Σπουδαστής :

Χιώτης Παναγιώτης – Α.Μ.: 09102241

Σχολή : Ε.Μ.Φ.Ε

Εξεταστική επιτροπή:

Χ. Κουκουβίνος – Καθηγητής Ε.Μ.Π.

Α. Παπαϊωάννου – Επίκουρος Καθηγητής Ε.Μ.Π.(επιβλέπων)

Π. Στεφανέας – Λέκτορας Ε.Μ.Π.

Θέμα : «Τεστ Πιστοποίησης Πρώτων Αριθμών»

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή στους πρώτους αριθμούς

Εισαγωγή

Στα μαθηματικά πρώτος αριθμός (ή απλά πρώτος) είναι ένας φυσικός αριθμός μεγαλύτερος της μονάδας με την ιδιότητα οι μόνοι φυσικοί διαιρέτες του να είναι η μονάδα και ο εαυτός του. Το μηδέν και το ένα δεν είναι πρώτοι αριθμοί, ενώ το μηδέν συχνά δεν θεωρείται ούτε φυσικός και η ακολουθία των 25 πρώτων αριθμών είναι η εξής:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

Ο αριθμός 2 είναι ο μόνος άρτιος (ζυγός) πρώτος αριθμός. Όλοι οι άλλοι πρώτοι είναι περιττοί (μονοί). Οι πρώτοι αριθμοί είναι ένα από τα αντικείμενα της θεωρίας αριθμών και είναι μια πολύ ενεργή ερευνητικά περιοχή των μαθηματικών. Διάσημες και άλυτες εικασίες, όπως η Εικασία του Riemann και η Εικασία του Goldbach εμπλέκουν ή αφορούν πρώτους αριθμούς.

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

Απόδειξη : Έστω ότι ο n είναι σύνθετος και $n = d_1 d_2$ με d_1, d_2 μεγαλύτερους της μονάδας. Αν $d_1 > \sqrt{n}$ και $d_2 > \sqrt{n}$ τότε $n = d_1 d_2 > \sqrt{n}\sqrt{n} = n$ άτοπο. Άρα έστω $d_1 \le \sqrt{n}$ και τότε ή ο d_1 πρώτος ή ο d_1 έχει πρώτο διαιρέτη μικρότερο ή ίσο της $\sqrt{n}$ που είναι άτοπο, άρα ο n είναι πρώτος.

Στην επόμενη παράγραφο γίνεται αναφορά στη σχέση των φυσικών με τους πρώτους αντίστοιχα.

Σχέση φυσικών με πρώτους

Το θεμελιώδες θεώρημα της αριθμητικής βεβαιώνει ότι κάθε θετικός ακέραιος γράφεται ως γινόμενο πρώτων παραγόντων με μοναδικό τρόπο. Για παράδειγμα:

$2184 = 2^3 * 3 * 7 * 13.$

Πλήθος πρώτων

Οι πρώτοι αριθμοί έχουν άπειρο πλήθος. Η πρόταση αυτή έχει αποδειχτεί με διάφορους τρόπους και η πρώτη γνωστή απόδειξη είναι του Ευκλείδη :

Έστω ότι οι πρώτοι έχουν πεπερασμένο πλήθος n και είναι οι $p_1, p_2, p_3, \ldots, p_n$

Ορίζουμε τον ακέραιο $q = 1 + \prod_{i=1}^{n} p_i$, αυτός ο αριθμός δεν διαιρείται με κανένα πρώτο και είναι μεγαλύτερος του p_n , που οδηγεί σε άτοπο.

Οι εικασίες του Γκόλντμπαχ

Είναι πολύ γνωστή η πρώτη εικασία που διατύπωσε ο Κρίστιαν Γκόλντμπαχ(1690-1764), η οποία σχετίζεται με τους πρώτους αριθμούς. Ο Γκόλντμπαχ υποστήριξε ότι κάθε άρτιος αριθμός μεγαλύτερος του 2, μπορεί να γραφεί ως άθροισμα δύο πρώτων αριθμών. Η απόδειξη της παραπάνω εικασίας ταλανίζει ακόμα και σήμερα τους μαθηματικούς, καθώς παράλληλα οι υπολογιστές επιβεβαιώνουν την εικασία για όλο και μεγαλύτερους αριθμούς. Το 1998, η εικασία επιβεβαιώθηκε για αριθμούς μέχρις και της τάξης του 10^{14}. Η δεύτερη εικασία του Γκόλντμπαχ έγκειται στο ότι κάθε περιττός αριθμός μεγαλύτερος του 6 είναι άθροισμα τριών πρώτων αριθμών.

Η εικασία αυτή παραμένει αναπόδεικτη, όπως επιβεβαιώνεται από τους ηλεκτρονικούς υπολογιστές και τυχόν απόδειξη της πρώτης εικασίας του Γκόλντμπαχ θα αποδείκνυε αμέσως και τη δεύτερη.

Αλγόριθμοι εύρεσης πρώτων

Οι αλγόριθμοι εύρεσης των πρώτων αναφέρονται παρακάτω.

Παρατίθενται μερικοί αλγόριθμοι (κατά σειρά ταχύτητας ή και απλότητας) για την εύρεση αν ο $N \geq 2$ είναι πρώτος. Η σειρά επίσης αυτών των αλγορίθμων είναι εκπαιδευτική για την εισαγωγή σε μια σειρά από προγράμματα για ηλεκτρονικούς υπολογιστές και περιγράφονται στις παρακάτω παράγραφους.

Απλός 1-από τον ορισμό του πρώτου αριθμού

Εξετάζουμε διαδοχικά όλους τους ακέραιους $M < N$ και μόλις βρεθεί διαιρέτης του N σταματάμε και ο N δεν είναι πρώτος. Αν εξαντληθούν οι M χωρίς να βρεθεί διαιρέτης, τότε ο M είναι πρώτος.

Απλός 2

Βασιζόμενοι στην παρατήρηση ότι κανένας αριθμός N δεν έχει διαιρέτη μεγαλύτερο του, $N/2$ τροποποιούμε τον παραπάνω αλγόριθμο εξετάζοντας όλους τους αριθμούς $M < N/2$.

Απλός 3

Παρατηρούμε ότι αν ένας αριθμός N δεν είναι πρώτος τότε έχει (τουλάχιστον) δύο διαιρέτες μεγαλύτερους από 1. Σε αυτήν την περίπτωση τουλάχιστον ένας διαιρέτης είναι μικρότερος από την τετραγωνική ρίζα του αριθμού. Τροποποιούμε τον αλγόριθμο 2 εξετάζοντας όλους τους αριθμούς M που είναι μικρότεροι από την τετραγωνική ρίζα του N, αν η τελευταία δεν είναι ακέραιος. Αλλιώς ο αριθμός *δεν* είναι πρώτος, επειδή τον διαιρεί και η τετραγωνική του ρίζα.

Απλός 4

Εφαρμόζοντας το Θεώρημα του Ουίλσον μπορούμε να εξετάσουμε, αν ένας αριθμός N είναι πρώτος ή όχι. Σύμφωνα με το θεώρημα αυτό ο N είναι πρώτος αν και μόνο αν ισχύει $(N-1)! \equiv -1 (\mathrm{mod}\, N)$, αν δηλαδή το υπόλοιπο της διαίρεσης $(N-1)/N$, είναι ίσο με το υπόλοιπο της διαίρεσης του -1 με το N. Η μέθοδος αυτή δεν εφαρμόζεται για μεγάλο N, αφού είναι δύσκολο να υπολογιστεί η συνάρτηση παραγοντικό. ! Ο μεγαλύτερος γνωστός πρώτος αριθμός περιγράφεται στο επόμενο κεφάλαιο.

Κλασσική Fermat, Βελτωμένη μέθοδος Euler

Ο μεγαλύτερος γνωστός πρώτος αριθμός

Ο μεγαλύτερος γνωστός πρώτος είναι ο $M_{48} = 2^{57,885,161} - 1$ και βρέθηκε στις 25 Ιανουαρίου 2013 μέσω του διαδικτυακού προγράμματος κατανεμημένης επεξεργασίας GIMPS (Great Internet Mersenne Prime Search)Θα πρέπει να σημειωθεί ότι, όλοι οι πρώτοι που ανακαλύφθηκαν έτσι ήταν Μερσέν πρώτοι. Στην επόμενη παράγραφο περιγράφονται οι ιδιότητες των πρώτων.

Ιδιότητες πρώτων

Το λεγόμενο πρώτο θεώρημα του Ευκλείδη :

Αν ο p είναι πρώτος και διαιρεί το γινόμενο ab για κάποιους ακέραιους a, b τότε ο p διαιρεί το a ή το b.

Αν p πρώτος και a ακέραιος, τότε το $a^p - a$ διαιρείται από το p (Μικρό Θεώρημα του Fermat).

Κρυπτοσύστημα RSA

Η ιδέα της κρυπτογραφίας δημοσίου κλειδιού παρουσιάσθηκε για πρώτη φορά το 1976 από τους Diffie και Hellman. Ένα χρόνο αργότερα, οι R. L.Rivest, A. Shamir και L. Adleman εφηύραν το κρυπτοσύστημα δημοσίου κλειδιού RSA, το οποίο βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων ακεραίων. Έστω $p, q > 2$ είναι δύο διαφορετικοί πρώτοι αριθμοί και $n = pq$ (με p,q να έχουν το ίδιο ή περίπου ίδιο πλήθος ψηφίων). Ο χώρος P των καθαρών μηνυμάτων και ο χώρος C των κρυπτογραφημένων μηνυμάτων είναι ο χώρος n και ο χώρος K των κλειδιών είναι η πολλαπλασιαστική ομάδα:

$$K = Z^*_{\varphi(n)}$$

Το σύνολο των συναρτήσεων κρυπτογράφησης είναι της μορφής:

$$f_e : Z_n \to Z_n,\ \bar{x} \to \bar{x^e}, e \in K,$$

και το σύνολο των συναρτήσεων αποκρυπτογράφησης είναι της μορφής:

$$g_d : Z_n \to Z_n, \bar{x} \to \bar{x^d}, \text{όπου } ed \equiv 1 \bmod \varphi(n). \text{ Προφανώς :}$$

$$g_d(f_e(\bar{x})) = \overline{x^{de}} = \overline{x^{1 \bmod \varphi(n)}} = \overline{x^{de}} = \overline{x^{1+k\varphi(n)}} = x^{1+k\varphi(n)} \bmod n.$$

- Έστω $(x,n) = 1,\ 0 < x < n$, επομένως από το θεώρημα Euler προκύπτει:

$$x^{\varphi(n)} \equiv 1 \bmod \varphi(n),$$

άρα

$$x^{k\varphi(n)} = 1 + jn \Leftrightarrow x^{k\varphi(n)} x = x + xjn \Leftrightarrow x^{1+k\varphi(n)} \equiv x \bmod n.$$

