ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΠΙΣΤΟΠΟΙΗΣΗ ΚΑΙ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ

ΧΡΗΣΤΟΣ Ν. ΒΑΡΔΑΤΣΙΚΟΣ

Εξεταστική Επιτροπή:

1. Α. Παπαϊωάννου, Καθηγητής ΕΜΠ (Επιβλέπων)
2. Θ. Ρασσιάς, Καθηγητής ΕΜΠ
3. Π. Στεφανέας, Λέκτορας ΕΜΠ

Αθήνα, Ιούλιος 2013

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Η παρούσα διπλωματική εργασία πραγματεύεται τη μελέτη αλγορίθμων πιστοποίησης και παραγοντοποίησης πρώτων αριθμών.

Ξεκινώντας, το πρώτο κεφάλαιο περιλαμβάνει βασικά θεωρήματα και στοιχεία από τη θεωρία αριθμών όπως το Θεώρημα του Lucas, οι γραμμικές ισοδυναμίες, οι ισοδυναμίες δευτέρου βαθμού, τα τετραγωνικά υπόλοιπα και οι πρωταρχικές ρίζες.

Εν συνεχεία, στο δεύτερο κεφάλαιο γίνεται παρουσίαση των βασικών αλγόριθμων που χρησιμοποιούνται για την πιστοποίηση πρώτων. Γίνεται αναφορά στο κόσκινο του Ερατοσθένη και στο κριτήριο του Fermat. Επίσης, αναλύονται τα κριτήρια Miller - Rabin και Solovay-Strassen.

Το τρίτο κεφάλαιο αφορά την παραγοντοποίηση ακεραίων. Παρατίθενται συνοπτικά η μέθοδος των διαδοχικών διαιρέσεων, η μέθοδος του Fermat και η μέθοδος του Euler, ενώ αναπτύσσονται ο αλγόριθμος p-1 του John Pollard (1974) και ο αλγόριθμος Pollard Rho.

ΚΕΦΑΛΑΙΟ 1
ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ

1.1 Εισάγωγη

Σε αρκετά κρυπτοσυστήματα δημόσιου κλειδιού, π.χ. το RSA, χρησιμοποιούνται μεγάλοι πρώτοι οι οποίοι επιλέγονται με τυχαίο τρόπο. Αυτό επιτυγχάνεται με την κατασκευή τυχαίων περιττών ακεραίων με το επιθυμητό μήκος οι οποίοι κατόπιν ελέγχονται για να διαπιστωθεί αν είναι πρώτοι. Η πιο απλή και παλιά μέθοδος για να κάνουμε αυτό τον έλεγχο βασίζεται στην παρακάτω πρόταση, γνωστή από την βασική Θεωρία Αριθμών.

Πρόταση *Αν n* είναι ένας σύνθετος θετικός ακέραιος, τότε έχει ένα πρώτο διαιρέτη p με $p \le \sqrt{n}$.

Συνεπώς, αν ένας θετικός ακέραιος n δεν έχει πρώτο διαιρέτη $\le \sqrt{n}$, τότε είναι πρώτος. Έτσι, για να διαπιστώσουμε αν ο n είναι πρώτος, δοκιμάζουμε αν αυτός διαιρείται από όλους τους πρώτους $\le \sqrt{n}$. Η διαδικασία αυτή καλείται μέθοδος των διαδοχικών διαιρέσεων.

Παράδειγμα Θα χρησιμοποιήσουμε την παραπάνω μέθοδο για να διαπιστώσουμε αν ο ακέραιος n = 2593 είναι πρώτος. Έχουμε $50 < \sqrt{2593} < 51$. Βρίσκουμε εύκολα ότι κανένας πρώτος < 50 δεν διαιρεί τον n. Συνεπώς, σύμφωνα με την Πρόταση 1.1, ο n είναι πρώτος.

Για να αποδειχθεί ότι ο n είναι πρώτος με την μέθοδο των διαδοχικών διαιρέσεων πρέπει να εκτελεστούν τουλάχιστον $\left(\sqrt{n}-2\right)/\log n$ διαιρέσεις και κατά συνέπεια ο χρόνος που απαιτείται για την εφαρμογή αυτής της μεθόδου είναι εκθετικός. Οπότε, αυτή η μέθοδος δεν είναι αποτελεσματική στη περίπτωση όπου ο n είναι αρκετά μεγάλος. Οι πρώτοι που χρησιμοποιούνται στο κρυπτοσύστημα RSA είναι > 10^{75}. Έτσι, για να διαπιστωθεί ότι ένας τέτοιος αριθμός είναι πρώτος απαιτούνται περισσότερες από 10^{34} διαιρέσεις, πράγμα που είναι ανέφικτο. Στη περίπτωση που θεωρήσουμε ότι όλοι οι πρώτοι $\le \sqrt{n}$ είναι γνωστοί, έπεται ότι ο

χρόνος εφαρμογής της μεθόδου είναι $O\left(\sqrt{n}\log n\right)$. Διαφορετικά, θα πρέπει να δοκιμάσουμε αν ο n διαιρείται από όλους τους περιττούς $\leq \sqrt{n}$ και επομένως ο χρόνος εφαρμογής της μεθόδου είναι $O\left(\sqrt{n}(\log n)^2\right)$.

Η σπουδαιότητα αυτού του προβλήματος και η σημαντική του εφαρμογή στη κρυπτογραφία την τελευταία εικοσαετία οδήγησε πολλούς ερευνητές από την εποχή του Ευκλείδη μέχρι σήμερα στη δημιουργία αρκετών αλγορίθμων για την πιστοποίηση πρώτου. Κανένας όμως από αυτούς εφαρμοζόμενος σ' έναν ακέραιο n δεν δίνει σε πολυωνυμικό χρόνο ως αποτέλεσμα αν ο n είναι πρώτος ή σύνθετος.

Στην επόμενη ενότητα θα περιγράφουμε έναν τρόπο κατασκευής πρώτων αριθμών που βασίζεται στο θεώρημα του Lucas.

1.2 Θεώρημα του Lucas

Σ' αυτή την ενότητα θα δώσουμε μία μέθοδο κατασκευής πρώτων αριθμών που βασίζεται στο παρακάτω θεώρημα του E. Lucas.

Θεώρημα

Ας είναι n ένας περιττός θετικός ακέραιος. Τότε ο n είναι πρώτος, αν και μόνον αν υπάρχει ακέραιος α με (α, n) = 1 τέτοιος, ώστε

$$\mathrm{a}^{n-1} \equiv 1(\mathrm{mod}\, n) \text{ και } \mathrm{a}^{n-1/p} \not\equiv 1(\mathrm{mod}\, n)$$

για κάθε πρώτο διαιρέτη του p του n-1

***Απόδειξη*:** Ας υποθέσουμε ότι ο n είναι πρώτος. Τότε οι παραπάνω σχέσεις ικανοποιούνται από μία πρωταρχική αρχική ρίζα (mod n). Αντιστρόφως, ας υποθέσουμε ότι υπάρχει ακέραιος α που να ικανοποιεί αυτές τις σχέσεις. Τότε $ord_n \alpha = n-1$. Οπότε $n-1 \mid \varphi(n)$ και καθώς $\varphi(n) \leq n-1$ έπεται $\varphi(n) = n-1$, απ' όπου έχουμε ότι ο n είναι πρώτος.

Για να κατασκευάσουμε μεγάλους πρώτους εργαζόμαστε ως εξής: Θεωρούμε μερικούς γνωστούς πρώτους $p_1, ..., p_k$ και θετικούς ακέραιους $e_0, e_1, ..., e_k$. Θέτουμε

$$n = 1 + 2^{e_0} p_1^{e_1} \cdots p_k^{e_k}$$

και επιλέγοντας τυχαία έναν ακέραιο α ελέγχουμε αν οι υποθέσεις του παραπάνω θεωρήματος ικανοποιούνται. Αυτό είναι εύκολο γιατί γνωρίζουμε τους πρώτους p_i. Αν μετά από μερικές επιλογές του α βλέπουμε ότι οι υποθέσεις του θεωρήματος δεν ικανοποιούνται, τότε θεωρούμε έναν άλλο n.

Ο χρόνος που απαιτείται για τον υπολογισμό της δύναμης $a^{n-1} \pmod n$ είναι $O\left((\log n)^3\right)$. Επίσης, για τον υπολογισμό κάδε δύναμης $a^{n-1/p} \pmod n$ χρειάζεται χρόνος $O\left((\log n)^2(\log n / p)\right)$. Καθώς το πλήθος των πρώτων διαιρετών του n είναι $O(\log n)$ έπεται ότι για κάθε α ο χρόνος που απαιτείται για να εφαρμόσουμε την παραπάνω διαδικασία είναι $O\left((\log n)^4\right)$.

Παράδειγμα Θεωρούμε τον αριθμό

$$n = 1 + 2 \cdot 3^2 \cdot 5^3 \cdot 7^2 \cdot 101 = 11135251$$

και κάνουμε τους εξής υπολογισμούς

$$2^{n-1} \equiv 1(mod\ n), \quad 2^{n-1/2} \equiv -1(mod\ n),$$
$$2^{n-1/3} \equiv 7009340(mod\ n), \quad 2^{n-1/5} \equiv 390964(mod\ n),$$
$$2^{n-1/7} \equiv 6654420(mod\ n), \quad 2^{n-1/101} \equiv 6577006(mod\ n).$$

Σύμφωνα με το θεώρημα 1.1, ο 11135251 είναι πρώτος.

1.3 Γραμμικές Ισοδυναμίες

Στη παράγραφο αυτή θα εξετάσουμε τη λύση πρωτοβάθμιων ισοδυναμιών και θα δούμε τα βασικά θεωρήματα της θεωρίας αριθμών συγκεκριμένα το θεώρημα του Euler, το μικρό θεώρημα του Fermat και το θεώρημα του Wilson. Επίσης θα εξετάσουμε την λύση ενός συστήματος πρωτοβαθμίων ισοδυναμιών.
Ένα τέτοιο πρόβλημα τέθηκε τον 1ο αιώνα μ.Χ. από τον Κινέζο μαθηματικό Sun-Tsu και έχει γίνει γνωστό σαν το κινέζικο θεώρημα υπολοίπων (Chinese remainder theorem(ΚΘΥ)).
Μπορούμε εύκολα να μετατρέψουμε την διοφαντική εξίσωση σε γραμμική ισοδυναμία παρατηρώντας ότι θέλουμε στην ουσία να βρούμε για ποιες τιμές του x η παράσταση $\frac{ax-c}{b}$ ισούται με ακέραιο αριθμό. Δηλαδή για ποιες τιμές του x

ισχύει η σχέση ax-c=πολb δηλαδή η ισοδυναμία ax=cmodb.

Αν λοιπόν a,b,c ακέραιοι μπορούμε να βρούμε ακέραιο n με

an=bmodc. (1)

Παρατηρούμε ότι αν ο n ικανοποιεί την ισοδυναμία τότε όλοι οι ακέραιοι της μορφής n+kc την ικανοποιούν διότι a(n+kc)=an+akc=an=bmodc.

Παράδειγμα Αν $a=5$, $b=3$, $c=8$ η ισοδυναμία 5n=3mod8 έχει την λύση n=7. Επίσης όλοι οι αριθμοί του συνόλου {-9, -1, 7, 15, 23, ...} ικανοποιούν την ισοδυναμία.

Βλέπουμε λοιπόν ότι αν υπάρχει μία λύση της ισοδυναμίας (1) τότε υπάρχουν άπειρες. Όμως όλες αυτές οι λύσεις είναι ισοδύναμες modc.

Μπαίνει λοιπόν και ένα δεύτερο ερώτημα υπάρχουν λύσεις που να μην είναι ισοδύναμες modn; και αν ναι πόσες είναι αυτές;

Θα απαντήσουμε χρησιμοποιώντας τα όσα γνωρίζουμε για Διοφαντικές εξισώσεις.

Πράγματι η (1) ισοδυναμεί με το να βρούμε ακεραίους n,k τέτοιους ώστε an-b=kc δηλαδή

an+(-c)k=b (2)

Όμως ακέραιοι n, k που να ικανοποιούν την (2) υπάρχουν αν και μόνο αν d|b όπου d=ΜΚΑ (a,c) και μάλιστα κάθε λύση της (2) έχει την μορφή

$$n = n_0 + \frac{ct}{d} \text{ και } k = k_0 + \frac{at}{d} \qquad (3)$$

όπου n_0, k_0 μία συγκεκριμένη λύση και t ακέραια παράμετρος.

Από τις άπειρες τιμές του n που δίνει η σχέση (3) παρατηρούμε ότι οι d τιμές n, $n_0 + \frac{c}{d}, n_0 + \frac{2c}{d}, ..., n_0 + (d-1)\frac{c}{d}$ είναι μη ισοδύναμες modc διότι προφανώς το απόλυτο της διαφοράς δύο οιονδήποτε από αυτές είναι μικρότερο του c.

Αν $n = n_0 + c\frac{t}{d}$ είναι οποιαδήποτε άλλη λύση θέτουμε t=qd+r με 0≤r<d και

έχουμε $n = n_0 + c\frac{(qd+r)}{d} = n_0 + cq + \frac{cr}{d} = n_0 + \frac{cr}{d} \bmod c.$

Δηλαδή κάθε λύση της (2) άρα και της (1) θα είναι ισοδύναμη με κάποια από τις d λύσεις που δίνει η (3). Συμπερασματικά αν υπάρχει λύση της (1)θα υπάρχουν d το πλήθος λύσεις της (1) μη ισοδύναμες μεταξύ τους με d=ΜΚΑ (a,c).

Θεώρημα Αν $d=MK\Delta(a,c)$ τότε η ισοδυναμία $an=b \bmod c$ δεν έχει λύση αν †$d \quad b$ και έχει d μη ισοδύναμες λύσεις αν d | b.

Παράδειγμα Η ισοδυναμία που είδαμε στο προηγούμενο παράδειγμα $5n=3 \bmod 8$ επειδή $MK\Delta(5,8)=1$ και $1|3$ έχει λύση και όλες οι λύσεις της είναι ισοδύναμες.

2) Η ισοδυναμία $21x=l1 \bmod 3$ αφού d=3 =ΜΚΔ (21,3) και 3|11 δεν έχει λύση.

3) Η ισοδυναμία $15x=9 \bmod 12$ αφού d=ΜΚΑ (15,12)=3 και 3|9 θα έχει 3 μη ισοδύναμες λύσεις.

Η x=3 είναι μία λύση. Όλες οι λύσεις δίδονται από την σχέση

$$x = 3 + \frac{12}{3}t = 3 + 4t, \qquad t \in \square.$$

Οι 3 διαφορετικές λύσεις δίνονται για τις τιμές t=0,l,...,d-l ήτοι t=0,l,2 και είναι οι

x = 3

x = 7

x = 11.

Θα εφαρμόσουμε το Θεώρημα για b=l. Πρώτα όπως δίνουμε δύο ορισμούς.

Λέμε ότι η **λύση μίας γραμμικής ισοδυναμίας είναι μοναδική** modc αν κάθε λύση n' της είναι ισοδύναμη με την n modc (όπως η πρώτη ισοδυναμία του προηγούμενου παραδείγματος).

Αν $a\bar{a} = 1 \bmod c$ λέμε ότι ο $\bar{a}$ είναι **αντίστροφος** του amodc.

Πόρισμα Αν ΜΚΔ(a,c)=1 τότε ο a έχει αντίστροφο που είναι μοναδικός modc.

Απόδειξη*:* Αν ΜΚΔ (a,c)=l τότε το Θεώρημα 1.3 λέει ότι η $an=1 \bmod c$ έχει d=l λύση που είναι μοναδική modc.

Παράδειγμα α) Αφού $5^2=25=1 \bmod 8$ ο 5 έχει έναν μόνο αντίστροφο, τον εαυτό του mod8. Προφανώς και ο -3 και ο 13 είναι αντίστροφοι του 5 mod8 που όμως είναι ισοδύναμες του 5 διότι

3=5=13mod8.

β) Ο αντίστροφος του a=2mod5 είναι ο 3 διότι 2*3 =1mod5.

Ο αντίστροφος του a=7mod9 είναι ο 4 διότι 7*4=1mod9.

Ο αντίστροφος του a=12mod17 είναι ο 10 διότι 12*10=1mod17.

Θα αποδείξουμε τώρα το θεώρημα του Euler και το πόρισμά του που είναι γνωστό σαν μικρό θεώρημα του Fermat. Τα δύο αυτά θεωρήματα έχουν μία σημαντική εφαρμογή στην κρυπτογραφία και συγκεκριμένα στην μέθοδο RSA της κρυπτογραφίας με δημόσιο κλειδί, που θα δούμε αναλυτικά αργότερα.

Θεώρημα (Euler) Αν ο ΜΚΔ (a,m)=l τότε $a^{\varphi(m)} = 1 \bmod m$.

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

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

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

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

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

Αλλά ΜΚΔ (R,m)=l διότι ο R είναι ένα γινόμενο φ(m) το πλήθος αριθμών όπου κάθε παράγοντας είναι πρώτος προς τον m. Άρα $a^{\varphi(m)} = 1 mod m$ από τον κανόνα της απλοποίησης.

Πόρισμα (Μικρό Θεώρημα του Fermat) Αν ο p πρώτος τότε $n^p = n mod p$.

Απόδειξη: Αν p | n τότε $n^p = 0 = n mod p$.

Αν p † n τότε ΜΚΔ (p,n)=1.

Άρα από το θεώρημα του Euler $n^{p-1} = 1 mod p$ διότι φ(p)=p-1

και αν πολλαπλασιάσουμε και τα δύο μέλη επί η έχουμε n^p=nmodp.

Θεώρημα (Wilson)

Η ισοδυναμία (m-l)!=-lmodm ισχύει αν και μόνο αν ο m είναι πρώτος.

Υπενθυμίζουμε ότι n!=l, 2..., n με 0!=1, και ότι η γενίκευση της συνάρτησης παραγοντικό είναι η συνάρτηση Γ (x) [η οποία ορίζεται και για αρνητικά αλλά όχι ακέραια αρνητικά x].

Απόδειξη: Υποθέτουμε ότι ο m είναι πρώτος και θεωρούμε τους m-1 ακεραίους 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 $a\bar{a}$ = lmodm.

Πιθανόν a=$\bar{a}$ δηλαδή a^2=lmodm δηλαδή ο a να συμπίπτει με τον αντίστροφό του. Όμως στην περίπτωση αυτή a^2- l=km

(a-l)(a+l) = km ήτοι m|(a-l)(a+l) και αφού ο m είναι πρώτος θα ισχύει:

m|a-l είτε m|a+1 άρα a=±lmodm.

Στο γινόμενο (m-2)(m-3)...32=(m-2)! αντιστοιχούμε σε κάθε αριθμό τον αντίστροφο του modulo m.

Για παράδειγμα αν m=11 γράφουμε

9·8·7·6·5·4·3·2 = (95) (87) (62) (43).

