ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ

ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΩΤΟΥ ΑΡΙΘΜΟΥ ΚΑΙ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΑΚΕΡΑΙΟΥ

ΛΑΙΟΥ ΕΡΩΦΙΛΗ

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ:

Χ.ΚΟΥΚΟΥΒΙΝΟΣ, ΚΑΘΗΓΗΤΗΣ ΕΜΠ

Α.ΠΑΠΑΙΩΑΝΝΟΥ, ΑΝΑΠ.ΚΑΘΗΓΗΤΗΣ ΕΜΠ(Επιβλέπων)

Π.ΣΤΕΦΑΝΕΑΣ , ΛΕΚΤΟΡΑΣ ΕΜΠ

ΑΘΗΝΑ 2013

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ

ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΩΤΟΥ ΑΡΙΘΜΟΥ ΚΑΙ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΑΚΕΡΑΙΟΥ

ΛΑΙΟΥ ΕΡΩΦΙΛΗ

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ:

Χ.ΚΟΥΚΟΥΒΙΝΟΣ, ΚΑΘΗΓΗΤΗΣ ΕΜΠ

Α.ΠΑΠΑΙΩΑΝΝΟΥ, ΑΝΑΠ.ΚΑΘΗΓΗΤΗΣ ΕΜΠ(Επιβλέπων)

Π.ΣΤΕΦΑΝΕΑΣ , ΛΕΚΤΟΡΑΣ ΕΜΠ

ΑΘΗΝΑ 2013

Στις κόρες μου Ίριδα και Άλκηστη.

Ευχαριστίες

Θέλω να ευχαριστήσω ιδιαίτερα τον κ. Παπαιωάννου ο οποίος ήταν και ο επιβλέπων για την παρούσα εργασία , τις γιαγιάδες Δέσποινα και Σοφία για την πολύτιμη βοήθειά τους , καθώς χωρίς εκείνες η κατάθεση της διπλωματικής μου εργασίας θα ήταν ένα μακρινό όνειρο. Επίσης τον Κωνσταντίνο για την υπομονή και την κατανόηση και ιδιαιτέρως την Μαρία για την παρακίνηση και υποστήριξη.

Περίληψη

Στην παρούσα εργασία , θα παρουσιασθούν μέθοδοι πιστοποίησης πρώτων αριθμών και αλγόριθμοι παραγοντοποίησης ακεραίων. Ξεκινώντας από τις κλασσικές μεθόδους , στο πρώτο κεφάλαιο παραθέτονται η μέθοδος των διαδοχικών διαιρέσεων , το κόσκινο του Ερατοσθένη , και η παραγοντοποίηση του Fermat και του Euler. Στο δεύτερο κεφάλαιο , αναφέρονται στοιχεία από τη Θεωρία Αριθμών τα οποία αποτελούν σημαντικές γνώσεις για την κατανόηση βασικών ιδεών στην πιστοποίηση πρώτων και την παραγοντοποίηση. Στο τρίτο κεφάλαιο αναλύονται τα κριτήρια των Fermat , Miller-Rabin και Solovay-Strassen για την πιστοποίηση πρώτων . Τέλος , το τέταρτο κεφάλαιο αφορά την παραγοντοποίηση ακεραίων και θα αναλυθούν οι αλγόριθμοι του Dixon , p-1 και Rho του J.Pollard.

Abstract

In the present thesis , tests for primality and algorithms for factoring integers will be presented. Starting from the classical methods , the first chapter cites the method of successive trial divisions , the sieve of Eratosthenes , Fermat's and Euler's factorization. In the second chapter , we state some elements from Number Theory that are significant Knowledge to understand basic ideas for factoring and primality. In the third chapter , the citeria of Fermat's , Miller-Rabin and Solovay-Strassen to certificate primes, will be analyzed. Finally , the fourth chapter is about factoring integers so algorithms of Dixon's , J.Pollard's p-1 and Rho will be presented and analyzed.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Πρώτοι λέγονται οι φυσικοί αριθμοί που είναι μεγαλύτεροι της μονάδας και έχουν μόνο δύο φυσικούς διαιρέτες.Το 1 και τον εαυτό τους.Παρά την φαινομενική απλότητα του ορισμού τους και το στοιχειώδες του χαρακτήρα τους παραμένουν από τα πιο μυστηριώδη αντικείμενα στα Μαθηματικά. Αρκετούς αιώνες άνθρωποι από τον επιστημονικό μαθηματικό κόσμο προσπαθούν να επινοήσουν μεθόδους πιστοποίησης πρώτων αριθμών και παραγοντοποίησης. Αναλυτικότερα επιλέγοντας έναν τυχαίο μεγάλο αριθμό , ενα ερώτημα που αναμφισβήτητα προκύπτει είναι εάν ο αριθμός αυτός ειναι πρώτος και εάν όχι ποιοί είναι οι παράγοντές του. Σύμφωνα με το θεμελιώδες θεώρημα της αριθμητικής κάθε σύνθετος φυσικός αριθμός αναλύεται μοναδικά σαν γινόμενο πρώτων παραγόντων.

Η πιστοποίηση πρώτου αριθμού είναι πολύ σημαντικό στοιχείο για την κρυπτογράφηση , αποκρυπτογράφηση αλλά κυρίως για την κρυπτανάλυση ενός κρυπτογραφικού συστήματος.Το πρόβλημα της παραγοντοποίησης ενός αριθμού έχει κρίσιμη θέση στη μοντέρνα κρυπτογραφία καθώς αρκετά κρυπτογραφικά πρωτόκολλα στηρίζουν την ασφάλειά τους στη δυσκολία επίλυσης αυτού του προβλήματος, με πιο γνωστό και διαδεδομένο το RSA. Οι σημερινές εφαρμογές δίνουν μια νέα διάσταση και η μελέτη του προβλήματος είναι αναγκαία ώστε να καθορίζονται οι παράμετροι ασφαλείας. Αν και αρκετοί αλγόριθμοι αναπτύχθηκαν την τελευταία εικοσαετία, κανένας δεν πέτυχε να απειλήσει σοβαρά την ασφάλεια του RSA.

Πέρα όμως από τις εφαρμογές τους, οι πρώτοι αριθμοί και γενικότερα οι ιδιότητες των θετικών ακεραίων τις οποίες πραγματεύεται η Θεωρία Αριθμών, πάντα γοήτευαν τους μαθηματικούς. Οι αρχαίοι Έλληνες ήταν οι πρώτοι που αντιλήφθηκαν τη σημασία των πρώτων αριθμών και τη δυναμική που κρύβουν , φτάνοντας σε σπουδαία συμπεράσματα σχετικά με τη φύση τους. Τα συμπεράσματα αυτά εμπλουτίστηκαν με τις ισχυρές μαθηματικές αποδείξεις και αποτελούν ακόμα και στις μέρες μας αριστουργήματα της ανθρώπινης διανόησης. Τα "Στοιχεία" του Ευκλείδη ,τα οποία γράφτηκαν περί το 300π.χ. στην

Αλεξάνδρεια , αποτελούνται από 13 βιβλία τα οποία θεωρούνται σήμερα από τα αρχαιότερα περιλαμβάνοντας και στοιχεία Θεωρίας Αριθμών .

