ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

ΕΙΣΑΓΩΓΗ ΣΤΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ ΚΑΙ ΜΕΘΟΔΟΙ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΑΚΕΡΑΙΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΣΙΑΝΤΟΥ ΜΑΡΘΑ

ΕΠΙΒΛΕΠΩΝ:

ΠΑΠΑΪΩΑΝΝΟΥ ΑΛΕΞΑΝΔΡΟΣ, ΑΝ. ΚΑΘΗΓΗΤΗΣ ΣΕΜΦΕ, ΕΜΠ

Αθήνα, Φεβρουάριος 2013

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΚΑΙ ΦΥΣΙΚΩΝ ΑΠΙΣΤΗΜΩΝ
ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

ΕΙΣΑΓΩΓΗ ΣΤΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ ΚΑΙ ΜΕΘΟΔΟΙ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΑΚΕΡΑΙΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΣΙΑΝΤΟΥ ΜΑΡΘΑ

ΕΠΙΒΛΕΠΩΝ:
ΠΑΠΑΪΩΑΝΝΟΥ ΑΛΕΞΑΝΔΡΟΣ, ΑΝ. ΚΑΘΗΓΗΤΗΣ ΣΕΜΦΕ, Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 2013.

……	……	……
Παπαϊωάννου Αλέξανδρος	**Κουκουβίνος Χρήστος**	**Στεφανέας Πέτρος**

Αθήνα, Φεβρουάριος 2013

……

Τσιάντου Μάρθα

Ευχαριστίες

Πριν ξεκινήσει η παρουσίαση της παρούσας διπλωματικής εργασίας θα ήθελα να σταθώ στους ανθρώπους οι οποίοι βοήθησαν, ο καθένας με το δικό του τρόπο, στην ολοκλήρωσή της. Ευχαριστώ λοιπόν από τα βάθη της καρδιάς μου:

- Τον κ. Παπαϊωάννου Αλέξανδρο, τόσο για την ανάθεση της διπλωματικής αυτής, όσο και για την καθοδήγηση και την συνδρομή του,
- Τον Βασίλη,
- Τον αδερφό μου, Γιώργο και
- Τους γονείς μου, Δημήτρη και Τασία, που με στηρίζουν όλα αυτά τα χρόνια.

Περίληψη

Στην παρούσα διπλωματική εργασία θα ασχοληθούμε με κάποια βασικά στοιχεία της Θεωρίας Αριθμών και της Κρυπτογραφίας.

Στο πρώτο κεφάλαιο θα παρουσιάσουμε μερικά βασικά θεωρήματα της Θεωρίας Αριθμών, όπως τα αυτά του Euler και του Wilson. Επίσης, θα εξετάσουμε την Θεωρία Τετραγωνικών Υπολοίπων.

Στο δεύτερο κεφάλαιο, θα επικεντρωθούμε στα τεστ πιστοποίησης πρώτων αριθμών: Fermat, Solovay – Strassen και Miller Rabin.

Στο τρίτο κεφάλαιο, θα περιγράψουμε τις μεθόδους παραγοντοποίησης ακεραίων αριθμών και τους αντίστοιχους αλγόριθμους που έχουν αναπτυχθεί ώστε να είναι εφικτή η παραγοντοποίησή τους.

Abstract

In the present thesis we state certain basic elements of the Theory of Numbers and Cryptography.

In the first chapter, we present certain basic theorems of the Theory of Numbers, as those of Euler and Wilson. Also, we examine the Theory of Square Residuals.

In the second chapter, we focus on primality certificates testing: presenting the Fermat, Solovay – Strassen and Miller Rabin tests.

In the third chapter, we describe the methods of factorization of integers and the corresponding algorithms that have been developed so that the factorization is feasible.

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ ΣΤΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

1.1. Βασικά Θεωρήματα

1.1.1. Το θεώρημα του Euler

Αν α, m ακέραιοι με $(\alpha, m) \equiv 1$, τότε $\alpha^{\varphi(m)} \equiv 1 \pmod{m}$, όπου $\varphi(m)$ η συνάρτηση του Euler και (α, m) ο μέγιστος κοινός διαιρέτης των α, m.

Απόδειξη:

Για $m = 2$, το θεώρημα ισχύει, διότι αν $(\alpha, 2) = 1$, ο α είναι περιττός.

Για $m \geq 3$, θεωρούμε τους $\varphi(m)$ το πλήθος αριθμούς $r_1, r_2, \dots, r_{\varphi(m)}$ σχετικά πρώτους με το m. Πολλαπλασιάζοντας με το α $(\text{mod } m)$ παίρνουμε τους αριθμούς:

$$\alpha \cdot r_1, \alpha \cdot r_2, \dots, , \alpha \cdot r_{\varphi(m)} \pmod{m}.$$

Επειδή $(\alpha, m) = 1$, ούτε ο α ούτε ο r_i έχουν παράγοντα τον αριθμό m, άρα ο αr_i είναι σχετικά πρώτος με τον m $\forall$ i. Άρα $\alpha r_i = r_j$ για κάποιο j. Ακόμα, για $i \neq j$ αποκλείεται να έχουμε $\alpha r_i = \alpha r_j \pmod{m}$, αφού τότε από το νόμο διαγραφής θα είχαμε $r_i = r_j \pmod{m}$, καθώς $(\alpha, m) = 1$. Άρα, οι αριθμοί $\alpha \cdot r_1, \alpha \cdot r_2, \dots, \alpha \cdot r_{\varphi(m)} \pmod{m}$ είναι ίδιοι με τους $r_1, r_2, \dots, r_{\varphi(m)}$ με διαφορετική ίσως διάταξη. Συνεπώς έχουμε:

$$(\alpha \cdot r_1), (\alpha \cdot r_2), \dots, (\alpha \cdot r_{\varphi(m)}) \equiv r_1 r_2 \dots r_{\varphi(m)} \pmod{m} \text{ ή}$$
$$\alpha^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)} \equiv r_1 r_2 \dots r_{\varphi(m)} \pmod{m} \text{ ή}$$
$$\alpha^{\varphi(m)} \equiv 1 \pmod{m}, \text{ αφού } (m, r_i) = 1 \ \forall \ i.$$

Μία ειδική περίπτωση του θεωρήματος Euler αποτελεί το "Μικρό θεώρημα του Fermat".

Το Μικρό Θεώρημα του Fermat:

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

Απόδειξη:

Ο p είναι πρώτος, συνεπώς έχουμε ότι $\varphi(p) = p - 1$, άρα από το προηγούμενο θεώρημα έχουμε το ζητούμενο.

1.1.2. Το θεώρημα του Wilson

Ο φυσικός $p > 2$ είναι πρώτος ανν $(p-1)! \equiv -1 \pmod p$.

Απόδειξη με θεωρία ομάδων:

Για κάθε πρώτο p, κάθε αριθμός μικρότερος του p και μεγαλύτερος του μηδενός έχει έναν μοναδικό πολλαπλασιαστικό αντίστροφο. Ακόμα, η ισοτιμία $x^2 \equiv \alpha \pmod p$ έχει ακριβώς δύο λύσεις. Άρα, εφόσον $(p-1)^2 \equiv 1^2 \equiv 1 \pmod p$, οι αριθμοί 2, 3, …., $p-2$ αποτελούν ζεύγη αντιστρόφων (mod p). Άρα, $2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod p$. Συνεπώς, $(p-1)! = 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv -1 \pmod p$.

Αντιστρόφως, αν $(p-1)! \equiv -1 \pmod p$ και p σύνθετος, βλέπουμε ότι για $p \leq 4$ δεν ισχύει. Για $p > 4$, θεωρούμε ότι $p = \alpha b$ για κάποιους α,b με $1 < \alpha, b < p$ και $\alpha \neq b$. Άρα, βλέπουμε ότι οι α, b υπάρχουν ως όροι στο $(p-1)!$, άρα $(p-1)! \equiv 0 \pmod p$.

Αν $p = q^2$ με q πρώτο, τότε οι q και 2q υπάρχουν στο γινόμενο, κάτι που οδηγεί σε άτοπο. Άρα, ο p είναι πρώτος.

Απόδειξη Lagrange:

Έστω το πολυώνυμο $f(x) = (x-1)(x-2) \cdot \ldots \cdot \big(x-(p-1)\big) - (x^{p-1} - 1)$, με p πρώτο αριθμό και $x = 1, 2, \ldots, p-1$. Συνεπώς, $(x, p) = 1$ και ένας από τους ακεραίους $(x-1), (x-2), \ldots, \big(x-(p-1)\big)$ θα ισούται με μηδέν.

Από το θεώρημα του Fermat ισχύει $x^{p-1} - 1 \equiv 0 \pmod p$, δηλαδή $p|(x^{p-1} - 1)$ και $p|(x-1)(x-2) \cdot \ldots \cdot \big(x-(p-1)\big)$, εφόσον $p|0$. Άρα, $p|\ f(x)$.

Ωστόσο, το πολυώνυμο f(x) είναι $p-2$ βαθμού, με γενική μορφή:

$$f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_{p-2} x^{p-2},\ a_\iota \in Z$$

$$\text{όπου } \alpha_0 = (p-1)! + 1.$$

Άρα, από το θεώρημα συντελεστών πολυωνύμου και από το ότι $p|\ f(x)$ έχουμε ότι $p|\ \alpha_0$ και, άρα, $(p-1)! \equiv -1 \pmod p$.

Αντιστρόφως, αν $(p-1)! \equiv -1 \pmod p$, τότε , $p|(p-1)! + 1$, όμως ο p είναι ο μικρότερος θετικός διαιρέτης του, αφού δεν έχει κανένα μικρότερο δεν διαιρέτη. Συνεπώς, ο p είναι πρώτος.

1.2. Τετραγωνικά υπόλοιπα

1.2.1. Τετραγωνικά υπόλοιπα – Ορισμοί και Προτάσεις

Ορισμός (Τετραγωνικό Υπόλοιπο):

Ο αριθμός α καλείται τετραγωνικό υπόλοιπο modulo p, αν η ισοτιμία $x^2 \equiv \alpha (\mathrm{mod}\ p)$ έχει λύση.

Παράδειγμα:

Έστω $p = 7$. Οι αριθμοί 1, 4, 9 είναι τέλεια τετράγωνα αλλά δεν διαιρούνται με τον 7. Άρα, είναι τετραγωνικά υπόλοιπα mod 7. Αλλά και όλοι οι ακέραιοι που είναι ισοδύναμοι με τα τετράγωνα αυτά mod 7 είναι επίσης τετραγωνικά υπόλοιπα mod 7, όπως οι 2, 11 κτλ. Ο 49 όμως αν και τέλειο τετράγωνο δεν είναι τετραγωνικό υπόλοιπο mod 7 διότι $7 \mid 49$.

