος πρώτος διαιρέτης του n και x, x' ακέραιοι στο $\mathbb{Z}_n$ τέτοιοι ώστε $x \neq x'$ και $x = x' \bmod p$. Τότε $p \leq \text{ΜΚΔ}(x - x', n) < n$ και υπολογίζοντας τον ΜΚΔ βρίσκουμε έναν μη τετριμμένο παράγοντα του n. Πρακτικά, εάν θέλουμε να παραγοντοποιήσουμε τον n, επιλέγουμε πρώτα ένα τυχαίο υποσύνολο X του $\mathbb{Z}_n$ και υπολογίζουμε τους $\text{ΜΚΔ}(x - x', n)$ για όλα τα x, x' στο X, με $x \neq x'$. Η διαδικασία αυτή όμως είναι επιτυχής μόνο στην περίπτωση που η απεικόνιση $x \to x \bmod p$ οδηγεί σε τουλάχιστον μία <<σύγκρουση>> για το $x \in X$. Η περίπτωση αυτή στηρίζεται στο παράδοξο των γενεθλίων: εάν $|X| \approx 1{,}17\sqrt{n}$ τότε υπάρχει 50% πιθανότητα να πετύχουμε σύγκρουση και επομένως να βρούμε έναν μη τετριμμένο παράγοντα του n. Πριν δούμε αναλυτικά τον αλγόριθμο θα παραθέσω τον ορισμό της σύγκρουσης και το θεώρημα που αναφέρεται στο παράδοξο των γενεθλίων.

ΟΡΙΣΜΟΣ Μία **σύγκρουση** (collision) της συνάρτησης f είναι ένα ζεύγος (x, x') στο πεδίο ορισμού για το οποίο ισχύει $x \neq x'$ και $f(x) = f(x')$.

ΘΕΩΡΗΜΑ (Παράδοξο των γενεθλίων(birthday paradox)) Σε μία τυχαία επιλογή 23 ανθρώπων , η πιθανότητα δύο από αυτούς να έχουν γενέθλια την ίδια μέρα είναι τουλάχιστον 0,5 (0,507 για την ακρίβεια).

Από μαθηματικής άποψης αν μια συνάρτηση f παράγει μία τιμή μεταξύ n διαφορετικών τιμών με την ίδια πιθανότητα και το n είναι αρκετά μεγάλο, τότε υπολογίζοντας τη συνάρτηση για ένα πλήθος περίπου $1{,}17\sqrt{n}$ διαφορετικών εισόδων περιμένουμε να βρούμε ένα ζεύγος εισόδων x και x' $(x \neq x')$ ώστε να ισχύει $f(x) = f(x')$.

Απόδειξη: Θεωρούμε την ομάδα των ακεραίων modn, δηλαδή το σύνολο $\mathbb{Z}_n = \{0,1,2,\ldots n-1\}$ με $|\mathbb{Z}_n| = n$. Θα υπολογίσουμε την πιθανότητα να μην επιλεχθούν ίσα στοιχεία (δηλαδή να μην έχουμε συγκρούσεις) σε μία τυχαία επιλογή k στοιχείων από το $\mathbb{Z}_n$. Η πιθανότητα επιλογής ενός συγκεκριμένου στοιχείου είναι $1/n$. Η πρώτη μας επιλογή είναι αυθαίρετη. Η πιθανότητα η δεύτερη επιλογή να είναι διαφορετική από την πρώτη είναι $(n-1)/n = 1 - 1/n$. Η πιθανότητα η τρίτη επιλογή να είναι διαφορετική από τις προηγούμενες δύο είναι $(n-2)/n = 1 - 2/n$ κ.ο.κ.

Έτσι η πιθανότητα επιλογής k στοιχείων χωρίς συγκρούσεις είναι :

$(1-1/n)(1-2/n)(1-3/n)\ldots(1-(k-1)/n)=\prod_{i=1}^{k-1}(1-i/n)$ όπως προκύπτει από την Πολλαπλασιαστική αρχή.

