



**ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ**

**ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ  
ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**ΑΛΓΟΡΙΘΜΟΙ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗΣ  
ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ**

**ΓΕΩΡΓΙΟΣ Β. ΚΑΛΚΑΝΤΖΗΣ**

Εξεταστική Επιτροπή:

Χ. Κουκουβίνος, Καθηγητής ΕΜΠ

Α. Παπαϊωάννου, Αναπληρωτής Καθηγητής ΕΜΠ (Επιβλέπων)

Π.Στεφανέας, Λέκτορας ΕΜΠ

Αθήνα, Φεβρουάριος 2013



**ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ**

**ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ  
ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**ΑΛΓΟΡΙΘΜΟΙ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗΣ  
ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ**

**ΓΕΩΡΓΙΟΣ Β. ΚΑΛΚΑΝΤΖΗΣ**

Εξεταστική Επιτροπή:

Χ. Κουκουβίνος, Καθηγητής ΕΜΠ

Α. Παπαϊωάννου, Αναπληρωτής Καθηγητής ΕΜΠ (Επιβλέπων)

Π.Στεφανέας, Λέκτορας ΕΜΠ

Αθήνα, Φεβρουάριος 2013

## ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

	ΣΕΛ.
<b>ΠΕΡΙΛΗΨΗ</b>	4
<b>ΚΕΦΑΛΑΙΟ 1: ΣΤΟΙΧΕΙΑ ΑΠΟ ΤΗΝ ΘΕΩΡΙΑ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ</b>	6
1.1 Εισαγωγή	6
1.2 Θεώρημα του Lucas	7
1.3 Γραμμικές Ισοδυναμίες	8
1.4 Ισοδυναμίες Δευτέρου Βαθμού	17
1.5 Τετραγωνικά Υπόλοιπα	22
1.6 Το σύμβολο του Jacobi	28
1.7 Πρωταρχικές Ρίζες	29
<b>ΚΕΦΑΛΑΙΟ 2: ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΩΤΩΝ</b>	39
2.1 Το Θεώρημα του Fermat	39
2.2 Το Κριτήριο Miller Rabin και Solovay Strassen	44
2.3 Κριτήριο Miller-Rabin (αναλυτικά)	47
<b>ΚΕΦΑΛΑΙΟ 3: ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΑΚΕΡΑΙΩΝ</b>	51
3.1 Μέθοδος των Διαδοχικών Διαιρέσεων	51
3.2 Μέθοδος του Fermat και του Euler	53
3.3 Ο αλγόριθμος παραγοντοποίησης του Dixon (1981)	56
3.4 Ο αλγόριθμος $p-1$ του John Pollard (1974)	60
3.5 Ο αλγόριθμος Pollard Rho	62
<b>ΒΙΒΛΙΟΓΡΑΦΙΑ</b>	66

## ΠΕΡΙΛΗΨΗ

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η μελέτη αλγορίθμων πιστοποίησης πρώτων και παραγοντοποίησης .

Η ανάπτυξη του θέματος πραγματοποιείται σε τρία κεφάλαια. Στο πρώτο κεφάλαιο παρατίθενται βασικά θεωρήματα που μας βοηθάνε να ελέγξουμε αν ένας ακέραιος  $n$  είναι πρώτος καθώς και βασικά στοιχεία από την θεωρία αριθμών όπως οι γραμμικές ισοδυναμίες οι ισοδυναμίες δευτέρου βαθμού τα τετραγωνικά υπόλοιπα και οι πρωταρχικές ρίζες.

Στο δεύτερο κεφάλαιο γίνεται παρουσίαση των βασικών αλγορίθμων που χρησιμοποιούνται για την πιστοποίηση πρώτων. Γίνεται αναφορά στο θεώρημα του Fermat, στον αλγόριθμο του Fermat και στο επαναληπτικό κριτήριο του Fermat. Στην συνέχεια γίνεται εκτενή αναφορά στο κριτήριο του Miller Rabin και Soloway-Strassen, στον αλγόριθμο Miller Rabin και στον αλγόριθμο Soloway –Strassen.