Πρόταση:

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

Απόδειξη:

Έστω x_0 μια λύση της ισοτιμίας, τότε $x_0^2 \equiv \alpha \ (\mathrm{mod}\ p)$. Παρατηρούμε ότι και το $-x_0$ είναι λύση, αφού $(-x_0)^2 = x_0^2 \equiv \alpha \ (\mathrm{mod}\ p)$. Ακόμα, ισχύει ότι το x_0 είναι διαφορετικό από το $-x_0$ αφού αν $x_0 \equiv -x_0 \ (\mathrm{mod}\ p)$ τότε $p \mid 2x_0$, δηλαδή $p \mid x_0$, και άρα $p \mid x_0^2$. Καταλήγουμε σε άτοπο.

Θα δείξουμε τώρα ότι δεν υπάρχουν άλλες λύσεις. Έστω x_1 μια άλλη λύση της ισοτιμίας, τότε $x_0^2 \equiv x_1^2 \equiv \alpha \ (\mathrm{mod}\ p)$ δηλαδή $x_0^2 - x_1^2 \equiv 0 \ (\mathrm{mod}\ p)$, άρα, $p \mid (x_0 - x_1)(x_0 + x_1)$. Συνεπώς, είτε $p \mid (x_0 - x_1)$, είτε $p \mid (x_0 + x_1)$, αφού ο p είναι πρώτος. Οπότε, $x_1 \equiv x_0 (\mathrm{mod}\ p)$ ή $x_1 \equiv -x_0 (\mathrm{mod}\ p)$, άρα, δεν υπάρχουν άλλες λύσεις.

Πρόταση:

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

Απόδειξη:

Βλέπουμε ότι για $x \in \{1, 2, \ldots, p-1\}$, $x^2 \equiv (-x)^2 \pmod{p}$ και αν για $x \neq y \pmod{p}$ ισχύει ότι $x^2 \equiv y^2 \pmod{p}$, τότε $x \equiv y \pmod{p}$ ή $x \equiv -y \pmod{p}$, που είναι άτοπο. Άρα, υπάρχουν ακριβώς $(p-1)/2$ τετραγωνικά υπόλοιπα και $(p-1)/2$ μη τετραγωνικά υπόλοιπα modulo p.

Θεώρημα (Κριτήριο Euler για τα τετραγωνικά υπόλοιπα):

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

$$\alpha^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Απόδειξη:

Έστω ότι το $\alpha \neq 0$ είναι τετραγωνικό υπόλοιπο modulo p. Τότε, υπάρχει ακέραιος x_0 τέτοιος ώστε $x_0^2 \equiv \alpha \pmod{p}$. Συνεπώς, έχουμε $x_0^{p-1} \equiv \alpha^{\frac{p-1}{2}} \pmod{p}$ και από το μικρό θεώρημα του Fermat έχουμε $x_0^{p-1} \equiv 1 \pmod{p}$, άρα $\alpha^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

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

$$1x, 2x, 3x, \ldots, (p-1)x \pmod{p}.$$

Αυτοί οι αριθμοί είναι διαφορετικοί μεταξύ τους, διότι αν $kx = jx \pmod{p}$, τότε $p|(kx - jx)$, δηλαδή $p|\, x$ ή $p|\,(k-j)$, άρα $k \equiv j \pmod{p}$, καταλήγουμε σε άτοπο. Άρα, οι παραπάνω αριθμοί θα είναι οι αριθμοί $1, 2, \ldots, (p-1)$ με διαφορετική ίσως διάταξη. Άρα, αφού $1 \leq \alpha \leq p-1$ για κάποιο x θα υπάρχει μοναδικό $y \in \{1, 2, \ldots, p-1\}$, έτσι ώστε $xy \equiv \alpha \pmod{p}$, με $y \neq x$ εφόσον το α δεν είναι τετραγωνικό υπόλοιπο. Συνεπώς, μπορούμε να χωρίσουμε το σύνολο $\{1, 2, \ldots, p-1\}$ σε $\frac{p-1}{2}$ ζεύγη, έτσι ώστε το γινόμενο των ζευγών κάθε ζεύγος να είναι α. Άρα $(p-1)! \equiv \alpha^{\frac{p-1}{2}} \pmod{p}$ το οποίο είναι ισοδύναμο με $\alpha^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ από το θεώρημα του Wilson. Καταλήγουμε στο συμπέρασμα

ότι αν α τετραγωνικό υπόλοιπο τότε $\alpha^{\frac{p-1}{2}} \equiv 1(\text{mod p})$, διαφορετικά $\alpha^{\frac{p-1}{2}} \equiv -1 \text{ (mod p)}$.

Πρόταση (Λήμμα του Gauss):

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

$$\alpha, 2\alpha, 3\alpha, \ldots, \frac{p-1}{2}\ \alpha \text{ (mod p)}.$$

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

$$n \equiv (\alpha - 1)\frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}}[\frac{j\,\alpha}{p}]\ (mod\ 2)$$

Απόδειξη:

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

Έστω $k_1, k_2, \ldots, k_n$ οι n αριθμοί που είναι μεγαλύτεροι από το $\frac{p}{2}$ και $l_1, l_2, \ldots, l_m$ οι $m=\frac{p-1}{2} - n$, οι υπόλοιποι αριθμοί που είναι μικρότεροι του $\frac{p}{2}$. (Κανένας αριθμός από τους $\alpha, 2\alpha, 3\alpha, \ldots, \frac{p-1}{2}\ \alpha(\text{mod p})$ δεν είναι ίσος με $\frac{p}{2}$, αφού ο p είναι περιττός πρώτος).

Επειδή $\frac{p}{2} < k_i < p$, έχουμε $0 < p - k_i < \frac{p}{2}$, $\forall$ i. Θα δείξουμε ότι οι αριθμοί $p - k_i$ είναι διαφορετικοί modulo p από τους $l_1, l_2, \ldots, l_m$. Πράγματι, αν είχαμε $p - k_i \equiv l_j (\text{mod p})$ για κάποιους k_i, l_j, τότε $k_i + l_j \equiv 0(\text{mod p})$ ή $x\alpha + y\alpha \equiv 0(\text{mod p})$, με $k_i = x\alpha$, $l_j = y\alpha$ και $1 \le x, y \le \frac{p-1}{2}$. Άρα, p| (x+y), αφού (α, p)=1, άτοπο, αφού $2 \le x + y \le p - 1$.
Επίσης, αφού οι αριθμοί $p - k_1, p - k_2, \ldots, p - k_n$ είναι διαφορετικοί μεταξύ τους έχουμε ότι οι $n + m = \frac{p-1}{2}$ αριθμοί $p - k_1, p - k_2, \ldots, p - k_n, l_1, l_2, \ldots, l_m$ είναι μια μετάθεση των αριθμών 1, 2 , 3,...., $\frac{p-1}{2}$.

$$\text{Άρα: } (p - k_1)(p - k_2)\ldots(p - k_n)\ l_1\, l_2\ \ldots . l_m \equiv (\tfrac{p-1}{2})!\ (\text{mod p})$$

ή

$$(-1)^n\, k_1\, k_2 \ldots\ldots k_n\, l_1\, l_2 \ldots\ldots l_m \equiv (\tfrac{p-1}{2})!\ (\mathrm{mod}\ p).$$

Επιπλέον, έχουμε ότι $k_1\, k_2 \ldots\ldots k_n\, l_1\, l_2 \ldots\ldots l_m = \alpha\,(2\alpha)(3\alpha)\ldots(\frac{p-1}{2}\ \alpha) = (\frac{p-1}{2})!\ \alpha^{\frac{p-1}{2}}$.

Άρα: $(-1)^n\, \alpha^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!\ (\mathrm{mod}\ p)$

ή

$$\alpha^{\frac{p-1}{2}} \equiv (-1)^n \bmod p.$$

Από το κριτήριο του Euler συνεπάγεται ότι το α είναι τετραγωνικό υπόλοιπο ανν ο n είναι άρτιος.

Πρέπει να δείξουμε ότι:

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

Έχουμε ότι:

$\alpha = \left[\frac{\alpha}{p}\right] p + r_1,\ 2\alpha = \left[\frac{2\,\alpha}{p}\right] p + r_2, \ldots., \frac{p-1}{2}\ \alpha = \left[\frac{r\,\alpha}{p}\right] p + r_{\frac{p-1}{2}}$, όπου $0 \le r_i < p,\ \forall\, i.$

Προσθέτουμε τα παραπάνω και προκύπτει ότι:

$$\alpha\,(1 + 2 + \ldots.. + \tfrac{p-1}{2}) = p \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{j\,\alpha}{p}\right] + \sum_{j=1}^{n} k_j + \sum_{j=1}^{\frac{p-1}{2}-n} l_j\,.$$

Όπως ξέρουμε από πριν :

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

Άρα:

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

ή

$$(\alpha-1)\,\frac{p^2-1}{8} = p \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{j\,\alpha}{p}\right] + np + 2\sum_{j=1}^{n} k_j \equiv p \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{j\,\alpha}{p}\right] + n (\mathrm{mod}\ 2)\,.$$

Οπότε:

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

1.2.2. Το σύμβολο του Legendre

Ορισμός (Το σύμβολο του Legendre):

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

$$\left(\frac{\alpha}{p}\right) = \begin{cases} +1, \text{αν το α είναι τετραγωνικό υπόλοιπο mod p} \\ -1, \text{αν το α είναι τετραγωνικό μη υπόλοιπο mod p} \end{cases}$$

Μπορούμε να ορίσουμε ισοδύναμα το $(\frac{\alpha}{p})$ ως εξής χρησιμοποιώντας το κριτήριο του Euler:

$$(\frac{\alpha}{p}) \coloneqq \alpha^{\frac{p-1}{2}} (\text{mod } p)\,.$$

Ισχύουν οι παρακάτω ιδιότητες:

1. Αν $\alpha \equiv b(\text{mod } p)$, τότε $(\frac{\alpha}{p}) = (\frac{b}{p})$.

<u>Απόδειξη:</u> Άμεση συνέπεια του κριτήριο του Euler και των ιδιοτήτων των ισοτιμιών.

2. $(\frac{\alpha b}{p}) = \left(\frac{\alpha}{p}\right)\left(\frac{b}{p}\right)$, με $(\alpha b, p) = 1$.

<u>Απόδειξη:</u> Άμεση συνέπεια του κριτήριο του Euler και των ιδιοτήτων των ισοτιμιών.

3. $(\frac{\alpha^2}{p}) = 1$.

<u>Απόδειξη:</u> Άμεση συνέπεια της ιδιότητας 2.

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

<u>Απόδειξη:</u> Άμεση συνέπεια του κριτηρίου του Euler.