- $(x,n) \neq 1,\ 0 < x < n$, εφόσον $n = pq$ θα πρέπει $x = lp$ ή $x = lq$. Αν $x = lp$, τότε θα πρέπει $(x,q) = 1,$ διότι αλλιώς θα πρέπει $x = jq,$ δηλαδή $x = mpq, m > 1$ που είναι άτοπο εξ υποθέσεως $0 < x < n = pq.$ Άρα

$$(x,q) = 1 \Rightarrow x^{\varphi(q)} \equiv 1 \bmod q \Leftrightarrow (x^{\varphi(q)})^{\varphi(p)} \equiv 1 \bmod q \Leftrightarrow x^{\varphi(n)} \equiv 1 \bmod q$$
$$\Leftrightarrow x^{\varphi(n)} = 1 + kq \Leftrightarrow x^{\varphi(n)} x = x + xkq = x + lkpq \Leftrightarrow x^{1+\varphi(n)} = x + lkn$$
$$\Leftrightarrow x^{1+k\varphi(n)} \equiv x \bmod n.$$

Τελικά : $g_d(f_e(\bar{x})) = x \bmod n \cdot 1^k = x \bmod n = \bar{x}.$ Το ζεύγος (n,e) καλείται δημόσιο κλειδί του κρυπτοσυστήματος και δημοσιοποιείται, ενώ ο φυσικός d καλείται ιδιωτικό κλειδί και κρατείται μυστικός και η μεταξύ τους σχέση είναι :

$$ed \equiv 1 \bmod(\varphi(n)).$$

Παράδειγμα 1: Έστω ότι ο Α διαλέγει τους πρώτους αριθμούς $p = 11, q = 23.$ Τότε $n = 11 \cdot 23 = 253$ και

$$\varphi(n) = 253(1 - \frac{1}{11}).(1 - \frac{1}{23}) = 220.$$

Έστω $e = 3$ τότε , χρησιμοποιώντας τον εκτεταμένο Ευκλείδιο αλγόριθμο, είμαστε σε θέση να υπολογίσουμε το ιδιωτικό κλειδί αποκρυπτογράφησης :

$220 = 3 \cdot 73 + 1 \Rightarrow 1 = 220 - 3 \cdot 73,$ άρα με βάση τα παραπάνω

$$d = -\overline{73} = 147 \bmod 220 \Rightarrow d = 147.$$

Ας υποθέσουμε ότι ο Β θέλει να στείλει το μήνυμα $x = 63,$ τότε χρησιμοποιεί τη συνάρτηση κρυπτογράφησης $x \to x^e = x^3 = 63^3 = 2500047 = 83 \bmod(253),$ άρα $c = 83.$ Επομένως ο Α αποκρυπτογραφεί κάνοντας τον παρακάτω υπολογισμό:

$$c^d = 83^{147} \equiv 63 \bmod 253.$$

Παρατήρηση: Ο υπολογσμός μεγάλων δυνάμεων , όπως η παραπάνω ποσότητα $83^{147} \bmod 253$, γίνεται με κανόνες της modular έκθετοποίησης. Η περιγραφή του υπολογισμού του $83^{147} \bmod 253$, γίνεται ως εξής :

Αρχικά υπολογίζουμε τη δυαδική αναπαράσταση του αριθμού 147:

$147 = (10010011)_2$. Στη συνέχεια υπολογίζουμε τις δυνάμεις του 83 της μορφής $2^r, 1 \le r \le N,$ όπου N είναι το πλήθος των δυαδικών ψηφίων του 147:

- $83^1 \bmod 253 = \overline{83}$
- $83^2 \bmod 253 = \overline{53}$
- $83^4 \bmod 253 = (83^2)^2 \bmod 253 = 58^2 \bmod 253 = \overline{75}$
- $83^8 \bmod 253 = (83^4)^2 \bmod 253 = 75^2 \bmod 253 = \overline{59}$
- $83^{16} \bmod 253 = (83^8)^2 \bmod 253 = 59^2 \bmod 253 = \overline{192}$
- $83^{32} \bmod 253 = (83^{16})^2 \bmod 253 = 192^2 \bmod 253 = \overline{179}$
- $83^{64} \bmod 253 = (83^{32})^2 \bmod 253 = 179^2 \bmod 253 = \overline{163}$
- $83^{128} \bmod 253 = (83^{64})^2 \bmod 253 = 163^2 \bmod 253 = \overline{4}$

Επομένως ο τελικός υπολογισμός είναι της μορφής :

$83^{147} \bmod 253 = 83^{128} \cdot 83^{16} \cdot 83^2 \cdot 83^1 \bmod 253 = 4 \cdot 192 \cdot 58 \cdot 83 \bmod 253 = \overline{63}$.

Παράδειγμα 2: Έστω p =281, q= 167, τότε n = 281*167 =46927 και εργαζόμενοι όπως προηγουμένως υπολογίζουμε ότι $\varphi(n) = 46480.$ Έστω ότι $e = 11,$ τότε με χρήση του Ευκλείδιου αλγορίθμου υπολογίζουμε ότι $d = 8451.$ Στη περίπτωση που ο Β επιθυμεί να στείλει το μύνημα ‘’ ΣΗΜΕΡΑ’’ με τη συνήθη αντιστοιχία $A \leftrightarrow 0, ... \Omega \leftrightarrow 23$ και εφόσον $n = 46927$ και το μήκος της αλφαβήτου είναι $N = 24,$ τότε υπολογίζουμε την ποσότητα $k = [\log_N n] = [\log_{24} 46927] = [3,38457] = 3.$

Στη συνέχεια χωρίζουμε το μήνυμα $k - \acute{\alpha}\delta\varepsilon\varsigma$, τις τριάδες στη προκειμένη περίπτωση σαν : ‘’ΣΗΜ’’ και ‘’ΕΡΑ’’ και μετά μετατρέπουμε κάθε τριάδα σε αριθμητική ακολουθία με τη συνήθη αντιστοιχία :

$$\begin{cases} ''\Sigma HM'' \to \{17,6,11\} \\ ''EPA'' \to \{4,16,0\} \end{cases}$$

Κάθε μία από τις δύο ακολουθίες που προκύπτουν τις μετατρέπουμε σε ένα αριθμό στο N-αδικό (στην προκειμένη περίπτωση στο 24-αδικό) σύστημα αρίθμησης ως εξής:

$$\begin{cases} a^{11} \bmod n = A_1 = 1898 \bmod 46927 \\ b^{11} \bmod n = B_1 = 25883 \bmod 46927 \end{cases}$$

Στη συνέχεια γράφουμε τους A_1, B_1 στο 24αδικό σύστημα αρίθμησης και προκύπτει

$$\begin{cases} 1898 \leftrightarrow \{0,3,2,7\} \leftrightarrow ''A\Delta\Gamma\Theta \\ 25833 \leftrightarrow \{1,20,20,9\} \Leftrightarrow ''B\Phi\Phi K' \end{cases}$$

οπότε το κρυπτογραφημένο μήνυμα είναι το $c = ''A\Delta\Gamma\Theta B\Phi\Phi K''$.

Ο δέκτης χωρίζει το μήνυμα ανά 4-άδες και κωδικοποιεί με 24αδική γραφή και αποκωδικοποιεί με χρήση του d.

Παρατηρήσεις:

- Εφόσον

$$ed = 1 \bmod q(n) \Leftrightarrow ed = 1 + l(p-1)(q-1),$$

Ο υπολογισμός του ιδιωτικού κλειδιού d , από το ζεύγος (n,e) ισοδυναμεί με την εύρεση των πρώτων παραγόντων $p,q.$ Η εύρεση της παραγοντοιήσης του n ισοδυναμεί με τη εύρεση της τιμής του $\varphi(n),$ που σημαίνει ότι αν γνωρίζουμε την τιμή του $\varphi(n),$ τότε $\varphi(n) = (p-1)(q-1),$ άρα:

$n = pq$ και $p + q = n + 1 - \varphi(n)$,όπου τα p,q είναι λύσεις της παρακάτω δευτεροβάθμιας εξίσωσης :

$$x^2 - (n + 1 - \varphi(n))x + n = 0.$$

- Αντιστρόφως, εάν γνωρίζουμε το ιδιωτικό κλειδί $d,$ τότε μπορούμε να υπολογίσουμε τους πρώτους παράγοντες p,q του n ως εξής :

θέτουμε $s = \max\{ n \in N : 2^n /(ed-1)\}$ και $k = \frac{ed-1}{2^s}$ (1).

Θεώρημα 1: Για κάθε ζεύγος πρώτων μεταξύ τους φυσικών αριθμών a, n τέτοιων ώστε $ord_p(a^k) \neq ord_q(a^k), (n = pq)$, όπου το k εκφράζεται στη σχέση (1) και ισχύει:

$\gcd(a^{2^r k} - 1, n) = q$ ή p , όταν $r < s.$

Επιπλέον υπάρχουν τουλάχιστον $(p-1)(q-1)/2$ τέτοιοι φυσικοί αριθμοί α στο διάστημα $[1, n]$. Συνεπώς,η πιθανότητα να επιλέξουμε ένα τέτοιο αριθμό μετά από r επαναλήψεις είναι τουλάχιστον $1 - \frac{1}{2^r}$.

Αλγόριθμος παραγοντοποίησης του n δοθέντος ιδιωτικού κλειδιού d:

- Επιλέγουμε τυχαίο $a \in [1, n]$.
- Ορίζουμε το k, όπως στην (1).
- Υπολογίζουμε : $\gcd(a^{2^r k} - 1, n)$ για $r < s.$
- Αν $\gcd(a^{2^r k} - 1, n) = 1 \forall r < s,$ επιλέγουμε άλλο α,
- αλλιώς αν $\exists r_0 : \gcd(a^{2^r k} - 1, n) > 1,$ τότε $\gcd(a^{2^r k} - 1, n) = p.$

Εφόσον η ασφάλεια του RSA βασίζεται στη δυσκολία παραγοντοποίησης του $n,$ ο ακέραιος $n,$ και κατά συνέπεια οι παράγοντες του p και q θα πρέπει να πληρούν μερικούς περιορισμούς ώστε η παραγοντοποιήση του n να είναι δύσκολη.

1. Πρέπει να διαλέγουμε πρώτους αριθμούς με το ίδιο μήκος περίπου, το οποίο να είναι μεγαλύτερο από το 512 και να μην είναι καποιας ειδικής μορφής. Ένας τρόπος κατασκευής τέτοιων πρώτων είναι με χρήση αλγορίθμων που παράγουν ακουλουθίες δυαδικών ψηφίων ώστε οι πιθανότητες εμφάνισης του 0 και 1 σε κάθε θέση να είναι περίπου ίδιες. Αυτοί οι αλγόριθμοι ονομάζονται γεννήτορες ψευδοτυχαίων αριθμών. Ένα τέτοιο παράδειγμα είναι τα γραμμικά συστήματα καταγραφής μετατόπισης με ανάδραση. Για να βρούμε έναν τυχαίο πρώτο μήκους k, θεωρούμε έναν γεννήτορα ψευδοτυχαίων αριθμών και παράγουμε μια ακολουθία $k-2$ στοιχείων $a_1, ..., a_{k-2} \in \{0,1\}$. Ο ακέραιος $a = 2^k + a_{k-1}2^{k-1} + ... + 2a_1 + 1$ είναι

περιττός και το μήκος του ισούται με k. Στη συνέχεια εφαρμόζουμε κάποιο κριτήριο πιστοποιήσης πρώτου για να διαπιστώσουμε αν ο α είναι πρώτος. Αν όχι θεωρούμε μια άλλη ακολουθία ψηφίων μέχρι να βρούμε κάποιον πρώτο.