Έχουμε λοιπόν

(m-1)! = (m-l)(m-2)! = (m-1) ·1·1 ...lmodm =-lmodm.

Αντίστροφα*:* Έστω ότι ο m δεν είναι πρώτος. Τότε υπάρχει a: l<a<m με a|m. Προφανώς επίσης a|(m-l)! (αφού ο παράγον a<m υπάρχει μέσα στο (m-1)!).

Αν λοιπόν (m-1)! = -lmodm τότε υπάρχει ακέραιος k με (m-l)!+l=km. Αφού a|m και a|(m-1)! ο a θα διαιρεί και την διαφορά τους άρα a|l αδύνατο διότι υπετέθη a>l. Βλέπουμε λοιπόν ότι όταν ο m δεν είναι πρώτος η σχέση (m-1)! = -1 mod m δεν μπορεί να ισχύει.

Θα εξετάσουμε τώρα την λύση όχι μίας πρωτοβάθμιας ισοδυναμίας αλλά την λύση ενός **συστήματος πρωτοβάθμιων ισοδυναμιών** και μάλιστα της μορφής

$a_1x = b_1 mod m_1$

$a_2x = b_2 mod m_2$

και $a_sx = b_s mod m_s$

Τα απλούστερα παραδείγματα τέτοιων συστημάτων εμφανίζονται όταν θέλουμε να λύσουμε μίαν πρωτοβάθμια ισοδυναμία με μέτρο μεγάλο αριθμό. Έστω $m = p_1^{\ell_1} p_2^{\ell_2} ... p_s^{\ell_s}$ η παραγοντοποίηση του m σε πρώτους παράγοντες.

Αλλά τότε από το Θεμελιώδες Θεώρημα της Αριθμητικής m|n αν και μόνο αν $p_1^{\ell_1}$ |n για κάθε i άρα

A=Bmodm αν και μόνο αν ισχύουν οι ισοδυναμίες

$A = Bmod\ p_1^{\ell_1}$

$A = Bmod p_2^{\ell_2}$

..... και

$A = Bmod p_s^{\ell_s}$.

Δηλαδή η ισοδυναμία ax=bmodm έχει το ίδιο σύνολο λύσεων με το σύστημα

$ax = bmod p_1^{\ell_1}$

$ax = bmod p_2^{\ell_2}$ (1)

$ax = bmod p_s^{\ell_s}$

Αν και στο (1) έχουμε πολλές ισοδυναμίες προς λύση τα μέτρα τους είναι πολύ μικρότερα από το m και οι πράξεις απλοποιούνται σημαντικά.

Παράδειγμα 2.4 Ας αντικαταστήσουμε την ισοδυναμία x = 1 1 m o d 2 2 7 5 με ένα γραμμικό οδυναμιών με μικρότερα μέτρσύστημα ισ α.

Έχουμε $2275=5^2 7 \cdot 13$ άρα η ισοδυναμία αντικαθίσταται από το

3x=11mod25

3x=11mod7

και 3x=11modl3 τις οποίες θα λύσουμε παρακάτω.

Τον πρώτο αιώνα μ.Χ. ο διάσημος Κινέζος μαθηματικός Sun Tsu έθεσε το πρόβλημα. Ποιος αριθμός αφήνει υπόλοιπα 2, 3 και 2 όταν διαιρεθεί αντιστοίχως με τους 3, 5, 7; Δηλαδή ο Sun Tsu με την ορολογία των ισοδυναμιών έψαχνε έναν ακέραιο n τέτοιον ώστε

n=2mod3

n=3mod5 και

n=2mod7.

Το βασικό θεώρημα ύπαρξης λύσης για ένα σύστημα ισοδυναμιών της μορφής (1) ή της ειδικής του περίπτωσης στο πρόβλημα του Sun - Tsu ονομάζεται Κινέζικο Θεώρημα Υπολοίπων [το επίθετο Κινεζικό προφανώς προς τιμή του Sun Tsu] και έχει την μορφή:

Θεώρημα (Κινεζικό Θεώρημα Υπολοίπων (ΚΘΥ))

Έστω οι s φυσικοί $m_1, m_2,..,m_s$ όπου όλοι είναι πρώτοι προς αλλήλους. και $M=m_1m_2...m_s$. Έστω επιπλέον οι s το πλήθος ακέραιοι a_i, $1\le i\le s$ με ΜΚΔ $(a_i\ m_i)=1$ για κάθε i.

Τότε οι s ισοδυναμίες

$a_1x=b_1 \mathrm{mod} m_1$

$a_2x=b_2 \mathrm{mod} m_2$

..... και

$a_sx=b_s \mathrm{mod} m_s$

έχουν μία λύση μοναδική modM.

Απόδειξη*:*

Από την λύση της κάθε ισοδυναμίας θα κατασκευάσουμε μία λύση για όλο το σύστημα.

Επιλέγουμε ακεραίους $c_1,c_2,...,c_s$ τέτοιους ώστε

$$a_i c_i = b_i \bmod m_i$$

οι αριθμοί αυτοί c_i , υπάρχουν από το Θεώρημα 2.1 που περιγράφει την λύση πρωτοβάθμιων ισοδυναμιών.

Θέτουμε τώρα $n_i = \frac{N}{m_i}$ και επειδή όλοι οι m_i είναι πρώτοι προς αλλήλους έχουμε ότι ΜΚΔ(n_i , m_i)=1. Αλλά τότε από Πόρισμα ο n_i έχει έναν μοναδικό αντίστροφο $\bmod m_i$; δηλαδή $\exists \overline{n_i}$ με $n_i\ \overline{n_i} = 1 \bmod m_i$, $1 \le i \le s$.

Σαν δεύτερο βήμα με την βοήθεια των c_i και $\overline{n_i}$ κατασκευάζουμε έναν αριθμό x_0 που θα αποδείξουμε ότι είναι λύση κάθε μίας από τις s ισοδυναμίες.

Έστω $x_0 = c_1 n_1 \overline{n_1} + c_2 n_2 \overline{n_2} + ... + c_s n_s \overline{n_s}$.

Ας παρατηρήσουμε ότι ο m_i διαιρεί όλους τους n_j εκτός από τον n_i, με τον οποίον έχει ΜΚΔ(n_i , m_i)=1.

Άρα $a_i x_0 = a_i c_1 n_1 \overline{n_1} + a_i c_2 n_2 \overline{n_2} + ... + a_i c_s n_s \overline{n_s} =$

$= a_i c_i n_i \overline{n_i} \bmod m_i$

$= a_i c_i \bmod m_i$

$a_i x_0 = b_i \bmod m_i$

Αρα ο x_0 είναι λύση και των s ισοδυναμιών.

Είναι όμως η μοναδική λύση mod M; Αν y είναι μία άλλη λύση των s ισοδυναμιών έχουμε:

$x_0 = c_i = y \bmod m_i$ Άρα $x_0 - y = \pi o \lambda m_i$ $\gamma \iota \alpha \; \kappa \acute{\alpha} \theta \varepsilon \; m_i$

αλλά όλα τα m_i είναι πρώτα μεταξύ τους άρα

$x_0 - y = \pi o \lambda m_1 m_2 ... m_s$ ήτοι $x_0 - y = \pi o \lambda M$ ήτοι

$y = x_0 \bmod M$

Παράδειγμα

Θα χρησιμοποιήσουμε το Κινεζικό Θεώρημα για να λύσουμε το πρόβλημα του Sun Tsu, δηλαδή να βρούμε τον ελάχιστο θετικό x με

x=2mod3

x=3mod5 και

x=2mod7.

Έχουμε με τον συμβολισμό του Κινεζικού Θεωρήματος $a_1 = a_2 = a_3 = 1$ $b_1 = 2 = c_1$ $b_2 = 3 = c_2$ $b_3 = 2 = c_3$, $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, $M = 105$ $n_1 = 35$ $n_2 = 21$ $n_3 = 15$.

Τώρα

$35\overline{n_1} = 1 \bmod 3 \Rightarrow 2\overline{n_1} = 1 \bmod 3 \Rightarrow \overline{n_1} = 2.$

Επίσης $21\overline{n_2} = 1 \bmod 5 \Rightarrow 1\overline{n_2} = 1 \bmod 5 \Rightarrow \overline{n_2} = 1$

και $15\overline{n_3} = 1 \bmod 7 \Rightarrow 1\overline{n_3} = 1 \bmod 7 \Rightarrow \overline{n_3} = 1$, διότι

$15\overline{n_3} = 1 \bmod 7 \Rightarrow 14\overline{n_3} + \overline{n_3} = -1 = \pi o \lambda 7 \Rightarrow \overline{n_3} - 1 = \pi o \lambda 7 \Rightarrow \overline{n_3} = 1 \bmod 7$

Άρα μία λύση του συστήματος είναι η

$x_0 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 140 + 63 + 30 = 233.$

Άρα όλες οι λύσεις είναι ισοδύναμες με το 233 και ο ελάχιστος ακέραιος είναι ο 23 διότι

233	105
23	2

Παράδειγμα Θα λύσουμε την ισοδυναμία 3x=11mod2275, δηλαδή το σύστημα

$3x=11 \bmod 25$

$3x=11 \bmod 7$ $\quad 3x-11=$πολ7

$3x=11 \bmod 13$ $\quad 3x-11=$πολ13

Αφού ΜΚΔ (2275,3)=1 η αρχική ισοδυναμία έχει λύση.

Η πρώτη ισοδυναμία έχει λύση $x=12=c_1$

Η δεύτερη ισοδυναμία έχει λύση $x=6=c_2$

Η τρίτη ισοδυναμία έχει λύση $x=8=c_3$

τώρα θα βρούμε $\overline{n_1}, \overline{n_2}, \overline{n_3}$ με

$$\frac{2275}{25}\overline{n_1} = 91\overline{n_1} = 1 \bmod 25 \Rightarrow 16\overline{n_1} = 1 \bmod 25,$$
$$\frac{2275}{7}\overline{n_2} = 325\overline{n_2} = 1 \bmod 7 \Rightarrow 3\overline{n_2} = 1 \bmod 7,$$
$$\frac{2275}{13}\overline{n_3} = 175\overline{n_3} = 1 \bmod 13 \Rightarrow 6\overline{n_3} = 1 \bmod 13.$$

Η πρώτη έχει λύση $\overline{n_1} = 11$

Η δεύτερη έχει λύση $\overline{n_2} = 5$

Η τρίτη έχει λύση $\overline{n_3} = 11$

οπότε $x_0=12\cdot 91\cdot 11+6\cdot 325\cdot 5+8\cdot 175\cdot 11=$

$=12012+9750+15\cdot 400=37162=762 \bmod 2275$

Άρα η μικρότερη λύση είναι η $x_0=762$.

Παρατηρούμε ότι λύσαμε 6 ισοδυναμίες αντί για 1 αλλά με πολύ μικρότερα μέτρα από το 2275 (συγκεκριμένα δύο με 25, δύο με 7 και δύο με 13).

Παράδειγμα Έστω ότι θέλουμε να βρούμε το $7^{-1}\text{mod}65$.

Έχουμε $$7x = 1 \bmod 65 = \begin{cases} 7x = 1 \bmod 5 \Rightarrow x_1 = 3 \\ 7x = 1 \bmod 13 \Rightarrow x_2 = 2 \end{cases}$$

Το Κινέζικο θεώρημα δίνει

$x=3\text{mod}5 \Rightarrow x=3$

$x=3\text{mod}13 \Rightarrow x=2$

άρα θα λύσουμε το $\left(\frac{65}{5}\right) y_1 = 13y_1 = 1 \bmod 5 \Rightarrow y_1 = 2 \quad \kappa\alpha\iota$

$$\left(\frac{65}{13}\right) y_2 = 5y_2 = 1 \bmod 13 \Rightarrow y_2 = 8.$$

Άρα $x_0 = \frac{65}{5} x_1 y_1 + \frac{65}{13} x_2 y_2 = 13 \cdot 3 \cdot 2 + 5 \cdot 2 \cdot 8 = 78 + 80 =$

$= 158 = 28 \bmod 65.$

Άρα $7^{-1} = 28 \bmod 65$. Πράγματι $7 \cdot 28 = 196 = 1 \bmod 65$.

Αναφέρουμε ότι το πρόβλημα του Sun Tsu αποδίδεται και στον σύγχρονό του ($1^{ος}$ αιώνας μ.Χ.) Νικόμαχο τον Γερασηνό, έναν Έλληνα μαθηματικό που έγραψε την Αριθμητική Εισαγωγή.

1.4 Ισοδυναμίες Δευτέρου Βαθμού

Στο Κεφάλαιο αυτό θα εξετάσουμε την λύση των ισοδυναμιών δευτέρου βαθμού με απλούστερη μορφή την x^2=amodp όπου p πρώτος. Η λύση οδηγεί στο περίφημο θεώρημα του Gauss τον νόμο τετραγωνικής αντιστρεπτότητας (quadratic reciprocity law). Πρώτα όπως θα αναφερθούμε σε κάποιες επιπλέον ιδιότητες των περιορισμένων συνόλων υπολοίπων. Είδαμε ότι τα στοιχεία ενός περιορισμένου συνόλου υπολοίπων αποτελούν μία πολλαπλασιαστική ομάδα. Μάλιστα θα δούμε ότι όταν ο p είναι πρώτος υπάρχει ακέραιος g με την ιδιότητα οι g, g^2, g^{p-1} να αποτελούν ένα περιορισμένο σύνολο υπολοίπων, δηλαδή με αλγεβρική ορολογία

έχουμε μία κυκλική ομάδα.
Ο ακέραιος g ονομάζεται αρχική ή πρωταρχική ρίζα modp.

Παράδειγμα Γνωρίζουμε ότι φ(10)=4 και $\{r_1=1, r_2=3, r_3=7, r_4=9\}$ περιορισμένο σύνολο υπολοίπων mod 10 . Πράγματι από τον ορισμό έχουμε

i) ΜΚΔ $(r_i,10)=1 \ \forall 1 \le i \le 4$.

ii) $r_i \neq r_j \bmod 10$ οπότε $i \neq j$.

iii) κάθε αριθμός n με (n,10)=1 αντιστοιχεί σ' έναν r_i, ήτοι $n= r_i \bmod m$ για ένα μόνο i.

Παρατηρούμε ότι $3^1=3=3 \bmod 10$ $7^1=7=7 \bmod 10$

$3^2=9=9 \bmod 10$ $7^2=49=9 \bmod 10$

$3^3=27=7 \bmod 10$ $7^3=343=3 \bmod 10$

$3^4=81=1 \bmod 10$ $7^4=2401 \bmod 10$

δηλαδή τα σύνολα $\{3^1, 3^2, 3^3, 3^4\}$ και $\{7^1, 7^2, 7^3, 7^4\}$ αποτελούν περιορισμένα σύνολα υπολοίπων mod10.
Το παράδειγμα αυτό σε συνδυασμό με την παρατήρηση ότι 4=φ(10) είναι ο ελάχιστος ακέραιος h με την ιδιότητα $g^h=1 \bmod 10$ όταν g=3, 7 μας οδηγεί στον ορισμό:
Ορισμός Αν h είναι ο μικρότερος θετικός ακέραιος τέτοιος ώστε $a^h=1 \bmod m$ τότε λέμε ότι ο a ανήκει στον εκθέτη h modulo m.

Θεώρημα Μία ικανή και αναγκαία συνθήκη για να ισχύει $a^b=1 \bmod m$ για κάποιον ακέραιο b είναι η ΜΚΔ (a,m)=1.
Απόδειξη: *Έστω* ΜΚΔ (a,m)=d. Αν d|a και d|m τότε ο d διαιρεί την διαφορά τους $a^b - \pi o \lambda m = 1$ ήτοι d|1 άρα d=1.
Αντίστροφα αν ΜΚΔ (a,m)=1 τότε $a^{\varphi(m)}=1 \bmod m$ από το θεώρημα του Eu1er οπότε $b=\varphi(m)$.

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

Απόδειξη*:* Από τον αλγόριθμο του Ευκλείδη r=kh+s $0 \le s < h$.

Αρα $1 = a^r = a^{kh+s} = (a^h)^k \cdot a^s = a^s \bmod m$ (αφού ο d ανήκει στον h ήτοι $1 = a^h \bmod m$). Αλλά αφού ο a ανήκει στον h, το h είναι n μικρότερος εκθέτης με $a^h = 1 \bmod m$ *οπότε s=0.* Αρα r=kh ήτοι h|r.

Ορισμός Αν ο ακέραιος g ανήκει στον εκθέτη φ(m)modm τότε ο g ονομάζεται **αρχική ή πρωταρχική ρίζα** modm.

Θεώρημα Αν ο g είναι αρχική 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.

Απόδειξη: Έστω $1 \le s < r < \varphi(m)$ και $g^r = g^s \bmod m$ (δηλαδή υπάρχουν δύο ισοδύναμες δυνάμεις του g). Τότε όμως $g^r - g^s = k \cdot m$ δηλαδή $m \mid g^r - g^s$ ήτοι $m \mid g^s \left(g^{r-s} - 1 \right)$ και αφού $m \nmid g^s$ έπεται ότι $m \mid g^{r-s} - 1$ δηλαδή $g^{r-s} = 1 \bmod m$.

Αλλά αφού ο g ανήκει στον εκθέτη φ(m) σημαίνει ότι $g^{\varphi(m)} = 1 \bmod m$ και φ(m) ο μικρότερος τέτοιος εκθέτης. Όμως r-s<φ(m) άρα φθάσαμε σε άτοπο. Άρα οι δυνάμεις του g είναι μη ισοδύναμες.

Παράδειγμα Θα δείξουμε ότι δεν υπάρχουν πρωταρχικές ρίζες mod8. Έστω g μία τέτοια, αφού φ(8)=4 η g θα ανήκει στον εκθέτη $4 \bmod 8$. Από το θεώρημα 3.1 έχουμε $\text{ΜΚΔ}(g,8)=1$ άρα $g = 1 \bmod 8$ ή 3mod8 ή 5mod8 ή 7mod8.

Πράγματι $1^4 = 1 \bmod 8$ αφού φ(8)=4

$3^4 = 1 \bmod 8$

$5^4 = 1 \bmod 8$

$7^4 = 1 \bmod 8$

όμως δεν είναι πρωταρχική ρίζα διότι **και** $1^2 = 1 \bmod 8$

$3^2 = 1 \bmod 8$

$5^2 = 1 \bmod 8$

$$7^2 = 1 \bmod 8$$

άρα η g δεν ανήκει στον εκθέτη 4mod8 άρα δεν υπάρχουν πρωταρχικές ρίζες mod8.

Ακολούθως θα βρούμε έναν απλό τύπο για το πλήθος των αμοιβαία μη ισοδύναμων πρωταρχικών ριζών mod8.

Θεώρημα Αν ο a ανήκει στον εκθέτη h modm και ΜΚΔ (k,h)=d τότε ο a^k ανήκει στον εκθέτη h/d modm.

