ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ **Ε**ΦΑΡΜΟΣΜΕΝΩΝ **Μ**ΑΘΗΜΑΤΙΚΩΝ

ΚΑΙ **Φ**ΥΣΙΚΩΝ **Ε**ΠΙΣΤΗΜΩΝ

ΤΕΣΤ ΠΙΣΤΟΠΟΙΗΣΗΣ ΠΡΩΤΩΝ ΚΑΙ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΑΚΕΡΑΙΩΝ

Διπλωματική εργασία

Λύκουρα Άννα

Τριμελής Επιτροπή :

Κουκουβίνος Χρήστος, Καθηγητής ΣΕΜΦΕ, ΕΜΠ

Παπαϊωάννου Αλέξανδρος, Αν. Καθηγητής ΣΕΜΦΕ, ΕΜΠ (Επιβλέπων)

Στεφανέας Πέτρος, Λέκτορας ΣΕΜΦΕ, ΕΜΠ

Αθήνα, Ιούλιος 2011

Πρόλογος

"… ο 317 είναι πρώτος όχι επειδή το πιστεύουμε ή επειδή τα μυαλά μας είναι διαμορφωμένα με τον ένα ή τον άλλο τρόπο, αλλά γιατί έτσι είναι, γιατί η μαθηματική πραγματικότητα είναι δομημένη με αυτό τον τρόπο. "

G.H.Hardy
"Απολογία ενός μαθηματικού"

Οι μαθηματικοί αγαπούν τους πρώτους αριθμούς, όπως οι χημικοί αγαπούν τα άτομα και οι βιολόγοι τα γονίδια. Με τον ίδιο τρόπο που τα άτομα είναι το βασικό συστατικό της ύλης και τα γονίδια το βασικό συστατικό της ζωής έτσι και οι πρώτοι αριθμοί είναι το κύριο "συστατικό" των μαθηματικών. Κατά συνέπεια, η μελέτη τους έχει πολύ σημαντική απήχηση σε όλους τους τομείς των μαθηματικών και εμπνέει εφαρμοσμένες τεχνολογίες, όπως για παράδειγμα η κρυπτογραφία.

Οι πρώτοι αριθμοί είναι εκείνοι που δε διαιρούνται με κανέναν αριθμό εκτός από το 1 και τον εαυτό τους. Για παράδειγμα, το 5 είναι πρώτος αριθμός, όχι όμως και το 6, αφού διαιρείται με το 2 και το 3. Όλοι οι αριθμοί μπορούν να γραφούν ως γινόμενο 2 ή περισσοτέρων πρώτων αριθμών (6=2x3, 90=2x3x3x5). Γι αυτόν ακριβώς το λόγο, οι μαθηματικοί πιστεύουν, ότι η μελέτη των πρώτων μπορεί να οδηγήσει στην κατανόηση όλων των αριθμών.

Οι μαθηματικοί ασχολούνται με τους πρώτους αριθμούς επί χιλιάδες χρόνων. Το πρώτο σημαντικό επίτευγμα ήρθε από τον Ευκλείδη περίπου το 300 π.Χ. στην Αλεξάνδρεια. Ο Ευκλείδης, ρώτησε τον εαυτό του το παρακάτω: "Υπάρχει ένα συγκεκριμένο πλήθος πρώτων αριθμών ή είναι άπειροι? Υπάρχει ένας μέγιστος πρώτος αριθμός ή μπορώ πάντα να βρω ένα μεγαλύτερο?" Ο Ευκλείδης έδωσε απάντηση στα παραπάνω με έναν κομψό συλλογισμό και απέδειξε ότι οι πρώτοι αριθμοί είναι τελικά άπειροι.

Υπάρχουν γενικά πάρα πολλά ερωτήματα σχετικά με τους πρώτους αριθμούς, που εξακολουθούν να βασανίζουν τους μαθηματικούς μέχρι και σήμερα. Για παράδειγμα, κανείς δεν έχει καταφέρει να εξηγήσει τον περίεργο τρόπο με τον οποίο είναι

κατανεμμημένοι οι πρώτοι αριθμοί, στον σύνολο των φυσικών. Σε 100 αριθμούς πριν τα 10 εκατομμύρια, υπάρχουν 10 πρώτοι, ενώ σε 100 αριθμούς μετά τα 10 εκατομμύρια υπάρχουν μόνο 2. Η διασπορά των πρώτων αποτελεί μέχρι και σήμερα το « Έβερεστ» των μαθηματικών.

Τα παραπάνω αφορούν κυρίως την καρδιά των θεωρητικών μαθηματικών. Παρόλα αυτά, οι πρώτοι αριθμοί έχουν ιδιαίτερη σημασία και στα εφαρμοσμένα μαθηματικά. Σημαντικότερα παραδείγματα, είναι η χρήση και συνεισφορά των πρώτων στην προστασία δεδομένων και στην παγκόσμια οικονομία, αφου οι πρώτοι αποτελούν τη βάση πολλών σύγχρονων αλγόριθμων κρυπτογράφησης .

Στο πρώτο μέρος της εργασίας αυτής γίνεται μια ιστορική αναδρομή για τους πρώτους αριθμούς και την εξέλιξη της μελέτης τους ανά τους αιώνες. Δίνονται περιληπτικά τα στάδια της μακραίωνης έρευνάς τους ξεκινώντας από τη σύλληψη των πρώτων αριθμών σε προιστορικά χρόνια. Μεταφερόμαστε φυσικά στην Αρχαία Ελλάδα όπου μελετάμε πιο αναλυτικά τη συμβολή του Ευκλείδη και βλέπουμε τα θεωρήματά του με τις αποδείξεις τους και φτάνουμε μέχρι τα σπουδαία αποτελέσματα μαθηματικών όπως οι Pierre de Fermat, Leonhard Euler και Carl Friedrich Gauss. Επίσης, διατυπώνεται και αποδεικνύεται το σημαντικότατο Θεμελιώδες Θεώρημα της Αριθμητικής.

Στο δεύτερο μέρος παρουσιάζουμε κάποιους βασικούς ορισμούς καθώς και στοιχεία από τη θεωρία αριθμών απαραίτητα για την κατανόηση της θεωρίας των πρώτων αριθμών καθώς και για τη μετέπειτα μελέτη μας στα επόμενα μέρη αυτής της εργασίας. Διατυπώνονται και αποδεικνύονται βασικά θεωρήματα για τη θεωρία των γραμμικών ισοδυναμιών και των τετραγωνικών υπολοίπων και παρουσιάζονται τα σύμβολα των Legendre και Jacobi. Τέλος, βλέπουμε επίσης συνοπτικά ορισμούς και θεωρήματα για τις πρωταρχικές ρίζες.

Το τρίτο μέρος της εργασίας αποτελείται από τα τρία πιο γνωστά καθώς και σημαντικότερα τεστ για την πιστοποίηση πρώτων αριθμών. Αναλύουμε το θεωρητικό υπόβαθρο γύρω από αυτά και παραθέτουμε τους αντίστοιχους αλγόριθμους (σε ένα είδος ψευδογλώσσας προγραμματισμού). Τα τεστ που θα δούμε είναι το τεστ του Fermat, το τεστ των Solovay-Strassen και τέλος το τεστ των Miller-Rabin.

Στο τελευταίο μέρος βλέπουμε πως μπορεί να γίνει η παραγοντοποίηση ενός ακεραίου σε περίπτωση που αυτός δεν είναι πρώτος. Τα τεστ παραγοντοποίησης που θα μελετήσουμε είναι τα εξής : αλγόριθμος παραγοντοποίησης Fermat, Dixon, p-1 Pollard και Pollard Rho.

Περιεχόμενα

1. Ιστορική αναδρομή

1.1. Το οστό Ishango

Η έναρξη της μελέτης των πρώτων αριθμών δεν μπορεί να τοποθετηθεί σε συγκεκριμένη χρονολογική περίοδο. Εντούτοις, η ανακάλυψη του οστού Ishango (που χρονολογείται στα 6500 π.Χ.) το 1960 στο ομώνυμο χωριό στα σύνορα Ουγκάντας και Ζαϊρ, είναι ίσως το πρώτο τεκμήριο ότι ο άνθρωπος γνώριζε τους πρώτους αριθμούς χιλιάδες χρόνια πριν. Το οστό αυτό φέρει τρείς στήλες με χαρακιές. Η μια στήλη έχει χαραγμένους τους πρώτους αριθμούς απο το 10 έως το 20. Η χρησιμότητά του όμως εξακολουθεί να μένει άγνωστη μέχρι σήμερα.

1.2. Αρχαίοι Έλληνες

Η σημασία των πρώτων αριθμών έγινε αντιληπτή από τους Αρχαίους Έλληνες καθώς ήταν οι πρώτοι που ασχολήθηκαν πραγματικά με αυτούς και την έννοιά τους και κατέληξαν σε σημαντικά συμπεράσματα σχετικά με τη φύση τους.

1.2.1. Ευκλείδης

Το πιο σημαντικό έργο στην ιστορία των ελληνικών μαθηματικών είναι αναμφίβολα τα "Στοιχεία" του Ευκλείδη (περ. $325-265$ π.Χ.). Τα Στοιχεία δεν αποτελούν σύνοψη όλων των ελληνικών μαθηματικών, αλλά συλλογή του στοιχειώδους τμήματός τους. Γράφτηκαν περί το 300 π.Χ. και αποτελούν ένα απο τα γραπτά έργα που κυριάρχησαν στους αιώνες. Αποτελείται από 13 βιβλία, εκ των οποίων τα βιβλία VII, $VIII$, IX θεωρούνται από τα αρχαιότερα βιβλία Θεωρίας Αριθμών και σε αυτά βρίσκονται τρία από τα σημαντικότερα συμπεράσματα για τους πρώτους αριθμούς. Αυτά είναι : η απειρία των πρώτων αριθμών, οι τέλειοι αριθμοί και το Θεμελιώδες Θεώρημα της Αριθμητικής.

Για τον Ευκλείδη, οι «αριθμοί» ήταν οι ακέραιοι. Από τους ορισμούς του στο βιβλίο $VIII$ βλέπουμε ότι η αντιμετώπιση των αριθμών γίνεται ουσιαστικά γεωμετρικά. Ο Ευκλείδης λέει ότι «ο μεγαλύτερος αριθμός είναι πολλαπλάσιο του μικρότερου όταν μπορεί να μετρηθεί από αυτόν» και ότι «το γινόμενο δύο αριθμών είναι το εμβαδόν ενός ορθογωνίου». Υπάρχει επίσης ο περίφημος κανόνας, γνωστός με το όνομα ευκλείδειος αλγόριθμος, για την εύρεση του μέγιστου κοινού διαιρέτη δύο αριθμών ή, με τα λόγια του Ευκλείδη, «του μεγαλύτερου κοινού μέτρου μεταξύ δύο μεγεθών».

Ξεκινώντας με το συμπέρασμα για την απειρία των πρώτων αριθμών, στο βιβλίο IX βρίσκουμε την περίφημη απόδειξη, η οποία, με σύγχρονη ορολογία, δηλώνει απλά ότι υπάρχουν άπειροι πρώτοι αριθμοί. Στην πραγματικότητα, ο Ευκλείδης σκόπιμα αποφεύγει την αναφορά στο άπειρο. Δηλώνει ότι ***«οι πρώτοι αριθμοί είναι περισσότεροι από οποιοδήποτε δεδομένο πλήθος πρώτων αριθμών»*** και προχωρεί στην απόδειξη αυτού του θεωρήματος για μόνο τρεις δεδομένους πρώτους.

Θεώρημα:

Οι πρώτοι αριθμοί είναι περισσότεροι από οποιοδήποτε δεδομένο πλήθος πρώτων αριθμών.

Απόδειξη:

Έστω τρείς δοσμένοι πρώτοι αριθμοί α, β, γ. Θα δείξουμε ότι δεν είναι οι μοναδικοί πρώτοι αριθμοί και ότι υπάρχουν περισσότεροι από αυτούς. Έστω ότι ο ε διαιρείται με τους α, β, γ. Προσθέτουμε στον ε την μονάδα μ και προκύπτει ο αριθμός $\delta = \varepsilon + \mu$. Άν τώρα ο δ είναι πρώτος τότε η πρόταση αποδείχτηκε. Άν δεν είναι πρώτος τότε θα διαιρείται από κάποιον άλλον αριθμό, έστω τον ζ. Θα δείξουμε ότι ο ζ δεν είναι ένας από τους α, β, γ. Έστω ότι είναι ένας από αυτούς, τότε θα διαιρείται με τον δ και θα διαιρείται και με τον ε, άρα θα διαιρεί τη διαφορά τους, δηλαδή τη μονάδα. Αυτό είναι άτοπο αφού υποθέσαμε ότι ο ζ δεν είναι ένας από τους α, β, γ. ■

Ο συλλογισμός του Ευκλείδη ξεκίνησε υποθέτωντας ότι υπάρχει ένα συγκεκριμένο πλήθος πρώτων αριθμών. Ας υποθέσουμε ότι κάποιος υποστηρίζει πως το $2,3$ και 5 είναι οι μόνοι πρώτοι στον κόσμο. Αν πολλαπλασιάσουμε τους παραπάνω αριθμούς $(2\times3\times5)$ και προσθέσουμε 1, το αποτέλεσμα είναι 31, το οποίο είναι πρώτος αριθμός. Επομένως η

λίστα των πρώτων είναι τώρα μεγαλύτερη $(2,3,5$ και $31)$. Παρόλα αυτά, δεν γνωρίζουμε αν αυτή είναι η τελική, πλήρης λίστα. Αν πολλαπλασιάσουμε τα $2,3,5$ και 31 και προσθέσουμε 1, αποδεικνύουμε ξανά ότι το σύνολο των πρώτων δεν είναι πλήρες. Με λίγα λόγια, από οποιαδήποτε λίστα πρώτων αριθμών και να ξεκινήσουμε, είναι πάντα δυνατό να αποδείξουμε ότι υπάρχουν ακόμα περισσότεροι πρώτοι. Γι αυτό, η λίστα πρέπει να είναι απείρως μεγάλη. Η απαραίτητη επέκταση στους υπόλοιπους πρώτους αριθμούς θεωρείται αυτονόητη.

Σε μια πιό σύγχρονη μορφή η διατύπωση και απόδειξη για το παραπάνω θεώρημα είναι η εξής:

Θεώρημα:

Οι πρώτοι αριθμοί είναι άπειροι στο πλήθος.

Απόδειξη:

Ας υποθέσουμε πώς το πλήθος των πρώτων αριθμών είναι πεπερασμένο και ότι ο μεγαλύτερος από αυτούς είναι ο p. Θεωρούμε τον αριθμό $Q = p!+1$. Τότε, αν ο Q ήταν πρώτος αριθμός θα ήταν μεγαλύτερος του p. Αν ο Q δεν είναι πρώτος αριθμός τότε προφανώς θα έχει πρώτους διαιρέτες. Αλλά, κάθε πρώτος αριθμός μικρότερος του p δεν μπορεί να διαιρεί τον Q, διότι θα αφήνει πάντα υπόλοιπο 1. Επομένως οι πρώτοι διαιρέτες του Q είναι όλοι μεγαλύτεροι του p. Άτοπο. Συνεπώς, οι πρώτοι αριθμοί είναι άπειροι. ■

Ως δεύτερο συμπέρασμα, στο βιβλίο IX αναφέρεται και ένας κανόνας κατασκευής τέλειων αριθμών. Ένας θετικός ακέραιος αριθμός n ονομάζεται τέλειος (perfect number) όταν ισούται με το άθροισμα των διαιρετών του χωρίς φυσικά να συμπεριλάβουμε τον ίδιο τον αριθμό n στην άθροιση. Για παράδειγμα ο αριθμός 6 έχει διαιρέτες του τους $1,2,3$ και ισχύει ότι $1+2+3=6$. Όμοια το 28 έχει διαιρέτες $1,2,4,7,14$ και $1+2+4+7+14=28$.

Το τρίτο σπουδαίο συμπέρασμα για τη θεωρία αριθμών από τα Στοιχεία του Ευκλείδη έχει να κάνει με το ρόλο των πρώτων αριθμών στη δομή των φυσικών. Η μελέτη των Αρχαίων

Ελλήνων σε αυτό το τομέα τους οδήγησε σε αποτελέσματα με βάση τα οποία διατυπώθηκε το Θεμελιώδες Θεώρημα της Αριθμητικής.

Για την απόδειξή του θα αναφέρουμε αρχικά και ένα άλλο θεώρημα γνωστό ώς πρώτο θεώρημα του Ευκλείδη.

<u>Θεώρημα (Το πρώτο Θεώρημα του Ευκλείδη):</u>

Έστω p ένας πρώτος αριθμός και $a,b \in \mathbb{Z}$. Άν $p \mid ab$, τότε $p \mid a$ ή $p \mid b$.

<u>Απόδειξη:</u>

Έστω ότι $p \nmid a$. Τότε $(a,p)=1$ και σύμφωνα με την ιδιότητα του μέγιστου κοινού διαιρέτη, θα ισχύει :

$$1 = ax + py \text{, όπου } x,y \in \mathbb{Z} \Leftrightarrow b = abx + pby \text{, όπου } x,y \in \mathbb{Z}.$$

Όμως, $p \mid abx$ και $p \mid pby$. Άρα, $p \mid b$.
Ομοίως, αν $p \nmid b$ αποδεικνύεται ότι $p \mid a$. Συνεπώς, $p \mid a$ ή $p \mid b$. ■

<u>Θεώρημα (Το Θεμελιώδες Θεώρημα της Αριθμητικής):</u>

Κάθε θετικός ακέραιος μπορεί να αναπαρασταθεί ως γινόμενο δυνάμεων πρώτων παραγόντων κατά μοναδικό τρόπο.

<u>Απόδειξη:</u>

Θα αποδείξουμε αρχικά ότι κάθε θετικός ακέραιος μπορεί να αναπαρασταθεί ως γινόμενο πρώτων παραγόντων.

Κάθε θετικός ακέραιος αριθμός n, έχει διαιρέτες τους ακέραιους αριθμούς d, τέτοιους ώστε $1 < d \le n$. Στην περίπτωση που ο d είναι πρώτος αριθμός θα ισχύει ότι $n = d$. Σε κάθε άλλη περίπτωση είναι $1 < d < n$. Στην περίπτωση τώρα που ο n είναι σύνθετος θα ισχύει ότι $1 < d < n$. Ο ελάχιστος διαιρέτης d θα είναι αναγκαστικά πρώτος. Αυτό συμβαίνει διότι, αν υπήρχε ένας ακέραιος αριθμός d_0, όπου $d_0 \mid d$ με $d_0 \neq d$, τότε

$d_0 < d$. Αυτό όμως αντιβαίνει στην επιλογή του d ως ελάχιστου διαιρέτη. Έστω λοιπόν d_1 ο ελάχιστος αυτός διαιρέτης. Τότε :

$$n = d_1 n_1 \text{ , όπου } n_1 \in \mathbb{N}.$$

Ομοίως, ο θετικός ακέραιος n_1 έχει έναν ελάχιστο διαιρέτη d_2 , που είναι πρώτος αριθμός. Έτσι προκύπτει :

$$n = d_1 d_2 n_2 \text{, όπου } n_2 \in \mathbb{N}.$$

Συνεχίζοντας λοιπόν αυτή τη διαδικασία συνεπάγεται ότι ο θετικός ακέραιος n μπορεί να αναπαρασταθεί ως γινόμενο πρώτων παραγόντων. Επειδή όμως κάποιοι παράγοντες μπορεί να παρουσιάζονται περισσότερες από μία φορά στο παραπάνω γινόμενο, μπορούμε να το εκφράσουμε σαν γινόμενο δυνάμεων πρώτων παραγόντων. Έτσι :

$$n = p_1^{a_1} p_2^{a_2} \ldots p_\kappa^{a_\kappa} \text{ , όπου } \kappa \in \mathbb{N}.$$

Αυτή η παράσταση ονομάζεται *κανονική μορφή (canonical form)* .