Στο τρίτο κεφάλαιο παρατίθενται η μέθοδος παραγοντοποίησης του Fermat και του Euler και στην συνέχεια γίνεται αναφορά στον αλγόριθμο παραγοντοποίησης του Dixon και τον αλγόριθμο  $p-1$  του John Pollard.

## ABSTRACT

The scope of this dissertation is the study of the prime factorization and the identification of prime numbers. The aim is to present and understand the algorithms used for the identification of primes and analyze the basics of prime factorization.

The dissertation is structured to three chapters.

The first chapter presents the basic theorems used to determine whether a number  $n$  is a prime or not. Additionally the basics from the number theory like linear congruence, second-degree congruence, quadratic residues as well as primitive roots are referenced.

The second chapter cites the basic algorithms that are used for prime numbers identification. The Fermat theorem is presented focused on the Fermat algorithm and the repetitive criteria. Extensive reference is made to Soloway-Strassen and Miller-Rabin primality test and especially to the Miller-Rabin and Soloway-Strassen algorithms.

Finally, the last chapter is about prime factorization algorithms. Fermat and Euler's algorithms are studied as well as Dixon's factorization algorithm and John Pollard's  $p-1$  algorithm.

# ΚΕΦΑΛΑΙΟ 1

## ΣΤΟΙΧΕΙΑ ΑΠΟ ΤΗΝ ΘΕΩΡΙΑ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ

### 1.1 Εισαγωγή

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

**Πρόταση 1.1** (Πουλάκης, 2006: 97): *Αν  $n$  είναι ένας σύνθετος θετικός ακέραιος, τότε έχει ένα πρώτο διαιρέτη  $p$  με  $p \leq \sqrt{n}$ .*

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

**Παράδειγμα 1.1** (Πουλάκης, 2006: 97-98): Θα χρησιμοποιήσουμε την παραπάνω μέθοδο για να διαπιστώσουμε αν ο ακέραιος  $n = 2593$  είναι πρώτος. Έχουμε  $50 < \sqrt{2593} < 51$ . Βρίσκουμε εύκολα ότι κανένας πρώτος  $< 50$  δεν διαιρεί τον  $n$ . Συνεπώς, σύμφωνα με την Πρόταση 1.1, ο  $n$  είναι πρώτος.

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

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

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

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

## 1.2 Θεώρημα του Lucas

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

**Θεώρημα 1.2** (Πουλάκης, 2006: 98-99): Ας είναι  $n$  ένας περιττός θετικός ακέραιος. Τότε ο  $n$  είναι πρώτος, αν και μόνον αν υπάρχει ακέραιος  $a$  με  $(a, n) = 1$  τέτοιος, ώστε

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

για κάθε πρώτο διαιρέτη του  $p$  του  $n-1$

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

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

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

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

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

**Παράδειγμα 1.2** (Πουλάκης, 2006: 99): Θεωρούμε τον αριθμό

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

και κάνουμε τους εξής υπολογισμούς

$$\begin{aligned} 2^{n-1} &\equiv 1 \pmod n, & 2^{n-1/2} &\equiv -1 \pmod n, \\ 2^{n-1/3} &\equiv 7009340 \pmod n, & 2^{n-1/5} &\equiv 390964 \pmod n, \\ 2^{n-1/7} &\equiv 6654420 \pmod n, & 2^{n-1/101} &\equiv 6577006 \pmod n. \end{aligned}$$

Σύμφωνα με το θεώρημα 1.1, ο 11135251 είναι πρώτος.

### 1.3 Γραμμικές Ισοδυναμίες

Στη παράγραφο αυτή θα εξετάσουμε τη λύση πρωτοβάθμιων ισοδυναμιών και θα δούμε τα βασικά θεωρήματα της θεωρίας αριθμών συγκεκριμένα το θεώρημα του Euler, το μικρό θεώρημα του Fermat και το θεώρημα του Wilson. Επίσης θα εξετάσουμε την λύση ενός συστήματος πρωτοβαθμίων ισοδυναμιών. Ένα τέτοιο πρόβλημα τέθηκε τον 1<sup>ο</sup> αιώνα μ.Χ. από τον Κινέζο μαθηματικό Sun-Tsu και έχει γίνει γνωστό σαν το κινέζικο θεώρημα υπολοίπων (Chinese remainder theorem(KΘΥ)).