Απόδειξη: Έστω ότι ο a^k ανήκει στον έκθετη j modm. Τότε a^{kj}=lmodm, άρα h| kj. Θέτω h/d=h_1 και k/d=k_1 τότε η σχέση h|k·j γίνεται $h_1|k_1 j$.

Και αφού ΜΚΔ (h,k)=d $\Rightarrow$ ΜΚΔ (h_1,k_1)=l οπότε η $h_1|$ k_1j δίνει $h_1|$ j.

Όμως $a^{kh_1} = a^{k_1 h_1 d} = a^{kh_1} = \left(a^h\right)^{k_1} = 1 \bmod m$

Άρα $j | h_1$. $j = h_1 = \frac{h}{d}$

Πόρισμα Αν g μια πρωταρχική ρίζα modm τότε η g^r είναι επίσης μία πρωταρχική ρίζα modm αν και μόνο αν ΜΚΔ (r,φ(m))=l.

Απόδειξη: Η πρωταρχική ρίζα εξ ορισμού ανήκει στον εκθέτη φ(m) άρα εξ υποθέσεως η g ανήκει στον εκθέτη φ(m). Άρα η g^r ανήκει στον εκθέτη

$\frac{\varphi(m)}{\text{ΜΚΔ}(r,\varphi(m))}$ που ισούται με φ(m) αν και μόνο αν ΜΚΔ (r,φ(m))=l.

Θεώρημα Αν υπάρχει κάποια πρωταρχική ρίζα modm τότε το πλήθος των αμοιβαία μη ισοδύναμων πρωταρχικών ριζών είναι φ(φ(m)).

Απόδειξη: Έστω g μία πρωταρχική ρίζα modm. Αλλά (Θ3.3) οι g, g^2, ..., $g^{\varphi(m)}$ είναι αμοιβαία μη ισοδύναμες και αποτελούν ένα περιορισμένο σύνολο υπολοίπων modm. Από το προηγούμενο πόρισμα η g^r είναι πρωταρχική ρίζα αν και μόνο αν ΜΚΔ (r,φ(m))=l.

Όμως από τον ορισμό της συνάρτησης του Euler υπάρχουν φ(φ(m)) αριθμοί στο διάστημα [l, φ(m)] σχετικά πρώτοι προς τον φ(m).

Παράδειγμα Αν m=10 από Θεώρημα έχουμε φ(φ(10))=φ(4)=2 αμοιβαία μη ισοδύναμες πρωταρχικές ρίζες mod10. Από το παράδειγμα 3.1 έχουμε ότι οι δύο είναι οι 3 και 7 με 3≠7mod10.

Το Θεώρημα είναι ειδική περίπτωση ενός γενικότερου θεωρήματος που υπολογίζει τις πρωταρχικές ρίζες mod p. Συγκεκριμένα θα δείξουμε ότι για κάθε πρώτο p υπάρχουν πρωταρχικές ρίζες modp.

Θεώρημα Για κάθε πρώτο p, υπάρχουν πρωταρχικές ρίζες modp.

Απόδειξη: Θεωρούμε το περιορισμένο σύνολο υπολοίπων 1, 2, . . . , p - 1 mod p Συμβολίζω με N(h) το πλήθος των ακεραίων αυτών που ανήκουν στον εκθέτη h modp.

Γνωρίζουμε ότι ο a ανήκει στον εκθέτη h mod p όπου p πρώτος σημαίνει h | p - 1 διότι a^{p-1} = lmodp (θεώρημα Fermat) και αν θέσω r = ρ - 1 στο θεώρημα 3.2 έχουμε h | p-1.

Επίσης γνωρίζουμε ότι κάθε στοιχείο ενός περιορισμένου συνόλου διαφόρων ανήκει σε κάποιο εκθέτη h modp. Άρα

$$p-1=\sum_{h|p-1} N(h)$$

Θα δείξουμε τώρα ότι N(h)=0 ή φ(h). Αν κανένας ακέραιος δεν ανήκει στο h modp τότε προφανώς N(h)=0. Αν a ανήκει στο h modp η εξίσωση

x^h= lmodp έχει το πολύ h μη ισοδύναμες λύσεις,

όμως οι h αριθμοί a, a^2,...,a^h είναι αμοιβαία μη ισοδύναμες λύσεις της εξίσωσης άρα η x^h = lmodp έχει ακριβώς h λύσεις. Άρα κάθε της λύση θα είναι ισοδύναμη με τον a^r για κάποιο r. Από Πόρισμα ο a^r ανήκει στο h αν και μόνο αν Μ.Κ.Δ. (r,h)=1. Άρα μεταξύ των αριθμών a, a^2, ..., a^h υπάρχουν ακριβώς φ(h) αριθμοί που ανήκουν στον h modp. Άρα N(h)=cp(h) εδώ.

Εν γένει λοιπόν έχουμε φ(h) ≥ N(h). Θα δείξω ότι ισχύει παντού η ισότητα. Αν υπήρχε ένας h με φ(h)>N(h) θα είχαμε από την $p-1=\sum_{h|p-1} N(h)$ και το ότι $\sum_{d|n} \varphi(d)=n$:

$$p-1=\sum_{h|p-1} N(h)<\sum_{h|p-1} \varphi(h)=\pi-1 \; \acute{\alpha}\tau o\pi o.$$

Άρα N(h)=φ(h) για όλα τα h που διαιρούν το p-1. Άρα φ(p-1) ακέραιοι ανήκουν στον εκθέτη p-1 modp δηλαδή υπάρχουν φ(p-1) πρωταρχικές ρίζες modp.

Υπενθυμίζουμε ότι αν p πρώτος φ(ρ)=p-1.

Για μικρά p, όπου p πρώτος, ο παρακάτω πίνακας δίνει κάποια πρωταρχική ρίζα (δες παράρτημα Β):

p	3	5	7	11	13	17	19	23	29	31	37	41
ρίζα	2	2	3	2	2	3	2	5	2	3	2	6

Για p=8, p=15 δεν υπάρχουν πρωτ. ρίζες mod8, mod15.

Παράδειγμα Έστω $p = 5$. Ένα περιορισμένο σύνολο υπολοίπων είναι το $\{ 1 , 2 , 3 , 4 \}$. Από το Θ3.7 υπάρχουν πρωταρχικές ρίζες mod5. Άρα από το Θ3.6 θα υπάρχουν φ(φ(5))=φ(4)=2 αμοιβαία μη ισοδύναμες πρωταρχικές ρίζες mod5.

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

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

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

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

άρα οι ρίζες 2 και 3 είναι πρωταρχικές ρίζες mod5.

Ο Gauss πρώτος, έδειξε οτι υπάρχουν πρωταρχικές ρίζες modn για $n=2,4,p,p^k ,2p^k$ όπου p μονός πρώτος και k φυσικός.

1.5 Τετραγωνικά Υπόλοιπα

Ορισμός Έστω ο πρώτος p και $ΜΚΔ(a,p)=1$. Αν $p \dagger a$ και η εξίσωση $x^2=a \bmod p$ έχει λύση λέμε ότι ο a είναι τετραγωνικό υπόλοιπο modp.

Παράδειγμα Έστω p=7. Οι αριθμοί 1, 4, 9 είναι τέλεια τετράγωνα και δεν διαιρούνται με τον 7. Άρα είναι τετραγωνικά υπόλοιπα mod7. Αλλά και όλοι οι ακέραιοι που είναι ισοδύναμοι με τα τετράγωνα

αυτά mod7 είναι επίσης τετραγωνικά υπόλοιπα mod7 όπως οι 2, 11 κοκ. Ο 49 όμως αν και τέλειο τετράγωνο δεν είναι τετραγωνικό υπόλοιπο mod7 διότι 7 | 49.
Το κριτήριο του Euler μας λέει πότε ακριβώς ένας αριθμός a είναι τετραγωνικό υπόλοιπο modp.

Θεώρημα (Κριτήριο του Euler)

Έστω $\alpha \neq 0$ *, p>2 πρώτος και (α,p)=1*

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=amodp.

Αφού $p \dagger a \Rightarrow p \dagger x$ ήτοι ΜΚΔ (x,p)=1 άρα

$$a^{\frac{p-1}{2}} = \left(x^2\right)^{\frac{p-1}{2}} = x^{p-1} = 1 \bmod p,$$

όπου τελευταία σχέση ισχύει από το θεώρημα του Euler και το γεγονός ότι φ(p)=p-1 για p πρώτο.

Αντίστροφα: αν $a^{\frac{p-1}{2}} = 1 \bmod p$ και έστω g μία πρωταρχική ρίζα modp. Υπάρχει ακέραιος r με g^r=amodp,

οπότε $g^{\frac{r(p-1)}{2}} = a^{\frac{p-1}{2}} = 1 \bmod p$

Από το θεώρημα 3.2 έχουμε $p-1 \mid \frac{r(p-1)}{2}$.

Άρα $\frac{r}{2}$ είναι ακέραιος έστω r=2s με s ακέραιο.

Αν λοιπόν $x=g^s$ έχουμε: $x^2 = g^{2s} = g^r$ = amodp.
Ένα πολύ χρήσιμο πόρισμα είναι το εξής

Πόρισμα Έστω g μία πρωταρχική ρίζα modp και έστω ΜΚΔ (a,p)=1. Έστω r ακέραιος με g^r=amodp. Τότε ο r είναι ζυγός αν και μόνο αν το a είναι τετραγωνικό υπόλοιπο modp.

Παράδειγμα

a) a=2 p=5 $\Rightarrow 2^1$ =4=-1mod5 άρα ο 2 δεν είναι τετραγωνικό υπόλοιπο mod5.

b) a=3 p=11 3^5=243=1mod11 άρα ο 3 είναι τετραγ. υπόλοιπο mod5.

c) a=4 p=7 $4^3=64=1 \bmod 7$ άρα ο 4 είναι τετραγ. υπόλοιπο mod7.

d) a=6 p=13 $6^6=45.656=-1 \bmod 13$ άρα ο 6 είναι δεν τετραγ. υπόλοιπο.

Το σύμβολο του Legendre $\left(\frac{b}{p}\right)$ όπου p περιττός πρώτος έχει τις τιμές

$$\begin{cases} 1 \ \alpha \nu \ o \ b \ \epsilon \acute{\iota} \nu \alpha \iota \ \tau \epsilon \tau \rho \alpha \gamma \omega \nu \iota \kappa \acute{o} \ \upsilon \pi \acute{o} \lambda o \iota \pi o \ m \ o \ d \ p \\ 0 \ \alpha \nu \ o \ b = \pi o \lambda \ p \\ -1 \ \sigma \tau \iota \varsigma \ \acute{\alpha} \lambda \lambda \epsilon \varsigma \ \pi \epsilon \rho \iota \pi \tau \acute{\omega} \sigma \epsilon \iota \varsigma \end{cases}$$

Ισοδύναμα $\left(\frac{b}{p}\right)=1$ αν ο b είναι τετραγωνικό υπόλοιπο στο σώμα GF (p) ή αν η

ισοδυναμία $x^2 = b \bmod p$ έχει λύση.

Ιδιότητες:

1) $\left(\frac{b}{p}\right)=\left(\frac{c}{p}\right)$ αν b = c mod p

2) $b^{\frac{p-1}{2}} = \left(\frac{b}{p}\right) \bmod p$

3) $\left(\frac{bc}{p}\right)=\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)$

4) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$

5) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$

6) $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}$ p≠q, $\pi \epsilon \rho \iota \tau \tau o \acute{\iota} \ \pi \rho \acute{\omega} \tau o \iota$

Η ιδιότητα 6 αποτελεί τον περίφημο νόμο της τετραγωνικής αντιστρεπτότητας του Gauss (1795).

Παράδειγμα

$\left(\frac{6}{13}\right)=-1$ διότι ο 6 δεν είναι τετραγωνικό υπόλοιπο mod13.

$\left(\frac{26}{13}\right)=0$

$\left(\frac{4}{13}\right)=1$ διότι $4^6 = 4096=1 \bmod 13$.

Θεώρημα Αν p μονός πρώτος

υπάρχουν $\frac{p-1}{2}$ ακριβώς μη ισοδύναμα τετραγωνικά υπόλοιπα (συντομογραφία

Q.R) του p που δίδονται από τη σχέση $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$

Απόδειξη: Έστω p μονός πρώτος. Θα προσδιορίσω τα a με l≤a≤p-l που είναι λύσεις της ισοδ. $x^2 = \text{a} \bmod p$.

Αλλά $x^2 \equiv (p-x)^2 \bmod p$.

[Πράγματι $x^2 - (p-x)^2 = x^2 - p^2 + 2px - x^2 = \pi o \lambda p$]. Τα τετράγωνα των αριθμών στα σύνολα $\left\{1, 2, .., \frac{p-1}{2}\right\}$ και $\left\{\frac{p+1}{2}, \frac{p+1}{2}+1, ..., p-1\right\}$ είναι ισοδύναμα κατά ζεύγη [όχι με την 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 $\left\{1, 2, .., \frac{p-1}{2}\right\}$ είναι όλα μη ισοδύναμα modp διότι αλλιώς η $x^2 = \text{a} \bmod p$ θα είχε 4 μη ισοδύναμες modp λύσεις, πράγμα που αντίκειται στο θεώρημα του Lagrange: «Το πλήθος των μη ισοδύναμων λύσεων της ισοδυναμίας f(x)=0modp ποτέ δεν υπερβαίνει τον βαθμό f(x). Άρα τα $\frac{p-1}{2}$ Q.R. modp είναι ακριβώς οι αριθμοί $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$.

Παράδειγμα

α) Τα QR του 19 είναι αριθμοί της μορφής

b,19-b

Πράγματι

$1^2 = 1 \bmod 19$	$18^2 = 324 = 1 \bmod 19$
$2^2 = 4 \bmod 19$	$17^2 = 289 = 4 \bmod 19$
$3^2 = 9 \bmod 19$	$16^2 = 256 = 9 \bmod 19$
$4^2 = 16 \bmod 19$	$15^2 = 225 = 16 \bmod 19$
$5^2 = 25 = 6 \bmod 19$	$14^2 = 196 = 6 \bmod 19$
$6^2 = 17 \bmod 19$	$13^2 = 169 = 17 \bmod 19$
$7^2 = 11 \bmod 19$	$12^2 = 144 = 1 \bmod 19$

$8^2 = 7\text{modl}9$ $11^2 = 121 = 7\text{modl}9$

$9^2 = 5\text{modl}\ 9$ $10^2 = 100 = 5\text{modl}9$

άρα Q.R. {1,4,5,6,7,9,11,16,17} QNR {2,3,8,10,12,13,14,15,18}

β) $x^2 \equiv 1 \bmod 31.$ Άρα QR31={1,2,4,5,7,8,9,10,14,16,18,19,20,25,28}

$1^2 \equiv 1 \bmod 31 \quad = 30^2$ QNR31={3,6,11,12,13,15,17,21,22,23,24,26,27,29,30}

$2^2 \equiv 4 \bmod 31 \quad = 29^2$

$3^2 \equiv 9 \bmod 31 \quad = 28^2$

$4^2 \equiv 16 \bmod 31 \quad = 27^2$

$5^2 \equiv 25 \bmod 31 \quad = 26^2$

$6^2 \equiv 5 \bmod 31 \quad = 25^2$

$7^2 \equiv 18 \bmod 31 \quad = 24^2$

$8^2 \equiv 2 \bmod 31 \quad = 23^2$

$9^2 \equiv 19 \bmod 31 \quad = 22^2$

$10^2 \equiv 7 \bmod 31 \quad = 21^2$

$11^2 \equiv 28 \bmod 31 \quad = 20^2$

$12^2 \equiv 20 \bmod 31 \quad = 19^2$

$13^2 \equiv 14 \bmod 31 \quad = 18^2$

$14^2 \equiv 10 \bmod 31 \quad = 17^2$

$15^2 \equiv 8 \bmod 31 \quad = 16^2$

γ) $1^2 = 1 \bmod 29 \quad = 28^2$ QR29={1,4,5,6,7,9,13,16,20,22,23,24,25,28}

$2^2 = 4 \bmod 29 \quad = 29^2$ QNR29={2.3,8,10,11,12,14,15,17,18,19,21,26,27}

$3^2 = 9 \bmod 29 \quad = 28^2$

$4^2 = 16 \bmod 29 \quad = 27^2$

$5^2 = 25 \bmod 29 \quad = 26^2$

$6^2 = 7 \bmod 29 \quad = 25^2$

$7^2 = 20 \bmod 29 \quad = 24^2$

$8^2 = 6 \bmod 29 \quad = 23^2$

$9^2 = 23 \bmod 29 \quad = 22^2$

$10^2 = 13 \bmod 29 \quad = 21^2$

$11^2 = 5 \bmod 29 \quad = 20^2$

$12^2 = 28 \bmod 31 \quad = 19^2$

$13^2 = 24 \bmod 31 \quad = 18^2$

$14^2 = 22 \bmod 31 \quad = 17^2$

Ο Euler (1755) εισήγαγε πρώτος ένα κριτήριο για να δούμε αν κάποιος αριθμός είναι QR ή όχι.
Προηγούμενα εξετάζουμε ένα λήμμα:

Λήμμα Αν p μονός πρώτος και (a,p)=1 τότε είτε

$$a^{\frac{p-1}{2}} = 1 \bmod p \text{ είτε } a^{\frac{p-1}{2}} = -1 \bmod p$$

Απόδειξη: Αφού p πρώτος και (a,p)=1 από το θεώρημα του Fermat ισχύει

$a^{p-1}=1 \bmod p$ ή $(a^{p-1}-1) = \pi o \lambda p$ ή

$$\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)\equiv 0 \bmod p$$

Οπότε είτε $a^{\frac{p-1}{2}}=1 \bmod p$ είτε $a^{\frac{p-1}{2}}=-1 \bmod p$

Θεώρημα (Κριτήριο του Euler)

Αν p μονός πρώτος και (a,p)=l τότε $\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}} \bmod p$.

Απόδειξη: Έστω μονός πρώτος p με (a,p)=l και 1≤r≤p-1. Αφού η ισοδυναμία rx=amodp έχει μοναδική λύση [(αφού (r,p)=l] υπάρχει ακριβώς ένα στοιχείο s με 1≤s<p-1 έτσι ώστε rs=amodp [το στοιχείο s είναι η λύση της ισοδυναμίας].

Περίπτωση 1: Αν a είναι QNR modp τότε $\left(\frac{a}{p}\right)=-1$ οπότε για τον s θα είναι $r \neq s$ διότι αν $r=s$, $r^2=a \bmod p$ ήτοι aQRp και τα στοιχεία του {1,2,….p-1} μπορούν να γίνουν ζεύγη r_i, s_i έτσι ώστε $r_i \cdot s_i = \text{amodpi=1,2,…, } \frac{p-1}{2}$. $\alpha \in QRmo\text{dp}$ $\acute{a}to\pi o$

Αλλά τότε το θεώρημα του Wilson $(-1)\equiv(p-1)\ !\equiv\prod_{i=1}^{\frac{p-1}{2}} r_i s_i \equiv a^{\frac{p-1}{2}} \bmod p$.