Στη συνέχεια θα αποδείξουμε ότι η αναπαράσταση αυτή είναι μοναδική.

Ας υποθέσουμε ότι ο θετικός ακέραιος αριθμός n μπορεί να αναπαρασταθεί και με τον εξής διαφορετικό τρόπο $n = q_1^{b_1} q_2^{b_2} \ldots q_\lambda^{b_\lambda}$, $\lambda \in \mathbb{N}$.
Τότε ισχύει :

$$p_1^{a_1} p_2^{a_2} \ldots p_\kappa^{a_\kappa} = q_1^{b_1} q_2^{b_2} \ldots q_\lambda^{b_\lambda} \text{ , } \kappa, \lambda \in \mathbb{N}.$$

Από το πρώτο θεώρημα του Ευκλείδη έχουμε :

$p_i \mid p_1^{a_1} p_2^{a_2} \ldots p_\kappa^{a_\kappa} \Rightarrow p_i \mid q_1^{b_1} q_2^{b_2} \ldots q_\lambda^{b_\lambda} \Rightarrow p_i \mid q_j$ για κάθε i, j όπου $i = 1, 2, \ldots, \kappa$ και $j = 1, 2, \ldots, \lambda$

Άρα κάθε p_i είναι ίσο με ένα q_j. Άρα, $\kappa = \lambda$.
Αρκεί να δείξουμε ότι :

$$a_i = b_i \text{ , για κάθε } i \text{, όπου } i = 1, 2, \ldots, \kappa = \lambda$$

Έστω $a_i \neq b_i$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $a_i > b_i$.
Τότε :

$$p_1^{a_1} p_2^{a_2} \ldots p_i^{a_i} \ldots p_\kappa^{a_\kappa} = q_1^{b_1} q_2^{b_2} \ldots q_i^{b_i} \ldots q_\kappa^{b_\kappa} = p_1^{b_1} p_2^{b_2} \ldots p_i^{b_i} \ldots p_\kappa^{b_\kappa} \Leftrightarrow$$

$$\Leftrightarrow p_1^{a_1} p_2^{a_2} \ldots p_i^{a_i - b_i} \ldots p_\kappa^{a_\kappa} = p_1^{b_1} p_2^{b_2} \ldots p_{i-1}^{b_{i-1}} p_{i+1}^{b_{i+1}} \ldots p_\kappa^{b_\kappa}$$

Αφού $a_i - b_i \geq 1$, από την παραπάνω ισότητα προκύπτει ότι :

$p_i \mid p_1^{a_1} p_2^{a_2} \ldots p_\kappa^{a_\kappa}$ αλλά $p_i \nmid p_1^{b_1} p_2^{b_2} \ldots p_i^{b_i} \ldots p_\kappa^{b_\kappa}$, το οποίο είναι αδύνατον.

Ομοίως, καταλήγουμε σε άτοπο στην περίπτωση που $a_i < b_i$. Άρα, αναγκαστικά θα ισχύει ότι :

$a_i = b_i$, για κάθε $i = 1, 2, \ldots, \kappa$.

Έτσι ολοκληρώνεται η απόδειξη του θεωρήματος. ■

1.2.2. Ερατοσθένης

Ο Ερατοσθένης, μαθηματικός της αρχαίας Ελλάδας, επινόησε το 200 π.Χ. έναν απλό αλγόριθμο για την εύρεση όλων των πρώτων αριθμών μέχρι ένα συγκεκριμένο ακέραιο. Ο αλγόριθμος αυτός που ονομάζεται “Το κόσκινο του Ερατοσθένη” είναι γρήγορος για μικρούς πρώτους. Η εύρεση όλων των πρώτων αριθμών που είναι μικρότεροι ή ίσοι από έναν ακέραιο n , σύμφωνα με τη μέθοδο του Ερατοσθένη, γίνεται ως εξής:

1. Δημιουργούμε μια λίστα από διαδοχικούς ακέραιους από το 2 μέχρι το n: $(2, 3, 4, \ldots, n)$
2. Αρχικά, έστω ότι το p είναι ίσο με 2, τον πρώτο αριθμό.
3. Διαγράφουμε από τη λίστα όλα τα πολλαπλάσια του p που είναι μικρότερα ή ίσα με n. $(2p, 3p, 4p, \text{κτλ})$
4. Βρίσκουμε τον 1^o αριθμό που απομένει στη λίστα μετά τον p (αυτός ο αριθμός είναι ο επόμενος πρώτος αριθμός) και αντικαθιστούμε το p με αυτόν τον αριθμό.
5. Επαναλαμβάνουμε τα βήματα 3 και 4 μέχρι το p^2 να είναι μεγαλύτερο από n.
6. Όλοι οι αριθμοί που απομένουν στη λίστα είναι πρώτοι αριθμοί.

Παράδειγμα :

Για να βρούμε τους πρώτους αριθμούς που είναι μικρότεροι ή ίσοι από το 20 δημιουργούμε αρχικά μια λίστα από το 2 μέχρι το 20 :

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Διαγράφουμε τα πολλαπλάσια του 2 :

2	3	5	7	9	11	13	15	17	19

και στη συνέχεια παρατηρούμε ότι ο πρώτος αριθμός μετά το 2 είναι το 3 και διαγράφουμε τα πολλαπλάσιά του :

2	3	5	7	11	13	17	19

Ο επόμενος αριθμός μετά το 3 είναι το 5 αλλα αφού $5^2 = 25 > 20$ σταματάμε τη διαδικασία και έχουμε βρεί τους πρώτους αριθμούς μέχρι το 20.

1.3. Νεότερα χρόνια

Οι επόμενες εξελίξεις διαδραματίστηκαν αρκετά αργότερα γύρω στις αρχές του $17^{ου}$ αιώνα.

Ο Pierre de Fermat $(1601-1665)$, αν και με τα μαθηματικά ασχολήθηκε ερασιτεχνικά, συνέβαλε σημαντικά σε διάφορους κλάδους των μαθηματικών και έγινε διάσημος χάρη στις εργασίες του στη Θεωρία Αριθμών. Ειδικότερα έμεινε γνωστός για το λεγόμενο "Τελευταίο Θεώρημα του Fermat".

Θεώρημα (Τελευταίο Θεώρημα του Fermat) :

Αν n είναι φυσικός με $n > 2$ τότε η εξίσωση $a^n + b^n = c^n$ δεν έχει θετικές, ακέραιες λύσεις.
■

Ο Fermat εξετάζοντας τους πρώτους αριθμούς της μορφής 2^n+1 κατέληξε στο γνωστό Μικρό Θεώρημα του Fermat την απόδειξη του οποίου βλέπουμε στο επόμενο κεφάλαιο.

Θεώρημα (Το Μικρό Θεώρημα του Fermat) :

Αν p είναι ένας πρώτος αριθμός και $a \in \mathbb{Z}$ με $(a, p)=1$, τότε $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

Απόδειξη :

Στο επόμενο κεφάλαιο. ■

Αυτό το θεώρημα αποδεικνύει μέρος της λεγόμενης *Κινέζικης Υπόθεσης* που χρονολογείται γύρω στα 2000 χρόνια νωρίτερα και που λέει ότι ένας ακέραιος n είναι πρώτος αν και μόνο αν ο αριθμός 2^n-2 διαιρείται από τον n. Το υπόλοιπο μέρος είναι λάθος καθώς, για παράδειγμα, ο $2^{341}-2$ διαιρείται από τον 341 παρότι είναι σύνθετος: $341=31\cdot 11$.

Το μικρό θεώρημα Fermat είναι η βάση για πολλά άλλα αποτελέσματα στη Θεωρία Αριθμών και είναι η βάση για μεθόδους πιστοποίησης ενός πρώτου αριθμού που χρησιμοποιούνται έως σήμερα.

Ο Fermat αλληλογραφούσε με άλλους μαθηματικούς της εποχής του και ιδιαίτερα με τον καλόγερο Marin Mersenne $(1588-1648)$. Σε ένα από τα γράμματά του στον Mersenne υπέθεσε ότι οι αριθμοί 2^n+1 είναι πάντα πρώτοι αν ο n είναι δύναμη του 2. Το πιστοποίησε αυτό για $n=1,2,4,8$ και 16 και γνώριζε ότι εάν ο n δεν ήταν δύναμη του 2, το αποτέλεσμα αποτύγχανε. Οι αριθμοί της μορφής $F_n=2^{2^n}+1$, όπου n = 0, 1, 2,... καλούνται *αριθμοί Fermat*. Άρα ισχύει ότι

$$F_0=3,\ F_1=5,\ F_2=17,\ F_3=257,\ F_4=65537$$

Ο Fermat υπέθεσε πως όλοι οι αριθμοί της μορφής αυτής είναι πρώτοι. Την ίδια άποψη είχαν και οι M.Mersenne και C.Goldbach, μέχρι που το 1732 ο *Leonhard Euler* απέδειξε πως ο ακέραιος $F_5=2^{2^5}+1$ είναι σύνθετος αριθμός. Επίσης, λίγο αργότερα, ο *F.Gauss* ανακάλυψε μια σχέση ανάμεσα σε αυτούς τους πρώτους του Fermat και την κατασκευή

κανονικών πολυγώνων με κανόνα και διαβήτη. Απέδειξε ότι ένα κανονικό πολύγωνο με m πλευρές μπορεί να κατασκευαστεί με κανόνα και διαβήτη μόνο αν ο m είναι γινόμενο με παράγοντες που είναι δυνάμεις του 2 και διακριτούς πρώτους του Fermat.

Το έτος 1644 ο *Mersenne* διατύπωσε την εικασία ότι ο ακέραιος αριθμός M_p , όπου $M_p = 2^p - 1$ είναι πρώτος για $p = 2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127,\ 257$ και σύνθετος για τους υπόλοιπους πρώτους που είναι μικρότεροι του αριθμού 257 . Ωστόσο δεν έδωσε καμία απόδειξη και αργότερα η εικασία του αποδείχτηκε εν μέρει εσφαλμένη. Προς τιμήν του όμως οι αριθμοί αυτού του τύπου ονομάζονται *αριθμοί Mersenne* γιατί πρώτος εκείνος τους μελέτησε.

Η δουλειά του Euler $(1707-1783)$ είχε μεγάλη επίδραση στη θεωρία αριθμών γενικά και στους πρώτους αριθμούς συγκεκριμένα. Επέκτεινε το Μικρό Θεώρημα του Fermat και εισήγαγε την συνάρτηση φ του Euler. Όπως προαναφέρθηκε, παραγοντοποίησε τον 5^o αριθμό Fermat $2^{2^5}+1$, βρήκε 60 ζευγάρια φίλιων αριθμών και διατύπωσε (αλλά δεν ήταν σε θέση να αποδείξει) αυτό που έγινε γνωστό ως Νόμος της τετραγωνικής αντιστροφής. Ήταν ο πρώτος που συνειδητοποίησε ότι η Θεωρία Αριθμών μπορούσε να μελετηθεί χρησιμοποιώντας εργαλεία της ανάλυσης και ανέπτυξε την Αναλυτική Θεωρία Αριθμών. Επίσης, έδειξε ότι αποκλίνουν όχι μόνο οι καλούμενες αρμονικές σειρές $\sum\left(1/n\right)$, αλλά και οι σειρές $1/2+1/3+1/5+1/7+1/11+\ldots$ αποτελούμενες από τα αντίστροφα των πρώτων αριθμών.

Το άθροισμα σε n όρους της αρμονικής σειράς μεγαλώνει περίπου όπως το $\log(n)$ ενώ η τελευταία σειρά αποκλίνει ακόμα πιο αργά όπως το $\log\left[\log(n)\right]$.

Με μια πρώτη ματιά οι πρώτοι αριθμοί φαίνεται να είναι κατανεμημένοι στους ακέραιους με έναν μάλλον τυχαίο τρόπο. Για παράδειγμα στους 100 αριθμούς αμέσως πριν το $10.000.000$ υπάρχουν 10 πρώτοι αριθμοί, ενώ στους 100 αμέσως επόμενους υπάρχουν μόλις 2 πρώτοι. Εντούτοις, σε μεγάλη κλίμακα, ο τρόπος με τον οποίο κατανέμονται οι πρώτοι είναι αρκετά τακτικός.

Δύο επίσης σπουδαίοι μαθηματικοί, ο Legendre και ο Gauss έκαναν και οι δύο εκτεταμένους υπολογισμούς για την πυκνότητα των πρώτων αριθμών. Ο Gauss είχε πει συγκεκριμένα σε κάποιον φίλο του ότι όποτε είχε ελεύθερα 15 λεπτά θα τα ξόδευε υπολογίζοντας πρώτους σε μια κλίμακα 1.000 αριθμών. Εκτιμάται ότι μέχρι το τέλος της ζωής του είχε υπολογίσει όλους τους πρώτους μέχρι περίπου το $3.000.000$. Το συμπέρασμα που έβγαλαν και οι δύο ήταν ότι για μεγάλο n (πλήθος αριθμών) η πυκνότητα των πρώτων αριθμών είναι κατά μέσο όρο $1/\log(n)$. Ο Legendre έδωσε την εξής εκτίμηση για το πλήθος των πρώτων αριθμών μικρότερων ή ίσων με το n :

$$\pi(n) = n/(\log(n) - 1.08366)$$

ενώ η εκτίμηση του Gauss δίνεται από το λογαριθμικό ολοκλήρωμα

$$\pi(n) = \int_2^n (1/\log(t))\,dt \quad .$$

Το συμπέρασμα λοιπόν για το ότι η πυκνότητα των πρώτων αριθμών είναι $1/\log(n)$ είναι γνωστό ως **Θεώρημα των Πρώτων Αριθμών (Prime number theorem (P. N. T.))** και αποτελεί σημείο αναφοράς στην αριθμοθεωρία. Παρ' όλο που δεν μας δίνει όλη την πληροφορία για το πότε ένας αριθμός είναι πρώτος αποτελεί το σημαντικότερο ίσως αποτέλεσμα που έχουμε σχετικά με τους πρώτους. Το Θ. Π. Α. για πολύ καιρό έμεινε αναπόδεικτο σαν υπόθεση μέχρι τη δημοσίευση δύο άρθρων (ανεξάρτητα το ένα από το άλλο) που το απέδειξαν χρησιμοποιώντας τη συνάρτηση $\zeta(s)$ του Ρίμαν όπου $s = \alpha + \beta i$ είναι μιγαδικός αριθμός . Ειδικότερα αποδείξανε ότι η $\zeta(s)$ δεν μηδενίζεται για $\alpha = 1$. Συγκεκριμένα αποδείχτηκε το εξής :

$$\pi(x) = x/\ln x + O(xe^{-\kappa\sqrt{\ln x}}) \text{ για κάποια σταθερά } \kappa > 0 \ .$$

Το αποτέλεσμα τελικά αποδείχτηκε από τους Hadamard και de la Vallée Poussin το 1896 .

2. Βασικοί ορισμοί και εισαγωγική θεωρία αριθμών

Ορισμός :

Ονομάζουμε *πρώτο αριθμό* (prime number) κάθε θετικό ακέραιο μεγαλύτερο της μονάδας, ο οποίος δεν έχει άλλους διαιρέτες εκτός από τον εαυτό του και την μονάδα.

Για παράδειγμα, οι ακέραιοι 2, 3, 5, 11, 13 είναι όλοι πρώτοι αριθμοί, ενώ οι ακέραιοι 4, 8, 12, 15, 21 δεν είναι πρώτοι αριθμοί. Ο αριθμός 2 είναι ο μοναδικός άρτιος πρώτος αριθμός. Επίσης ο αριθμός 1 δεν θεωρείται πρώτος αριθμός.

Ορισμός :

Οι ακέραιοι οι οποίοι δεν είναι πρώτοι και είναι μεγαλύτεροι της μονάδας, ονομάζονται *σύνθετοι αριθμοί.*

Ορισμός :

Δύο ακέραιοι αριθμοί a και b ονομάζονται *πρώτοι μεταξύ τους* (relatively prime) αν δεν υπάρχει φυσικός αριθμός c μεγαλύτερος της μονάδας, τέτοιος ώστε να διαιρεί ταυτόχρονα τους a και b.

Ορισμός :

Η *συνάρτηση* $\varphi(n)$ *του Euler* μας δίνει το πλήθος των θετικών ακεραίων των μικρότερων (ή μικρότερων ή ίσων) του n που είναι ίσοι με τον n .

2.1. Γραμμικές ισοδυναμίες – Βασικά θεωρήματα

Ορισμός :

Δύο ακέραιοι ορισμοί a,b λέγονται ισοδύναμοι *ή ισότιμοι (ή ισουπόλοιποι) modulo* m , όπου m ένας ακέραιος αριθμός, αν ο m διαιρεί τη διαφορά $a-b$ και συμβολίζουμε

$$a \equiv b(\mathrm{mod}\, m).$$

Στην περίπτωση που η διαφορά $a-b$ δεν διαιρείται με τον m, τότε συμβολίζουμε

$$a \neq b(\mathrm{mod}\, m) .$$

Θεώρημα (Euler):

Αν a,m ακέραιοι με $(a,m)=1$ τότε

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

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

Απόδειξη:

Θεωρούμε τους $\varphi(m)$ το πλήθος αριθμούς $r_1, r_2, ..., r_{\varphi(m)}$ που αποτελούν ένα περιορισμένο σύνολο υπολοίπων $\mathrm{mod}\, m$. Αν πολλαπλασιάσουμε με το $a(\mathrm{mod}\, m)$ παίρνουμε τους αριθμούς

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

Εφόσον $\mathrm{MK\Delta}(a,m)=1$ έχουμε ότι ούτε ο a ούτε ο r_i έχουν παράγοντα τον αριθμό m, άρα οι αριθμοί ar_i είναι και αυτοί πρώτοι προς τον m για κάθε i. Επίσης είναι όλοι μη ισοδύναμοι μεταξύ τους διότι αν $ar_i = ar_j \mathrm{mod}\, m$,για $i \neq j$, θα είχαμε από τον κανόνα της απλοποίησης $r_i = r_j \mathrm{mod}\, m$, αφού $(a,m)=1$, κάτι το οποίο είναι άτοπο. Μπορούμε λοιπόν να αντιστοιχίσουμε κάθε αριθμό ar_i με κάποιον r_j έτσι ώστε $ar_i = r_j \mathrm{mod}\, m$ και

μάλιστα ο κάθε r_j ορίζεται μοναδικά για κάθε ar_i. Αλλά και ο κάθε r_j αντιστοιχεί με κάποιον ar_i διότι έχουμε $\varphi(m)$ το πλήθος r_j και $\varphi(m)$ το πλήθος ar_i. Συνεπώς οι αριθμοί $a\cdot r_1, a\cdot r_2, ..., a\cdot r_{\varphi(m)} (\mathrm{mod}\, m)$ είναι ίδιοι με τους $r_1, r_2, ..., r_{\varphi(m)}$, με διαφορετική ίσως διάταξη. Οπότε έχουμε

$$\begin{aligned} \left(a\cdot r_1\right)\left(a\cdot r_2\right)...\left(a\cdot r_{\varphi(m)}\right) &\equiv r_1 r_2 ... r_{\varphi(m)} (\mathrm{mod}\, m) \quad \text{ή} \\ a^{\varphi(m)} r_1 r_2 ... r_{\varphi(m)} &\equiv r_1 r_2 ... r_{\varphi(m)} (\mathrm{mod}\, m) \quad \text{ή} \\ a^{\varphi(m)} &\equiv 1 (\mathrm{mod}\, m), \end{aligned}$$

όπως προκύπτει από τον κανόνα της απλοποίησης αφού το γινόμενο $r_1, r_2, ..., r_{\varphi(m)}$ είναι ένα γινόμενο $\varphi(m)$ παραγόντων που είναι πρώτοι προς τον m. ■

Το Μικρό Θεώρημα του Fermat που βλέπουμε στη συνέχεια είναι μια ειδική περίπτωση του θεωρήματος του Euler.