2. Κάθε δυο μέλη μιας ομάδας χρηστών του RSA πρέπει να έχουν διαφορετικό ακέραιο n στα δημόσια κλειδιά τους. Πράγματι αν $(n_A, e_A), (n_B, e_B)$ είναι τα δημόσια κλειδιά τους και αν $n_A = n_B = n,$ τότε ο καθένας τους μπορεί με χρήση του ιδιωτικού κλειδιού του, να παραγοντοποιήσει το n και συνεπώς να υπολογίσει το ιδιωτικό κλειδί του άλλου. Αν επιπλέον υποθέσουμε $(e_A, e_B) = 1,$ τότε $\exists x, y \in Z$:¨

$xe_A + ye_B = 1,$ οπότε εάν κάποιος τρίτος χρήστης στέλνει το ίδιο μήνυμα στους A,B υπάρχουν ακέραιοι $0 \le c_A, c_B < n$ ώστε:

$$c_A = m^{e_A} \bmod n$$
$$c_B = m^{e_B} \bmod n$$

Άρα:

$$c_A{}^x c_B^y = m^{xe_A + ye_B} \bmod n \equiv m \bmod n,$$

που σημαίνει ότι όποιος έχει στη κατοχή του τα κρυπτογραφημένα κείμενα c_A, c_B, μπορεί να βρει το $m.$

3. Είναι ασφαλέστερο να αποφεύγεται η χρήση μικρών κλειδιών κρυπτογράφησης. Για παράδειγμα, αν υποθέσουμε ότι ένα μήνυμα m κρυπτογραφείται e-φορές με τη χρήση δημοσίων κλειδιών (n_i, e) και c_i είναι τα αντίστοιχα κρυπτογραφήματα τότε έχουμε :

$$c_i = m^e \mod(n_i)$$

Αν $(n_i, n_j) = 1, \forall i \ne j$ τότε από το Κινέζικο Θεώρημα Υπολοίπων υπάρχει μοναδική λύση $\mod(n_1, \ldots n_e)$, άρα : $m = c^{1/e}$.

4. Θεωρείται ασφαλέστερο ένα κλειδί αποκρυπτογράφησης που η τιμή του είναι μεγαλύτερη της $\sqrt[4]{n}/3.$

5. Έστω (n, e) δημόσιο κλειδί RSA. Εφόσον $(e, \varphi(n)) = 1,$ έχουμε:

$$\exists k \in N : e^k \equiv 1 \bmod \varphi(n),\ k \text{ η τάξη του } e,$$

$$c \equiv m^e \bmod \varphi(n) \Rightarrow c^{e^{k-1}} \equiv m^{e^k} \equiv m \bmod n,$$

επομένως εάν κάποιος γνωρίζει το c χωρίς να ξέρει το κλειδί αποκρυπτογράφησης , υπολογίζει τις ποσότητες

$$c^e \bmod n, c^{e^2} \bmod n, ...$$

μέχρι να βρεθεί u ώστε $c^{e^u} \equiv c \bmod n.$ Τότε $m \equiv c^{e^{u-1}} \bmod n$ και αυτό χρησιμοποιείται στην περίπτωση που ο u είναι μικρός.

Τεστ Πιστοποιήσης Πρώτων Αριθμών

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 κρυπτοσυστημάτων δημοσίου κλειδιού (RSA, el Gamal) βασίζεται στη χρήση μεγάλων πρώτων αριθμών, δηλαδή με σημερινά δεδομένα της τάξεως των 150-200 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 με περίπου 200 ψηφία. Την απάντηση σε αυτό το ερώτημα δίνει το θεώρημα των πρώτων αριθμών (Prime number theorem) που αναφέρεται στην επόμενη παράγραφο.

Θεώρημα(Το θεώρημα των πρώτων αριθμών)

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

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1 \text{ ,ή } \pi(\chi) \approx \frac{x}{\ln x}$$

Σύμφωνα λοιπόν με το θεώρημα των πρώτων αριθμών ,η πιθανότητα να επιλέξουμε τυχαία έναν αριθμό k με $1 \le k \le x$ και να ειναι και αυτός 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 αριθμούς $\ln 10^{200} \cong 461$, εξαιρώντας τους 230 άρτιους περίπου αριθμούς. Συνεπώς μπορούμε να πούμε ότι υπολογιστικά είναι μια μή 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, γίνεται και με την πρόσφατη δημοσίευση του αλγορίθμου (Agrawal-Kayal-Saxena primality test, AKS), 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 πιθανοτικα τεστ ,όπως τα τεστ των Fermat, Solovay-Strassen, Miller-Rabin.

<u>Το Θεώρημα του Fermat</u>

Το <<μικρό >> θεώρημα του Fermat λέει ότι αν ο p πρώτος και $1 \le a \le p$ τότε $a^{p-1} \bmod p = 1$. Το θεώρημα αυτό δίνει ένα (αρνητικό) κριτήριο για την πιστοποίηση πρώτων .Ας πάρουμε $a = 2$ και ας υπολογίσουμε το $2^{n-1} \bmod n$ (η πολυπλοκότητα της διαδικασίας είναι $O((\log n)^3)$.. 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 $n \le 17$. Οι πρώτοι δίνουν 1 ενώ οι σύνθετοι αποτέλεσμα $\neq 1$. Από το θεώρημα του Fermat αν $2^{n-1} \bmod n \neq 1$ 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: Ο $a, 1 \le a \le n,$ ονομάζεται F-μάρτυρας για το n αν $a^{n-1} \bmod n \neq 1.$ 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 (με υπομονή ή με ένα πρόγραμμα στον υπολογιστή) ότι ο 2 είναι F-μάρτυρας για όλους τους σύνθετους αριθμούς $n \le 340.$ 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 $2^{10} = 1024 = 3 \cdot 341 + 1 = 1 \bmod 341.$

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≤α≤n-1 είναι F-ψεύτης αν $a^{n-1} \bmod n = 1.$

Τετριμμένα έχουμε ότι οι 1 και n-1 είναι 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 $3^{340} \bmod 341 = 56,$ άρα ο 3 είναι F-μάρτυρας του 341.

Το ‘’αντίστροφο‘’ του μικρού θεωρήματος του Fermat δεν ισχύει όπως είδαμε παρόλο που οι Κινέζοι πίστευαν λαθεμένα ότι ισχύει, π.χ. ο $2^{340} \bmod 341 = 1,$ αλλά ο 341 δεν είναι πρώτος, είμαστε όμως σε θέση να περισώσουμε κάτι.

Λήμμα 2.1: a) Αν $1 \le a \le n,$ ικανοποιεί την $a^r \bmod n = 1$ τότε $a \in Z_n^*.$

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 $r \geq 1 \Rightarrow a * a^{r-1} \bmod n = 1 \Rightarrow a \in Z_n^*$.

b) Έστω $a^{n-1} \bmod n = 1,$ για κάθε $a \in [1, n]$ άρα (από το α) $Z_n^* = \{1,,,n-1\}$ που σημαίνει αυτομάτως ότι ο n είναι πρώτος. Το β μέρος του λήμματος λέει επίσης ότι υπάρχει πάντα ένας F-μάρτυρας για τον σύνθετο μονό n. Πράγματι τα $n-1-\varphi(n)$ στοιχεία με

$\{1 \leq a \leq n$ και $(a,n) > 1\}$ δεν μπορούν όλα να ικανοποιούν την σχέση $a^{n-1} \bmod n = 1.$ Όμως για πολλούς σύνθετους το σύνολο αυτό έχει πολύ λίγα στοιχεία.

Παράδειγμα:2.1: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
Πολ13	13,26,39,52,65,78
F-μάρτυρες Στο Z_{91}^*	2,5,6,8,11,15,18,19,20,24,31,32,33,34,37,41,44,45,46,47,50,54, 57,58,59,60,67,71,72,73,76,80,83,85,86,89
F-ψεύτες	1,3,4,9,10,12,16,17,22,23,25,27,29,30,36,38,40,43,48,51,53,55 61,62,64,66,68,69,74,75,79,81,82,87,88,90

Παρατηρούμε ότι και τα πολ7,πολ13 είναι F-μάρτυρες [διότι (α n)>1]. Πράγματι αν πάρω ένα πολλαπλάσιο του 7 (ή του 13) πχ. το 14 έχω: $14^{90} \bmod 91 = 2^{90} * 7^{90} \bmod 91 = 64 \cdot 77^6 = 14 \neq 1 \bmod 91,$ άρα το 14 είναι F-μάρτυρας. Για τους ψεύτες όμως $3^{90} = 1 \bmod 91$ από Fermat, αποτέλεσμα που μας οδηγεί στην πρώτη προσπάθεια πιθανοτικής πιστοποίησης πρώτου.

Αλγόριθμος 1(Fermat Test)

Είσοδος: Μονός φυσικός $n \geq 3$

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

2.αν $a^{n-1} \bmod n \neq 1$

3.τότε επιστροφή 1

4.αλλιώς επιστροφή 0

Η χρονική διάρκεια περιγράφεται μέσω της γρήγορης εκθετοποίησης(fast exponentiation) $a^{n-1} \bmod n$ είναι $O(\log n)$ αριθμητικές πράξεις και $O((\log n)^3)$ πράξεις bit. Αν ο αλγόριθμος δώσει 1 έχει βρεί 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 1και 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 ικανοποιείται με σταθερή πιθανότητα.

Θεώρημα 2.2: Αν $n \geq 3$ ένας μονός σύνθετος αριθμός που έχει τουλάχιστον έναν F-μάρτυρα *α*, τότε το τέστ του Fermat αν εφαρμοστεί στον n δίνει απάντηση 1 με πιθανότητα μεγαλύτερη $\frac{1}{2}$.

Απόδειξη: Το σύνολο $L_n^F = \{a \mid 1 \leq a \leq n$ με $a^{n-1} \bmod n = 1\}$ των F-ψευτών για το n είναι προφανώς υποσύνολο του Z_n^*. Θα δειξουμε ότι είναι και υποομάδα της ομάδας του Z_n^* με ($\left|Z_n^*\right| = \varphi(n)$). Γι αυτό αρκεί να δείξουμε ότι:

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

ii) Η L_n^F είναι κλειστή ως προς την πράξη πολλαπλασιασμός $\bmod n$ (η πράξη της Z_n^*), διότι $a^{n-1} \bmod n = 1$ και $b^{n-1} \bmod n = 1$ συνεπάγεται $(ab)^{n-1} = a^{n-1}b^{n-1} = 1.1 = 1 \bmod n.$

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 του $\varphi(n)$, όπου $\varphi(n) < n-1$(διότι ο n σύνθετος), άρα $\left| L_n^F \leq \frac{n-1}{2}\right.$. Άρα η πιθανότητα του μία τυχαία επιλογή από το $\{2,.....n-2\}$ να ανήκει στο $L_n^F - \{1, n-1\}$ είναι το πολύ $\frac{\frac{n-2}{2}-2}{n-3} = \frac{n-6}{2(n-3)} < \frac{1}{2}.$ Βεβαίως ένας αλγόριθμος που δίνει πιθανότητα λάθους $< \frac{1}{2}$ δεν είναι έμπιστος.