Περίπτωση 2: Αν a είναι QR modp τότε $\left(\frac{a}{p}\right)=1$ οπότε υπάρχει b: $b^2=a \bmod p$.

Από το Θεώρημα Fermat $a^{\frac{p-1}{2}}=b^{p-1}=1 \bmod p$ άρα

$$a^{\frac{p-1}{2}}=1 \bmod p=\left(\frac{a}{p}\right) \bmod p.$$

1.6 Το σύμβολο του Jacobi

Μπορούμε να γενικεύσουμε το σύμβολο του Legendre για ζεύγη α, n (n≥3) όπου ο n να μην είναι πια πρώτος. Αναλυτικά έστω $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{kr}$ η ανάλυση του

n. Για ακέραιους α έχουμε:

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)^{k_1}\cdot\left(\frac{a}{p_2}\right)^{k_2}\cdots\left(\frac{a}{p_r}\right)^{k_r}$$

Παρατηρήσεις:

1. Αν n πρώτος το σύμβολο Jacobi συμπίπτει με το σύμβολο Legendre.
2. Αν (α, n)>1 $\Rightarrow$ τα α, n έχουν κοινό παράγοντα $\Rightarrow p_i \mid a$ για κάποιο i

$$\Rightarrow\left(\frac{a}{p_i}\right)^{k_i}=0\Rightarrow\left(\frac{a}{n}\right)=0$$

Το σύμβολο Jacobi ενδιαφέρει μόνο αν (α, n)=1

3. Και στην περίπτωση αυτή δηλαδή που (α, n)=1 το σύμβολο Jacobi δεν δίνει πληροφορία αν $a \in QR \bmod n$ ή όχι.

1.7 Πρωταρχικές Ρίζες

Έστω η ισοδυναμία $x^m = a \bmod p$, p μονός πρώτος, $\alpha > 2, (\alpha, p) = 1$. Αν η ισοτιμία επιλύεται το α είναι το m τάξης υπόλοιπο του p.

Έστω ο φυσικός n με $(\alpha, n) = 1$, και ο ελάχιστος φυσικός k με $a^k = 1 \bmod n$: ο k λέγεται τάξη (order) του $a \bmod n$ και συμβολίζεται με $\text{ord}_n(\alpha)$.

Από το θεώρημα του Euler έχουμε για κάθε φυσικό n με (α, n) = 1 $a^{\varphi(n)} = 1$ άρα η $ord_n(a)$ είναι καλά ορισμένη συνάρτηση και $k \le \varphi(n)$.

Θεώρημα Αν $ord_n(a) = k$ τότε $a^h = 1 \bmod n$ αν και μόνο αν $k \mid h$.

Απόδειξη: Έστω (α, n) = 1, $ord_n(a) = k$ και $a^k = 1 \bmod n$. Από τον αλγόριθμο της διαίρεσης υπάρχουν ακέραιοι q, s τέτοιοι ώστε h = kq + s με 0 < s < k (αν s= 0 τότε k | h). Αλλά τότε $a^h = a^{kq+s} = \left(a^k\right)^q \cdot a^s$. Όμως $a^k = 1 \bmod n$ από τον ορισμό της τάξης οπότε και $a^s = 1 \bmod n$ που έρχεται σε αντίφαση με το ότι ο k είναι ο ελάχιστος ακέραιος με την ιδιότητα $a^k = 1 \bmod n$. Άρα s = 0 και k | h.

Αντίστροφα αν k|h τότε kt = h και αφού ord_n (a) = k τότε

$a^h = a^{kt} = \left(a^k\right)^t = 1 \bmod n$.

Το επόμενο θεώρημα μας δίνει την $ord_n\left(a^m\right)$ αν γνωρίζουμε την $\text{ord}_n(\alpha)$.

Θεώρημα 1.25 (Κουκουβίνος - Παπαϊωάννου, 2007: 120-121)**:** Αν $\text{ord}_n(a)= k$ τότε $ord_n\left(a^m\right) = k / \text{ΜΚΔ}(m,k)$.

Απόδειξη:Έστω $ord_n\left(a\right) = k$,

$$ord_n\left(a^m\right) = r,$$

ΜΚΔ(m,k)=d --> m = bd,k =cd με ΜΚΔ(b,c)=1

Άρα $\left(a^m\right)^c = \left(a^{bd}\right)^c = \left(a^{cd}\right)^b = \left(a^k\right)^b = 1 \bmod n.$ Από το θεώρημα 4.1 έχουμε ότι

$\text{r} \mid \text{c}.$ (1)

Αφού $ord_n\left(a\right) = k$ έχουμε $\left(a^{mr}\right) = \left(a^m\right)^r = 1 \bmod n.$ Από το θεώρημα 4.1 έχουμε

$\text{k} \mid \text{mr}$ ήτοι $\text{cd} \mid (bd)r \Rightarrow c \mid \text{br}.$ Αφού όμως $(c,b) = 1 \Rightarrow c \mid r.$ (2)

Από την (1) και (2) έχουμε r=c οπότε $ord_n\left(a^m\right) = r = c = \frac{k}{d} = \frac{k}{\text{ΜΚΔ}\left(m,k\right)}$.

Το Θεώρημα λέει ότι η τάξη κάθε στοιχείου modulo έναν πρώτο είναι διαιρέτης του $p-1$. Το Θεώρημα 4.2 λέει επιπλέον ότι αν d διαιρέτης του $p-1$ υπάρχουν $\varphi(d)$ μη ισοδύναμοι ακέραιοι mod p που έχουν τάξη d.

Παράδειγμα Για $p = 17$, ο 8 είναι διαιρέτης του p - 1 = 16.

Επιλέγω $\alpha = 3$ με (3,17) = 1 και υπολογίζω $ord_{17}\left(3\right) = 16$. Πράγματι οι δυνάμεις του 3 είναι 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, $1 = 3^{16}$ άρα $ord_{17}\left(3\right) = 16$.

Τα φ (8) = 4 στοιχεία του $\mathbb{Z}_{17}^*$ τάξης 8 είναι τα:

Υπολογίζω τα $1 \le k \le 16$ με $\text{ΜΚΔ}(k,16) = 2 \Rightarrow k = 2,6,10,14$ οπότε τα στοιχεία είναι τα: $3^2 = 9$, $3^6 = 15$, $3^{10}=8$, $3^{14} = 2$.

Πράγματι $ord_{17}\left(9\right) = ord_{17}\left(15\right) = ord_{17}\left(8\right) = ord_{17}\left(2\right) = 8$ και $3^8 = 16$.

Άμεσα πορίσματα των δύο αυτών θεωρημάτων είναι τα:

- Αν $\text{ord}_n(\alpha) = k$ τότε $k \mid \varphi(n)$.
- Αν $\text{ord}_n(\alpha) = k$ τότε $a^r = a^s \bmod n$ αν και μόνο αν $r = s \bmod k$.
- Αν $k > 0$ και $\text{ord}_n(a) = hk$ τότε $\text{ord}_n(\alpha^h) = k$
- Αν $ord_n(a) = k$, $ord_n(b) = h$, ΜΚΔ (h,k)=1 τότε $ord_n(ab) = h \cdot k$ ήτοι η συνάρτηση ord_n είναι πολλαπλασιαστική.

Οι αριθμοί $F_n = 2^{(2^n)} + 1$, με n>0 λέγονται αριθμοί Fermat.

Έχουμε ένα κριτήριο πιστοποίησης πρώτων για τους αριθμούς Fermat που προτάθηκε τον 19° αιώνα από τον Γάλλο J. Pepin.

Θεώρημα (Κριτήριο του Pepin) 1.26 (Κουκουβίνος - Παπαϊωάννου, 2007: 122-123)**:** Ο αριθμός Fermat n τάξης F_n είναι πρώτος αν και μόνο αν $3^{\frac{F_n-1}{2}} = -1 \bmod F_n$.

Απόδειξη: Έστω ότι ο F_n (n ≥ 1) είναι πρώτος. Από τον ορισμό έχουμε $F_n = 2^{(2^n)} + 1$. Ο εκθέτης του 2 είναι της μορφής 2^n άρα ζυγός, έστω $2l$, άρα $F_n = 2^{(2^n)}$ εργαζόμενοι mod3 έχουμε $F_n = 2^{2l} + 1 \bmod 3 = \left(2^2\right)^l + 1 \bmod 3 = 1 + 1 = 2 \bmod 3$ για κάθε n, ήτοι $F_n = 2 \bmod 3$. Παρόμοια $F_n = 1 \bmod 4$.

Ο QRL του Gauss δίνει $\left(\frac{3}{F_n}\right) \cdot \left(\frac{F_n}{3}\right) = 1$ αφού $F_n = 1 \bmod 4$, αλλά $\left(\frac{3}{F_n}\right) \cdot \left(\frac{F_n}{3}\right) = \left(\frac{3}{F_n}\right) \cdot \left(\frac{2}{3}\right) = \left(\frac{3}{F_n}\right) \cdot (-1)^{\frac{9-1}{8}} = \left(\frac{3}{F_n}\right) \cdot (-1)$. Άρα $\left(\frac{3}{F_n}\right) = -1$ και από το κριτήριο του Euler $3^{\frac{F_n-1}{2}} = -1 \bmod F_n$

Αντίστροφα: Έστω $3^{\frac{F_n-1}{2}} = -1 \bmod F_n$. Έστω p πρώτος διαιρέτης του F_n (άρα ο F_n όχι πρώτος) οπότε $3^{\frac{F_n-1}{2}} = -1 \bmod p$ (αφού $p \backslash F_n$). Τετραγωνίζοντας έχουμε $3^{F_n-1} = 1 \bmod p$. Αν $ord_p(3) = m$ από το θεώρημα 4.1 $m \mid F_n - 1$ ήτοι (ορισμός αριθμών Fermat) $m \mid 2^{2^n}$. Άρα $m = 2^r$ με $0 \le r \le 2^n$. Έστω $r = 2^n - s$ με s > 0.

Αλλά τότε $3^{\frac{F_n-1}{2}} = 3^{2^{2^n-1}} = 3^{2^{r+s-1}} = 1 \bmod p$ [αφού $3^m = 3^{2^r} = 1 \bmod p$] άτοπο διότι

υποθέσαμε $3^{\frac{F_n-1}{2}} = -1 \bmod p.$

Άρα s = 0 και το 3 έχει τάξη $m = 2^r = 2^{2^n} \bmod p$. Από το θεώρημα 4.1 $2^{2^n} \mid p-1$ $\acute{\alpha}\rho\alpha\ 2^{2^n} \leq p-1\ \pi o\upsilon\ \gamma\acute{\iota}\nu\varepsilon\tau\alpha\iota\ \alpha\nu\ \pi\rho o\sigma\theta\acute{\varepsilon}\sigma\omega\ \tau\eta\ \mu o\nu\acute{\alpha}\delta\alpha$

$F_n \leq p.\ A\lambda\lambda\acute{\alpha}\ p\ \pi\rho\acute{\omega}\tau o\varsigma\ \delta\iota\alpha\iota\rho\acute{\varepsilon}\tau\eta\varsigma\ \tau o\upsilon\ F_n\ \acute{\alpha}\rho\alpha\ \ F_n = p\ \kappa\alpha\iota\ F_n\ \pi\rho\acute{\omega}\tau o\varsigma.$

Για κάποιους φυσικούς *n,* υπάρχει φυσικός *q* με *1≤q≤n-1* τέτοιος ώστε οι δυνάμεις του *q* να παράγουν το περιορισμένο σύνολο υπολοίπων mod n (reduced residue system). [Δηλαδή αφαιρώ από το {0, 1, …, n – 1} τα στοιχεία που δεν είναι πρώτα προς το *n*.]

Δηλαδή για κάθε ακέραιο *r* με $1<q \leq n-1$ και με ΜΚΔ (r, n) =1 υπάρχει *k* με

$q^k = r.$ Στην περίπτωση αυτή ο *q* βοηθά στο να βρίσκουμε την τάξη των στοιχείων του περιορισμένου συνόλου υπολοίπων αλλά και τα *QR* και *QNR* του *n*.

Ονομάζουμε ένα φυσικό q **πρωταρχική** (ή αρχική) **ρίζα** αν $ord_n(q) = \varphi(n)$. Θα δείξουμε ότι οι πρωταρχικές ρίζες του *n* παράγουν το περιορισμένο σύνολο υπολοίπων mod n.

Θεώρημα 1.27 Αν ο q είναι πρωταρχική ρίζα του *n* τότε τα $q\ q^2, , ... , q^{\varphi(n)}$ αποτελούν ένα περιορισμένο σύνολο υπολοίπων mod *n*.

Απόδειξη: Αφού q πρωταρχική ρίζα $\Rightarrow ord_n(q)=\varphi(n)$ οπότε $\text{ΜΚΔ}(q,n)=1$. Άρα $\text{ΜΚΔ}(q^i,n)=1$ για i = 1,2,...,φ(n). Άρα τα $q,q^2,...,q^{\varphi(n)}$ είναι φ(n) το πλήθος φυσικοί μη ισοδύναμοι μεταξύ τους. Πράγματι αν $q^i=q^j \bmod n$ με $1\le i<j\le\varphi(n)$ τότε από το δεύτερο πόρισμα $i=j \bmod \varphi(n)$ οπότε $\varphi(n)\,|\,j-i.$ Άτοπο διότι $0<j-i<\varphi(n),$ οπότε οι δυνάμεις του $q,q^2,...,q^{\varphi(n)}$ αποτελούν ένα περιορισμένο σύνολο υπολοίπων modn.

Το 1769 ο J. Lambert μελετώντας τα δεκαδικά αναπτύγματα του $\frac{1}{p}$ *(p* πρώτος) απέδειξε το παρακάτω θεώρημα και ισχυρίστηκε ότι υπάρχουν πρωταρχικές ρίζες του *p* για κάθε πρώτο *p*. Ο Euler εισήγαγε τον όρο πρωταρχική ρίζα το 1773 και έδειξε ότι υπάρχουν φ (*p* - 1) το πλήθος πρωταρχικές ρίζες για τον πρώτο *p*. Ο Gauss έδειξε ότι αν ο πρώτος *p* έχει το 10 σαν πρωταρχική ρίζα τότε το δεκαδικό ανάπτυγμα του $\frac{1}{p}$ έχει περίοδο *p* - 1. Ο Gauss επίσης έδειξε το παρακάτω θεώρημα.

Θεώρημα (Lambert)

Αν p μονός πρώτος, h φυσικός και q πρώτος τέτοιος ώστε $q^h|p$ *- 1* τότε υπάρχει φυσικός b με $ord_p(b)=q^h.$

Απόδειξη: Αφού p ≥ 3 , από το θεώρημα του Lagrange [Υπενθύμιση: το πλήθος των μη ισοδύναμων λύσεων της πολυωνυμικής εξίσωσης f(x) = 0mod p δεν υπερβαίνει το βαθμό του πολυωνύμου f(x)] η εξίσωση $x^{\frac{p-1}{q}}=1 \bmod p$ έχει το πολύ $\frac{p-1}{q}$ λύσεις όπου $\frac{p-1}{q}\le\frac{p-1}{2}\le p-2.$ Άρα τουλάχιστον ένα στοιχείο, έστω το $\alpha,$ με

$1 \le a \le p-1$ και ΜΚΔ(α, p) = 1 <u>δεν</u> είναι λύση. Άρα $a^{\frac{p-1}{q}} \neq 1 \bmod p$. Θέτουμε $b = a^{\frac{p-1}{q^h}}$ και επίσης θέτουμε $ord_p(b) = m$. Ισχύει: $b^{q^h} = a^{p-1} \bmod p = 1 \bmod p$ και το θεώρημα λέει ότι $|m \ \ q^{\ h}$. Έστω ότι $<m \ \ q^{\ h}$. Αφού ο q πρώτος $|m \ \ q^{\ h-1}$ άρα υπάρχει ακέραιος k με $q^{h-1} = mk$. Άρα $a^{\frac{p-1}{q}} = b^{q^{h-1}} \bmod p = b^{mk} = \left(b^m\right)^k = 1^k = 1 \bmod p$ άτοπο διότι $a^{\frac{p-1}{q}} \neq 1 \bmod p$. Άρα $m = q^h = ord_p(b)$.

Θεώρημα Δεν υπάρχουν πρωταρχικές ρίζες του 2^n για n > 2.

Απόδειξη: Θα δείξουμε επαγωγικά ότι αν $\text{ΜΚΔ}\left(a, 2^n\right) = 1$ για $n>2$, τότε $ord_{2^n}(a) = 2^{n-2}$, άρα *ο α δεν* είναι πρωταρχική ρίζα του 2^n.

$$\left[\varphi\left(2^n\right) = 2^n\left(1-\frac{1}{2}\right) = 2^{n-1}\right]$$

Για $n = 3$ και $\text{ΜΚΔ}\left(a, 2^3\right) = 1$ είναι a = 1,3,5,7mod8, αλλά ισχύει

$$\left.\begin{array}{l} 1^2 = 1 \bmod 8 \\ 3^2 = 1 \bmod 8 \\ 5^2 = 1 \bmod 8 \\ 7^2 = 1 \bmod 8 \end{array}\right\} \textit{Άρα αν } \text{ΜΚΔ}(\alpha, 8) = 1 \textit{ τότε } ord_8(a) = 2 = 2^{3-2},$$

δηλαδή το θεώρημα ισχύει για $n = 3$.

Έστω λοιπόν k>3 και αν $\text{ΜΚΔ}\left(m, 2^k\right) = 1$ για θετικό m τότε $ord_{2^k}(m) = 2^{k-2}$ ήτοι $m^{2^{k-2}} = 1 \bmod 2^k$ και $m^s \neq 1 \bmod 2^k$

Έστω τώρα b: *ΜΚΔ* (b, 2^{k+1})= 1, *οπότε και* (b, 2^k)=1 *και από την επαγωγική* υπόθεση $ord_{2^k}(b) = 2^{k-2}$. Δηλαδή υπάρχει ακέραιος r με $b^{2^{k-2}} = 1 \bmod 2^k$ ήτοι $b^{2^{k-2}} = 1 + r \cdot 2^k$.

αλλά επίσης $b^{2^{k-1}} = \left(b^{2^{k-2}}\right)^2 = \left(1 + r \cdot 2^k\right)^2 = 1 + 2r \cdot 2^k + r^2 \cdot 2^{2k} = 1 \bmod 2^{k+1}.$

Υπάρχει ακέραιος s με $b^s = 1 \bmod 2^{k+1}$ και $1 \le s < 2^{k-1}$; όχι διότι τότε $b^s = 1 + t \cdot 2^{k+1} = 1 + 2t \cdot 2^k$ ήτοι $b^s = 1 \bmod 2^k$. Άρα αν $\text{ΜΚΔ}\left(b, 2^{k+1}\right) = 1 \Rightarrow ord_{2^{k+1}}(b) = 2^{k-1}$ και η επαγωγική απόδειξη ολοκληρώθηκε.