Μπορούμε εύκολα να μετατρέψουμε την διοφαντική εξίσωση σε γραμμική ισοδυναμία παρατηρώντας ότι θέλουμε στην ουσία να βρούμε για ποιες τιμές του  $x$

η παράσταση  $\frac{ax-c}{b}$  ισούται με ακέραιο αριθμό. Δηλαδή για ποιες τιμές του  $x$



ισχύει η σχέση  $ax-c \equiv \text{πολ}b$  δηλαδή η ισοδυναμία  $ax \equiv c \pmod{b}$ .

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

$$an \equiv b \pmod{c}. \quad (1)$$

Παρατηρούμε ότι αν ο  $n$  ικανοποιεί την ισοδυναμία τότε όλοι οι ακέραιοι της μορφής  $n+kc$  την ικανοποιούν διότι  $a(n+kc) \equiv an+akc \equiv an \equiv b \pmod{c}$ .

**Παράδειγμα 1.3** (Κουκουβίνος - Παπαϊωάννου, 2007: 33): Αν  $a=5$ ,  $b=3$ ,  $c=8$  η ισοδυναμία  $5n \equiv 3 \pmod{8}$  έχει την λύση  $n=7$ . Επίσης όλοι οι αριθμοί του συνόλου  $\{-9, -1, 7, 15, 23, \dots\}$  ικανοποιούν την ισοδυναμία.

Βλέπουμε λοιπόν ότι αν υπάρχει μία λύση της ισοδυναμίας (1) τότε υπάρχουν άπειρες. Όμως όλες αυτές οι λύσεις είναι ισοδύναμες  $\pmod{c}$ .

Μπαίνει λοιπόν και ένα δεύτερο ερώτημα υπάρχουν λύσεις που να μην είναι ισοδύναμες  $\pmod{cn}$ ; και αν ναι πόσες είναι αυτές;

Θα απαντήσουμε χρησιμοποιώντας τα όσα γνωρίζουμε για Διοφαντικές εξισώσεις.

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

$$an+(-c)k=b \quad (2)$$

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

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

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

Από τις άπειρες τιμές του  $n$  που δίνει η σχέση (3) παρατηρούμε ότι οι  $d$  τιμές  $n,$

$n_0 + \frac{c}{d}, n_0 + \frac{2c}{d}, \dots, n_0 + (d-1)\frac{c}{d}$  είναι μη ισοδύναμες  $\pmod{c}$  διότι προφανώς το

απόλυτο της διαφοράς δύο οιονδήποτε από αυτές είναι μικρότερο του  $c$ .

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

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

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

**Θεώρημα 1.3** (Κουκουβίνος - Παπαϊωάννου, 2007: 35): Αν  $d = \text{MKΔ}(a, c)$  τότε η ισοδυναμία  $ax = b \pmod{c}$  δεν έχει λύση αν  $d \nmid b$  και έχει  $d$  μη ισοδύναμες λύσεις αν  $d \mid b$ .

**Παράδειγμα 1.4** (Κουκουβίνος - Παπαϊωάννου, 2007: 35): 1) Η ισοδυναμία που είδαμε στο προηγούμενο παράδειγμα  $5x = 3 \pmod{8}$  επειδή  $\text{MKΔ}(5, 8) = 1$  και  $1 \mid 3$  έχει λύση και όλες οι λύσεις της είναι ισοδύναμες.

2) Η ισοδυναμία  $21x = 11 \pmod{3}$  αφού  $d = 3 = \text{MKΔ}(21, 3)$  και  $3 \nmid 11$  δεν έχει λύση.

3) Η ισοδυναμία  $15x = 9 \pmod{12}$  αφού  $d = \text{MKΔ}(15, 12) = 3$  και  $3 \mid 9$  θα έχει 3 μη ισοδύναμες λύσεις.