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

Αλγόριθμος 2 (Iterated Fermat Test)

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

Διαδικασία : 1.Επαναλαμβάνω l φορές

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

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

4. Επιστροφή 0

Παρατηρούμε ότι αν η έξοδος είναι 1 ο αλγόριθμος έχει βρει έναν F- μάρτυρα άρα ο n σύνθετος . Αν ο n είναι σύνθετος και ισχύει το προηγούμενο θεώρημα (δηλαδή

υπάρχει τουλάχιστον ένας F-μάρτυρας a με $(a,n)=1)$ η πιθανότητα να επιλέξουμε F-ψεύτη μετά από l δοκιμές γίνεται μικρότερη από $(\frac{1}{2})^l$. Άρα για μεγάλα l η πιθανότητα 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=3.11.17. Το 1994 απεδείχθη ότι υπάρχουν άπειροι αριθμοί Carmichael (από τους Alford-Granville-Pomerance) που είναι μάλιστα ομοιόμορφα κατανεμημένοι.

Αν ένας αριθμός Carmichael n υποστεί το τέστ του Fermat η πιθανότητα να πάρουμε την λάθος απάντηση 0 είναι $\frac{\varphi(n)-2}{n-3} > \frac{\varphi(n)}{n} = (1-\frac{1}{p_1})(1-\frac{1}{p_2})..(1-\frac{1}{p_k})$, που είναι ~1 αν το n έχει λίγους μεγάλους παράγοντες.

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

Άρα χρειαζόμαστε καλύτερα τεστ από τα τεστ του Fermat.

Πρώτα όμως περιγράφουμε την βασική ιδιότητα των αριθμών Carmichael.

Θεώρημα 2.3: Αν ο n είναι αριθμός Carmichael, τότε ο n είναι γινόμενο τουλάχιστον τριών (διαφορετικών) πρώτων παραγόντων.

Περίπτωση 1: Έστω $p^2 | n$ για κάποιο πρώτο $p \geq 3$. Γράφουμε $n = p^k * m$ με $k \geq 2$ και

p δεν διαιρεί το m.

Αν $m = 1$ τότε $a = 1 \dagger p$.

Αν $m \geq 3$ τότε από ΚΘΥ επιλέγω τον a

$1 \leq a < p^2 * m \leq n$ με $a = 1 + p \bmod p^2$ και $a = 1 \bmod m$.

Θα δείξω ότι α είναι F-μάρτυρας στο Z_n^*

Παρατηρώ από την δεύτερη ισοδυναμία ότι $(a,m)=1$, ενώ η πρώτη δίνει

$a-(1+p)=\lambda p^2 \Rightarrow a \neq \mu p.$ Αλλά $n=p^k m$, άρα $(a,n)=1.$

Έστω λοιπόν ότι $a \in Z_n^*$ δεν είναι F-μάρτυρας για το n ,ήτοι $a^{n-1} \bmod n = 1.$

Αφού $p^2 \mid n$, έχουμε $a^{n-1} = 1 \bmod p^2.$

{Πράγματι $a^{n+1}-1 = k*n$ και $n = sp^2 \Rightarrow a^{n+1}-1 = ks*p^2 \Rightarrow a^{n-1} = 1 \bmod p^2$ }

Από το θεώρημα του δυωνύμου προκύπτει :

$$a^{n-1} = (1+p)^{n-1} = 1+(n-1)p+\sum_{1\le l\le n-1}\binom{n-1}{i}p^i = 1+(n-1)p \bmod p^2.$$

Άρα $a^{n-1} = 1 \bmod p^2$ και $a^{n-1} = 1+(n-1)p \bmod p^2$, που δίνουν $(n-1)p = 0 \bmod p^2 \Rightarrow p^2 \mid p(n-1)$, που δίνει άτοπο διότι p δεν διαιρεί το $n-1$ που ισούται με $p^k * m-1.$

Περίπτωση 2: $n = p*q$ για διακεκριμένους πρώτους p,q και έστω $p>q.$ Πάλι θα κατασκευάσουμε έναν F-μάρτυρα $a \in Z_n^*$. Η ομάδα Z_p^* είναι κυκλική, ήτοι έχει έναν γεννήτορα g. Από το ΚΘΥ πάλι επιλέγουμε τον $a, 1 \le a < n$ με

$$a = g \bmod p \text{ και}$$

$$a = 1 \bmod q.$$

Προφανώς $a \neq kp, a \neq \lambda q$, άρα $a \in Z_n^*.$

Υποθέτουμε ότι $a^{n-1} \bmod n = 1.$

Αλλά $p \mid n \Rightarrow g^{n-1} \bmod p = a^{n-1} \bmod p = 1.$ [πράγματι $a^{n-1}-1 = kn \Rightarrow a^{n-1}-1 = klp$, ήτοι $a^{n-1} = 1 \bmod p.$] Όμως ο γεννήτορας g της κυκλικής ομάδας Z_p^* θα χει τάξη $p-1$, οπότε $p-1 \mid n-1$ Αλλά $n-1 = pq-1 = (p-1)q+q-1,$ άρα $p-1 \mid q-1,$ το οποίο σημαίνει ότι $p-1 \le q-1 = p \le q,$ που είναι άτοπο διότι $p>q.$

Μία ισχυρότερη μορφή του θεωρήματος είναι η ακόλουθη που οφείλεται στον A.Korselt.

Θεώρημα 2.4 : Ένας περιττός σύνθετος ακέραιος $n \geq 3$ είναι αριθμός Carmichael αν και μόνο αν είναι ελεύθερος τετραγώνου (*squarefree* δηλαδή δεν διαιρείται από το 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 $6t+1, 12t+1$ και $18t+1$ να έιναι πρώτοι, τότε ο ακέραιος $n=(6t+1)(12t+1)(18t+1)$ 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 πρώτους 105.212 αριθμούς Carmichael. Οι 20 μικρότεροι αριθμοί Carmichael είναι οι εξής:

561=3.11.17	41.041=7.11.13.41
1105=5.13.17	46657=13.37.97
1729=7.13.19	52633=7.73.103
2465=5.17.29	62.745=3.5.47.89
2821=7.13.31	63.973=7.13.19.37
6601=7.23.41	75361=11.13.17.31
8911=7.19.67	101.101=7.11.13.101
10.585=5.29.73	115.921=13.37.241
15.841=7.31.73	126.217=7.13.19.73
29.341=13.37.61	162.401=17.41.233

Υπάρχουν πίνακες πρώτων. Χρονολογικά έχουμε:

Fibonacci	1202	πρώτοι ≤ 100
Cataldi	1603	≤ 750
Frans van Schooten	1657	≤ 9929
Johan Rahn ή Rohnius (Algebra)	1659	≤ 24.000
Brancker	1668	$\leq 10^5$
Lambert	1770	≤ 102.000
Felkel	1776	≤ 408.00

(για το Αυστριακό Υπουρ. Οικονομικών. Το χαρτί των απούλητων αντιτύπων του βιβλίου χρησιμοποιήθηκε στο πόλεμο με την Τουρκία)

Crelle	1856	6.000.000 πρώτοι
Dase	1861	9.000.000 πρώτοι
J.P.Kulik	1863	$\leq 100.000.000$. (22 τόμοι).

Το 1630 ο Mersenne ρώτησε τον Fermat αν ο 100.895.598.169 είναι πρώτος και ο Fermat απάντησε ότι ισούται με 898.423*112.303.

Μη Τετριμμένες Τετραγωνικές Ρίζες της Μονάδας

Το Κριτήριο Miller Rabin και Solovay Strassen

Ορισμός: Έστω $1 < a < n$. Ο a ονομάζεται τετραγωνική ρίζα της μονάδας $\bmod n$, αν $a^2 \bmod n = 1$. Παρατηρούμε ότι ο 1 και $n-1$ είναι πάντα τετραγωνικές ρίζες της μονάδας $\bmod n$. Πράγματι $1^2 \bmod n = 1,\ (n-1)^2 = (-1)^2 = 1 \bmod n$ αυτές είναι οι τετριμμένες ρίζες της μονάδας. Αν ο n είναι πρώτος δεν υπάρχουν άλλες ρίζες της μονάδας $\bmod n$.

Λήμμα 3.1 **:** Αν p πρώτος και $1 \leq a \leq p$ με $a^2 = 1 \bmod p,$ τότε $a = 1$ ή $a = p-1.$

Απόδειξη: Έχουμε $a^2 - 1 \bmod p = (a+1)(a-1) \bmod p = 0$,άρα $p \mid (a+1)(a-1)$.

Αφού ο p έιναι πρώτος τότε:

$p \mid a+1 \Rightarrow \alpha+1 = kp \Rightarrow a = -1 \bmod p = p-1 \bmod p$ ή

$p \mid a-1 \Rightarrow \alpha-1 = kp \Rightarrow a = 1 \bmod p.$

Αν λοιπόν βρούμε μη τετριμμένες ρίζες της μονάδας $\bmod n$ τότε ο n είναι σίγουρα σύνθετος.

Παράδειγμα 3.1: Οι τετραγωνικές ρίζες του $1 \bmod 91$ είναι 1,27,64 και 90.

Πράγματι $27^2 = 729 = 1 \bmod 91,\ 64^2 = (-27^2) = 729 = 1 \bmod 91$

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

Πρόταση 3.2: Έστω ο πρώτος $p = 3 \bmod 4$ και ο ακέραιος y. Έστω $x = y^{\frac{p+1}{4}} \bmod p.$

1) Αν ο y έχει τετραγωνική ρίζα $\bmod p$, τότε οι τετραγωνικές ρίζες του $y \bmod p$ είναι $\pm x.$

2) Αν ο y <u>δεν</u> έχει τετραγωνικές ρίζες $\bmod p$ τότε ο $-y$ έχει και οι τετραγωνικές ρίζες του $-y \bmod p$ είναι $\pm x.$

Απόδειξη: Υποθέτω $y \neq 0$, διαφορετικά έχουμε τετριμμένη περίπτωση. Από το θεώρημα του Fermat $y^{p-1} = 1 \bmod p.$ Άρα $x^4 = y^{p+1} = y^2 y^{p-1} = y^2 \bmod p$, ήτοι

$(x^2 + y)(x^2 - y) = 0 \bmod p,$ άρα $x^2 = \pm y \bmod p,$ που σημαίνει 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 $-1 = (\frac{a}{b})^2 \bmod p$ αν διαιρέσουμε κατά μέλη, ήτοι το -1 είναι τετράγωνο $\bmod p$ και εφόσον $p = 3 \bmod 4$

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 $(x^2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \bmod p \Rightarrow x^{p-1} = -1 \bmod p$, αλλά $x^{p-1} = 1 \bmod p$ από 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 $x^2 = y$ και οι δύο ρίζες του $y \bmod p$ είναι $\pm x$. Αν το $-y$ έχει, τότε $x^2 = -y$ και οι δυο ρίζες του $-y$ είναι $\pm x$.