Η εύρεση πρωταρχικών ριζών ακόμα και για πρώτους είναι επίπονη εργασία. Η **μέθοδος του A. L. Crelle** δουλεύει για μικρούς πρώτους.

Χρησιμοποιεί την ιδιότητα αν για $1 \le a \le p-1$

- s_i ναι το ελάχιστο υπόλοιπο του α·imodp και
- t_j είναι το ελάχιστο υπόλοιπο του $a^j \bmod p$ $(1 \le i < j \le p-1)$

Τότε $t_k = s_{t_{k-1}}$ modp για $1 \le k \le p-1$.

Ο αλγόριθμος του Crelle δουλεύει διότι

$a^{j-1} \cdot a = a^j \bmod p$ $(1 \le i < j \le p-1)$.

Παράδειγμα

Έστω p=17, α=3. Τα πολλαπλάσια του 3 μας δίνουν τις δυνάμεις του 3 όπως φαίνεται στον πίνακα:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3κ	0	3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
3^k	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Με την βοήθεια πχ. του $3^2 = 9$ θα υπολογίσουμε το 3^3.

Αφού $3^2 = 9$ πάω στην στήλη 9 και βρίσκω το 3·9 = 10 στην δεύτερη γραμμή.

Αρα $3^3 = 3 \cdot 9 = 10 \bmod 17$, $3^4 = 3 \cdot 10 = 13 \bmod 17$,

Αφού η μικρότερη τιμή του k $1 \le k \le 16$ που δίνει $3^k = 1 \bmod 17$ είναι η k=16 το 3 είναι πρωταρχική ρίζα του 17.

Θεώρημα Αν p μονός πρώτος τότε υπάρχουν φ(p-1) πρωτ. ρίζες modp.

Απόδειξη: Έστω $p-1 = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ με $a_i \ge 1$ για i=l,2,...,r η ανάλυση του p-1

από το ΘΘΑ. Τότε από το θεώρημα του Lambert υπάρχουν φυσικοί n_i με $ord_p(n_i) = p_i$ για $1 \le i \le r$. Από το τέταρτο πόρισμα των θεωρημάτων 4.1 και 4.2, αν $m = n_1 n_2 ... n_r$ τότε $ord_p(m) = p_1^{a_1} p_2^{a_2} ... p_r^{a_r} = p - 1 \bmod p$ και αφού φ(p)=p-1 ο m είναι μία πρωταρχική ρίζα. Από το θεώρημα 4.2 αν q πρωτ. ρίζα του p και $ΜΚΔ(r, p-1) = 1$ τότε και το q^r είναι πρωτ. ρίζα του p. Άρα υπάρχουν φ(p-1) πρωτ. ρίζες του p.

Αν λοιπόν q πρωτ. ρίζα του p υπάρχουν $\varphi(p-1)$ μη ισοδύναμες πρωτ. ρίζες του p που δίνονται από την: $q_1^{a_1}, q_2^{a_2}, ... q_r^{a_{\varphi(p-1)}}$ *όπου* οι φ(p-1) φυσικοί μικρότεροι του p-1 είναι πρώτοι προς τον $p-1$.

Παράδειγμα

Οι πρωταρχικές ρίζες του 17 είναι φ (16) = $16 \cdot \frac{1}{2}$ =8.

Είδαμε ότι το 3 είναι πρωταρχική ρίζα του 17.

Οι 8 ακέραιοι μικρότεροι του 16 και πρώτοι προς τον 16 είναι οι 1,3,5,7,9,11,13,15 οπότε οι 8 πρωταρχικές ρίζες του 17 είναι $3^1 = 3,\ 3^3 = 10,\ 3^5 = 5,\ 3^7 = 11,\ 3^9 = 14,\ 3^{11} = 7,\ 3^{13} = 12,\ 3^{15} = 6 \bmod 17.$

Παράδειγμα Υπολογίστε όλους τους φυσικούς που έχουν ακριβώς 1 πρωτ. ρίζα.

φ (φ *(m))* $= 1$ συνεπάγεται $\begin{cases} \varepsilon ί \tau \varepsilon\ \varphi(m) = 1 \Rightarrow m = 1 \\ \varepsilon ί \tau \varepsilon\ \varphi(m) = 2 \Rightarrow m = 2, 3, 4, 6. \end{cases}$

Θεώρημα Αν q πρωταρχική ρίζα του p τα QR του p δίνονται από την παράσταση q^{2k} και τα QNR από την q^{2k-1} $0 \le k \le \frac{p-1}{2}$.

Απόδειξη: Αν q πρωτ. ρίζα modp με ΜΚΔ(q,p)=1 έχουμε:

$\left(q^{2k}\right)^{\frac{p-1}{2}} = q^{(p-1)k} = q^{\varphi(p)k} = 1 \bmod p$ από Fermat. Άρα

$q^{2k} \in QR \bmod p$. Επίσης $\left(q^{2k-1}\right)^{\frac{p-1}{2}} = q^{(p-1)k}\left(q^{\frac{p-1}{2}}\right)^{-1} = -1 \bmod p$

[διότι $\frac{p-1}{2} < p-1 = \varphi(p)$]. Άρα $q^{2k-1} \in QNR$.

Αντίστροφα: Αν $a \in QR \bmod p$ τότε $a = \left(q^k\right)^2 = q^{2k}$.

Αν $a \in QNR \bmod p$ τότε $a = \left(q^2\right)^k q = q^{2k+1}$, $0 \le k \le \frac{p-1}{2}$ ήτοι για $0 \le k \le \frac{p-1}{2}$

$q^k \neq 1$ άρα ο q είναι πρωτ. ρίζα.

Παράδειγμα

Τα QR του 17 είναι λοιπόν
$3^0 = 1, 3^2 = 9, 3^4 = 13, 3^6 = 15, 3^8 = 16, 3^{10} = 8, 3^{12} = 4, 3^{14} = 2, 3^{16}. = 1$

Θεώρημα Μία αναγκαία συνθήκη

για να επιλύεται η $x^m = a \bmod p$ με d=ΜΚΔ(m,p-1) είναι $a^{\frac{p-1}{d}} = 1 \bmod p$.

Απόδειξη: Έστω ΜΚΔ(a,b)=1 και b λύση της $x^m = a \bmod p$. Από το θεώρημα του Fermat $a^{\frac{p-1}{d}} = a^{\frac{(p-1)m}{md}} = b^{(p-1)\frac{m}{d}} = \left(b^{(p-1)}\right)^{\frac{m}{d}} = 1 \bmod p$.

Παράδειγμα

i) Η $x^7 = 15 \bmod 29$ δεν επιλύεται:

Έχω m = 7, α = 15, $p = 29$, d = ΜΚΔ(7,28) = 7.

$15^4 \neq 1 \bmod 29$ πράγματι 15^4 = 50.625 = 10mod29.

ii) Για την $x^{16} = 8 \bmod 73$ είναι

m = 16, α = 8, p = 73, d = ΜΚΔ(16,72) = 8

και $8^{\frac{72}{8}} = 8^9 = 8^4 \cdot 8^4 \cdot 8 = 8 \cdot 8 \cdot 8 = 512 = 1 \bmod 73$ άρα επιλύεται.

Βρίσκω μία πρωτ. ρίζα του 73.

Επίλυση: $5^6 = 3 \bmod 73, 5^{24} = 3^4 = 8 \bmod 73$

$5^{72} = \left(5^{24}\right)^3 = 8^3 = 1 \bmod 73$ άρα q=5.

Η εξίσωση 5^s =8 mod73 έχει λύση $s = 24$. Η ρίζα είναι λοιπόν x=5^6= 3mod73.

Επίλυση: Πράγματι $3^{16} \bmod 73 = \left(3^4\right)^4 = 81^4 = 8^4 = 4096 = 8 \bmod 73.$

ΚΕΦΑΛΑΙΟ 2
ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΩΤΩΝ

2.0 Το κόσκινο του Ερατοσθένη

Κόσκινο στη Θεωρία Αριθμών είναι μια μέθοδος ή διαδικασία κατά την οποία βρίσκεις αριθμούς με συγκεκριμένες ιδιότητες, διαπερνώντας όλους τους φυσικούς αριθμούς μέχρι ένα άνω όριο. Όσοι δεν ικανοποιούν αυτή την ιδιότητα διαγράφονται. Στο τέλος της διαδικασίας θα έχουν μείνει μόνο οι φυσικοί με την επιθυμητή ιδιότητα.
Το κόσκινο του Ερατοσθένη είναι μια μέθοδος εύρεσης όλων των πρώτων μικρότερων ή ίσων ενός συγκεκριμένου αριθμού x. Η μέθοδος είναι η ακόλουθη: Για δοθέν $x > 0$ καταγράφουμε όλους τους πρώτους που είναι $\leq x$. Ξεκινώντας με το 2, που είναι πρώτος, διαγράφουμε όλα τα πολλαπλάσια του 2 στη λίστα. Ο επόμενος μη διεγραμμένος αριθμός στη λίστα, δηλαδή το 3, είναι πρώτος.

Διαγράφουμε όλα τα πολλαπλάσια του 3. Ο επόμενος μη διεγραμμένος αριθμός στη λίστα, δηλαδή το 5, είναι πρώτος. Συνεχίζουμε με τον ίδιο τρόπο. Όπως εξηγήσαμε προηγουμένως η διαγραφή σταματά όταν φτάσουμε σε αριθμούς $> \sqrt{x}$. Όσοι αριθμοί δεν έχουν διαγραφεί είναι πρώτοι.

Παράδειγμα
Ποιοι είναι οι πρώτοι μέχρι το 100;

Θα εφαρμόσουμε το Κόσκινο του Ερατοσθένη για αριθμούς ≤ 100. Ξεκινώντας κάθε γύρο διαγραφών θα συνεχίζουμε τη διαδικασία όσο οι αριθμοί είναι $\leq \sqrt{100} = 10$.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	60
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Έτσι προκύπτει η λίστα

$$\{2, 3, 5, 7, \ldots, 83, 89, 97\}$$

που αποτελείται από τους 25 πρώτους που είναι μικρότεροι του 100.

2.1 Το Θεώρημα του Fermat

Το «μικρό» θεώρημα του Fermat λέει ότι αν ο p πρώτος και $1 \leq \alpha < p$ τότε $\alpha^{p-1} \bmod p = 1$.

Το θεώρημα αυτό δίνει ένα (αρνητικό) κριτήριο για την πιστοποίηση πρώτων. Ας πάρουμε α=2 και ας υπολογίσουμε το $2^{n-1} \bmod n$ (η πολυπλοκότητα της διαδικασίας είναι $O\left((\log n)^3\right)$). Έχουμε:

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$2^{n-1} \bmod n$	1	0	1	2	1	0	4	2	1	8	1	2	4	0	1

που είναι αποδοτικό κριτήριο για n ≤ 17. Οι πρώτοι δίνουν 1 ενώ οι σύνθετοι αποτέλεσμα ≠ 1. Από το θεώρημα του Fermat αν 2^{n-1} modn ≠ 1 έχουμε το συμπέρασμα ότι ο n δεν είναι πρώτος. Ονομάζουμε τον 2 μάρτυρα του Fermat για το n (ή αναλυτικότερα μάρτυρας ότι ο n είναι σύνθετος). Προφανώς τίποτα δεν είναι ιδιαίτερο για τον αριθμό 2 και μπορούμε εύκολα να γενικεύσουμε:

Ορισμός 2.1 (Κουκουβίνος - Παπαϊωάννου, 2007: 78)**:** Ο α, 1 ≤ α < n, ονομάζεται **F-μάρτυρας** για το n αν 2^{n-1} modn ≠ 1.

Άρα αν ο n έχει έναν F-μάρτυρα τότε ο n είναι σύνθετος. Δυστυχώς όμως η ύπαρξη του F-μάρτυρα δεν δίδει πληροφορία για το πιο σύνθετο πρόβλημα της πιθανής παραγοντοποίησης του n.

Είναι σχετικά εύκολο να δούμε ότι ο 2 είναι F-μάρτυρας για όλους τους σύνθετους αριθμούς n ≤ 340. Όμως για τον σύνθετο αριθμό 341 = 11 · 31 έχουμε $2^{340} \bmod 341 = 1$.

Πράγματι $2^{340} = (2^{10})^{34} = 1^{34} = 1 \bmod 341$ διότι 2^{10} = 1024 = 3 · 341 + 1 = 1mod341.

Ονομάζουμε τον 2 Fermat-ψεύτη (από την άποψη ότι δεν ικανοποιεί το αντίστροφο του θεωρήματος του Fermat).

Γενικεύοντας έχουμε τον ορισμό:

Ορισμός Για έναν (μονό) σύνθετο αριθμό n ένα στοιχείο $1 \le \alpha \le n - 1$ είναι F-ψεύτης αν $\alpha^{n-1} \bmod n = 1$.

Τετριμμένα έχουμε ότι οι 1 και n - 1 είναι F - ψεύτες για κάθε n μονό σύνθετο, αφού $1^{n-1} \bmod n = 1$ και $(n-1)^{n-1} \bmod n = (-1)^{n-1} \bmod n = 1$ (αφού ο n - 1 είναι ζυγός). Παρατηρούμε ότι το γεγονός ότι ο 2 είναι F-ψεύτης mod341, δεν δίνει παραπάνω πληροφορία. Πράγματι 3^{340} mod341 = 56 άρα ο 3 είναι F-μάρτυρας του 341.

Το «αντίστροφο» του μικρού θεωρήματος του Fermat δεν ισχύει όπως είδαμε (οι Κινέζοι πίστευαν λαθεμένα ότι ισχύει) [πχ. ο 2^{340} mod341 = 1 αλλά ο 341 δεν είναι πρώτος], αλλά μπορούμε να περισώσουμε κάτι.

Λήμμα 2.3 a) Αν 1 ≤ a < n ικανοποιεί την $a^r \bmod n = 1$ (για r ≥ 1) τότε $a \in \mathbb{Z}_n^*$.

b) Αν $a^{n-1} \bmod n = 1$ για κάθε a $1 \le a \le n$ τότε ο n είναι πρώτος.

(Παρατηρούμε ότι το σημαντικό κομμάτι του λήμματος είναι το b).

Απόδειξη: a) $a^r \bmod n = 1$ για κάποιο r ≥ 1 => $a \cdot a^{r-1} \bmod n = 1 \Rightarrow a \in \mathbb{Z}_n^*$.

b) Έστω $a^{n-1} \bmod n = 1 \forall a \in [1, n]$ άρα (από το a) $\square_n^* = \{1, \ldots n-1\}$ άρα ο n πρώτος.

Το β μέρος του λήμματος λέει επίσης ότι υπάρχει πάντα ένας F-μάρτυρας για τον σύνθετο μονό n. Πράγματι τα n – 1 – φ(n) στοιχεία με $\{a \mid 1 \le a < n \; \kappa\alpha\iota \; (a,n) > 1\}$ δεν μπορούν όλα να ικανοποιούν την σχέση $a^{n-1} \bmod n = 1$. Όμως για πολλούς μονούς σύνθετους το σύνολο αυτό έχει πολύ λίγα στοιχεία.

Παράδειγμα Έστω n = 91 = 7 · 13. Έχουμε: 18 πολλαπλάσια του 7 και 13,

36 F-μάρτυρες και

36 F-ψεύτες στο {1,2, ...,90}.

πολ7	7,14,21,28,35,42,49,56,63,70,77,84
πολ7	13,26,39,52,65,78
F-μάρτυρες στο $\mathbb{Z}_{91}^*$	2,5,6,8,11,15,18,19,20,24,31,32,33,34,41,44,45,46,47,50,54, 57,58,59,60,67,71,72,73,76,80,83,85,86,89

F-ψεύτες	1,6,4,9,10,12,16,17,22,23,25,27,29,30,36,38,40,43,48,51,53,55, 61,62,64,66,68,69,74,75,79,81,82,87,88,90

Παρατηρούμε ότι και τα πολ7, πολ13 είναι F-μάρτυρες [διότι $(a,n)>1$]. Πράγματι αν πάρω ένα πολλαπλάσιο του 7 (ή του 13) πχ. το 14 έχω: $14^{90} \bmod 91 = 2^{90} \cdot 7^{90} \bmod 91$ $= 6477=14 \neq 1 \bmod 91$ άρα το 14 είναι F-μάρτυρας. Για τους ψεύτες όμως έχουμε 3^{90} $= 1 \bmod 91$ από το θεώρημα του Fermat.

Αυτό μας οδηγεί στην πρώτη προσπάθεια πιθανοτικής πιστοποιήσης πρώτου.

Αλγόριθμος 1 (Fermat Test)

Είσοδος: Μονός φυσικός $n \geq 3$

Μέθοδος: 1. Επιλέγω τυχαία $a \in \{2,...,n-2\}$

2. αν $a^{n-1} \bmod n = 1$

3. τότε επιστροφή 1

4. αλλιώς επιστροφή 0

Η χρονική διάρκεια έχει ως εξής:

Η γρήγορη εκθετοποίηση (fast exponentiation) $a^{n-1} \bmod n$ έχει $O(\log \eta)$ αριθμητικές πράξεις και O $[(\log n)^3]$ πράξεις bit.

Αν ο αλγόριθμος δώσει 1 έχει βρει έναν F-μάρτυρα α για τον n άρα ο n είναι σύνθετος. Για n = 91 το κακό αποτέλεσμα 0 λαμβάνεται αν η τυχαία επιλογή μας είναι ένας από τους 34 F-ψεύτες (εξαιρούμε τις τετριμμένες τιμές 1 και 90) που δίνει πιθανότητα $\frac{34}{88} = \frac{17}{44}$.

Με λίγη θεωρία ομάδων παρατηρούμε ότι για πολλούς σύνθετους n υπάρχει αφθονία F-μαρτύρων οπότε το απλό αυτό κριτήριο πετυχαίνει με σταθερή πιθανότητα.

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

Απόδειξη: Το σύνολο $L_n^F = \{a \mid 1 \leq a < n \ \mu\varepsilon \ a^{n-1} \bmod n = 1\}$ των F-ψευτών για το n είναι προφανώς υποσύνολο του Z^*_n. Θα δείξουμε ότι είναι και υποομάδα της Z_n^*.

Αφού η Z_n^* είναι πεπερασμένη ομάδα (με $\left|Z_n^*\right| = \varphi(n)$) αρκεί να δείξουμε ότι:

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

2. Η L_n^F είναι κλειστή ως προς την πράξη πολλαπλασιασμός modn (η πράξη της $\mathbb{Z}_n^*$) 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 Z_n^* από το Λήμμα 2.1 έχει τουλάχιστον ένα στοιχείο, το L_n^F είναι γνήσια υποομάδα του Z_n^*. Από το θεώρημα του Lagrange λοιπόν η τάξη του θα είναι γνήσιος διαιρέτης $\varphi(n)$, όπου $\varphi(n) < n-1$ (διότι ο n σύνθετος), άρα $L_n^F \leq \frac{n-2}{2}$.