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

<u>Απόδειξη:</u> Σύμφωνα με το λήμμα του Gauss, αρκεί να υπολογίσουμε πόσοι από τους αριθμούς 2,4,6,…,p-1 είναι μεγαλύτεροι του $\frac{p}{2}$. Χρησιμοποιώντας τον ίδιο συμβολισμό με την απόδειξη του λήμματος του Gauss έχουμε:

$$2+4+6+\ldots..+(p-1)=k_1+k_2+\cdots+k_n+l_1+l_2+\cdots+l_m \text{ ή}$$
$$\frac{p^2-1}{4}=k_1+k_2+\cdots+k_n+l_1+l_2+\cdots+l_m \qquad (1)$$

Όμως, είδαμε ότι οι αριθμοί $p-k_1$, $p-k_2$, …. , $p-k_n, l_1$, l_2, … , l_m είναι μια μετάθεση των αριθμών 1, 2 ,3, …., $\frac{p-1}{2}$.
Άρα έχουμε ότι:

$$(p-k_1)+(p-k_2)+\ldots\ldots+(p-k_n)+l_1+l_2+\ldots+l_m=1+2+3+\ldots+\frac{p-1}{2}$$
$$np-(k_1+k_2+\ldots+k_n)(l_1+l_2+\ldots l_m)=\frac{p^2-1}{8} \qquad (2)$$

Προσθέτοντας τις (1),(2) κατά μέλη έχουμε $np\equiv\frac{p^2-1}{8}+2(k_1+k_2+\ldots+k_n)$.
Συνεπώς, $np\equiv\frac{p^2-1}{8}\pmod 2$, άρα $np\equiv\frac{p^2-1}{8}\pmod 2$, αφού ο p περιττός.
΄Αρα, $(\frac{2}{p})=(-1)^n=(-1)^{\frac{p^2-1}{8}}$.

Θεώρημα (Νόμος τετραγωνικής αντιστροφής του Legendre):

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

ή ισοδύναμα:

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

Απόδειξη:

Σύμφωνα με το Λήμμα του Gauss έχουμε:

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

Άρα, 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:

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

Αν $(x, y) \neq (0,0)$, τότε $f(x,y) \neq 0$. Πραγματικά βλέπουμε ότι αν $f(x,y) = 0$, τότε $qx = py$. Καθώς $(p,q)=1$, έχουμε $p|\ x$ και $q|\ y$ που είναι άτοπο, γιατί $|x| < \frac{p}{2}$ και $|y| < \frac{q}{2}$, απ' όπου $f(x,y) - f(x', y') = f(x - x', y - y') \neq 0$.
Συνεπώς, $f(x,y) \neq f(x',y')$. Άρα, 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.

Στη συνέχεια, θα υπολογίσουμε το πλήθος των θετικών τιμών και το πλήθος των αρνητικών του $f(x,y)$, με $x \in S$ και $y \in T$.

Για κάθε $x \in S$, θα έχουμε $f(x,y) > 0$ με $y \in T$, αν και μόνο αν, $y < \frac{qx}{p}$, ή $y \leq [\frac{qx}{p}]$.

Συνεπώς, το πλήθος m των θετικών τιμών του $f(x,y)$, με $x \in S$ και $y \in T$, είναι:

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

και το πλήθος n των αρνητικών τιμών του του $f(x,y)$, με $x \in S$ και $y \in T$, είναι:

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

Άρα θα έχουμε:

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

απ'όπου προκύπτει το ζητούμενο.

1.2.3. Γενική μορφή λύσης ισοτιμίας δευτέρου βαθμού

Θεώρημα:

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

Απόδειξη:

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

$$x_1^2 \equiv \alpha(\mathrm{mod}\ p^r) \text{ ή}$$

$$p^r \mid x_1^2 - \alpha \text{ ή}$$

$$x_1^2 - \alpha \text{ ή}$$

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

δηλαδή η $x^2 \equiv \alpha(\mathrm{mod}\ p)$ είναι επιλύσιμη.

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

Έστω $x= x_0 + p^{r-1}y$.

Θεωρούμε την ισοτιμία: $(x=x_0+p^{r-1}y)^2 \equiv \alpha(\mathrm{mod}\ p^r)$

με άγνωστο τον y.

Έχουμε : $x_0^2 + p^{2r-2}y^2 + 2x_0yp^{r-1} \equiv \alpha(\mathrm{mod}\ p^r)$ ή

$$x_0^2 + 2x_0yp^{r-1} \equiv \alpha(\mathrm{mod}\ p^r)$$

εφόσον $p^r \mid p^{2r-2}$.

Άρα θα έχουμε ότι:

$$2x_0yp^{r-1} \equiv \alpha - x_0^2 (\mathrm{mod}\ p^r).$$

Όμως, ισχύει ότι $\alpha - x_0^2 \equiv 0(\mathrm{mod}\ p^{r-1})$, συνεπώς ο αριθμός $\frac{\alpha - x_0^2}{p^{r-1}}$ είναι ακέραιος, άρα:

$$2x_0y \equiv \frac{\alpha - x_0^2}{p^{r-1}} (\mathrm{mod}\ p).$$

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 $x^2 \equiv \alpha(\mathrm{mod}\, p^r)$ είναι:

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

συνεπώς είναι επιλύσιμη.

Θεώρημα:

Η ισοτιμία $x^2 \equiv \alpha \pmod{2^k}$, $k \geq 3$, α περιττός, είναι επιλύσιμη αν και μόνο αν

$\alpha \equiv 1(\mathrm{mod}\, 8)$.

Απόδειξη:

Για k=3 η ισοτιμία γράφεται $x^2 \equiv \alpha \pmod 8$. Εφόσον ο α είναι περιττός πρέπει και ο x να είναι περιττός. Όμως, επειδή το τετράγωνο οποιουδήποτε περιττού είναι 1 (mod 8), πρέπει $\alpha \equiv 1(\mathrm{mod}\, 8)$. Αντιστρόφως, αν $\alpha \equiv 1(\mathrm{mod}\, 8)$, τότε η $x^2 \equiv 1(\mathrm{mod}\, 8)$ έχει προφανείς λύσεις $x \equiv 1, 3, 5, 7(\mathrm{mod}\, 8)$.

Υποθέτουμε ότι η πρόταση ισχύει για κάποιο k και έστω ότι η ισοτιμία $x^2 \equiv \alpha(\mathrm{mod}\ 2^{k+1})$ είναι επιλύσιμη με λύση x_0. Τότε $x_0^2 \equiv \alpha \pmod{2^k}$, άρα από την υπόθεση έχουμε ότι $\alpha \equiv 1(\mathrm{mod}\, 8)$.

Αντιστρόφως, αν $\alpha \equiv 1(\mathrm{mod}\, 8)$ θέτουμε $x= x_0 + 2^k y$ Και εργαζόμενοι όπως στο προηγούμενο θεώρημα καταλήγουμε στο συμπέρασμα ότι η ισοτιμία είναι επιλύσιμη.

Θεώρημα:

Έστω η ισοτιμία $x^2 \equiv \alpha \pmod m$ όπου $m= m_1 \cdot \ldots \cdot m_k$ με $(m_i, m_j) = 1 \ \forall\, i, j$. Η παραπάνω ισοτιμία είναι επιλύσιμη αν και μόνο αν καθεμία από τις ισοτιμίες $x^2 \equiv \alpha \pmod{m_i}, i = 1, 2, \ldots, k$ είναι επιλύσιμη.

Απόδειξη:

Αν $x^2 \equiv \alpha(\mathrm{mod}\, m) \Rightarrow m|(x^2 - \alpha) \Rightarrow m_1 \cdot \ldots \cdot m_k | (x^2 - \alpha) \Rightarrow m_i | (x^2 - \alpha) \ \forall\, i,$

δηλαδή $x^2 \equiv \alpha(\mathrm{mod}\, m_i),\ i = 1, 2, \ldots, k$, αφού $(m_i, m_j) = 1 \ \forall$ i,j.

Αντιστρόφως, αν $x^2 \equiv \alpha(\mathrm{mod}\, m_i), i = 1, 2, \ldots, k$ το ζητούμενο είναι προφανές.

1.2.4. Το σύμβολο Jacobi και ο αλγόριθμος για την εύρεσή του

Ορισμός (Το σύμβολο του Jacobi):

Έστω P περιττός θετικός ακέραιος και α ένας ακέραιος αριθμός, τέτοιος ώστε (α, P)=1.

Τότε, ορίζουμε το σύμβολο του Jacobi $\left(\frac{\alpha}{P}\right)$ ως εξής:

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

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

Άρα, για το σύμβολο του Jacobi έχουμε ότι:

$$\left(\frac{\alpha}{P}\right)=\begin{cases}0, \text{αν } \alpha\equiv 0(\text{mod } P)\\ 1, \text{αν για κάποιο ακέραιο x, } \alpha\equiv x^2(\text{mod } P) \text{και p δεν διαιρεί το } \alpha\\ -1, \text{αν δεν υπάρχει τέτοιο x}\end{cases}$$

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

Ισχύουν οι παρακάτω ιδιότητες:

1. Αν P περιττός πρώτος, τότε το σύμβολο $\left(\frac{\alpha}{P}\right)$ του Jacobi ταυτίζεται με το σύμβολο του Legendre.
2. Αν $\alpha\equiv b(\text{mod } P)$ τότε $\left(\frac{\alpha}{P}\right)=\left(\frac{b}{P}\right)$.
3. $\left(\frac{\alpha}{P}\right)\left(\frac{b}{P}\right)=\left(\frac{\alpha b}{P}\right)$
4. $\left(\frac{\alpha}{PQ}\right)=\left(\frac{\alpha}{P}\right)\left(\frac{\alpha}{Q}\right)$
5. $\left(\frac{m}{P}\right)=\left(\frac{P}{m}\right)\left(-1^{\frac{P-1}{2}\cdot\frac{m-1}{2}}\right)=\begin{cases}\left(\frac{P}{m}\right), \text{αν } P\equiv 1\ (\text{mod } 4) \text{ ή } m\equiv 1\ (\text{mod } 4)\\ -\left(\frac{P}{m}\right), \text{αν } P\equiv m\equiv 3\ (\text{mod } 4)\end{cases}$,

   για (P,m)=1 (Νόμος Τετραγωνικής Αντιστροφής).
6. $\left(-\frac{1}{P}\right)=(-1)^{\frac{P-1}{2}}=\begin{cases}1, \text{αν } P\equiv 1\ (\text{mod } 4)\\ -1, \text{αν } P\equiv 3(\text{mod } 4)\end{cases}$.
7. $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}=\begin{cases}1, \text{αν } P\equiv 1 \text{ ή } 7(\text{mod } 8)\\ -1, \text{αν } P\equiv 3 \text{ ή } 5\ (\text{mod } 8)\end{cases}$.