<u>Θεώρημα (Το μικρό θεώρημα Fermat):</u>

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

<u>Απόδειξη:</u>

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

Παρατήρηση:

Στην απόδειξη του επόμενου θεωρήματος χρησιμοποιούμε τα εξής:

1. Άν $a\bar{a} = 1 \mathrm{mod}\, p$ τότε ο $\bar{a}$ είναι ο αντίστροφος του $a \,\mathrm{mod}\, p$.
2. Άν $\mathrm{ΜΚΔ}(a, p) = 1$ τότε ο a έχει αντίστροφο που είναι μοναδικός $\mathrm{mod}\, p$

Θεώρημα (Wilson):

Ο φυσικός $p > 2$ είναι πρώτος αν και μόνο αν

$$(p-1)! \equiv -1 (\mathrm{mod}\ p).$$

Απόδειξη:

Υποθέτουμε ότι ο p είναι πρώτος και θεωρούμε τους $p-1$ ακεραίους $1, 2, ..., p-1$. Άν a κάποιος από τους αριθμούς αυτούς, τότε υπάρχει ο αντίστροφος του $\bar{a}$ με $1 \le \bar{a} \le p-1$ και $a\bar{a} = 1 \mathrm{mod}\ p$.

Πιθανόν, $a = \bar{a}$ δηλαδή $a^2 = 1 \mathrm{mod}\ p$ δηλαδή ο a να συμπίπτει με τον αντίστροφό του. Όμως στην περίπτωση αυτή

$$a^2 - 1 = kp \Rightarrow (a-1)(a+1) = kp \text{ ήτοι } p \mid (a-1)(a+1)$$

Και αφού ο p είναι πρώτος θα ισχύει:

$$p \mid a-1 \text{ είτε } p \mid a+1 \text{ άρα } a = \pm 1 \mathrm{mod}\ p.$$

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

Για παράδειγμα αν $p = 11$ γράφουμε

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

Έχουμε λοιπόν

$$(p-1)! = (p-1)(p-2)! = (p-1)\cdot 1\cdot 1...1 \mathrm{mod}\ p = -1 \mathrm{mod}\ p\ .$$

Αντίστροφα :

Έστω ότι ο p δεν είναι πρώτος. Τότε υπάρχει a : $1 < a < p$ με $a \mid p$. Προφανώς επίσης $a \mid (p-1)!$ (αφού ο παράγοντας $a < p$ υπάρχει μέσα στο $(p-1)!$). Άν λοιπόν $(p-1)! = -1 \mathrm{mod}\ p$ τότε υπάρχει ακέραιος k με $(p-1)!+1 = kp$. Αφού $a \mid p$ και $a \mid (p-1)!$ ο a θα διαιρεί και τη διαφορά τους, άρα $a \mid 1$, αδύνατο διότι υποθέσαμε ότι $a > 1$. Βλέπουμε λοιπόν ότι όταν ο p δεν είναι πρώτος η σχέση $(p-1)! = -1 \mathrm{mod}\ p$ δεν μπορεί να ισχύει. ■

Παρατήρηση :

Το θεώρημα Wilson αποτελεί ένα από τα λίγα καθολικά κριτήρια με το οποίο μπορούμε να διαπιστώσουμε αν ένας αριθμός είναι πρώτος, το οποίο είναι ωστόσο ιδιαίτερα δύσχρηστο λόγω των μεγάλων αριθμών που προκύπτουν από τη συνάρτηση παραγοντικό και γι αυτό δεν χρησιμοποιείται συχνά.

Στη συνέχεια θα εξετάσουμε τη λύση ενός συστήματος πρωτοβάθμιων ισοδυναμιών μέσω του λεγόμενου Κινέζικου Θεωρήματος Υπολοίπων.

<u>Θεώρημα (Κινέζικο Θεώρημα Υπολοίπων) :</u>

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

$$a_1 x = b_1 \bmod m_1$$
$$a_2 x = b_2 \bmod m_2$$
$$.....$$
$$\mathrm{a}_s x = b_s \bmod m_s$$

έχουν μία μοναδική λύση $\bmod M$.

<u>Απόδειξη :</u>

Από τη λύση κάθε ισοδυναμίας θα κατασκευάσουμε μια λύση για όλο το σύστημα. Επιλέγουμε ακεραίους $c_1, c_2, ..., c_s$ τέτοιους ώστε

$$a_i c_i = b_i \bmod m_i \ .$$

Θέτουμε $n_i = \dfrac{M}{m_i}$ και επειδή όλοι οι m_i είναι πρώτοι προς αλλήλους έχουμε ότι $\text{ΜΚΔ}(n_i, m_i) = 1$. Τότε όμως ο n_i έχει μοναδικό αντίστροφο $\bmod m_i$, δηλαδή υπάρχει $\overline{n}_i$ με $n_i \overline{n}_i = 1 \bmod m_i$, $1 \le i \le s$.

Στη συνέχεια με τη βοήθεια των c_i και $\overline{n}_i$ κατασκευάζουμε έναν αριθμό x_0 που θα αποδείξουμε ότι είναι λύση κάθε μίας από τις s ισοδυναμίες.

Έστω $x_0 = c_1 n_1 \overline{n}_1 + c_2 n_2 \overline{n}_2 + \ldots + c_s n_s \overline{n}_s$.

Ας παρατηρήσουμε ότι ο m_i διαιρεί όλους τους n_j εκτός από τον n_i με τον οποίο έχει $\text{ΜΚΔ}(n_i, m_i) = 1$.

Άρα

$$\begin{aligned} a_i x_0 &= a_i c_1 n_1 \overline{n}_1 + a_i c_2 n_2 \overline{n}_2 + \ldots + a_i c_s n_s \overline{n}_s = \\ &= a_i c_i n_i \overline{n}_i \bmod m_i = \\ &= a_i c_i \bmod m_i = \\ &= b_i \bmod m_i \end{aligned}$$

Οπότε το x_0 είναι λύση και των s ισοδυναμιών και επιπλέον είναι μοναδική.

Πράγματι αν y είναι μια άλλη λύση των s ισοδυναμιών έχουμε $x_0 = c_i = \text{y} \bmod m_i$. Άρα $x_0 - \text{y} = \text{πολ} m_i$ για κάθε m_i . Όμως όλα τα m_i είναι πρώτα μεταξύ τους άρα $x_0 - \text{y} = \text{πολ} m_1 m_2 \ldots m_s$, δηλαδή $\text{y} = x_0 \bmod M$. ■

<u>Παράδειγμα :</u>

Έστω η ισοδυναμία $3x = 11 \bmod 2275$. Έχουμε δηλαδή το σύστημα

$$\begin{aligned} 3x &= 11 \bmod 25 \\ 3x &= 11 \bmod 7 \\ 3x &= 11 \bmod 13 \end{aligned}$$

Είναι $\text{ΜΚΔ}(2275, 3) = 1$ άρα η αρχική ισοδυναμία έχει λύση.

Η παραπάνω ισοδυναμίες έχουν αντίστοιχα λύσεις

$$x = 12 = c_1$$
$$x = 6 = c_2$$
$$x = 8 = c_3$$

Στη συνέχεια βρίσκουμε $\bar{n}_1, \bar{n}_2, \bar{n}_3$ με

$$\frac{2275}{25}\bar{n}_1 = 91\bar{n}_1 = 1 \bmod 25 \Rightarrow 16\bar{n}_1 = 1 \bmod 25$$
$$\frac{2275}{7}\bar{n}_2 = 325\bar{n}_2 = 1 \bmod 7 \Rightarrow 3\bar{n}_2 = 1 \bmod 7$$
$$\frac{2275}{13}\bar{n}_3 = 175\bar{n}_3 = 1 \bmod 13 \Rightarrow 6\bar{n}_3 = 1 \bmod 13$$

με λύσεις :

$$\bar{n}_1 = 11$$
$$\bar{n}_2 = 5$$
$$\bar{n}_3 = 11$$

Οπότε

$$\begin{aligned} x_0 &= 12 \cdot 91 \cdot 11 + 6 \cdot 325 \cdot 5 + 8 \cdot 175 \cdot 11 \\ &= 12012 + 9750 + 15 \cdot 400 \\ &= 37162 = 762 \bmod 2275 . \end{aligned}$$

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

Παρατηρούμε λοιπόν ότι λύσαμε 6 ισοδυναμίες αντί για 1 αλλά με πολύ μικρότερα μέτρα απο το 2275 .

2.2. Τετραγωνικά υπόλοιπα

Ορισμός :

Ο ακέραιος αριθμός a είναι τετραγωνικό υπόλοιπο (quadratic residue) του θετικού ακεραίου p, αν $(a, p)=1$ και η ισοτιμία $x^2 \equiv a(\mathrm{mod}\, p)$ έχει λύση. Διαφορετικά ο a καλείται μη τετραγωνικό υπόλοιπο modulo p.

Στη συνέχεια θα δούμε κάποια από τα βασικά θεωρήματα σχετικά με τα τετραγωνικά υπόλοιπα.

Θεώρημα:

Έστω p περιττός πρώτος αριθμός και a ένας ακέραιος αριθμός τέτοιος ώστε $(a, p)=1$. Τότε, η

$$x^2 \equiv a(\mathrm{mod}\, p) \qquad (1)$$

είτε δεν θα έχει καμμία λύση ή θα έχει δύο διαφορετικές λύσεις, δηλαδή δύο λύσεις μη-ισοδύναμες $\mathrm{mod}\, p$.

Απόδειξη:

Έστω x_0 μια λύση της ισοτιμίας. Τότε $x_0 \equiv a(\mathrm{mod}\, p)$. Είναι προφανές ότι και το $-x_0$ είναι λύση αφού $(-x_0)^2 = {x_0}^2 \equiv a(\mathrm{mod}\, p)$. Ισχύει όμως ότι $x_0 \neq -x_0(\mathrm{mod}\, p)$, αφού αν ήταν $x_0 \equiv -x_0(\mathrm{mod}\, p)$ τότε $p \mid 2x_0$ δηλαδή, $p \mid x_0$ άρα $p \mid {x_0}^2$, άτοπο. Θα δείξουμε ότι δεν υπάρχουν άλλες, διαφορετικές μεταξύ τους, λύσεις. Έστω x_1 μια άλλη λύση. Τότε ${x_0}^2 \equiv a(\mathrm{mod}\, p)$ και ${x_1}^2 \equiv a(\mathrm{mod}\, p)$. Άρα

$${x_0}^2 = {x_1}^2 \equiv a(\mathrm{mod}\, p)\ \text{, δηλαδή}\ {x_0}^2 - {x_1}^2 \equiv 0(\mathrm{mod}\, p)$$

οπότε έχουμε

$$p \mid {x_0}^2 - {x_1}^2$$
$$\Rightarrow p \mid (x_0 - x_1)(x_0 + x_1)$$

Δηλαδή

$$p \mid (x_0 - x_1) \text{ ή } p \mid (x_0 + x_1).$$

Αυτό όμως σημαίνει ότι

$$x_0 \equiv x_1 (\text{mod } p) \text{ ή } -x_0 \equiv x_1 (\text{mod } p).$$

Άτοπο διότι υποθέσαμε ότι η x_1 είναι διαφορετική λύση. Επομένως δεν υπάρχουν άλλες λύσεις και οι μοναδικές λύσεις είναι οι x_0 και $-x_0$. ■

Θεώρημα:

Έστω p περιττός αριθμός, τότε υπάρχουν $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα και $\frac{p-1}{2}$ τετραγωνικά μη υπόλοιπα modulo p.

Απόδειξη:

Παρατηρούμε ότι

$$p-1 \equiv -1 (\text{mod } p)$$
$$p-2 \equiv -2 (\text{mod } p)$$
$$\vdots$$
$$p - \frac{p-1}{2} \equiv -\frac{p-1}{2} (\text{mod } p).$$

Άρα

$$(p-1)^2 \equiv 1^2 (\text{mod } p)$$
$$(p-2)^2 \equiv 2^2 (\text{mod } p)$$
$$\vdots$$
$$(p - \frac{p-1}{2})^2 \equiv (\frac{p-1}{2})^2 (\text{mod } p).$$

Επομένως, οι ακέραιοι $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$ είναι όλοι τετραγωνικά υπόλοιπα $\bmod p$. Θα δείξουμε τώρα ότι είναι και ανα δύο μη-ισοδύναμοι $\bmod p$.

Έστω

$$x_1, x_2 \in \left\{1, 2, ..., \frac{p-1}{2}\right\}.$$

Τότε λοιπόν θα ισχύει

$$1 < x_1 + x_2 < p \qquad (1)$$

Άρα για $x_1 \neq x_2$, αν ισχύει $x_1^2 \equiv x_2^2 (\bmod p)$, τότε $p \mid (x_1 - x_2)(x_1 + x_2)$, δηλαδή $p \mid (x_1 - x_2)$ ή $p \mid (x_1 + x_2)$. Επειδή όμως ισχύει η ανισότητα (1) προκύπτει ότι

$$p \mid (x_1 - x_2).$$

Όμως $|x_1 - x_2| < p$. Άρα πρέπει να ισχύει $x_1 = x_2$ το οποίο είναι άτοπο αφού υποθέσαμε ότι $x_1 \neq x_2$.

Επομένως, σύμφωνα με τα παραπάνω, υπάρχουν ακριβώς $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα τα οποία είναι οι αριθμοί $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$ και $\frac{p-1}{2}$ τετραγωνικά μη-υπόλοιπα του p. ■

2.2.1. Σύμβολο Legendre

Στη θεωρία των τετραγωνικών υπολοίπων τα πράγματα διευκολύνονται ιδιαίτερα με την εισαγωγή ενός συμβόλου, του συμβόλου Legendre. Το σύμβολο αυτό είναι ένας άλλος τρόπος για τον έλεγχο των τετραγωνικών υπολοίπων καθώς μας επιτρέπει να εκφράσουμε τυποποιημένα πότε ένας αριθμός είναι τετραγωνικό υπόλοιπο κάποιου πρώτου αριθμού.

Ορισμός :

Έστω p ένας περιττός πρώτος αριθμός και a ένας ακέραιος αριθμός ώστε $(a, p) = 1$. Τότε ορίζουμε το σύμβολο Legendre

$$\left(\frac{a}{p}\right)$$

ως εξής :

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ αν ο ακέραιος } a \text{ είναι τετραγωνικό υπόλοιπο } \bmod p \\ -1, \text{ αν ο ακέραιος } a \text{ δεν είναι τετραγωνικό υπόλοιπο } \bmod p \end{cases}$$

Το σύμβολο του Legendre γενικεύεται και στην περίπτωση όπου $p \mid a$ λαμβάνοντας μηδενική τιμή. Δηλαδή

$$\left(\frac{a}{p}\right) = 0 \text{, αν } p \mid a \text{ .}$$

Ιδιότητες :

1. Άν $a \equiv b \bmod p$, τότε $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $b^{\frac{p-1}{2}} = \left(\frac{b}{p}\right) \bmod p$
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, με $(ab, p) = 1$
4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
5. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
6. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

Ο Euler εισήγαγε πρώτος ένα κριτήριο για να δούμε αν κάποιος αριθμός είναι τετραγωνικό υπόλοιπο ή όχι.

Εξετάζουμε αρχικά ένα λήμμα και στη συνέχεια το Κριτήριο του Euler.

Λήμμα:

Άν p μονός πρώτος και $(a, p)=1$ τότε είτε

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

Απόδειξη:

Αφού p πρώτος και $(a, p)=1$ από θεώρημα Fermat έχουμε ότι

$$a^{p-1} = 1 \bmod p \text{ ή } (a^{p-1}-1) = \pi\text{ολ}p \text{ ή } \left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right) \equiv 0 \bmod p .$$

Άρα, είτε $a^{\frac{p-1}{2}} = 1 \bmod p$ είτε $a^{\frac{p-1}{2}} = -1 \bmod p$. ■

Θεώρημα (Το Κριτήριο του Euler):

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

Απόδειξη:

Έστω μονός πρώτος p με $(a, p)=1$ και $1 \le r \le p-1$. Αφού η ισοδυναμία $rx = a \bmod p$ έχει μοναδική λύση, διότι $(r, p)=1$, τότε υπάρχει ακριβώς ένα στοιχείο s με $1 \le s \le p-1$ έτσι ώστε $rs = a \bmod p$, δηλαδή το στοιχείο s είναι η λύση της ισοδυναμίας. Γνωρίζουμε ότι $(a, p)=1$. Άρα, αποκλείεται η περίπτωση $\left(\frac{a}{p}\right)=0$. Οπότε θα έχουμε

$$\left(\frac{a}{p}\right) = \pm 1 .$$

Περίπτωση 1^{η}

Άν $\left(\frac{a}{p}\right)=1$, τότε ο ακέραιος a είναι τετραγωνικό υπόλοιπο του p και συνεπώς υπάρχει ακέραιος αριθμός x_0 τέτοιος ώστε

$$x_0{}^2 \equiv a(\mathrm{mod}\ p)\ .$$

Συνεπώς

$$\begin{aligned}(x_0{}^2)^{\frac{p-1}{2}} &\equiv a^{\frac{p-1}{2}}(\mathrm{mod}\ p)\\ \Rightarrow (x_0{}^{p-1}) &\equiv a^{\frac{p-1}{2}}(\mathrm{mod}\ p)\\ \Rightarrow \left(a^{\frac{p-1}{2}}\right) &\equiv x_0{}^{p-1}(\mathrm{mod}\ p) \qquad (1)\end{aligned}$$

Όμως, γνωρίζουμε ότι $(x_0, p)=1$ αφού $p\,|\,(x_0^2-a)$ και $(a, p)=1$. Επομένως από το Μικρό Θεώρημα του Fermat προκύπτει

$$x_0^{p-1} \equiv 1(\mathrm{mod}\ p) \qquad (2)$$

Άρα από τις σχέσεις (1) και (2) προκύπτει

$$\begin{aligned}a^{\frac{p-1}{2}} &\equiv 1 \mathrm{mod}\ p\\ \Rightarrow 1 &\equiv a^{\frac{p-1}{2}}\ \mathrm{mod}\ p\end{aligned}$$

Δηλαδή

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

Περίπτωση 2^{η}

Άν $\left(\frac{a}{p}\right)=-1$, τότε ο ακέραιος a είναι τετραγωνικό μη-υπόλοιπο του p οπότε για τον s θα είναι $r \neq s$, διότι αν $r=s$ τότε $r^2 = a \bmod p$ ήτοι το a είναι τετραγωνικό υπόλοιπο,

άτοπο. Τα στοιχεία του $\{1,2,\ldots,p-1\}$ μπορούν να γίνουν ζεύγη r_i, s_i έτσι ώστε $r_i \cdot s_i = a \bmod p \quad i = 1,2,\ldots,\frac{p-1}{2}$. Αλλά τότε από το θεώρημα Wilson έχουμε

$$(-1) \equiv (p-1)! \equiv \prod_{i=1}^{\frac{p-1}{2}} r_i s_i \equiv a^{\frac{p-1}{2}} \bmod p \ .$$

Δηλαδή

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

Παρατήρηση:

Το κριτήριο του Euler είναι μια μέθοδος με την οποία μπορούμε να δούμε αν ο ακέραιος a είναι τετραγωνικό υπόλοιπο του περιττού πρώτου p. Υπολογίζω το $a^{\frac{p-1}{2}} \bmod p$ και εάν είναι 1 τότε το a είναι τετραγωνκό υπόλοιπο, διαφορετικά εάν είναι -1 τότε το a δεν είναι τετραγωνικό υπόλοιπο.