Άρα η πιθανότητα του μια τυχαία επιλογή από το $\{2,...n-2\}$ ανήκει στο $L_n^F - \{1, n-1\}$ είναι το πολύ $\frac{\frac{n-2}{2} - 2}{n-3} = \frac{n-6}{2(n-3)} < \frac{1}{2}.$

Βεβαίως ένας αλγόριθμος που δίνει πιθανότητα λάθους < $\frac{1}{2}$ δεν είναι έμπιστος.

Καλλίτερα αποτελέσματα όμως θα είχαμε από επαναλήψεις του τεστ του Fermat ήτοι:

Αλγόριθμος 2 (Iterated Fermat Test)

(Επαναληπτικό κριτήριο Fermat)

Είσοδος: Μονός ακέραιος $n \geq 3$, φυσικός $l \geq 1$

Διαδικασία: 1. Επαναλαμβάνω *l* φορές

2. α τυχαίο στοιχείο του $\{2,...n-2\}$

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

4. επιστροφή 0

Παρατηρούμε ότι αν η έξοδος είναι 1 ο αλγόριθμος έχει έναν F-μάρτυρα άρα ο n σύνθετος.

Αν ο n είναι σύνθετος και ισχύει το προηγούμενο θεώρημα (δηλαδή υπάρχει τουλάχιστον ένας F-μάρτυρας α με (α, n) = 1) η πιθανότητα να επιλέξουμε F-ψεύτη μετά από l δοκιμές γίνεται μικρότερη από $\left(\frac{1}{2}\right)^l$. Άρα για μεγάλα l η πιθανότητά λάθους γίνεται όσο θέλουμε μικρή.

Όμως υπάρχουν κάποιοι σπάνιοι μεν άπειροι δε σύνθετοι αριθμοί που δεν ικανοποιούν το τεστ του Fermat διότι όλα τα στοιχεία του Z_n^* είναι F-ψεύτες.

Ορισμός Ένας μονός σύνθετος αριθμός n λέγεται αριθμός Carmichael αν $a^{n-1} \bmod n = 1 \forall a \in Z_n^*$. Ο μικρότερος αριθμός Carmichael είναι ο $561 = 3 \cdot 11 \cdot 17$.

Το 1994 απεδείχθη ότι υπάρχουν άπειροι αριθμοί Carmichael. [Alford-Granville-Pomerance] «ομοιόμορφα» μάλιστα κατανεμημένοι.

Αν ένας αριθμός Carmichael n υποστεί το τεστ του Fermat η πιθανότητα να πάρουμε την λάθος απάντηση 0 είναι $\frac{\varphi(n)-2}{n-3} > \frac{\varphi(n)}{n} = \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right)$

που είναι περίπου 1 αν το n έχει λίγους μεγάλους πρώτους παράγοντες.

Πχ. ο n = 651.693.055.693.681 = 72.931 · 87.517 · 102.103 έχουμε $\frac{\varphi(n)}{n} > 0.99996$.

Άρα χρειαζόμαστε καλλίτερα τεστ από το τέστ του Fermat.

Πρώτα όμως περιγράφουμε την βασική ιδιότητα των αριθμών Carmichael.

Θεώρημα Αν ο n είναι αριθμός Carmichael, τότε ο n είναι γινόμενο τουλάχιστον τριών διαφορετικών πρώτων παραγόντων.

Θεώρημα(Korselt) : Ένας περιττός σύνθετος ακέραιος n≥ 3 είναι αριθμός Carmichael αν και μόνο αν είναι ελεύθερος τετραγώνου (squarefree δηλαδή δεν διαιρείται από τετράγωνο ενός πρώτου) και
κάθε πρώτος διαιρέτης p του n είναι τέτοιος ώστε ο $p-1 \mid n-1$.

Κατασκευή (J. Chernick 1939): αν t ακέραιος τέτοιος ώστε οι 6t+1, 12t+1, 18t+1 να είναι πρώτοι αριθμοί, τότε ο ακέραιος n όπου $n=(6t+1)(12t+1)(18t+1)$ από το παραπάνω θεώρημα είναι αριθμός Carmichael.
Για t = 1 έχω 1729=7·13·19 που είναι αριθμός Carmichael.
Ο Richard Pinch του πανεπιστημίου του Cambridge υπολόγισε τους 105.212 αριθμούς Carmichael τους μικρότερους του 10^{15}.

2.3 Το Κριτήριο Miller Rabin και Solovay Strassen

Ορισμός (Κουκουβίνος - Παπαϊωάννου, 2007: 86)**:** Έστω $1\leq < a \quad n$. Ο α ονομάζεται τετραγωνική ρίζα της μονάδας modn αν $a^2 \bmod n = 1$.
Παρατηρούμε ότι ο 1 και ο $n-1$ είναι πάντα τετραγωνικές ρίζες της μονάδας $\bmod n$. Πράγματι $1^2 \bmod n = 1, \left(n-1\right)^2 = \left(-1\right)^2 = 1 \bmod n$ αυτές είναι οι τετριμμένες ρίζες της μονάδας. Αν ο n είναι πρώτος δεν υπάρχουν άλλες ρίζες της μονάδας modn.

Λήμμα 2.9 (Κουκουβίνος - Παπαϊωάννου, 2007: 86)**:** Αν p πρώτος και $1 \le a < p$ με $a^2 \bmod p = 1$ τότε α = 1 ή a=p-1.

Απόδειξη: Έχουμε $a^2 - 1 \bmod p = \left(a+1\right)\left(a-1\right) \bmod p = 0$ άρα $p \mid \left(a+1\right)\left(a-1\right)$.
Αφού ο p πρώτος

$p \mid \left(a+1\right) \Rightarrow a+1 = kp \;\; a = -1 \bmod p = p-1 \bmod p$

$ή\; p \mid \left(a-1\right) \Rightarrow a-1 = kp \Rightarrow a = 1 \bmod p$.

Αν λοιπόν βρούμε μη τετριμμένες ρίζες της μονάδας modn τότε ο n είναι σίγουρα σύνθετος.

Παράδειγμα Οι τετραγωνικές ρίζες του 1mod91 είναι 1, 27, 64 και 90.

Γενικότερα από το ΚΘΥ αν $n = p_1 ... p_r$ για διακεκριμένους μονούς πρώτους $p_1, ..., p_r$ τότε υπάρχουν ακριβώς 2^r ρίζες της μονάδας modn, συγκεκριμένα οι αριθμοί $0 \le a < n$ που ικανοποιούν $a \bmod p_j \in \{1, p_j - 1\}$ για $1 \le j \le r$.

Πρόταση Έστω ο πρώτος p = 3mod4 και ο ακέραιος y. Έστω $x = y^{\frac{p-1}{4}} \bmod p$.

1) Αν ο y έχει τετραγωνική ρίζα mod p τότε οι τετριμμένες ρίζες του y modp είναι $\pm x$.
2) Αν ο y δεν έχει τετριμμένες ρίζες modp τότε ο –y έχει και οι τετριμμένες ρίζες του -y modp είναι $\pm x$.

Απόδειξη: Υποθέτω $y \neq 0$, διαφορετικά έχουμε τετριμμένη περίπτωση. Από το θεώρημα του Fermat $y^{p-1} = 1 \bmod p$. Άρα $x^4 = y^{p-1} = y^2 \cdot y^{p-1} = y^2 \bmod p$ ήτοι $\left(x^2 + y\right)\left(x^2 - y\right) = 0 \bmod p$ άρα $x^2 = \pm y \bmod p$. Άρα είτε το y είτε το $-y$ είναι τετράγωνα $\bmod p$.

Έστω y και $-y$ τετράγωνα $\bmod p$ ήτοι $y = a^2, -y = b^2$ τότε $-1 = \left(\frac{a}{b}\right)^2 \bmod p$ αν διαιρέσουμε κατά μέλη, ήτοι το -1 είναι τετράγωνο $\bmod p$. Αλλά αφού $p = 3 \bmod 4$ τούτο είναι αδύνατο. Πράγματι αν $p = 3 \bmod 4$ η εξίσωση $x^2 = -1 \bmod p$ δεν έχει λύσεις διότι αν είχε, ήτοι αν υπήρχε τέτοιο x, τότε

$\left(x^2\right)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \bmod p \Rightarrow$

$x^{p-1} = -1 \bmod p$, αλλά $x^{p-1} = 1 \bmod p$ από το θεώρημα του Fermat.

Από, $p = 3 \bmod 4$, έχω $p - 1 = 2 \bmod 4, \frac{p-1}{2}$ μονός και $(-1)^{\frac{p-1}{2}} = -1$

Άρα ακριβώς ένα από τα y και –y έχει τετραγωνική ρίζα $\bmod p$. Αν το y έχει, τότε $y = x^2$ και οι δύο ρίζες του $y \bmod p$ είναι $\pm x$. Αν το $-y$ έχει, τότε $x^2 = -y$ και οι δύο ρίζες του $-y$ είναι $\pm x$.

Ορισμός 2.11 (Κουκουβίνος - Παπαϊωάννου, 2007: 91-92)**:** Έστω $n \ge 3$ μονός και γράφουμε $n - 1 = u \cdot 2^k$ με u μονό και $k \ge 1$. Ο αριθμός a, $1 \le a < n$ ονομάζεται **A-**

μάρτυρας για τον n αν $a^u \bmod n \neq 1$ και $a^{u\cdot 2^i} \bmod n \neq n-1$ για όλα τα i με $0 \leq i < k$. Αν ο n σύνθετος και ο α δεν είναι Α-μάρτυρας του n, τότε ο α λέγεται Α-ψεύτης .

Λήμμα Αν ο α Α-μάρτυρας του n
τότε ο n σύνθετος.
Το Λήμμα αυτό και η τυχαία επιλογή του α από το {2,…,n-2} ενισχύουν το τεστ του Fermat σ' ένα ισχυρότερο κριτήριο που ονομάζεται κριτήριο Miller-Rabin.

Υπολογιστικά ο αλγόριθμος Miller-Rabin απαιτεί χρόνο εκτέλεσης $O\left(\left(\log n\right)^3\right)$.

Κριτήριο 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. Επιλεγώ τυχαίο στοιχείο $a \in \{2,...n-2\}$

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

4. αν $b = 1$ ή $b = n-1$ επιστροφή 0

5. επανάληψη k-1 φορές

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

7. αν b=n-1 επιστροφή 0

8. αν b=1 τότε επιστροφή 1

9. επιστροφή 1

Θέλουμε να εξετάσουμε αν ένας αριθμός n με 200 ψηφία είναι πρώτος ή όχι. Αν προσπαθήσουμε με δοκιμαστικές διαιρέσεις με όλους τους πρώτους τους $\sqrt{n}$

(κόσκινο Ερατοσθένη) πρέπει να εξετάσουμε 40 1 0 ^{97} πρώτους τους μικρότερους του 10^{100} □ $\sqrt{n}$ (αριθμός μεγαλύτερος απ' όλα τα μόρια του σύμπαντος). Αν ο υπολογιστής εξετάζει 10^9 πρώτους ανά δευτερόλεπτο θα χρειαστώ περίπου 10^{81} χρόνια!!

Ένα πολύ βασικό κριτήριο συγγενές με τις τετραγωνικές ρίζες της μονάδας $\bmod n$ είναι το εξής:

Θεώρημα (Βασικό Κριτήριο Παραγοντοποίησης) Έστω ο φυσικός n και έστω ότι υπάρχουν φυσικοί x.y με $x^2 = y^2 \bmod n$ αλλά $x \neq \pm \bmod y \quad n$.

Τότε n είναι σύνθετός και ο d=ΜΚΔ(x- y, n) δίδει μη τετριμμένο παράγοντα του n.

Απόδειξη: Αν d = n τότε $x = \bmod y \quad n$ που δεν ισχύει εξ υποθέσεως.

Αν d=1 από το θεώρημα $a \mid bc$ και $(a,b)=1 \Rightarrow a \mid c$ έχουμε $n \mid x^2 - y^2 = (x-y)(x+y)$ και *d=1 ήτοι* $\Rightarrow n \mid x+y \Rightarrow x = -y \bmod n$ που δεν ισχύει εξ υποθέσεως. Αν $d \neq 1, n$ και ο d μη τετριμμένος παράγοντας του σύνθετου n.

Παράδειγμα 2.3 (Κουκουβίνος - Παπαϊωάννου, 2007: 94)**:** Είναι $12^2 = 2^2 \bmod 35$ με $12 \neq \pm 2 \bmod 35$. Άρα 35 σύνθετος και ΜΚΔ(12 - 2,35) = 5 μη τετριμμένος παράγοντας του 35.

2.4 Κριτήριο Miller-Rabin (αναλυτικά)

Έστω n > 1 ένας μονός φυσικός. Θέτουμε $n-1 = 2^k \cdot m$ με m μονό και $k \geq 1$. Επιλέγουμε τυχαίο ακέραιο a, 1 < α < n-1. Υπολογίζωτον $b_0 = a^m \bmod n$. Αν $b_0 = \pm 1$ σταματάμε και λέμε ότι ο n είναι πιθανά πρώτος. Αλλιώς υπολογίζουμε τον $b_1 = b_0^2 \bmod n$. Αν $b_1 = 1 \bmod n$ τότε ο n είναι σύνθετος και ο ΜΚΔ $(b_0 - 1, n)$ δίνει μη τετριμμένο παράγοντα του n.

Αν $b_1 = -1 \bmod n$ σταματάμε και λέμε ότι ο n είναι πιθανά πρώτος. Αλλιώς υπολογίζουμε το $b_2 = b_1^2 \bmod n$. Αν $b_2 = 1 \bmod n$ ο n σύνθετος, αν b_2 = -lmodn

σταματάμε λέγοντας ότι ο n είναι πιθανά πρώτος. Συνεχίζουμε έως ότου είτε σταματήσουμε είτε φθάσουμε στο b_{k-1}. Αν $b_{k-1} \neq -1 \bmod n$ τότε ο n είναι σύνθετος.

Παράδειγμα

Για n = 561 είναι n-1 = 560 = 16 · 35.

Άρα $2^k = 2^4 \left(k = 4\right)$ και m=35.

Έστω α = 2.

Τότε $b_0 = 2^{35} = 263 \bmod 561$.

$b_1 = 263^2 = 166 \bmod 561$.

$b_2 = 166^2 = 67 \bmod 561$.

$b_3 = 67^2 = 1 \bmod 561$.

Αφού $b_3 \neq -1 \bmod n$ *ο 561* σύνθετος με d =ΜΚΔ (66, 561)= 33 μητετριμμένο παράγοντα του 561. Υπενθύμιση: 561 = 3 · 11 · 17 .

(561= Αριθμός Carmicheal)

Αν n σύνθετος και $a^{n-1} = 1 \bmod n$ λέμε ότι ο n είναι ψευδοπρώτος για την βάση α . Αν επιπλέον οι α, n είναι τέτοιοι ώστε ο n να επιτυχαίνει το test Miller-Rabin, ο n είναι ισχυρός ψευδοπρώτος για την βάση α.

Ο 561 είναι ψευδοπρώτος για την βάση 2 αλλά δεν είναι ισχυρός ψευδοπρώτος για τη βάση 2 (το ορίσαμε πριν σαν Α-ψεύτη).

Για δοσμένη βάση οι ισχυροί ψευδοπρώτοι είναι πάρα πολύ λιγότεροι από τους ψευδοπρώτους.

Μέχρι το 10^{10} υπάρχουν 455.052.511 πρώτοι, υπάρχουν 14.884 ψευδοπρώτοι για την βάση 2 και 3.291 ισχυροί ψευδοπρώτοι για την βάση 2. Άρα ο υπολογισμός $2^{n-1} \bmod n$ (το κριτήριο του Fermat) θα αποτύχει να αναγνωρίσει έναν σύνθετο στην περιοχή αυτή με πιθανότητα $< \frac{1}{30.000}$ ενώ το κριτήριο του Miller Rabin με α = 2 αποτυγχάνει με πιθανότητα $< \frac{1}{1000.000}$. Ο πρώτος ισχυρός ψευδοπρώτος για τις βάσεις 2, 3, 5, 7 είναι ο 3.215.031.751 ενώ για όλες τις πρώτες βάσεις τις <200 είναι ένας ισχυρός ψευδοπρώτος με 337 ψηφία.

Ορισμός (Αν $\in a \quad Z \quad , m \geq 2 (\ , \ a \ m \ ) = 1$ λέμε ότι ο α είναι τετραγωνικό υπόλοιπο (quadratic residue *(QR))* modm αν $= a \quad x \quad ^2 \bmod m$ για $x \in Z$.
Αν (a,m)=1 και a $\notin$ QR, ο α λέγεται μη τετραγωνικό υπόλοιπο modm (QNR)

Θεώρημα (Κριτήριο του Euler)

Αν p *μονός πρώτος τότε το* QR *είναι* υποομάδα του Z^*_p τάξης $\frac{p-1}{2}$. Επίσης αν $a \in \square^*_p$ έχουμε $a^{\frac{p-1}{2}} = \begin{cases} 1, \alpha \nu \ \alpha \in QR \\ -1 \ \alpha \nu \ \alpha \notin QR \end{cases}$.

Απόδειξη: Αφού ο p πρώτος η ομάδα $\square^*_p$ είναι κυκλική. Έστω ο γεννήτορας g (που είναι και πρωταρχική ρίζα) τότε $Z^*_p = \{1, g, g^2, ..., g^{p-2}\}$. Έχουμε $g^{p-1} = 1$ (αφού είναι πρωταρχική ρίζα) και $(g)^{\frac{p-1}{2}} \neq 1$ ένα στοιχείο του οποίου το τετράγωνο ισούται με 1. Αλλά τότε $(g)^{\frac{p-1}{2}} = -1$ αφού το $1 \in \square^*_p$ δεν έχει μη τετριμμένες τετραγωνικές ρίζες (p πρώτος). Τα τετράγωνα στην πολλαπλασιαστική αυτή ομάδα είναι τα στοιχεία g^{2i} 0≤ i <p - 1 ήτοι (p-1)/2 το πλήθος στοιχεία.

[Παρατηρούμε ότι αν $\frac{1}{2}(p-1) \leq i < p-1$ τότε $\left(g^i\right)^2 = g^{2j}$ όπου $j = \left(i - \frac{(p-1)}{2}\right)$].

Ένα στοιχείο g^{2i} ικανοποιεί την $\left(g^{2i}\right)^{\frac{p-1}{2}} = g^{i(p-1)} = \left(g^{p-1}\right)^i = 1$. ενώ ένα στοιχείο g^{2i+1} την $\left(g^{2i+1}\right)^{\frac{p-1}{2}} = g^{i(p-1)} \cdot g^{\frac{p-1}{2}} = -1 \cdot 1$.

Η διαδικασία αυτή μας κάνει εύκολο τον υπολογισμό τετραγωνικών ριζών για τους μισούς περίπου πρώτους p . Αν $p \geq 3$ είναι πρώτος και p + 1 = πολ4
(ήτοι p = 3 m o d 4)

θεωρούμε τον γεννήτορα της g Z^*_p και $a = g^{2i}$ ένα τυχαίο QR στη Z^*_p.