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

$$x = 3 + \frac{12}{3}t = 3 + 4t, \quad t \in \mathbb{Z}.$$

Οι 3 διαφορετικές λύσεις δίνονται για τις τιμές  $t = 0, 1, \dots, d-1$  ήτοι  $t = 0, 1, 2$  και είναι οι

$$x = 3$$

$$x = 7$$

$$x = 11.$$

Θα εφαρμόσουμε το Θεώρημα 1.3 για  $b = 1$ . Πρώτα όπως δίνουμε δύο ορισμούς.

Λέμε ότι η **λύση μίας γραμμικής ισοδυναμίας είναι μοναδική**  $\pmod{c}$  αν κάθε λύση  $n'$  της είναι ισοδύναμη με την  $n \pmod{c}$  (όπως η πρώτη ισοδυναμία του προηγούμενου παραδείγματος).

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

**Πόρισμα 1.4** (Κουκουβίνος - Παπαϊωάννου, 2007: 35): Αν  $\text{MKΔ}(a, c) = 1$  τότε ο  $a$  έχει αντίστροφο που είναι μοναδικός  $\pmod{c}$ .

**Απόδειξη:** Αν  $\text{MKΔ}(a, c) = 1$  τότε το Θεώρημα 1.3 λέει ότι η  $ax = 1 \pmod{c}$  έχει  $d = 1$  λύση που είναι μοναδική  $\pmod{c}$ .

**Παράδειγμα 1.5** (Κουκουβίνος - Παπαϊωάννου, 2007: 36): α) Αφού  $5^2 = 25 = 1 \pmod{8}$  ο 5 έχει έναν μόνο αντίστροφο, τον εαυτό του  $\pmod{8}$ . Προφανώς και ο -3 και ο 13 είναι αντίστροφοι του  $5 \pmod{8}$  που όμως είναι ισοδύναμες του 5 διότι -

$$3=5=13 \pmod{8}.$$

β) Ο αντίστροφος του  $a=2 \pmod{5}$  είναι ο 3 διότι  $2 \cdot 3 = 1 \pmod{5}$ .

Ο αντίστροφος του  $a=7 \pmod{9}$  είναι ο 4 διότι  $7 \cdot 4 = 1 \pmod{9}$ .

Ο αντίστροφος του  $a=12 \pmod{17}$  είναι ο 10 διότι  $12 \cdot 10 = 1 \pmod{17}$ .

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

**Θεώρημα (Euler) 1.5** (Κουκουβίνος - Παπαϊωάννου, 2007: 36): Αν ο ΜΚΔ  $(a,m)=1$  τότε  $a^{\varphi(m)} = 1 \pmod{m}$ .

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

Μπορούμε λοιπόν να αντιστοιχίσουμε κάθε αριθμό  $ar_i$ , με κάποιον  $r_j$  έτσι ώστε  $ar_i = r_j \pmod{m}$  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  $ar_i$ . Άρα

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

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

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

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

**Πόρισμα (Μικρό Θεώρημα του Fermat) 1.6** (Κουκουβίνος - Παπαϊωάννου, 2007: 37): Αν ο  $p$  πρώτος τότε  $n^p = n \pmod{p}$ .

**Απόδειξη:** Αν  $p \mid n$  τότε  $n^p = 0 = n \pmod{p}$ .

Αν  $p \nmid n$  τότε  $\text{MKΔ}(p,n)=1$ .

Άρα από το θεώρημα του Euler  $n^{p-1} \equiv 1 \pmod{p}$  διότι  $\varphi(p)=p-1$   
και αν πολλαπλασιάσουμε και τα δύο μέλη επί η έχουμε  $n^p \equiv n \pmod{p}$ .

**Θεώρημα (Wilson) 1.7** (Κουκουβίνος - Παπαϊωάννου, 2007: 37-38):

Η ισοδυναμία  $(m-1)! \equiv -1 \pmod{m}$  ισχύει αν και μόνο αν ο  $m$  είναι πρώτος.

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

**Απόδειξη:** Υποθέτουμε ότι ο  $m$  είναι πρώτος και θεωρούμε τους  $m-1$  ακεραίους  $1, 2, \dots, m-1$ .

Αν  $a$  κάποιος από τους αριθμούς αυτούς τότε υπάρχει ο αντίστροφος  $\bar{a}$  αυτού με  $1 \leq \bar{a} \leq m-1$  και  $a\bar{a} \equiv 1 \pmod{m}$ .

