ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ

ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΥΠΟΛΟΓΙΣΤΙΚΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ:

ΤΕΣΤ ΠΙΣΤΟΠΟΙΗΣΗΣ ΠΡΩΤΩΝ ΚΑΙ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΑΚΕΡΑΙΩΝ

Διπλωματική Εργασία

Ελευθερίου Γεώργιος

Τριμελής Επιτροπή:

Χρήστος Κουκουβίνος, Καθηγητής ΣΕΜΦΕ, ΕΜΠ
Αλέξανδρος Παπαϊωάννου, Αν. Καθηγητής ΣΕΜΦΕ, ΕΜΠ (Επιβλέπων)
Πέτρος Στεφανέας, Λέκτορας ΣΕΜΦΕ, ΕΜΠ

Αθήνα, Μάιος 2011

Περιεχόμενα

1. Εισαγωγική θεωρία αριθμών και ορισμοί
    - 1.1. Βασικά θεωρήματα αλγεβρικών ισοτιμιών (Wilson,Euler,Fermat)
    - 1.2. Θεωρία τετραγωνικών υπολοίπων
        - 1.2.1. Τετραγωνικά υπόλοιπα
        - 1.2.2. Ο συμβολισμός του Legendre
        - 1.2.3. Γενική μορφή λύσης ισοτιμίας δευτέρου βαθμού και το σύμβολο του Jacobi
        - 1.2.4. Ο αλγόριθμος για την εύρεση του συμβόλου του Jacobi
2. Τεστ πιστοποίησης πρώτων αριθμών
    - 2.1. Το τεστ του Fermat
    - 2.2. Το τεστ των Solovay-Strassen
    - 2.3. Το τεστ των Miller-Rabin
    - 2.4. Συγκρίσεις των τεστ Fermat, Solovay - Strassen και Miller – Rabin
3. Παραγοντοποίηση ακεραίων
    - 3.1. Η μέθοδος παραγοντοποίησης του Fermat
    - 3.2. Ο αλγόριθμος παραγοντοποίησης του Dixon
    - 3.3. Η μέθοδος Quadratic Sieve ή QS (Τετραγωνικό κόσκινο)
    - 3.4. Ο αλγόριθμος Pollard Rho

1. ΕΙΣΑΓΩΓΙΚΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ ΚΑΙ ΟΡΙΣΜΟΙ

1.1. ΒΑΣΙΚΑ ΘΕΩΡΗΜΑΤΑ ΑΛΓΕΒΡΙΚΩΝ ΙΣΟΤΙΜΙΩΝ

Θεώρημα (Το θεώρημα του Wilson)

Ο φυσικός p>2 είναι πρώτος ανν

$$(p-1)! \equiv -1(mod\ p)$$

1η Απόδειξη (με θεωρία ομάδων)

Γνωρίζουμε ότι για p πρώτο, κάθε αριθμός μικρότερος του p και μεγαλύτερος του μηδενός έχει μοναδικό πολλαπλασιαστικό αντίστροφο. Επίσης γνωρίζουμε ,όπως θα δούμε παρακάτω, ότι η ισοτιμία $x^2 \equiv a(mod\ p)$ έχει ακριβώς δύο λύσεις. Συνεπώς αφού $(p-1)^2 \equiv 1^2 \equiv 1\ (mod\ p)$, οι αριθμοί 2,3,…,p-2 αποτελούν ζεύγη αντιστρόφων $modp$. Οπότε $2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1(mod\ p)$.
Άρα $(p-1)! = 2 \cdot 3 \cdot \ldots \cdot (p-2)(p-1) \equiv -1\ (mod\ p)$
Αντίστροφα αν $(p-1)! \equiv -1\ (mod\ p)$ και p σύνθετος τότε παρατηρούμε ότι για $p \leq 4$ δεν ισχύει. Για $p > 4$ θεωρούμε ότι $p = ab$ (αφού p σύνθετος) για κάποιους a, b με $1 < a, b < p$ και $a \neq b$. Τότε οι a, b υπάρχουν ως όροι στο $(p-1)!$ οπότε $(p-1)! \equiv 0\ (mod\ p)$. Τέλος αν $p = q^2$ με q πρώτο τότε και ο q και ο $2q$ υπάρχουν στο γινόμενο, άτοπο. Άρα ο p είναι πρώτος. ■

2η Απόδειξη (ο τρόπος του Lagrange):

Έστω το πολυώνυμο $f(x) = (x-1)(x-2) \cdot \ldots \cdot \big(x-(p-1)\big) - (x^{p-1}-1)$,όπου p πρώτος αριθμός και $x = 1,2, \ldots, p-1$. Άρα $(x,p) = 1$ και ένας από τους ακεραίους $x-1, x-2, \ldots, x-(p-1)$ θα είναι ίσος με μηδέν. Συνεπώς από το θεώρημα του Fermat έχουμε ότι $x^{p-1}-1 \equiv 0(mod\ p)$, δηλαδή $p|(x^{p-1}-1)$ και $p|(x-1)(x-2) \cdot \ldots \cdot \big(x-(p-1)\big)$,αφού $p|0$. Άρα $p|f(x)$. Όμως το πολυώνυμο $f(x)$ είναι βαθμού $p-2$ και άρα η γενική του μορφή είναι:

$$f(x) = a_0 + a_1 x + \cdots + a_{p-2}x^{p-2}\ με\ \alpha_\iota \in Z$$

όπου παρατηρούμε ότι $a_0 = (p-1)! + 1$. Συνεπώς από το θεώρημα συντελεστών πολυωνύμου και ότι $p|f(x)$ έχουμε ότι $p|a_0$ και τελικά $(p-1)! \equiv -1(mod\ p)$

Αντίστροφα αν $(p-1)! \equiv -1(mod\ p)$ τότε $p|(p-1)! + 1$,όμως p είναι ο μικρότερος θετικός διαιρέτης του $(p-1)! + 1$, αφού κανένας μικρότερος δεν τον διαιρεί. Άρα ο p είναι πρώτος. ■

3η Απόδειξη (Συνδυαστικά):

Έστω p πρώτος. Για $p = 2$ το θεώρημα ισχύει. Για $p > 2$ ας υποθέσουμε ότι έχουμε p σημεία στο επίπεδο , τα οποία σχηματίζουν ένα $p - γωνο$. Τα διαφορετικά $p - γωνα$ που μπορούμε να σχηματίσουμε με ακριβώς p πλευρές ,όπου επιτρέπουμε τις διασταυρώσεις πλευρών και δεν μας ενδιαφέρει αν τα $p - γωνα$ είναι εκ περιστροφής ίσα, είναι $p!/2p$. Αυτό προκύπτει από το γεγονός ότι αυτά τα $p - γωνα$ μπορούμε να τα δημιουργήσουμε επιλέγοντας μια κορυφή από τις p , στη συνέχεια μια κορυφή διαφορετική από αυτήν που επιλέξαμε, οπότε $p - 1$ επιλογές, και ούτω κάθε εξής. Οπότε στο τέλος με τη σειρά που επιλέξαμε τις κορυφές, τις ενώνουμε και δημιουργείται το $p - γωνο$. Συνεπώς έχουμε $p!$ τρόπους να δημιουργήσουμε ένα $p - γωνο$. Όμως με αυτόν τον τρόπο έχουμε μετρήσει κάθε $p - γωνο$ $2p - φορές$, αφού για τη δημιουργία του $p - γωνου$ σε κάθε κορυφή του, στην οποία αντιστοιχούν δύο πλευρές , χρησιμοποιήσαμε την κάθε πλευρά σε διαφορετικό τρόπο δημιουργίας , καταλήγοντας όμως στο ίδιο $p - γωνο$.

Από τα $p!/2p$ $p - γωνα$, ακριβώς $(p - 1)/2$ είναι εκείνα τα οποία δεν αλλάζουν, όταν περιστραφούν κατά πολλαπλάσια της γωνίας $2\pi/p$. Αυτό προκύπτει από το γεγονός ότι για τη δημιουργία ενός τέτοιου $p - γωνου$, μπορούμε σε μια από τις p κορυφές να χαράξουμε τον άξονα συμμετρίας του $p - γωνου$ που διέρχεται από το p. Στη συνέχεια για κάθε επιλογή μιας κορυφής αριστερά του άξονα συμμετρίας , πρέπει να επιλέξουμε αναγκαστικά τη συμμετρική κορυφή δεξιά του άξονα. Συνεπώς έχουμε $(p - 1)/2$ επιλογές. Όμως κάθε τέτοια επιλογή προσδιορίζει μοναδικά κάθε τέτοιο $p - γωνο$.

Άρα τα $p - γωνα$, τα οποία αλλάζουν όταν περιστραφούν κατά κάποια πολλαπλάσια της γωνίας $2\pi/p$ είναι $\frac{p!}{2p} - \frac{p-1}{2}$ το πλήθος. Έστω k_i ο ελάχιστος αριθμός περιστροφών, ως μια περιστροφή ορίζουμε τη στροφή κατά $2\pi/p$, που χρειάζεται το i τέτοιο $p - γωνο$,ώστε να επανέλθει στην αρχική του κατάσταση. Προφανώς με p περιστροφές κάθε $p - γωνο$ επανέρχεται στην αρχική του κατάσταση. Άρα $k_i \leq p$ για κάθε i. Όμως από την ευκλείδεια διαίρεση έχουμε ότι $p = h_i k_i + r_i \, με \;\; 0 \leq r_i < k_i$ και επειδή το $p - γωνο$ επανέρχεται στην αρχική του κατάσταση μετά από $h_i k_i$ περιστροφές αλλά και μετά από p περιστροφές, πρέπει να επανέρχεται και μετά από r_i περιστροφές. Όμως $r_i < k_i$ και k_i είναι οι ελάχιστες περιστροφές που απαιτούνται. Συνεπώς $r_i = 0$ και $p = h_i k_i$, δηλαδή $p = k_i$ για κάθε i, αφού p πρώτος. Όποτε κάθε $p - γωνο$ από τα $\frac{p!}{2p} - \frac{p-1}{2}$ εμφανίζεται p φορές με διαφορετική στροφή. Άρα $p \left| \frac{p!}{2p} - \frac{p-1}{2} \right.$ ή $2p \left| (p-1)! - (p-1) \right.$ ή $p|(p-1)! + 1$, το ζητούμενο.

Για το αντίστροφο μπορούμε να χρησιμοποιήσουμε ένα από τα επιχειρήματα των αποδείξεων 1 και 2. ■

Θεώρημα (Το θεώρημα του Euler)

Αν a, m ακέραιοι με $(a, m) = 1$, τότε

$$a^{\varphi(m)} \equiv 1(mod\ m)\ ,$$

όπου $\varphi(m)$ η συνάρτηση του Euler και (a, m) ο μέγιστος κοινός διαιρέτης των a και m.

Απόδειξη :

Για $m = 2$ το θεώρημα ισχύει, αφού αν $(a, 2) = 1$ ο a είναι περιττός.

Για $m \geq 3$, θεωρούμε τους $\varphi(m)$ το πλήθος αριθμούς $r_1, r_2, \dots, r_{\varphi(m)}$ που είναι σχετικά πρώτοι με το m. Αν πολλαπλασιάσουμε με το $a(mod\ m)$ παίρνουμε τους αριθμούς

$$a \cdot r_1, a \cdot r_2, \dots, a \cdot r_{\varphi(m)}\ (mod\ m).$$

Επειδή $(a, m) = 1$, ούτε ο a ούτε ο r_i έχουν παράγοντα τον αριθμό m, οπότε ο ar_i είναι σχετικά πρώτος με τον m για κάθε i . Άρα $ar_i = r_j$ για κάποιο j. Επίσης για $i \neq j$ αποκλείεται να έχουμε $ar_i = ar_j\ (mod\ m)$ αφού τότε από το νόμο διαγραφής θα είχαμε $r_i = r_j(mod\ m)$, αφού $(a, m) = 1$. Συνεπώς οι αριθμοί $a \cdot r_1, a \cdot r_2, \dots, a \cdot r_{\varphi(m)}\ (mod\ m)$ είναι ίδιοι με τους $r_1, r_2, \dots, r_{\varphi(m)}$, με διαφορετική ίσως διάταξη. Οπότε

$$(a \cdot r_1)(a \cdot r_2) \dots (a \cdot r_{\varphi(m)}) \equiv r_1 r_2, \dots r_{\varphi(m)}(mod\ m) \quad \text{ή}$$

$$a^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)} \equiv r_1 r_2 \dots r_{\varphi(m)}(mod\ m) \quad \text{ή}$$

$$a^{\varphi(m)} \equiv 1\ (mod\ m),$$

αφού $(m, r_i) = 1$ για κάθε i.

<u>Παρατήρηση:</u> Το Μικρό Θεώρημα του Fermat(Pierre de Fermat 1601-1665) αποτελεί ειδική περίπτωση του θεωρήματος του Euler.

Θεώρημα (Το μικρό θεώρημα του Fermat)

Αν p πρώτος και $(p, a) = 1$ τότε $a^{p-1} \equiv 1\ mod\ p$.

Απόδειξη:

Αφού p πρώτος έχουμε ότι $\varphi(p) = p - 1$, οπότε από το προηγούμενο θεώρημα έχουμε το ζητούμενο.

1.2. ΘΕΩΡΙΑ ΤΕΤΡΑΓΩΝΙΚΩΝ ΥΠΟΛΟΙΠΩΝ

1.2.1. ΤΕΤΡΑΓΩΝΙΚΑ ΥΠΟΛΟΙΠΑ

Πρόταση

Αν $p > 2$, $(a, p) = 1$ με p πρώτο και η ισοτιμία $x^2 \equiv a(mod\ p)$ έχει λύσεις, τότε θα έχει ακριβώς δύο λύσεις $(mod\ p)$.

Απόδειξη:

Έστω x_0 μια λύση της ισοτιμίας τότε ${x_0}^2 \equiv a(mod\ p)$. Παρατηρούμε ότι και το $-x_0$ είναι λύση, αφού $(-x_0)^2 = {x_0}^2 \equiv a(mod\ p)$. Επίσης ισχύει ότι το x_0 είναι διαφορετικό από το $-x_0$, αφού αν $x_0 \equiv -x_0(mod\ p)\ τότε\ p|2x_0$, δηλαδή $p|x_0$ και άρα $p|{x_0}^2$, άτοπο.

Θα δείξουμε τώρα ότι δεν υπάρχουν άλλες λύσεις. Έστω x_1 μια άλλη λύση της ισοτιμίας, τότε ${x_0}^2 \equiv {x_1}^2 \equiv a(mod\ p)$, δηλαδή ${x_0}^2 - {x_1}^2 \equiv 0(mod\ p)$, οπότε $p|(x_0 - x_1)(x_0 + x_1)$. Άρα είτε $p|(x_0 - x_1)\ είτε\ p|(x_0 + x_1)$, αφού ο p πρώτος.

Συνεπώς $x_1 \equiv x_0(mod\ p)$ ή $x_1 \equiv -x_0(mod\ p)$, οπότε δεν υπάρχουν άλλες λύσεις.■

Ορισμός

Ο αριθμός a καλείται τετραγωνικό υπόλοιπο modulo p ,αν η ισοτιμία $x^2 \equiv a(mod\ p)$ έχει λύση. Διαφορετικά ο a καλείται μη τετραγωνικό υπόλοιπο modulo p.

Πρόταση

Έστω $p > 2$ πρώτος. Στο σύνολο {1,2,…,$p-1$} υπάρχουν ακριβώς $(p-1)/2$ τετραγωνικά υπόλοιπα και $(p-1)/2$ μη τετραγωνικά υπόλοιπα modulo p.

Απόδειξη:

Παρατηρούμε ότι για $x \in \{1,2,\dots,p-1\}$,$x^2 \equiv (-x)^2\ (mod\ p)$ και αν για $x \neq y(mod\ p)$ ισχύει $x^2 \equiv y^2(mod\ p)\ τότε\ x \equiv y(mod\ p)$ ή $x \equiv -y(mod\ p), αντίφαση$. Συνεπώς υπάρχουν ακριβώς $(p-1)/2$ τετραγωνικά υπόλοιπα και $(p-1)/2$ μη τετραγωνικά υπόλοιπα modulo p. ■

1.2.2. Ο ΣΥΜΒΟΛΙΣΜΟΣ ΤΟΥ LEGENDRE

Θεώρημα (Κριτήριο Euler για τα τετραγωνικά υπόλοιπα)

Ο ακέραιος $a \neq 0$ είναι τετραγωνικό υπόλοιπο $modulo\ p$, όπου $p > 2$ πρώτος και $(a, p) = 1$ ανν

$$a^{\frac{p-1}{2}} \equiv 1(mod\ p)$$

Απόδειξη:

Έστω ότι το $a \neq 0$ είναι τετραγωνικό υπόλοιπο $modulo\ p$. Τότε θα υπάρχει ακέραιος x_0 τέτοιος ώστε ${x_0}^2 \equiv a(mod\ p)$. Άρα έχουμε ${x_0}^{p-1} \equiv a^{\frac{p-1}{2}}(mod\ p)$ και από το μικρό θεώρημα του Fermat έχουμε ${x_0}^{p-1} \equiv 1(mod\ p)$, οπότε $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$.