Στην παρούσα εργασία θα παρουσιασθούν μέθοδοι πιστοποίησης πρώτου αριθμού και παραγοντοποίησης ακεραίου ξεκινώντας απο τις κλασσικές μεθόδους όπως η μέθοδος των διαδοχικών διαιρέσεων, το κόσκινο του Ερατοσθένη ,η παραγοντοποίηση του Fermat και η μέθοδος του Euler.θα ακολουθήσουν στοιχεία απο τη Θεωρία Αριθμών και στη συνέχεια θα αναλυθούν 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.

ΚΕΦΑΛΑΙΟ 1

ΚΛΑΣΣΙΚΕΣ ΜΕΘΟΔΟΙ

1.1 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 αν 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 $O(\sqrt{n}(\log n)^2)$.

Παράδειγμα

Έστω ότι θέλουμε να διαπιστώσουμε, με την παραπάνω μέθοδο, αν ο n=4.567 είναι πρώτος. Έχουμε $\sqrt{4.567} = 67{,}5$ και κάνουμε τις διαιρέσεις. Διαπιστώνουμε ότι κανένας πρώτος αριθμός μέχρι τον 67 δεν διαιρεί τον 4.567 , οπότε είναι πρώτος.

1.2 ΤΟ ΚΟΣΚΙΝΟ ΤΟΥ ΕΡΑΤΟΣΘΕΝΗ

Ο **Ερατοσθένης** (276π.χ. - 194π.χ.) από την Κυρήνη, το σημερινό Um Sahad στην Λιβύη, ήταν διευθυντής στην βιβλιοθήκη της Αλεξάνδρειας. Αξίζει να αναφερθεί οτι 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 απο 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.

<u>Κόσκινο του Ερατοσθένη</u> :

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

2. Διαλέγουμε διαδοχικά τους πρώτους αριθμούς ξεκινώντας απο τον 2 έως τον ακέραιο p που είναι μικρότερος ή ίσος από τον $\sqrt{n}$, τους μαρκάρουμε σαν πρώτους αριθμούς και ύστερα διαγράφουμε όλα τα πολλαπλάσιά τους (2p, 3p, 4p, 5p ,.....). 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 οτι ο σχετικά μικρός αριθμός Mersenne 2^{127}-1 είναι πράγματι πρώτος.

Παράδειγμα

Θα βρούμε όλους τους πρώτους αριθμούς μέχρι τον αριθμό 53 και θα αποφανθούμε για το αν ο 53 είναι πρώτος.

Υπολογίζουμε $\sqrt{53}$ =7,28 άρα ο μεγαλύτερος πρώτος που θα χρειαστεί να μαρκάρουμε και να διαγράψουμε τα πολλαπλάσιά του, είναι ο 7.

	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~~
~~52~~	53								

1.3 Η ΜΕΘΟΔΟΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΤΟΥ FERMAT

Ο **Pierre de Fermat** (1601-1665μ.χ.) 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 απο την αλληλογραφία του με τον Αββά Marin Mersenne, έναν Φραγκισκανό καλόγερο και ενθουσιώδη αριθμοθεωρητικό που δίδασκε Θεωρία Αριθμών στην Σορβόνη(Παρίσι).

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) = 829·809 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 μακρυά , 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 $t \cdot n = (x+y)(x-y)$.

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

$t < x - y < x + y < n$ άρα $1 < \text{ΜΚΔ}(x \pm y, n) < n$ και κατά συνέπεια οι ακέραιοι $\text{ΜΚΔ}(x \pm y, n)$ είναι γνήσιοι παράγοντες του n.

<u>ΒΑΣΙΚΟ ΚΡΙΤΗΡΙΟ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ</u>

Γενικότερα , αν βρούμε ακεραίους x , y με

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

τότε οι ακέραιοι $\text{ΜΚΔ}(x \pm y, n)$ 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 - 3·329.345 = 1

3·329.345 = (994+1)(994-1) = 995·993

329.345 = 995·331

ΜΚΔ(329.345 , 995) = 995

ΜΚΔ(329.345 , 993) = 331

Με την κλασσική μέθοδο του Fermat θα χρεαζόταν να δοκιμάσουμε αρκετά περισσότερες τιμές για το k για να φτάσουμε στην παραγοντοποίηση.

1.4 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 2

ΕΙΣΑΓΩΓΙΚΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

2.1 ΙΣΟΔΥΝΑΜΙΕΣ΄Η 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 Αρχιμήδη 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 modm λέγεται **ισοδυναμία**.

Λέμε ότι:

- ο a είναι ισοδύναμος του b κατά μέτρο m
- ο b είναι ισοϋπόλοιπος του α 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≠0 a=amodc (αυτοπαθής)
2. αν a=bmodc τότε b=amodc (συμμετρική)
3. αν a=bmodc και b=dmodc τότε a=dmodc (μεταβατική)
4. αν a=a'modc και b=b'modc τότε a±b=a'±b'modc και ab=a'b'modc
5. αν bd=bd'modc και ΜΚΔ(b,c)=1 τότε d=d'modc (κανόνας απλοποίησης)

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

2.2 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 n 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 ή $\mathbb{Z}_p^*$

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 , $\varphi(m)$ το πλήθος όπως θα δούμε αμέσως .

ΣΥΝΑΡΤΗΣΗ $\varphi(n)$ ΤΟΥ EULER

Η συνάρτηση $\varphi(n)$ του Euler είναι μια αριθμητική συνάρτηση(δηλ. 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 $\varphi(1) = 1$
2. εάν p πρώτος τότε $\varphi(p) = p - 1$
3. $\sum_{d|n} \varphi(d)$ = n (η άθροιση γίνεται πάνω σε όλους τους διαιρέτες του n)
4. η συνάρτηση $\varphi(n)$ είναι πολλαπλασιαστική δηλ. $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ όταν ΜΚΔ(m,n)=1
5. εάν p πρώτος και κ>0 τότε $\varphi(p^k) = p^k - p^{k-1}$
6. εάν n>1 και $n=p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ τότε $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_r})$

Η τελευταία σχέση αποδεικνύεται από την αρχή του εγκλεισμού-αποκλεισμού ή με επαγωγή στο r.

2.3 ΒΑΣΙΚΑ ΘΕΩΡΗΜΑΤΑ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ

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

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 $ar_i = ar_j \bmod m$ τότε αφού ΜΚΔ(a,m)=1, από τον κανόνα της απλοποίησης θα είχαμε $r_i = r_j \bmod m$, το οποίο είναι άτοπο διότι οι αριθμοί r_i ανήκουν σε περιορισμένο σύνολο υπολοίπων.