Παράδειγμα 3.2 :1) Να βρεθούν οι τετραγωνικές ρίζες του $5 \bmod 11$, όπου $11 = 3 \bmod 4$.

Λύση: $\frac{p+1}{4} = 3$ άρα $x = 5^3 \bmod 11 = 4 \bmod 11$, άρα οι τετραγωνικές ρίζες του $5 \bmod 11$ είναι ± 4. Πράγματι, $4^2 = 16 = 5 \bmod 11$.

2) Έστω η $x^2 = 71 \bmod 77$ (όπου ο 77 σύνθετος 77=7.11), λύνοντας έχουμε

$$x^2 = 71 = 1 \bmod 7, x^2 = 71 = 5 \bmod 11.$$
$$x = \pm 1 \bmod 7, x = \pm 4 \bmod 11$$

Με το ΚΘΥ θα ενώσω τις δύο ισοδυναμίες

$$\text{Η} \quad \begin{matrix} x = 1 \bmod 7 \ldots\ldots\ldots \{1,8,15,22,29,36,43,50,57,64,71\} \\ x = 4 \bmod 11 \ldots\ldots\ldots \{4,15,26,37,48,59,70,81\} \end{matrix} \Big\{ \Rightarrow x = 15 \bmod 77.$$

$$\text{Η} \quad \begin{matrix} x = -1 \bmod 7. \Rightarrow x = 6 \bmod 7 \ldots . \{6,13,81,20,27,34,41,48,55,62 \ldots .\} \\ x = 4 \bmod 11 \end{matrix}$$

$$\Big\{ \Rightarrow x = 48 \bmod 77 \Rightarrow x = -29 \bmod 77.$$

$$\text{Η} \quad \begin{matrix} x = 1 \bmod 7 \\ x = -4 \bmod 11 \Rightarrow x = 7 \bmod 11 \ldots \{7,18,29,40,51,62 \ldots .\} \end{matrix} \Rightarrow x = 29 \bmod 77.$$

Η $\begin{matrix} x=-11 \bmod 7 \\ x=-4 \bmod 11 \end{matrix} \begin{cases} \Rightarrow x=6 \bmod 7 \\ x=7 \bmod 11 \end{cases} \Rightarrow x=62 \bmod 77 \Rightarrow x=-15 \bmod 77.$

Άρα $x=\pm 15 \bmod 77, x=\pm 29 \bmod 77.$

Αν λοιπόν $n=pq$ και έστω οι τέσσερεις τετραγωνικές ρίζες $x=\pm a, x=\pm b$

χ=±α, x=±b της $x^2=y \bmod n.$

Από τα προηγούμενα γνωρίζουμε ότι :

$\begin{matrix} a=b \bmod p \\ a=-b \bmod q \end{matrix}$ { ή $\begin{matrix} a=-b \bmod p \\ a=b \bmod p \end{matrix}$

Το πρώτο σύστημα δίνει $p \mid a-b$ και q δεν διαιρεί το $a-b.$

Άρα $\text{ΜΚΔ}(a-b,n)=p$ από το βασικό κριτήριο και άρα βρήκαμε έναν μη τετριμμένο παράγοντα του $n.$ Συνεχίζοντας το παράδειγμα 3.2: $15^2=29^2=71 \bmod 77,$ άρα $(15-29,77)=7$ μας δίνει μη τετριμμένο παράγοντα του 77. Από τα παραπάνω βγαίνει η εξής αρχή:

Έστω $n=pq$ το γινόμενο δύο πρώτων με $p,q=3 \bmod 4$ και έστω ο y με

$\text{ΜΚΔ}(y,n)=1$ και που ο y έχει τετραγωνική ρίζα $\bmod n.$ Τότε η εύρεση των 4 ριζών

$x=\pm a, x=\pm b$ της $x^2=y \bmod n$ είναι υπολογιστικά ισοδύναμη με την παραγοντοποιήση του $n.$ Άρα, εκτός αν ο n έχει πολλούς πρώτους παράγοντες, η τυχαία επιλογή του a δεν αποδίδει. Η διαδικασία μας επιστρέφει στο τεστ του Fermat. Αφού ο n είναι μονός πρώτος, ο ζυγός $n-1$ γράφεται $n-1=u*2^k$ με $k \geq 1$ και u μονό. Άρα $a^{n-1}=(a^u \bmod n)^{2^k}$ το οποίο σημαίνει ότι μπορούμε να υπολογίσουμε το a^{n-1} σε $k+1$ βήματα. Θέτουμε $b_o=a^u \bmod n,$ $b_i=b_{i-1}^2 \bmod n,.....i=1,.....k$ οπότε $b_k=a^{n-1} \bmod n.$

Παράδειγμα 3.3 : $\begin{matrix} n=325=5^2 \cdot 13, \\ n-1=324=81 \cdot 2^2. \end{matrix}$

Υπολογίζουμε σε τρία βήματα τις δυνάμεις $a^{81}, a^{162}, a^{324} \bmod 325$ για διάφορα α (Πίνακας 1.0)

Παρατηρούμε ότι : το 2 είναι F-μάρτυρας $\in Z^*_{325}$, ενώ το 65 είναι F-μάρτυρας $\notin Z^*_{325}$.

Οι 7,32,49,126,210,224 είναι F-ψεύτες για το 325. $a^{n-1} \bmod n = 1.$

α	$b_o = a^{81}$	$b_1 = a^{81}$	$b_2 = a^{81}$
2	252	129	66
7	307	324	1
32	57	324	1
49	324	1	1
65	0	0	0
126	1	1	1
201	226	51	1
224	274	1	1

Πίνακας 1.0

Στα δύο βήματα $201^{162} = 51$ είναι μή τετριμμένη ρίζα της μονάδας, άρα 325 όχι πρώτος. Στο ένα βήμα το $224^{81} = 274$ μας δίνει επίσης μη τετριμμένη ρίζα της μονάδας. Άρα πάλι 325 όχι πρώτος, όμως για $a = 7,32,49$ και 126 δεν έχουμε περισσότερη πληροφορία αφού

$$7^{162} = 32^{162} = 49^{81} = -1 \bmod 325 = 324 \bmod 325.$$

Η ακολουθία λοιπόν $b_0,,,,,,,,b_k$ έχει τις παρακάτω μορφές:

Αν $b_i = 1$ ή $b_i = n-1$ τα υπόλοιπα στοιχεία $b_{i+1},,,,,,,,b_k$ είναι όλα 1, επομένως η ακολουθία αρχίζει με 0 ή με $b_0 \notin \{1, n-1\}$ και τελειώνει με 0 ή με 1 και τα κομμάτια χωρίζονται (όχι υποχρεωτικά) από το $n-1$. Ο πίνακας 2.0 δείχνει όλα τα δυνατά patterns, όπου * σημαίνει τυχόν αριθμό $\notin \{1, n-1\}$.

b_0	b_1	...				....	b_{k-1}	b_k	Περίπτωση
1	1		1	1	1		1	1	1α
$n-1$	1		1	1	1		1	1	1β
*	*		*	$n-1$	1		1	1	1β
*	*		*	*	*		*	$n-1$	2
*	*		*	*	*		*	*	2
*	*		*	1	1		1	1	3
*	*		*	*	*		*	1	3

Πίνακας 2.0 Δυνατές περιπτώσεις των δυνάμεων $a^{n-1} \bmod n$.

Περίπτωση 1α $b_0 = 1,$

1β $b_0 \neq 1$ αλλά $\exists\ i \leq k-1$ με $b_i = n-1.$

Και στις δυο υποπερπτώσεις έχουμε $b_k = 1,$ άρα δεν υφίσταται η πληροφορία αν ο n είναι πρώτος ή όχι.

Περίπτωση 2: Και στις δυο υποπεριπτώσεις $b_k \neq 1.$ Άρα ο n είναι σύνθετος και ο α είναι ένας F-μάρτυρας για τον $n.$

Περίπτωση 3: $b_0 \neq 1, b_k = 1,$ το $n-1$ δεν υπάρχει στην ακολουθία $b_i.$ Θεωρώ το ελάχιστο $i \geq 1$ με $b_i = 1.$ Από την υπόθεση $b_{i-1} \notin \{1, n-1\}$ άρα ο b_{i-1} είναι μη τετριμμένη ρίζα της μονάδας $\bmod n,$ που σημαίνει ότι ο n είναι πάλι σύνθετος.

Ορισμός : Έστω $n \geq 3$ μονός και γράφουμε $n-1 = u \cdot 2^k$ με u μονό και $k \geq 1.$ Ο αριθμός α, $1 \leq a \leq n$ ονομάζεται A-μάρτυρας για τον n αν $a^u \bmod n \neq 1$ και $a^{u*2^i} \bmod n \neq n-1$ για όλα τα i με $0 \leq i < k.$ Αν ο n είναι σύνθετος και ο α δεν είναι A-μάρτυρας του n, τότε ο α λέγεται A-ψεύτης του $n.$

Λήμμα 3.3*:* Αν ο *α* είναι Α-μάρτυρας του n, τότε ο n, είναι σύνθετος.

Απόδειξη: Αν ο α είναι Α-μάρτυρας του n, τότε ισχύουν οι περιπτώσεις 2 ή 3 άρα ο n σύνθετος. [Πρέπει να ληφθεί υπόψην ότι $j < k$, άρα το $b_k = n-1$ στην πρώτη γραμμή της περίπτωσης 2 και δεν δημιουργεί πρόβλημα].

Το Λήμμα αυτό και η τυχαία επιλογή του a από το $\{2,....n-2\}$ ενισχύουν το τεστ του Fermat σ' ένα ισχυρότερο κριτήριο που ονομάζεται κριτήριο Miller-Rabin.

Ιστορικό σχόλιο : Από την δεκαετία του 60 ο Artjuhov είχε προτείνει την ακολουθία b_i για ισχυροποίηση του τεστ του Fermat. Ο Miller με τη σειρά του το 1975 επινόησε έναν ντετερμινιστικό αλγόριθμο, που βασιζόταν στην εκτεταμένη υπόθεση του Riemann (Extended Riemann Hypothesis ή ERH) μία σημαντικότατη εικασία στη θεωρία των αριθμών. Το 1980 ο Rabin (και ο Monier ανεξάρτητα) είδαν την δυνατότητα μετατροπής της ντετερμινιστικής αναζήτησης για έναν Α-μάρτυρα σε έναν ικανοποιητικό πιθανοτικό αλγόριθμο. Ανεξάρτητα ένας άλλος πιθανοτικός αλγόριθμος με παρόμοιες ιδιότητες αλλά που βασίζεται σε διαφορετικές αριθμοθεωρητικές αρχές ανακαλύφθηκε στην ίδια χρονική περίοδο από τους Solovay Strassen.Μάλιστα ιστορικά οι δύο αυτοί πιθανοτικοί αλγόριθμοι για ένα πρόβλημα που δεν προϋπήρχε ικανοποιητικός ντετερμινιστικός αλγόριθμος ήταν βασικά παραδείγματα για την χρησιμότητα πιθανοτικών αλγορίθμων σε υπολογιστικά προβλήματα. Θα πρέπει να σημειωθεί ότι υπολογιστικά ο αλγόριθμος Miller-Rabin απαιτεί χρόνο εκτέλεσης $O((\log n)^3)$. Στην επόμενη παράγραφο αναφερόμαστε στο κριτήριο Miller-Rabin αναλυτικά.