Αντίστροφα έστω ότι το a δεν είναι τετραγωνικό υπόλοιπο $modulo\ p$. Για όλους τους ακεραίους αριθμούς x, με $1 \leq x \leq p-1$ θεωρούμε τους αριθμούς

$$1x, 2x, 3x, \dots, (p-1)x\ (mod\ p).$$

Αυτοί οι αριθμοί είναι διαφορετικοί μεταξύ τους, αφού αν $kx \equiv lx(mod\ p)$ τότε $p|(kx - lx), δηλαδή\ p|x$ ή $p|(k-l), οπότε\ k \equiv l(mod\ p), άτοπο$. Οπότε οι παραπάνω αριθμοί θα είναι οι αριθμοί $1,2, \dots, (p-1)$ με διαφορετική ίσως διάταξη. Συνεπώς αφού $1 \leq a \leq p-1$ για κάποιο x θα υπάρχει μοναδικό $y \in \{1,2, \dots, p-1\}$ έτσι ώστε $xy \equiv a(mod\ p)$, με $y \neq x$ αφού το a δεν είναι τετραγωνικό υπόλοιπο. Άρα το σύνολο $\{1,2, \dots, p-1\}$ μπορούμε να το χωρίσουμε σε $\frac{p-1}{2}$ ζεύγη έτσι ώστε το γινόμενο των ζευγών κάθε ζεύγους να είναι a. Οπότε $(p-1)! \equiv a^{\frac{p-1}{2}}(mod\ p)$ το οποίο από το θεώρημα του Wilson είναι ισοδύναμο με $a^{\frac{p-1}{2}} \equiv -1(mod\ p)$.

Συμπέρασμα: Αν a τετραγωνικό υπόλοιπο τότε $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$

αλλιώς $a^{\frac{p-1}{2}} \equiv -1(mod\ p)$. ■

Πρόταση (Λήμμα του Gauss)

Έστω $p > 2$ πρώτος και a ακέραιος με $(a, p) = 1$. Θεωρούμε τους αριθμούς:

$$a, 2a, 3a, \dots, \frac{p-1}{2}a(mod\ p).$$

Έστω n το πλήθος των παραπάνω αριθμών που είναι μεγαλύτεροι από $p/2$. Τότε το α είναι τετραγωνικό υπόλοιπο $modulo\ p$ ανν ο n είναι άρτιος και

$$n \equiv (a-1)\frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] (mod\ 2)$$

Απόδειξη:

Από την απόδειξη του κριτηρίου του Euler έχουμε ότι οι αριθμοί $a, 2a, 3a, \dots, \frac{p-1}{2}a(mod\ p)$ είναι όλοι διαφορετικοί μεταξύ τους.

Έστω $k_1, k_2, \dots, k_n$ οι n αριθμοί που είναι μεγαλύτεροι από το $\frac{p}{2}$ και $l_1, l_2, \dots, l_m$

$οι\ \ m = \frac{p-1}{2} - n$ υπόλοιποι αριθμοί που είναι μικρότεροι του $\frac{p}{2}$. (Προφανώς κανένας αριθμός από τους $a, 2a, 3a, \dots, \frac{p-1}{2}a(mod\ p)$ δεν είναι ίσος με $\frac{p}{2}$, αφού ο $p: περιττός\ πρώτος$)

Επειδή $\frac{p}{2} < k_i < p$, θα έχουμε $0 < p - k_i < \frac{p}{2}$, για κάθε i. Θα δείξουμε ότι οι αριθμοί $p - k_i$ είναι διαφορετικοί $modulo\ p$ από τους $l_1, l_2, \dots, l_m$. Πράγματι, αν είχαμε

$p - k_i \equiv l_j(mod\ p)$ για κάποιους k_i, l_j τότε $k_i + l_j \equiv 0(mod\ p)$ ή $xa + ya \equiv 0(mod\ p)$,

$με\ k_i = xa\ , l_j = ya\ και\ 1 \le x, y \le \frac{p-1}{2}$. Συνεπώς $p|(x+y), αφού\ (\alpha, p) = 1$, κάτι που είναι αδύνατο αφού $2 \le x + y \le p - 1$. Επιπλέον αφού και οι αριθμοί

$p - k_1, p - k_2, \dots, p - k_n$ είναι διαφορετικοί μεταξύ τους έχουμε ότι οι $n + m = \frac{p-1}{2}$ αριθμοί: $p - k_1, p - k_2, \dots, p - k_n, l_1, l_2, \dots, l_m$

είναι μια μετάθεση των αριθμών $1,2,3, \dots, \frac{p-1}{2}$. Έτσι

$$(p-k_1)(p-k_2)\dots(p-k_n)l_1l_2\dots l_m \equiv \left(\frac{p-1}{2}\right)!\ (mod\ p)\ \text{ή}$$

$$(-1)^n k_1k_2\dots k_nl_1l_2\dots l_m \equiv \left(\frac{p-1}{2}\right)!\ (mod\ p).$$

Ακόμη έχουμε ότι $k_1k_2\dots k_nl_1l_2\dots l_m = a(2a)(3a)\dots\left(\frac{p-1}{2}a\right) = \left(\frac{p-1}{2}\right)!\ a^{\frac{p-1}{2}}$.

Οπότε

$$(-1)^n a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \,(mod\ p) \text{ ή}$$

$$a^{\frac{p-1}{2}} \equiv (-1)^n (mod\ p).$$

Άρα από το κριτήριο του Euler συνεπάγεται ότι το a είναι τετραγωνικό υπόλοιπο ανν ο n είναι άρτιος.

Μένει να δείξουμε ότι $n \equiv (a-1)\frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] (mod\ 2)$.

Έχουμε ότι $a = \left[\frac{a}{p}\right]p + r_1$, $2a = \left[\frac{2a}{p}\right]p + r_2$, … , $\frac{p-1}{2}a = \left[\frac{ra}{p}\right]p + r_{\frac{p-1}{2}}$, όπου $0 \le r_i < p$ για κάθε i. Προσθέτοντας τα παραπάνω έχουμε ότι:

$$a\left(1 + 2 + \cdots + \frac{p-1}{2}\right) = p\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + \sum_{j=1}^{n} k_j + \sum_{j=1}^{\frac{p-1}{2}-n} l_j.$$

και επίσης γνωρίζουμε από τα προηγούμενα ότι:

$$\sum_{j=1}^{n}(p - k_j) + \sum_{j=1}^{\frac{p-1}{2}-n} l_j = 1 + \cdots + \frac{p-1}{2} = \frac{p^2-1}{8}$$

Οπότε

$$a\frac{p^2-1}{8} = p\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + np + \frac{p^2-1}{8} + 2\sum_{j=1}^{n} k_j$$

$$\text{ή} \qquad (a-1)\frac{p^2-1}{8} = p\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + np + 2\sum_{j=1}^{n} k_j \equiv p\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + n\ (mod\ 2)$$

Επομένως

$$n \equiv (a-1)\frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] (mod\ 2). \blacksquare$$

Ορισμός (Το σύμβολο του Legendre)

Για $p > 2$ πρώτο και a ακέραιο με $(a, p) = 1$ το σύμβολο του Legendre ορίζεται ως εξής:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, \alpha\nu\ \tau o\ \alpha\ \epsilon\acute{\iota}\nu\alpha\iota\ \tau\epsilon\tau\rho\alpha\gamma\omega\nu\iota\kappa\acute{o}\ \upsilon\pi\acute{o}\lambda o\iota\pi o\ modulo\ p \\ -1, \alpha\nu\ \tau o\ \alpha\ \epsilon\acute{\iota}\nu\alpha\iota\ \mu\eta\ \tau\epsilon\tau\rho\alpha\gamma\omega\nu\iota\kappa\acute{o}\ \upsilon\pi\acute{o}\lambda o\iota\pi o\ modulo\ p \end{cases}$$

Χρησιμοποιώντας το κριτήριο του Euler μπορούμε να ορίσουμε ισοδύναμα το $\left(\frac{a}{p}\right)$ ως εξής:

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

<u>Ιδιότητες</u>

1. Αν $a \equiv b(mod\ p), \tau\acute{o}\tau\epsilon\ \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, με $(ab, p) = 1$
3. $\left(\frac{a^2}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
5. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Αποδείξεις

1. Άμεση συνέπεια του κριτηρίου του Euler και των ιδιοτήτων των ισοτιμιών
2. Άμεση συνέπεια του κριτηρίου του Euler και των ιδιοτήτων των ισοτιμιών
3. Άμεση συνέπεια της ιδιότητας 2
4. Άμεση συνέπεια του κριτηρίου του Euler
5. Σύμφωνα με το λήμμα του Gauss ,αρκεί να υπολογίσουμε πόσοι από τους αριθμούς $2,4,6, \dots, p-1$ είναι μεγαλύτεροι του $\frac{p}{2}$. Χρησιμοποιώντας τον ίδιο συμβολισμό με την απόδειξη του λήμματος του Gauss έχουμε:

$$2 + 4 + 6 + \cdots + (p-1) = k_1 + k_2 + \cdots + k_n + l_1 + l_2 + \cdots + l_m \quad \text{ή}$$

$$\frac{p^2-1}{4} = k_1 + k_2 + \cdots + k_n + l_1 + l_2 + \cdots + l_m \quad (1)$$

Όμως είδαμε ότι οι αριθμοί

$$p - k_1, p - k_2, \dots, p - k_n, l_1, l_2, \dots, l_m$$

είναι μια μετάθεση των αριθμών $1,2,3, \dots, \frac{p-1}{2}$.

Οπότε

$$(p-k_1)+(p-k_2)+\cdots+(p-k_n)+l_1+l_2+\cdots+l_m = 1+2+3+\cdots+\frac{p-1}{2}$$

$$np-(k_1+k_2+\cdots+k_n)+(l_1+l_2+\cdots+l_m)=\frac{p^2-1}{8} \quad (2)$$

Προσθέτοντας τις (1),(2) κατά μέλη έχουμε $np=\frac{p^2-1}{8}+2(k_1+k_2+\cdots+k_n)$,

$άρα\ np\equiv\frac{p^2-1}{8}(mod\ 2), οπότε\ n\equiv\frac{p^2-1}{8}(mod\ 2)$, $αφού\ p\ περιττός.$

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

Θεώρημα (Νόμος τετραγωνικής αντιστροφής του Legendre)

Αν p, q δύο περιττοί πρώτοι τότε

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=\begin{cases}+1, αν\ τουλάχιστον\ ένας\ από\ τους \\ p,q\equiv 1(mod\ 4) \\ -1, αν\ και\ οι\ δύο\ p,q\equiv 3(mod\ 4)\end{cases}$$

ή $ισοδύναμα$

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

Απόδειξη:

Σύμφωνα με το Λήμμα του Gauss έχουμε

$$\left(\frac{q}{p}\right)=(-1)^m \quad και \quad \left(\frac{p}{q}\right)=(-1)^n\ με$$

$$m=\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{jq}{p}\right]\ και\ n=\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{jp}{p}\right]$$

Συνεπώς αρκεί να δείξουμε ότι $m+n=\frac{(p-1)(q-1)}{4}$.

Θεωρούμε την συνάρτηση f που ορίζεται από την σχέση

$$f(x,y)=qx-py, για\ x,y\in Z\ με\ |x|<\frac{p}{2}\ και\ |y|<\frac{q}{2}$$

και τα σύνολα

$$S = \left\{1, \dots, \frac{p-1}{2}\right\} \text{ και } T = \left\{1, \dots, \frac{q-1}{2}\right\}.$$

Αν $(x, y) \neq (0,0), \tau\acute{o}\tau\varepsilon\ f(x, y) \neq 0$. Πραγματικά, αν $f(x, y) = 0, \tau\acute{o}\tau\varepsilon\ qx = py$.

Καθώς $(p, q) = 1, \acute{\varepsilon}\chi ουμε\ p|x\ \kappa\alpha\iota\ q|y$ που είναι άτοπο, γιατί $|x| < \frac{p}{2}$ και $|y| < \frac{q}{2}, \alpha\pi'\acute{o}\pi ου$

$$f(x, y) - f(x', y') = f(x - x', y - y') \neq 0$$

Άρα $f(x, y) \neq f(x', y')$. Συνεπώς, όταν ο x διατρέχει τα στοιχεία του S και ο y τα στοιχεία του T, ο $f(x, y)$ παίρνει $\frac{(p-1)(q-1)}{4}$ ανά δύο ανισότιμες τιμές.

Θα υπολογίσουμε στη συνέχεια το πλήθος των θετικών τιμών του $f(x, y)$ και το πλήθος των αρνητικών, με $x \in S\ \kappa\alpha\iota\ y \in T$. Για κάθε $x \in S$, είναι $f(x, y) > 0$ με $y \in T$, αν και μόνο αν, $y < \frac{qx}{p}$, ή $y \leq \left[\frac{qx}{p}\right]$. Συνεπώς, το πλήθος των θετικών τιμών του $f(x, y)$, με $x \in S\ \kappa\alpha\iota\ y \in T$, είναι

$$m = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right]$$

Ομοίως συμπεραίνουμε ότι το πλήθος των αρνητικών τιμών του $f(x, y)$, με $x \in S\ \kappa\alpha\iota$ $y \in T, \varepsilon\acute{\iota}\nu\alpha\iota$

$$n = \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{p}\right]$$

Επομένως

$$m + n = \frac{(p-1)(q-1)}{4}$$

απ' όπου παίρνουμε το αποτέλεσμα. ■

1.2.3. ΓΕΝΙΚΗ ΜΟΡΦΗ ΛΥΣΗΣ ΙΣΟΤΙΜΙΑΣ ΔΕΥΤΕΡΟΥ ΒΑΘΜΟΥ ΚΑΙ ΤΟ ΣΥΜΒΟΛΟ ΤΟΥ JACOBI

Θεώρημα

Αν $p \geq 3$ πρώτος,$r \geq 1$ και $(a,p)=1$, τότε η ισοτιμία $x^2 \equiv a(mod\ p^r)$ έχει λύση αν και μόνο αν $\left(\frac{a}{p}\right)=1$, δηλαδή αν και μόνο αν η $x^2 \equiv a(mod\ p)$ είναι επιλύσιμη.

Απόδειξη:

Αν x_1 είναι η λύση της $x^2 \equiv a(mod\ p^r)$, τότε είναι λύση και της $x^2 \equiv a(mod\ p)$, αφού:

$$x_1{}^2 \equiv a(mod\ p^r) \quad \text{ή}$$

$$p^r | x_1{}^2 - a \quad \text{ή}$$

$$p | x_1{}^2 - a \quad \text{ή}$$

$$x_1{}^2 \equiv a(mod\ p),$$

δηλαδή η $x^2 \equiv a(mod\ p)$ είναι επιλύσιμη.

Αντίστροφα, θα αποδείξουμε με επαγωγή ότι και η $x^2 \equiv a(mod\ p^r)$ έχει λύση. Υποθέτουμε ότι η $x^2 \equiv a(mod\ p^{r-1})$ είναι επιλύσιμη και έχει λύση τη x_0.

Έστω $x = x_0 + p^{r-1}y$. Θεωρούμε την ισοτιμία

$$(x_0 + p^{r-1}y)^2 \equiv a(mod\ p^r)$$

με άγνωστο τον y. Τότε

$$x_0{}^2 + p^{2r-2}y^2 + 2x_0 y p^{r-1} \equiv a(mod\ p^r) \quad \text{ή}$$

$$x_0{}^2 + 2x_0 y p^{r-1} \equiv a(mod\ p^r)$$

αφού $p^r | p^{2r-2}$.

Επομένως, θα είναι $2x_0 y p^{r-1} \equiv a - x_0{}^2 (mod\ p^r)$.

Αλλά $a - x_0{}^2 \equiv 0(mod\ p^{r-1})$, άρα ο αριθμός $\frac{a-x_0{}^2}{p^{r-1}}$ είναι ακέραιος, οπότε:

$$2x_0 y \equiv \frac{a-x_0{}^2}{p^{r-1}} (mod\ p).$$

Αυτή η εξίσωση είναι γραμμική και έχει λύση ως προς y, αφού $(x_0, p) = 1, p > 2\ και$ $(2x_0, p) = 1$.

Αν y_0 είναι μια λύση αυτής, τότε οι λύσεις της $x^2 \equiv a(mod\ p^r)$ είναι

$$x = x_0 + p^{r-1}(y_0 + kp) = x_0 + p^{r-1}y_0 + kp^r, k \in Z,$$

άρα είναι επιλύσιμη. ■

Θεώρημα

Η ισοτιμία η $x^2 \equiv a\left(mod\ 2^k\right), k \geq 3, a\ περιττός$, είναι επιλύσιμη αν και μόνο αν

$$a \equiv 1(mod\ 8).$$

Απόδειξη:

Για $k = 3$ η ισοτιμία γράφεται $x^2 \equiv a(mod\ 8)$. Επειδή ο a είναι περιττός πρέπει και ο x να είναι περιττός. Όμως επειδή το τετράγωνο οποιουδήποτε περιττού είναι $1(mod\ 8)$, πρέπει $a \equiv 1(mod\ 8)$. Αντίστροφα, αν $a \equiv 1(mod\ 8)$,τότε η $x^2 \equiv 1(mod\ 8)$ έχει προφανείς λύσεις $x \equiv 1,3,5,7(mod\ 8)$.