Μπορούμε λοιπόν να αντιστοιχίσουμε κάθε αριθμό ar_i με κάποιον r_j έτσι ώστε $ar_i = r_j \bmod m$ 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

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

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

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

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 απο τον κανόνα της απλοποίησης έχουμε :

$$a^{\varphi(m)}=1 \bmod m . \quad \bullet$$

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 θεώρημα αυτό είναι ειδική περίπτωση του θεωρήματος του Euler για αυτό σήμερα θεωρείται πόρισμά του.

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

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

ΟΡΙΣΜΟΣ Λέμε ότι ο ā είναι ο **αντίστροφος** του a modn εάν a ā = 1 modn.

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)!=-1 modm 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 ā αυτού με $1 \leq \bar{a} \leq m-1$ και $a\bar{a} = 1 \text{ mod} m$.

Πιθανόν a=ā δηλαδή $a^2=1 \text{mod} m$ 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 $a=\pm 1 \text{mod} m$.

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

Έχουμε λοιπόν $(m-1)!=(m-1)(m-2)!=(m-1)1\cdot 1 ...1=-1 \text{mod} m$.

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)! =-1modm 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)! =-1modm δεν μπορεί να ισχύει. ●

2.4 ΠΡΩΤΑΡΧΙΚΕΣ ΡΙΖΕΣ ΚΑΙ ΤΕΤΡΑΓΩΝΙΚΑ ΥΠΟΛΟΙΠΑ

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

ΘΕΩΡΗΜΑ Μια ικανή και αναγκαία συνθήκη για να ισχύει a^b=1modm 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=1modm άρα d|1 και για να συμβαίνει αυτό πρέπει d=1.Άρα ΜΚΔ(a,m)=1.

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

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

Απόδειξη: Από τον αλγόριθμο του Ευκλείδη r=kh+s , 0≤ s<h.
Άρα $a^r=a^{kh+s}=(a^h)^k\cdot a^s=a^s$modm (διότι ο a ανήκει στον εκθέτη h modm).
Όμως a^r=1modm άρα a^s=1modm.Αλλά ο h είναι ο μικρότερος εκθέτης για τον οποίο ισχύει a^h=1modm 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)
Αλλιώς λέμε ότι η μικρότερη δύναμη του g που ισούται με 1modm είναι η φ(m).

ΘΕΩΡΗΜΑ Αν ο g είναι πρωταρχική ρίζα modm τότε οι δυνάμεις του g δηλαδή $g,g^2,...,g^{\varphi(m)}$ 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 $g^r=g^s \bmod m$ (δηλ. 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 δηλ. $g^{\varphi(m)}=1 \bmod m$ 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.
   (ειδική περίπτωση της ιδιότητας 3.)

Παράδειγμα

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

Από το 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 (ο p δεν διαιρεί τον α) ⇒ 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.●

ΠΟΡΙΣΜΑ 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 $1^2,2^2,\ldots,\left(\frac{p-1}{2}\right)^2$ modp.

Απόδειξη: Έστω p μονός πρώτος. Θα προσδιορίσω τα a με 1≤a≤p-1 που είναι λύσεις της ισοδυναμίας x^2=amodp.

Αλλά $x^2=(p-x)^2$modp ,διότι $x^2-(p-x)^2$=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≤x≤ $\frac{p-1}{2}$.

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=amodp θα είχε 4 μη ισοδύναμες λύσεις modp πράγμα που αντίκειται στο θεώρημα του Lagrange :

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

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

<u>ΛΗΜΜΑ</u> Αν p πρώτος και (a,p)=1 τότε είτε $a^{\frac{p-1}{2}}$ = 1modp είτε $a^{\frac{p-1}{2}}$ = -1modp .

Απόδειξη: Αφού ο p είναι πρώτος και (a,p)=1 από το Θ.Fermat a^{p-1}=1modp ⇒ a^{p-1}-1=πολ.p ⇒

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

Παράδειγμα

Τα QR του 11 είναι 5 αριθμοί .

1^2=1mod11=10^2 Άρα QR:$\{1,3,4,5,9\}$

2^2=4mod11=9^2 QNR:$\{2,6,7,8,10\}$

3^2=9mod11=8^2

4^2=5mod11=7^2

5^2=3mod11=6^2

2.5 ΣΥΜΒΟΛΟ LEGENDRE ΚΑΙ ΣΥΜΒΟΛΟ JACOBI

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

$$\left(\frac{a}{p}\right)=\begin{cases} 1 \ \text{αν} \ \alpha \in \text{QR mod}p \\ -1 \ \text{αν} \ \alpha \notin \text{QR mod}p \\ 0 \ \text{αν} \ \alpha = \text{πολ. p} \end{cases}$$

Ιδιότητες:

1. $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$ αν α=bmodp
2. $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$ modp (α,p)=1 (Κριτήριο Euler)
3. $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
4. $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$ $\left(=\begin{cases} 1 \ \text{αν} \ \text{p} = 1\text{mod}4 \\ -1 \ \text{αν} \ \text{p} = 3\text{mod}4 \end{cases}\right)$
5. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$ $\left(=\begin{cases} 1 \ \text{αν} \ \text{p} = \pm 1\text{mod}8 \\ -1 \ \text{αν} \ \text{p} = \pm 3\text{mod}8 \end{cases}\right)$
6. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ p,q πρώτοι, **Τετραγωνικός νόμος αντιστροφής** (QRL του Gauss)

<u>ΛΗΜΜΑ ΤΟΥ GAUSS</u> Αν p πρώτος και (α,p)=1 τότε $\left(\frac{a}{p}\right)=(-1)^{s}$ όπου s το πλήθος των στοιχείων του συνόλου $\left\{\alpha, 2\alpha, 3\alpha, \dots, \frac{\mathrm{p}-1}{2}\mathrm{a}\right\}$ που είναι μεγαλύτερα του $\frac{p}{2}$. (Απόδειξη: (1) Σελ. 57)

<u>ΟΡΙΣΜΟΣ</u> 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 $\mathrm{n}=\mathrm{p}_1^{\mathrm{k}_1}\ \mathrm{p}_2^{\mathrm{k}_2}\dots\mathrm{p}_{\mathrm{r}}^{\mathrm{k}_{\mathrm{r}}}$, το σύμβολο Jacobi θα είναι :

$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)^{k_1}\left(\frac{a}{p_2}\right)^{k_2}\dots\left(\frac{a}{p_r}\right)^{k_r}$, όπου $\left(\frac{a}{p_i}\right)$ το σύμβολο του Legendre.

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

Ιδιότητες:

Για n,m μονούς ακεραίους ≥3 και α,b ακεραίους.