Πιθανόν  $a = \bar{a}$  δηλαδή  $a^2 \equiv 1 \pmod{m}$  δηλαδή ο  $a$  να συμπίπτει με τον αντίστροφό του. Όμως στην περίπτωση αυτή  $a^2 - 1 = km$

$$(a-1)(a+1) = km \text{ ήτοι } m|(a-1)(a+1) \text{ και αφού ο } m \text{ είναι πρώτος}$$

θα ισχύει:

$$m|a-1 \text{ είτε } m|a+1 \text{ άρα } a \equiv \pm 1 \pmod{m}.$$

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

Για παράδειγμα αν  $m=11$  γράφουμε

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

Έχουμε λοιπόν

$$(m-1)! = (m-1)(m-2)! = (m-1) \cdot 1 \cdot 1 \dots \pmod{m} \equiv -1 \pmod{m}.$$

**Αντίστροφα:** Έστω ότι ο  $m$  δεν είναι πρώτος. Τότε υπάρχει  $a: 1 < a < m$  με  $a|m$ .

Προφανώς επίσης  $a|(m-1)!$  (αφού ο παράγον  $a < m$  υπάρχει μέσα στο  $(m-1)!$ ).

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

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

$$a_1x = b_1 \pmod{m_1}$$

$$a_2x = b_2 \pmod{m_2}$$

$$\text{και } a_sx = b_s \pmod{m_s}$$

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

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

$A \equiv B \pmod{m}$  αν και μόνο αν ισχύουν οι ισοδυναμίες

$$A \equiv B \pmod{p_1^{\ell_1}}$$

$$A \equiv B \pmod{p_2^{\ell_2}}$$

..... και

$$A \equiv B \pmod{p_s^{\ell_s}}.$$

Δηλαδή η ισοδυναμία  $ax \equiv b \pmod{m}$  έχει το ίδιο σύνολο λύσεων με το σύστημα

$$ax \equiv b \pmod{p_1^{\ell_1}}$$

$$ax \equiv b \pmod{p_2^{\ell_2}} \quad (1)$$

$$ax \equiv b \pmod{p_s^{\ell_s}}$$

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

**Παράδειγμα 2.4** (Κουκουβίνος - Παπαϊωάννου, 2007: 39): Ας αντικαταστήσουμε την ισοδυναμία  $3x \equiv 11 \pmod{2275}$  με ένα γραμμικό σύστημα ισοδυναμιών με μικρότερα μέτρα.

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

$$3x \equiv 11 \pmod{25}$$

$$3x \equiv 11 \pmod{7}$$

και  $3x \equiv 11 \pmod{13}$  τις οποίες θα λύσουμε παρακάτω.

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

$$n \equiv 2 \pmod{3}$$

$$n \equiv 3 \pmod{5} \quad \text{και}$$

$$n \equiv 2 \pmod{7}.$$

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

**Θεώρημα (Κινέζικό Θεώρημα Υπολοίπων (ΚΘΥ)) 1.8** (Κουκουβίνος - Παπαϊωάννου, 2007: 40-41):

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

Τότε οι  $s$  ισοδυναμίες

$$a_1 x \equiv b_1 \pmod{m_1}$$

$$a_2 x \equiv b_2 \pmod{m_2}$$

..... και

$$a_s x \equiv b_s \pmod{m_s}$$

έχουν μία λύση μοναδική  $\pmod{M}$ .

**Απόδειξη:**

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

Επιλέγουμε ακεραίους  $c_1, c_2, \dots, c_s$  τέτοιους ώστε

$$a_i c_i \equiv b_i \pmod{m_i}$$

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

Θέτουμε τώρα  $n_i = \frac{N}{m_i}$  και επειδή όλοι οι  $m_i$  είναι πρώτοι προς αλλήλους έχουμε

ότι  $\text{MKΔ}(n_i, m_i) = 1$ . Αλλά τότε από το Πρόσχημα 2.2 ο  $n_i$  έχει έναν μοναδικό αντίστροφο  $\pmod{m_i}$ ; δηλαδή  $\exists \bar{n}_i$  με  $n_i \bar{n}_i \equiv 1 \pmod{m_i}, 1 \leq i \leq s$ .