Έστω ότι η πρόταση ισχύει για κάποιο k και έστω ότι η ισοτιμία $x^2 \equiv a\left(mod\ 2^{k+1}\right)$ είναι επιλύσιμη, με λύση x_0. Τότε ${x_0}^2 \equiv a\left(mod\ 2^k\right)$, οπότε από την υπόθεση $a \equiv 1(mod\ 8)$.

Αντίστροφα αν $a \equiv 1(mod\ 8)$ θέτουμε $x = x_0 + 2^k y$ και εργαζόμενοι όπως στο προηγούμενο θεώρημα διαπιστώνουμε ότι η ισοτιμία είναι επιλύσιμη. ■

Θεώρημα

Έστω η ισοτιμία $x^2 \equiv a(mod\ m)$ όπου $m = m_1 \cdot \ldots \cdot m_k$ με $\left(m_i, m_j\right) = 1, για\ κάθε\ i, j$. Η παραπάνω ισοτιμία είναι επιλύσιμη αν και μόνο αν καθεμία από τις ισοτιμίες

$x^2 \equiv a(mod\ m_i), i = 1,2, \ldots, k$ είναι επιλύσιμη.

Απόδειξη:

Αν $x^2 \equiv a(mod\ m)\ \Rightarrow m \left|(x^2 - a) \Rightarrow m_1 \cdot \ldots \cdot m_k\right| (x^2 - a) \Rightarrow m_i|(x^2 - a)\ για\ κάθε\ i$,

δηλαδή $x^2 \equiv a(mod\ m_i), i = 1,2, \ldots, k$, αφού $\left(m_i, m_j\right) = 1, για\ κάθε\ i, j$.

Αντίστροφα αν $x^2 \equiv a(mod\ m_i), i = 1,2, \ldots, k$ το ζητούμενο είναι προφανές. ■

Ορισμός (Το σύμβολο του Jacobi)

Έστω P περιττός θετικός ακέραιος και a ένας ακέραιος αριθμός, τέτοιος ώστε $(a, P) = 1$. Τότε, ορίζουμε το σύμβολο του Jacobi $\left(\frac{\alpha}{P}\right)$ ως εξής:

$$\left(\frac{a}{P}\right) = \begin{cases} 1, \alpha\nu\ P = 1 \\ \left(\frac{a}{p_1}\right)^{m_1}\left(\frac{a}{p_2}\right)^{m_2}\dots\left(\frac{a}{p_k}\right)^{m_k}, \alpha\nu\ P = {p_1}^{m_1}{p_2}^{m_2}\dots{p_k}^{m_k} \end{cases}$$

όπου $\left(\frac{a}{p_i}\right)$ είναι το σύμβολο του Legendre.

<u>Παρατήρηση:</u>

Συνεπώς για το σύμβολο του Jacobi έχουμε ότι:

$$\left(\frac{a}{P}\right) = \begin{cases} 0, \alpha\nu\ a \equiv 0(mod\ P) \\ 1, \alpha\nu\ \gamma\iota\alpha\ \kappa\acute{\alpha}\pi\omega\iota o\ \alpha\kappa\acute{\epsilon}\rho\alpha\iota o\ x, a \equiv x^2(mod\ P)\ \kappa\alpha\iota\ p\ \delta\epsilon\nu\ \delta\iota\alpha\iota\rho\epsilon\acute{\iota}\ \tau o\ \alpha \\ -1, \alpha\nu\ \delta\epsilon\nu\ \upsilon\pi\acute{\alpha}\rho\chi\epsilon\iota\ \tau\acute{\epsilon}\tau o\iota o\ x \end{cases}$$

όπου θεωρήσαμε το γενικευμένο σύμβολο του Legendre και κατά συνέπεια του Jacobi, για τα οποία θεωρούμε ότι είναι ίσα με το μηδέν αν $a|P$.

<u>Ιδιότητες</u>

1. Αν P περιττός πρώτος , τότε το σύμβολο $\left(\frac{a}{P}\right)$ του Jacobi ταυτίζεται με το σύμβολο του Legendre.
2. Αν $a \equiv b(mod\ P)\ \tau\acute{o}\tau\epsilon\ \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$
3. $\left(\frac{a}{P}\right)\left(\frac{b}{P}\right) = \left(\frac{ab}{P}\right)$
4. $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$
5. $\left(\frac{m}{P}\right) = \left(\frac{P}{m}\right)(-1)^{\frac{P-1}{2}\cdot\frac{m-1}{2}} = \begin{cases} \left(\frac{P}{m}\right), \alpha\nu\ P \equiv 1\ (mod\ 4) \acute{\eta}\ m \equiv 1\ (mod\ 4) \\ -\left(\frac{P}{m}\right), \alpha\nu\ P \equiv m \equiv 3\ (mod\ 4) \end{cases}$, $\gamma\iota\alpha\ (P, m) = 1$ (Νόμος Τετραγωνικής Αντιστροφής)
6. $\left(-\frac{1}{P}\right) = (-1)^{\frac{P-1}{2}} = \begin{cases} 1, \alpha\nu\ P \equiv 1(mod\ 4) \\ -1, \alpha\nu\ P \equiv 3(mod\ 4) \end{cases}$
7. $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}} = \begin{cases} 1, \alpha\nu\ P \equiv 1\ \acute{\eta}\ 7(mod\ 8) \\ -1, \alpha\nu\ P \equiv 3\ \acute{\eta}\ 5(mod\ 8) \end{cases}$

Παρατήρηση:

Σημαντικό για τα παρακάτω είναι να παρατηρήσουμε ότι με τη βοήθεια των παραπάνω ιδιοτήτων μπορούμε να υπολογίσουμε το σύμβολο του Jacobi ενός αριθμού, χωρίς να ξέρουμε την παραγοντοποίηση του.

1.2.4. Ο ΑΛΓΟΡΙΘΜΟΣ ΓΙΑ ΤΗΝ ΕΥΡΕΣΗ ΤΟΥ ΣΥΜΒΟΛΟΥ ΤΟΥ JACOBI

Αλγόριθμος (Σύμβολο του Jacobi)

Input (ακέραιος α, μονός ακέραιος $n \geq 3$)

$b \leftarrow a \ mod \ n$

$c \leftarrow n$

$s \leftarrow 1$

while $b \geq 2$ repeat

    while $4|b$ repeat $b \leftarrow b/4$

    if $2|b$ then

        if $c \ mod \ 8 \in \{3,5\}$ then $s \leftarrow -s$

        $b \leftarrow b/2$

    end_if

    if $b = 1$ then break

    if $b \ mod \ 4 = c \ mod \ 4 = 3$ then $s \leftarrow -s$

    $(b, c) \leftarrow (c \ mod \ b, b)$

end_while

return $s \cdot b$

Παρατήρησεις:

1)Παρατηρούμε ότι ο αλγόριθμος αποτελεί απλή εφαρμογή των ιδιοτήτων του συμβόλου του Jacobi.

2)Η πολυπλοκότητα του αλγορίθμου για δύο αριθμούς με n ψηφία είναι $O(M(n)logn)$, όπου $M(n)$ είναι η πολυπλοκότητα του αλγορίθμου που θα χρησιμοποιηθεί για τον πολλαπλασιασμό των αριθμών.

Παράδειγμα

Εύρεση του $\left(\frac{1828}{757}\right)$:

Ο παραπάνω αλγόριθμος ακολουθεί τα εξής βήματα

$a = 1828$, $n = 757$

b	c	s
314	757	1
157	757	-1
129	157	-1
28	129	-1
7	129	-1
3	7	-1
3	7	1
1	3	**1**

Συνεπώς $\left(\frac{1828}{757}\right)$=1.

Ας ελέγξουμε το αποτέλεσμα πιο αναλυτικά:

Ο 757 είναι πρώτος. Άρα το $\left(\frac{1828}{757}\right)$ είναι ένα σύμβολο Legendre

$$\left(\frac{1828}{757}\right) = \left(\frac{314}{757}\right) = \left(\frac{2}{757}\right) \cdot \left(\frac{157}{757}\right) = (-1)^{\frac{757^2-1}{8}} \cdot 157^{\frac{757-1}{2}} (mod\ 757) =$$

$$(-1) \cdot 157^{378} (mod\ 757) = (-1) \cdot (-1) = 1.$$

2. ΤΕΣΤ ΠΙΣΤΟΠΟΙΗΣΗΣ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ

Τα τεστ πιστοποίησης πρώτων αριθμών, δηλαδή αλγόριθμοι που μπορούν να αποφανθούν αν ένας αριθμός είναι πρώτος ή όχι, εκτός από το ενδιαφέρον που παρουσιάζουν σε διάφορους κλάδους της μαθηματικής έρευνας, παίζουν καθοριστικό ρόλο στα κρυπτοσυστήματα δημοσίου κλειδιού. Αυτό συμβαίνει, γιατί η λειτουργία των περισσοτέρων (αν όχι όλων) κρυπτοσυστημάτων δημοσίου κλειδιού (RSA, El Gamal, Paillier,…) βασίζεται στη χρήση μεγάλων πρώτων αριθμών, δηλαδή με σημερινά δεδομένα της τάξεως των $150-300$ ψηφίων ή $512-1024$ bits .

Η βασική μεθοδολογία για να βρίσκουμε τόσο μεγάλους πρώτους είναι να παράγουμε τυχαία αριθμούς, της κλίμακας που μας ενδιαφέρει, και να ελέγχουμε αν είναι πρώτοι ή όχι. Είναι λογικό να αναρωτηθούμε πόσους αριθμούς πρέπει να ελέγξουμε ώστε να πετύχουμε έναν ο οποίος είναι πρώτος και μάλιστα με 200 περίπου ψηφία. Την απάντηση σε αυτό το ερώτημα δίνει το θεώρημα των πρώτων αριθμών (prime number theorem).

Θεώρημα(Το θεώρημα των πρώτων αριθμών)

Έστω $\pi(x)$ ο αριθμός των πρώτων που δεν ξεπερνούν το x, τότε

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

Σύμφωνα λοιπόν με το *Θεώρημα των πρώτων αριθμών* ,η πιθανότητα να επιλέξουμε τυχαία έναν αριθμό k με $1 < k \leq x$ και αυτός να είναι πρώτος είναι $\frac{x}{\pi(x)} = \frac{1}{\ln x}$. Άρα αν ψάχναμε για έναν πρώτο με 200 περίπου ψηφία θα χρειαζόταν να εξετάσουμε κατά μέσο όρο $\ln 10^{200} \cong 461$ αριθμούς ή εξαιρώντας τους άρτιους περίπου 230 αριθμούς. Συνεπώς μπορούμε να πούμε ότι υπολογιστικά είναι μια εφικτή διαδικασία , με δεδομένο όμως ότι η πολυπλοκότητα του τεστ πιστοποίησης πρώτου που θα χρησιμοποιηθεί είναι μικρή.

Γενικά το πρόβλημα να διαπιστώσουμε αν ένας αριθμός είναι πρώτος ή όχι , διεθνώς ονομάζεται *"PRIMES"* και με την σχετικά πρόσφατη δημοσίευση του αλγορίθμου AKS (Agrawal-Kayal-Saxena primality test) το 2002 , αποδείχθηκε ότι το πρόβλημα "$PRIMES$" ανήκει στο P, από άποψη υπολογιστικής πολυπλοκότητας.

Γενικά τα τεστ πιστοποίησης πρώτων που χρησιμοποιούνται στην πράξη είναι είτε ντετερμινιστικά είτε πιθανοτικά, με τα περισσότερα από αυτά να είναι πιθανοτικά. Στο συγκεκριμένο κείμενο θα εξετάσουμε μόνο πιθανοτικά τεστ ,όπως τα τεστ των Fermat, Solovay-Strassen, Miller-Rabin.

2.1. ΤΟ ΤΕΣΤ ΤΟΥ FERMAT

Από το μικρό θεώρημα του Fermat έχουμε ότι για έναν πρώτο αριθμό n και για ακέραιο a με $1 \leq a \leq n-1$,ισχύει $a^{n-1} \equiv 1\ mod\ n$. Συνεπώς αν θέλουμε να εξετάσουμε αν ένας δοσμένος ακέραιος n είναι πρώτος και βρούμε ένα a, με $1 \leq a \leq n-1$, για τον οποίο δεν ισχύει το μικρό θεώρημα του Fermat , τότε μπορούμε να πούμε με βεβαιότητα ότι ο n είναι σύνθετος. Η παραπάνω διαδικασία αποτελεί ουσιαστικά το τεστ του Fermat, το οποίο θα αναλύσουμε περαιτέρω παρακάτω.

Ορισμός

Έστω n ένας περιττός σύνθετος ακέραιος. Ο ακέραιος a, για τον οποίο ισχύει $1 \leq a \leq n-1$ και $a^{n-1} \neq 1\ mod\ n$, ονομάζεται *Fermat-μάρτυρας* για το n.

Ορισμός

Έστω n ένας περιττός σύνθετος ακέραιος και έστω a, με $1 \leq a \leq n-1$ και $a^{n-1} \equiv 1\ mod\ n$. Τότε ο n ονομάζεται *ψευδοπρώτος με βάση το* a και ο a ονομάζεται *Fermat-ψεύτης* για το n.

Παράδειγμα

Έστω οι αριθμοί $n = 91 = 7 \cdot 13$ και $a = 3$. Παρατηρούμε ότι $3^{90} \equiv 1\ mod\ 91$, δηλαδή με βάση το 3 ο 91 είναι *ψευδοπρώτος* και ο 3 είναι *Fermat-ψεύτης* για το n. Αν τώρα είχαμε επιλέξει $a = 2$, θα είχαμε ότι $2^{90} \equiv 64\ mod\ 91$ και άρα το 2 είναι *Fermat-μάρτυρας* για το n.

Αλγόριθμος (Τεστ του Fermat)

FERMAT(n, t)

INPUT: ένα περιττό ακέραιο $n \geq 3$ και συντελεστή ασφάλειας $t \geq 1$.

OUTPUT: θα απαντάει στην ερώτηση "είναι ο n πρώτος;" με δυνατές απαντήσεις "ο n είναι πρώτος με συντελεστή ασφάλειας t" ," ο n είναι σύνθετος.

1. For i from 1 to t
    a. Διάλεξε έναν τυχαίο ακέραιο $a, 2 \leq a \leq n-2$.
    b. Υπολόγισε το $r = a^{n-1} \ mod \ n$.
    c. If $r \neq 1$ then return("ο n είναι σύνθετος").
2. Return("ο n είναι πρώτος με συντελεστή ασφάλειας t").

<u>Παρατήρηση:</u> Αν ο παραπάνω αλγόριθμος μας επιστρέψει "ο n είναι σύνθετος" , τότε μπορούμε να πούμε ότι ο n είναι σίγουρα σύνθετος. Από την άλλη αν μας επιστρέψει "ο n είναι πρώτος με συντελεστή ασφάλειας t" τότε δεν μπορούμε να πούμε με βεβαιότητα ότι ο n είναι πρώτος. Παρακάτω θα αναλύσουμε το πόσο βέβαιοι μπορούμε να είμαστε αλλά και τι σημαίνει "ο n είναι πρώτος με συντελεστή ασφαλείας t".

Λήμμα

Έστω n περιττός ακέραιος , a ακέραιος με $1 \leq a \leq n-1, \ d = (a, n)$ και $r = a^{n-1} \ mod \ n$. Τότε $d|r$.

Απόδειξη

Από την Ευκλείδεια διαίρεση έχουμε ότι $a^{n-1} = k \cdot n + u$, με $0 \leq u < n$ και $k \in \mathbb{Z}$. Αφού $d|a$ και $d|n \ \Rightarrow d|a^{n-1}$ και $d|k \cdot n \ \Rightarrow \ d|u$. Άρα $d|r$. ■

<u>Παρατήρηση</u>

Συνεπώς αν a ακέραιος με $1 \leq a \leq n-1$ και $(a, n) \neq 1$, τότε $a^{n-1} \neq 1 \ mod \ n$. Δηλαδή το *τεστ του Fermat* θα μας είχε επιστρέψει ότι ο n είναι σύνθετος.

Θεώρημα

Αν $n \geq 3$ περιττός σύνθετος ακέραιος και υπάρχει τουλάχιστον ένα a , ώστε ο a να είναι *Fermat-μάρτυρας* με $(a,n) = 1$, τότε η πιθανότητα να βρούμε έναν ακέραιο $k, 1 \leq k \leq n-1$ με $k^{n-1} \neq 1 \; mod \; n$ και $(k,n) = 1$ είναι μεγαλύτερη του $\frac{1}{2}$.

Απόδειξη:

Έστω το σύνολο $G_n = \{x: x \in \mathbb{Z}_n^* \; και \; (x,n) = 1\}$. Είναι γνωστό ότι το G_n είναι πολλαπλασιαστική ομάδα στο $modulo \; n$.