<u>Θεώρημα (Λήμμα του Gauss):</u>

Άν p μονός πρώτος και $(a, p) = 1$ τότε

$$\left(\frac{a}{p}\right) = (-1)^s$$

όπου s το πλήθος των στοιχείων του $\left\{a, 2a, 3a, \ldots, \frac{(p-1)}{2}a\right\}$ που είναι μεγαλυτερα του $\frac{p}{2}$.

Απόδειξη:

Βιβλίο "Κρυπτογραφία" , Χ.Κουκουβίνος, Α.Παπαιωάννου

Σελίδες $57-59$. ■

Θεώρημα (Νόμος τετραγωνικής αντιστροφής ή αμοιβαιότητας):

Άν $p \neq q$ μονοί πρώτοι τότε $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}$.

Απόδειξη:

Βιβλίο "Κρυπτογραφία" , Χ.Κουκουβίνος, Α.Παπαιωάννου

Σελίδες $59-62$. ■

2.2.2. Σύμβολο Jacobi

Το σύμβολο Jacobi είναι μία γενίκευση του συμβόλου Legendre και χρησιμεύει στα τεστ πιστοποίησης πρώτων αριθμών καθώς και στην παραγοντοποίηση ακεραίων.

Ορισμός :

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

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

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

Ιδιότητες :

1. Άν $a \equiv b(\mathrm{mod}\, P)$ τότε $\left(\frac{a}{P}\right)=\left(\frac{b}{P}\right)$
2. $\left(\frac{ab}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$
3. $\left(\frac{a}{PQ}\right)=\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$
4. $\left(\frac{ab^2}{P}\right)=\left(\frac{a}{P}\right)$ αν $\mathrm{ΜΚΔ}(b,P)=1$
5. $\left(\frac{a}{PQ^2}\right)=\left(\frac{a}{P}\right)$ αν $\mathrm{ΜΚΔ}(a,Q)=1$
6. $\left(\frac{a+cP}{P}\right)=\left(\frac{a}{P}\right)$ για ακεραίους c . Παρόμοια $\left(\frac{a}{P}\right)=\left(\frac{a \bmod P}{P}\right)$
7. $\left(\frac{2^{2k}\cdot a}{P}\right)=\left(\frac{a}{P}\right)$ και $\left(\frac{2^{2k+1}\cdot a}{P}\right)=\left(\frac{2}{P}\right)\left(\frac{a}{P}\right)$, $k \geq 1$
8. $\left(-\frac{1}{P}\right)=(-1)^{\frac{P-1}{2}}=\begin{cases} 1, & \alpha\nu\ P \equiv 1(\mathrm{mod}\, 4) \\ -1, & \alpha\nu\ P \equiv 3(\mathrm{mod}\, 4) \end{cases}$
9. $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}=\begin{cases} 1, & \alpha\nu\ P \equiv 1 \text{ ή } 7(\mathrm{mod}\, 8) \\ -1, & \alpha\nu\ P \equiv 3 \text{ ή } 5(\mathrm{mod}\, 8) \end{cases}$
10. $\left(\frac{m}{P}\right)=\left(\frac{P}{m}\right)(-1)^{\frac{P-1}{2}\cdot\frac{m-1}{2}}=\begin{cases} \left(\frac{P}{m}\right), & \alpha\nu\ P \equiv 1(\mathrm{mod}\, 4) \text{ ή } \mathrm{m} \equiv 1(\mathrm{mod}\, 4) \\ -\left(\frac{P}{m}\right), & \alpha\nu\ P \equiv m \equiv 3(\mathrm{mod}\, 4) \end{cases}$

(Νόμος Τετραγωνικής Αντιστροφής)

Παρατηρήσεις :

1. Σημαντικό για τα παρακάτω είναι να παρατηρήσουμε ότι με τη βοήθεια των παραπάνω ιδιοτήτων μπορούμε να υπολογίσουμε το σύμβολο Jacobi ενός αριθμού χωρίς να ξέρουμε την παραγοντοποίησή του.
2. Άν P πρώτος το σύμβολο του Jacobi συμπίπτει με το σύμβολο του Legendre.
3. Άν $(a,P)>1 \Rightarrow$ τα $a,\ P$ έχουν κοινό παράγοντα $\Rightarrow p_i \mid a$ για κάποιο i
   $\Rightarrow \left(\frac{a}{p_i}\right)^{k_i} = 0 \Rightarrow \left(\frac{a}{P}\right) = 0$.
4. Στην περίπτωση που $(a,P)=1$ το σύμβολο Jacobi δεν δίνει πληροφορία αν το a είναι τετραγωνικό υπόλοιπο $\bmod n$ ή όχι.

Για την εύρεση του συμβόλου Jacobi χρησιμοποιούμε τον παρακάτω αλγόριθμο που προκύπτει από τις ιδιότητες του συμβόλου Jacobi.

Αλγόριθμος (Σύμβολο του Jacobi)

Input : ακέραιος a , μονός ακέραιος $n \geq 3$
Method :

1. b, c, s ακέραιοι
2. $b \leftarrow a \bmod n$;
3. $c \leftarrow n$;
4. $s \leftarrow 1$
5. while $b \geq 2$ repeat
   6. while $4 \mid b$ repeat $b \leftarrow b \mid 4$
   7. if $2 \mid b$ then
      8. if $c \bmod 8 \in \{3,5\}$ then $s \leftarrow (-s)$
      9. $b \leftarrow b \mid 2$
   10. if $b = 1$ then break
   11. if $b \bmod 4 = c \bmod 4 = 3$ then $s \leftarrow (-s)$
   12. $(b,c) \leftarrow (c \bmod b, b)$;
13. return $s \cdot b$

Παράδειγμα :

Θα υπολογίσουμε το σύμβολο Jacobi $\left(\frac{1828}{757}\right)$ ακολουθώντας τα βήματα του παραπάνω αλγόριθμου.

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

Άρα προκύπτει ότι $\left(\frac{1828}{757}\right)=1$.

2.3. Πρωταρχικές Ρίζες

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

Θεώρημα :

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

Απόδειξη :

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

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

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

Θεώρημα :

Αν $\text{ord}_n(a) = k$ τότε $a^h = 1 \bmod n$ αν και μόνο αν $k \mid h$.

Απόδειξη :

Έστω $(a,n) = 1$, $\text{ord}_n(a) = k$ και $a^h = 1 \bmod n$. Από τον αλγόριθμο της διαίρεσης υπάρχουν ακέραιοι q, s τέτοιοι ώστε $h = kq + s$ με $0 < s < k$ (αν $s = 0$ τότε $k \mid h$). Αλλά

τότε $a^h = a^{kq+s} = \left(a^k\right)^q \cdot a^s$. Όμως $a^k = 1 \bmod n$ από τον ορισμό της τάξης οπότε θα πρέπει να ισχύει και ότι $a^s = 1 \bmod n$ που έρχεται σε αντίφαση με το ότι ο k είναι ο ελάχιστος ακέραιος με την ιδιότητα $a^k = 1 \bmod n$. Άρα $s = 0$ και $k \mid h$. ■

Αν λοπόν γνωρίζουμε την τάξη $\mathrm{ord}_n(a)$ το παρακάτω θεώρημα μας δίνει την $\mathrm{ord}_n\left(a^m\right)$.

<u>Θεώρημα :</u>

Αν $\mathrm{ord}_n(a) = k$ τότε $\mathrm{ord}_n\left(a^m\right) = \dfrac{k}{\mathrm{MK\Delta}(m,k)}$.

<u>Απόδειξη :</u>

Έστω $\mathrm{ord}_n(a) = k$,

$\mathrm{ord}_n\left(a^m\right) = r$ και

$\mathrm{MK\Delta}(m,k) = d \Rightarrow m = bd,\ k = cd$ με $\mathrm{MK\Delta}(b,c) = 1.$

Άρα $\left(a^m\right)^c = \left(a^{bd}\right)^c = \left(a^{cd}\right)^b = \left(a^k\right)^b = 1 \bmod n$.

Χρησιμοποιώντας το προηγούμενο θεώρημα έχουμε ότι $r \mid c$. (1)

Αφού $\mathrm{ord}_n(a) = k$ έχουμε $\left(a^{mr}\right) = \left(a^m\right)^r = 1 \bmod n$. Πάλι από το προηγούμενο θεώρημα έχουμε $k \mid mr$, δηλαδή $cd \mid (bd)r \Rightarrow c \mid br$.

Όμως, αφού $(c,b) = 1$ συνεπάγεται ότι $c \mid r$. (2)

Από τις σχέσεις (1) και (2) έχουμε $r = c$ οπότε $\mathrm{ord}_n\left(a^m\right) = r = c = \dfrac{k}{d} = \dfrac{k}{\mathrm{MK\Delta}(m,k)}$. ■

Παρατηρήσεις :

1. Το πρώτο θεώρημα μας λέει ότι η τάξη κάθε στοιχείου modulo έναν πρώτο αριθμό είναι διαιρέτης του $n-1$ διότι από το θεώρημα του Fermat έχουμε ότι για έναν

πρώτο αριθμό n ισχύει $a^{n-1}=1 \bmod n$. Οπότε αν $\text{ord}_n(a)=k$ τότε $k \mid n-1$. Το δεύτερο θεώρημα μας λέει επιπλέον ότι αν d διαιρέτης του $n-1$ τότε υπάρχουν $\varphi(d)$ μη ισοδύναμοι ακέραιοι $\bmod p$ που έχουν τάξη d.

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

Παράδειγμα :

Για $n=17$, ο 8 είναι διαιρέτης του $n-1=16$. Επιλέγω $a=3$ με $(3,17)=1$ και υπολογίζω το $\text{ord}_{17}(3)$. Βρίσκουμε τις δυνάμεις του 3:

$3,\ 9,\ 10,\ 13,\ 5,\ 15,\ 11,\ 16,\ 14,\ 8,\ 7,\ 4,\ 12,\ 2,\ 6,\ 1=3^{16}$ και βλέπουμε ότι $3^{16}=1$. Άρα $\text{ord}_{17}(3)=16$.

Βρίσκουμε στη συνέχεια τα $\varphi(8)=4$ στοιχεία του $\mathbb{Z}_{17}^*$ τάξης 8 :

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

Πράγματι, $\text{ord}_{17}(9)=\text{ord}_{17}(15)=\text{ord}_{17}(8)=\text{ord}_{17}(2)=8$ και $3^8=16$.

Ορισμός :

Ονομάζουμε έναν φυσικό q πρωταρχική (ή αρχική) ρίζα αν $\text{ord}_n(q)=\varphi(n)$.

Το 1769 ο J. Lambert μελετώντας τα δεκαδικά αναπτύγματα του $\frac{1}{p}$ (p πρώτος) ισχυρίστηκε ότι υπάρχουν πρωταρχικές ρίζες του p για κάθε πρώτο p.

Ο Euler εισήγαγε τον όρο πρωταρχική ρίζα το 1773 και έδειξε ότι υπάρχουν $\varphi(p-1)$ το πλήθος πρωταρχικές ρίζες για τον πρώτο p.

Ο Gauss έδειξε ότι αν ο πρώτος p έχει το 10 σαν πρωταρχική ρίζα τότε το δεκαδικό ανάπτυγμα του $\frac{1}{p}$ έχει περίοδο $p-1$. **Έδειξε επίσης ότι υπάρχουν πρωταρχικές ρίζες** $\bmod n$ **για** $n=2,4,p,p^k,2p^k$ **όπου** p **μονός πρώτος και** k **φυσικός .** Έδειξε ακόμα ότι αν q πρωταρχική ρίζα του μονού πρώτου p τότε οι αριθμοί q^p-p, q^p-qp, και τουλάχιστον ένας από τους q και $q+p$ είναι πρωταρχικές ρίζες του p^2. Επίσης αν το r είναι πρωταρχική ρίζα του p^2 τότε το r είναι πρωταρχική ρίζα του p^k για $k\geq 2$. Τέλος έχουμε ότι αν το s είναι πρωταρχική ρίζα του p^k και s μονός τότε ο s είναι πρωταρχική ρίζα του $2p^k$, ενώ αν s ζυγός τότε ο $s+p^k$ είναι πρωταρχική ρίζα του $2p^k$.

Η εύρεση όμως πρωταρχικών ριζών ακόμα και για τους πρώτους είναι δύσκολο να γίνει. Για μικρούς πρώτους υπάρχει μια μέθοδος, η μέθοδος του A. L. Crelle που έχει αποτελέσματα. Χρησιμοποιεί την εξής ιδιότητα :

Αν για $1\leq a\leq p-1$

- το s_i είναι το ελάχιστο υπόλοιπο του $a\cdot i \bmod p$ και
- το t_j είναι το ελάχιστο υπόλοιπο του $a^j \bmod p$ $(1\leq i<j\leq p-1)$

τότε $t_k=s_{t_{k-1}} \bmod p$ για $1\leq k\leq p-1$.

Ο αλγόριθμος του Crelle δουλεύει διότι είναι $a^{j-1}\cdot a=a^j \bmod p$ $(1\leq a\leq p-1)$.

<u>Παράδειγμα 1 :</u>

Έστω $p=17$ και $a=3$. Στον παρακάτω πίνακα για $0\leq k\leq 16$ βρίσκουμε τα πολλαπλάσια του 3 και τις δυνάμεις του 3.

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

Ο αλγόριθμος λειτουργεί ως εξής :

Τα πολλαπλάσια του 3 μας δίνουν τις δυνάμεις του 3. Με τη βοήθεια για παράδειγμα του $3^2=9$ θα υπολογίσουμε το 3^3. Αφού $3^2=9$ πηγαίνω στη στήλη 9 και βρίσκω το $3\cdot 9=27=10\bmod 17$ στη δεύτερη γραμμή. Άρα $3^3=3\cdot 9=10\bmod 17$, $3^4=3\cdot 10=13\bmod 17$, $3^5=3\cdot 13=5\bmod 17$ κ.ο.κ.

Βλέπουμε λοιπόν ότι η μικρότερη τιμή του k , $1\le k\le 16$, που δίνει $3^k=1\bmod 17$ είναι η $k=16$ άρα $\text{ord}_{17}(3)=16$. Επίσης είναι $\varphi(17)=16$ διότι ο 17 είναι πρώτος. Αφού ισχύει ότι $\text{ord}_{17}(3)=\varphi(17)=16$ συμπεραίνουμε ότι ο 3 είναι πρωταρχική ρίζα του 17 .

Παράδειγμα 2 :

Στο παράδειγμα αυτό θέλουμε να δούμε αν ο 5 είναι πρωταρχική ρίζα του 29. Για $0\le k\le 29$ βρίσκουμε τα πολλαπλάσια του 5 και τις δυνάμεις του 5.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$5k$	0	5	10	15	20	25	1	6	11	16	21	26	2	7	12
5^k	1	5	25	9	16	22	23	28	24	4	20	13	7	6	1

k	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$5k$	17	22	27	3	8	13	18	23	28	4	9	14	19	24
5^k														

Είναι $5^2=25$. Πηγαίνω στη στήλη 25 και βρίσκω στη δεύτερη γραμμή το $5\cdot 25=9$. Άρα $5^3=5\cdot 25=9\bmod 29$. Συνεχίζω το ίδιο για να βρω και τις υπόλοιπες δυνάμεις του 5: $5^4=5\cdot 9=16\bmod 29$, $5^5=5\cdot 16=22\bmod 29$, $5^6=5\cdot 22=23\bmod 29$ κ.ο.κ. Παρατηρούμε ότι $5^{14}=1\bmod 29$. Δηλαδή υπάρχει $1\le k\le 29$ για το οποίο ισχύει

$5^k = 1 \bmod 29$ άρα ο 5 δεν είναι πρωταρχική ρίζα του 29 (και είναι περιττό να βρούμε τις υπόλοιπες δυνάμεις του 5 για $k > 14$).

Το επόμενο θεώρημα μας περιγράφει ποιο είναι το πλήθος των πρωταρχικών ριζών του μονού πρώτου p.

Θεώρημα :

Αν p μονός πρώτος τότε υπάρχουν $\varphi(p-1)$ πρωταρχικές ρίζες $\bmod p$.

Απόδειξη :

Βιβλίο "Κρυπτογραφία", Χ.Κουκουβίνος, Α.Παπαιωάννου

Σελίδα 128. ■

Έχουμε λοιπόν πως αν q πρωταρχική ρίζα του p, υπάρχουν τότε $\varphi(p-1)$ μη ισοδύναμες πρωταρχικές ρίζες του p που δίνονται από τη σχέση : $q^{a_1}, q^{a_2}, ..., q^{a_{\varphi(p-1)}}$ όπου οι $\varphi(p-1)$ φυσικοί μικρότεροι του $p-1$ είναι πρώτοι προς τον $p-1$.

Παράδειγμα :

Βρίσκουμε τις πρωταρχικές ρίζες του 17. Είναι $\varphi(16) = 16 \cdot \frac{1}{2} = 8$. Στο παράδειγμα 1 είδαμε ότι το 3 είναι πρωταρχική ρίζα του 17. Οι 8 ακέραιοι μικρότεροι του 16 και πρώτοι προς τον 16 είναι οι 1, 3, 5, 7, 9, 11, 13, 15 οπότε οι 8 πρώταρχικές ρίζες του 17 είναι :

$3^1 = 3,\ 3^3 = 10,\ 3^5 = 5,\ 3^7 = 11,\ 3^9 = 14,\ 3^{11} = 7,\ 3^{13} = 12,\ 3^{15} = 6 \bmod 17$ όπου είναι $(3,16) = 1$, $(5,16) = 1$ κ.ο.κ.

Παρακάτω βλέπουμε μια γενίκευση του προηγούμενου θεωρήματος .

Θεώρημα :

Αν υπάρχει πρωταρχική ρίζα για τον (μη πρώτο) m θα έχουμε $\varphi\left(\varphi\left(m\right)\right)$ μη ισοδύναμες πρωταρχικές ρίζες του m .

Υπενθύμιση : αν $m=p$ πρώτος τότε $\varphi\left(\varphi\left(p\right)\right)=\varphi\left(p-1\right)$. ■

3. Τέστ πιστοποίησης πρώτων αριθμών

Τα τεστ πιστοποίησης πρώτων αριθμών είναι αλγόριθμοι που μπορούν να αποφανθούν για το εάν ένας αριθμός είναι πρώτος ή όχι. Σε σύγκριση με την παραγοντοποίηση ακεραίων, που είναι ο προσδιορισμός πρώτων παραγόντων ενός δεδομένου φυσικού αριθμού, η πιστοποίηση πρώτων αποδεικνύεται να είναι ευκολότερη.