Αλγόριθμος (Σύμβολο Jacobi):

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

$b \leftarrow \alpha \bmod n$

$c \leftarrow n$

$s \leftarrow 1$

while $b \geq 2$ repeat

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

  if $2|b$ then

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

    $b \leftarrow b/2$

  end_if

  if $b = 1$ then break

  if $b \bmod 4 = c \bmod 4 = 3$ 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 συμβούλου του Jacobi.

2) Η πολυπλοκότητα του αλγορίθμου για δύο 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:

$\alpha=1828$, $n=757$

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 αριθμός 757 είναι πρώτος. Συνεπώς, το $\left(\frac{1828}{757}\right)$ είναι ένα σύμβολο Legendre:

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

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

2. ΤΕΣΤ ΠΙΣΤΟΠΟΙΗΣΗΣ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ

Ο διαχωρισμός των πρώτων αριθμών από τους σύνθετους έχει αποτελέσει ένα από τα δυσκολότερα και, ταυτόχρονα, πιο ενδιαφέροντα προβλήματα της αριθμητικής.

Στις 4 Σεπτεμβρίου 2006 ανακαλύφθηκε ο μεγαλύτερος γνωστός πρώτος αριθμός. Είναι ο $2^{32.582.657} - 1$ και έχει 9.808.358 ψηφία. Έχει 650.000 περισσότερα ψηφία από τον προηγούμενο μεγαλύτερο πρώτο αριθμό, που είχε βρεθεί τον Δεκέμβριο του 2005. Τον ανακάλυψαν οι Κέρτις Κούπερ και Στίβεν Μπουν, καθηγητές του Κρατικού Πανεπιστημίου του Κεντρικού Μιζούρι, μέσω του προγράμματος GIMPS (Great Internet Mersenne Prime Search).

Στη συνέχεια, θα δούμε το Θεώρημα πρώτων αριθμών, το οποίο απαντά στην ερώτηση "πόσους αριθμούς θα πρέπει να ελέγξουμε, ώστε να βρούμε έναν ο οποίος να είναι πρώτος".

Θεώρημα (Το θεώρημα των πρώτων αριθμών):

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

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

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 $\frac{\chi}{\pi(x)} = \frac{1}{\ln x}$. 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. Άρα, 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 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 και Miller-Rabin.

2.1. Το τεστ του Fermat

Περιγραφή του τεστ του Fermat:

Από το μικρό θεώρημα του Fermat έχουμε ότι για έναν πρώτο αριθμό n και για ακέραιο α με $1 \leq \alpha \leq n - 1$, ισχύει $\alpha^{n-1} \equiv 1 \bmod n$. Συνεπώς αν θέλουμε να εξετάσουμε αν ένας δοσμένος ακέραιος n είναι πρώτος και βρούμε ένα α, με $1 \leq \alpha \leq n - 1$, για τον οποίο δεν ισχύει το μικρό θεώρημα του Fermat, τότε μπορούμε να πούμε με βεβαιότητα ότι ο n είναι σύνθετος.

Ορισμός:

Έστω n ένας περιττός σύνθετος ακέραιος. Ο ακέραιος α, για τον οποίο ισχύει $1 \leq \alpha \leq n - 1$ και $\alpha^{n-1} \neq 1 \bmod n$, ονομάζεται Fermat – μάρτυρας για το n.

Ορισμός:

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

Παράδειγμα:

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

Αλγόριθμος (Τεστ του Fermat):

FERMAT (n, t)

INPUT: ένα περιττό ακέραιο n ≥3 και συντελεστή ασφάλειας t≥1.

OUTPUT: θα απαντά 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 α, $2 \leq \alpha \leq n-2$.
   B. Υπολόγισε το $r = \alpha^{n-1} \bmod n$.
   C. If $r \neq 1$ then return (" ο n είναι σύνθετος").
2. Return ("ο n είναι πρώτος με συντελεστή ασφάλειας t").■

Παρατήρηση: Αν ο παραπάνω αλγόριθμος μας επιστρέψει "ο n είναι σύνθετος", τότε μπορούμε να πούμε ότι ο n είναι σίγουρα σύνθετος, όμως, 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 ασφάλειας t".

Λήμμα:

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

Απόδειξη:

Από την Ευκλείδεια διαίρεση έχουμε ότι $\alpha^{n-1} = k \cdot n + u$, με $0 \leq u \leq n$ και $k \in Z$. Αφού d| α και d| n ⇒ d| α^{n-1} και d| $k \cdot n$ ⇒ d| u. Συνεπώς, d| r.

Παρατήρηση:

Άρα, αν α ακέραιος με $1 \leq \alpha \leq n-1$ και $(\alpha, n) \neq 1$, τότε $\alpha^{n-1} \neq 1 \bmod n$. Δηλαδή το τέστ του Fermat θα μας είχε επιστρέψει ότι ο n είναι σύνθετος.

Θεώρημα:

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

Απόδειξη:

Έστω το σύνολο $G_n = \{x: x \in \mathbb{Z}_n^* \text{ και } (x, n) = 1\}$. Είναι γνωστό ότι το G_n είναι ομάδα με πράξη τον πολλαπλασιασμό mod n.

Έστω το σύνολο $A=\{k:k\in G_n \text{ και } k^{n-1} \equiv 1 \bmod n\}$ των Fermat – ψευτών.

Θα δείξουμε ότι τι 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 $1^{n-1} \equiv 1 \bmod n$, $(1, n) \equiv 1$ 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, αφού $l\in G_n$ λόγω του ότι ισχύει ότι $A\subseteq G_n$ και G_n ομάδα. Έστω $h\in G_n$ ο αντίστροφος του l, άρα $hl\equiv 1 \bmod n \Rightarrow (hl)^{n-1} \equiv 1 \bmod n \Rightarrow h^{n-1} \cdot l^{n-1} \equiv 1 \bmod n \Rightarrow h^{n-1} \equiv 1 \bmod n$, άρα $h \in A$, αφού $l^{n-1} \equiv 1 \bmod n$.
E. Το A είναι κλειστό ως προς το πολλαπλασιασμό modulo n. Έστω $u, w \in A$, τότε επειδή $A \subseteq G_n$ και G_n ομάδα, έχουμε ότι $u \cdot w \in G_n$. Αρκεί να δείξουμε ότι το $u \cdot w \in A$, δηλαδή ότι $(u \cdot w)^{n-1} \equiv 1 \bmod n$.Όμως, $(u \cdot w)^{n-1} = u^{n-1} \cdot w^{n-1} \equiv 1 \cdot 1 = 1 \bmod n$.

Άρα, το A είναι υποομάδα του G_n.

Από υπόθεση υπάρχει α με $(\alpha, n)=1$, $\alpha^{n-1} \neq 1 \bmod n$ και $\alpha \in \mathbb{Z}_n^*$.

Άρα $\alpha \in G_n$ και $\alpha \notin A$, δηλαδή η A είναι γνήσια υποομάδα της G_n.

Άρα, 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 $s\geq 2$. Άρα, η πιθανότητα να βρούμε έναν ακέραιο k, $1\leq k \leq n\text{-}1$ με $k^{n-1} \neq 1 \bmod n$ και $(k, n) = 1$ είναι $P = 1 - \frac{|A|}{|G_n|} = 1 - \frac{|A|}{|A| \cdot s} = 1 - \frac{1}{s}$ 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 τεστ 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). Παρ' όλα αυτά, έχει το μειονέκτημα ότι υπάρχουν αριθμοί που είναι σύνθετοι και δεν υπάρχουν Fermat – μάρτυρες για αυτούς.

Ορισμός:

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

Παράδειγμα:

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 $n-1$.

Απόδειξη:

Έστω n αριθμός του Carmichael. Έστω p^t, p πρώτος, η μεγαλύτερος δύναμη του p που διαιρεί το n και g μια πρωταρχική ρίζα $\bmod p^t$. Επειδή $(p^t, \frac{n}{p^t}) = 1$, από το Κινέζικο θεώρημα των υπολοίπων έχουμε ότι υπάρχει ακέραιος b με $b \equiv g \bmod p^t$ και $b \equiv 1 \bmod \frac{n}{p^t}$. Συνεπώς, $(b, p) = 1, \left(b\frac{n}{p^t}\right) = 1$και άρα $(b, n) = 1$. Αφού ο n είναι αριθμός Carmichael έχουμε ότι $b^{n-1} \equiv 1 \bmod n \overset{p^t|n}{\Longrightarrow} b^{n-1} \equiv 1 \bmod p^t$ και επειδή ο b είναι πρωταρχική ρίζα $\bmod p^t$, έχουμε ότι $\varphi(p^t)|n-1 \Rightarrow p^{t-1}(p-1)|n-1$, όπου $\varphi(x)$ η συνάρτηση του Euler. Άρα, $p-1|\ n-1$.

Αντιστρόφως, υποθέτουμε ότι ο n είναι ελεύθερος τετραγώνου και για κάθε πρώτο διαιρέτη p του n ισχύει $p-1|\ n-1$.

Έστω α ακέραιος με (α,n)=1. Επειδή p πρώτος, από το μικρό θεώρημα του Fermat έχουμε $\alpha^{p-1} \equiv 1 \bmod p$ και επειδή $p-1|n-1$, έχουμε $\alpha^{n-1} \equiv 1 \bmod p$. Όμως ο n είναι ελεύθερος τετραγώνου, συνεπώς από το Κινέζικο θεώρημα υπολοίπων έχουμε ότι $\alpha^{n-1} \equiv 1 \bmod n$.

Πόρισμα

Ένας αριθμός Carmichael έχει τουλάχιστον τρείς πρώτους παράγοντες.

Απόδειξη

Έστω n ένας αριθμός Carmichael. Άρα, ο n είναι σύνθετος.

Υποθέτουμε ότι $n = pq$, όπου p,q πρώτοι με p>q. Από το παραπάνω θεώρημα έχουμε ότι $p-1|n-1 \Rightarrow p-1|pq-1 \Rightarrow p-1|(p-1)q+q-1 \Rightarrow p-1|q-1$ $\Rightarrow p \leq q$, άτοπο. Άρα ο n έχει τουλάχιστον τρείς 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 $C(n)<ne^{\frac{\ln\ln\ln\ln n}{\ln\ln n}}$.

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 , 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.

Από το κριτήριο του Euler έχουμε ότι για έναν περιττό πρώτο ισχύει το εξής:
$\alpha^{\frac{n-1}{2}} \equiv \left(\frac{\alpha}{n}\right) \bmod n$, για κάθε ακέραιο α με $(\alpha, n) = 1$ και $\left(\frac{\alpha}{n}\right)$ το σύμβολο του Jacobi.