Έστω το σύνολο $A = \{k: k \in G_n \; και \; k^{n-1} \equiv 1 \; mod \; n\}$ των *Fermat-ψευτών.*

Θα δείξουμε ότι το A είναι υποομάδα του G_n:

a) Παρατηρούμε ότι $A \subseteq G_n$.
b) Η διμελής πράξη του πολ/μου στο A είναι προσεταιριστική ως η επαγόμενη πράξη από την ομάδα G_n.
c) Υπάρχει ταυτοτικό στοιχείο και είναι το $1 \in A$, αφού $1^{n-1} \equiv 1 \; mod \; n$,$(1,n) = 1$ και $1 \in \mathbb{Z}_n^*$.
d) Κάθε στοιχείο του A έχει πολλαπλασιαστικό αντίστροφο. Έστω $l \in A$, τότε το l έχει πολλαπλασιαστικό αντίστροφο $modulo \; n$, αφου $l \in G_n$ λόγω του ότι ισχύει ότι $A \subseteq G_n$ και G_n ομάδα. Έστω $h \in G_n$ ο αντίστροφος του l, άρα $hl \equiv 1 \; mod \; n$

   $\Rightarrow \; (hl)^{n-1} \equiv 1 \; mod \; n \; \Rightarrow \; h^{n-1} \cdot l^{n-1} \equiv 1 \; mod \; n \; \Rightarrow \; h^{n-1} \equiv 1 \; mod \; n$, άρα $h \in A$, αφού $l^{n-1} \equiv 1 \; mod \; n$.
e) Το A είναι κλειστό ως προς τον πολλαπλασιασμό $modulo \; n$. Έστω $u, w \in A$ τότε επειδή $A \subseteq G_n$ και G_n ομάδα, έχουμε ότι $u \cdot w \in G_n$. Μένει να δείξουμε ότι το $u \cdot w \in A$, δηλαδή ότι $(u \cdot w)^{n-1} \equiv 1 \; mod \; n$. Όμως $(u \cdot w)^{n-1} = u^{n-1} \cdot w^{n-1} \equiv 1 \cdot 1 = 1 \; mod \; n$.

Άρα το Α είναι υποομάδα του G_n.

Από υπόθεση υπάρχει α με $(a,n) = 1$, $\alpha^{n-1} \neq 1 \; mod \; n$ και $a \in \mathbb{Z}_n^*$. Άρα $a \in G_n$ και $a \notin A$, δηλαδή η A είναι γνήσια υποομάδα της G_n.

Συνεπώς από το θεώρημα του Langrage έχουμε ότι η τάξη του A θα είναι γνήσιος διαιρέτης της τάξης του G_n, δηλαδή $|G_n| = |A| \cdot s$, για κάποιο θετικό ακέραιο $s \geq 2$. Συνεπώς η πιθανότητα να βρούμε έναν ακέραιο $k, 1 \leq k \leq n-1$ με $k^{n-1} \neq 1 \; mod \; n$ και $(k,n) = 1$ είναι $P = 1 - \frac{|A|}{|G_{n|}} = 1 - \frac{|A|}{|A| \cdot s} = 1 - \frac{1}{s}$ και άρα $P \geq \frac{1}{2}$, αφού $s \geq 2$. ■

Βλέπουμε λοιπόν, σύμφωνα με το παραπάνω θεώρημα ,ότι για δεδομένο σύνθετο n ,έτσι ώστε ο n να έχει *Fermat-μάρτυρες* ,όταν το τέστ του Fermat μας επιστρέφει "ο n είναι πρώτος με συντελεστή ασφαλείας t" σημαίνει ότι ο n είναι πρώτος με πιθανότητα μεγαλύτερη του $1 - \frac{1}{2^t}$.

Το τεστ του Fermat, λόγω της απλότητας του σε σχέση με άλλα πιθανοτικά τεστ πιστοποίησης πρώτου, χρησιμοποιείται σε πολλές περιπτώσεις στην πράξη , όπως στο κρυπτοσύστημα PGP (Pretty Good Privacy). Παρόλα αυτά έχει το μειονέκτημα ότι υπάρχουν αριθμοί που είναι σύνθετοι και δεν υπάρχουν Fermat-μάρτυρες για αυτούς τους αριθμούς. Αυτοί οι αριθμοί ονομάζονται *αριθμοί Carmichael*.

Ορισμός

Ένας περιττός σύνθετος ακέραιος $n > 3$ λέγεται *αριθμός Carmichael* αν δεν έχει *Fermat-μάρτυρες*.

<u>Παράδειγμα</u>

Οι αριθμοί $561 = 3 \cdot 11 \cdot 17, 1105 = 5 \cdot 13 \cdot 17, 126217 = 7 \cdot 13 \cdot 19 \cdot 73$ είναι όλοι *αριθμοί Carmichael*.

Θεώρημα

Ένας περιττός σύνθετος ακέραιος $n > 3$ είναι *αριθμός Carmichael*, αν και μόνο αν δεν διαιρείται από το τετράγωνο ενός πρώτου (είναι ελεύθερος τετραγώνου) και κάθε πρώτος διαιρέτης p του n είναι τέτοιος, ώστε ο $p - 1$ να διαιρεί τον $n - 1$.

Απόδειξη:

Έστω n *αριθμός του Carmichael*. Έστω p^t, p πρώτος, η μεγαλύτερη δύναμη του p που διαιρεί το n και g μια πρωταρχική ρίζα $mod\ p^t$.

Επειδή $\left(p^t, \frac{n}{p^t}\right) = 1$, από το *Κινέζικο θεώρημα των υπολοίπων* έχουμε ότι υπάρχει ακέραιος b με $b \equiv g\ mod\ p^t$ και $b \equiv 1\ mod\ \frac{n}{p^t}$. Άρα $(b, p) = 1, \left(b, \frac{n}{p^t}\right) = 1$ και επομένως $(b, n) = 1$.

Αφού ο n είναι *αριθμός του Carmichael* έχουμε ότι $b^{n-1} \equiv 1\ mod\ n \overset{p^t|n}{\Longrightarrow} b^{n-1} \equiv 1\ mod\ p^t$ και επειδή ο b είναι πρωταρχική ρίζα $mod\ p^t$,έχουμε $\varphi(p^t) \Big| n-1 \Rightarrow p^{t-1}(p-1) \Big| n-1$, όπου $\varphi(x)$η συνάρτηση του Euler.

Συνεπώς $p-1|\ n-1$, το ζητούμενο.

Αντίστροφα, ας υποθέσουμε ότι ο n είναι ελεύθερος τετραγώνου και για κάθε πρώτο διαιρέτη p του n ισχύει $p-1|n-1$.

Έστω a ακέραιος με $(a,n)=1$.

Επειδή p πρώτος, από *το μικρό θεώρημα του Fermat* έχουμε $a^{p-1} \equiv 1\ mod\ p$ και επειδή $p-1|n-1$, έχουμε $a^{n-1} \equiv 1\ mod\ p$. Όμως ο n είναι ελεύθερος τετραγώνου, άρα από το *Κινέζικο θεώρημα υπολοίπων* έχουμε ότι $a^{n-1} \equiv 1\ mod\ n$, το ζητούμενο. ■

Πόρισμα

Ένας *αριθμός Carmichael* έχει τουλάχιστον τρείς πρώτους παράγοντες.

Απόδειξη:

Έστω n ένας *αριθμός Carmichael* .

Συνεπώς ο n είναι σύνθετος.

Υποθέτουμε ότι $n=pq$, όπου p,q πρώτοι με $p>q$. Από το παραπάνω θεώρημα έχουμε ότι $p-1 \Big| n-1 \Rightarrow p-1 \Big| pq-1 \Rightarrow p-1 \Big| (p-1)q+q-1 \Rightarrow p-1 \Big| q-1 \Rightarrow p \leq q$, άτοπο.

Άρα ο n έχει τουλάχιστον τρείς πρώτους παράγοντες. ■

Υπάρχουν πολλά αποτελέσματα για τους *αριθμούς Carmichael* ,μεταξύ των οποίων και ότι είναι άπειροι, εκείνο όμως που έχει μεγάλο ενδιαφέρον για το τεστ του Fermat είναι εκείνο που οφείλεται στον R.G.E. Pinch. Σύμφωνα με αυτό για το πλήθος των *αριθμών Carmichael* , που είναι μικρότεροι από έναν αριθμό n, έστω $C(n)$ ισχύει ότι $C(n) < n\, e^{-\frac{\ln n \ln\ln\ln n}{\ln\ln n}}$. Βλέπουμε λοιπόν ότι η πιθανότητα να πέσουμε σε έναν *αριθμό Carmichael* είναι αρκετά μικρή. Παρόλα αυτά λόγω αυτής της αδυναμίας του *τεστ του Fermat* έχουν δημιουργηθεί άλλα πιθανοτικά τεστ πιστοποίησης πρώτου που αποφεύγουν αυτό το πρόβλημα.

2.2. ΤΟ ΤΕΣΤ ΤΩΝ SOLOVAY - STRASSEN

Το *τεστ Solovay – Strassen* ήταν το πρώτο πιθανοτικό τεστ πιστοποίησης πρώτου που χρησιμοποιήθηκε στην κρυπτογραφία δημοσίου κλειδιού, συγκεκριμένα στο κρυπτοσύστημα RSA. Σήμερα όμως έχει ξεπεραστεί από το *τεστ Miller-Rabin*, το οποίο είναι καλύτερο από όλες τις απόψεις. Γι' αυτό το λόγο το τεστ Solovay-Strassen δεν χρησιμοποιείται πλέον, παρόλα αυτά το παραθέτουμε για ιστορικούς λόγους αλλά και για την πληρότητα του κειμένου.

Από το κριτήριο του Euler έχουμε ότι για έναν περιττό πρώτο ισχύει το εξής:

$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \ mod\ n$, για κάθε ακέραιο a με $(a,n) = 1$ και $\left(\frac{a}{n}\right)$ το *σύμβολο του Jacobi* .

Σε αυτό ακριβώς το γεγονός στηρίζεται το τεστ των Solovay – Strassen , όπως θα δούμε και θα αναλύσουμε παρακάτω.

Ορισμός

Έστω n ένας περιττός σύνθετος αριθμός και a ακέραιος, με $1 \leq a \leq n-1$. Αν ισχύει ότι $(a,n) > 1$ είτε $a^{\frac{n-1}{2}} \neq \left(\frac{a}{n}\right) \ mod\ n$, τότε ο a καλείται *Euler-μάρτυρας* για το n.

Ορισμός

Έστω n ένας περιττός σύνθετος αριθμός και a ακέραιος, με $1 \leq a \leq n-1$. Αν ισχύει ότι $(a,n) = 1$ και $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \ mod\ n$, τότε ο a καλείται *Euler-ψεύτης* για το n και ο n καλείται *Euler ψευδοπρώτος* με βάση το a.

Παράδειγμα:

Έστω ο ακέραιος $91 = 7 \cdot 13$. Παρατηρούμε ότι $9^{\frac{91-1}{2}} = 9^{45} \equiv 1\ mod\ 91$ και $\left(\frac{9}{91}\right) = 1$. Άρα το 91 είναι *Euler ψευδοπρώτος* με βάση το *9* και το 9 είναι *Euler-ψεύτης* για το 91.

Έστω $783 = 3^3 \cdot 29$. Παρατηρούμε ότι $7^{\frac{783-1}{2}} = 7^{391} \equiv 25\ mod\ 783$ και $\left(\frac{7}{783}\right) = 1$. Άρα ο 7 είναι *Euler-μάρτυρας* για το n.

Αλγόριθμος (Τεστ Solovay-Strassen)

INPUT: ένα περιττό ακέραιο $n \geq 3$ και συντελεστή ασφάλειας $t \geq 1$.

OUTPUT: θα απαντάει στην ερώτηση "είναι ο n πρώτος;" με δυνατές απαντήσεις "ο n είναι πρώτος με συντελεστή ασφάλειας t" ," ο n είναι σύνθετος".

1. For i from 1 to t
    a. Διάλεξε έναν τυχαίο ακέραιο $a, 2 \leq a \leq n-2$.
    b. Υπολόγισε το $r = a^{\frac{n-1}{2}} \, mod \, n$.
    c. If $r \neq 1$ και $r \neq n-1$ then return("ο n είναι σύνθετος").
    d. Υπολόγισε το *σύμβολο του Jacobi* $s = \left(\frac{a}{n}\right)$.
    e. if $r \neq s \, mod \, n$ then return("ο n είναι σύνθετος").
2. Return("ο n είναι πρώτος με συντελεστή ασφαλείας t").

Παρατήρηση: Αν ο παραπάνω αλγόριθμος μας επιστρέψει "ο n είναι σύνθετος, τότε μπορούμε να πούμε με βεβαιότητα, ότι ο n είναι σύνθετος. Από την άλλη αν μας επιστρέψει "ο n είναι πρώτος με συντελεστή ασφαλείας t" τότε δεν μπορούμε να είμαστε σίγουροι ότι ο n είναι πρώτος. Παρακάτω θα αναλύσουμε το πόσο βέβαιοι μπορούμε να είμαστε αλλά και τι σημαίνει "ο n είναι πρώτος με συντελεστή ασφαλείας t".

Λήμμα

Έστω n περιττός ακέραιος , a ακέραιος με $1 \leq a \leq n-1$, $d = (a, n)$ και $r = a^{\frac{n-1}{2}} \, mod \, n$. Τότε $d|r$.

Απόδειξη

Από την Ευκλείδεια διαίρεση έχουμε ότι $a^{\frac{n-1}{2}} = k \cdot n + u$, με $0 \leq u < n$ και $k \in \mathbb{Z}$. Αφού $d|a$ και $d|n \Rightarrow d|a^{\frac{n-1}{2}}$ και $d|k \cdot n \Rightarrow d|u$. Άρα $d|r$. ■

Πρόταση

Έστω μονός σύνθετος $n \geq 3$, τότε κάθε *Euler-ψεύτης* του n είναι και *Fermat-ψεύτης* του n.

Απόδειξη:

Έστω a *Euler-ψεύτης* του n, τότε $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)\ mod\ n$ και επειδή $\left(\frac{a}{n}\right) = \begin{cases} +1,\ \alpha\nu\ \alpha\ \tau\epsilon\tau\rho\alpha\gamma\omega\nu\iota\kappa\acute{o}\ \upsilon\pi\acute{o}\lambda o\iota\pi o\ mod\ n \\ -1, \alpha\nu\ \alpha\ \mu\eta\ \tau\epsilon\tau\rho\alpha\gamma\omega\nu\iota\kappa\acute{o}\ \upsilon\pi\acute{o}\lambda o\iota\pi o\ mod\ n \end{cases}$, έχουμε ότι $a^{\frac{n-1}{2}} \cdot \left(\frac{a}{n}\right) \equiv 1\ mod\ n.$

Συνεπώς $(a^{\frac{n-1}{2}} \cdot \left(\frac{a}{n}\right))^2 \equiv 1^2\ mod\ n\ \Rightarrow\ a^{n-1} \cdot \left(\frac{a}{n}\right)^2 \equiv 1\ mod\ n \Rightarrow\ a^{n-1} \equiv 1\ mod\ n$, και αφού ο n είναι σύνθετος έχουμε ότι ο a είναι *Fermat-ψεύτης*. ■

Πρόταση

Έστω $n \geq 3$ περιττός σύνθετος ακέραιος και το σύνολο $G_n = \{x: x \in \mathbb{Z}_n^*\ \kappa\alpha\iota\ (x,n) = 1\}$. Το σύνολο $B = \{k: k \in G_n\ \kappa\alpha\iota\ \left(\frac{k}{n}\right) \equiv k^{\frac{n-1}{2}}\ mod\ n\}$ είναι γνήσια υποομάδα του G_n.

Απόδειξη:

Από το αντίστοιχο θεώρημα που αποδείξαμε για το *τεστ του Fermat* και την παραπάνω πρόταση , έχουμε ότι $B \subseteq A(\tau o\ \sigma\acute{\upsilon}\nu o\lambda o\ \tau\omega\nu\ Fermat\ \psi\epsilon\upsilon\tau\acute{\omega}\nu) \subseteq G_n$.

Επίσης είναι γνωστό ότι το G_n είναι πολλαπλασιαστική ομάδα στο $modulo\ n$.

a) Συνεπώς $B \subseteq G_n$.
b) Η διμελής πράξη του πολ/μου στο B είναι προσεταιριστική ως η επαγόμενη πράξη από την ομάδα G_n.
c) Υπάρχει ταυτοτικό στοιχείο και είναι το $1 \in B$, αφού $1^{\frac{n-1}{2}} \equiv \left(\frac{1}{n}\right)\ mod\ n$,$(1,n) = 1$ και $1 \in \mathbb{Z}_n^*$.
d) Κάθε στοιχείο του B έχει πολλαπλασιαστικό αντίστροφο. Έστω $l \in B$, τότε το l έχει πολλαπλασιαστικό αντίστροφο $modulo\ n$, αφου $l \in G_n$ λόγω του ότι ισχύει ότι $B \subseteq G_n$ και G_n ομάδα. Έστω $h \in G_n$ ο αντίστροφος του l, άρα $hl \equiv 1\ mod\ n$ $\Rightarrow\ (hl)^{\frac{n-1}{2}} \equiv 1\ mod\ n\ \Rightarrow\ h^{\frac{n-1}{2}} \cdot l^{\frac{n-1}{2}} \equiv 1\ mod\ n\ \Rightarrow\ h^{\frac{n-1}{2}} \cdot \left(\frac{l}{n}\right) \equiv 1 = \left(\frac{l}{n}\right)^2\ mod\ n$ $\Rightarrow h^{\frac{n-1}{2}} \equiv \left(\frac{l}{n}\right)\ mod\ n$. Όμως $hl \equiv 1\ mod\ n\ \Rightarrow \left(\frac{hl}{n}\right) = \left(\frac{1}{n}\right) = 1$ και επειδή $\left(\frac{h}{n}\right) \cdot \left(\frac{l}{n}\right) = \left(\frac{hl}{n}\right)$ έχουμε ότι $\left(\frac{l}{n}\right) = \left(\frac{h}{n}\right)$. Άρα $h^{\frac{n-1}{2}} \equiv \left(\frac{h}{n}\right)\ mod\ n$, δηλαδή $h \in B$.
e) Το B είναι κλειστό ως προς τον πολλαπλασιασμό $modulo\ n$. Έστω $u, w \in B$ τότε επειδή $B \subseteq G_n$ και G_n ομάδα, έχουμε ότι $u \cdot w \in G_n$. Μένει να δείξουμε ότι το $u \cdot w \in B$, δηλαδή ότι $(u \cdot w)^{\frac{n-1}{2}} \equiv \left(\frac{uw}{n}\right)\ mod\ n$. Όμως $(u \cdot w)^{\frac{n-1}{2}} = u^{\frac{n-1}{2}} \cdot w^{\frac{n-1}{2}} \equiv \left(\frac{u}{n}\right) \cdot \left(\frac{w}{n}\right) = \left(\frac{uw}{n}\right)\ mod\ n.$

Άρα το B είναι υποομάδα του G_n.