Το πρόβλημα διαπίστωσης εάν ένας αριθμός είναι πρώτος ή όχι, ονομάζεται διεθνώς *"PRIMES"* και με τη σχετικά πρόσφατη δημοσίευση του αλγορίθμου *AKS* (Agrawal-Kayal-Saxena primality test) το 2002, αποδείχθηκε ότι το πρόβλημα *"PRIMES"* ανήκει στην κλάση *P*, από άποψη υπολογιστικής πολυπλοκότητας.

Γενικά τα τεστ πιστοποίησης πρώτων χωρίζονται σε δύο κατηγορίες, τα ντετερμινιστικά και τα πιθανοτικά με τα περισσότερα από αυτά που χρησιμοποιούνται στην πράξη να είναι πιθανοτικά. Στο συγκεκριμένο κείμενο θα ασχοληθούμε μόνο με πιθανοτικά τεστ και συγκεκριμένα με τις τρείς δημοφιλέστερες μεθόδους πιστοποίησης πρώτων που είναι τα τεστ των Fermat, Solovay-Strassen και τέλος των Miller-Rabin.

3.1. Το τέστ του Fermat

Από το μικρό θεώρημα του Fermat έχουμε ότι αν ο p πρώτος και $1 \le a < p$ τότε $a^{p-1} \equiv 1 \bmod p$. Το θεώρημα αυτό μας δίνει ένα αρνητικό κριτήριο για την πιστοποίηση πρώτων. Δηλαδή αν θέλουμε να εξετάσουμε εάν ένας δοσμένος ακέραιος p είναι πρώτος και βρούμε κάποιο a για το οποίο δεν ισχύει το μικρό θεώρημα του Fermat τότε συμπεραίνουμε ότι ο p είναι σύνθετος. Η παραπάνω διαδικασία αποτελεί ουσιαστικά το τεστ του Fermat, το οποίο αναλύουμε περαιτέρω παρακάτω.

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. Όμως, δυστυχώς, η ύπαρξη του F-μάρτυρα δεν δίνει πληροφορία για το πιο σύνθετο πρόβλημα της παραγοντοποίησης του n.

Ορισμός:

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

Το «αντίστροφο» του θεωρήματος του Fermat δεν ισχύει, μπορούμε όμως να αντλήσουμε κάποιες πληροφορίες από αυτό όπως βλέπουμε στο παρακάτω Λήμμα.

Λήμμα :

α) Αν ο αριθμός a, $1 \le a \le n$ ικανοποιεί την $a^r \bmod n = 1$ (για $r \ge 1$) τότε $a \in \mathbb{Z}_n^*$.
β) Αν ισχύει $a^{n-1} \bmod n = 1$ για κάθε a με $1 \le a \le n$ τότε ο n είναι πρώτος.

Απόδειξη :

α) Ισχύει ότι $a^r \bmod n = 1$ για κάποιο $r \geq 1$. Άρα αυτό συνεπάγεται ότι $a \cdot a^{r-1} \bmod n = 1$, δηλαδή $a \in \mathbb{Z}_n^*$.

β) Έστω $a^{n-1} \bmod n = 1 \ \ \forall a \in [1, n]$ άρα από το (α) του λήμματος θα είναι $\mathbb{Z}_n^* = \{1, \ldots, n-1\}$ άρα ο n είναι πρώτος. ■

Παρατηρούμε ότι το σημαντικό κομμάτι του λήμματος είναι το (β) μέρος το οποίο μας λέει ότι υπάρχει πάντα ένας F-μάρτυρας για τον σύνθετο μονό n.

Τα παραπάνω μας οδηγούν σε μια πρώτη προσπάθεια πιθανοτικής πιστοποίησης πρώτου.

Αλγόριθμος (Fermat Test)

Input : Μονός φυσικός $n \geq 3$

Method :

1. Επιλέγω τυχαία $a \in \{2, \ldots, n-2\}$
    2. αν $a^{n-1} \bmod n \neq 1$
        3. Τότε επιστροφή 1
    4. Αλλιώς επιστροφή 0.

Για τη χρονική διάρκεια του αλγορίθμου αυτού έχουμε $O(\log n)$ αριθμητικές πράξεις για τη γρήγορη εκθετοποίηση και $O\left((\log n)^3\right)$ πράξεις bit.

Παράδειγμα :

Έχουμε ότι $91 = 13 \cdot 7$ και το κριτήριο του Fermat για $a = 2$ μας δίνει

$$2^{90} \equiv 64 (\bmod 91)$$

και επομένως αποδεικνύει ότι ο 91 είναι σύνθετος. Παρατηρούμε ότι για $a=3$ έχουμε

$$3^{90} \equiv 1 (\mathrm{mod} 91)$$

άρα δεν μπορούμε να αποφανθούμε αν ο 91 είναι πρώτος ή όχι.

Παρατηρήσεις :

1. Άν ο παραπάνω αλγόριθμος μας επιστρέψει 1 τότε μπορούμε να πούμε ότι ο n είναι σίγουρα σύνθετος, δηλαδή ο αλγόριθμος έχει βρει έναν F-μάρτυρα για τον n . Διαφορετικά, αν επιστρέψει 0 τότε δεν μπορούμε να πούμε με βεβαιότητα ότι ο n είναι πρώτος.

2. Για πολλούς σύνθετους n υπάρχει αφθονία F-μαρτύρων οπότε το απλό αυτό κριτήριο πετυχαίνει με σταθερή πιθανότητα.

Θεώρημα :

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

Απόδειξη :

Το σύνολο $L_n^F = \{a \mid 1 \leq a \leq n \text{ με } a^{n-1} \bmod n = 1\}$ των F-ψευτών για το n είναι προφανώς υποσύνολο του συνόλου $\mathbb{Z}_n^*$. Θα δείξουμε ότι είναι και υποομάδα της $\mathbb{Z}_n^*$. Αφού η $\mathbb{Z}_n^*$ είναι πεπερασμένη ομάδα (με $\left|\mathbb{Z}_n^*\right| = \varphi(n)$) 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 ομάδας $\mathbb{Z}_n^*$) διότι $a^{n-1} \bmod n = 1$ και $b^{n-1} mod n = 1$ συνεπάγεται $(ab)^{n-1} = a^{n-1}b^{n-1} = 1 \cdot 1 = 1 \bmod n$.

Αφού το $\mathbb{Z}_n^*$ απο το προηγούμενο Λήμμα έχει ένα τουλάχιστον στοιχείο, το L_n^F είναι γνήσια υποομάδα του $\mathbb{Z}_n^*$. Από το θεώρημα του Lagrange λοιπόν η τάξη του θα είναι γνήσιος διαιρέτης του $\varphi(n)$, όπου $\varphi(n) < n-1$ (διότι ο n είναι σύνθετος), άρα $\left|L_n^F\right| \le \frac{n-2}{2}$. Άρα η πιθανότητα μία επιλογή από το σύνολο $\{2,...,n-2\}$ να ανήκει στο $L_n^F - \{1, n-1\}$ είναι το πολύ $\frac{\frac{n-2}{2}-2}{n-3} = \frac{n-6}{2(n-3)} < \frac{1}{2}$. ■

Παρατήρηση:

Είναι εύκολο να παρατηρήσουμε ότι ένας αλγόριθμος που δίνει πιθανότητα λάθους μικρότερη του $\frac{1}{2}$ δεν μπορεί να είναι έμπιστος. Γι αυτό το λόγο, επαναλήψεις του τεστ του Fermat θα μας δώσουν καλύτερα αποτελέσματα.

Αλγόριθμος (Iterated Fermat Test)

Input : Μονός ακέραιος $n \ge 3$, φυσικός $l \ge 1$

Method :

1. Επαναλαμβάνω l φορές
   2. επιλέγω τυχαία $a \in \{2,...,n-2\}$
      3. αν $a^{n-1} \bmod n \ne 1$ επιστροφή 1
   4. επιστροφή 0

Παρατηρήσεις :

1. Άν ο αλγόριθμος μας επιστρέψει 1 τότε έχει βρει έναν F-μάρτυρα, άρα ο n είναι σύνθετος.

2. Άν 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 απο l δοκιμές γίνεται μικρότερη από $\left(\frac{1}{2}\right)^l$. Άρα για μεγάλα l η πιθανότητα λάθους γίνεται όσο μικρή θέλουμε.

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

Ορισμός:

Ένας μονός σύνθετος αριθμός n ονομάζεται *αριθμός Carmichael* αν $a^{n-1} \bmod n = 1 \ \ \forall a \in \mathbb{Z}_n^*$.

Παράδειγμα :

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

Θεώρημα :

Άν ο n είναι αριθμός Carmichael, τότε ο n είναι γινόμενο τουλάχιστον τριών (διαφορετικών) πρώτων παραγόντων.

Απόδειξη :

Έστω ότι ο n δεν είναι γινόμενο όπως στην υπόθεση. Θα βρούμε έναν F-μάρτυρα $a \in \mathbb{Z}_n^*$. Έχουμε δύο περιπτώσεις :

Περίπτωση 1 : *Έστω* $p^2 \mid n$ *για κάποιο πρώτο* $p \geq 3$.

Γράφουμε $n = p^k \cdot m$ με $k \geq 2$ και $p \nmid m$. Αν $m = 1$ τότε $a = 1 \nmid p$. Αν $m \geq 3$ τότε από ΚΘΥ επιλέγω τον a ώστε να ισχύουν :

$1 \leq a \leq p^2 \cdot m \leq n$ με $a = 1 + p \bmod p^2$ (1)

και $a = 1 \bmod m$ (2).

Θα δείξω ότι ο a *είναι F-μάρτυρας στο* $\mathbb{Z}_n^*$ *:*

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

$$a - (1 + p) = \lambda p^2 \Rightarrow a \neq \mu p$$

Αλλά $n = p^k \cdot m$ άρα $(a, n) = 1$.

Έστω λοιπόν ότι ο $a \in \mathbb{Z}_n^*$ δεν είναι F-μάρτυρας για τον n, ήτοι $a^{n-1} \bmod n = 1$.

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

(Πράγματι : $a^{n-1} - 1 = k \cdot n$ και $n = sp^2 \Rightarrow a^{n-1} - 1 = ks \cdot p^2 \Rightarrow a^{n-1} = a \bmod p^2$).

Από το διωνυμικό θεώρημα έχουμε

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

Άρα $a^{n-1} = 1 \bmod p^2$ και

$a^{n-1} = 1 + (n-1)\, p \bmod p^2$

που δίνουν $(n-1)\, p = 0 \bmod p^2 \Rightarrow p^2 \mid p(n-1)$ το οποίο είναι άτοπο διότι

$p \nmid n - 1 = p^k m - 1$.

Περίπτωση 2 : $n = p \cdot q$ *για διακεκριμένους πρώτους* p, q *και έστω* $p > q$.

Θα κατασκευάσουμε πάλι έναν F-μάρτυρα $a \in \mathbb{Z}_n^*$. Η ομάδα $\mathbb{Z}_p^*$ είναι κυκλική, ήτοι έχει έναν γεννήτορα g. Από το ΚΘΥ και πάλι επιλέγουμε τον $a,\ 1 \le a < n$ με

$$\begin{aligned} a &= g \bmod p \\ a &= 1 \bmod q \end{aligned} \quad \text{και}$$

Προφανώς λοιπόν $a \neq kp,\ a \neq \lambda q$ άρα $a \in \mathbb{Z}_n^*$. 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, $a^{n-1} = kn \Rightarrow a^{n-1} - 1 = klp$ ήτοι $a^{n-1} = 1 \bmod p$). Όμως ο γεννήτορας g της κυκλικής ομάδας $\mathbb{Z}_p^*$ θα έχει 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 $p-1 \le q-1 \Rightarrow p \le q$ άτοπο διότι υποθέσαμε αρχικά ότι $p > q$. ■

<u>Θεώρημα (Κριτήριο του Korselt) :</u>

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

<u>Απόδειξη:</u>

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

Σελίδα 101 . ■

Κατασκευή (J.Chernick 1939) :

Άν t ακέραιος τέτοιος ώστε οι αριθμοί $6t+1,\ 12t+1$ και $18t+1$ να είναι πρώτοι, τότε ο ακέραιος $n = (6t+1)(12t+1)(18t+1)$ από το προηγούμενο θεώρημα είναι αριθμός Carmichael. Παράδειγμα, για $t = 1$ έχουμε τον αριθμό $1729 = 7 \cdot 13 \cdot 19$ που είναι αριθμός Carmichael. ■

Υπάρχουν πολλά αποτελέσματα για τους αριθμούς Carmichael , μεταξύ των οποίων και το ότι είναι άπειροι και μάλιστα «ομοιόμορφα» κατανεμημένοι, πράγμα το οποίο απεδείχθη το 1994 (Alford-Granville-Pomerance). Ο μικρότερος αριθμός Carmichael είναι ο $561 = 3 \cdot 11 \cdot 17$. Οι αριθμοί Carmichael είναι σημαντικοί διότι περνάνε το τεστ του Fermat αλλά δεν είναι πρώτοι. Η ύπαρξη αυτών των αριθμών μειώνει την αξιοπιστία αυτού του τεστ και για το λόγο αυτό έχουν δημιουργηθεί άλλα πιθανοτικά τεστ πιστοποίησης πρώτου που αποφεύγουν αυτό το πρόβλημα.

3.2. Το τεστ των Solovay-Strassen

Το τεστ πιστοποίησης πρώτων των Solovay-Strassen είναι ένα πιθανοτικό τεστ για να προσδιορίζουμε εάν ένας αριθμός είναι σύνθετος ή πιθανόν πρώτος. Ήταν το πρώτο πιθανοτικό τεστ πιστοποίησης πρώτου που χρησιμοποιήθηκε στην κρυπτογραφία δημόσιου κλειδιού και συγκεκριμένα στο κρυπτοσύστημα RSA. Άν και έχουν υπερισχύσει αυτού άλλα πιθανοτικά τεστ, όπως το τεστ των Miller-Rabin που θα μελετήσουμε παρακάτω, το παραθέτουμε εδώ καθώς έχει πολύ μεγάλη ιστορική σημασία δείχνοντας την πρακτική σκοπιμότητα του κρυπτογραφικού συστήματος RSA.

Το τεστ των Solovay-Strassen στηρίζεται στο κριτήριο του Euler, σύμφωνα με το οποίο όπως έχουμε δει, ισχύει το εξής :

Άν p μονός πρώτος και $(a,p)=1$ τότε $\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}} \bmod p$, όπου $\left(\frac{a}{p}\right)$ το σύμβολο του Jacobi.

Ορισμός :

Έστω n ένας περιττός σύνθετος αριθμός . Ένας ακέραιος a με $1\le a\le n$ λέγεται *Euler-μάρτυρας* του n αν $a^{\frac{n-1}{2}}\cdot\left(\frac{a}{n}\right)\neq 1$. Διαφορετικά καλείται *Euler-ψεύτης* .

Παράδειγμα :

Έστω ο σύνθετος $n=325=13\cdot 5^2$.

Για $a=2$ έχουμε ότι $(15,325)=5$ και $\left(\frac{15}{325}\right)$ άρα ο 15 είναι ένας Ε-μάρτυρας του 325.

Για $a=7$ έχουμε $7^{\frac{325-1}{2}} \bmod 325 = 7^{162} \bmod 325 = -1 \bmod 325$ και

$\left(\frac{7}{325}\right)=\left(\frac{7}{5^2\cdot 13}\right)=\left(\frac{7}{5}\right)^2\cdot\left(\frac{7}{13}\right)=\left(\frac{7}{13}\right)=-1$ διότι $7\notin QR \bmod 13$. Άρα ο 7 είναι E-ψεύτης για τον 325.

Αλγόριθμος (Τεστ των Solovay-Strassen)

Input : Μονός ακέραιος $n\geq 3$

Method :

1. Έστω a τυχαία επιλογή από το $\{2,...,n-2\}$
2. Αν $a^{\frac{n-1}{2}}\cdot\left(\frac{a}{n}\right)\bmod n\neq 1$
3. τότε επέστρεψε 1
4. αλλιώς επέστρεψε 0.

Όπου, στη γραμμή 2, ο υπολογισμός του συμβόλου Jacobi $\left(\frac{a}{n}\right)$ γίνεται από τον αλγόριθμο και η εκθετοποίηση $a^{\frac{n-1}{2}} \bmod n$ γίνεται με fast exponentiation. Η πολυπλοκότητα του αλγόριθμου είναι $O\left((\log n)^3\right)$. Τέλος παρατηρούμε ότι αν το n είναι πρώτος έχουμε έξοδο 0 ενώ,διαφορετικά, αν ο n είναι σύνθετος η πιθανότητα να πάρω στην έξοδο 0 είναι μικρότερη της $1/2$.

Λήμμα :

Έστω ο μονός σύνθετος $n\geq 3$. Τότε κάθε E-ψεύτης του n είναι επίσης και F-ψεύτης του n.

Απόδειξη :

Άν ο a είναι E-ψεύτης τότε $1 = a^{\frac{n-1}{2}} \cdot \left(\frac{a}{n}\right) \bmod n$ αλλά $\left(\frac{a}{n}\right) = +1$ ή $\left(\frac{a}{n}\right) = -1$, οπότε τετραγωνίζοντας έχουμε $1 = \left[a^{\frac{n-1}{2}} \cdot \left(\frac{a}{n}\right) \right]^2 \bmod n = a^{n-1} \bmod n$. Άρα ο a είναι και F-ψεύτης. ■

Στο παρακάτω Λήμμα θα δείξουμε ότι το $\mathbb{Z}_n^*$ περιέχει πάντα έναν E-μάρτυρα (για n μονό σύνθετο ≥ 3) και οι E-ψεύτες είναι τα μισά στοιχεία του $\mathbb{Z}_n^*$.

Λήμμα :

Έστω $n \geq 3$ ένας μονός σύνθετος. Τότε το σύνολο $L_n^E = \{a \mid a \text{ είναι E-ψεύτης του } n\}$ είναι γνήσια υποομάδα του $\mathbb{Z}_n^*$.

Απόδειξη :

Όπως έχουμε ήδη δει στην παράγραφο με το τεστ του Fermat, το σύνολο των F-ψευτών του n είναι υποσύνολο του $\mathbb{Z}_n^*$. Από το προηγούμενο Λήμμα συμπεραίνουμε ότι και το σύνολο των E-ψευτών είναι υποσύνολο του $\mathbb{Z}_n^*$. Θα δείξουμε ότι το σύνολο των E-ψευτών είναι υποομάδα του $\mathbb{Z}_n^*$ και, τέλος, θα δείξουμε ότι το $\mathbb{Z}_n^*$ περιέχει τουλάχιστον έναν E-μάρτυρα.

Ισχύει ότι ένα υποσύνολο της ομάδας $\mathbb{Z}_n^*$ είναι υποομάδα αν :

i. το 1 ανήκει στο υποσύνολο,
ii. το υποσύνολο είναι κλειστό ως προς την πράξη της υποομάδας.

Τα αποδεικνύουμε :

i. Το 1 είναι προφανώς E-ψεύτης άρα $1 \in L_n^E$.

ii. Υποθέτουμε ότι $a,b\in\mathbb{Z}_n^*$ είναι E-ψεύτες για τον n. Τότε

$$(a\cdot b)^{\frac{(n-1)}{2}}\cdot\left(\frac{a\cdot b}{n}\right)\bmod n=a^{\frac{n-1}{2}}\cdot\left(\frac{a}{n}\right)\bmod n\cdot b^{\frac{n-1}{2}}\cdot\left(\frac{b}{n}\right)\bmod n=1\cdot 1=1,$$

λόγω της πολλαπλασιαστικότητας του συμβόλου Jacobi.