<u>Αλγόριθμος Miller-Rabin</u>

Είσοδος: Μονός φυσικός $n \geq 3$

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

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

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 $\sim 4*10^{97}$ πρώτους τους μικρότερους του $10^{100} \sim \sqrt{n}$ (αριθμός μεγαλύτερος από ολα τα μόρια του σύμπαντος). Αν ο υπολογιστής εξετάζει 10^9 πρώτους ανά δευτερόλεπτο χρειαζόμαστε περίπου 10^{81} χρόνια.

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

Θεώρημα 3.4 (Βασικό Κριτήριο Παραγοντοποίησης) : Έστω ο φυσικός n και έστω ότι υπάρχουν φυσικοί x, y με $x^2 = y^2 \bmod n$, αλλά $x \neq \pm y \bmod n.$ Τότε ο n είναι σύνθετος και ο $d = MK\Delta(x-y, n)$ δίδει μή τετριμμένο παράγοντα του $n.$

Απόδειξη: Αν $d=n$ τότε $x = y \bmod n$ που δεν ισχύει εξ υποθέσεως. Αν $d=1$ από το θεώρημα $a \mid bc$ και $(a,b)=1 \Rightarrow a \mid$c, έχουμε $n \mid x^2 - y^2 = (x-y)\cdot(x+y)$ και

$d=1$ ήτοι $(n, x-y)=1 \Rightarrow n \mid x+y \Rightarrow x = -y \bmod n$ που δεν ισχύει εξ υποθέσεως. Άρα $d \neq 1, n$ και ο d μή τετριμμένος παράγοντας του σύνθετου $n.$

Παράδειγμα 3.4 : Είναι $12^2 = 2^2 \bmod 35$ με $12 \neq \pm 2 \bmod 35.$ Άρα ο 35 είναι σύνθετος και $MK\Delta(12-2, 35) = 5$ μή τετριμμένος παράγοντας του 35.

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 $a,\ 1<a<n-1.$ Υπολογίζω τον $b_0=a^m \bmod n.$ 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 $\text{ΜΚΔ}(b_0-1,n)$ 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 $b_2=-1 \bmod n$ τότε πιθανά είναι 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 3.5: Για $n=561$ είναι $n-1=560=16\cdot 35.$

Άρα $2^k=2^4 (k=4)$ και $m=35.$ Έστω $a=2,$ 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 $d=\text{ΜΚΔ}(66,561)=33$ μή τετριμμένο παράγοντα του 561. Πράγματι $561=3\cdot 11\cdot 17.$

Αν n σύνθετος και $\alpha^{n-1}=1 \bmod n$ λέμε ότι ο n είναι ψευδοπρώτος για την βάση α (ή και F-ψεύτης). Αν επιπλέον οι a,n είναι τέτοιοι ώστε ο n να επιτυγχάνει το test-Miller–Rabin, ο n είναι ισχυρός ψευδοπρώτος για τη βάση α.

Ο 561 είναι με τη σειρά του ψευδοπρώτος για τη βάση2 αλλά δεν είναι ισχυρός ψευδοπρώτος για τη βάση2 (Το ορίσαμε 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 τη 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 ένα σύνθετο με πιθανότητα $< \frac{1}{30.000}$ ενώ το κριτήριο Miller-Rabin με α=2 αποτυγχάνει με πιθανότητα $< \frac{1}{100.000}$. Ο πρώτος ισχυρός ψευδοπρώτος για τις βάσεις 2,3,5,7 είναι ο 3.215.031.751 ενώ για όλες τις πρώτες βάσεις τις < 200 είναι ένας ισχυρός ψευδοπρώτος με 337 ψηφία.

Κριτήριο των Miller –Rabin

Ας είναι n περιττός θετικός ακέραιος και $n-1 = 2^s d$, όπου d περιττός και s θετικός ακέραιος . Το κριτήριο των Miller-Rabin βασίζεται στο παρακάτω θεώρημα.

Θεώρημα 5.2 Αν ο n είναι πρώτος και α ένας ακέραιος ο οποίος δεν διαιρείται από τον η, τότε ισχύει $a^d \equiv 1(\mathrm{mod}\, n)$ είτε υπάρχει $r \in \{0,1,.....s-1\}$ με $a^{2^r * d} \equiv -1(\mathrm{mod}\, n).$

Απόδειξη: Ας είναι $k = ord_n(a^d)$ και καθώς ο n είναι πρώτος, έχουμε $(a^d)^{2^s} \equiv 1(\mathrm{mod}\, n)$ και επομένως ο k διαιρεί το 2^s. Αν $k = 1$ τότε $(a^d) \equiv 1(\mathrm{mod}\, n)$.

Αν $k > 1$, τότε $k = 2^i$, $1 \le i \le s$ και επομένως $ord_n(a^{2^{l-1} d}) = 2.$ Από την άλλη πλευρά,μόνον η κλάση του -1 μέσα στο Z_n^* έχει τάξη ίση με 2 και κατά συνέπεια έχουμε

$a^{2^{l-1} d} \neq -1(\mathrm{mod}\, n)$.

Παράδειγμα 5.4 Ας είναι $n = 561.$ Καθώς ο n είναι αριθμός του Carmicheal, το κριτήριο του Fermat δεν μπορεί να αποδείξει ότι ο n είναι σύνθετος. Επομένως με βάση τα παραπάνω έχουμε : $n-1 = 560 = 2^4.35$ και κάνουμε τους παρακάτω υπολογισμούς:

$2^{35} \equiv 263(\mathrm{mod}\, 561),\ 2^{35} \equiv \mathrm{mod}(561),$

$2^{4.35} \equiv 67(\mathrm{mod}\,561),\ 2^{8.35} \equiv 1\mathrm{mod}(561)$

όπου βλέπουμε ότι ο 2 είναι ένας μάρτυρας για την συνθετότητα του 561.

Επομένως ,σύμφωνα με το κριτήριο των Miller-Rabin ,συμπεραίνουμε ότι ο 561 είναι σύνθετος. Υπενθυμίζουμε ότι ο 561= $3\cdot 11\cdot 17$ είναι πρώτος αριθμός Carmichael. Η παρακάτω πρόταση μας εξασφαλίζει την ύπαρξη ενός ικανοποιητικού πλήθους μαρτύρων της συνθετότητας ενός σύνθετου ακέραιου.Αυτό είναι σημάντικό για την αποτελεσματικότητα του κριτηρίου των Miller-Rabin.

Πρόταση 5.1 Αν ο η είναι σύνθετος , τότε το σύνολο $\{1,...,n-1\}$ περιέχει το πολύ $(n-1)/4$ ακέραιους που είναι πρώτοι προς τον n και δεν είναι μάρτυρες της συνθετότητας του.

Απόδειξη.: θα προσδιορίσουμε το πλήθος των ακέραιων a με $(a,n)=1,$

$2 \le a \le n-1$ και $a^d \equiv 1(\mathrm{mod}\, n)$ ή $a^{2^r * d} \equiv -1(\mathrm{mod}\, n)$ για κάποιο $r \in \{0,1,.....s-1\}$. Ας υποθέσουμε ότι ένας τέτοιος ακέραιος a υπάρχει. Σ' αυτή την περίπτωση παρατηρούμε ότι πάντα υπάρχει ακέραιος a που ικανοποιεί την δεύτερη από τις δύο ισοτιμίες. Πράγματι,αν $a^d \equiv 1(\mathrm{mod}\, n),$ τότε $(-a^d) \equiv -1(\mathrm{mod}\, n).$ Ας είναι k ο μεγαλύτερος ακέραιος του συνόλου $\{0,1,....s-1\}$ για τον οποίο υπάρχει ακέραιος A με $(A,n)=1$ και $A^{2^k * d} \equiv -1(\mathrm{mod}\, n).$ Θέτουμε $m = 2^k d$ τότε ας είναι η $n = p_1^{s_1} ... p_v^{s_v}$ η πρωτογενής ανάλυση του $n.$ Επομένως θεωρούμε τα εξής υποσύνολα του Z_n^* :

$$J = \{\bar{a} \in \frac{Z_n^*}{a^{n-1}} \equiv 1(\mathrm{mod}\, n)\},$$

$$K = \{\bar{a} \in Z_n^* / a^m \equiv \pm 1(\mathrm{mod}\ p_i^{si}), (i = 1,...v))\},$$

$$L = \{\bar{\bar{a}} \in Z_n^* / a^m \equiv \pm 1(\mathrm{mod}\, n)\},$$

$$M = \{\bar{\bar{a}} \in Z_n^* / a^m \equiv 1(\mathrm{mod}\, n)\},$$

Διαπιστώνουμε εύκολα ότι τα παραπάνω σύνολα είναι υποομάδες του Z_n^* και ισχύει

$M \subseteq L \subseteq K \subseteq J$. Για κάθε $a \in Z$ με $(a,n)=1$ που δεν είναι μάρτυρας για την συνθετότητα του a, έχουμε $\bar{a} \in Z$ με $(a,n)=1$, που δεν είναι μάρτυρας γα την συνθετότητα του a, έχουμε $\bar{a} \in L$. Θα δείξουμε ότι $[Z_n^* : L \geq 4]$. Αν $\bar{a} \in K$, τότε $\bar{a} \in M$ και επομένως $[K:M]=2^i$, για κάποιον ακέραιο $i \geq 0$.

Άρα : $[K:M]=2^i, j \leq i$. Στην περίπτωση όπου $j \geq 2$, τότε η προς απόδειξη ανισότητα ισχύει. Υποθέτωντας ότι $j=0$, τότε $K=L$. Αν $\nu \geq 2$, τότε $\delta \in Z$ με $\delta \equiv A(\text{mod } p_1^{s_1})$ και $\delta \equiv 1(\text{mod } p_i^{si})(i=2,....\nu)$. Άρα ,έχουμε $\bar{\delta} \in K$ και $\bar{\delta} \notin L$ που είναι άτοπο. Ας είναι $\nu=1$ και ας θέσουμε $p=p_1, e=e_1$, άρα $\bar{a} \in J$, τότε $ord_p s(a) \mid p^s - 1$. Έτσι, καθώς $ord_p s(a) \mid \varphi(p^s)$, παίρνουμε $ord_p s(a) \mid p - 1$.