Θα δείξουμε ότι το G_n περιέχει τουλάχιστον ένα στοιχείο που δεν περιέχεται στο B.

Διακρίνουμε δύο περιπτώσεις:

a) Έστω ότι ο n είναι ελεύθερος τετραγώνου, δηλαδή δεν διαιρείται από το τετράγωνο κάποιου πρώτου μικρότερου του n.
Θέτουμε $n = p \cdot m$, p περιττός πρώτος και $m \geq 3$ περιττός ακέραιος με $p \nmid m$.
Έστω $b \epsilon G_n$ κάποιο μη τετραγωνικό υπόλοιπο $mod\ p$, δηλαδή $\left(\frac{b}{p}\right) = -1$. Από το Κινέζικο Θεώρημα των υπολοίπων υπάρχει $1 \leq a < n$ με $a \equiv b\ mod\ p$ (1) και $a \equiv 1\ mod\ m$ (2).
Θα δείξουμε ότι $a \in G_n$ και *a Euler-μάρτυρας* του n.
Απόδειξη ισχυρισμού

Από την σχέση (1) έχουμε ότι $a - b \equiv 0\ mod\ p \Rightarrow a - b = πολ\ p$ και επειδή $\left(\frac{b}{p}\right) = -1 \Rightarrow b \neq 0\ mod\ p \Rightarrow p \nmid b$, συμπεραίνουμε ότι $p \nmid \alpha$.
Ακόμη από τη σχέση (2) έχουμε ότι $(a, m) = 1$, διότι $a - 1 = πολ\ m$.
Συνεπώς $a \in G_n$.
Τέλος παρατηρούμε ότι $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{m}\right) = \left(\frac{b}{p}\right) \cdot \left(\frac{1}{m}\right) = \left(\frac{b}{p}\right) \cdot 1 = -1$ και $a^{\frac{n-1}{2}} \neq -1\ mod\ n$, αφού αν $a^{\frac{n-1}{2}} = -1\ mod\ n \Rightarrow a^{\frac{n-1}{2}} = -1\ mod\ m$, άτοπο λόγω της (2). Άρα $a^{\frac{n-1}{2}} \neq \left(\frac{\alpha}{n}\right)\ mod\ n$ και αυτό συμπληρώνει την απόδειξη του ισχυρισμού.
Οπότε για κάθε n ελεύθερο τετραγώνου έχουμε ότι υπάρχει $1 \leq a < n$ και *a Euler-μάρτυρας*.

b) Έστω τώρα ότι ο n δεν είναι ελεύθερος τετραγώνου και άρα υπάρχει $p \geq 3$ πρώτος με $p^2 | n$. Γράφουμε $n = p^k \cdot m$ με $k \geq 2$ ακέραιο και $p \nmid m$. Θα βρούμε a, ο οποίος είναι *Euler-μάρτυρας*.
Αν $m = 1$ τότε $a = 1 + p$, καθώς $\left(\frac{a}{n}\right) = \left(\frac{a}{p^k}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{p}\right) \cdot \ldots \cdot \left(\frac{a}{p}\right) = 1^k = 1$ και από το διωνυμικό θεώρημα

$$a^{\frac{n-1}{2}} = (1+p)^{\frac{n-1}{2}} = 1 + \binom{\frac{n-1}{2}}{1} p + \cdots + \binom{\frac{n-1}{2}}{\frac{n-1}{2}} p^{\frac{n-1}{2}} \equiv 1 + \frac{(n-1)}{2} p\ mod\ p^2$$

$\Rightarrow a^{\frac{n-1}{2}} \neq 1\ mod\ n$, δηλαδή $a^{\frac{n-1}{2}} \neq \left(\frac{\alpha}{n}\right)\ mod\ n$.
Αν $m \geq 3$ τότε από το Κινέζικο θεώρημα υπολοίπων επιλέγω το a:
$1 \leq a < p^2 \cdot m \leq n$ με $a = 1 + p\ mod\ p^2$ (3) και $a = 1\ mod\ m$ (4). Θα δείξουμε ότι ο α είναι *Euler-μάρτυρας* για το n.
Από την (4) έχουμε ότι $(a, m) = 1$ και από την (1) ότι $a - (1 + p) = πολ\ p^2$
$\Rightarrow a \neq πολ\ p$. Όμως $n = p^k\ m$, οπότε $(a, n) = 1$. Συνεπώς $a \in G_n$.

Έστω ότι ο a δεν είναι Euler-μάρτυρας για το n, δηλαδή $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \ mod\ n$.

Όμως $a^{\frac{n-1}{2}} = (1+p)^{\frac{n-1}{2}} = 1 + \binom{\frac{n-1}{2}}{1} p + \cdots + \binom{\frac{n-1}{2}}{\frac{n-1}{2}} p^{\frac{n-1}{2}} \equiv 1 + \frac{(n-1)}{2} p \ mod\ p^2$,

δηλαδή $a^{\frac{n-1}{2}} \neq 1\ mod\ n$, και $\left(\frac{a}{n}\right) = \left(\frac{a}{p^k\ m}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{p}\right) \cdot \ldots \cdot \left(\frac{a}{p}\right) \cdot \left(\frac{a}{m}\right) = 1^k \cdot 1 = 1$

, οπότε το a είναι *Euler-μάρτυρας*.

Συνεπώς G_n περιέχει ένα a, το οποίο είναι Euler-μάρτυρας και άρα δεν ανήκει στο B.

Άρα το B είναι γνήσια υποομάδα του G_n . ■

<u>Παρατήρησεις:</u>

1) Από το θεώρημα του Langrange η τάξη του B θα διαιρεί γνήσια την τάξη του G_n και επειδή $|G_n| = \varphi(n)$ έχουμε ότι $|B| \leq \frac{\varphi(n)}{2}$, δηλαδή το πολύ $\frac{\varphi(n)}{2}$ αριθμοί μικρότεροι του n και μεγαλύτεροι ή ίσοι του 1, είναι *Euler-ψεύτες.*
2) Εάν *το τεστ Solovay-Strassen* μας επιστρέψει "ο n είναι πρώτος με συντελεστή ασφαλείας t", αυτό σημαίνει ότι η πιθανότητα ο n να είναι πρώτος είναι μεγαλύτερη ή ίση από $1 - \frac{1}{2^t}$.
3) Το πλεονέκτημα του *τεστ Solovay-Strassen* έναντι του *τεστ του Fermat* είναι ότι δεν υπάρχουν αριθμοί , όπως οι *αριθμοί του Carmichael* για το *τεστ του Fermat*, για τους οποίους το τεστ δεν μπορεί να αποφανθεί αν είναι πρώτοι ή όχι ανεξάρτητα από τις επαναλήψεις t (εκτός αν πέσουμε σε α με $(a, n) \neq 1$).

2.3. ΤΟ ΤΕΣΤ MILLER-RABIN

Το *τεστ Miller-Rabin* είναι το πιθανοτικό τεστ για πιστοποίηση πρώτων που χρησιμοποιείται πιο πολύ στην πράξη σήμερα. Η πρώτη μορφή που είχε αυτό το τεστ οφείλεται στον Gary L. Miller και δεν ήταν πιθανοτικό , αλλά ντετερμινιστικό τεστ και στηριζόταν στην *γενικευμένη υπόθεση του Riemann*, η οποία δεν έχει αποδειχθεί μέχρι σήμερα. Ο Michael O. Rabin το τροποποίησε και πρότεινε το σημερινό *τεστ Miller-Rabin*, το οποίο δεν στηρίζεται στη *γενικευμένη υπόθεση του Riemann* , αλλά είναι πιθανοτικό.

Το τεστ Miller-Rabin βασίζεται στην παρακάτω πρόταση.

Πρόταση

Έστω n πρώτος, a ακέραιος ,ο οποίος δεν διαιρείται από το n και θέτουμε $n-1=2^s\,r$ με r περιττό θετικό ακέραιο και s θετικό ακέραιο. Τότε είτε ισχύει ότι $a^r=1\ mod\ n$, είτε ότι υπάρχει $u\in\{0,1,2,\dots,s-1\}$ με $a^{2^u r}\equiv -1\ mod\ n$.

Απόδειξη:

Έστω $k=ord_n(a^r)$. Από το μικρό *θεώρημα του Fermat* έχουμε ότι $(a^r)^{2^u}\equiv 1\ mod\ n$, συνεπώς $k|2^u$. Διακρίνουμε τις περιπτώσεις:

a) Έστω $k=1$, τότε $a^r\equiv 1\ mod\ n$.
b) Έστω $k>1$, τότε $k=2^l$ με $1\le l\le s$ και επομένως $ord_n\left(a^{2^{l-1}r}\right)=2$. Όμως μόνο η κλάση -1 μέσα στο $\mathbb{Z}_n^*$ έχει τάξη ίση με 2 και κατά συνέπεια έχουμε ότι $a^{2^{l-1}r}\equiv -1\ mod\ n$. ■

Ορισμοί

Έστω n ένας περιττός σύνθετος ακέραιος και $n-1=2^s\,r$, όπου r περιττός και $s\ge 0$ ακεραιος . Έστω a ακέραιος με $1\le a\le n-1$.

a) Αν $a^r\neq 1\ mod\ n$ και αν $a^{2^j r}\neq -1\ mod\ n$ για κάθε $j, 0\le j\le s-1$, τότε ο a καλείται *ισχυρός μάρτυρας* για το n.
b) Αν $a^r\equiv 1\ mod\ n$ ή $a^{2^j r}\equiv -1\ mod\ n$ για κάποιο $j, 0\le j\le s-1$, τότε ο a καλείται *ισχυρός ψεύτης* για το n και ο n καλείται *ισχυρός ψευδοπρώτος* με βάση το a.

Παράδειγμα

Έστω $n = 561 = 3 \cdot 11 \cdot 17$, άρα $n - 1 = 560 = 2^4 \cdot 35$, οπότε σύμφωνα με τον παραπάνω ορισμό $s = 4$ και $r = 35$. Για $a = 2$ έχουμε $2^{35} \equiv 263\ mod\ 561\ \rightarrow$

$263^2 \equiv 166\ mod\ 561\ \rightarrow 166^2 \equiv 67 mod\ 561\ \rightarrow 67^2 = 1\ mod\ 561$. Βλέπουμε λοιπόν ότι και $a^r \neq 1\ mod\ n$ και $a^{2^j r} \neq -1\ mod\ n$ για κάθε $j, 0 \leq j \leq s - 1$, συνεπώς ο $a = 2$ είναι *ισχυρός μάρτυρας* για το n και ο n είναι σύνθετος.

Από την άλλη έστω $n = 91 = 7 \cdot 13$, άρα $n - 1 = 90 = 2 \cdot 45, s = 1$ και $r = 45$. Για $a = 9$ έχουμε $9^{45} \equiv 1\ mod\ 91$, δηλαδή $a^r \equiv 1\ mod\ n$. Άρα ο $a = 9$ είναι *ισχυρός ψεύτης* για το 91 και ο n είναι *ισχυρός ψευδοπρώτος*.

Αλγόριθμος (Τεστ Miller-Rabin)

INPUT: ένα περιττό ακέραιο $n \geq 3$ και συντελεστή ασφάλειας $t \geq 1$.

OUTPUT: θα απαντάει στην ερώτηση "είναι ο n πρώτος;" με δυνατές απαντήσεις "ο n είναι πρώτος με συντελεστή ασφάλειας t" ," ο n είναι σύνθετος".

1. Βρες $s > 1$ και r περιττό , ώστε $n - 1 = 2^s r$.
2. For i from 1 to t
    a. Διάλεξε έναν τυχαίο ακέραιο $a, 2 \leq a \leq n - 2$.
    b. Υπολόγισε το $y = a^r\ mod\ n$.
    c. If $y \neq 1$ και $y \neq n - a$ then
        1) $j \leftarrow 1$.
        2) While $j \leq s - 1$ και $y \neq n - 1$
            a) $y \leftarrow y^2\ mod\ n$.
            b) If $y = 1$ then return("Ο n είναι σύνθετος").
            c) $j \leftarrow j + 1$.
        3) If $y \neq n - 1$ then return("Ο n είναι σύνθετος").
3. Return(" Ο n είναι πρώτος με συντελεστή ασφάλειας t").

Παρατηρήσεις

1. Ο παραπάνω αλγόριθμος είναι πιθανοτικός. Αυτό σημαίνει ότι δεν μπορούμε να είμαστε σίγουροι για όλα τα αποτελέσματα που επιστρέφει. Συγκεκριμένα αν το τεστ Miller-Rabin μας επιστρέψει "Ο n είναι σύνθετος" , τότε είμαστε βέβαιοι ότι ο n είναι σύνθετος. Αν μας επιστρέψει " Ο n είναι πρώτος με συντελεστή ασφάλειας t" σημαίνει

ότι η πιθανότητα ο n να είναι πρώτος είναι μεγαλύτερη από $1-\frac{1}{4^t}$, όπως θα δούμε και παρακάτω.

2. Η ομοιότητα του *τεστ Miller Rabin* με αυτό του *Fermat* είναι φανερή. Και τα δύο αυτά τεστ στηρίζονται στο *μικρό θεώρημα του Fermat*, με τη διαφορά ότι το τεστ Miller-Rabin χρησιμοποιεί επιπλέον την παραπάνω πρόταση. Αυτό έχει σαν αποτέλεσμα οι *αριθμοί Carmichael* να μη δημιουργούν πλέον πρόβλημα και ακόμη ότι το τεστ Miller-Rabin χρειάζεται λιγότερες επαναλήψεις t ,από το τεστ του Fermat, για να μας απαντήσει με την ίδια αξιοπιστία ,αν ένας αριθμός είναι πρώτος .

Πρόταση

Έστω $n \geq 3$ περιττός σύνθετος. Το σύνολο $\{1, \dots, n-1\}$ περιέχει το πολύ $\frac{n-1}{4}$ ακεραίους που είναι πρώτοι προς το n και δεν είναι ισχυροί μάρτυρες της συνθετότητας του.

Απόδειξη:

Θα προσδιορίσουμε το πλήθος των ακεραίων a με $(a,n)=1, 2 \leq a \leq n-1$ και $a^r \equiv 1 \; mod \; n$ ή $a^{2^s r} \equiv -1 \; mod \; n$ για $s \in \{0,1, \dots, l-1\}$, με την προϋπόθεση ότι ένα τέτοιο a υπάρχει. Με αυτό σα δεδομένο παρατηρούμε ότι πάντα θα υπάρχει ακέραιος , ο οποίος ικανοποιεί τη δεύτερη εξίσωση, αφού αν $a^r \equiv 1 \; mod \; n \Rightarrow (-a)^r \equiv -1 \; mod \; n$ ή $(-a)^{2^0 \cdot r} \equiv -1 \; mod \; n$.

Έστω k ο μεγαλύτερος ακέραιος του συνόλου $\{0,1, \dots, l-1\}$ για τον οποίο υπάρχει ακέραιος A με $(A,n)=1$ και $A^{2^k r} \equiv -1 \; mod \; n$. Θέτουμε $m = 2^k \cdot r$ και έστω

$n = {p_1}^{e_1} \dots {p_\nu}^{e_\nu}$ η πρωτογενής ανάλυση του n. Έστω το σύνολο $G_n = \{x : x \in \mathbb{Z}_n^* \; και \; (x,n)=1\}$ το οποίο είναι ομάδα. Μπορεί να διαπιστωθεί ότι τα σύνολα $J = \{x \in G_n : \; x^{n-1} \equiv 1 \; mod \; n\}$, $K = \{x \in G_n : x^m \equiv \pm 1 \; mod \; {p_i}^{e_i}, i = 1, \dots, \nu\}$, $L = \{x \in G_n : x^m \equiv \pm 1 \; mod \; n\}$ και $M = \{x \in G_n : x^m \equiv 1 \; mod \; n\}$ είναι υποσύνολα του G_n και μάλιστα ισχύει $M \subseteq L \subseteq K \subseteq J$.

Βλέπουμε ότι για κάθε $a \in G_n$, το οποίο όμως δεν είναι *ισχυρός μάρτυρας* για τη συνθετότητα του n , έχουμε ότι $a \in L$. Θα δείξουμε ότι $[G_n : L] \geq 4$.