Άρα, η $\mathbb{Z}_n^E$ είναι υποομάδα.

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

Περίπτωση 1 : $p^2\mid n$ *για κάποιο πρώτο* $p\geq 3$.

Από το Θεώρημα για τους αριθμούς Carmichael είδαμε πώς κατασκευάζουμε έναν F-μάρτυρα στο $\mathbb{Z}_n^*$ ο οποίος από το προηγούμενο Λήμμα θα είναι και E-μάρτυρας.

Περίπτωση 2 : *Έστω ότι ο* n *είναι γινόμενο κάποιων διαφορετικών πρώτων.*

Τότε θέτουμε $n=p\cdot m$ όπου p μονός πρώτος και $m\geq 3$ μονός με $p\nmid m$. Έστω $b\in\mathbb{Z}_p^*$ κάποιο μη τετραγωνικό υπόλοιπο $\bmod p$, δηλαδή $\left(\frac{b}{p}\right)=-1$. Από το ΚΘΥ υπάρχει $1\leq a<n$ με

$$a=b\bmod p \qquad (1)$$

$$a=1\bmod m \qquad (2)$$

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

Απόδειξη ισχυρισμού : $p\nmid a$ ήτοι $a\neq \text{πολ}p$, διότι από τη σχέση (1) είναι $a-b=\text{πολ}p$ και αν ίσχυε $a=\text{πολ}p$ τότε θα είχα $b=0$ ή $b=\text{πολ}p$, όμως ισχύει $\left(\frac{b}{p}\right)=-1$. Επίσης από τη σχέση (2) έχουμε ότι $(a,m)=1$, διότι $a-1=\text{πολ}m$ άρα $a\in\mathbb{Z}_n^*$. Ακόμα ισχύει :

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

Αν ο a ήταν E-ψεύτης θα είχα $a^{\frac{n-1}{2}}=-1\bmod n$ αφού $\left(\frac{a}{n}\right)=-1$. Αλλά $n=\text{πολ}m$ και θα

είχα $a^{\frac{n-1}{2}} = -1 \bmod m$, που έρχεται σε αντίθεση με το ότι $a \equiv 1 \bmod m$ (σχέση (2)). Άρα ο a είναι Ε-μάρτυρας για το n. ■

Από το Λήμμα έχω ότι το πλήθος των Ε-ψευτών του n είναι γνήσιος διαιρέτης του $\left|\mathbb{Z}_n^*\right| = \varphi(n)$, άρα τουλάχιστον τα μισά στοιχεία του $\mathbb{Z}_n^*$ είναι Ε-μάρτυρες.

3.3. Μη τετριμμένες τετραγωνικές ρίζες της μονάδας και το Κριτήριο Miller-Rabin

Ορισμός :

Έστω $1 \le a < n$. Ο a ονομάζεται τετραγωνική ρίζα της μονάδας $\bmod n$ αν $a^2 \bmod n = 1$.

Παρατηρούμε ότι ο 1 και ο $n-1$ είναι πάντα τετραγωνικές ρίζες της μονάδας διότι $1^2 \bmod n = 1$ και $(n-1)^2 = (-1)^2 = 1 \bmod n$. Αυτές είναι οι τετριμμένες τετραγωνικές ρίζες της μονάδας . Αν ο n είναι πρώτος δεν υπάρχουν άλλες τετραγωνικές ρίζες της μονάδας $\bmod n$. Αυτό μας λέει και το παρακάτω Λήμμα .

Λήμμα :

Αν p πρώτος και $1 \le a < p$ με $a^2 \bmod p = 1$ 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 πρώτος τότε ισχύει ότι :

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

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

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

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

Πρόταση :

Έστω ο πρώτος $p = 3 \bmod 4$ 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 δεν έχει τετραγωνικές ρίζες $\bmod p$ τότε ο $-y$ έχει και οι τετραγωνικές ρίζες του $-y \bmod p$ είναι $\pm x$.

Απόδειξη :

Υποθέτουμε ότι $y \neq 0$, 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 $\left(x^2 + y\right)\left(x^2 - y\right) = 0 \bmod p$ άρα $x^2 = \pm y \bmod p$. Άρα είτε το y είτε το $-y$ είναι τετράγωνα $\bmod p$.

Έστω ότι τα y και $-y$ είναι τετράγωνα $\bmod p$ ήτοι $y = a^2$, $-y = b^2$. Τότε, αν διαιρέσουμε κατά μέλη έχουμε ότι $-1 = \left(\frac{a}{b}\right)^2 \bmod p$, που σημαίνει ότι το -1 είναι τετράγωνο $\bmod p$. Αυτό όμως είναι αδύνατο διότι $p = 3 \bmod 4$.

Πράγματι, αν $p = 3 \bmod 4$ η εξίσωση $x^2 = -1 \bmod p$ δεν έχει λύσεις διότι αν είχε, δηλαδή αν υπήρχε τέτοιο x, τότε θα ίσχυε $\left(x^2\right)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \bmod p \Rightarrow x^{p-1} = -1 \bmod p$, διότι από $p = 3 \bmod 4$, έχω ότι $p - 1 = 2 \bmod 4$, άρα ο $\frac{p-1}{2}$ είναι μονός οπότε $(-1)^{\frac{p-1}{2}} = -1$. Όμως από Fermat ισχύει ότι $x^{p-1} = 1 \bmod p$ για p μονό.

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

Παραδείγματα :

1) Τετραγωνικές ρίζες του $5 \bmod 11$, όπου $11 = 3 \bmod 4$.

Είναι $\frac{p+1}{4} = 3$ 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 είναι σύνθετος : $77 = 7 \cdot 11$).

Άρα λύνω

$x^2 = 71 = 1 \bmod 7$ $\qquad$ $x^2 = 71 = 5 \bmod 11$

$x = \pm 1 \bmod 7$ $\qquad$ $x = \pm 4 \bmod 11$ (προκύπτει από το προηγούμενο παράδειγμα)

Με το ΚΘΥ θα ενώσω τις δύο ισοδυναμίες :

Η $\left.\begin{array}{ll} x = 1 \bmod 7 & \{1, 8, \boxed{15}, 22, 29, 36, 43, 50, 57, 64, 71\} \\ x = 4 \bmod 11 & \{4, \boxed{15}, 26, 37, 48, 59, 70, 81\} \end{array}\right\} \Rightarrow x = 15 \bmod 77$.

Η $\left.\begin{array}{ll} x = -1 \bmod 7 \Rightarrow x = 6 \bmod 7 & \{6, 13, 20, 27, 34, 41, \boxed{48}, 55, 62, \ldots\} \\ x = 4 \bmod 11 & \{4, 15, 26, 37, \boxed{48}, 59, 70, 81\} \end{array}\right\} \Rightarrow$

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

Η $\left.\begin{array}{ll} x = 1 \bmod 7 & \{1, 8, 15, 22, \boxed{29}, 36, 43, 50, 57, 64, 71\} \\ x = -4 \bmod 11 \Rightarrow x = 7 \bmod 11 & \{7, 18, \boxed{29}, 40, 51, 62, \ldots\} \end{array}\right\} \Rightarrow x = 29 \bmod 77$.

Η $\left.\begin{array}{l} x = -1 \bmod 77 \\ x = -4 \bmod 77 \end{array}\right\} \Rightarrow \left.\begin{array}{l} x = 6 \bmod 7 \\ x = 7 \bmod 11 \end{array}\right\} \Rightarrow x = 62 \bmod 77 \Rightarrow x = -15 \bmod 77$.

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

Αν λοιπόν ο αριθμός n γράφεται στη μορφή $n = pq$ και η $x^2 = y \bmod n$ έχει τέσσερις τετραγωνικές ρίζες $x = \pm a$ και $x = \pm b$, τότε γνωρίζω ότι θα ισχύει :

$$\left.\begin{array}{l} a=b \bmod p \\ a=-b \bmod q \end{array}\right\} \quad \text{ή} \quad \left.\begin{array}{l} a=-b \bmod p \\ a=b \bmod q \end{array}\right\}$$

Το πρώτο σύστημα μας δίνει $p \mid a-b$ και $q \nmid a-b$.

Άρα $\text{ΜΚΔ}(a-b,n)=p$ από το Βασικό Κριτήριο, που βλεπουμε αμέσως παρακάτω, οπότε βρήκαμε έναν μη τετριμμένο παράγοντα του n.

Θεώρημα (Βασικό Κριτήριο Παραγοντοποίησης) :

Έστω ο φυσικός n και έστω ότι υπάρχουν φυσικοί x, y με $x^2 = y^2 \bmod n$ αλλά $x \neq \pm y \bmod n$. Τότε ο n είναι σύνθετος και ο $d = \text{ΜΚΔ}(x-y, n)$ δίνει μη τετριμμένο παράγοντα του n.

Απόδειξη :

Αν $d = n$ τότε $x = y \bmod n$ που δεν ισχύει εξ υποθέσεως.
Αν $d = 1$, επειδή ισχύει (από θεώρημα) ότι αν $a \mid bc$ και $(a,b)=1$ τότε συνεπάγεται ότι $a \mid c$, έχουμε ότι $n \mid x^2 - y^2 = (x-y)(x+y)$ και $d = 1$, δηλαδή,
$(n, x-y) = 1 \Rightarrow n \mid x+y \Rightarrow x = -y \bmod n$ που δεν ισχύει από την υπόθεσή μας. Άρα τελικά θα έχουμε ότι $d \neq 1, n$ και ο d είναι μη τετριμμένος παράγοντας του σύνθετου n.
■

Συνεχίζοντας λοιπόν τώρα το προηγούμενο παράδειγμα έχουμε ότι $15^2 = 29^2 = 71 \bmod 77$ άρα $(15-29, 77) = 7$ μας δίνει μη τετριμμένο παράγοντα του 77.

Παρατηρώντας τα παραπάνω συμπεραίνουμε το εξής :

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

$x = \pm a$ και $x = \pm b$ της $x^2 = y \bmod n$ είναι υπολογιστικά ισοδύναμη με την παραγοντοποίηση του n.

Άρα, εκτός κ αν ο n έχει πολλούς πρώτους παράγοντες, η τυχαία επιλογή του a δεν αποδίδει.

Η παραπάνω διαδικασία μας επιστρέφει στο τεστ του Fermat και μας οδηγεί τελικά σε ένα ισχυρότερο κριτήριο που ονομάζεται κριτήριο Miller-Rabin.

Αφού ο n είναι μονός πρώτος, ο ζυγός $n-1$ γράφεται $n-1 = u \cdot 2^k$ με $k \geq 1$ και u μονό. Άρα $a^{n-1} = \left(a^u \bmod n\right)^{2^k}$ 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 $b_k = a^{n-1} \bmod n$.

Η ακολουθία $b_0,...,b_k$ έχει τις εξής δυνατές μορφές :

Αν $b_i = 1$ ή $b_i = n-1$ τα υπόλοιπα στοιχεία $b_{i+1},...b_k$ είναι όλα 1. Άρα η ακολουθία αρχίζει εν γένει με 0 ή με $b_0 \notin \{1, n-1\}$ και τελειώνει με 0 ή 1. Τα δύο κομμάτια χωρίζονται (όχι υποχρεωτικά) από το $n-1$. Παρακάτω παραθέτουμε έναν πίνακα στον οποίο μπορούμε να δούμε τις δυνατές περιπτώσεις των δυνάμεων $a^{n-1} \bmod n$, όπου το σύμβολο * σημαίνει τυχόν στοιχείο $\notin \{1, n-1\}$.

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 1 : Δυνατές περιπτώσεις δυνάμεων $a^{n-1} \bmod n$.

Αναλύουμε λοιπόν τις περιπτώσεις του παραπάνω πίνακα :

Περίπτωση 1α : $b_0 = 1$

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

Και στις δύο υποπεριπτώσεις $b_k = 1$ άρα δεν πήραμε πληροφορία αν ο n είναι πρώτος ή όχι.

Περίπτωση 2 : Και στις δύο υποπεριπτώσεις $b_k \neq 1$. Άρα ο n είναι σύνθετος και ο a 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 $\bmod n$. Άρα πάλι ο n σύνθετος.

Ορισμός :

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

Λήμμα :

Αν ο a είναι A-μάρτυρας του n, τότε ο n είναι σύνθετος.

Απόδειξη :

Αν ο a είναι A-μάρτυρας του n τότε ισχύουν οι περιπτώσεις 2 ή 3 που είδαμε παραπάνω άρα ο n είναι σύνθετος. ■

Αυτό λοιπόν το Λήμμα και η τυχαία επιλογή του a από το σύνολο $\{2, \ldots, n-2\}$ είναι τα στοιχεία που ενισχύουν το τεστ του Fermat σε ένα ισχυρότερο κριτήριο, το κριτήριο Miller-Rabin.

Αλγόριθμος (Κριτήριο Miller-Rabin)

Input : Μονός φυσικός $n \geq 3$

Method :

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 $b = 1$ επιστροφή 1
9. επιστροφή 1.

Ανάλυση του κριτηρίου :

Έστω $n > 1$ ένας μονός φυσικός. Θέτουμε $n-1 = u \cdot 2^k$ με u μονό και $k \geq 1$. Επιλέγουμε τυχαίο ακέραιο a, $1 < a < n-1$. Υπολογίζω τον $b_o = a^u \bmod n$. Αν $b_o = \pm 1$ 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 είναι σύνθετος ενώ αν $b_2 = -1 \bmod n$ σταματάμε και τότε ο n είναι πιθανά πρώτος. Συνεχίζουμε μέχρι είτε να σταματήσουμε είτε να φτάσουμε στο b_{k-1}. Αν $b_{k-1} \neq -1 \bmod n$ τότε ο n είναι σύνθετος.

<u>Παράδειγμα :</u>

Έστω ότι έχουμε το μονό φυσικό $n = 561$. Είναι $n-1 = 16 \cdot 35 = 2^4 \cdot 35$. Άρα $k = 4$ και $m = 35$.

Έστω $a = 2$.
Τότε εφαρμόζοντας το κριτήριο Miller-Rabin έχουμε :

$$b_0 = 2^{35} = 263 \bmod 561$$
$$b_1 = 263^2 = 166 \bmod 561$$
$$b_2 = 166^2 = 67 \bmod 561$$
$$b_3 = 67^2 = 1 \bmod 561$$

Αφού $b_3 \neq -1 \bmod n$ ο 561 είναι σύνθετος με $d = \text{ΜΚΔ}(67-1, 561) = 33$ μη τετριμμένο παράγοντα του 561.

4. Παραγοντοποίηση ακεραίων

Στη θεωρία αριθμών η παραγοντοποίηση ακεραίων είναι η διάσπαση ενός σύνθετου αριθμού σε μικρότερους μη τετριμμένους διαιρέτες, οι οποίοι πολλαπλασιαζόμενοι μεταξύ τους δίνουν τον αρχικό ακέραιο.

Η εύρεση των πρώτων παραγόντων ενός ακεραίου είναι δύσκολο πρόβλημα από υπολογιστικής άποψης και αυτή ακριβώς η δυσκολία του προβλήματος είναι που ενέπνευσε τη δημιουργία αλγορίθμων στην κρυπτογραφία όπως είναι το κρυπτοσύστημα RSA.

Δεν έχουν όμως όλοι οι αριθμοί την ίδια δυσκολία ως προς την παραγοντοποίηση. Οι δυσκολότερες περιπτώσεις τέτοιων προβλημάτων, με τις μέχρι σήμερα γνωστές τεχνικές, είναι οι αριθμοί που αποτελούνται από το γινόμενο δύο μεγάλων πρώτων, παρόμοιου μεγέθους και είναι μάλιστα αυτοί που χρησιμοποιούνται σε εφαρμογές της κρυπτογραφίας. Δεν υπάρχουν γνωστοί αλγόριθμοι παραγοντοποίησης για αυτές τις περιπτώσεις. Μια προσπάθεια παραγοντοποίησης τέτοιων αριθμών έγινε το 2009 από διάφορους ερευνητές που παραγοντοποίησαν έναν αριθμό με 232 δεκαδικά ψηφία (τον RSA-768).

Στη συγκεκριμένη εργασία μελετάμε τους αλγόριθμους παραγοντοποίησης Fermat, Dixon, p-1 Pollard και Pollard Rho.

4.1. Μέθοδος παραγοντοποίησης του Fermat

Η πρώτη μέθοδος παραγοντοποίησης που θα παρουσιάσουμε σε αυτήν την εργασία οφείλεται στον Pierre de Fermat. Η ιδέα της βασίζεται στην έκφραση ενός ακεραίου σαν διαφορά δύο τέλειων τετραγώνων. Αν αυτό επιτυγχάνεται τότε η παραγοντοποίηση γίνεται εύκολα. Επειδή, προφανώς, ο αριθμός που παραγοντοποιείται είναι μονός οι δύο παράγοντες που προκύπτουν είναι και αυτοί μονοί.

Αν είναι $x = u \cdot v = x^2 - y^2 = (x+y)(x-y)$ τότε

$$\left.\begin{array}{l} u = x + y \\ v = x - y \end{array}\right\} \Rightarrow \begin{array}{l} x = \dfrac{u+v}{2} \\ y = \dfrac{u-v}{2} \end{array} .$$

Η ιδέα της μεθόδου του Fermat βασίζεται στην παρακάτω πρόταση :

Πρόταση :

Αν n θετικός περιττός ακέραιος τότε υπάρχει μια ένα προς ένα αντιστοιχία ανάμεσα στις παραγοντοποιήσεις του $n = ab$, όπου $a,\ b$ ακέραιοι με $a \geq b > 0$ και των παραστάσεων του n της μορφής $n = t^2 - s^2$, όπου $t,\ s$ ακέραιοι ≥ 0 .
Η αντιστοιχία δίνεται από τις σχέσεις :

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

$$a = t + s,\ \ b = t - s \ .$$

Απόδειξη :

Έστω $n = ab$, όπου $a,\ b$ ακέραιοι με $a \geq b > 0$. Τότε

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

Έτσι, θέτοντας $t=\frac{a+b}{2}$ και $s=\frac{a-b}{2}$, έχουμε $n=t^2-s^2$.

Αντιστρόφως, αν $n=t^2-s^2$, όπου $t,\ s$ ακέραιοι ≥ 0, τότε

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

Συνεπώς οι αντιστοιχίες

$$(a,b)\to((a+b)/2,(a-b)/2)$$

και

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

δίνουν μια ένα προς ένα αντιστοιχία μεταξύ των δύο τρόπων γραφής του n . ■

Η διαδικασία λοιπόν που ακολούθησε ο Fermat έχει ως εξής :

Μέθοδος παραγοντοποίησης Fermat

Έστω n ο προς παραγοντοποίηση αριθμός. Ο Fermat όρισε ως k τον μικρότερο φυσικό για τον οποίο ισχύει ότι $k^2>n$ και χρησιμοποιώντας αυτόν κατασκεύασε την ακολουθία :

k^2-n
$(k+1)^2-n$
$(k+2)^2-n$

κ.ο.κ. μέχρι η διαφορά $(k+m)^2-n$ να γίνει τέλειο τετράγωνο. Δηλαδή μέχρι να βρεθεί κάποιο y με $(k+m)^2-n=y^2$.(Αυτό βέβαια είναι κάτι το οποίο για πολλούς αριθμούς δεν επιτυγχάνεται ποτέ). Τότε θα έχουμε ότι

$$x=k+m\quad y=\sqrt{(k+m)^2-n}\quad \in\mathbb{N}\ .$$

Οπότε, τελικά, μια παραγοντοποίηση του ακεραίου n δίνεται από τη σχέση

$$n=(k+m)^2-y^2=x^2-y^2=(x+y)(x-y)\ .$$

Παράδειγμα :

1. Έστω $n=451$. Τότε $k=22$ διότι είναι $k^2=22^2=484>451$, ενώ για τον αμέσως μικρότερο από τον k είναι $21^2=441<451$. Οπότε κατασκευάζουμε την ακολουθία :

   $22^2-451=33$
   $(22+1)^2-451=78$
   $(22+2)^2-451=125$
   $(22+3)^2-451=174$
   $(22+4)^2-451=225=15^2$

   Άρα $y=15$ και $x=26$ και τότε έχουμε $451=(26-15)(26+15)=11\cdot 41$.