Ορισμός:

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

Ορισμός:

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

Παράδειγμα:

Έστω ο ακέραιος $91 = 7 \cdot 13$. Παρατηρούμε ότι $9^{\frac{91-1}{2}} = 9^{45} \equiv 1 \bmod 91$ και $\left(\frac{9}{91}\right) = 1$.
Συνεπώς, 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 $7^{\frac{783-1}{2}} = 7^{391} \equiv 25 \bmod 783$ και $\left(\frac{7}{783}\right) = 1$.
Συνεπώς, ο 7 είναι Euler – μάρτυρας για το n.

Αλγόριθμος (Τεστ Solovay – Strassen):

INPUT: έναν περιττό ακέραιο $n \geq 3$ και συντελεστή ασφαλείας $t \geq 1$.

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 α, $2 \leq \alpha \leq n-2$.
   b. Υπολόγισε το $r = \alpha^{\frac{n-1}{2}} \bmod n$.
   c. If $r \neq 1$ και $r \neq n-1$ then return ("ο n είναι σύνθετος").
   d. Υπολόγισε το σύμβολο του Jacobi $s = (\frac{\alpha}{n})$.
   e. If $r \neq s \bmod n$ then return ("ο n είναι σύνθετος").
2. Return ("ο n είναι πρώτος με συντελεστή ασφαλείας t").■

Παρατήρηση:

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

Λήμμα:

Έστω n περιττός ακέραιος, α ακέραιος με $1 \leq \alpha \leq n-1$, $d = (\alpha, n)$ και $r = \alpha^{\frac{n-1}{2}} \bmod n$. Τότε $d \mid r$.

Απόδειξη:

Από την ευκλείδεια διαίρεση έχουμε ότι $\alpha^{\frac{n-1}{2}} = k \cdot n = u$, με $0 \leq u < n$ και $k \in Z$. Αφού $d \mid \alpha$ και $d \mid n \Rightarrow d \mid \alpha^{\frac{n-1}{2}}$ και $d \mid k \cdot n \Rightarrow d \mid u$. Άρα, $d \mid r$.

Πρόταση:

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

Απόδειξη:

Έστω α Euler –ψεύτης του n, τότε $\alpha^{\frac{n-1}{2}} \equiv \left(\frac{\alpha}{n}\right) \bmod n$ και επειδή

$\left(\frac{\alpha}{n}\right) = \begin{cases} +1, \text{αν α τετραγωνικό υπόλοιπο mod n} \\ -1, \text{αν α μη τετραγωνικό υπόλοιπο mod n} \end{cases}$,

έχουμε ότι $\alpha^{\frac{n-1}{2}} \cdot \left(\frac{\alpha}{n}\right) \equiv 1 \bmod n$.

Άρα $(\alpha^{\frac{n-1}{2}} \cdot \left(\frac{\alpha}{n}\right))^2 \equiv 1^2 \bmod n \Rightarrow \alpha^{n-1} \cdot (\frac{\alpha}{n})^2 \equiv 1 \bmod n \Rightarrow \alpha^{n-1} \equiv 1 \bmod n$ και εφόσον ο n είναι σύνθετος έχουμε ότι ο α είναι Fermat – ψεύτης.

Πρόταση:

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

Απόδειξη:

Από το αντίστοιχο θεώρημα που αποδείξαμε για το τεστ του Fermat και την παραπάνω πρόταση, έχουμε ότι $B \subseteq A$ (το σύνολο των Fermat ψευτών)$\subseteq G_n$.

Επίσης, όπως αναφέραμε και νωρίτερα το G_n είναι πολλαπλασιαστική ομάδα.

A. Άρα, $B \subseteq G_n$

B. Η διμελής πράξη του πολλαπλασιασμού στο B είναι προσεταιριστική ως η επαγόμενη πράξη από την ομάδα G_n.

C. Υπάρχει ταυτοτικό στοιχείο και είναι το $1 \in B$, αφού $1^{\frac{n-1}{2}} \equiv \left(\frac{1}{n}\right) \bmod n, (1, n) = 1$ 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, αφού $l \in G_n$ λόγω του ότι ισχύει ότι $B \subseteq G_n$ και G_n ομάδα. Έστω $h \in G_n$ ο αντίστροφος του l, άρα $hl \equiv 1 \bmod n \Rightarrow (hl)^{\frac{n-1}{2}} \equiv 1 \bmod n \Rightarrow h^{\frac{n-1}{2}} \cdot l^{\frac{n-1}{2}} \equiv 1 \bmod n \Rightarrow h^{\frac{n-1}{2}} \cdot \left(\frac{l}{n}\right) \equiv 1 = (\frac{l}{n})^2 \bmod n \Rightarrow h^{\frac{n-1}{2}} \equiv \left(\frac{l}{n}\right) \bmod n$. Όμως, $hl \equiv 1 \bmod n \Rightarrow \left(\frac{hl}{n}\right) = \left(\frac{1}{n}\right) = 1$ 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 $h^{\frac{n-1}{2}} \equiv \left(\frac{h}{n}\right) \bmod n$, δηλαδή $h \in B$.

Ε. Το Β είναι κλειστό ως προς τον πολλαπλασιασμό modulo n. Έστω $u,w \in B$ τότε επειδή $B \subseteq G_n$ και G_n υποομάδα έχουμε ότι $u \cdot w \in G_n$. Αρκεί να δείξουμε ότι το $u \cdot w \in B$, δηλαδή ότι $(u \cdot w)^{\frac{n-1}{2}} \equiv \left(\frac{uw}{n}\right) \bmod n$. Όμως, $(u \cdot w)^{\frac{n-1}{2}} = u^{\frac{n-1}{2}} \cdot w^{\frac{n-1}{2}} \equiv \left(\frac{u}{n}\right) \cdot \left(\frac{w}{n}\right) = \left(\frac{uw}{n}\right) \bmod n$.

Συνεπώς, το Β είναι υποομάδα του G_n.

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

Διακρίνουμε δύο περιπτώσεις:

Α. 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 $b \in G_n$ κάποιο μη τετραγωνικό υπόλοιπο mod p, δηλαδή $\left(\frac{b}{p}\right) = -1$. Από το Κινέζικο Θεώρημα των υπολοίπων υπάρχει $1 \leq \alpha < n$ με $\alpha \equiv b \bmod p$ (1) και $\alpha \equiv 1 \bmod m$ (2).

θα δείξουμε ότι $\alpha \in G_n$ και α Euler – μάρτυρας του n.

<u>Απόδειξη ισχυρισμού:</u>
Από την σχέση (1) έχουμε ότι $\alpha - b \equiv 0 \bmod p \Rightarrow \alpha - b = \text{πολ } p$ και επειδή $\left(\frac{b}{p}\right) = 1 \Rightarrow b \neq 0 \bmod p \Rightarrow p \nmid b$, συμπεραίνουμε ότι $p \nmid \alpha$.
Ακόμη από τη σχέση (2) έχουμε ότι $(\alpha, m)=1$, διότι $\alpha - 1 = \text{πολ } m$.
Άρα, $\alpha \in G_n$.
Τέλος, παρατηρούμε ότι $\left(\frac{\alpha}{n}\right) = \left(\frac{\alpha}{p}\right) \cdot \left(\frac{\alpha}{m}\right) = \left(\frac{b}{p}\right) \cdot \left(\frac{1}{m}\right) = \left(\frac{b}{p}\right) \cdot 1 = -1$ και $\alpha^{\frac{n-1}{2}} \neq -1 \bmod n$, αφού αν $\alpha^{\frac{n-1}{2}} \neq -1 \bmod n \Rightarrow \alpha^{\frac{n-1}{2}} \neq -1 \bmod m$, άτοπο λόγω της σχέσης (2). Άρα $\alpha^{\frac{n-1}{2}} \neq \left(\frac{\alpha}{n}\right) \bmod n$. Άρα, για κάθε n ελεύθερο τετραγώνου έχουμε ότι υπάρχει $1 \leq \alpha < n$ και α Euler – μάρτυρας.

Β. Έστω τώρα ότι ο n δεν είναι ελεύθερος τετραγώνου και άρα υπάρχει $p \geq 3$ πρώτος με $p^2 \mid n$. Γράφουμε $n = p^k \cdot m$ με $k \geq 2$ ακέραιο και $p \nmid m$. Θα βρούμε έναν α, ο οποίος είναι Euler – μάρτυρας.

Αν $m=1$ τότε $\alpha = 1 + p$, καθώς: $\left(\frac{\alpha}{n}\right) = \left(\frac{\alpha}{p^k}\right) = \left(\frac{\alpha}{p}\right) \cdot \left(\frac{\alpha}{p}\right) \cdot \ldots \cdot \left(\frac{\alpha}{p}\right) = 1^k = 1$
και από το διωνυμικό θεώρημα:

$\alpha^{\frac{n-1}{2}} = (1+p)^{\frac{n-1}{2}} = 1 + \binom{\frac{n-1}{2}}{1} p + \cdots . + \binom{\frac{n-1}{2}}{\frac{n-1}{2}} p^{\frac{n-1}{2}} \equiv 1 + \frac{(n-1)}{2} p \bmod p^2 \Rightarrow$
$\alpha^{\frac{n-1}{2}} \neq 1 \bmod n$, δηλαδή $\alpha^{\frac{n-1}{2}} \neq \left(\frac{\alpha}{n}\right) \bmod n$.

Αν $m \geq 3$, τότε από το Κινέζικο θεώρημα υπολοίπων επιλέγω το α:
$1 \leq \alpha < p^2 \cdot m \leq n$ με $\alpha = 1 + p \bmod p^2$ (3) και $\alpha = 1 \bmod m$ (4).

θα δείξουμε ότι ο α είναι Euler – μάρτυρας για το n.

Από την (4) έχουμε ότι $(\alpha,m)=1$ και από την (1) ότι $\alpha - (1 + p) = \text{πολ } p^2 \Rightarrow \alpha \neq \text{πολ } p$. Όμως, $n = p^k m$, άρα $(\alpha, n) = 1$. Άρα, $\alpha \in G_n$.

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

$$\alpha^{\frac{n-1}{2}} = (1+p)^{\frac{n-1}{2}} = 1 + \binom{\frac{n-1}{2}}{1} p + \cdots + \binom{\frac{n-1}{2}}{\frac{n-1}{2}} p^{\frac{n-1}{2}} \equiv 1 + \frac{(n-1)}{2} p \bmod p^2,$$

Δηλαδή

$$\alpha^{\frac{n-1}{2}} \neq 1 \bmod n, \text{και } \left(\frac{\alpha}{n}\right) = \left(\frac{\alpha}{p^k m}\right) = \left(\frac{\alpha}{p}\right) \cdot \left(\frac{\alpha}{p}\right) \cdot \ldots \cdot \left(\frac{\alpha}{p}\right) \cdot \left(\frac{\alpha}{m}\right) = 1^k \cdot 1 = 1,$$

άρα το α είναι Euler – μάρτυρας.