1. $\left(\frac{a}{n}\right)=\left(\frac{b}{n}\right)$ αν α=bmodn
2. $\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
3. $\left(\frac{a}{mn}\right)=\left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
4. $\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}$
5. $\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$

Παράδειγμα

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

$1573=11^2\cdot13$, $1050=2\cdot3\cdot5^2\cdot7$

$\left(\frac{1050}{1573}\right)=\left(\frac{1050}{11\cdot11\cdot13}\right)=\left(\frac{1050}{11}\right)\left(\frac{1050}{11}\right)\left(\frac{1050}{13}\right)=\left(\frac{1050}{11}\right)^2\left(\frac{1050}{13}\right)=1\cdot\left(\frac{1050}{13}\right)=\left(\frac{1050}{13}\right)$
$=\left(\frac{1050\mathrm{mod}13}{13}\right)=\left(\frac{10}{13}\right)=\left(\frac{2\cdot5}{13}\right)=\left(\frac{2}{13}\right)\left(\frac{5}{13}\right)$

$\left(\frac{2}{13}\right)=(-1)^{\frac{13^2-1}{8}}=(-1)^{21}$=-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 3

ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΩΤΟΥ ΑΡΙΘΜΟΥ

3.1 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 325 π.χ. και πέθανε το 265 π.χ., 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 ανθρωπότητας τα τελευταία 2000 χρόνια.

ΘΕΩΡΗΜΑ(Ευκλείδης) Υπάρχουν άπειροι πρώτοι αριθμοί.

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

Θεωρώ τον φυσικό αριθμό $P= p_1.p_2...p_n+1$ 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:

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

$p_k|P \Rightarrow p_k| P- p_1.p_2...p_n \Rightarrow p_k|1$ 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 $\frac{1}{lnx}$.

<u>ΘΕΩΡΗΜΑ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ</u>

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

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1 \quad \text{ή} \quad \pi(x) \sim \frac{x}{\ln x} \ .$$

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, συνήθως για τα δύο τελευταία.

3.2 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 $n \leq 340$ όμως για τον σύνθετο n=341=31·11 :

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

Παράδειγμα

n=91=7·13

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

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

ΑΛΓΟΡΙΘΜΟΣ 1 (FERMAT TEST)

Είσοδος: Μονός φυσικός $n \geq 3$.

Μέθοδος: 1.Επιλέγω τυχαία $\alpha \in \{2,3, \dots, n-2\}$

2.εάν $\alpha^{n-1} \neq 1 \bmod n$

3.τότε επιστροφή 1

4.αλλιώς επιστροφή 0

Αν ο αλγόριθμος δώσει 1 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 $\alpha^{n-1} \bmod n$ είναι $O(\log n)$ αριθμητικές πράξεις και $O((\log n)^3)$ 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={α| $1 \leq \alpha < n$ $\mu\varepsilon$ $\alpha^{n-1}\text{mod}n = 1\}$ 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∈ L_n^F που ισχύει διότι 1^{n-1}=1modn τετριμμένα.
2) Η L_n^F είναι κλειστή ως προς την πράξη πολλαπλασιασμός modn διότι α^{n-1}modn=1 και b^{n-1}modn=1 συνεπάγεται $(\alpha b)^{n-1}=\alpha^{n-1}b^{n-1}=1\cdot 1=1$modn.

Αφού το $\mathbb{Z}_n^*$ έχει τουλάχιστον ένα στοιχείο , το L_n^F είναι γνήσια υποομάδα του $\mathbb{Z}_n^*$. 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 $|L_n^F| \leq \frac{n-2}{2}$.Άρα η πιθανότητα μία τυχαία επιλογή από το $\{2,3,\dots,n-2\}$ να ανήκει στο L_n^F-$\{1, n-1\}$ είναι το πολύ $\frac{\frac{n-2}{2}-2}{n-3} = \frac{n-6}{2(n-3)} < \frac{1}{2}$. ●

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 $\alpha \in \{2,3, \dots, n-2\}$

3. εάν $\alpha^{n-1} \neq 1 \bmod n$ 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 α με (α,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 σύνθετοι αριθμοί που ονομάζονται αριθμοί Carmichael που δεν ικανοποιούν το τεστ του Fermat διότι όλα τα στοιχεία του $\mathbb{Z}_n^*$ είναι F-ψεύτες. Οι αριθμοί αυτοί είναι άπειροι και σχετικά ομοιόμορφα κατανεμημένοι.

3.2.1 ΟΙ ΑΡΙΘΜΟΙ CARMICHAEL

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

$$\alpha^{n-1} \mathrm{mod} n=1 \quad \forall\, \alpha \in \mathbb{Z}_n^*.$$

ΠΑΡΑΤΗΡΗΣΕΙΣ

- Ο μικρότερος αριθμός Carmichael είναι ο 561=3·11·17.
- 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 (A.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 $\mathrm{mod} p^t$.Καθώς $(p^t, n/p^t)=1$ υπάρχει ακέραιος b με

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

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

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

Επίσης ο b είναι αρχική ρίζα $\mathrm{mod} p^t$. 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 α ακέραιος με (α,n)=1.

Αν p πρώτος διαιρέτης του n , τότε

$$\alpha^{p-1}=1 \text{ mod} p$$

και καθώς p-1|n-1 , έχουμε

$$\alpha^{n-1}=1 \text{ mod} p .$$

Τέλος , επειδή ο n είναι ελεύθερος τετραγώνου ισχύει

$$\alpha^{n-1}=1 \text{ mod} n.$$ ●

<u>ΘΕΩΡΗΜΑ</u> 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. ●

<u>ΚΑΤΑΣΚΕΥΗ</u> (J. 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.

3.3 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 (α,p)=1 τότε $\left(\frac{\alpha}{p}\right)= \alpha^{\frac{p-1}{2}}$ modp.Εάν α είναι τετραγωνικό υπόλοιπο modp θα ισχύει $\left(\frac{\alpha}{p}\right)= \alpha^{\frac{p-1}{2}} =1$modp και εάν α δεν είναι τετραγωνικό υπόλοιπο modp θα έχουμε $\left(\frac{\alpha}{p}\right)= \alpha^{\frac{p-1}{2}} = -1$modp. Άρα λοιπόν εάν p μονός πρώτος τότε $\alpha^{\frac{p-1}{2}} \cdot \left(\frac{\alpha}{p}\right)= 1$modp για κάθε $\alpha\in \{1,2,\dots,p-1\}$. Καταλήγουμε λοιπόν στο ότι εάν $\alpha^{\frac{n-1}{2}} \cdot \left(\frac{\alpha}{n}\right) \neq 1$modn τότε ο n δεν είναι πρώτος , για μονό $n\geq 3$ και $\alpha\in \{2,\dots,n-2\}$. Η πολυπλοκότητα της διαδικασίας είναι $O((\log n)^3)$.

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

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

Παράδειγμα

Έστω $n=325=13\cdot 5^2$.

- για α=15 έχουμε (325,15)=5 άρα $\left(\frac{15}{325}\right)$=0.Ο 15 είναι Ε- μάρτυρας του 325.
- για α=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.

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

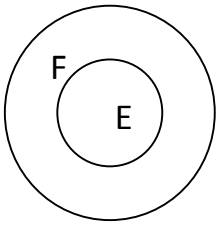
Άρα ο 2 είναι Ε-μάρτυρας του 325.