Αν ο x είναι μικρός πραγματικός αριθμός τότε $1-x \approx e^{-x}$ όπως προκύπτει από την ανάπτυξη σε δυναμοσειρά του e^{-x} : $e^{-x} = 1 - x + x^2/2! - x^3/3! + \ldots$.

Κατά συνέπεια αφού ο n είναι αρκετά μεγάλος έπεται ότι $1 - 1/n \approx e^{-1/n}$.

Από τα παραπάνω, μια εκτίμηση της ζητούμενης πιθανότητας είναι η :

$$\prod_{i=1}^{k-1}(1-i/n) \approx \prod_{i=1}^{k-1}(e^{-i/n}) = e^{-k(k-1)/2n} .$$

Αν p είναι η πιθανότητα εύρεσης μίας σύγκρουσης τότε $p \approx 1 - e^{-k(k-1)/2n} \Rightarrow$

$e^{-k(k-1)/2n} \approx 1-p \Rightarrow (-k(k-1))/2n \approx \ln(1-p) \Rightarrow (k(k-1))/2n \approx -\ln(1-p) \Rightarrow (k(k-1))/2n \approx \ln [\![(1-p)]\!]^{-1} \Rightarrow k^2 - k \approx 2n\ln 1/(1-p)$.

Αγνοώντας τον όρο $-k$ έχουμε την εκτίμηση $k \approx \sqrt{(2n\ln 1/(1-p))}$ και για πιθανότητα σύγκρουσης p=1/2 θα είναι $k \approx 1{,}17\sqrt{n}$.

Επομένως, επιλέγοντας τυχαία λίγο περισσότερα από $\sqrt{n}$ στοιχεία του $\mathbb{Z}_n$ πετυχαίνουμε σύγκρουση με πιθανότητα τουλάχιστον 50%.

Στο παράδοξο των γενεθλίων όπου n=365 , η προσέγγιση μας δίνει

$k \approx 1{,}17\sqrt{365} \approx 22{,}3$.

Αναλυτική περιγραφή βασικών ιδεών του αλγορίθμου Rho :

Θεωρώ τη συνάρτηση f(x)=x^2 + a όπου a είναι μικρή σταθερά , συνήθως a=1.

Έστω 〚 x〛_1 ∈ $\mathbb{Z}$_n και X ⊆ $\mathbb{Z}$_n με

X
={ 〚 x〛_1, 〚 x〛_2, … , 〚 x〛_m | 〚 x〛_j = f(〚 x〛_(j − 1))modn ∀ j = 2,3, … , m} .

Σκοπός είναι η εύρεση δύο διαφορετικών τιμών 〚 x〛_i, 〚 x〛_j ∈ X τέτοιες ώστε ΜΚΔ(〚 x〛_j-x_i) >1. Κάθε φορά που υπολογίζουμε έναν καινούργιο όρο 〚 x〛_j της ακολουθίας , μπορούμε να υπολογίζουμε τους ΜΚΔ(〚 x〛_j-x_i) με i<j . Αυτό όμως θα απαιτούσε (($|X|$)¦2)=(m¦2) υπολογισμούς , κάτι το οποίο είναι αρκετά χρονοβόρο.
Ο αριθμός των υπολογισμών αυτών για την εύρεση μη τετριμμένου παράγοντα του n μπορεί να μειωθεί αρκετά και σε αυτό έγκειται η μέθοδος Pollard Rho.

Έστω μία σύγκρουση 〚 x〛_i ≡ 〚 x〛_j (modp) . Η f είναι πολυωνυμική συνάρτηση με ακέραιους συντελεστές οπότε f(〚 x〛_i) = f(〚 x〛_j)(modp) . Από την κατασκευή του υποσυνόλου X έχουμε ότι 〚 x〛_j = f(〚 x〛_(j − 1))modn ∀ j = 2,3, … , m. Τότε

〚 x〛_(i + 1) modp=(f(〚 x〛_i) modn) modp= f(〚 x〛_i) modp

(διότι p|n)

ομοίως 〚 x〛_(j + 1) modp=(f(〚 x〛_j) modn) modp= f(〚 x〛_j) modp

Συνεπώς θα έχουμε 〚 x〛_(i + 1) ≡ 〚 x〛_(j + 1) (modp).