Αντιστρόφως , αν $ord_p s(a) \mid p - 1$, τότε $\bar{a} \in J$. Συνέπως, το J είναι η υποομάδα τάξης $p-1$ της ομάδας Z_{pe}^* και επομένως $[Z_{pe}^* : J] \geq 4$. Αν $p^e = 3^2$, τότε $d=1, s=3$. Άρα από τις ισοτιμίες προκύπτει το εξής:

$X \equiv 1(\text{mod } 9), X \equiv -1(\text{mod } 9),$
$X^2 \equiv -1(\text{mod } 9), X^4 \equiv -1(\text{mod } 9)$

προκύπτει ότι οι μονοί ακέραιοι του συνόλου {1,....8} που δεν είναι μάρτυρες της συνθετότητας του 9 είναι οι 1και 8.

Ας υποθέσουμε στη συνέχεια ότι $j=1$. Τότε υπάρχει $\bar{a} \in Z_n^*$ με $L \cup \bar{a}L = K$ και $a \bar{\notin}$. Ας είναι $\nu \geq 3)$, τότε χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $\nu \geq 3$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $\alpha^m \equiv 1(\text{mod } p_i^{si})(i=1,....r)$, $a^m \equiv -1(\text{mod } p_i^{si})(i=r+1,...\nu)$ με $r \geq 2$ και αν $r=1$, τότε αντικαθιστούμε τον a από αA. Θεωρούμε έναν ακέραιο c, όπου $c \equiv Aa(\text{mod } p_1^{e_1}), c \equiv 1(\text{mod}_2^{e_2}),...c \equiv 1(\text{mod } p_v^{e_v})$. Έχουμε $\bar{a} \notin L \cup \overline{aL}$ και κατά συνέπεια $\bar{c} \notin K$ που είναι άτοπο. Άρα ο n έχει μόνο δυο παράγοντες και επομένως δεν

είναι αριθμός Carmichael. Οπότε $J \neq Z_n^*$ και έτσι έχουμε $[Z_n^* : J] \geq 2$. Συνεπώς $[Z_n^* : L] \geq 4$. Από την παραπάνω πρόταση έπεται ότι η πιθανότητα ο n να είναι σύνθετος και ο τυχαίος ακέραιος a που παίρνουμε για να εφαρμόσουμε το Κριτήριο των Miller-Rabin να είναι μάρτυρας για την συνθετότητα του n είναι $\leq \frac{1}{4}$. Συνεπώς,αν επαναλάβουμε το κριτήριο r φορές, η πιθανότητα ο n να είναι σύνθετος και να μην βρεθεί μάρτυρας για την συνθετητότητα του είναι $\leq 1/4^r$. Για $r = 10$ βλέπουμε ότι αυτή η πιθανότητα είναι $\leq 1/2^{20}$ και συνεπώς η πιθανότητα ο n να είναι πρώτος είναι μεγαλύτερη από 0,999999.

Σύμβολο Legendre

Ορίζουμε το σύμβολο για πρώτο $p \geq 3$ και ακέραιο α

$$(\frac{a}{P}) = \begin{cases} 1, \ \alpha\nu \ \ \alpha \ E \ Q \ R \bmod p \\ -1, \ \alpha\nu \ \ \alpha \ R \ \mathbf{N} \ R \bmod p \\ 0, \ \alpha\nu \ \ \alpha = \pi o \lambda p \end{cases}$$

και το σύμβολο αυτό ονομάζεται **σύμβολο Legendre** των α και p.

Ιδιότητες

---

a) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ για α,b € Z.

b) $\left(\frac{a+cp}{p}\right) = \left(\frac{a}{p}\right)$ για α,c € Z.

c) $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$ για α € Z.

d) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ για p†b.

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

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

$\left(\frac{2}{p}\right)$ = 1 αν p = ± 1mod8 ή

$\left(\frac{2}{p}\right)$ = -1 αν p = ± 3mod8 .

Σύμβολο Jacobi

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

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

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

Παρατήρηση :

Συνεπώς για τος σύμβολο του Jacobi έχουμε ότι:

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

Όπου θεωρήσαμε το γενικευμένο σύμβολο του Legendre και κατά συνέπεια του Jacobi, για τα οποία θεωρούμε ότι είναι ίσα με το μηδέν αν $a\,|\,P.$ Οι ιδιότητες του συμβόλου περιγράφονται στην παρακάτω παράγραφο.

Ιδιότητες

1. Αν P περιττός πρώτος, τότε το σύμβολο $(\frac{a}{P})$ του Jacobi ταυτίζεται με το σύμβολο του Legendre.

2. Αν $a\equiv b(\mathrm{mod}\,P)$ τότε $(\frac{a}{P})=(\frac{b}{P}).$

3. $(\frac{a}{P})(\frac{b}{P})=(\frac{ab}{P})$

4. $(\frac{a}{PQ}) = (\frac{a}{P})(\frac{a}{Q})$

5. Νόμος Τετραγωνικής Αντιστροφής. Αν p≠q μόνοι πρώτοι τότε $(\frac{P}{Q})(\frac{q}{p}) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$

6. $(\frac{-1}{P}) = (-1)^{\frac{P-1}{2}} = \begin{cases} 1, \alpha\nu\ P \equiv 1 (\mathrm{mod}\, 4) \\ -1, \alpha\nu\ P \equiv 3 (\mathrm{mod}\, 4) \end{cases}$

7. $(\frac{2}{P}) = (-1)^{\frac{P^2-1}{8}} = \begin{cases} 1, \alpha\nu\ P \equiv 1\ \acute{\eta}\ 7 (\mathrm{mod}\, 8) \\ -1, \alpha\nu\ P \equiv 3\ \acute{\eta}\ 5 (\mathrm{mod}\, 8) \end{cases}$

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.

Αλγόριθμος για την εύρεση του συμβόλου Jacobi

Αλγόριθμος (Σύμβολο του Jacobi)

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

$b \leftarrow a \bmod n$
$c \leftarrow n$
$s \leftarrow 1$

While $b \geq 2$ repeat

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

if $2 \mid b$ then

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

$b \leftarrow b/2$

end_if

if $b = 1$ then break

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

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

end_while

return $s \cdot b$

Παρατηρήσεις:

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

2) Η πολυπλοκότητα του αλγόριθμου για δυο αριθμούς με n ψηφία είναι $O(M(n)\log n)$, 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
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

$$\left(\frac{1828}{757}\right)=(\frac{314}{757})=(\frac{2}{757})(\frac{157}{757})=(-1)^{\frac{757^2-1}{8}}\cdot 157^{\frac{757-1}{2}}(\mathrm{mod}\,757)=$$
$$(-1)\cdot 157^{378}(\mathrm{mod}\,757)=(-1)\cdot(-1)=1.$$

Κριτήριο των Solovay – Strassen

Είσοδος : μονός ακέραιος n ≥ 3

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

2 if $\alpha^{(n-1)/2}*\left(\frac{a}{n}\right)\mathrm{mod}n \neq 1$

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 $\alpha^{(n-1)/2}\mathrm{mod}n$ γίνεται με fast exponentiation. Ο παραπάνω αλγόριθμος είναι $O((\log n)^3)$. 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 .

Σύγκριση των Fermat, Solovay-Strassen και Miller-Rabin.

Από αυτά τα τρία τεστ πιστοποιησης πρώτων, το τεστ Miller-Rabin είναι το καλύτερο και μάλιστα είναι αυτό που χρησιμοποιείται, στην κρυπτογραφία.

Πρόταση

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

Απόδειξη:

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

Αν $a^r \equiv 1 \bmod n \Rightarrow a^{r2^{s-1}} \equiv a^{\frac{n-1}{2}} \equiv 1 \bmod n \Rightarrow (\frac{a}{n}) \equiv 1$, αφού $a^{\frac{n-1}{2}} \equiv 1 \bmod n$, για κάθε k παράγοντα του n και $(\frac{a}{k_1 k_2}) = (\frac{a}{k_1}) \cdot (\frac{a}{k_2})$, $a^r \neq 1 \bmod n$ και $a^{2^j r} \equiv -1 \bmod n$, άρα ο α είναι ισχυρός μάρτυρας. Αν $a^r \neq 1 \bmod n$ και $a^{2^j r} \equiv -1 \bmod n$ για κάποιο $j, 0 \le j \le s-1$, τότε εντελώς όμοια καταλήγουμε ότι ο είναι ισχυρός μάρτυρας για το n. Σύμφωνα λοιπόν με τα παραπάνω μπορούμε να πούμε ότι :

Fermat-ψεύτες $\subseteq$ Euler- ψεύτες $\subseteq$ ισχυροί ψεύτες Συνεπώς από άποψη ακρίβειας των τεστ, το τεστ Miller-Rabin είναι καλύτερο, εκτός της περίπτωσης που $n \equiv 3 \bmod 4$, όπου είναι το ίδιο καλό όσο το Solovay-Strassen. Από άποψη πολυπλοκότητας το Miller Rabin είναι καλύτερο από το Solovay-Stassen, λόγω του ότι στο 2^o πρέπει να υπολογιστεί το σύμβολο Jacobi.

Από άποψη πολυπλοκότητας το Miller-Rabin δεν είναι καλύτερο από αυτό του Fermat και για αυτό το τελευταίο χρησιμοποιείται κατά κόρον ακόμα και στην κρυπτογραφία. Παρόλα αυτά το τεστ του Fermat έχει ως βασικό μειονέκτημα τους απείρως το πλήθος αριθμούς Carmichael.

Αλγόριθμος AKS

Σ' αυτή την ενότητα θα περιγράψουμε τον αλγόριθμο AKS ο οποίος αποφασίζει σε πολυωνυμικό χρόνο αν ένας θετικός ακέραιος n είναι πρώτος ή σύνθετος. Τα βήματα του είναι τα εξής:

1. Αν υπάρχουν ακέραιοι $a \ge 2$ και $k \ge 2$ με $n = a^k$, τότε ο n είναι σύνθετος.

2. Να βρεθεί ο μικρότερος πρώτος r με $ord_r(n) \ge 4(\log_2 n)^2 + 2$ και θέτουμε $j = [2\sqrt{r} \log n] + 1.$

3. Αν κάποιος από τους ακέραιους $2,3.....,j$ διαιρεί τον n, τότε ο n είναι σύνθετος.

4. Αν ισχύει $(X-a)^n \neq X^n - a(R_{n,r})$, για κάποιο $a \in \{1,....j\}$, τότε ο n σύνθετος.

5. Αν ο n δεν έχει βρεθεί σύνθετος σε κάποιο από τα προηγούμενα βήματα, τότε αυτός είναι ο πρώτος.