- για α=7, $7^{162}=((7^9)^9)^2=(307^9)^2=((307^3)^3)^2=(18^3)^2=307^2=324=-1 \bmod 325$

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

  Άρα ο 7 είναι Ε-ψεύτης για τον 325.

ΛΗΜΜΑ Έστω ο μονός σύνθετος $n \geq 3$ τότε κάθε Ε-ψεύτης του n είναι επίσης και F- ψεύτης του n.



Απόδειξη: Αν α είναι Ε- ψεύτης τότε $\alpha^{\frac{n-1}{2}} \cdot \left(\frac{\alpha}{n}\right) \bmod n=1$ αλλά τότε $\left(\frac{\alpha}{n}\right)=1$ ή -1 , οπότε τετραγωνίζοντας έχω $\left[\alpha^{\frac{n-1}{2}} \cdot \left(\frac{\alpha}{n}\right)\right]^2 \bmod n=1 \Rightarrow \alpha^{n-1} \bmod n=1$. Άρα ο α είναι και F-ψεύτης. ●

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

ΛΗΜΜΑ Έστω $n \geq 3$ ένας μονός σύνθετος . Τότε το σύνολο $L_n^E=\{a \mid \alpha \text{ είναι } E-\text{ψεύτης του } n\}$ 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 Ε-ψευτών είναι υποσύνολο του $\mathbb{Z}_n^*$. Θα εφαρμόσουμε το κριτήριο για υποομάδες για να δείξουμε ότι το σύνολο των Ε-ψευτών είναι υποομάδα του $\mathbb{Z}_n^*$.

Τέλος θα δείξουμε ότι το $\mathbb{Z}_n^*$ περιέχει τουλάχιστον έναν Ε-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 α,b ∈ $\mathbb{Z}_n^*$ είναι E-ψεύτες για τον n. Τότε

$$(\alpha \cdot b)^{\frac{n-1}{2}} \cdot \left(\frac{\alpha \cdot b}{n}\right) \text{mod} n = \alpha^{\frac{n-1}{2}} \cdot \left(\frac{\alpha}{n}\right) \text{mod} n \cdot b^{\frac{n-1}{2}} \cdot \left(\frac{b}{n}\right) \text{mod} n = 1 \cdot 1 = 1$$

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

Περίπτωση 1η: Έστω $p^2|n$ για κάποιο πρώτο p≥3. Από το θεώρημα περί αριθμών Carmichael είδαμε πώς κατασκευάζουμε έναν F-μάρτυρα στο $\mathbb{Z}_n^*$,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·m όπου p μονός πρώτος και m≥3 μονός με p†m.

Έστω b∈ $\mathbb{Z}_p^*$ κάποιο μη τετραγωνικό υπόλοιπο modp , δηλαδή $\left(\frac{b}{p}\right)$=-1. Από το ΚΘΥ (Κινέζικο Θεώρημα Υπολοίπων) υπάρχει 1≤α<n με :

$$\alpha = b \text{ mod} p \quad (1)$$

$$\alpha = 1 \text{ mod} m \quad (2)$$

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

Απόδειξη ισχυρισμού: p†α άρα α≠ πολ.p , διότι από (1) α-b=πολ.p και αν α=πολ.p θα είχα b=0 ή b=πολ.p , ενώ $\left(\frac{b}{p}\right)$=-1.

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

Ακόμα $\left(\frac{\alpha}{n}\right)=\left(\frac{\alpha}{p}\right)\cdot\left(\frac{\alpha}{m}\right)=\left(\frac{b}{p}\right)\cdot\left(\frac{1}{m}\right)=\left(\frac{b}{p}\right)\cdot 1=-1\cdot 1=-1$.

Αν ο α ήταν Ε-ψεύτης θα είχα $\alpha^{\frac{n-1}{2}}$ =-1modn αφού $\left(\frac{\alpha}{n}\right)$=-1. Όμως n=πολ.m και θα είχα $\alpha^{\frac{n-1}{2}}$ =-1modm , που έρχεται σε αντίθεση με το ότι α=1modm(η σχέση (2)).Άρα ο α είναι Ε-μάρτυρας για το n. ●

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

ΚΡΙΤΗΡΙΟ SOLOVAY-STRASSEN

Είσοδος: Μονός ακέραιος n≥3

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

2.Αν $\alpha^{\frac{n-1}{2}} \cdot \left(\frac{\alpha}{n}\right)$modn ≠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 $\alpha^{\frac{n-1}{2}}$ modn γίνεται με fast exponentiation και ο υπολογισμός του συμβόλου Jacobi γίνεται από τον παρακάτω αλγόριθμο.

3.3.1 Ο ΑΛΓΟΡΙΘΜΟΣ ΓΙΑ ΤΟ ΣΥΜΒΟΛΟ ΤΟΥ JACOBI

Είσοδος: Ακέραιος α , μονός ακέραιος n≥3

Μέθοδος: 0. b,c,s ακέραιοι

1. b←α modn ; c← n ;
2. s← 1
3. while b≥2 repeat
    4. while 4|b repeat b← b|4
    5. if 2|b then
        6. if c mod8 ∈ {3,5} then s← (-s)
        7. b← b|2
    8. if b=1 then break
    9. if b mod4=c mod4=3 then s← (-s)
    10. (b,c)← (c modb,b);
11. return s·b ;

3.4 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 $O((\log n)^3)$.

Το κριτήριο βασίζεται στο παρακάτω θεώρημα.

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

$\alpha^u \equiv 1 \bmod n$

είτε υπάρχει $r \in \{0,1,\dots,k-1\}$ με

$\alpha^{2^r \cdot u} \equiv -1 \bmod n$.

Απόδειξη: Έστω $d=\mathrm{ord}_n(\alpha^u)$ δηλαδή d είναι ο μικρότερος φυσικός για τον οποίο ισχύει $(\alpha^u)^d \equiv 1 \bmod n$.

Καθώς ο n είναι πρώτος έχουμε $(\alpha^u)^{2^k} \equiv 1 \bmod n$ και επομένως ο d διαιρεί τον 2^k.

Αν d=1 τότε $\alpha^u \equiv 1 \bmod n$.

Αν d>1 τότε $d=2^\ell$ με $1 \leq \ell \leq k$ και επομένως $\mathrm{ord}_n(a^{2^{\ell-1}\cdot u})=2$.

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

$a^{2^{\ell-1}\cdot u} \equiv -1 \bmod n$. ●

ΟΡΙΣΜΟΣ Έστω n≥3 μονός θετικός ακέραιος και γράφουμε $n-1=u\cdot 2^k$ με u μονό και $k \geq 1$. Ο αριθμός α , 1≤α<n ονομάζεται **Α-μάρτυρας** για τον n εάν $\alpha^u \neq \pm 1 \bmod n$ και $\alpha^{u\cdot 2^i} \neq -1 \bmod n$ για όλα τα i με $0 \leq i < k$.

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≥3.

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

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

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

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 , $2\leq\alpha\leq n-2$.