Επαναλαμβάνοντας την διαδικασία,υποθέτοντας ότι ισχύει 〚 x〛_i ≡ 〚 x〛_j (modp) , καταλήγουμε στα εξής σημαντικά αποτελέσματα:

(1) 〚 x〛_(i + δ) ≡ 〚 x〛_(j + δ) (modp) , ∀ δ≥0.

(2) 〚 x〛_i′ ≡ 〚 x〛_j′ (modp) , j'>i'≥i και j'-i'≡0mod$l$ όπου l=j-i .

(3) 〚 x〛_i′ ≡ 〚 x〛_2i′ (modp) , i'≥i και i'≡0 mod$l$ όπου l=j-i .

ΑΛΓΟΡΙΘΜΟΣ POLLARD Rho

1. Επιλέγουμε ⟦x⟧_1 ∈ $\mathbb{Z}_n$ και υπολογίζουμε το ⟦x⟧_2 = f(⟦x⟧_1) = ⟦ ⟦x⟧_1⟧^2 + 1(modn).
Υπολογίζουμε τον ΜΚΔ(⟦x⟧_2- ⟦x⟧_1,n)=p.
Αν p=1 προχωράμε στο επόμενο βήμα.

2. Υπολογίζουμε τους ακεραίους ⟦x⟧_i = f(⟦x⟧_(i − 1))modn και ⟦x⟧_2i = f(⟦x⟧_(2i − 1))modn για i=2 . Έπειτα βρίσκουμε τον ΜΚΔ(⟦x⟧_2i- ⟦x⟧_i,n)= p .
Αν 1< p<n τότε ⟦x⟧_i ≡ ⟦x⟧_2i(modp) και ο p είναι μη τετριμμένος παράγοντας του n.
Αν p=n ο αλγόριθμος επιστρέφει μήνυμα <<αποτυχία>>.
Αν p=1 επαναλαμβάνουμε το βήμα 2 για i=3 κ.ο.κ

Παρατηρήσεις

- Αν ⟦x⟧_i ≡ ⟦x⟧_j (modp) τότε μεταξύ των l ακεραίων (l = j − i) θα υπάρχει κάποιο i′ ≥ i πολλαπλάσιο του l και από τη σχέση (3) στην προηγούμενη σελίδα, θα έχουμε ⟦x⟧_i′ ≡ ⟦x⟧_2i′ (modp). Ο i′ εντοπίζεται το πολύ σε j βήματα, άρα στη χειρότερη περίπτωση ο αλγόριθμος θα χρειαστεί j επαναλήψεις για να βρεί μία σύγκρουση. Ο αναμενόμενος αριθμός επαναλήψεων μειώνεται στο √p και επειδή p ≤ √n , η αναμενόμενη πολυπλοκότητα προκύπτει $\boldsymbol{O(n^{(1/4)})}$.
- Στην περίπτωση που οι τιμές ⟦x⟧_i, ⟦x⟧_j εμφανίζουν την πρώτη σύγκρουση και ικανοποιούν την σχέση ⟦x⟧_i ≡ ⟦x⟧_j (mod$n$) παράλληλα με την ⟦x⟧_i ≡ ⟦x⟧_j (modp), ο αλγόριθμος δεν θα καταφέρει να εντοπίσει έναν μη τετριμμένο παράγοντα. Η πιθανότητα για αυτήν την περίπτωση είναι περίπου p/n, αρκετά μικρή όταν ο n είναι μεγάλος (αφού p ≤ √n). Συνεπώς επαναλαμβάνουμε τη διαδικασία επιλέγοντας διαφορετική αρχική τιμή ή διαφορετική συνάρτηση f.

<u>Παράδειγμα</u>
Θα παραγοντοποιήσουμε τον n=7.171
Θέτουμε f(x)=x^2+1 και ⟦x⟧_1=1.