Άρα, το G_n περιέχει ένα α, το οποίο είναι Euler – μάρτυρας και δεν ανήκει στο Β. Άρα, το Β είναι γνήσια υποομάδα του G_n.

Παρατηρήσεις:

1. Από το θεώρημα του Lagrange η τάξη του Β θα διαιρεί 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 $(\alpha,n) \neq 1$).

2.3. Το τεστ Miller Rabin

Πρόταση:

Έστω n πρώτος, α 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 $\alpha^r = 1 \bmod n$, είτε ότι υπάρχει $u \in \{0, 1, 2, 3, \dots \dots, s-1\}$με $\alpha^{2^u r} \equiv -1 \bmod n$.

Απόδειξη:

Έστω $k = \mathrm{ord}_n(\alpha^r)$. Από το μικρό θεώρημα του Fermat έχουμε ότι $(\alpha^r)^{2^u} \equiv 1 \bmod n$, άρα, $k \mid 2^u$. Διακρίνουμε τις εξής περιπτώσεις:

A. Έστω k =1, τότε $\alpha^r \equiv 1 \bmod n$.

B. Έστω k >1, τότε $k= 2^l$ με $1 \le l \le s$ και συνεπώς $\mathrm{ord}_n\left(\alpha^{2^{l-1}r}\right) = 2$. Όμως, μόνο η κλάση -1 έχει τάξη ίση με 2 μέσα στο $\mathbb{Z}_n^*$ και άρα έχουμε ότι $\left(\alpha^{2^{l-1}r}\right) = -1 \bmod n$.

Παρατήρηση:

Το τεστ Miller Rabin στηρίζεται στο παραπάνω θεώρημα.

Ορισμοί:

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

A. Αν $\alpha^r \neq 1 \bmod n$ και αν $\alpha^{2^l r} \neq -1 \bmod n$ για κάθε l, $0 \le l \le s-1$, τότε ο α καλείται ισχυρός μάρτυρας για το n.

B. Αν $\alpha^r \equiv 1 \bmod n$ ή $\alpha^{2^l r} \equiv -1 \bmod n$ για κάποιο l, $0 \le l \le s-1$, τότε ο α καλείται ισχυρός ψεύτης για το n και ο n καλείται ισχυρός ψευδοπρώτος με βάση το α.

Παράδειγμα:

Έστω $n = 561 = 3 \cdot 11 \cdot 17$, άρα $n-1= 560 = 2^4 \cdot 35$, άρα σύμφωνα με τον παραπάνω ορισμό $s = 4$ και $r = 35$. Για $\alpha = 2$ έχουμε $2^{35} \equiv 263 \bmod 561 \rightarrow 263^2 \equiv 166 \bmod 561 \rightarrow 166^2 \equiv 67 \bmod 561 \rightarrow 67^2 = 1 \bmod 561$. Βλέπουμε,

λοιπόν, ότι $\alpha^r \neq 1 \bmod n$ και $\alpha^{2^j r} \neq -1 \bmod n$ για κάθε $j, 0 \leq j \leq s-1$, άρα, ο $\alpha = 2$ 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 α=9 έχουμε $9^{45} \equiv 1 \bmod 91$, $\alpha^r \equiv 1 \bmod n$. Άρα, ο $\alpha = 9$ είναι ισχυρός ψεύτης για 91 και ο n ισχυρός ψευδοπρώτος.

Αλγόριθμος (Τεστ Miller – Rabin):

INPUT: έναν περιττό ακέραιο $n \geq 3$ και συντελεστή ασφαλείας $t \geq 1$.

OUTPUT: θα απαντάει στην ερώτηση «είναι ο n ο 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 α, $2 \leq \alpha \leq n - 2$.
   b. Υπολόγισε το $y = \alpha^r \bmod n$.
   c. If $y \neq 1$ και $y \neq n - \alpha$ then
      1) $j \leftarrow 1$.
      2) While $j \leq s - 1$ και $y \neq n - 1$
         a) $y \leftarrow y^2 \bmod n$.
         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 ασφαλείας t»).■

Παρατηρήσεις:

1. Ο παραπάνω αλγόριθμος είναι πιθανοτικός. Αυτό σημαίνει ότι δεν μπορούμε να είμαστε σίγουροι για όλα τα αποτελέσματα που επιστρέφει. 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 ασφαλείας 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 μην δημιουργούν πλέον πρόβλημα και ακόμη ότι το 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 $\{1, \ldots, n-1\}$ περιέχει το πολύ $\frac{n-1}{1}$ ακέραιους που είναι πρώτοι προς το n και δεν είναι ισχυροί μάρτυρες της συνθετότητας του.

Απόδειξη:

Θα προσδιορίσουμε το πλήθος των ακέραιων α με $(\alpha,n)= 1$, $2 \leq \alpha \leq n-1$ και $\alpha^r \equiv 1 \bmod n$ ή $\alpha^{2^s r} \equiv -1 \bmod n$ για $s \epsilon \{0, 1, \ldots, l-1\}$ με την προϋπόθεση ότι υπάρχει ένα τέτοιο α. Με αυτό ως δεδομένο παρατηρούμε ότι πάντα θα υπάρχει ακέραιος, ο οποίος ικανοποιεί τη δεύτερη εξίσωση, αφού αν $\alpha^r \equiv 1 \bmod n \Rightarrow (-\alpha)^r \equiv -1 \bmod n$ ή $(-\alpha)^{2^0 r} \equiv -1 \bmod n$.

Έστω k ο μεγαλύτερος ακέραιος του συνόλου {0, 1,….., l-1} για το οποίο υπάρχει ακέραιος A με $(A,n)=1$ και $A^{2^k r} \equiv -1 \bmod n$. Θέτουμε $m=2^k \cdot r$ και έστω $n = p_1^{e_1} \ldots . p_v^{e_v}$ η πρωτογενής ανάλυση του n. Έστω η ομάδα $G_n = \{x: x \in \mathbb{Z}_n^* \text{ και } (x, n) = 1\}$. Μπορεί να διαπιστωθεί ότι τα σύνολα $J = \{x \in G_n: x^{n-1} \equiv 1 \bmod n\}$, $K = \left\{x \in G_n: x^m \equiv \pm 1 \bmod p_i^{e_i}, i = 1, \ldots, v\right\}$, $L = \{x \in G_n: x^m \equiv \pm 1 \bmod n\}$ και $M = \{x \in G_n: x^m \equiv 1 \bmod n\}$ είναι υποσύνολα του G_n και μάλιστα ισχύει $M \subseteq L \subseteq K \subseteq J$.

Βλέπουμε ότι για κάθε $\alpha \in G_n$, το οποίο όμως δεν είναι ισχυρός μάρτυρας για τη συνθετότητα του n, έχουμε ότι $\alpha \in L$. Θα δείξουμε ότι $[G_n: L] \geq 4$. Έστω $\alpha \in K$, τότε $\alpha^2 \in M$ και επομένως $[K:M]=2^i$, για κάποιο ακέραιο $i \geq 0$. Συνεπώς, $[K:M]=2^i, j \leq i$. Στην περίπτωση όπου $j \geq 2$, τότε η προς απόδειξη ανισότητα ισχύει.

Έστω $j = 0$, τότε $K = L$.

Για $v \geq 2$ υπάρχει δ τέτοιο ώστε $\delta \equiv A \bmod p_1^{e_1}$ και $\delta \equiv 1 \bmod p_1^{e_1}$, για για $i = 2, \ldots, v$. Άρα $\delta^m \equiv -1 \bmod p_1^{e_1}$ και $\delta^m \equiv 1 \bmod p_1^{e_1}$, δηλαδή $\delta \in K$ και $\delta \notin L$, άτοπο.

Για ν=1 έχουμε ότι αν $\alpha \in J$, τότε $ord_{p_1^{e_1}}(\alpha) \mid p-1$.

Αντίστροφα, αν $ord_{p_1^{e_1}}(\alpha) \mid p-1$ τότε $\alpha \in J$. Άρα, το j είναι η υποομάδα τάξης $p-1$ της ομάδας $G_{p_1^{e_1}}$ και επομένως $[G_{p_1^{e_1}}: J] = p_1^{e_1-1}$. Για $p_1^{e_1} > 9$ έχουμε ότι $[G_{p_1^{e_1}}: J] \geq 4$. Αν $p_1^{e_1} > 9$, τότε r=1 και l=3.

Από τις ισοτιμίες $x \equiv 1 \bmod 9$, $x \equiv -1 \bmod 9$, $x^2 \equiv -1 \bmod 9$, $x^4 \equiv -1 \bmod 9$ προκύπτει ότι οι μόνοι ακέραιοι του συνόλου {1 ,….., 8} που δεν είναι ισχυροί μάρτυρες της συνθετότητας του 9 είναι οι 1 και 8.

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

Θεωρούμε έναν ακέραιο c με $c \equiv A\alpha \bmod p_1^{e_1}$,
$c \equiv 1 \bmod p_2^{e_2}, \dots, c \equiv 1 \bmod p_v^{e_v}$.

Έχουμε $c \notin LU\alpha L$ και συνεπώς $c \notin K$ που είναι άτοπο. Άρα, ο n έχει δύο μόνο πρώτους παράγοντες και επομένως δεν είναι αριθμός Carmichael.

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

Παρατήρηση:

Βλέπουμε λοιπόν ότι αν το n είναι περιττός σύνθετος ακέραιος, τότε το πολύ το $\frac{1}{4}$ όλων των αριθμών α, $1 \leq \alpha \leq n-1$, είναι ισχυροί ψεύτες για το n. συγκεκριμένα, αν n≠ 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 $1 - \frac{1}{4^t}$.

3. ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΑΚΕΡΑΙΩΝ

Η εύρεση των πρώτων παραγόντων ενός ακέραιου υπολογιστικά αποτελεί ένα πάρα πολύ δύσκολο πρόβλημα. Συνεχώς ανακαλύπτονται πιο γρήγοροι και πιο αποδοτικοί αλγόριθμοι για αυτό το πρόβλημα. Ο πιο γρήγορος αλγόριθμος για τα σημερινά δεδομένα είναι ο 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.

Οι πιο δύσκολο ως προς την παραγοντοποίηση αριθμοί είναι αυτοί που αποτελούνται από το γινόμενο δύο μεγάλων πρώτων. Το ρεκόρ παραγοντοποίησης τέτοιου είδους αριθμών είναι η παραγοντοποίηση του RSA – 768 με 232 δεκαδικά ψηφία. Η προσέγγιση έγινε με το GNFS.