- Υπολογίζω τον $b_0=\alpha^u \mod n$. Αν $b_0=\pm 1$ σταματάμε και ο n είναι πιθανά πρώτος.

- Αλλιώς υπολογίζουμε τον $b_1=b_0^2 \mod n$.
  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

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

Έστω $\alpha=2$.

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, $561=33\cdot 17=3\cdot 11\cdot 17$.

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 πολύ λιγότεροι από τους ψευδοπρώτους. Συγκεκριμένα μέχρι το 10^{10} υπάρχουν 455.052.511 πρώτοι αριθμοί. Στο διάστημα αυτό και για δοσμένη βάση α=2 , υπάρχουν 14.884 ψευδοπρώτοι και 3.291 ισχυροί ψευδοπρώτοι. Άρα το κριτήριο του Fermat θα αποτύχει να αναγνωρίσει έναν σύνθετο στην περιοχή αυτή με πιθανότητα $<\frac{1}{30.000}$ ενώ το κριτήριο Miller-Rabin αποτυχαίνει με πιθανότητα $<\frac{1}{100.000}$. Ο πρώτος ισχυρός ψευδοπρώτος για τις βάσεις 2,3,5,7 είναι ο 3.215.031.751 ενώ για όλες τις πρώτες βάσεις που είναι μικρότερες του 200 , υπάρχει ένας ισχυρός ψευδοπρώτος με 337 ψηφία.

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

ΚΕΦΑΛΑΙΟ 4

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.

4.1 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. $x^2 = y^2 \mathrm{mod} n$
2. $x \neq \pm y \mathrm{mod} n$

Οπότε $(x + y)(x - y) = k \cdot n$, δηλαδή ο n παραγοντοποιείται και οι αριθμοί $\mathrm{ΜΚΔ}(x - y, n), \mathrm{ΜΚΔ}(x + y, n)$ 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 n, τις οποίες θα δούμε παρακάτω.

ΟΡΙΣΜΟΙ

1. **Βάση παραγοντοποίησης B** είναι το σύνολο των διακεκριμένων πρώτων $B=\{-1, p_1, p_2, \dots, p_h\}$ όπου $-1=n-1 \bmod n$
2. Ένας ακέραιος καλείται **B-λείος** αν γράφεται σαν γινόμενο στοιχείων του B.
3. Ένας ακέραιος b λέγεται **B-προσαρμοσμένος ως προς τον φυσικό n** αν ο ακέραιος c, με $-n/2 \le c \le n/2$ και $b^2 = c \bmod n$, είναι B-λείος.(Παρατηρούμε ότι ο b είναι B-προσαρμοσμένος ως προς τον φυσικό n εάν το τετράγωνό του αναλύεται σε πρώτους παράγοντες της βάσης B.)

Παράδειγμα

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

Ο αριθμός 59 είναι B-προσαρμοσμένος ως προς τον 1147 και ο αριθμός 71 είναι B-προσαρμοσμένος ως προς τον 2489 διότι:

- $59^2=40 \bmod 1147$, $-1147/2 \le 40 \le 1147/2$ και ο 40 είναι B-λείος

- $71^2=63 \bmod 2489$, $-2489/2 \le 63 \le 2489/2$ και ο 71 είναι B-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 $\bmod 2$ γραμμικές εξαρτήσεις μεταξύ των γραμμών.Οι γραμμικά εξαρτημένες γραμμές δίνουν το ζητούμενο $x^2 = y^2 \bmod n$ (για διάφορα x, y).Αν $x \neq \pm y \bmod n$ καταλήγουμε κατά τα γνωστά σε μη τετριμμένο παράγοντα του n. Η πολυπλοκότητα του αλγορίθμου,με

κατάλληλα μικρή βάση, δίνει χρόνο εκτέλεσης $O(e^{c\sqrt{logn\cdot loglogn}})$, άρα είναι υποεκθετικού χρόνου.

ΑΛΓΟΡΙΘΜΟΣ ΤΟΥ DIXON

1. Επιλέγω φυσικό y και θεωρώ την βάση B 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 $1\le b_i\le n$ όπου $i=1,\ldots,\pi(y)+2$ που να είναι B-προσαρμοσμένοι ως προς τον n.
3. Αν $b_i^2=(-1)^{a_{i0}}p_1^{a_{i1}}\ldots p_{\pi(y)}^{a_{i\pi(y)}} \bmod n$ τότε αντιστοιχώ στο b_i το διάνυσμα u_i των εκθετών : $u_i=(u_{i0},u_{i1},\ldots,u_{i\pi(y)})$ 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 περιττός.(0,1 τα στοιχεία του $\mathbb{Z}_2$)
4. Υπολογίζω το υποσύνολο I του $\{1,\ldots,\pi(y)+2\}$ με $\sum_{i\in I}u_i=0$. (δηλαδή τα γραμμικά εξαρτημένα mod2).
5. Υπολογίζω τα γινόμενα $b=\prod_{i\in I}b_i$, $c=p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_{\pi(y)}^{\gamma_{\pi(y)}}$ όπου $2\gamma_j=\sum_{i\in I}a_{ij}$.
   Προσοχή: κάθε πρώτος της βάσης B πρέπει να χρησιμοποιείται άρτιο πλήθος φορών.
6. Αν $b\neq \pm c \bmod n$ υπολογίζω τον ΜΚΔ$(b+c,n)$ που δίνει μη τετριμμένο παράγοντα του n. Αν $b=\pm c \bmod n$ τότε υπολογίζω άλλο $I\subset\{1,\ldots,\pi(y)+2\}$ 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 ($r\ge 2$) τότε η

πολυωνυμική ισοδυναμία $x^2 = b^2 \mathrm{mod} n$ θα έχει r λύσεις. Η πιθανότητα λοιπόν να έχω $b = \pm c \ \mathrm{mod} n$ ισούται με $1/2^{r-1}$.
Ένας απλός τρόπος εύρεσης των ακεραίων b_i είναι να δοκιμάζουμε ακεραίους της μορφής $\lfloor \sqrt{kn} \rfloor + j \quad (j = 0,1, \dots \ , k = 1,2, \dots)$. Ο μικρότερος κατ' απόλυτη τιμή ακέραιος της κλάσης του τετραγώνου τέτοιων ακεραίων $\mathrm{mod} n$ είναι αρκετά μικρός και άρα έχουν μεγάλη πιθανότητα να είναι B-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=1,2,...9 , j=0,1,2,... και προκύπτουν τα παρακάτω:

$\sqrt{n} = 305{,}9\dots \qquad b_1 : 306^2 = 93.636 = 13 \mathrm{mod} n \in B$

$\sqrt{2n} = 432{,}7\dots \qquad b_2 : 433^2 = 187.489 = 243 = 3^5 \mathrm{mod} n \in B$

$\sqrt{3n} = 529{,}9\dots \qquad b_3 : 531^2 = 281.961 = 1.092 = 2^2 \cdot 3 \cdot 7 \cdot 13 \mathrm{mod} n \in B$