Ο χρόνος εκτέλεσης του αλγόριθμου σύμφωνα με το Λήμμα 5.5, που απαιτείται για το πρώτο βήμα είναι $O((\log n)^4)$. Για τον πρώτο r του δεύτερου βήματος , καθώς $ord_r(n) \geq 4(\log_2 n)^2 + 2$ θα έχουμε $r \geq [(4(\log_2 n)^2] + 3$. Η εύρεση του γίνεται με τον εξής τρόπο, για κάθε $q = 4(\log_2 n)^2 + 2$, υπολογίζουμε το υπόλοιπο u της διαίρεσης του n με τον q και κατόπιν τις δυνάμεις $u^i (i = 1,2,....4(\log_2 n)^2 + 2)(\text{mod}\, q)$. Αν $u^i \neq 1(\text{mod}\, q)$ για κάθε $(i = 1,2,....4(\log_2 n)^2)$, τότε εξετάζουμε αν ο q είναι πρώτος

εφαρμόζοντας την μέθοδο της Ενότητας 5.1. Από το Λήμμα 5.1 έχουμε ότι για τον πρώτο r του δεύτερου βήματος ισχύει $r = O(\log n)^5)$. Επομένως, ο χρόνος που απαιτείται για να βρεθεί ο r είναι $r = O(\log n)^8)$. Στο τρίτο βήμα, η εκτέλεση όλων των διαιρέσεων απαιτεί χρόνο $O((\log n)^5)$. Τέλος, από τα Λήμματα 5.5 έχουμε ότι ο χρόνος που χρειάζεται για το τέταρτο βήμα είναι $O((\log n)^{17})$, που συνεπάγεται ότι είναι και ο χρόνος εκτέλεσης του αλγορίθμου.

Στην συνέχεια θ' αποδείξουμε την ορθότητα του αλγόριθμου. Κατ' αρχάς ας υποθέσουμε ότι ο ακέραιος n είναι πρώτος. Από τα βήματα 1 και 3 δεν συνάγεται ότι n είναι σύνθετος. Επίσης έχουμε $(X-a)^n \equiv X^n - a(R_{n,r})$, οπότε ο αλγόριθμος. Ας υποθέσουμε τώρα ότι ο ακέραιος n είναι σύνθετος και ότι ο αλγόριθμος διαπιστώνει ότι είναι πρώτος .Θα δείξουμε ότι δεν είναι δυνατόν να συμβαίνει αυτό . Σ' αυτή την περίπτωση έχουμε ότι για $a = 1,....., j$ ισχύει :

$(X-a)^n \equiv X^n - a(R_{n,r})$.

Ας είναι p ένας διαιρέτης του n. Τότε

$$(X-a)^n \equiv X^n - a(R_{p-r}).$$

Καθώς ο p είναι πρώτος , ισχύει

$(X-a)^p \equiv X^p - a(R_{p,r})$.

Από τις παραπάνω σχέσεις και από το λήμμα βάση του οποίου αν p πρώτος και είναι m_1, m_2 θετικοί ακέραιοι τέτοιοι ώστε να ισχύει $(X-a)^{m_i} \equiv X^{m_i} - a(R_{p,r})(i=1,2)$, τότε $(X-a)^{m_1 m_2} \equiv X^{m_1 m_2} - a(R_{p,r})$ συνεπάγεται ότι για κάθε ζεύγος ακεραίων $i \geq 0,\ j \geq 0$ και $a = 1,.....,l$ ισχύει:

$$(X-a)^{p^i n^j} \equiv X^{p^i n^j} - a(R_{p,r}).$$

Ας είναι t η τάξη της υποομάδας που παράγεται μέσα στη Z_R^* από τις κλάσεις των p και $n.$ Θεωρούμε το σύνολο

$$E = \left\{ \frac{n^i p^j}{0} \leq i, j \leq [\sqrt{t}] \right\}$$

Επομένως με βάση το λήμμα ότι αν είναι n θετικός ακέραιος που δεν είναι δύναμη πρώτου, t θετικός ακέραιος και p πρώτος και το σύνολο $E = \left\{ \frac{n^i p^j}{0} \leq i, j \leq [\sqrt{t}] \right\}$, έχουμε $|E| > t.$ Οπότε υπάρχουν δύο ακέραιοι $m_1 = p^{i_1} n^{j_1}$ και $m_2 = p^{i_2} n^{j_2}$ του Ε με $(i_1, j_1) \neq (i_2, j_2)$ και $m_1 = m_2 (\mathrm{mod}\, r).$ Άρα ,υπάρχει ακέραιος k με $m_2 = m_1 + kr$ και ισχύει $(X-a)^{m_2} \equiv X^{m_1+kr} - a \equiv X^{m_1} - a \equiv (X-a)^{m_1} (R_{p,r}).$

Συνεπώς , για $a = 1,.....j$ έχουμε $(X-a)^{m_2} \equiv (X-a)^{m_1} (R_{p,r}).$

Σύμφωνα με το Λήμμα βάση του οποίου αν είναι p πρώτοι με $r \neq p$ τότε υπάρχει ένα πεπερασμένο σώμα K χαρακτηριστικής p και $\omega \in K$ έτσι, ώστε η τάξη του ω μέσα στη πολλαπλασιαστική ομάδα του K να ισούται με r. Καθώς η χαρακτηριστική του K ισούται με p , μπορούμε να υποθέσουμε, χωρίς βλάβη της γενικότητας, ότι το Z_p είναι υπόσωμα του $K.$ Οπότε , για $a = 1,...., j$ έχουμε ότι $(\omega - a)^{m_1} = (\omega - a)^{m_2}$ (όπου $\bar{\bar{a}}$ είναι η λύση του a μέσα στο Z_p)και επομένως το $(\omega - \bar{\bar{a}})$ είναι ρίζα του πολυώνυμου $F(X) = X^{m_1} - X^{m_2}$ μέσα στο $K.$ Θέτουμε $L = [2\sqrt{t}] \log_2 n] + 1$ και παρατηρούμε ότι αν ρ_1, ρ_2 είναι ρίζες του $F(X),$ τότε το γινόμενο $\rho_1 . \rho_2$ είναι επίσης

Ρίζα του $F(X)$, και επομένως κάθε στοιχείο του συνόλου $S=\left\{\prod_{a=1}^{L}(\omega-\bar{a})^{e_2/e^a}\in\{0,1\}\right\}$ είναι ρίζα του $F(X)$. Θα αποδειχθεί ότι τα στοιχεία του S είναι διακεκριμμένα. Από το τρίτο βήμα του αλγόριθμου έχουμε ότι κανένας από τους ακέραιους $2,3,.....j$ δεν διαιρεί τον n. Καθώς $t\le r-1$, έχουμε $L\le j$ και κατ'επέκταση $L<p$. Άρα, οι κλάσεις των ακεραίων $1,....L(\mathrm{mod}\,p)$ είναι διαφορετικές ανά δύο και κατά συνέπεια πολυώνυμα της μορφής $g(X)=\prod_{a=1}^{L}(X-\bar{a})^{e_a}$ είναι διακεκριμμένα. Παρατηρούμε ότι τα στοιχεία του S είναι της μορφής $g(\omega)$. Επομένως για κάθε ζεύγος ακεραίων $i\ge 0,\ j\ge 0$ έχουμε τα εξής:

$g(X)^{n^i p^j}\equiv g(X^{n^i p^j})(R_{p,r})$ και επομένως $g(\omega)^{n^i p^j}=g(\omega^{n^i p^j})$.

Ας είναι $g_1(X)$ και $g_2(X)$ πολυώνυμα της παραπάνω μορφής με $g_1(\omega)=g_2(\omega)$.

Οπότε για κάθε ζεύγος ακεραίων $i,j\ge 0$ έχουμε $g_1(\omega^{n^i p^j})=g_2(\omega^{n^{ip^j}})$ καθώς η τάξη του ω ισούται με r, το $\omega^{n^i p^j}$ παίρνει τόσες διακεκριμμένες τιμές όσο είναι το πλήθος των διακεκριμμένων κλάσεων ($(\mathrm{mod}\,r)$ των στοιχείων $n^i p^j$. Άρα το πολυώνυμο $g_1(X)-g_2(X)$ έχει τουλάχιστον t ρίζες μέσα στο K. Από την άλλη πλευρά έχουμε $t\ge ord_{(n)}\ge 4(\log_2 n)^2+2$ και επομένως $L\le 2\sqrt{t}\log_2 n+1\le\sqrt{t^2-2t}+1<t$.

Καθώς $g_1(X)-g_2(X)$ έχει βαθμό $\le L$ και τουλάχιστον t ρίζες, παίρνουμε $g_1(X)=g_2(X)$. Επομένως, τα στοιχεία του S είναι διακεκριμμένα και κατά συνέπεια $|S|=2^L$. Έτσι ,το $F(X)$ έχει τουλάχιστον 2^L ρίζες μέσα στο K. Από την άλλη πλευρά ο βαθμός του $F(X)$ είναι $\max\{m_1,m_2\}\le n^{2[\sqrt{t}]}<2^L$. Συνεπώς ,το $F(X)$ είναι το μηδενικό πολυώνυμο και επομένως $m_1=m_2$ δηλαδή $p^{i_1}n^{j_1}=p^{i_2}n^{j_2}$.

Καθώς $(i_1,j_1)\ne(i_2,j_2)$ παίρνουμε $n=p^s$ για κάποιο ακέραιο $s\ge 1$. Αν $s>1$, τότε από το βήμα 1 θα είχαμε ότι ο n είναι σύνθετος, ενώ αν $s=1$, τότε ο n είναι πρώτος. Και στις δύο περιπτώσεις καταλήγουμε σε άτοπο γιατί υποθέσαμε ότι ο n είναι σύνθετος και ότι ο αλγόριθμος διαπιστώνει ότι είναι πρώτος. Συνεπώς, αν ο n είναι σύνθετος , τότε ο αλγόριθμος το διαπιστώνει σε κάποιο από τα βήματά του.

Επίλογος: Ο *Euler σχολίασε: «Οι μαθηματικοί προσπάθησαν μάταια, για να ανακαλύψουν κάποια τάξη στην ακολουθία των πρώτων αριθμών και έχουμε λόγο να πιστεύουμε ότι αυτό είναι ένα μυστήριο μέσα στο οποίο το μυαλό δεν πρόκειται ποτέ να διεισδύσει.»*

Βιβλιογραφία

[1] http://en.wikipedia.org/wiki/Great_Internet_Mersenne_Prime_Search.

[2] http://en.wikipedia.org/wiki/RSA_(algorithm).

[3] http://users.auth.gr/users/4/2/050524/public_html/crypto/Kef.3.pdf.

[4]http://el.wikipedia.org/..../Εικασία_.....

[5] Havil.J.''Exploring Euler's constant ,'Princeton University Press', ISBN 0-691-09983-09.

[6] Πουλάκης Δ.Μ., '' ΚΡΥΠΤΟΓΡΑΦΙΑ. Η ΕΠΙΣΤΗΜΗ ΤΗΣ ΑΣΦΑΛΟΥΣ ΕΠΙΚΟΝΩΝΙΑΣ '', ΕΚΔΟΣΕΙΣ ΖΗΤΗ, ΘΕΣΣΑΛΟΝΙΚΗ 2006.

[7] Ε. Ζάχος – Επιστήμη στη Θεωρία Αριθμών και την Κρυπτογραφία.

[8] Χ. Κουκουβίνος & Α. Παπαιωάννου - Κρυπτογραφία