Έστω $a \in K$, τότε $a^2 \in M$ και επομένως $[K:M] = 2^i$, για κάποιο ακέραιο $i \geq 0$. Άρα $[K:L] = 2^j, j \leq i$. Στην περίπτωση όπου $j \geq 2$, τότε η προς απόδειξη ανισότητα ισχύει.

Έστω $j = 0$, τότε $K = L$.

Για $\nu \geq 2$, υπάρχει δ τέτοιο ώστε $\delta \equiv A \; mod \; {p_1}^{e_1}$ και $\delta \equiv 1 \; mod \; {p_1}^{e_\iota}$, για $i = 2, \dots, \nu$.

Άρα $\delta^m \equiv -1 \; mod \; {p_1}^{e_1}$ και $\delta^m \equiv 1 \; mod \; {p_1}^{e_\iota}$, δηλαδή $\delta \in K$ και $\delta \notin L$, άτοπο.

Για $\nu = 1$ έχουμε ότι αν $a \in J$, τότε $ord_{{p_1}^{e_1}}(a)|p-1$. Αντιστρόφως, αν $ord_{{p_1}^{e_1}}(a)|p-1$, τότε $a \in J$. Συνεπώς το J είναι η υποομάδα τάξης $p-1$ της ομάδας $G_{{p_1}^{e_1}}$ και επομένως $\left[G_{{p_1}^{e_1}}:J\right] = {p_1}^{e_1-1}$. Για ${p_1}^{e_1} > 9$ έχουμε ότι $\left[G_{{p_1}^{e_1}}:J\right] \geq 4$. Αν ${p_1}^{e_1} = 9$, τότε $r = 1$ και $l = 3$. Από τις ισοτιμίες:

$$x \equiv 1\ mod\ 9\ , x \equiv -1\ mod\ 9\ , x^2 \equiv -1\ mod\ 9\ , x^4 \equiv -1\ mod\ 9$$

προκύπτει ότι οι μόνοι ακέραιοι του συνόλου $\{1, \dots, 8\}$ που δεν είναι ισχυροί μάρτυρες της συνθετότητας του 9 είναι οι 1 και 8.

Ας υποθέσουμε στη συνέχεια ότι $j = 1$. Τότε υπάρχει $a \in G_n$ με $L \cup aL = K$ και $a \notin L$. Για $\nu \geq 3$, χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $a^m \equiv 1\ mod\ {p_i}^{e_i},\ i = 1, \dots, s$ και $a^m \equiv -1\ mod\ {p_i}^{e_i}\ ,\ i = s+1, \dots, \nu$, με $s \geq 2$ (Αν $s = 1$, τότε αντικαθιστούμε τον a από τον aA).

Θεωρούμε έναν ακέραιο c με $c \equiv Aa\ mod\ {p_1}^{e_1},\ c \equiv 1\ mod\ {p_2}^{e_2}$, ..., $c \equiv 1\ mod\ {p_\nu}^{e_\nu}$.

Έχουμε $c \notin L \cup aL$ και κατά συνέπεια $c \notin K$ που είναι άτοπο. Άρα ο n έχει δύο μόνο πρώτους παράγοντες και επομένως δεν είναι *αριθμός Carmichael* .

Οπότε $J \neq G_n \Rightarrow [G_n:J] \geq 2$, και άρα $[G_n:L] \geq 4$. ■

<u>Παρατήρηση:</u>

Βλέπουμε λοιπόν ότι αν το n είναι περιττός σύνθετος ακέραιος, τότε το πολύ το $\frac{1}{4}$ όλων των αριθμών $a, 1 \leq a \leq n-1$, είναι *ισχυροί ψεύτες* για το n. Συγκεκριμένα , αν $n \neq 9$, ο αριθμός των ισχυρών ψευτών είναι το πολύ $\frac{\varphi(n)}{4}$, όπου φ η συνάρτηση του Euler. Δηλαδή τις περισσότερες φορές το *τεστ Miller-Rabin* μας απαντάει ότι το n είναι πρώτος με πιθανότητα πολύ μεγαλύτερη από $1 - \frac{1}{4^t}$.

2.4. ΣΥΓΚΡΙΣΕΙΣ ΤΩΝ ΤΕΣΤ FERMAT, SOLOVAY-STRASSEN ΚΑΙ MILLER-RABIN

Από αυτά τα τρία τεστ πιστοποίησης πρώτων , δε χωράει αμφιβολία ότι το τεστ Miller-Rabin είναι το καλύτερο και μάλιστα είναι αυτό που χρησιμοποιείται κατά κόρον σήμερα στην πράξη, στην κρυπτογραφία. Ας δούμε γιατί:

Έχει αποδειχτεί στα προηγούμενα ότι κάθε *Euler-ψεύτης* είναι και *Fermat-ψεύτης* .

Πρόταση

Έστω ότι ο a είναι *ισχυρός ψεύτης* για το n, τότε ο a είναι και *Euler-ψεύτης* για το n.

Απόδειξη:

Αφού ο a είναι *ισχυρός ψεύτης* για το n, έχουμε ότι $a^r \equiv 1 \, mod \, n$ ή $a^{2^j r} \equiv -1 \, mod \, n$ για κάθε $j, 0 \leq j \leq s-1$.

Αν $a^r \equiv 1 \, mod \, n \Rightarrow a^{r\,2^{s-1}} = a^{\frac{n-1}{2}} \equiv 1 \, mod \, n \Rightarrow \left(\frac{a}{n}\right) = 1$, αφού $a^{\frac{n-1}{2}} \equiv 1 \, mod \, k$ για κάθε k παράγοντα του n και $\left(\frac{a}{k_1 \cdot k_2}\right) = \left(\frac{a}{k_1}\right) \cdot \left(\frac{a}{k_2}\right)$. Άρα ο α είναι *ισχυρός μάρτυρας.*

Αν $a^r \neq 1 \, mod \, n$ και $a^{2^j r} \equiv -1 \, mod \, n$ για κάποιο $j, 0 \leq j \leq s-1$, τότε εντελώς όμοια καταλήγουμε ότι ο a είναι *ισχυρός μάρτυρας* για το n. ■

Σύμφωνα λοιπόν με τα παραπάνω μπορούμε να πούμε ότι :

Fermat-ψεύτες ⊇*Euler- ψεύτες* ⊇ *ισχυροί ψεύτες*

Συνεπώς από άποψη ακρίβειας των τεστ, το τεστ Miller-Rabin είναι καλύτερο, εκτός της περίπτωσης που $n \equiv 3 \, mod \, 4$, όπου είναι το ίδιο καλό όσο το Solovay-Strassen.

Από άποψη πολυπλοκότητας το Miller-Rabin είναι καλύτερο από το Solovay –Strassen, λόγω του ότι στο Solovay-Strassen πρέπει να υπολογιστεί το *σύμβολο του Jacobi*.

Όμως το Miller-Rabin από άποψη πολυπλοκότητας δεν είναι καλύτερο του *τεστ του Fermat* και γι' αυτό άλλωστε το τεστ του Fermat χρησιμοποιείται ακόμη στην κρυπτογραφία. Παρόλα αυτά το *τεστ του Fermat* έχει ως βασικό μειονέκτημα τους *αριθμούς Carmichael*.

3. ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΑΚΕΡΑΙΩΝ

Η εύρεση των πρώτων παραγόντων ενός ακεραίου αποτελεί ένα πάρα πολύ δύσκολο υπολογιστικά πρόβλημα. Το γεγονός αυτό είναι που ενέπνευσε άλλωστε τη δημιουργία του κρυπτοσυστήματος RSA , το οποίο με τη σειρά του πυροδότησε την έρευνα για την εύρεση αποτελεσματικών τρόπων για την επίλυση αυτού του προβλήματος και κατά συνέπεια την αποκρυπτογράφηση RSA −κρυπτογραφημένων μηνυμάτων.

Η πολυπλοκότητα του προβλήματος της παραγοντοποίησης ακεραίων ανήκει στις κατηγορίες NP και $co\text{-}NP$ και δεν γνωρίζουμε αν ανήκει στην κλάση P. Παρόλα αυτά συνεχώς ανακαλύπτονται πιο γρήγοροι και πιο αποδοτικοί αλγόριθμοι για αυτό το πρόβλημα. Ο πιο γρήγορος αλγόριθμος για τα σημερινά δεδομένα είναι $General\ Number\ Field\ Sieve\ (GNFS)$ με πολυπλοκότητα $O\left(\exp\left(\left(\frac{64}{9}b\right)^{\frac{1}{3}}(log\ b)^{\frac{2}{3}}\right)\right)$ για έναν αριθμό n με b bits.

Δεν έχουν όλοι οι αριθμοί την ίδια δυσκολία ως προς την παραγοντοποίηση. Συγκεκριμένα οι πιο δύσκολο να παραγοντοποιηθούν αριθμοί , με τις σημερινές τεχνικές , είναι αυτοί που αποτελούνται από το γινόμενο δύο μεγάλων πρώτων. Το ρεκόρ παραγοντοποίησης τέτοιου είδους αριθμών είναι η παραγοντοποίηση του $RSA\text{-}768$ με 232 δεκαδικά ψηφία. Η προσέγγιση έγινε με το $GNFS$.

Στο παρόν κείμενο εξετάζουμε τους αλγορίθμους $Fermat, Pollard\ Rho,\ Dixon$ και $Quadratic\ Sieve$.

3.1. Η ΜΕΘΟΔΟΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΤΟΥ FERMAT

Η μέθοδος αυτή στηρίζεται στο να εκφραστεί ο αριθμός n που θέλουμε να παραγοντοποιήσουμε σαν διαφορά δύο τέλειων τετραγώνων. Οπότε αν το πετύχουμε αυτό, θα έχουμε ότι $n = a^2 - b^2 \Rightarrow n = (a-b)\cdot(a+b)$ και αν ακόμη $(a-b) > 1$, τότε η παραγοντοποίηση θα αποτελείται από μη τετριμμένους παράγοντες . Μάλιστα αν το n είναι περιττός σύνθετος, τότε όλοι οι παράγοντες του μπορούν να βρεθούν με αυτόν τον τρόπο, αφού αν $n = u \cdot v$ τότε με $a = \frac{1}{2}(u+v)$ και $b = \frac{1}{2}|u-v|$, έχουμε τη ζητούμενη διαφορά τετραγώνων.

Η *μέθοδος παραγοντοποίησης του Fermat* έχει ως εξής. Ξεκινώντας από τον αριθμό $a = \lceil \sqrt{n} \rceil$ παίρνουμε το $b^2 = n - a^2$, τότε αν το b είναι ακέραιος και αν η διαφορά $a^2 - b^2$ μας δώσει μη τετριμμένο παράγοντα του n έχουμε τελειώσει. Διαφορετικά παίρνουμε $a = \lceil \sqrt{n} \rceil + 1$, $a = \lceil \sqrt{n} \rceil + 2$, κλπ. Έτσι αν ο αριθμός n είναι περιττός και σύνθετος, η διαδικασία θα μας δώσει μη τετριμμένο παράγοντα για $a \leq \frac{(n+9)}{6}$. Η χειρότερη περίπτωση προκύπτει για $n = 3p$, p πρώτο, καθώς μια μη τετριμμένη παραγοντοποίηση θα προκύψει μόνο για $a = \frac{(n+9)}{6}$.

Αλγόριθμος(Μέθοδος παραγοντοποίησης Fermat)

INPUT: ένα περιττό ακέραιο > 1 .

OUTPUT: θα επιστρέφει είτε έναν μη τετριμμένο παράγοντα του n ,είτε ότι ο n είναι πρώτος.

1. $a = \lceil \sqrt{n} \rceil$
2. While $a \leq \frac{n+9}{6}$ do
    a. $b = \sqrt{a^2 - n}$
    b. if b ακέραιος και $a - b \neq 1$ return "$a - b$"
    c. $a \leftarrow a + 1$
3. return " ο n είναι πρώτος"

Η παραπάνω μέθοδος είναι πολύ πιο αργή , στη χειρότερη περίπτωση , ακόμη και από το κόσκινο του Ερατοσθένη. Παρόλα αυτά βλέπουμε ότι αν το n έχει δύο παράγοντες πολύ κοντά στο $\sqrt{n}$, η *παραγοντοποίηση του Fermat* είναι πολύ πιο αποτελεσματική από το *κόσκινο του Ερατοσθένη*. Αυτός είναι και ο λόγος που χρησιμοποιούμε ένα πολλαπλασιαστή για να κάνουμε το τεστ του Fermat πιο αποτελεσματικό, δηλαδή αν για μερικές επαναλήψεις δεν βρούμε τετριμμένο παράγοντα για το n , πολλαπλασιάζουμε το n με ένα μικρό φυσικό i και αυξάνουμε τις πιθανότητες έτσι ο in να έχει κάποιο μη τετριμμένο παράγοντα κοντά στο $\sqrt{in}$. Έτσι στη συνέχεια παίρνουμε το μέγιστο κοινό διαιρέτη του παράγοντα που βρήκαμε με το n.

<u>Παραδείγματα</u>

Έστω $n = 26563\ (= 101 \cdot 263)$. Σύμφωνα με τη μέθοδο του Fermat ξεκινάμε και έχουμε

$\lceil\sqrt{26563}\rceil = 163$

$a^2 = 163^2 = 26569,\ b^2 = 26569 - 26563 = 6$

$a^2 = 164^2 = 26896,\ b^2 = 26896 - 26563 = 333$

$\vdots$

$a^2 = 182^2 = 33124,\ b^2 = 33124 - 26563 = 6561\ \Rightarrow\ b = 81$

Άρα $182^2 - 81^2 = 26563\ \Rightarrow\ 26563 = (182 - 81) \cdot (182 + 81) = 101 \cdot 263$

Βλέπουμε λοιπόν ότι η κλασσική μέθοδος του Fermat μας έδωσε αποτέλεσμα μετά από 20 επαναλήψεις.

Έστω $n = 3811(= 103 \cdot 37)$. Σε αυτό το παράδειγμα η απλή μέθοδος του Fermat θα μας επιστρέψει αποτέλεσμα μετά από 9 επαναλήψεις, ενώ αν χρησιμοποιήσουμε πολλαπλασιαστή 3 έχουμε:

$3n = 11433$

$\lceil\sqrt{11433}\rceil = 107$

$a^2 = 107^2 = 11449,\ b^2 = 11449 - 11433 = 16\ \Rightarrow b = 4$

Άρα $107^2 - 4^2 = 11433\ \Rightarrow\ 11433 = (107 - 4) \cdot (107 + 4) = 103 \cdot 111$

$n = \frac{103 \cdot 111}{3} = 103 \cdot 37$

Βλέπουμε λοιπόν πόσο επιταχύνθηκε η διαδικασία με τη χρήση του πολλαπλασιαστή.

Σχόλιο

Η μέθοδος του Fermat μπορεί να βελτιωθεί κι άλλο με διάφορους τρόπους, όπως το να ψάχνουμε για τετράγωνα σε κάποιο modulo, το σημαντικό όμως είναι να δούμε την αρχή λειτουργίας αυτής της μεθόδου καθώς είναι η βάση ακόμη και για τις πιο σύγχρονες και γρήγορες μεθόδους παραγοντοποίησης, όπως είναι τα quadratic sieve και number field sieve.

3.2. Ο ΑΛΓΟΡΙΘΜΟΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΤΟΥ DIXON

Η μέθοδος του Dixon,για την παραγοντοποίηση ενός αριθμού n, βασίζεται , όπως και η μέθοδος του Fermat, στην εύρεση ακεραίων a, b με $a^2 \equiv b^2 \, mod \, n$ και $a \neq \pm b \, mod \, n$.

Έτσι θα έχουμε ότι $a^2 - b^2 \equiv 0 \, mod \, n \Rightarrow (a-b)(a+b) = k \cdot n \Rightarrow n|(a-b)(a+b)$, χωρίς το $(a-b)$ ή το $(a+b)$ να διαιρείται από το n , αφού $a \neq \pm b \, mod \, n$. Οπότε έχουμε ότι ο αριθμός $(a-b, n)$ είναι ένας μη τετριμμένος παράγοντας για το n. Η διαφορά της μεθόδου Dixon είναι ότι χρησιμοποιεί μια *βάση παραγοντοποίησης*, η οποία θα εξηγήσουμε τι είναι και πως δουλεύει παρακάτω.

Ορισμοί

Ορίζουμε *βάση παραγοντοποίησης* για τη μέθοδο Dixon ένα σύνολο $B = \{-1, p_1, p_2, \dots, p_h\}$, με p_i διακεκριμένοι πρώτοι $modulo \, n$ και $-1 \equiv n - 1 \, mod \, n$.

Ο ακέραιος n καλείται *B-λείος* αν δεν έχει πρώτους παράγοντες μεγαλύτερους του B. (Επίσης σε μερικές περιπτώσεις ονομάζουμε έναν ακέραιο n $B-λείο$, αν όλοι οι πρώτοι παράγοντες του βρίσκονται μέσα σε ένα σύνολο B.)

Ο ακέραιος x καλείται *B-προσαρμοσμένος* ως προς τον φυσικό n, αν ο ακέραιος c, με $-\frac{n}{2} \leq c \leq \frac{n}{2}$ και $x^2 \equiv c \; mod \; n$, είναι *B-λείος*.