$b_4 : 537^2 = 288.369 = 7.500 = 2^2 \cdot 3 \cdot 5^4 \mathrm{mod} n \in B$

$\sqrt{4n} = 611{,}9\dots \qquad b_5 : 612^2 = 374.544 = 52 = 2^2 \cdot 13 \mathrm{mod} n \in B$

$\sqrt{7n} = 809{,}5\dots \qquad b_6 : 809^2 = 654.481 = -880 = -2^4 \cdot 5 \cdot 11 \mathrm{mod} n \in B$

$\sqrt{8n} = 865{,}4\dots \qquad b_7 : 866^2 = 749.956 = 972 = 2^2 \cdot 3^5 \mathrm{mod} n \in B$

$\sqrt{9n} = 917{,}9\dots \qquad b_8 : 918^2 = 842.724 = 117 = 3^2 \cdot 13 \mathrm{mod} n \in B$

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 $x_1 \cdot u_1 + x_2 \cdot u_2 + \ldots + x_8 \cdot u_8 = 0 \bmod 2$ για να βρω μια σχέση γραμμικής εξάρτησης μεταξύ τους.Ισοδύναμα έχουμε :

$$\begin{cases} x_6 = 0 \\ x_2 + x_3 + x_4 + x_7 = 0 \\ x_3 = 0 \\ x_1 + x_3 + x_5 + x_8 = 0 \end{cases} \pmod 2$$

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

$$b = \prod_{i \in I} b_i = b_1 b_5 = 306 \cdot 612 = 187.272$$

$$c^2 = 13 \cdot 2^2 \cdot 13 \;\Rightarrow\; c = 26$$

Όμως $187.272 = 26 \bmod 93.623$ 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 $b = b_2 b_4 = 433 \cdot 537 = 232.521$

$c^2 = 3^5 \cdot 2^2 \cdot 3 \cdot 5^4 = 3^6 \cdot 2^2 \cdot 5^4 \Rightarrow c = 1350$

Καθώς $232.521 = 45.275 \bmod 93.623$ δηλαδή $b \neq \pm c \bmod n$ 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 $\text{ΜΚΔ} = 373$ και $93.623 = 373 \cdot 251.$

4.2 Ο ΑΛΓΟΡΙΘΜΟΣ p-1 ΤΟΥ J.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 J.POLLARD

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

<u>Παράδειγμα Βήμα 1ο</u>

Έστω $\mathrm{B} = 19$ 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 παράγοντες δίνουν εκθέτη 1.

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

$$\alpha^{\kappa}=\alpha^{l\cdot(\mathrm{p}-1)}=(\alpha^{\mathrm{p}-1})^{l}=1 \mathrm{mod} \mathrm{p} \Rightarrow \alpha^{\kappa}-1=\text{πολ.}\,\mathrm{p} \Rightarrow \mathrm{p} \mid \alpha^{\kappa}-1 .$$

Αν λοιπόν $1<\mathrm{d}<\mathrm{n}$ τότε ο d είναι μη τετριμμένος παράγοντας του n.

Η πολυπλοκότητα του αλγορίθμου είναι $O(\mathrm{B}^2(\log \mathrm{B})^2(\log \mathrm{n})^2)$ και για $\mathrm{B}=O((\log \mathrm{n})^c)$, 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.Πρακτικά για B>100 ο αλγόριθμος δεν αποδίδει.

Παράδειγμα

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	

4.3 Ο ΑΛΓΟΡΙΘΜΟΣ Rho ΤΟΥ J.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 $\mathrm{x} \neq \mathrm{x}'$ και $\mathrm{x} = \mathrm{x}' \mathrm{mod p}$. Τότε $\mathrm{p} \leq \mathrm{ΜΚΔ}(\mathrm{x} - \mathrm{x}', \mathrm{n}) < \mathrm{n}$ και υπολογίζοντας τον ΜΚΔ βρίσκουμε έναν μη τετριμμένο παράγοντα του n. Παρακτικά ,εάν θέλουμε να παραγοντοποιήσουμε τον n , επιλέγουμε πρώτα ένα τυχαίο υποσύνολο X του $\mathbb{Z}_n$ και υπολογίζουμε τους $\mathrm{ΜΚΔ}(\mathrm{x} - \mathrm{x}', \mathrm{n})$ για όλα τα x, x' στο X, με $\mathrm{x} \neq \mathrm{x}'$. Η διαδικασία αυτή όμως είναι επιτυχής μόνο στην περίπτωση που η απεικόνιση $\mathrm{x} \to \mathrm{x mod p}$ οδηγεί σε τουλάχιστον μία <<σύγκρουση>> για το $\mathrm{x} \in \mathrm{X}$. Η περίπτωση αυτή στηρίζεται στο παράδοξο των γενεθλίων: εάν $|\mathrm{X}| \approx 1{,}17\sqrt{\mathrm{n}}$ 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 $(\mathrm{x}, \mathrm{x}')$ στο πεδίο ορισμού για το οποίο ισχύει $\mathrm{x} \neq \mathrm{x}'$ και $f(\mathrm{x}) = f(\mathrm{x}')$.

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 $1{,}17\sqrt{\mathrm{n}}$ διαφορετικών εισόδων περιμένουμε να βρούμε ένα ζεύγος εισόδων x και x' $(\mathrm{x} \neq \mathrm{x}')$ ώστε να ισχύει $f(\mathrm{x}) = f(\mathrm{x}')$.

Απόδειξη: Θεωρούμε την ομάδα των ακεραίων $\mathrm{mod n}$, δηλαδή το σύνολο $\mathbb{Z}_n = \{0,1,2, \ldots \mathrm{n} - 1\}$ με $|\mathbb{Z}_n| = \mathrm{n}$. 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 $1/\mathrm{n}$. Η πρώτη μας επιλογή είναι αυθαίρετη. Η πιθανότητα η

δεύτερη επιλογή να είναι διαφορετική από την πρώτη είναι $\frac{n-1}{n}$ =1 - $\frac{1}{n}$. Η πιθανότητα η τρίτη επιλογή να είναι διαφορετική από τις προηγούμενες δύο είναι $\frac{n-2}{n}$ =1 - $\frac{2}{n}$ κ.ο.κ.

Έτσι η πιθανότητα επιλογής k στοιχείων χωρίς συγκρούσεις είναι :

$\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\left(1-\frac{3}{n}\right)\ldots\left(1-\frac{k-1}{n}\right)=\prod_{i=1}^{k-1}\left(1-\frac{i}{n}\right)$ 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- $x + \frac{x^2}{2!} - \frac{x^3}{3!} + \ldots$.

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

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

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

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

$e^{-k(k-1)/2n} \approx 1\text{-}p \Rightarrow \frac{-k(k-1)}{2n} \approx \ln(1-p) \Rightarrow \frac{k(k-1)}{2n} \approx -\ln(1-p) \Rightarrow$
$\frac{k(k-1)}{2n} \approx \ln(1-p)^{-1} \Rightarrow k^2 - k \approx 2n\ln\frac{1}{1-p}$.