2. Αν $n=1131$ τότε $k=34$ διότι $34^2=1156>1131$ ενώ $33^2=1089<1131$. Κατασκευάζουμε την ακολουθία :

   $k^2-n=34^2-1131=1156-1131=25=5^2$.

   Άρα με μία μόνο δοκιμή βρήκαμε τους αριθμούς $x=34$ και $y=5$ οι οποίοι μας δίνουν σύμφωνα με τον τύπο της παραγοντοποίησης $1131=34^2-5^2=(34+5)(34-5)=39\cdot 29$.

Η μέθοδος αυτή είναι αποτελεσματική όταν ο n είναι γινόμενο δύο ακεραίων που ο ένας είναι κοντά στον άλλο. Διαφορετικά, αν $n=ab$ με τους ακεραίους a και b να βρίσκονται αρκετά μακρυά, τότε έχουμε βελτίωση της μεθόδου του Fermat με τον εξής τρόπο :

Βελτίωση της μεθόδου του Fermat αν $n = ab$ **με** $a >> b$**.**

Επιλέγω μικρό k και θεωρώ $t = \left\lfloor \sqrt{kn} \right\rfloor + 1,\ \left\lfloor \sqrt{kn} \right\rfloor + 2,\ \ldots$ και υπολογίζω το $t^2 - kn$ μέχρι να ισχύει $t^2 - kn = s^2$. Οπότε τότε έχουμε $(t+s)(t-s) = kn$. Είναι $k < t-s < t+s < n$. Άρα $1 < \text{ΜΚΔ}(t \pm s, n) < n$ και οι $t \pm s$ είναι γνήσιοι παράγοντες του n.

Γενικότερα, αν βρούμε ακεραίους t και s με

$$t^2 \equiv s^2 \bmod n \quad \text{και} \quad t \neq \pm s \bmod n$$

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

<u>Παράδειγμα :</u>

Έστω $n = 329.345$. Θεωρώ τον αριθμό $k = 3$ και υπολογίζω το $\sqrt{3 \cdot 329.345} = 993,\ldots$ Θεωρούμε τις τιμές $t = 994,\ldots$ και παίρνουμε $t^2 - kn = 944^2 - 3 \cdot 329345 = 1 = 1^2$.

Άρα θα έχουμε $3 \cdot 329.345 = (994+1)(994-1) = 995 \cdot 993$.

Υπολογίζω και τον $\text{ΜΚΔ}(329.345, 995) = \text{ΜΚΔ}(331 \cdot 995, 995) = 995$, επομένως έχουμε την παραγοντοποίηση του n : $329.345 = 331 \cdot 995$.

Παρατηρούμε λοιπόν ότι η απλή μέθοδος του Fermat μπορεί να είναι πολύ αργή για κάποιους αριθμούς καθώς απαιτούνται πολύ περισσότερες δοκιμές.

Βασιζόμενος σε αυτή τη μέθοδο το 1641 ο Frenicle ζήτησε από τον Fermat να παραγοντοποιήσει έναν φυσικό που γράφεται σαν άθροισμα τετραγώνων με δύο όμως διαφορετικούς τρόπους. Δεν γνωρίζουμε αν δόθηκε απάντηση από τον Fermat αλλά το 1745, έναν αιώνα αργότερα δηλαδή, ο Euler έδειξε ότι αν $n = a^2 + b^2 = c^2 + d^2$ τότε έχουμε την παρακάτω παραγοντοποίηση του n :

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

Η παράσταση προκύπτει αν εκτελέσω τις πράξεις στο δεύτερο μέλος.

Παράδειγμα :

Για τον $n=425$ έχουμε ότι $425=20^2+5^2=19^2+8^2$**.** Άρα θα είναι $a=20$, $b=5$, $c=19$, $d=8$. Εφαρμόζουμε τον τύπο :

$$425=\frac{\left(1^2+\left(-3\right)^2\right)\left(39^2+\left(-3\right)^2\right)}{4\left(\left(-3\right)^2\right)}=\frac{10\cdot1530}{4\cdot9}=\left(\frac{10}{2}\right)\left(\frac{1530}{2\cdot9}\right)=5\cdot85\,.$$

Μπορούμε επίσης να δούμε μια γενίκευση της παραπάνω μεθόδου.

Θεώρημα :

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

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

Απόδειξη :

Από τους παραπάνω τύπους βρίσκουμε τα a,b,c,d και αντικαθιστούμε στον τύπο για το N . Είναι $a=\frac{kmr+ns}{2}$, $b=\frac{ms-nr}{2}$, $c=\frac{kmr-ns}{2}$, $d=\frac{ms+nr}{2}$.

Άρα έχουμε για το N :

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

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

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

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

<u>Παράδειγμα :</u>

Έστω ο αριθμός 34.889 που γράφεται ώς :

$34.889 = 157^2 + 10 \cdot 32^2 = 143^2 + 10 \cdot 38^2$, οπότε έχουμε :

$a + c = 10 \cdot 30$ όπου $k = 10$ και $mr = 30$, άρα $m = 10,\ r = 3$
$a - c = 14 = ns$
$d + b = 70 = ms$, άρα και από το προηγούμενο προκύπτει $s = 7$
$d - b = 6 = nr$, άρα $n = 2$.

Επομένως τελικά έχουμε την παραγοντοποίηση του αριθμού :

$$34.889 = \frac{\left(10 \cdot 10^2 + 2^2\right)\left(10 \cdot 3^2 + 7^2\right)}{4} = \frac{1004 \cdot 139}{4} = 251 \cdot 139 \ .$$

4.2. Ο Αλγόριθμος παραγοντοποίησης του Dixon

Ο αλγόριθμος του Dixon είναι μια βελτίωση θα λέγαμε της μεθόδου παραγοντοποίησης ακεραίων του Fermat. Η διαφορά είναι ότι η μέθοδος Dixon χρησιμοποιεί μια βάση παραγοντοποίησης την οποία θα δούμε παρακάτω. Όπως και η μέθοδος του Fermat έτσι και αυτή στηρίζεται στην εύρεση ακεραίων a, b με $a^2 = b^2 \bmod n$ και $a \neq \pm b \bmod n$. Άρα λοιπόν τότε θα έχουμε

$$a^2 - b^2 = 0 \bmod n \Rightarrow (a-b)(a+b) = k \cdot n \Rightarrow n \mid (a-b)(a+b) .$$

Επειδή όμως $a \neq \pm b \bmod n$ το $(a-b)$ ή το $(a+b)$ δεν διαιρούνται από το n. Οπότε ο αριθμός $\text{ΜΚΔ}(a-b, \text{n})$ θα είναι ένας μη τετριμμένος παράγοντας για το n .

Ορισμός :

Καλούμε *βάση παραγοντοποίησης* ένα σύνολο $B = \{-1, p_1, ..., \text{p}_h\}$ όπου $p_1, ..., p_h$ είναι διακεκριμένοι πρώτοι. Προφανώς ισχύει $-1 = (n-1) \bmod n$. Ο ακέραιος n καλείται *B-λείος* αν γράφεται σαν γινόμενο στοιχείων του B. Επίσης ένας ακέραιος b καλείται *B-προσαρμοσμένος ως προς τον φυσικό* n αν ο ακέραιος c με $-\frac{n}{2} \leq c \leq \frac{n}{2}$ και $b^2 = c \bmod n$ είναι B-λείος.

Παράδειγμα :

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

Επίσης έχουμε $71^2 = 63 \bmod 2849$. Είναι $-\frac{2849}{2} \leq 63 \leq \frac{2849}{2}$, άρα ο $b = 71$ είναι B-προσαρμοσμένος ως προς τον 2849.

Το βασικό κομμάτι του αλγόριθμου του Dixon είναι ότι επιλέγουμε μια βάση που αποτελείται από μικρούς πρώτους και κατασκευάζουμε τετράγωνα αριθμών τα οποία

γράφονται σαν γινόμενα μικρών πρώτων και στοιχείων της βάσης. Κάθε τέτοιο τετράγωνο αντιστοιχεί σε μια γραμμή ενός πίνακα και σε αυτή τη γραμμή αποθηκεύονται οι εκθέτες των πρώτων αριθμών της βάσης που αποτελούν το συγκεκριμένο γινόμενο. Αν λοιπόν πάρουμε περισσότερους τέτοιους αριθμούς από το πλήθος των στοιχείων της βάσης ο τελικός πίνακας θα αποτελείται από γραμμικώς εξαρτημένα διανύσματα. Συγκεκριμένα θα έχουμε $\mod 2$ το πλήθος γραμμικές εξαρτήσεις μεταξύ των γραμμών. Οι γραμμικά εξαρτημένες γραμμές για διάφορα x , y δίνουν $x^2 = y^2 \bmod n$. Οπότε, τελικά, αν ισχύει ότι $x \neq \pm y \bmod n$ τότε έχουμε βρεί μη τετριμμένο παράγοντα του n και έχουμε πετύχει την παραγοντοποίηση.

Πιο συγκεκριμένα για να παραγοντοποιήσουμε έναν ακέραιο σύμφωνα με τη μέθοδο του Dixon ακολουθούμε τα παρακάτω βήματα.

Αλγόριθμος Dixon

1. Επιλέγουμε ένα θετικό ακέραιο y και θεωρούμε τη βάση παραγοντοποίησης B που σχηματίζεται από όλους τους πρώτους $p_1, p_2, ..., p_{\pi(y)}$ που είναι $\leq y$.
2. Αν κανένας από τους πρώτους p_i δεν διαιρεί τον n , τότε βρίσκουμε ακεραίους b_i με $1 < b_i < n$, $i = 1, ..., \pi(y) + 2$ που είναι B-προσαρμοσμένοι ως προς τον n .
3. Αν
$$b_i^2 = (-1)^{a_{i0}} \, p_1^{a_{i1}} ... p_{\pi(y)}^{a_{i\pi(y)}} \bmod n$$
τότε αντιστοιχούμε στο b_i το διάνυσμα των εκθετών $u_i = (u_{i0}, ..., u_{i\pi(y)})$ του $\mathbb{Z}_2^{\pi(y)+1}$ θέτοντας $u_{ij} = 0$ αν ο a_{ij} είναι άρτιος και $u_{ij} = 1$ αν ο a_{ij} είναι περιττός (συμβολίζουμε πιο απλά με 0 και 1 τα στοιχεία του $\mathbb{Z}_2$).
4. Προσδιορίζω ένα υποσύνολο I του $\{1, ..., \pi(y) + 2\}$ τέτοιο, ώστε
$$\sum_{i \in I} u_i = 0 .$$
5. Υπολογίζουμε τα γινόμενα
$$b = \prod_{i \in I} b_i \ , \quad c = p_1^{\gamma_1} ... p_{\pi(y)}^{\gamma_{\pi(y)}} \ ,$$
όπου $2\gamma_j = \sum_{i \in I} a_{ij}$.

Προσοχή : Θέλω κάθε πρώτος της βάσης B να χρησιμοποιείται **άρτιο** πλήθος φορών.

6. Αν $b \neq \pm c \bmod n$ υπολογίζουμε τον $\text{ΜΚΔ}(b+c, n)$ που μας δίνει μη τετριμμένο παράγοντα του n. Αν $b = \pm c \bmod n$ τότε επιλέγω ένα άλλο σύνολο $I \subset \{1, ..., \pi(y)+2\}$ ή παίρνουμε ένα μεγαλύτερο ακέραιο y και επαναλαμβάνουμε τη διαδικασία.

Παρατηρούμε ότι στο τέταρτο βήμα το πλήθος των διανυσμάτων u_i $(i = 1, 2, ..., \pi(y)+2)$ είναι μεγαλύτερο από τη διάσταση του διανυσματικού χώρου $\mathbb{Z}_2^{\pi(y)+1}$ επομένως τα διανύσματα αυτά είναι γραμμικώς εξαρτημένα. Άρα το σύνολο I υπάρχει πάντα και μπορεί να προσδιοριστεί με τη χρήση απαλοιφής. Από την κατασκευή των ακεραίων b και c έχουμε $b^2 \equiv c^2 \bmod n$ και κατά συνέπεια, στην περίπτωση όπου $b \neq \pm c \bmod n$, ο μέγιστος κοινός διαιρέτης $(b+c, n)$ είναι ένας μη τετριμμένος παράγοντας του n.

Επίσης, καθώς οι πρώτοι $p_1, p_2, ..., p_{\pi(y)}$ δεν διαιρούν τον n, έχουμε $(b, n) = 1$. Αν λοιπόν ο n έχει r πρώτους παράγοντες $(r \geq 2)$, τότε η πολυωνυμική ισοτιμία

$$x^2 = b^2 \bmod n$$

έχει ακριβώς 2^r λύσεις. Οπότε η πιθανότητα να έχουμε $b \equiv \pm c \bmod n$ ισούται με $1/2^{r-1}$.

Ένας απλός τρόπος εύρεσης των ακεραίων b_i είναι να δοκιμάζουμε ακεραίους της μορφής $\lfloor \sqrt{kn} \rfloor + j$, $j = 0, 1, ...$, $k = 1, 2, ...$. Ο μικρότερος κατ' απόλυτη τιμή ακέραιος της κλάσης του τετραγώνου τέτοιων ακεραίων $(\bmod n)$ είναι αρκετά μικρός και κατά συνέπεια έχουν μεγάλη πιθανότητα ναι είναι B-προσαρμοσμένοι ως προς τον n .

<u>Παράδειγμα :</u>

Έστω ο αριθμός $n = 93623$. Θεωρώ τη βάση $B = \{-1, 2, 3, 5, 7, 11, 13\}$ που έχει 7 στοιχεία και άρα θα προσπαθήσω να βρώ τουλάχιστον 8 B-προσαρμοσμένους ακεραίους ως προς

τον $n = 93623$. Παρατηρώ ότι τα στοιχεία της βάσης δεν διαιρούν τον n. Δοκιμάζω ακεραίους της μορφής $\lfloor \sqrt{kn} \rfloor + j$ με $k, j = 1,2,...,9$.

Έχουμε :

$\sqrt{n} = 305,9...$ άρα η πρώτη μου δοκιμή είναι $b_1 : 306^2 = 93636 = 13 \bmod n \in B$

$\sqrt{2n} = 432,...$ και βρίσκω τον $b_2 : 432^2 = 187.489 = 243 = 3^5 \bmod n \in B$.

Συνεχίζοντας έτσι προκύπτουν οι εξής ισοτιμίες :

$$306^2 \equiv 13 \bmod n$$
$$433^2 \equiv 3^5 \bmod n$$
$$531^2 \equiv 2^2 \cdot 3 \cdot 7 \cdot 13 \bmod n$$
$$537^2 \equiv 2^2 \cdot 3 \cdot 5^4 \bmod n$$
$$612^2 \equiv 2^2 \cdot 13 \bmod n$$
$$809^2 \equiv -2^4 \cdot 5 \cdot 11 \bmod n$$
$$866^2 \equiv 2^2 \cdot 3^5 \bmod n$$
$$918^2 \equiv 3^2 \cdot 13 \bmod n$$

Οπότε, έχω στο $\mathbb{Z}_2^7$ τα εξής διανύσματα :

$$u_1 = (0,0,0,0,0,0,1)$$
$$u_2 = (0,0,1,0,0,0,0)$$
$$u_3 = (0,0,1,0,1,0,1)$$
$$u_4 = (0,0,1,0,0,0,0)$$
$$u_5 = (0,0,0,0,0,0,1)$$
$$u_6 = (1,0,0,1,0,1,0)$$
$$u_7 = (0,0,1,0,0,0,0)$$
$$u_8 = (0,0,0,0,0,0,1)$$

Θεωρούμε το ομογενές γραμμικό σύστημα

$$x_1 u_1 + ... + x_8 u_8 = 0 \bmod 2$$

με αγνώστους $x_1,...,x_8$ και από αυτό θα βρούμε μια σχέση γραμμικής εξάρτησης μεταξύ των διανυσμάτων. Ισοδύναμα έχουμε

$$\left.\begin{aligned} x_6 &= 0 \\ x_2 + x_3 + x_4 + x_7 &= 0 \\ x_3 &= 0 \\ x_1 + x_3 + x_5 + x_8 &= 0 \end{aligned}\right\} \bmod 2$$

Μια λύση του συστήματος είναι :

$$x_1 = x_5 = 1$$
$$x_2 = x_3 = x_4 = x_6 = x_7 = x_8 = 0$$

Άρα το σύνολο I είναι το $I = \{x_1, x_5\}$. Υπολογίζω τα b και c.

$$b = \prod_{i \in I} b_i = b_1 b_5 = 306 \cdot 602 = 187.272$$
$$c^2 = 13 \cdot 2^2 \cdot 13 \Rightarrow c^2 = 2^2 \cdot 13^2 \Rightarrow c = 26 .$$

Παρατηρούμε ότι $187.272 = 26 \bmod n$, άρα δεν μπορούμε να προσδιορίσουμε ένα μη τετριμμένο παράγοντα του n.

Βρίσκω λοιπόν μια άλλη λύση του συστήματος, ήτοι την

$$x_2 = x_4 = 1$$
$$x_1 = x_3 = x_5 = x_6 = x_7 = x_8 = 0$$

όπου $I' = \{x_2, x_4\}$.

Τότε είναι $b = 433 \cdot 537 = 232521$ και

$$c^2 = 3^5 \cdot 2^2 \cdot 3 \cdot 5^4 = \left(2 \cdot 3^3 \cdot 5^2\right)^2 \Rightarrow c = 2 \cdot 3^3 \cdot 5^2 = 1350 .$$

Όμως σε αυτή την περίπτωση βλέπουμε ότι $232.521 = 45.275 \bmod n$, δηλαδή $b \neq \pm c \bmod n$. Άρα, $\text{ΜΚΔ}(b + c, n) = (233.871, 93.623) = 373$.

Οπότε τελικά έχουμε την παραγοντοποίηση του n: $93.623 = 373 \cdot 251$.

Ας σημειώσουμε ότι, αναφορικά με την πολυπλοκότητα του αλγορίθμου, στην περίπτωση που έχει επιλεγεί κατάλληλη βάση παραγοντοποίησης, ο χρόνος εκτέλεσής του είναι $O\left(e^{c\sqrt{\log n \cdot \log\log n}}\right)$, δηλαδή υποεκθετικού χρόνου.