Παράδειγμα

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

Επίσης ο $71 \rightarrow 71^2 = 63 \; mod \; 2849$, $-\frac{2849}{2} \leq 63 \leq \frac{2849}{2}$ είναι $7 - προσαρμοσμένος$ ως προς τον 2849.

Θα σκιαγραφήσουμε τώρα τον αλγόριθμο του Dixon. Για δοθέν n και για δοθείσα βάση παραγοντοποίησης B, όπως ορίστηκε παραπάνω, ο αλγόριθμος του Dixon ψάχνει αριθμούς, έστω x, κοντά στο $\lfloor \sqrt{n} \rfloor$, για τους οποίους ισχύει, ότι όλοι οι πρώτοι παράγοντες του $x^2 \; mod \; n$ υπάρχουν μέσα στο σύνολο B. Στη συνέχεια παίρνει το γινόμενο κάποιων x , έτσι ώστε ο αριθμός των φορών που χρησιμοποιείται κάθε πρώτος της βάσης B, να είναι άρτιος. Κάνοντας αυτά καταλήγει σε μια σχέση του τύπου $x^2 \equiv y^2 \; mod \; n$, από την οποία ελπίζουμε ότι θα πάρουμε μια μη τετριμμένη παραγοντοποίηση του n.

Παράδειγμα

Έστω $n = 849239$ και η βάση παραγοντοποίησης $B = \{-1,2,3,5,7,11,13,17\}$.

Έχουμε ότι $\lfloor \sqrt{n} \rfloor = 921$.

$921^2 = -998 \equiv 2 \cdot 499 \; mod \; 849239$

$922^2 \equiv 845 = 5 \cdot 13^2 \; mod \; 849239 \qquad \surd$

$\vdots$

$933^2 \equiv 21250 = 2 \cdot 5^4 \cdot 17 \; mod \; 849239 \qquad \surd$

$934^2 \equiv 23117 \; mod \; 849239$

$\vdots$

$937^2 \equiv 28730 = 2 \cdot 5 \cdot 13^2 \cdot 17 \; mod \; 849239 \; \surd$

Οι αριθμοί που είναι τσεκαρισμένοι αναλύονται σε πρώτους παράγοντες μόνο από πρώτους της βάσης B.

Παρατηρούμε το εξής $(922 \cdot 933 \cdot 937)^2 = 2^2 \cdot 5^6 \cdot 13^4 \cdot 17^2 = (2 \cdot 5^3 \cdot 13^2 \cdot 17)^2$ και επειδή $922 \cdot 933 \cdot 937 \equiv 103951 \; mod \; 849239$ και $2 \cdot 5^3 \cdot 13^2 \cdot 17 = 718250$, έχουμε ότι $103951^2 \equiv 718250^2 \; mod \; 849239$. Οπότε από το μέγιστο κοινό διαιρέτη

$$(103951 - 718250,849239) = (614299,849239) = 691$$

$$(103951 + 718250,849239) = (822201,849239) = 1229$$

Συνεπώς βλέπουμε ότι με την παραπάνω μέθοδο βρήκαμε δύο μη τετριμμένους παράγοντες του 849239, που είναι το 691 και το 1229.

Το παραπάνω παράδειγμα εξηγεί τη βάση πάνω στην οποία δουλεύει η μέθοδος του Dixon, όμως έχουν παραλειφθεί κάποιες τεχνικές λεπτομέρειες, οι οποίες θα φανούν καλύτερα αφού παρουσιάσουμε τον αλγόριθμο του Dixon.

Αλγόριθμος(Μέθοδος παραγοντοποίησης Dixon)

INPUT: ένα περιττό ακέραιο $n \geq 3$ και μια βάση παραγοντοποίησης $B = \{-1,2,3, \dots, p_k\}$.

OUTPUT: θα επιστρέφει έναν μη τετριμμένο παράγοντα του n.

1. Υπολόγισε το $m = \lfloor \sqrt{n} \rfloor$.
2. (Βρες $k+1$ ζευγάρια $(a_i, a2_i)$. Οι τιμές w επιλέγονται με τη σειρά $0, \pm 1, \pm 2, \dots$)

   $i \leftarrow 1$

   While $i \leq k+1$
   a. Υπολόγισε το $a2 = (m+w)^2 \; mod \; n$ και έλεγξε με διαδοχικές διαιρέσεις αν είναι $B - \lambda \epsilon \acute{\iota} o \varsigma$. Αν όχι επέλεξε το επόμενο w και επανέλαβε το 2a.
   b. If $a2$ είναι $B - \lambda \epsilon \acute{\iota} o \varsigma$ με $a2 = \prod_{j=1}^{k} {p_j}^{e_{ij}}$ then

      i. $a_i \leftarrow m + w, \; a2_i \leftarrow a2$ και $v_i = (v_{i1}, v_{i2}, \dots, v_{ik})$, όπου $v_{ij} = e_{ij} \; mod \; 2$ για $1 \leq j \leq k$.

   c. $i \leftarrow i + 1$.
3. Χρησιμοποιώντας μεθόδους γραμμικής άλγεβρας βρες ένα μη κενό υποσύνολο $T \subseteq \{1,2, \dots, k+1\}$ τέτοιο ώστε $\sum_{i \in T} v_i = 0$ στο $\mathbb{Z}_2$.
4. Υπολόγισε το $x = \prod_{i \in T} a_i \; mod \; n$.
5. Για κάθε j, $1 \leq j \leq k$, υπολόγισε το $l_j = \frac{\sum_{i \in T} e_{ij}}{2}$.
6. Υπολόγισε το $y = \prod_{j=1}^{k} {p_j}^{l_j} \; mod \; n$.
7. If $x \equiv \pm y \; mod \; n$ then βρες ένα άλλο μη κενό υποσύνολο $T \subseteq \{1,2, \dots, k+1\}$ τέτοιο ώστε $\sum_{i \in T} v_i = 0$ και πήγαινε στο βήμα 4. (Στην περίπτωση που δεν υπάρχει

τέτοιο υποσύνολο T ,πήγαινε στο βήμα 2, βρές μερικά ακόμη $(\alpha_\iota, \alpha 2_\iota)$ ζευγάρια, αντικατέστησε τα στα ήδη υπάρχοντα και πήγαινε στο βήμα 3.

8. Υπολόγισε το $d = (x - y, n)$.
9. Return d.

Όπως βλέπουμε στον παραπάνω αλγόριθμο, ψάχνουμε ένα μη κενό υποσύνολο $T \subseteq \{1,2, \dots, k+1\}$ τέτοιο ώστε $\sum_{i \in T} v_i = 0$ στο $\mathbb{Z}_2$. Συνεπώς ψάχνουμε μια γραμμική εξάρτηση μεταξύ των v_i διανυσμάτων, κάτι που μπορούμε να βρούμε εύκολα μέσω της μεθόδου απαλοιφής του Gauss, αφού $k \leq k+1$. Με αυτόν τον τρόπο βρίσκουμε ουσιαστικά , ποια a_i πρέπει να πολλαπλασιάσουμε ώστε να καταλήξουμε σε ένα τέλειο τετράγωνο.

Σημαντικό για τον παραπάνω αλγόριθμο είναι να παρατηρήσουμε ότι μπορεί να υλοποιηθεί εύκολα με παράλληλη επεξεργασία , αναθέτοντας σε κάθε επεξεργαστή διαφορετική τιμή του w.

3.3. Η ΜΕΘΟΔΟΣ QUADRATIC SIEVE Η QS (ΤΕΤΡΑΓΩΝΙΚΟ ΚΟΣΚΙΝΟ)

Η μέθοδος Quadratic Sieve είναι μέχρι σήμερα η πιο γρήγορη μέθοδος παραγοντοποίησης για αριθμούς μέχρι 110 ψηφίων και η δεύτερη γενικά πιο γρήγορη μέθοδος παραγοντοποίησης μετά το Number Field Sieve. Οφείλεται στον Carl Pomerance το 1981 και πρόκειται ουσιαστικά για μια βελτίωση της μεθόδου Dixon.

Η διαφορά του Quadratic Sieve (QS) από τη μέθοδο του Dixon είναι ότι χρησιμοποιεί μια μέθοδο, παρόμοια με αυτή του Κόσκινου του Ερατοσθένη (εξού και η ονομασία Quadratic Sieve), για να βρίσκει πιο γρήγορα λείους αριθμούς , όπως αυτοί ορίστηκαν στη μέθοδο του Dixon.

Τρόπος λειτουργίας

Έστω ότι θέλουμε να βρούμε έναν παράγοντα του αριθμού n. Η ιδέα πίσω από το QS , όπως και με τη μέθοδο του Dixon, είναι ότι προσπαθούμε να βρούμε αριθμούς a, b, έτσι ώστε $a^2 \equiv b^2 \; mod \; n$. Με αυτόν τον τρόπο θα έχουμε ότι $(a-b)(a+b) = πολ \; n$ και έτσι είναι πολύ πιθανό ο μέγιστος κοινός διαιρέτης του $(a-b)$ ή του $(a+b)$ με το n να δώσει ένα μη τετριμμένο παράγοντα του n. Για να το καταφέρουμε αυτό, ψάχνουμε τετράγωνα αριθμών $mod \; n$, τα οποία αναλύονται σε μικρούς πρώτους παράγοντες, με πρώτους που βρίσκονται μέσα στη βάση παραγοντοποίησης , την οποία θα ορίσουμε παρακάτω για το QS. Τα τετράγωνα αυτά προσπαθούμε να είναι όσο το δυνατόν μικρότερα $mod \; n$, καθώς έτσι αυξάνονται οι πιθανότητες να αναλύονται σε μικρούς μόνο πρώτους παράγοντες. Συγκεκριμένα στο QS εξετάζουμε αριθμούς της μορφής $\left(x + \lceil \sqrt{n} \rceil\right)^2 - n$, με το x να είναι ένας μικρός ακέραιος. Ο αριθμός αυτός είναι αρκετά μικρός $mod \; n$, αφού $\left(x + \lceil \sqrt{n} \rceil\right)^2 - n \approx x^2 + 2x\sqrt{n}$. Έτσι έχοντας βρει αρκετά τέτοια τετράγωνα βρίσκουμε έναν συνδυασμό τους , έτσι ώστε να προκύψει μια παρόμοια σχέση όπως αυτή παραπάνω με τα a, b.

Για παράδειγμα έστω ότι θέλουμε να βρούμε έναν παράγοντα του αριθμού 583. Παρατηρούμε ότι $25^2 \equiv 42 = 2 \cdot 3 \cdot 7 \; mod \; 583$ και $31^2 \equiv 378 = 2 \cdot 3^3 \cdot 7 \; mod \; 583$, οπότε $(31 \cdot 25)^2 = 775^2 \equiv 192^2 \equiv 2^2 \cdot 3^4 \cdot 7^2 = (2 \cdot 3^2 \cdot 7)^2 = 126^2 \; mod \; 583$,δηλαδή $192^2 \equiv 126^2 \; mod \; 583$, η σχέση που ζητούσαμε. Άρα $(192-126)(192+126) = πολ 583$ $\Rightarrow \; 66 \cdot 318 = πολ \; 583$, από όπου προκύπτει ότι το 11 διαιρεί το $583 (= 11 \cdot 53)$.

Το ερώτημα στο παραπάνω παράδειγμα είναι πως βρήκαμε αποδοτικά το 25 και το 31. Σύμφωνα με τη μέθοδο του Dixon θα δοκιμάζαμε όλους τους αριθμούς από το $\lfloor \sqrt{583} \rfloor = 24$ μέχρι το 31. Η διαφορά του QS είναι ότι χρησιμοποιεί έναν πολύ πιο αποτελεσματικό τρόπο, ο οποίος ονομάζεται sieving (κοσκίνισμα) και θα τον αναλύσουμε παρακάτω.

Πρώτα όμως ας ορίσουμε τη βάση παραγοντοποίησης για το QS, καθώς ο λόγος που θα την ορίσουμε με αυτόν τον τρόπο θα φανεί στην ανάλυση του κοσκινίσματος.

Ορισμός

Ορίζουμε *βάση παραγοντοποίησης* για τη μέθοδο Quadratic Sieve το σύνολο $B = \{p : p \; πρώτος \; , p \leq B \; και \; \left(\frac{n}{p}\right) = 1\}$.

Κοσκίνισμα

Οι αριθμοί όπως είπαμε που εξετάζει το QS είναι της μορφής $\left(x+\lceil\sqrt{n}\rceil\right)^2-n$ και ψάχνουμε ποιοι από αυτούς τους αριθμούς διαιρούνται αποκλειστικά με πρώτους της βάσης παραγοντοποίησης. Το κοσκίνισμα έγκειται στο να βρούμε όλους τους αριθμούς της μορφής $\left(x+\lceil\sqrt{n}\rceil\right)^2-n$ που διαιρούνται με τον p_1 πρώτο της βάσης, δηλαδή $\left(x+\lceil\sqrt{n}\rceil\right)^2-n\equiv 0\ mod\ p_1$, μετά με τον p_2, κλπ. Συνδυάζοντας όλες αυτές τις ισοτιμίες θα πάρουμε αριθμούς που διαιρούνται με όλους ή με κάποιους αριθμούς της βάσης παραγοντοποίησης και αυτοί με τη σειρά τους που διαιρούνται με τους περισσότερους αριθμούς της βάσης θα είναι και πιο πιθανό να είναι λείοι. Στους πρώτους της βάσεις που εφαρμόζουμε το κοσκίνισμα μπορούμε να προσθέσουμε και κάποιες δυνάμεις τους ώστε να βελτιώσουμε την ακρίβεια.

<u>Σχόλια και παρατηρήσεις για το Κοσκίνισμα</u>

1. Σημαντικό είναι να παρατηρήσουμε ότι $\left(x+kp+\lceil\sqrt{n}\rceil\right)^2-n\equiv\left(x+\lceil\sqrt{n}\rceil\right)^2-n\ mod\ p$, με p πρώτο και k ακέραιο. Άρα σε κάθε x αντιστοιχεί μια ολόκληρη οικογένεια από αριθμούς που απέχουν p μεταξύ τους.
2. Ακόμη βλέπουμε γιατί στον ορισμό της βάσης παραγοντοποίησης βάλαμε και τη συνθήκη $\left(\frac{n}{p}\right)=1$, καθώς λύνουμε ισοτιμίες της μορφής $\left(x+\lceil\sqrt{n}\rceil\right)^2-n\equiv 0\ mod\ p\ \Rightarrow\ n\equiv\left(x+\lceil\sqrt{n}\rceil\right)^2\ mod\ p\ \Rightarrow\left(\frac{n}{p}\right)=1$.

Ας δούμε ένα παράδειγμα για το πώς λειτουργεί το κοσκίνισμα.

<u>Παράδειγμα</u>

Έστω ότι θέλουμε να βρούμε ένα μη τετριμμένο παράγοντα του αριθμού $n=583$ του προηγούμενου παραδείγματος. Η βάση παραγοντοποίησης που θα χρησιμοποιήσουμε θα είναι η $B=\{2,3,7\}$, οι οποίοι είναι οι μόνοι πρώτοι αριθμοί μέχρι το 19 για τους οποίους το 583 είναι τετραγωνικό υπόλοιπο.

$\lceil\sqrt{583}\rceil=24$

$(x+24)^2-583\equiv 0\ mod\ 2\ \Rightarrow x\equiv 1\ mod\ 2$, άρα για $x=1+2k$, ο $(x+24)^2-583$ διαιρείται με το 2.

$(x+24)^2-583\equiv 0\ mod\ 3\ \Rightarrow x=1+3k$ ή $x=2+3k$.

$(x+24)^2 - 583 \equiv 0\ mod\ 7\ \Rightarrow x = 1 + 7k$ ή $x = 0 + 7k$

Σχηματίζουμε τον παρακάτω πίνακα

X	1	2	3	4	5	6	7	8	9	10
$(x+24)^2 - 583$	42	93	146	201	258	317	378	441	506	573
διαρ. με 2	21	93	73	201	129	317	189	441	253	573
διαρ. με 3	7	31	73	67	43	317	63	147	253	191
διαρ. με 7	1	31	73	67	43	317	9	21	253	191

Βλέπουμε λοιπόν ότι μετά τις διαδοχικές διαιρέσεις, για $x = 1$ και $x = 7$ η ποσότητα $(x+24)^2 - 583$ έχει πάρει τις ελάχιστες τιμές της, 1 και 9 αντίστοιχα. Συνεπώς για $x = 1$ και $x = 7$ έχουμε τις περισσότερες πιθανότητες να πετύχουμε λείους αριθμούς. (Για $x = 1$ σίγουρα έχουμε πετύχει έναν λείο αριθμό)

Οπότε έχουμε

$x = 1$: $(1+24)^2 - 583 = 42 = 2 \cdot 3 \cdot 7$

$x = 7$: $(7+24)^2 - 583 = 378 = 2 \cdot 3^3 \cdot 7$, οι οποίοι είναι λείοι αριθμοί

και συνεχίζουμε όπως στο προηγούμενο παράδειγμα.

Όπως βλέπουμε η διαδικασία αυτή είναι αρκετά χρονοβόρα για αριθμούς μικρούς όπως το 583 είναι όμως αρκετά αποδοτική για μεγάλους ακεραίους, πχ 100 ψηφίων.