Βήμα 1 〖x〗_1=1 , 〖x〗_2 = f(〖x〗_1) = 1^2 + 1=2 (mod7.171)
ΜΚΔ(2-1,7.171)=ΜΚΔ(1,7.171)=1

Βήμα 2 〖x〗_2=2 , 〖x〗_3 = f(〖x〗_2) = 2^2 + 1=5 (mod7.171)
〖x〗_4 = f(〖x〗_3) = 5^2 + 1=26 (mod7.171)
ΜΚΔ(〖x〗_4- 〖x〗_2,n)=ΜΚΔ(24,7.171)=1

Βήμα 3 〖x〗_3=5 , 〖x〗_4=26 , 〖x〗_5 = f(〖x〗_4) = 〖26〗^2 + 1=677 (mod7.171)
〖x〗_6 = f(〖x〗_5) = 〖677〗^2 + 1=458.330=6.557 (mod7.171)
ΜΚΔ(〖x〗_6- 〖x〗_3,n)=ΜΚΔ(6.552,7.171)=1

Βήμα 4 〖x〗_4=26 , 〖x〗_5=677 , 〖x〗_6=6.557
〖x〗_7 = f(〖x〗_6) = 〖6.557〗^2 + 1=42.994.250=4.105 (mod7.171)
〖x〗_8 = f(〖x〗_7) = 〖4.105〗^2 + 1=16.851.026=6.347 (mod7.171)
ΜΚΔ(〖x〗_8- 〖x〗_4,n)=ΜΚΔ(6.321,7.171)=1

Βήμα 5 〖x〗_5=677 , 〖x〗_6=6.557 , 〖x〗_7=4.105 , 〖x〗_8=6.347
〖x〗_9 = f(〖x〗_8) = 〖6.347〗^2 + 1=40.284.410=4.903 (mod7.171)
〖x〗_10 = f(〖x〗_9) = 〖4.903〗^2 + 1=24.039.410=2.218 (mod7.171)
ΜΚΔ(〖x〗_10- 〖x〗_5,n)=ΜΚΔ(1.541,7.171)=1

Βήμα 6 〖x〗_6=6.557 , 〖x〗_7=4.105 , 〖x〗_8=6.347 , 〖x〗_9=4.903 , 〖x〗_10=2.218
〖x〗_11 = f(〖x〗_10) = 〖2.218〗^2 + 1=4.919.525=219 (mod7.171)
〖x〗_12 = f(〖x〗_11) = 〖219〗^2 + 1=47.962=4.936 (mod7.171)
ΜΚΔ(〖x〗_12- 〖x〗_6,n)=ΜΚΔ(1.621,7.171)=1

Βήμα 7 〖x〗_7=4.105 , 〖x〗_8=6.347 , 〖x〗_9=4.903 , 〖x〗_10=2.218 , 〖x〗_11=219 , 〖x〗_12=4.936
〖x〗_13 = f(〖x〗_12) = 〖4.936〗^2 + 1=24.364.097=4.210 (mod7.171)

〖x〗_14 = f(〖x〗_13) = 〖4.210〗^2 + 1=17.724.101=4.560 (mod7.171)

ΜΚΔ(〖x〗_14- 〖x〗_7,n)=ΜΚΔ(455,7.171)=1

Βήμα 8 〖x〗_8=6.347 , 〖x〗_9=4.903 , 〖x〗_10=2.218 , 〖x〗_11=219 , 〖x〗_12=4.936 , 〖x〗_13=4.210

〖x〗_14=4.560

〖x〗_15 = f(〖x〗_14) = 〖4.560〗^2 + 1=20.793.601=4.872 (mod7.171)

〖x〗_16 = f(〖x〗_15) = 〖4.872〗^2 + 1=23.736.385=375 (mod7.171)