4.3. Ο αλγόριθμος p - 1 του John Pollard (1974)

Ο αλγόριθμος $p-1$ του Pollard είναι ένας αριθμοθεωρητικός αλγόριθμος παραγοντοποίησης ακεραίων που δημιουργήθηκε από τον John Pollard to 1974. Είναι ένας αλγόριθμος που δουλεύει ικανοποιητικά μόνο για ακεραίους n με συγκεκριμένες ιδιότητες. Η μέθοδος λοιπόν αυτή δουλεύει όταν ο σύνθετος n έχει έναν πρώτο παράγοντα p τέτοιον ώστε ο $p-1$ να έχει μόνο μικρούς πρώτους παράγοντες. Ο αλγόριθμος αυτός, όπως και ο αλγόριθμος του Dixon, στηρίζεται στην προκαθορισμένη βάση παραγοντοποίησης (με μικρούς πρώτους αριθμούς).

Ο αλγόριθμος έχει δύο εισόδους : τον προς παραγοντοποίηση αριθμό n, ο οποίος έχει την παραπάνω ιδιότητα την οποία όμως δεν την γνωρίζουμε πριν την παραγοντοποίηση, και το προκαθορισμένο φράγμα B.

Αλγόριθμος $p-1$ του Pollard

1. Επιλέγουμε ένα θετικό ακέραιο B και υπολογίζουμε το γινόμενο
$$k=\prod_{q\le B} q^{\lfloor \log_q B \rfloor}$$
όπου το q παίρνει τιμές από το σύνολο των πρώτων $\le B$.
2. Επιλέγουμε έναν ακέραιο a με $1<a<n$ και υπολογίζουμε τον $\text{ΜΚΔ}(a,n)=\delta$. (συνήθως αρχίζω με $a=2$, $a=3$ κοκ.)
3. Αν $\delta>1$, τότε ο δ είναι μη τετριμμένος παράγοντας του n .
Αν $\delta=1$, υπολογίζω τον $d=\text{ΜΚΔ}\left(a^k-1,n\right)$.
4. Αν $1<d<n$, τότε ο d είναι μη τετριμμένος παράγοντας του n .
Αν $d=1$ ή $d=n$ επιλέγουμε άλλο B και επαναλαμβάνουμε την διαδικασία.

Παρατηρούμε λοιπόν ότι αν ο p είναι πρώτος παράγοντας του n και κάθε δύναμη πρώτου που διαιρεί τον $p-1$ είναι $\le B$ τότε ο $p-1$ αναλύεται ως εξής : $p-1=2^a\cdot 3^b\cdot 5^\gamma\cdot\ldots$,

όπου κάθε παράγοντας είναι $<\mathrm{B}$. Οπότε ο k θα είναι πολλαπλάσιο του $p-1$, δηλαδή $p-1|\,k \Rightarrow k=l\left(p-1\right)$. Τότε όμως για κάθε a με $1<a<n$ και $\left(a,p\right)=1$ έχω από το μικρό θεώρημα του Fermat $a^k=a^{l(p-1)}=\left(a^{p-1}\right)^l=1\mathrm{mod}\,p \Rightarrow a^k-1=\pi o\lambda\, p$ δηλαδή $p\,|\,a^k-1$. Αν λοιπόν ισχύει ότι $d\neq n$ τότε $1<d<n$ και ο d είναι μη τετριμμένος παράγοντας του n και ο αλγόριθμος δουλεύει.

<u>Παράδειγμα :</u>

Θα παραγοντοποιήσουμε τον ακέραιο $n=1.127.041$.

Παίρνουμε $B=19$ και έχουμε $k=2^4\cdot 3^2\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19=232.792.560$. Στη συνέχεια υπολογίζουμε $\mathrm{MK\Delta}(2^k-1,n)=761$, άρα προκύπτει η παραγοντοποίηση $1.127.041=761\cdot 1481$, όπου 761 και 1481 πρώτοι.

Έχουμε ότι $p-1=760=2^3\cdot 5\cdot 19$ άρα η τιμή για τη βάση $B=19$ είναι μια εφικτή τιμή.

Σημειώνουμε και για αυτόν τον αλγόριθμο ότι ο χρόνος που απαιτείται για την παραγοντοποίηση του n είναι $O\left(B^2\left(\log B\right)^2\left(\log n\right)^2\right)$. Για $B=O\left(\left(\log n\right)^i\right)$ με i θετικό ακέραιο ο αλγόριθμος είναι πολυωνυμικού χρόνου σαν συνάρτηση του $\log n$, όμως μια τέτοια επιλογή του B δίνει μικρή πιθανότητα επιτυχίας. Αν όμως αυξήσουμε δραστικά το μέγεθος της βάσης B ο αλγόριθμος, αν και γίνεται πολύ πιο αργός, αποδεικνύεται επιτυχής.

4.4. Ο Αλγόριθμος Pollard Rho

Μια άλλη μέθοδος που δημοσιοποίησε ο John Pollard στα 1975 για την παραγοντοποίηση ακεραίων είναι ο αλγόριθμος ρ που είναι και γνωστός με την ονομασία *μέθοδος Monte Carlo*.

Ας δούμε αρχικά τη βασική ιδέα του αλγόριθμου : Έστω p ο μικρότερος πρώτος διαιρέτης του προς παραγοντοποίηση αριθμού n και x, x' ακέραιοι στο $\mathbb{Z}_n$ τέτοιοι ώστε $x \neq x'$ και $x = x' \bmod p$. Τότε $p \leq \text{ΜΚΔ}(x - x', n) \leq n$. Έτσι υπολογίζοντας τον ΜΚΔ βρίσκουμε έναν μη τετριμμένο παράγοντα του n.

Αν τώρα θέλουμε να παραγοντοποιήσουμε τον n επιλέγοντας πρώτα ένα τυχαίο υποσύνολο X του $\mathbb{Z}_n$ και ύστερα υπολογίζοντας τους $\text{ΜΚΔ}(x - x', n)$ για όλα τα x, x' στο X με $x \neq x'$, τότε η μέθοδος θα είχε επιτυχία μόνο στην περίπτωση που η απεικόνιση $x \to x \bmod p$ οδηγεί σε μια τουλάχιστον «σύγκρουση» για το $x \in X$. Η περίπτωση αυτή στηρίζεται στο παράδοξο των γενεθλίων και σύμφωνα με αυτό θα έχουμε πως αν $|X| \approx 1{,}17\sqrt{n}$ τότε υπάρχει 50% πιθανότητα να πετύχουμε σύγκρουση και να βρούμε έτσι έναν μη τετριμμένο παράγοντα του n.

Αναλύουμε παρακάτω την έννοια της σύγκρουσης και το παράδοξο των γενεθλίων.

Ορισμός :

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

Θεώρημα (Παράδοξο των γενεθλίων (birthday paradox)) :

Σύμφωνα με το παράδοξο των γενεθλίων, σε μια τυχαία επιλογή 23 ανθρώπων, η πιθανότητα δύο απο αυτούς να έχουν γενέθλια την ίδια μέρα είναι τουλάχιστον $0{,}5$ (για την ακρίβεια $0{,}507$).

Από μαθηματικής άποψης, αν μια συνάρτηση f παράγει μια τιμή μεταξύ n διαφορετικών τιμών με την ίδια πιθανότητα και το n είναι αρκετά μεγάλο, τότε υπολογίζοντας τη συνάρτηση για ένα πλήθος περίπου $1{,}17\sqrt{n}$ διαφορετικών εισόδων περιμένουμε να βρούμε ένα ζεύγος εισόδων x και x' $\left(x \neq x'\right)$ τέτοια ώστε $f\left(x\right) = f\left(x'\right)$.

Απόδειξη :

Θεωρούμε την ομάδα των ακεραίων $\bmod n$, δηλαδή το σύνολο $\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$ με $\left|\mathbb{Z}_n\right| = n$. Θα υπολογίζουμε την πιθανότητα να μην επιλεχθούν ίσα στοιχεία (να μην έχουμε δηλαδή συγκρούσεις) σε μια τυχαία επιλογή k στοιχείων 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 δύο προηγούμενες είναι $\frac{n-2}{n} = 1-\frac{2}{n}$ κ.ο.κ. Έτσι η πιθανότητα επιλογής k στοιχείων χωρίς συγκρούσεις είναι $\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\left(1-\frac{3}{n}\right)\ldots\left(1-\frac{k-1}{n}\right) = \prod_{i=1}^{k-1}\left(1-\frac{i}{n}\right)$, όπως προκύπτει από την Πολλαπλασιαστική Αρχή.

Ισχύει ότι $e^{-x} = 1-x+\frac{x^2}{2!}-\frac{x^3}{3!}+\ldots$, $-\infty < x < \infty$. Άρα αν ο x είναι μικρός πραγματικός, τότε $1-x \approx e^{-x}$. Κατά συνέπεια αφού το n είναι πολύ μεγάλο, το $\frac{1}{n}$ είναι πολύ μικρό άρα έπεται ότι $1-\frac{1}{n} \approx e^{-1/n}$.

Οπότε μια εκτίμηση της ζητούμενης πιθανότητας είναι η

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

Αν P είναι η πιθανότητα εύρεσης μιας σύγκρουσης τότε $P \approx 1-e^{-k(k-1)/2n}$ και ύστερα από πράξεις έχουμε την εκτίμηση $k \approx \sqrt{2n \ln \frac{1}{1-p}}$ και για την πιθανότητα σύγκρουσης $P = 1/2$ θα είναι $k \approx 1{,}17\sqrt{n}$.

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

Να σημειώσουμε ότι στο παράδοξο των γενεθλίων έχουμε $n = 365$ και η προσέγγιση μας δίνει $k \approx 1{,}17\sqrt{365} \approx 22{,}3$. ■

Αναλύουμε παρακάτω τη διαδικασία παραγοντοποίησης ακεραίου n με τη μέθοδο Pollard Rho καθώς και το θεωρητικό της υπόβαθρο.

Παραγοντοποίηση μονού ακεραίου n

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

Έστω $x_1 \in \mathbb{Z}_n$ και $X \subseteq \mathbb{Z}_n$ με

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

Σκοπός είναι η εύρεση δύο διαφορετικών τιμών $x_i, x_j \in X$ τέτοιες ώστε $\text{ΜΚΔ}\left(x_j - x_i, n\right) > 1$. Κάθε φορά που υπολογίζουμε έναν καινούριο όρο x_j της ακολουθίας, μπορούμε να υπολογίζουμε τους $\text{ΜΚΔ}\left(x_j - x_i, n\right)$ για όλα τα $i < j$. Όμως αυτό θα απαιτούσε $\binom{|X|}{2} = \binom{m}{2}$ υπολογισμούς, περισσότερους από $p/2$.

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

Ας είναι p ένας πρώτος διαιρέτης του n. Τότε για κάποιους δείκτες i, j με $i < j$ έχουμε

$$x_i \equiv x_j \bmod p .$$

Θα δείξουμε ότι για κάθε ακέραιο $m \geq 0$ ισχύει

$$x_{i+m} \equiv x_{j+m} \bmod p .$$

Πράγματι, η f είναι πολυωνυμική συνάρτηση με ακέραιους συντελεστές οπότε

$$f(x_i) \equiv f(x_j) \bmod p$$

και καθώς

$$x_{i+1} \equiv f(x_i) \bmod n \quad \text{και} \quad x_{j+1} \equiv f(x_j) \bmod n ,$$

Παίρνουμε

$$x_{i+1} \equiv x_{j+1} \bmod p .$$

Υποθέτουμε ότι η προς απόδειξη σχέση ισχύει για $m = k$ και με τον ίδιο τρόπο όπως παραπάνω συμπεραίνουμε ότι ισχύει για $m = k+1$. Συνεπώς ισχύει για κάθε ακέραιο $m \geq 0$.

Ας υποθέσουμε τώρα ότι i και j είναι οι μικρότεροι δείκτες με $i < j$ και

$$x_i \equiv x_j \bmod p .$$

Θέτουμε $l = j - i$. Οπότε, για κάθε ακέραιο $t \geq i$ έχουμε

$$x_t \equiv x_{t+l} \bmod p .$$

Ας είναι r, s δείκτες με $s > r \geq i$ και $s - r \equiv 0 \bmod l$. Τότε $s = r + Al$ για κάποιο ακέραιο A. Έχουμε

$$x_r \equiv x_{l+r} \bmod p \equiv \ldots \equiv x_{(A-1)l+r} \equiv x_s \bmod p .$$

Μεταξύ των ακεραίων $i,\ldots, j-1$ υπάρχει ένας ο οποίος διαιρείταιαπό τον l. Αν b είναι αυτός ο ακέραιος, τότε, σύμφωνα με τα παραπάνω, ισχύει

$$x_b \equiv x_{2b} \bmod p .$$

Αν επιπλέον έχουμε

$$x_b \neq x_{2b} \bmodn ,$$

τότε $p \leq \left(x_b - x_{2b}, n\right) < n$ και επομένως ο $\text{ΜΚΔ}\left(x_b - x_{2b}, n\right)$ είναι ένας μη τετριμμένος παράγοντας του n.

Παρατηρούμε ότι είναι πιθανό ο αλγόριθμος να μην εντοπίσει έναν μη τετριμμένο παράγοντα του n στην περίπτωση που οι τιμές x_i και x_j που εμφανίζουν την πρώτη σύγκρουση, ικανοποιούν στην ουσία τη σχέση $x_i \equiv x_j \bmod n$ αντί απλά της $x_i \equiv x_j \bmod p$.

<u>Σημείωση :</u>

Ας είναι G το γράφημα το οποίο έχει ως κορυφές τα $\overline{x}_t \ \left(t = 0,1,\ldots\right)$ και πλευρές προσανατολισμένες από το $\overline{x}_t$ στο $\overline{x}_{t+1}$, όπου με $\overline{x}_t$ συμβολίζουμε την κλάση ακεραίου $x_t \bmod p$. Από τα παραπάνω βλέπουμε ότι το G αποτελείται από μια ουρά

$$\overline{x}_0 \to \overline{x}_1 \to \ldots \to \overline{x}_{i-1}$$

και έναν κύκλο μήκους l

$$\overline{x}_i \to \overline{x}_{i+1} \to \ldots \to \overline{x}_j = \overline{x}_i$$

ο οποίος επαναλαμβάνεται χωρίς τέλος. Έτσι το γράφημα G έχει την μορφή του ελληνικού γράμματος ρ, απ' όπου και το όνομα αλγόριθμος ρ του Rollard.

Ας δούμε λοιπόν τα βήματα που ακολουθούμε για την παραγοντοποίηση ακεραίου με την μέθοδο του Pollard Rho.

Αλγόριθμος Pollard Rho

Βήμα 1 Επιλέγουμε $x_1 \in \mathbb{Z}_n$ και υπολογίζουμε το $x_2 = f(x_1) = x_1^2 + 1 (\mathrm{mod}\, n)$.

Υπολογίζουμε τον $\mathrm{MK\Delta}(x_2 - x_1, n) = p$.

Αν $p = 1$ προχωράμε στο βήμα 2 .

Βήμα 2 Υπολογίζουμε τους ακεραίους $x_i = f(x_{i-1}) \bmod n$ και $x_{2i} = f(x_{2i-1}) \bmod n$

Βρίσκουμε τον $\mathrm{MK\Delta}(x_{2i} - x_i, n) = p$ για $i = 2$.

Αν $i < p < n$ τότε $x_i \equiv x_{2i} (\mathrm{mod}\, p)$ και p είναι μη τετριμμένος

παράγοντας του n .

Αν $p = n$ ο αλγόριθμος επιστρέφει μήνυμα «αποτυχία».

Αν $p = 1$ επαναλαμβάνουμε το βήμα 2 για $i = 3$, έπειτα για $i = 4$ κ.ο.κ.

<u>Παράδειγμα :</u>

Έστω $n = 7171$, $f(x) = x^2 + 1$ και $x_1 = 1$. Θα παραγοντοποιήσουμε τον n .

Βήμα 1 : $x_1 = 1$, $x_2 = f(x_1) = 1^2 + 1 = 2 \bmod 7171$,

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

Βήμα 2 : $x_2 = 2$, $x_3 = f(x_2) = 2^2 + 1 = 5 \bmod 7171$,

$x_4 = f(x_3) = 5^2 + 1 = 26 \bmod 7171$,

$\gcd(x_4 - x_2, n) = \gcd(24, 7171) = 1$.

Βήμα 3 : $x_3 = 5$, $x_4 = 26$, $x_5 = f(x_4) = 26^2 + 1 = 677 \bmod 7171$,

$$x_6 = f(x_5) = 677^2 + 1 = 458330 = 6557 \bmod 7171,$$

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

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

$$x_7 = f(x_6) = 6557^2 + 1 = 42994250 = 4105 \bmod 7171,$$

$$x_8 = f(x_7) = 4105^2 + 1 = 16851026 = 6347 \bmod 7171,$$

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

Βήμα 5 : $x_5 = 677,\ x_6 = 6557,\ x_7 = 4105,\ x_8 = 6347 \bmod 7171,$

$$x_9 = f(x_8) = 6347^2 + 1 = 40284410 = 4903 \bmod 7171,$$

$$x_{10} = f(x_9) = 4903^2 + 1 = 24039410 = 2218 \bmod 7171,$$

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

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

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

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

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

Βήμα 7 : $x_7 = 4105,\ x_8 = 6347,\ x_9 = 4903,\ x_{10} = 2218,\ x_{11} = 219,\ x_{12} = 4936$

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

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

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

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

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

$x_{15} = f\left(x_{14}\right) = 4560^2 + 1 = 20793601 = 4782 \bmod 7171$,

$x_{16} = f\left(x_{15}\right) = 4872^2 + 1 = 23736385 = 375 \bmod 7171$.

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

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

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

$x_{17} = f\left(x_{16}\right) = 375^2 + 1 = 140626 = 4377 \bmod 7171$,

$x_{18} = f\left(x_{17}\right) = 4377^2 + 1 = 19158130 = 4389 \bmod 7171$,

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

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

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

$x_{19} = f\left(x_{18}\right) = 4389^2 + 1 = 19263322 = 2016 \bmod 7171$,

$x_{20} = f\left(x_{19}\right) = 2016^2 + 1 = 4064257 = 5471 \bmod 7171$,

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

Βήμα 11 : $x_{11} = 219$, $x_{12} = 4936$, $x_{13} = 4210$, $x_{14} = 4560$, $x_{15} = 4872$, $x_{16} = 375$,

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

$x_{21} = f\left(x_{20}\right) = 5471^2 + 1 = 29931842 = 88 \bmod 7171$,

$x_{22} = f\left(x_{21}\right) = 88^2 + 1 = 7745 = 574 \bmod 7171$,

$\gcd\left(x_{22} - x_{11}, n\right) = \gcd\left(355, 7171\right) = 71$.

Βλέπουμε λοιπόν ότι μετά από 11 επαναλήψεις ο αλγόριθμος εντόπισε τη σύγκρουση $x_{11} = x_{22} \pmod{p}$ και τον μη τετριμμένο παράγοντα $p = 71$ του $n = 7171$. Άρα, τελικά, $n = 7171 = 71 \cdot 101$. Η πρώτη σύγκρουση είναι η $x_7 \bmod 71 = x_{18} \bmod 71 = 58$.

Βιβλιογραφία

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

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

Πουλάκης Δ. , "Θεωρία αριθμών", Εκδόσεις ΖΗΤΗ, 2001

Παπαϊωάννου Α. / Ρασσιάς Μ. , "Εισαγωγή στη θεωρία αριθμών" , Εκδόσεις ΣΥΜΕΩΝ, 2010

Frayleigh B. John, "Εισαγωγή στην Άλγεβρα" , Πανεπιστημιακές Εκδόσεις Κρήτης, 2003

Gareth A. Jones and J. Mary Jones , "Elementary Number Theory", Springer

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

Trappe W. / Washinghton L. , "Introduction to Cryptography with coding Theory" , Pearson Education

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