Στη συνέχεια, θα εξετάσουμε τους αλγόριθμους Fermat, Pollard Rho, Dixon και Quadratic Sieve και Pollard Rho.

3.1. Η μέθοδος παραγοντοποίησης του Fermat

Στόχος της μεθόδου αυτής είναι να εκφραστεί ο αριθμός n που θέλουμε να παραγοντοποιήσουμε ως διαφορά δύο τέλειων τετραγώνων. Άρα, αν το πετύχουμε αυτό, θα έχουμε ότι $n=\alpha^2-b^2 \Rightarrow n=(\alpha-b)\cdot(\alpha+b)$. Αν $(\alpha-b)>1$, 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 $\alpha=\frac{1}{2}(u+v)$ και $b=\frac{1}{2}|u-v|$, έχουμε το ζητούμενο.

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

Αλγόριθμος (Μέθοδος παραγοντοποίησης του Fermat):

INPUT: ένα περιττό ακέραιο>1.

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

1) $\alpha=|\sqrt{n}|$
2) While $\alpha\leq\frac{(n+9)}{6}$ do
   A. $b=\sqrt{\alpha^2-n}$
   B. if b ακέραιος και $\alpha-b\neq 1$ return " $\alpha-b$"
   C. $\alpha\leftarrow\alpha+1$
3) return "o n είναι πρώτος ".■

Η παραπάνω μέθοδος είναι πολύ πιο αργή ακόμη και από το κόσκινο του Ερατοσθένη. Όμως, 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 έναν 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 $\sqrt{\text{in}}$. Στη συνέχεια παίρνουμε το μέγιστο κοινό διαιρέτη του παράγοντα που βρήκαμε με το n.

Παραδείγματα:

- <u>Χωρίς χρήση πολλαπλασιαστή:</u>

  Έστω n= 26563 (=$101 \cdot 263$). Σύμφωνα με τη μέθοδο του Fermat έχουμε $|\sqrt{265663}\,| = 163$

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

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

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

  Συνεπώς,

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

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

- <u>Με χρήση πολλαπλασιαστή:</u>

  Έστω n=3811(=$103 \cdot 37$).

  3n=11433

  $|\sqrt{11433}| = 107$

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

  Συνεπώς,

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

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

  Σε αυτό το παράδειγμα η απλή μέθοδος του Fermat θα μας επέστρεφε αποτέλεσμα μετά από 9 επαναλήψεις.

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

3.2. Η μέθοδος παραγοντοποίησης του Dixon

Η μέθοδος του Dixon για την παραγοντοποίηση ενός αριθμού n βασίζεται στην εύρεση ακεραίων α, b με $\alpha^2 \equiv b^2 \bmod n$ και $\alpha \neq \pm b \bmod n$. Έχουμε ότι $\alpha^2 - b^2 \equiv 0 \bmod n \Rightarrow (\alpha - b)(\alpha + b) = k \cdot n \Rightarrow n \mid |(\alpha - b)(\alpha + b)$, χωρίς το $(\alpha - b)$ ή το $(\alpha + b)$ να διαιρείται από το n, εφόσον $\alpha \neq \pm b \bmod n$. Άρα, έχουμε ότι ο αριθμός $(\alpha - b, n)$ είναι ένας μη τετριμμένος παράγοντας για το n. Η μέθοδος Dixon χρησιμοποιεί μια βάση παραγοντοποίησης.

Ορισμοί:

- Ορίζουμε βάση παραγοντοποίησης για τη μέθοδο Dixon ένα σύνολο $B=\{-1, p_1, p_2, \ldots, p_h\}$ με p_i διακεκριμένοι πρώτοι modulo n και $-1 \equiv n-1 \bmod n$.
- Ο ακέραιος n καλείται B-λείος αν δεν έχει πρώτους παράγοντες μεγαλύτερους του B. (Ακόμα, 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 $x^2 \equiv c \bmod n$, 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-λείοι.

Ακόμα ο $71 \rightarrow 71^2 = 63 \bmod 2849$, $-\frac{2849}{2} \leq 63 \leq \frac{2849}{2}$ είναι 7 − προσαρμοσμένος ως προς τον 2849.

Περιγραφή αλγορίθμου του Dixon:

Για δοθέν n και για δοθείσα βάση παραγοντοποίησης B, όπως ορίστηκε παραπάνω, ο αλγόριθμος του Dixon ψάχνει αριθμούς, έστω x, κοντά στο $\lceil\sqrt{n}\rceil$, για τους οποίους ισχύει, ότι όλοι οι πρώτοι παράγοντες του $x^2 \bmod n$ υπάρχουν μέσα στο σύνολο B.

Ακολούθως, 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 $x^2 \equiv y^2 \bmod n$, 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 $|\sqrt{n}|=921$.

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

$922^2 \equiv 845 = 5 \cdot 13^2 \bmod 849239$ $\surd$

……..

$933^2 \equiv 21250 = 2 \cdot 5^4 \cdot 17 \bmod 849239$ $\surd$

$934^2 \equiv 23117 \bmod 849239$

……..

$937^2 \equiv 28730 = 2 \cdot 5 \cdot 13^2 \cdot 17 \bmod 849239.$ $\surd$

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

Παρατηρούμε ότι $(922 \cdot 933 \cdot 937)^2 = 2^2 \cdot 5^6 \cdot 13^4 \cdot 17^2 = (2 \cdot 5^3 \cdot 13^2 \cdot 17)^2$ και αφού $922 \cdot 933 \cdot 937 \equiv 103951 \bmod 849239$ και $2 \cdot 5^3 \cdot 13^2 \cdot 17 = 718250$, έχουμε ότι $103951^2 \equiv 718250^2 \bmod 849239$. Άρα, από το μέγιστο κοινό διαιρέτη έχουμε:

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

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

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

Αλγόριθμος (Μέθοδος παραγοντοποίησης Dixon):

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

OUTPUT: έναν μη τετριμμένο παράγοντα του n.

1. Υπολόγισε το $m = [\sqrt{n}]$
2. (Βρες $k+1$ ζευγάρια $(\alpha_i, \alpha 2_i)$. Οι τιμές επιλέγονται με τη σειρά $0, \pm 1, \pm 2, \ldots.$)
   $i \leftarrow 1$
   While $i \leq k + 1$
   a. Υπολόγισε το $\alpha 2 = (m + w)^2 \bmod n$ και έλεγξε με διαδοχικές διαιρέσεις αν είναι B-λείος. Αν όχι επέλεξε το επόμενο w και επανέλαβε το $\alpha 2$.
   b. If $\alpha 2$ είναι B-λείος με $\alpha 2 = \prod_{j=1}^{k} p_j^{e_{ij}}$ then
      I. $\alpha_i \leftarrow m + w$, $\alpha 2_i \leftarrow \alpha 2$ και $v_i = (v_{i1}, v_{i2}, \ldots\ldots, v_{ik})$, όπου $v_{ij} = e_{ij} \bmod 2$ για $1 \leq j \leq k$.
   c. $i \leftarrow i + 1$.
3. Χρησιμοποιώντας μεθόδους γραμμικής άλγεβρας βρες ένα μη κενό υποσύνολο $T \subseteq \{1, 2, \ldots., k+1\}$ τέτοιο ώστε $\Sigma_{i \in T} v_i = 0$ στο $\mathbb{Z}_2$.
4. Υπολόγισε το $x = \Pi_{i \in T} \alpha_i \bmod n$.
5. Για κάθε $j, 1 \leq j \leq k$, υπολόγισε το $l_j = \frac{\Sigma_{i \in T} e_{ij}}{2}$.
6. Υπολόγισε το $y = \Pi_{j=1}^{k} p_j^{lj} \bmod n$.
7. If $x \equiv \pm y \bmod n$ then βρες ένα άλλο μη κενό υποσύνολο $T \subseteq \{1, 2, \ldots.., k+1\}$ τέτοιο ώστε $\Sigma_{i \in T} v_i = 0$ και πήγαινε στο βήμα 4. (Στην περίπτωση που δεν υπάρχει τέτοιο υποσύνολο T, πήγαινε στο βήμα 2, βρες μερικά ακόμη $(\alpha_i, \alpha 2_i)$ 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 $T \subseteq \{1, 2, \ldots.., k+1\}$ τέτοιο ώστε $\Sigma_{i \in T} v_i = 0$ στο $\mathbb{Z}_2$. Άρα, 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 α_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 μέθοδος Quadratic Sieve (Τετραγωνικό Κόσκινο)

Η μέθοδος Quadratic Sieve είναι μέχρι σήμερα η πιο γρήγορη μέθοδος παραγοντοποίησης για αριθμούς που έχουν μέχρι 110 ψηφία και η δεύτερη γενικά πιο γρήγορη μέθοδος παραγοντοποίησης μετά το Number Field Sieve. 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 του QS:

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 α, b, έτσι ώστε $\alpha^2 \equiv b^2 \bmod n$. Με αυτόν τον τρόπο θα έχουμε ότι $(\alpha-b)(\alpha+b)=$πολ n και έτσι είναι πολύ πιθανό ο μέγιστος κοινός διαιρέτης του $(\alpha-b)$ ή του $(\alpha+b)$ με το n δώσει ένα μη τετριμμένο παράγοντα του n. Για να καταφέρουμε αυτό, ψάχνουμε τετράγωνα αριθμούς mod n, τα οποία αναλύονται σε μικρούς πρώτους παράγοντες, με πρώτους που βρίσκονται μέσα στη βάση παραγοντοποίησης 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 $(x+|\sqrt{n}|)^2 - n$, με το x να είναι ένας μικρός ακέραιος. Ο αριθμός αυτός είναι αρκετά μικρός mod n, αφού $(x+|\sqrt{n}|)^2 - n \approx x^2 + 2x\sqrt{n}$. Με αυτόν τον τρόπο, έχοντας βρει αρκετά τέτοια τετράγωνα βρίσκουμε έναν συνδυασμό τους, έτσι ώστε να προκύψει μια παρόμοια σχέση όπως αυτή παραπάνω με τα α, b.

Για παράδειγμα έστω ότι θέλουμε να βρούμε έναν παράγοντα του αριθμού 583.

Παρατηρούμε ότι:

$$25^2 \equiv 42 = 2 \cdot 3 \cdot 7 \bmod 583 \quad \text{και} \quad 31^2 \equiv 378 = 2 \cdot 3^3 \cdot 7 \bmod 583,$$

$$\text{άρα, } (31 \cdot 25)^2 = 775^2 \equiv 192^2 \equiv 2^2 \cdot 3^4 \cdot 7^2 = (2 \cdot 3^2 \cdot 7)^2 = 126^2 \bmod 583,$$

δηλαδή $192^2 \equiv 126^2 \bmod 583$ που είναι η σχέση που ψάχναμε.