ΜΚΔ(〖x〗_8- 〖x〗_16,n)=ΜΚΔ(5.972,7.171)=1

Βήμα 9 x_9=4.903 , 〖x〗_10=2.218 , 〖x〗_11=219 , 〖x〗_12=4.936 , 〖x〗_13=4.210 , 〖x〗_14=4.560

x_15=4.872 , x_16=375

x_17 = f(〖x〗_16) = 〖375〗^2 + 1=140.626=4.377 (mod7.171)

x_18 = f(〖x〗_17) = 〖4.377〗^2 + 1=19.158.130=4.389 (mod7.171)

ΜΚΔ(〖x〗_9- 〖x〗_18,n)=ΜΚΔ(514,7.171)=1

Βήμα 10 x_10=2.218 , 〖x〗_11=219 , 〖x〗_12=4.936 , 〖x〗_13=4.210 , 〖x〗_14=4.560

x_15=4.872 , x_16=375 , x_17=4.377 , x_18=4.389

x_19 = f(〖x〗_18) = 〖4.389〗^2 + 1=19.263.322=2.016 (mod7.171)

x_20 = f(〖x〗_19) = 〖2.016〗^2 + 1=4.064.257=5.471 (mod7.171)

ΜΚΔ(〖x〗_20- 〖x〗_10,n)=ΜΚΔ(3.253,7.171)=1

Βήμα 11 x_11=219 , 〖x〗_12=4.936 , 〖x〗_13=4.210 , 〖x〗_14=4.560 , x_15=4.872 , x_16=375

x_17=4.377 , x_18=4.389 , x_19=2.016 , x_20=5.471

x_21 = f(〖x〗_20) = 〖5.471〗^2 + 1=29.931.842=88 (mod7.171)

x_22 = f(〖x〗_21) = 〖88〗^2 + 1=7.745=574 (mod7.171)

ΜΚΔ(〖x〗_22- 〖x〗_11,n)=ΜΚΔ(355,7.171)= 71 .

Μετά από 11 επαναλήψεις ο αλγόριθμος εντόπισε τη σύγκρουση 〖x〗_11 ≡ 〖x〗_22 (modp) και τον μη τετριμμένο παράγοντα 71. Άρα 7.171=71·101 όπου 71, 101 είναι πρώτοι αριθμοί. Η πρώτη σύγκρουση είναι η 〖x〗_7mod71=x_18mod71=6 .

ΒΙΒΛΙΟΓΡΑΦΙΑ

- "ΚΡΥΠΤΟΓΡΑΦΙΑ"
  Α.ΠΑΠΑΪΩΑΝΝΟΥ - Χ.ΚΟΥΚΟΥΒΙΝΟΣ
  ΕΚΔΟΣΗ ΕΘΝΙΚΟΥ ΜΕΤΣΟΒΙΟΥ ΠΟΛΥΤΕΧΝΕΙΟΥ, ΑΘΗΝΑ 2007

- "ΣΗΜΕΙΩΣΕΙΣ ΣΤΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ ΚΑΙ ΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ"
  Ε.ΖΑΧΟΣ, ΕΜΠ 2007

- "LECTURE NOTES ON CRYPTOGRAPHY"
  S.Goldwasser - M.Bellare, 2008

- "ΚΡΥΠΤΟΓΡΑΦΙΑ. Η ΕΠΙΣΤΗΜΗ ΤΗΣ ΑΣΦΑΛΟΥΣ ΕΠΙΚΟΙΝΩΝΙΑΣ"
  ΔΗΜΗΤΡΙΟΣ Μ. ΠΟΥΛΑΚΗΣ,
  ΕΚΔΟΣΕΙΣ ΖΗΤΗ, ΑΘΗΝΑ 2004

- "CRYPTOGRAPHY : AN INTRODUCTION"
  N.P.SMART, McGRAW HILL 2002

- "ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ"
  Ε.ΖΑΧΟΣ, ΕΜΠ 1998

- WWW.WIKIPEDIA.GR

- Νεγρεπόντης Σ. (2009) , Σημειώσεις του μαθήματος "Ιστορία των Αρχαίων Ελληνικών Μαθηματικών - Στοιχεία Ευκλείδη

- Dickson L.E. (2005) History of the theory of numbers, Vol 1 : Divisibility and Primality, Dover