Αλγόριθμος(Quadratic Sieve)

INPUT: ένα περιττό ακέραιο $n \geq 3$,ο οποίος δεν είναι πρώτος.

OUTPUT: θα επιστρέφει έναν μη τετριμμένο παράγοντα d του n.

1. Η βάση παραγοντοποίησης $B = \{p_1, p_2, \dots, p_t\}$, όπου $p_1 = 2$ και $p_j (j > 2)$ είναι ο j −πρώτος, για τον οποίο το n είναι τετραγωνικό υπόλοιπο.
2. $a_1 \leftarrow 1$.
3. For$(2 \leq i \leq t)$ βρες ρίζες $\pm a_i$ της ισοτιμίας $a_i{}^2 \equiv n\ mod\ p_i$.
4. Εφάρμοσε το κοσκίνισμα στην ακολουθία $x^2 - n$, με $x = \lceil \sqrt{n} \rceil$, $\lceil \sqrt{n} \rceil + 1$, … για να βρεις $t+1$ διαφορετικά ζευγάρια $(x, x^2 - n)$, με $x^2 - n \quad B - \lambda\epsilon\acute{\iota}o$ και βάλτα στο σύνολο S.
5. For $((x, x^2 - n) \in S)$
    a. Βρες την παραγοντοποίηση του $x^2 - n = \prod_{i=1}^{t} p_i{}^{e_i}$.
    b. $\vec{v}(x^2 - n) \leftarrow (e_1, e_2, \dots, e_t)$.

6. Δημιούργησε έναν πίνακα $(t+1) \times t$, με γραμμές τα στοιχεία του v για τα διάφορα $x^2 - n$, υπολογισμένα όμως $modulo\ 2$.
7. Χρησιμοποίησε αλγορίθμους γραμμικής άλγεβρας, πχ μέθοδο απαλοιφής Gauss, για να βρεις ένα μη τετριμμένο σύνολο των γραμμών του πίνακα , του οποίου το άθροισμα των στοιχείων να κάνει μηδέν, έστω $\vec{v}(x_1) + \vec{v}(x_2) + \cdots + \vec{v}(x_t) = \vec{0}$.
8. Θέσε $x \leftarrow x_1 x_2 \cdot \ldots \cdot x_t \ mod\ n$.
9. $y \leftarrow \sqrt{({x_1}^2 - n)({x_2}^2 - n) \cdot \ldots \cdot ({x_t}^2 - n)}$, η ρίζα θα προκύψει άμεσα από το ότι γνωρίζουμε την παραγοντοποίηση του τέλειου τετραγώνου $({x_1}^2 - n)({x_2}^2 - n) \cdot \ldots \cdot ({x_t}^2 - n)$.
10. Υπολόγισε το $d = (x - y, n)$.
11. Return d.

<u>Παρατηρήσεις:</u>

1. Βλέπουμε ότι ο αλγόριθμος έχει ως είσοδο έναν περιττό, οποίος δεν είναι πρώτος. Το αν είναι πρώτος ή όχι αυτός ο αριθμός μπορεί να ελεγχθεί με ένα τεστ πιστοποίησης πρώτου, πχ *Miller-Rabin*.
2. Γενικότερα ο παραπάνω αλγόριθμος είναι εντελώς παρόμοιος με αυτόν της μεθόδου Dixon , με τη μόνη διαφορά να είναι στη διαδικασία του κοσκινίσματος και στην εύρεση των λείων αριθμών.
3. Μπορούμε να βελτιώσουμε την υπολογιστική πολυπλοκότητα του παραπάνω αλγορίθμου, αν επιλέξουμε $t \approx L_n[\frac{1}{2}, \frac{1}{2}]$, κάτι που προκύπτει από τη θεωρία για την κατανομή των λείων αριθμών κοντά στο $\sqrt{n}$.
4. Με τη βελτίωση της 3ης παρατήρησης η υπολογιστική πολυπλοκότητα του QS είναι $L_n\left[\frac{1}{2}, \frac{1}{2}\right]$, όπου γενικά $L_q[a, c] = O\left(\exp\left(\left(c + O(1)\right)(\ln q)^a (\ln \ln q)^{1-a}\right)\right)$.

3.4. Ο ΑΛΓΟΡΙΘΜΟΣ POLLARD RHO

Ο αλγόριθμος παραγοντοποίησης Pollard Rho, οφείλεται στον John Pollard το 1975 και είναι ένας εξαιρετικά αποδοτικός αλγόριθμος για την παραγοντοποίηση αριθμών με μικρούς πρώτους παράγοντες.

Έστω μια τυχαία συνάρτηση $f: S \to S$, με $S = \{0,1, \dots, l-1\}$ και $s \in S$ ένα τυχαίο στοιχείο του S, σχηματίζουμε την ακολουθία

$$s, f(s), f\big(f(s)\big), \dots$$

Αφού η f παίρνει τιμές από ένα πεπερασμένο σύνολο, είναι φανερό ότι η παραπάνω ακολουθία κάποια στιγμή θα αρχίσει να επαναλαμβάνεται και θα γίνει κυκλική. Όπως θα δούμε παρακάτω σε αυτό στηρίζεται ο συγκεκριμένος αλγόριθμος και μάλιστα έτσι πήρε και το όνομα του , αφού αν σκεφτούμε σχηματικά αυτήν την ακολουθία σχηματίζει το ελληνικό γράμμα ρ , με τον κύκλο στο ρ να είναι η ακολουθία που επαναλαμβάνεται.

Έστω τώρα ότι έχουμε το σύνολο $S = \{0,1, \dots, p-1\}$, με p πρώτο αριθμό, και τη συνάρτηση $f(x) = x^2 + 1 \; mod \; p$. Από το παράδοξο των γενεθλίων από τις πιθανότητες, το οποίο θα αναλύσουμε αργότερα, έχουμε ότι αν η $f(x)$ είναι αρκετά "τυχαία" , τότε η ακολουθία $(f^{(i)}(s))$ θα αρχίσει να επαναλαμβάνεται μετά από ένα τυχαίο στοιχείο $s \in S$, μετά από $O(\sqrt{p})$ βήματα. Δηλαδή θα υπάρχουν j, k , $0 \leq j < k = O(\sqrt{p})$ με $f^{(j)}(s) = f^{(k)}(s)$.

Ας υποθέσουμε τώρα το ζητούμενο, δηλαδή ότι θέλουμε να παραγοντοποιήσουμε έναν αριθμό n, και p ο ελάχιστος πρώτος παράγοντας του n. Έστω $F(x) = x^2 + 1 \; mod \; n$, από όπου προφανώς $f(x) = F(x) \; mod \; p$ και άρα $F^{(j)}(s) \equiv F^{(k)}(s) \; mod \; p$. Συνεπώς έχουμε ότι το $\big(F^{(j)}(s) - F^{(k)}(s), n\big)$ διαιρείται από το p, αφού ο p πρώτος. Αν $\big(F^{(j)}(s) - F^{(k)}(s), n\big) \neq n$, τότε θα έχουμε έναν μη τετριμμένο παράγοντα του n.

Ουσιαστικά αυτή είναι η ιδέα πίσω από τη μέθοδο Pollard Rho με μια ακόμη προσθήκη, τον αλγόριθμο του Floyd για την εύρεση κύκλων. Όπως καταλαβαίνουμε αν ψάχναμε όλα τα ζευγάρια j, k με $0 \leq j < k$ και υπολογίζαμε το $\big(F^{(j)}(s) - F^{(k)}(s), n\big)$, ο Pollard Rho θα ήταν πιο χρονοβόρος και από το κόσκινο του Ερατοσθένη. Εδώ είναι που φαίνεται η χρησιμότητα της μεθόδου του Floyd. Έστω $l = k - j$, για κάθε $m \geq j$ έχουμε ότι

$F^{(m)}(s) \equiv F^{(m+l)}(s) \equiv F^{(m+2l)}(s) \equiv \cdots \; mod \; p$. Άρα αν υποθέσουμε ότι το m είναι ένα πολλαπλάσιο του l μεγαλύτερο του j, καταλήγουμε στη σχέση $F^{(m)}(s) \equiv F^{(2m)}(s) \; mod \; p$ και $m \leq k$.

Συνεπώς η βασική ιδέα της μεθόδου Pollard Rho είναι να υπολογίζουμε τους όρους της ακολουθίας $\big(F^{(i)}(s) - F^{(2i)}(s)\,, n\big)$ και αυτό κατά πάσα πιθανότητα θα μας επιστρέψει έναν μη τετριμμένο παράγοντα του n σε $O\big(\sqrt{p}\big)$ βήματα, όπου p, ο μικρότερος πρώτος διαιρέτης του n.

Αλγόριθμος(Μέθοδος παραγοντοποίησης Pollard Rho)

INPUT: ένας σύνθετος ακέραιος n, ο οποίος δεν είναι πρώτος.

OUTPUT: θα επιστρέφει έναν μη τετριμμένο παράγοντα d του n.

1. Θέσε $a \leftarrow 2, b \leftarrow 2$.
2. For $i = 1,2, \dots$
    a. Υπολόγισε $a \leftarrow a^2 + 1 \; mod \; n, b \leftarrow b^2 + 1 \; mod \; n, \; b \leftarrow b^2 + 1 \; mod \; n$.
    b. Υπολόγισε το $d = (a - b, n)$.
    c. If $1 < d < n$ then return(d) και τερμάτισε το πρόγραμμα με επιτυχία.
    d. If $d = n$ then τερμάτισε το πρόγραμμα με αποτυχία.

Παράδειγμα

Έστω $n = 1261 (= 13 \cdot 97)$. Θα εφαρμόσουμε τον αλγόριθμο Pollard Rho.

$a \leftarrow 2, a \leftarrow 2^2 + 1 \; mod \; 1261 = 5 \quad , \quad b \leftarrow 2, \; b \leftarrow 5, \; b \leftarrow 5^2 + 1 \; mod \; 1261 = 26.$

$d = (5 - 26,1261) = 1$

$a \leftarrow 26, b \leftarrow 26^2 + 1 \; mod \; 1261 = 677, b \leftarrow 677^2 + 1 \; mod \; 1261 = 587.$

$d = (26 - 587,1261) = 1.$

$a \leftarrow 677, b \leftarrow 587^2 + 1 \; mod \; 1261 = 317, b \leftarrow 317^2 + 1 \; mod \; 1261 = 871.$

$d = (677 - 871,1261) = 97.$

Οπότε ο αλγόριθμος βρήκε έναν μη τετριμμένο παράγοντα του 1261, το 97 και τον επιστρέφει. Η διαδικασία τελείωσε σε 3 βήματα.

<u>Παρατηρήσεις :</u>

1. Για τον υπολογισμό των a, b όπως είδαμε , χρησιμοποιήσαμε συνάρτηση της μορφής $f(x) = x^2 + 1 \; mod \; n$. Η συνάρτηση αυτή δεν είναι κάτι το ιδιαίτερο, απλώς μια γεννήτρια ψευδοτυχαίων αριθμών. Θα μπορούσε να αντικατασταθεί με ένα οποιοδήποτε πολυώνυμο με ακέραιους συντελεστές. Στην πράξη χρησιμοποιείται η $f(x) = x^2 + c \; mod \; n$, με $c \neq 0, -2$. (Για $c = -2$ έχουμε ότι $f^{(m-1)}(x) = r^{2^m} + r^{-2^m}$)

2. Αν ο αλγόριθμος εμφανίσει αποτυχία και δεν πάρουμε έναν μη τετριμμένο παράγοντα του n, η πρώτη επιλογή είναι να αλλάξουμε συνάρτηση f και να ξαναδοκιμάσουμε.
3. Οι Pollard και Brent παρατηρώντας ότι αν $(a,n) > 1$, τότε και $(ab,n) > 1$, για κάθε θετικό ακέραιο b. Οπότε αντί να υπολογίζουμε σε κάθε βήμα το $\left(F^{(i)}(s) - F^{(2i)}(s)\right., n)$ μπορούμε για παράδειγμα να πολλαπλασιάσουμε 50 διαδοχικά $\left|F^{(i)}(s) - F^{(2i)}(s)\right|$ στο $modulo\ n$ και μετά να υπολογίζουμε το (z,n), με z το γινόμενο που θα βρούμε. Με αυτόν τον τρόπο ο αλγόριθμος γίνεται αρκετά πιο γρήγορος , αλλά θα αυξηθούν οι φορές που θα τερματίζει με αποτυχία.
4. Η περίπτωση ο αλγόριθμος να επιστρέψει αποτυχία συμβαίνει μόνο αν για τα a, b που εμφανίζουν σύγκρουση $a \equiv b\ mod\ p$, ισχύει και ότι $a \equiv b\ mod\ n$. Η πιθανότητα να συμβεί κάτι τέτοιο είναι $\frac{p}{n}$, πολύ μικρή για μεγάλο n και μικρό p.
5. Η πολυπλοκότητα του αλγορίθμου είναι $O\left(n^{\frac{1}{4}}\right)$.

Ας δούμε τώρα πως εφαρμόζεται το παράδοξο των γενεθλίων στη συγκεκριμένη περίπτωση.

Θεώρημα (Το παράδοξο των γενεθλίων)

Έστω n θετικός ακέραιος και p ο μικρότερος μη τετριμμένος διαιρέτης . Η πιθανότητα να επιλέξουμε δύο τυχαίους αριθμούς x_1, x_2, με $x_1 \neq x_2$ και $x_1 \equiv x_2\ modulo\ n$ (δηλαδή να υπάρχει σύγκρουση) ανάμεσα σε περίπου $1.17\sqrt{n}$ είναι μεγαλύτερη από $\frac{1}{2}$.

Απόδειξη:

Εφόσον μιλάμε για αριθμούς στο $modulo\ n$ είναι το ίδιο να μιλάμε για αριθμούς της ομάδας $Z_n = \{0,1,2,\dots,n-1\}$. Έχουμε ότι $|Z_n| = n$. Θα υπολογίσουμε την πιθανότητα μετά από k διαδοχικές τυχαίες επιλογές αριθμών από το Z_n , να μην έχουμε ούτε μια σύγκρουση.

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 δύο είναι $\frac{n-2}{n} = 1 - \frac{2}{n}$, κτλ.

Έτσι η πιθανότητα επιλογής k στοιχείων χωρίς συγκρούσεις είναι

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

Ξέρουμε ότι $e^{-x} = 1 - \frac{x}{1!} + \frac{x^2}{2!} - \frac{x^3}{3!} + \cdots$, $-\infty < x < \infty$. Συνεπώς μπορούμε να πούμε ότι για μικρά x ισχύει ότι $1 - x \sim e^{-x}$, το οποίο για μεγάλο n και κατά συνέπεια μικρό $\frac{1}{n}$ γίνεται, $1 - \frac{1}{n} \sim e^{-\frac{1}{n}}$. Οπότε για το παραπάνω γινόμενο έχουμε $\prod_{i=1}^{k-1}\left(1 - \frac{i}{n}\right) \sim \prod_{i=1}^{k-1} e^{-\frac{i}{n}} = e^{-\frac{k(k-1)}{2n}}$.

Άρα η πιθανότητα εύρεσης μιας σύγκρουσης είναι $P \approx 1 - e^{-\frac{k(k-1)}{2n}}$ και με συνεπαγωγές καταλήγουμε $k^2 - k \approx 2n \ln\frac{1}{1-P}$, δηλαδή $k \approx \sqrt{2n \ln\frac{1}{1-P}}$. Οπότε για πιθανότητα σύγκρουσης $P = \frac{1}{2}$, έχουμε $k \approx 1.17\sqrt{n}$. ■

Βιβλιογραφία

Κουκουβίνος Χ./Παπαϊωάννου Α.,"Κρυπτογραφία", Ε.Μ.Π., 2007

Πουλάκης Δ., "Κρυπτογραφία: Η επιστήμη της ασφαλούς επικοινωνίας", ΖΗΤΗ, 2006

Alfred J. Menezes/Paul C. Van Oorschot/Scott A. Vanstone, "Handbook of applied cryptography", CRC, 1996

Douglas R. Stinson, "Cryptography: Theory and Practice", CHAPMAN&HALL/CRC, 2002

Trappe W. /Washington L. , "Introduction to Cryptography with coding Theory", Pearson education

Richard Crandall/Carl Pomerance, "Prime Numbers: A Computational Perspective", Springer, 2005

Song Y. Yan, "Number Theory for Computing", Springer, 1998

Agrawal/Kayal/Saxena, "PRIMES is in P", Annals of Mathematics, 2004

Andrew Granville, "It is easy to determine whether a given integer is prime" /Bulletin of the American Mathematical society- Volume 42 Number 1, 2004

Vasilenko, "Number-theoretic algorithms in cryptography", American Mathematical Society, 2003

Cormen/Leiserson/Rivest/Stein, “Introduction to Algorithms”, MIT Press, 2009

Donald E. Knuth, “Art of Computer Programming, Volume 2: Seminumerical Algorithms”,Addison-Wesley,1981

Fraleigh B. John, “Εισαγωγή στην Άλγεβρα”, Πανεπιστημιακές Εκδόσεις Κρήτης, 2003

Ρασσιάς Μ.Θ./Παπαϊωάννου Α., “Εισαγωγή στη θεωρία αριθμών”, Συμεών, 2010

Πουλάκης Δ., “Θεωρία αριθμών”, Ζήτη , 2001

Andrews G.E., “Number theory”, Dover, 1994