Τότε $x = a^{\frac{p+1}{4}} = g^{i\frac{(p-1)}{2}+i} = \left(g^{\frac{p-1}{2}}\right)^i \cdot g^i = (-1)^i g^i$, αλλά υψώνοντας στο τετράγωνο $x^2 = (-1)^{2i} g^{2i} = 1 \cdot a = a$ ήτοι το x είναι τετραγωνική ρίζα (η άλλη είναι η p – x) δηλαδή για να βρω το x από το α δεν χρειάζεται ο γεννήτορας g.

Κριτήριο των Solovay-Strassen

Είσοδος: Μονός ακέραιος $n \geq 3$

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

2. if $a^{\frac{(n-1)}{2}} \cdot \left(\frac{a}{n}\right) \bmod n \neq 1$

3. then return 1

4. else return 0.

Στην γραμμή 2 ο υπολογισμός του συμβόλου Jacobi $\left(\frac{a}{n}\right)$ γίνεται από τον αλγόριθμο και η εκθετοποίηση $a^{\frac{n-1}{2}} \bmod n$ γίνεται με fast exponentiation,

Ο παραπάνω αλγόριθμος είναι $O\left((\log n)^3\right)$. Αν το n είναι πρώτος έχουμε σαν έξοδο το 0 αν ο n είναι σύνθετος η πιθανότητα να πάρω στην έξοδο 0 είναι μικρότερη της $1/2$.

ΚΕΦΑΛΑΙΟ 3
ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΑΚΕΡΑΙΩΝ

3.1 Μέθοδος των Διαδοχικών Διαιρέσεων

Ένα από τα πλέον δύσκολα προβλήματα της κλασσικής Θεωρίας Αριθμών είναι η παραγοντοποίηση μεγάλων ακεραίων. Η έλλειψη ενός πολυωνυμικού αλγόριθμου για την επίλυση του ενέπνευσε την δημιουργία του κρυπτοσυστήματος RSA. Από την άλλη πλευρά, η στενή σύνδεση της ασφάλειας του RSA μ' αυτό το πρόβλημα συνετέλεσε στην αύξηση του ενδιαφέροντος και της ενασχόλησης μ' αυτό. Αν και αρκετοί αλγόριθμοι αναπτύχθηκαν την τελευταία εικοσαετία για την επίλυσή του, κανένας δεν πέτυχε να απειλήσει σοβαρά την ασφάλεια του RSA. Η αύξηση του μήκους των χρησιμοποιουμένων πρώτων και κάποιοι περιορισμοί στην επιλογή τους ήταν ικανά μέτρα για να παραμείνει το RSA ένα ασφαλές κρυπτοσύστημα.

Η πιο παλιά μέθοδος για την εύρεση της πρωτογενούς ανάλυσης ενός ακεραίου είναι η μέθοδος των διαδοχικών διαιρέσεων Σύμφωνα μ' αυτή, αν n είναι ένας σύνθετος θετικός ακέραιος, τότε τον διαιρούμε διαδοχικά με κάθε πρώτο $\leq \sqrt{n}$, μέχρι να βρούμε ένα πρώτο διαιρέτη του p. Τότε έχουμε $n = pn_1$, όπου n_1 ακέραιος. Επαναλαμβάνουμε την ίδια διαδικασία επί του n_1 μέχρι να βρούμε ένα πρώτο διαιρέτη του. Συνεχίζοντας μ' αυτό τον τρόπο, παίρνουμε την πρωτογενή ανάλυση του n σε πρώτους.

Παράδειγμα

Θα παραγοντοποιήσουμε τον ακέραιο
225277. Έχουμε $474 < \sqrt{225277} < 475$. Οπότε, αν ο 225277 είναι σύνθετος θα έχει ένα πρώτο διαιρέτη < 474. Δοκιμάζοντας κάθε πρώτο αρχίζοντας από τον 3, βρίσκουμε ότι ο 13 διαιρεί τον 225277 και έτσι προκύπτει $225277 = 13 \cdot 17329$. Έχουμε $131 < \sqrt{17329} < 132$. Ομοίως, βρίσκουμε οτι ο 13 διαιρεί τον 17329 και επομένως $225277 = 13^2 \cdot 1333$. Τέλος, παίρνουμε $1333 = 31 \cdot 43$. Συνεπώς, η ανάλυση του 225277 είναι $225277 = 13^2 \cdot 31 \cdot 43$.

Στην περίπτωση όπου ο ακέραιος n έχει έναν αρκετά μεγάλο πρώτο παράγοντα, τότε η μέθοδος αυτή δεν είναι αποτελεσματική. Ας σημειωθεί ότι οι ακέραιοι επί των

οποίων βασίζει την ασφάλεια του το RSA είναι γινόμενα δύο μεγάλων πρώτων και κατά συνέπεια η μέθοδος των διαδοχικών διαιρέσεων είναι τελείως ανεφάρμοστη για την παραγοντοποίηση τους.

Οι περισσότεροι αλγόριθμοι παραγοντοποίησης δίνουν έναν μη τετριμμένο παράγοντα του ακέραιου που επιθυμούμε να παραγοντοποιήσουμε. Δηλαδή, αν n είναι ένας σύνθετος θετικός ακέραιος, τότε παίρνουμε μία παραγοντοποίησή του της μορφής $n = n_1 n_2$, όπου n_1, n_2 είναι ακέραιοι με $1 < n_1 < n$ και $1 < n_2 < n$. Στη συνέχεια πρέπει να διαπιστώσουμε αν οι n_1, n_2 είναι πρώτοι ή σύνθετοι εφαρμόζοντας κάποια από τις μεθόδους που είδαμε στο προηγούμενο κεφάλαιο. Αν κάποιος από αυτούς είναι σύνθετος, τότε εφαρμόζουμε σ' αυτόν τον αλγόριθμο παραγοντοποίησης κ.ο.κ. μέχρι να βρούμε την ανάλυση του n.

Οι πλέον αποτελεσματικοί αλγόριθμοι παραγοντοποίησης σήμερα είναι το κόσκινο των σωμάτων αλγεβρικών αριθμών και η μέθοδος των ελλειπτικών καμπυλών. Σ' αυτό το κεφάλαιο, καθώς η ανάπτυξη των απαραίτητων μαθηματικών εργαλείων για την παρουσίαση τους εκφεύγει της παρούσας εργασίας, θα περιοριστούμε στη παρουσίαση μερικών από τους πιο κλασσικούς αλγόριθμους οι οποίοι υπήρξαν πρόδρομοι τους.

3.2 Μέθοδος του Fermat και του Euler

Η πρώτη μέθοδος παραγοντοποίησης με την οποία θ' ασχοληθούμε είναι αρκετά παλιά και ανάγεται στον F e r m a t . Η ιδέα της μεθόδου βασίζεται στην παρακάτω πρόταση.

Πρόταση (Πουλάκης, 2006: 116-117)**:** *Ας είναι n θετικός περιττός ακέραιος. Τότε υπάρχει μία αμφίεση (αμφιμονοσήμαντη αντιστοιχία) μεταξύ των παραγοντοποιήσεων του n της μορφής* $n = ab$, *όπου* a, b *ακέραιοι* $a \geq b > 0$ *και των παραστάσεων του n της μορφής* $t^2 - s^2$, *όπου* s *και* t *είναι ακέραιοι* ≥ 0. *Η αμφίεση αυτή δίνεται από τις εξισώσεις:*

$$t = \frac{a+b}{2}, \quad s = \frac{a-b}{2}$$

$$\alpha = t + s, \quad b = t - s$$

Απόδειξη: ας είναι n = ab, όπου α, b ακέραιοι με α ≥ b >0. Τότε

$$\left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 = ab$$

Έτσι, θέτοντας t = (a + b)/2 και s = (a - b)/2, έχουμε $n = t^2 - s^2$. Αντιστρόφως, αν $n = t^2 - s^2$, όπου s και t είναι ακέραιοι ≥ 0, τότε

n = (t + s)(t - s).

Συνεπώς, οι αντιστοιχίες

(a, b) → ((a + b)/ 2, (a + b)/ 2)

και

$$(s, t) \rightarrow (t + s, t - s)$$

δίνουν μία αμφίεση μεταξύ των δύο τρόπων γραφής του n.

Για να παραγοντοποιήσουμε λοιπόν τον n παίρνουμε $t = \left[\sqrt{n}\right] + 1$, $\left[\sqrt{n}\right] + 2$ ... και υπολογίζουμε τις τιμές $t^2 - n$ μέχρι να βρούμε ακέραιο s τέτοιο, ώστε $t^2 - n = s^2$. Οπότε, θα έχουμε n = (t + s)(t - s). Αν n = ab και οι ακέραιοι α και b βρίσκονται πολύ κοντά, τότε ο s = (α - b)/2 είναι πολύ μικρός και επομένους ο t = (α + b)/2 λίγο μεγαλύτερος από τον $\left[\sqrt{n}\right]$. Σ' αυτή την περίπτωση, η μέθοδος θα μας δώσει την παραγοντοποίηση του n μετά από ένα μικρό πλήθος δοκιμών για τον t, όπως στο παρακάτω παράδειγμα.

Παράδειγμα (Πουλάκης, 2006: 117-118)**:** Θα παραγοντοποιήσουμε τον ακέραιο 670661. Έχουμε $\sqrt{670661} = 818$. Βρίσκουμε $819^2 - 670661 = 10^2$. Οπότε 670661 = 829 · 809.

Αν για κάθε παραγοντοποίηση n = ab του n, οι ακέραιοι α και b βρίσκονται αρκετά μακριά, τότε·θα χρειαστεί ένα μεγάλο πλήθος δοκιμών για τον t. Για να επιταχυνθεί η διαδικασία σ' αυτή την περίπτωση, μπορούμε να χρησιμοποιήσουμε

την εξής γενίκευση της μεθόδου του Fermat. Επιλέγουμε ένα μικρό θετικό ακέραιο k και παίρνοντας διαδοχικά $t = \left[\sqrt{kn}\right] + 1$, $t = \left[\sqrt{kn}\right] + 2 \ldots$ υπολογίζουμε τις τιμές t^2 - kn μέχρι να βρούμε ακέραιο s τέτοιο, ώστε t^2 - kn = s^2. Τότε

$$(t + s)(t — s) = kn.$$

Καθώς οι t και s βρίσκονται αρκετά μακριά και ο k είναι μικρός, έχουμε $k < t - s < t + s < \eta$. Επομένως $1 < (t \pm s, n) < \eta$ και κατά συνέπεια οι ακέραιοι $(t \pm s, n)$ είναι γνήσιοι παράγοντες του n.

Γενικότερα, αν βρούμε ακεραίους t και s με

$$t^2 \equiv s^2 \pmod{n} \text{ και } t \equiv \pm s \pmod{n}$$

τότε οι μέγιστοι κοινοί διαιρέτες $(t \pm s, n)$ δίνουν μη τετριμμένους παράγοντες του n.

Παράδειγμα
Θα παραγοντοποιήσουμε τον ακέραιο
329345. Έχουμε $\left[\sqrt{3} \cdot 329345\right] = 993$. θεωρούμε τις τιμές t = 994, ... και παίρνουμε αμέσως 994^2 - 3 · 329345 = 1. Επομένως 3 · 329345 = 995 · 993. Κατόπιν υπολογίζουμε τον μέγιστο κοινό διαιρέτη (329345, 995) = 995. Οπότε 329345 = 331 · 995. Παρατηρούμε ότι με την κλασσική μέθοδο του Fermat θα χρειαστεί να πάρουμε πολύ περισσότερες από μία τιμές για τον t.

Παράδειγμα Για n = 931, k=31, διότι k^2= 961>931 και

$31^2 - 931 = 30$
$32^2 - 931 = 93$
$33^2 - 931 = 158$
$34^2 - 931 = 225 = 15^2 = y^2$.

Άρα y = 15, m = 3, x = k + m = 31 + 3 = 34 και (34 – 15)(34 + 15) = 19 · 49.
Όμως η διαδικασία αυτή στον αριθμό που ρώτησε ο Mersenne έχει m = 75.000.

Μέθοδος Euler

Το 1641 ο Frenicle ρώτησε τον Fermat αν μπορεί να παραγοντοποιήσει τον αριθμό n αν αυτός γράφεται σαν άθροισμα δύο τετραγώνων με δύο διαφορετικούς τρόπους. Δεν γνωρίζουμε τι απάντησε ο Fermat αλλά ο Euler το 1745 έδειξε ότι αν $n = a^2 + b^2 = c^2 + d^2$ τότε:

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

ήτοι ο n παραγοντοποιείται.

Η παράσταση προκύπτει αν κάνω τις πράξεις στο 2ο μέλος.

Παράδειγμα 3.6 (Κουκουβίνος - Παπαϊωάννου, 2007: 118)**:**

$2501 = 50^2 + 1^2 = 49^2 + 10^2 \Rightarrow a = 50, b = 1, c = 49, d = 10$

$$2501 = \frac{(1^2 + 9^2)(99^2 + 9^2)}{4 \cdot 9^2} = \frac{82 \cdot 9882}{4 \cdot 81} = \left(\frac{82}{2}\right)\left(\frac{9882}{81 \cdot 2}\right) = 41 \cdot 61.$$

Θεώρημα 3.2 (Κουκουβίνος - Παπαϊωάννου, 2007: 118)**:** Αν $N = a^2 + kb^2 = c^2 + kd^2$

τότε $N = \frac{\left(km^2 + n^2\right)\left(kr^2 + s^2\right)}{4}$, όπου

$a + c = kmr$
$a - c = ns$
$d + b = ms$
$d - b = nr.$

Απόδειξη: $a = \frac{kmr + ns}{2}$, $b = \frac{ms - nr}{2}$, $c = \frac{kmr - ns}{2}$, $d = \frac{ms + nr}{2}$.

$N = a^2 + kb^2 = \frac{k^2m^2r^2 + kn^2r^2 + n^2s^2 + km^2s^2}{4}$ και

$N = c^2 + kd^2 = \frac{k^2m^2r^2 + kn^2r^2 + km^2s^2 + n^2s^2}{4}$.

Αρα $2N = \dfrac{2\left(k^2m^2r^2 + kn^2r^2 + km^2s^2 + n^2s^2\right)}{4}$ και συνεπώς

$$N = \frac{k^2m^2r^2 + kn^2r^2 + km^2s^2 + n^2s^2}{4} = \frac{\left(km^2 + n^2\right)\left(kr^2 + s^2\right)}{4}.$$

Παράδειγμα

Θα παραγοντοποιήσουμε τον 34.889.

$$34.889 = \underbrace{157^2}_{a^2} + \underbrace{10}_{k} \cdot \underbrace{32^2}_{b^2} = \underbrace{143^2}_{c^2} + \underbrace{10}_{k} \cdot \underbrace{38^2}_{d^2}.$$

$$a + c = \overbrace{10}^{k} \cdot \overbrace{30}^{mr} \Rightarrow mr = 30, m = 10, r = 3$$
$$a - c = 14 = ns \qquad \Rightarrow s = 7.$$
$$d + b = 70 = ms$$
$$d - b = 6 = nr \qquad \Rightarrow n = 2$$

Άρα $34.889 = \dfrac{1004 \cdot 139}{4} = 251 \cdot 139.$

3.3 Ο αλγόριθμος p -1 του John Pollard (1974)

Υπάρχουν κάποιοι αλγόριθμοι παραγοντοποίησης που δουλεύουν ικανοποιητικά για σύνθετους αριθμούς n με κάποιες ιδιότητες. Οι αριθμοί αυτοί n πρέπει να αποφεύγονται για modula σε μεθόδους όπως το RSA ή το κρυπτοσύστημα Rabin. Μία τέτοια μέθοδος είναι η μέθοδος p -1 του Pollard που προτάθηκε το 1974.

Η μέθοδος δουλεύει όταν ο σύνθετος n έχει έναν πρώτο παράγοντα p τέτοιον ώστε ο p -1 να έχει μόνο μικρούς πρώτους παράγοντες. Τότε μπορούμε να υπολογίσουμε ένα πολλαπλάσιο του p -1,χωρίς προφανώς να γνωρίζουμε τον p -1 (άρα και τον p), σαν γινόμενο δυνάμεων μικρών πρώτων.

Παρατηρούμε ότι ο p -1 αλγόριθμος του Pollard όπως και ο αλγόριθμος των Pohling-Hellman στο διακριτό λογάριθμο, στηρίζεται στο προκαθορισμένο φράγμα Β δηλαδή ουσιαστικά στην βάση Β **μικρών** πρώτων αριθμών.

Ο αλγόριθμος λοιπόν έχει δύο εισόδους: Τον αριθμό n που θέλουμε να παραγοντοποιήσουμε (που έχει και την περαιτέρω ιδιότητα, αλλά που δεν την γνωρίζουμε πριν τον παραγοντοποιήσουμε) και το προκαθορισμένο φράγμα Β.

Ο αλγόριθμος p-1 του John Polland

1. Υπολογίζουμε το γινόμενο $k = \prod_{q \le B, q \text{ πρώτος}} q^{\left\lfloor \log_q B \right\rfloor}$ (το q παίρνει τιμές: πρώτοι μικρότεροι Β).

Πχ.: Για Β=19: $\kappa = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 232.792.560.$

Προσοχή $2^4 = 16 < 19$ άρα $\log_2 19 = 4,$

…… $3^2 = 9 < 19 \left(3^3 = 27 > 19\right)$ άρα $\log_3 19 = 2.$

Οι άλλοι πρώτοι δίνουν εκθέτη 1.

2. Επιλέγουμε έναν ακέραιο α με $1 < a < n$ και υπολογίζουμε ΜΚΔ(α,n) =δ.

Αρχίζω α=2, α=3 κοκ.

3. Αν $\delta > 1$ (που συνήθως δεν είναι διότι n μονός, α=2) τότε ο δ είναι μη τετριμμένος παράγοντας του n.

Αν δ=1 υπολογίζω τον $\delta = \text{ΜΚΔ}\left(\alpha^{\kappa} - 1, n\right).$

(βασικό βήμα του αλγ. όχι όμως πολύ πολύπλοκο)

4. Αν 1<δ<n ο δ είναι μη τετριμμένος παράγοντας του n. Αν δ=1 ή δ=n επιλέγουμε άλλο B και επαναλαμβάνουμε τη διαδικασία.

Αν λοιπόν ο p είναι πρώτος παράγοντας του n και κάθε δύναμη πρώτου που διαιρεί τον p-1 είναι $\le B$ τότε ο $(p-1)=2^a\cdot 3^b\cdot 5^y\cdot 7^\lambda...$ η ανάλυση του p-1 όπου κάθε παράγοντας είναι $< B$. Άρα ο k (που χει την ίδια μορφή με τον p-1 με μεγαλύτερους πιθανόν εκθέτες) θα είναι πολλαπλάσιο του p-1 ήτοι $p-1|k \Rightarrow k=l(p-1)$. Αλλά τότε για κάθε α με $1 < \alpha < n$ και $(\alpha, p) = 1$ έχω από το μικρό θεώρημα του $a^k=a^{l(p-1)}=(a^{p-1})^l=1 \bmod p \Rightarrow a^k-1=\pi o\lambda p$ ήτοι ο $p|a^k-1$. Αν λοιπόν και $\delta \ne n$ τότε $1 < \delta < n$ και ο δ είναι μη τετριμμένος παράγοντας του n, άρα ο αλγόριθμος δουλεύει.