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 $[\sqrt{583}] = 24$ 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.

Ορισμός (Βάση Παραγοντοποίησης QS):

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

Κοσκίνισμα (Sieving):

Οι αριθμοί όπως είπαμε που εξετάζει το QS είναι της μορφής $(x+|\sqrt{n}|)^2 - n$. Ψάχνουμε ποιοι από τους αριθμούς διαιρούνται αποκλειστικά με πρώτους της βάσης παραγοντοποίησης. Το κοσκίνισμα έγκειται στο να βρούμε όλους τους αριθμούς της μορφής $(x+|\sqrt{n}|)^2 - n$ που διαιρούνται με τον p_1, πρώτο της βάσης, δηλαδή $(x+|\sqrt{n}|)^2 - n \equiv 0 \bmod p_1$, 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. 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 μπορούν να προσθέσουμε και κάποιες δυνάμεις τους, έτσι ώστε να βελτιώσουμε την ακρίβεια.

Σχόλια και παρατηρήσεις για το Κοσκίνισμα:

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

Παράδειγμα:

Έστω ότι θέλουμε να βρούμε έναν 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.

$|\sqrt{583}\,| = 24$

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

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

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

Έχουμε 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
Διαίρ. με 2	21	93	73	201	129	317	189	441	253	573
Διαίρ . με 3	7	31	73	67	43	317	63	147	253	191
Διαίρ . 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. Άρα, για x=1 και x=7 έχουμε τις περισσότερες πιθανότητες να πετύχουμε λείους αριθμούς. (Για x=1 σίγουρα έχουμε πετύχει έναν λείο αριθμό).

Άρα 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 μικρούς αριθμούς, όπως το 583, είναι όμως αποδοτική για μεγάλους ακεραίους, για παράδειγμα 100 ψηφίων.

Αλγόριθμος (Quadratic Sieve):

INPUT: ένα περιττό ακέραιο n≥ 3, ο οποίος δεν είναι πρώτος.

OUTPUT: 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. $\alpha_1 \leftarrow 1$.
3. For $(2 \leq i \leq t)$ βρες ρίζες $\pm\ \alpha_i$ της ισοτιμίας $\alpha_i^2 \equiv n \bmod p_i$.
4. Εφάρμοσε το κοσκίνισμα στην ακολουθία $x^2 - n$, με $x = |\sqrt{n}|$, $|\sqrt{n}| + 1$, … για να βρεις t=1 διαφορετικά ζευγάρια $(x, x^2 - n)$, με $x^2 - n$ B-λείο και ενσωμάτωσέ τα 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. $\vec{v}(x^2 - n) \leftarrow (e_1, e_2, \dots \dots, e_t)$.
6. Δημιούργησε έναν πίνακα (t+1) x t, με γραμμές τα στοιχεία του v για τα διάφορα $x^2 - n$, υπολογισμένα όμως modulo 2.
7. Χρησιμοποίησε αλγόριθμους γραμμικής άλγεβρας, για παράδειγμα τη μέθοδο απαλοιφής Gauss, για να βρεις ένα μη τετριμμένο σύνολο των γραμμών του πίνακα, του οποίου το άθροισμα των στοιχείων να είναι ίσο με μηδέν, έστω $\vec{v}(x_1) + \vec{v}(x_2) + \cdots + \vec{v}(x_t) = \vec{0}$.
8. Θέσε $x \leftarrow x_1 x_2 \cdot \dots \dots \cdot x_t \bmod n$.
9. $y \leftarrow \sqrt{(x_1^2 - n)(x_2^2 - n) \cdot \dots \cdot (x_t^2 - n)}$, η ρίζα θα προκύψει άμεσα από το ότι γνωρίζουμε την παραγοντοποίηση του τέλειου τετραγώνου $(x_1^2 - n)(x_2^2 - n) \cdot \dots \cdot (x_t^2 - n)$.
10. Υπολόγισε το $d = (x - y, n)$.
11. Return d.■

Παρατηρήσεις:

1. Βλέπουμε ότι ο αλγόριθμος έχει ως είσοδο έναν περιττό, ο 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 στη διαδικασία του κοσκινίσματος και στην εύρεση των λείων αριθμών.
3. Μπορούμε να βελτιώσουμε την υπολογιστική πολυπλοκότητα του παραπάνω αλγορίθμου, αν επιλέξουμε t≈ $L_n\left[\frac{1}{2},\frac{1}{2}\right]$, 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 $L_q[\alpha, c] = 0\left(\exp\left((c + 0(1))\right)(\ln q)^{\alpha}(\ln \ln q)^{1-\alpha}\right)$.

3.4. Ο αλγόριθμος Pollard Rho

Η βασική ιδέα του αλγορίθμου:

Έστω p ο μικρότερος πρώτος διαιρέτης του n και x, x' ακέραιοι στο $\mathbb{Z}_n$, τέτοιοι ώστε $x \neq x'$ και $x = x' \bmod p$. Τότε $p \leq$ ΜΚΔ $(x-x', n) < n$ και υπολογίζοντας τον ΜΚΔ θα βρούμε έναν μη τετριμμένο παράγοντα του n. Έστω ότι θέλουμε να παραγοντοποιήσουμε τον n επιλέγοντας πρώτα ένα τυχαίο υποσύνολο X του $\mathbb{Z}_n$ και στη συνέχεια υπολογίζοντας τους ΜΚΔ $(x-x', n)$ για όλα τα x, x' στο X με $x \neq x'$.

Η μέθοδος αυτή θα είναι επιτυχής μόνο στην περίπτωση που η απεικόνιση $x \rightarrow x \bmod p$ οδηγεί σε τουλάχιστον μία σύγκρουση για το $x \in X$. Η περίπτωση αυτή στηρίζεται το παράδοξο των γενεθλίων το οποίο θα δούμε παρακάτω.

Ορισμός:

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

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:

Θεωρούμε την ομάδα των ακεραίων modulo n, δηλαδή το σύνολο $\mathbb{Z}_n = \{0,1,2, \ldots, n-1\}$, με $|\mathbb{Z}_n| = n$. Θα υπολογίσουμε την πιθανότητα να μην επιλεχθούν ίσα στοιχεία μετά από k διαδοχικές τυχαίες επιλογές αριθμών από το $\mathbb{Z}_n$.Η πιθανότητα επιλογής ενός συγκεκριμένου στοιχείου είναι $\frac{1}{n}$. Η πρώτη μας επιλογή είναι αυθαίρετη. Η πιθανότητα η δεύτερη επιλογή να είναι διαφορετική από την πρώτη είναι $\frac{n-1}{n} = 1 - \frac{1}{n}$. Η πιθανότητα η τρίτη επιλογή να είναι διαφορετική από τις προηγούμενες δύο είναι $\frac{n-1}{n} = 1 - \frac{1}{n}$ κ.ο.κ.
Έτσι, η πιθανότητα επιλογής k στοιχείων χωρίς συγκρούσεις είναι

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

Αν ο x είναι μικρός πραγματικός, τότε $1-x\approx e^{-x}$, όπως προκύπτει από την ανάπτυξη σε δυναμοσειρά του e^{-x}: $e^{-x}=1-\frac{x}{1!}+\frac{x^2}{2!}-\frac{x^3}{3!}+\cdots,-\infty<x<\infty$. Συνεπώς, αφού n πολύ μεγάλο έπεται ότι $1-\frac{1}{n}\sim e^{\frac{1}{n}}$. Άρα, η ζητούμενη πιθανότητα είναι η :

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

Η πιθανότητα εύρεσης μιας σύγκρουσης είναι $p\approx 1-e^{-\frac{k(k-1)}{2n}}$ και με συνεπαγωγές καταλήγουμε $k^2-k\approx 2n\,in\,\frac{1}{1-p}$ και αγνοώντας τον όρο $-k$ καταλήγουμε $k\approx\sqrt{2n\ln\frac{1}{1-p}}$. Άρα, για πιθανότητα σύγκρουσης $P=\frac{1}{2}$, έχουμε $k\approx 1.17\sqrt{n}$.

Αλγόριθμος (Μέθοδος παραγοντοποίησης Pollard Rho):

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

1. Θέσε $\alpha\leftarrow 2, b\leftarrow 2$.
2. For i=1,2,……
   a. Υπολόγισε $\alpha\leftarrow\ \alpha^2+1 \bmod n, b\leftarrow b^2+1 \bmod n, b\leftarrow b^2+1 \bmod n$.
   b. Υπολόγισε το d=(α-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 · 97). Θα εφαρμόσουμε τον αλγόριθμο Pollard Rho.

$A\leftarrow 2,\alpha\leftarrow 2^2+1 \bmod 1261=5, b\leftarrow 2, b\leftarrow 5, b\leftarrow 5^2+1 \bmod 1261=26.$

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

$A\leftarrow 26, b\leftarrow 26^2+1 \bmod 1261=677, b\leftarrow 677^2+1 \bmod 1261=587.$

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

$A \leftarrow 677, b \leftarrow 587^2 + 1 \bmod 1261 = 317, b \leftarrow 317^2 + 1 \bmod 1261 = 871.$

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

Άρα, ο αλγόριθμος βρήκε έναν μη τετριμμένο παράγοντα του 1261, το 97 σε 3 βήματα.

4. Βιβλιογραφία και πηγές

- Κουκουβίνος Χ.-Παπαϊωάννου Α., «Κρυπτογραφία», Ε.Μ.Π., 2007
- Ρασσιάς Μ.Θ.- Παπαϊωάννου Α., «Εισαγωγή στη θεωρία αριθμών», Εκδόσεις Συμεών, 2010
- Πουλάκης Δ., «Κρυπτογραφία: Η επιστήμη της ασφαλούς επικοινωνίας», Εκδόσεις Ζήτη, 2006
- Πουλάκης Δ., «Θεωρία Αριθμών», Εκδόσεις Ζήτη, 2001
- Douglas R. Stinson, «Cryptography: Theory and Practice», Chapman&Hall/CRC, 2002
- Trappe W.-Washington L., «Introduction to Cryptography with coding theory», Pearson Education
- Τζανάκης Γ. Ν., «Θεμελιώδης Θεωρία Αριθμών», Τμήμα Μαθηματικών, Πανεπιστήμιο Κρήτης, 2008
- Buhler J.-Wagon S., «Basic Algorithms in number theory», MSRI publications, Vol. 44, 2008
- Stevenhagen P., «The number field sieve», MSRI publications, Vol. 44, 2008
- Scoof R., «Four primality testing algorithms», MSRI publications, Vol. 44, 2008
- Granville A., «It is easy to determine whether a given integer is prime», Bulletin of the American Mathematical Society, Vol 42, No. 1, 2004