Αγνοώντας τον όρο $-k$ έχουμε την εκτίμηση $k \approx \sqrt{2n\ln\frac{1}{1-p}}$ 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 $f(\mathrm{x})=\mathrm{x}^2+a$ όπου α είναι μικρή σταθερά , συνήθως α=1.

Έστω $\mathrm{x}_1 \in \mathbb{Z}_n$ και $\mathrm{X} \subseteq \mathbb{Z}_n$ με

$$\mathrm{X}=\{\mathrm{x}_1, \mathrm{x}_2, \dots, \mathrm{x}_m \mid \mathrm{x}_\mathrm{j}=f(\mathrm{x}_{\mathrm{j}-1}) \mathrm{mod} n \quad \forall \mathrm{j}=2,3,\dots,\mathrm{m}\} .$$

Σκοπός είναι η εύρεση δύο διαφορετικών τιμών $\mathrm{x}_\mathrm{i}, \mathrm{x}_\mathrm{j} \in \mathrm{X}$ 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 $\binom{|X|}{2}=\binom{m}{2}$ 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 $\mathrm{x}_\mathrm{i} \equiv \mathrm{x}_\mathrm{j} (\mathrm{mod} p)$. Η f είναι πολυωνυμική συνάρτηση με ακέραιους συντελεστές οπότε $f(\mathrm{x}_\mathrm{i})=f(\mathrm{x}_\mathrm{j})(\mathrm{mod} p)$. Από την κατασκευή του υποσυνόλου X έχουμε ότι $\mathrm{x}_\mathrm{j}=f(\mathrm{x}_{\mathrm{j}-1})\mathrm{mod} n \quad \forall \mathrm{j}=2,3,\dots,\mathrm{m}$. Τότε

$$\mathrm{x}_{\mathrm{i}+1}\mathrm{mod} p=(f(\mathrm{x}_\mathrm{i}) \mathrm{mod} n) \mathrm{mod} p=f(\mathrm{x}_\mathrm{i}) \mathrm{mod} p \quad (\text{διότι } p|n)$$

ομοίως $\mathrm{x}_{j+1}\mathrm{mod} p=(f(\mathrm{x}_\mathrm{j}) \mathrm{mod} n) \mathrm{mod} p=f(\mathrm{x}_\mathrm{j}) \mathrm{mod} p$

Συνεπώς θα έχουμε $\mathrm{x}_{\mathrm{i}+1} \equiv \mathrm{x}_{\mathrm{j}+1} (\mathrm{mod} p)$.

Επαναλαμβάνοντας την διαδικασία,υποθέτοντας ότι ισχύει $\mathrm{x}_\mathrm{i} \equiv \mathrm{x}_\mathrm{j} (\mathrm{mod} p)$, καταλήγουμε στα εξής σημαντικά αποτελέσματα:

(1) $\mathrm{x}_{\mathrm{i}+\delta} \equiv \mathrm{x}_{\mathrm{j}+\delta} (\mathrm{mod} p)$, $\forall \delta \geq 0$.

(2) $\mathrm{x}_{\mathrm{i}'} \equiv \mathrm{x}_{\mathrm{j}'} (\mathrm{mod} p)$, $\mathrm{j}'>\mathrm{i}' \geq \mathrm{i}$ και $\mathrm{j}'-\mathrm{i}' \equiv 0 \mathrm{mod} l$ όπου l=j-i .

(3) $\mathrm{x}_{\mathrm{i}'} \equiv \mathrm{x}_{2\mathrm{i}'} (\mathrm{mod} p)$, $\mathrm{i}' \geq \mathrm{i}$ και $\mathrm{i}' \equiv 0 \mathrm{mod} l$ όπου l=j-i .

ΑΛΓΟΡΙΘΜΟΣ POLLARD Rho

1. Επιλέγουμε $x_1 \in \mathbb{Z}_n$ και υπολογίζουμε το $x_2 = f(x_1) = {x_1}^2 + 1(\mathrm{mod} n)$. Υπολογίζουμε τον ΜΚΔ(x_2- x_1,n)=p.
   Αν p=1 προχωράμε στο επόμενο βήμα.

2. Υπολογίζουμε τους ακεραίους $x_i = f(x_{i-1})\mathrm{mod} n$ και $x_{2i} = f(x_{2i-1})\mathrm{mod} n$ για i=2 . Έπειτα βρίσκουμε τον ΜΚΔ(x_{2i}- x_i,n)= p .
   Αν 1< p<n τότε $x_i \equiv x_{2i}(\mathrm{mod} p)$ 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 $x_i \equiv x_j \ (\mathrm{mod} p)$ τότε μεταξύ των l ακεραίων (l = j − i) θα υπάρχει κάποιο $i' \geq i$ πολλαπλάσιο του l και από τη σχέση (3) στην προηγούμενη σελίδα , θα έχουμε $x_{i'} \equiv x_{2i'} \ (\mathrm{mod} p)$.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 $\sqrt{p}$ και επειδή $p \leq \sqrt{n}$, 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 $x_i \equiv x_j \ (\mathrm{mod} n)$ παράλληλα με την $x_i \equiv x_j \ (\mathrm{mod} p)$, 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 $p \leq \sqrt{n}$). Συνεπώς επαναλαμβάνουμε τη διαδικασία επιλέγοντας διαφορετική αρχική τιμή ή διαφορετική συνάρτηση f.

Παράδειγμα

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 $x_{11} \equiv x_{22}$ (modp) και τον μη τετριμμένο παράγοντα 71 . Άρα 7.171=71·101 όπου 71 , 101 είναι πρώτοι αριθμοί. Η πρώτη σύγκρουση είναι η $x_7$mod71=x_{18}mod71=58 .

Βιβλιογραφία

(1) ''ΚΡΥΠΤΟΓΡΑΦΙΑ'', Α.ΠΑΠΑΪΩΑΝΝΟΥ , Χ.ΚΟΥΚΟΥΒΙΝΟΣ ,ΕΜΠ 2007

(2) "ΚΡΥΠΤΟΓΡΑΦΙΑ.Η ΕΠΙΣΤΗΜΗ ΤΗΣ ΑΣΦΑΛΟΥΣ ΕΠΙΚΟΙΝΩΝΙΑΣ", ΔΗΜΗΤΡΙΟΣ Μ. ΠΟΥΛΑΚΗΣ , ΖΗΤΗ 2004

(3) "ΣΗΜΕΙΩΣΕΙΣ ΣΤΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ ΚΑΙ ΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ" Ε.ΖΑΧΟΣ , ΕΜΠ 2004

(4) www.wikipedia.gr

(5) "CRYPTOGRAPHY:AN INTRODUCTION", SMART N. , Mc GRAW-HILL 2003

(6) "CRYPTOGRAPHY:THEORY AND PRACTICE" ,3rd EDITION, DOUGLAS R.STINSON , CHAPMAN & HALL /CRC 2006