Παράδειγμα

1) Να παραγοντοποιηθεί ο n = 1.241.143.

Ας πάρουμε B = 13.

Τότε $k=2^3\cdot 3^2\cdot 5\cdot 7\cdot 11\cdot 13$ $\text{ΜΚΔ}(2^\kappa-1,n)=547$ άρα ο n = 2269·547 που είναι αμφότεροι πρώτοι. Παρατηρούμε ότι p = 547, $(p-1)=546=2\cdot 3\cdot 7\cdot 13$ έχει μικρούς μόνο πρώτους άρα B = 13 είναι εφικτή τιμή.

2) Στο παράδειγμα για τον $k=232.792.560$ έχουμε για α = 2 $(2^{232.792.560}-1,1.127.041)=761$ άρα $1.127.041=761\cdot 1481$ που είναι αμφότεροι πρώτοι. Και εδώ $p-1=760=2^3\cdot 5\cdot 19$ άρα B = 19.

Πολυπλοκότητα: Αφού κάθε παράγοντας του k είναι μικρότερος της βάσης B, $k<B^b$ $\kappa\alpha\iota$ o k $\upsilon\pi o$λογίζεται σε χρόνο $O\left((B\log B)^2\right)$. Ο ΜΚΔ(α, n) υπολογίζεται σε χρόνο $O\left((\log n)^2\right)$ και ο $\text{ΜΚΔ}(a^\kappa-1,n)$ σε χρόνο 0 $O\left((1+\log k)\left((\log n)^2+\log n\right)\right)$. Έτσι ο χρόνος που απαιτείται για παραγοντοποίηση του n με τον p-1 αλγόριθμο είναι συνολικά $O\left(B^2(\log B)^2(\log n)^2\right)$. Για $B=O\left((\log n)^i\right)$ με i θετικό ακέραιο ο αλγόριθμος είναι πολυωνυμικού χρόνου σαν συνάρτηση του logn, όμως τέτοια επιλογή του B μειώνει αρκετά την πιθανότητα επιτυχίας. Από την άλλη αν αυξήσουμε δραστικά το μέγεθος της βάσης B (π.χ. στο $\sqrt{n}$), ο αλγόριθμος αποδεικνύεται επιτυχής, γίνεται όμως πάρα πολύ αργός.

0 αλγόριθμος του Lenstra για παραγοντοποίηση με ελλειπτικές καμπύλες δίνει μία γενίκευση αλλά και βελτίωση της διαδικασίας του Pollard. Χρησιμοποιεί τυχαίους αριθμούς πλησίον του p -1 και απαιτεί μόνο ένας από αυτούς να έχει μικρούς πρώτους παράγοντες. Η μέθοδος αυτή είναι πολύ πιο χρήσιμη σήμερα από την μέθοδο του Pollard.

3.5 Ο αλγόριθμος Pollard Rho

Έστω p ο μικρότερος πρώτος διαιρέτης του n, και x , x ′ ακέραιοι στο $\mathbb{Z}_n$ τέτοιοι ώστε x ≠x′ και x = x'mod$p$. Τότε $p \leq$ ΜΚΔ (x-x′, n) < n και έτσι υπολογίζοντας τον ΜΚΔ βρίσκουμε έναν μη τετριμμένο παράγοντα του n . Υποθέτουμε τώρα ότι θέλουμε να παραγοντοποιήσουμε τον n επιλέγοντας πρώτα ένα τυχαίο υποσύνολο X του Z_n και υπολογίζοντας έπειτα τους ΜΚΔ (x - x ′, n) για όλα τα x , x′ στο X , με x ≠x′ . H μέθοδος θα ήταν όμως επιτυχής μόνο στην περίπτωση που η απεικόνιση $x \to x \bmod p$ οδηγεί σε μία τουλάχιστον «σύγκρουση» για το $x \in X$. Η περίπτωση αυτή στηρίζεται στο *παράδοξο των γενεθλίων:* Αν $|X| \approx 1{,}17\sqrt{n}$ τότε υπάρχει 50% πιθανότητα να πετύχουμε σύγκρουση και επομένως να βρούμε έναν μη τετριμμένο παράγοντα του n.

Ορισμός Μία σύγκρουση (collision) της συνάρτησης f είναι ένα ζεύγος (x,x′) στο πεδίο ορισμού για το οποίο ισχύει x ≠x′ και f(x) = f(x').

Θεώρημα (Παράδοξο των γενεθλίων (b i r t h d a y p a r a d o x))

Σύμφωνα με το παράδοξο των γενεθλίων, σε μια τυχαία επιλογή 23 ανθρώπων, η πιθανότητα δύο από αυτούς να έχουν γενέθλια την ίδια μέρα είναι τουλάχιστον 0,5 (για την ακρίβεια 0,507).
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 ≠ x′) τέτοια ώστε f(x) = f(x').

Απόδειξη: Θεωρούμε την ομάδα των ακεραίων modn, δηλαδή το σύνολο $\mathbf{Z}_n = \{0,1,2,...,n-1\}$ με $|\mathbf{Z}_n| = n$. Θα υπολογίσουμε την πιθανότητα να μην επιλεχθούν ίσα στοιχεία (όχι συγκρούσεις) σε μία τυχαία επιλογή *k* στοιχείων από το $\mathbf{Z}_n$. Η πιθανότητα επιλογής ενός συγκεκριμένου στοιχείου είναι $\frac{1}{n}$. 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 είναι $\frac{n-2}{n} = 1 - \frac{2}{n}$ κ.ο.κ.

Ετσι η πιθανότητα επιλογής k στοιχείων χωρίς συγκρούσεις είναι

$\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\left(1-\frac{3}{n}\right)...\left(1-\frac{k-1}{n}\right) = \prod_{i=1}^{k-1}\left(1-\frac{i}{n}\right)$ όπως προκύπτει από την Πολλαπλασιαστική Αρχή.

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

Κατά συνέπεια αφού n πολύ μεγάλο έπεται ότι $1-\frac{1}{n} \approx e^{-1/n}$.

Μία 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 $p \approx 1 - e^{-k(k-1)/2n}$

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

Αγνοώντας τον όρο –k έχουμε την εκτίμηση $k \approx \sqrt{2n \ln\frac{1}{1-p}}$ και για την

πιθανότητα σύγκρουσης $p = 1/2$ θα είναι $k \approx 1{,}17\sqrt{n}$.

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

Στο παράδοξο των γενεθλίων n = 365 και η προσέγγιση μας δίνει $k \approx 1{,}17\sqrt{365} \approx 22{,}3$.

Παραγοντοποίηση μονού ακεραίου n

Θεωρούμε τη συνάρτηση $f(x) = x^2 + a$ όπου α μικρή σταθερά, α = 1

Έστω $x_i \in Z_n$ και $X \subseteq Z_n$ με

$$X = \{x_1, x_2, ..., x_m \mid x_j = f(x_{j-1}) \bmod n \; \forall j = 2, ..., m\}$$

Σκοπός είναι η εύρεση δύο διαφορετικών τιμών $x_i, x_j \in X$ τέτοιες ώστε $\text{ΜΚΔ}(x_j - x_i, n) > 1$. Κάθε φορά που υπολογίζουμε έναν καινούριο όρο x_j της ακολουθίας, μπορούμε να υπολογίζουμε τους $\text{ΜΚΔ}(x_j - x_i, n)$ για όλα τα i < j.

Αυτό όμως θα απαιτούσε $\binom{|X|}{2} = \binom{m}{2}$ υπολογισμούς, περισσότερους από $p/2$.

Ο αριθμός των υπολογισμών αυτών για εύρεση μη τετριμμένου παράγοντα του n μπορεί να μειωθεί και σ' αυτό ακριβώς έγκειται η μέθοδος Pollard Rho.

Έστω μία σύγκρουση $x_i \equiv x_j \pmod p$. Η f είναι πολυωνυμική συνάρτηση με ακέραιους συντελεστές οπότε $f(x_i) \equiv f(x_j) \pmod p$. Από την κατασκευή του υποσυνόλου X έχουμε ότι $x_j = f(x_{j-1}) \bmod n \; \forall j = 2, ..., m$. Τότε

$x_{i+1} \bmod p = (f(x_i) \bmod n) \bmod p = f(x_i) \bmod p$ αφού $p \mid n$

Ομοίως $x_{j+1} \bmod p = (f(x_j) \bmod n) \bmod p = f(x_j) \bmod p$.

Έτσι θα έχουμε $x_{i+1} \equiv x_{j+1} \pmod p$ και επαναλαμβάνοντας τη διαδικασία καταλήγουμε στα εξής σημαντικά αποτελέσματα:

Αν $x_i \equiv x_j \pmod p$ τότε $x_{i+\delta} \equiv x_{j+\delta} \pmod p, \forall \delta \geq 0.$ (1)

Θέτοντας $l = j - i$ τότε $x_{i'} \equiv x_{j'} \pmod p$ αν $j' > i' \geq i$ και $j' - i' \equiv 0 \bmod l.$ (2)

Αν $x_i \equiv x_j \pmod p$ τότε $x_{i'} \equiv x_{2i'} \pmod p$ για όλα τα i με $i' = 0 \bmod l$ και $i' \geq i$. ...(3)

Πολυπλοκότητα αλγορίθμου Pollard Rho

Αν $x_i \equiv x_j(modp)$ τότε μεταξύ των l ακεραίων i, …, j-1 θα υπάρχει κάποιο $i' \geq i$ πολλαπλάσιο του l = j-1 και από την σχέση 3 της προηγούμενης παραγράφου θα έχουμε ότι $x_{i'} \equiv x_{2i}(modp)$. Τότε ο αλγόριθμος θα εντοπίσει μια σύγκρουση και θα δώσει ένα μη τετριμμένο παράγοντα του n, τον p=ΜΚΔ$(x_{2i} - x_i, n)$.

Ο i' εντοπίζεται το πολύ σε j βήματα, άρα στη χειρότερη των περιπτώσεων ο αλγόριθμος απαιτεί j επαναλήψεις για να βρει μια σύγκρουση και επομένως να δώσει τον παράγοντα p που προαναφέρθηκε. Ο αναμενόμενος αριθμός επαναλήψεων μειώνεται στις $\sqrt{p}$ και επειδή $p < \sqrt{n}$, η αναμενόμενη πολυπλοκότητα προκύπτει $O\left(n^{1/4}\right)$.

Είναι πιθανό ο αλγόριθμος να μην εντοπίσει έναν μη τετριμμένο παράγοντα του n. Αυτό συμβαίνει μόνο στην περίπτωση που οι τιμές x και x' που εμφανίζουν την πρώτη σύγκρουση, ικανοποιούν στην ουσία τη σχέση $x \equiv x' modn$ αντί απλά της $x \equiv x' modp$. Η πιθανότητα γι αυτή την περίπτωση είναι περίπου p/n, αρκετά μικρή αν ο n είναι μεγάλος (γιατί $p < \sqrt{n}$). Αν ο αλγόριθμος αποτύχει με αυτό τον τρόπο τότε επαλαμβάνουμε επιλέγοντας διαφορετική αρχική τιμή ή διαφορετική συνάρτηση f.

Παράδειγμα

Έστω $n = 7171, f(x) = x^2 + 1, x_i = 1.$ $Ζητείται\ παραγοντοποίηση\ του\ n.$

$$\boldsymbol{Βήμα\ 1}: x_1 = 1, x_2 = f(x_1) = 1^2 + 1 = 2mod7171$$

$$\gcd(2 - 1,7171) = \gcd(1,7171) = 1$$

$$\boldsymbol{Βήμα\ 2}: x_2 = 2, x_3 = f(x_2) = 2^2 + 1 = 5mod7171$$

$$x_4 = f(x_3) = 5^2 + 1 = 26mod7171, \gcd(x_4 - x_2, n) = \gcd(24,7171) = 1$$

$$\boldsymbol{Βήμα\ 3}: x_3 = 5, x_4 = 26, x_5 = f(x_4) = 26^2 + 1 = 677mod7171$$

$$x_6 = f(x_5) = 667^2 + 1 = 458330 = 6557mod7171$$

$$\gcd(x_6 - x_3, n) = \gcd(6552,7171) = 1$$

$$\boldsymbol{Βήμα\ 4}: x_4 = 26, x_5 = 677, x_6 = 6557$$

$$x_7 = f(x_6) = 6557^2 + 1 = 42994250 = 4105mod7171$$

$$x_8 = f(x_7) = 4105^2 + 1 = 16851026 = 6347mod7171$$

$$\gcd(x_8 - x_4, n) = \gcd(6321,7171) = 1$$

$$\boldsymbol{Βήμα\ 5}: x_5 = 677, x_6 = 6557, x_7 = 4105, x_8 = 6347mod7171$$

$$x_9 = f(x_8) = 6347^2 + 1 = 40284410 = 4903mod7171$$

$$x_{10} = f(x_9) = 4903^2 + 1 = 24039410 = 2218mod7171$$

$$\gcd(x_{10} - x_5, n) = \gcd(1541,7171) = 1$$

$$\boldsymbol{Βήμα\ 6}: x_6 = 6557, x_7 = 4105, x_8 = 6347mod, x_9 = 4903, x_{10} = 2218$$

$$x_{11} = f(x_{10}) = 2218^2 + 1 = 4919525 = 219 mod 7171$$

$$x_{12} = f(x_{11}) = 219^2 + 1 = 47962 = 4936 mod 7171$$

$$\gcd(x_{12} - x_6, n) = \gcd(1621,7171) = 1$$

Βήμα 7: $x_7 = 4105, x_8 = 6347 mod, x_9 = 4903, x_{10} = 2218, x_{11} = 219,$

$$x_{12} = 4936, x_{13} = f(x_{12}) = 4936^2 + 1 = 24364097 = 4210 mod 7171$$

$$x_{14} = f(x_{13}) = 4210^2 + 1 = 17724101 = 4560 mod 7171$$

$$\gcd(x_{14} - x_7, n) = \gcd(455,7171) = 1$$

Βήμα 8: $x_8 = 6347 mod, x_9 = 4903, x_{10} = 2218, x_{11} = 219, x_{12} = 4936$

$$x_{13} = 4210, x_{14} = 4560$$

$$x_{15} = f(x_{14}) = 4560^2 + 1 = 20793601 = 4782 mod 7171$$

$$x_{16} = f(x_{15}) = 4872^2 + 1 = 23736385 = 375 mod 7171$$

$$\gcd(x_{16} - x_8, n) = \gcd(5972,7171) = 1$$

Βήμα 9: $x_9 = 4903, x_{10} = 2218, x_{11} = 219, x_{12} = 4936, x_{13} = 4210, x_{14} = 4560$

$$x_{15} = 4872, x_{16} = 375$$

$$x_{17} = f(x_{16}) = 375^2 + 1 = 140626 = 4377 mod 7171$$

$$x_{18} = f(x_{17}) = 4377^2 + 1 = 19158130 = 4389 mod 7171$$

$$\gcd(x_{18} - x_9, n) = \gcd(514,7171) = 1$$

Βήμα 10: $x_{10} = 2218, x_{11} = 219, x_{12} = 4936, x_{13} = 4210, x_{14} = 4560$

$$x_{15} = 4872, x_{16} = 375, x_{17} = 4377, x_{18} = 4389$$

$$x_{19} = f(x_{18}) = 4389^2 + 1 = 19263322 = 2016 mod 7171$$

$$x_{20} = f(x_{19}) = 2016^2 + 1 = 4064257 = 5471 mod 7171$$

$$\gcd(x_{20} - x_{10}, n) = \gcd(3253,7171) = 1$$

Βήμα 11: $x_{11} = 219, x_{12} = 4936, x_{13} = 4210, x_{14} = 4560, x_{15} = 4872,$

$$x_{16} = 375, x_{17} = 4377, x_{18} = 4389, x_{19} = 2016, x_{20} = 5471$$

$$x_{21} = f(x_{20}) = 5471^2 + 1 = 29931842 = 88 mod 7171$$

$$x_{22} = f(x_{21}) = 88^2 + 1 = 7745 = 574 mod 7171$$

$$\gcd(x_{22} - x_{11}, n) = \gcd(355,7171) = 1$$

Άρα τελικά, ύστερα από 11 επαναλήψεις ο αλγόριθμος εντόπισε τη σύγκρουση $x_{11} \equiv x_{22}(modp)$ και τον μη τετριμμένο παράγοντα p = 71 του 7171. Έτσι, n = 7171 = 71 x 101. Η πρώτη σύγκρουση είναι η $x_7 mod 71 = x_{18} mod 71 = 58$.

Μπορούμε να δούμε μια υλοποίηση του αλγορίθμου Pollard Rho παρακάτω:

Pollard Rho factoring algorithm (n, x_1)

$$external\ f$$

$$x \longrightarrow x_1$$

$$x' \longrightarrow f(x) mod n$$

$$p \longrightarrow \gcd(x - x', n)$$

while $p = 1\ do$

$$x \longrightarrow f(x) mod n$$

$$x' \longrightarrow f(x') mod n$$

$$x' \longrightarrow f(x) mod n$$

$$p \longrightarrow \gcd(x - x', n)$$

if $p = n$

$$then\ return\ (\text{"failure"})$$

$$else\ return\ (p).$$

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Πουλάκης Μ. Δημήτριος, Θεσσαλονίκη, *Κρυπτογραφία Η επιστήμη επικοινωνίας,* Εκδόσεις Ζήτη, 2009

- Κουκουβίνος Χ., Παπαϊωάννου Α., Αθήνα, *Κρυπτογραφία,* Εκδόσεις Ε.Μ.Π, 2007

- Lewand R.,Cryptological Mathematics,the Mathematical Association of America,2000

- Menezes A.,van Oorschot P.Vanstone S.,"Handbook of applied Cryptography",1996.

- Rivest R.L.,Shamir A.,Adleman L.M.,"a method for obtaining digital signatures and public key cryptosystems,Communications of the ACU",V.21 no 2,1978

- Singh S., Κώδικες και Μυστικά, Τραυλός 2003 (ιστορική αναδρομή κρυπτολογίας)

- Smart N.,Cryptography:An introduction,Mc Graw-Hill 2003

- Stinson D.,"Cryptography. Theory and Practice",third ed., Chapman and Hall,2006

- Trappe W. and Washington L. "Introduction to Cryptography with coding Theory", Pearson education international, 2006

- Ε.Ζάχος, «Εισαγωγή στη Θεωρία Αριθμών και την Κρυπτολογία»,Ε.Π.Μ.2005

- Α.Παπαϊωάννου.,Μ.Ρασσιάς, «Εισαγωγή στη Θεωρία Αριθμών» 2010