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

$$\text{Έστω } x_0 = c_1 n_1 \bar{n}_1 + c_2 n_2 \bar{n}_2 + \dots + c_s n_s \bar{n}_s.$$

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

$$\begin{aligned} \text{Άρα } a_i x_0 &= a_i c_1 n_1 \bar{n}_1 + a_i c_2 n_2 \bar{n}_2 + \dots + a_i c_s n_s \bar{n}_s = \\ &= a_i c_i \bar{n}_i \text{ mod } m_i \\ &= a_i c_i \text{ mod } m_i \\ a_i x_0 &= b_i \text{ mod } m_i \end{aligned}$$

Άρα ο  $x_0$  είναι λύση και των  $s$  ισοδυναμιών.

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

$$x_0 = c_i = y \text{ mod } m_i \quad \text{Άρα } x_0 - y = \text{πολ} m_i \quad \text{για κάθε } m_i$$

αλλά όλα τα  $m_i$  είναι πρώτα μεταξύ τους άρα

$$\begin{aligned} x_0 - y = \text{πολ} m_1 m_2 \dots m_s \quad \text{ήτοι } x_0 - y = \text{πολ } M \quad \text{ήτοι} \\ y = x_0 \text{ mod } M \end{aligned}$$

**Παράδειγμα 1.6** (Κουκουβίνος - Παπαϊωάννου, 2007: 41-42): Θα χρησιμοποιήσουμε το Κινεζικό Θεώρημα για να λύσουμε το πρόβλημα του Sun Tsu, δηλαδή να βρούμε τον ελάχιστο θετικό  $x$  με

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5} \text{ και}$$

$$x \equiv 2 \pmod{7}.$$

Έχουμε με τον συμβολισμό του Κινεζικού Θεωρήματος  $a_1 = a_2 = a_3 = 1$   $b_1 = 2 = c_1$

$$b_2 = 3 = c_2 \quad b_3 = 2 = c_3, \quad m_1 = 3, \quad m_2 = 5, \quad m_3 = 7, \quad M = 105 \quad n_1 = 35 \quad n_2 = 21 \quad n_3 = 15.$$

Τώρα

$$35 \bar{n}_1 \equiv 1 \pmod{3} \Rightarrow 2 \bar{n}_1 \equiv 1 \pmod{3} \Rightarrow \bar{n}_1 = 2.$$

$$\text{Επίσης } 21 \bar{n}_2 \equiv 1 \pmod{5} \Rightarrow 1 \bar{n}_2 \equiv 1 \pmod{5} \Rightarrow \bar{n}_2 = 1$$

$$\text{και } 15 \bar{n}_3 \equiv 1 \pmod{7} \Rightarrow 1 \bar{n}_3 \equiv 1 \pmod{7} \Rightarrow \bar{n}_3 = 1, \quad \text{διότι}$$

$$15 \bar{n}_3 \equiv 1 \pmod{7} \Rightarrow 14 \bar{n}_3 + \bar{n}_3 \equiv -1 \pmod{7} \Rightarrow \bar{n}_3 - 1 \equiv \text{πολ} 7 \Rightarrow \bar{n}_3 = 1 \pmod{7}$$

Άρα μία λύση του συστήματος είναι η

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

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

$$\begin{array}{r|l} 233 & 105 \\ \hline 23 & 2 \end{array}$$

**Παράδειγμα 2.6** (Κουκουβίνος - Παπαϊωάννου, 2007: 42-43): θα λύσουμε την  
ισοδυναμία  $3x \equiv 11 \pmod{2275}$ , δηλαδή το σύστημα

$$3x \equiv 11 \pmod{25}$$

$$3x \equiv 11 \pmod{7} \quad 3x - 11 = \text{πολ}7$$

$$3x \equiv 11 \pmod{13} \quad 3x - 11 = \text{πολ}13$$

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

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

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

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

τώρα θα βρούμε  $\bar{n}_1, \bar{n}_2, \bar{n}_3$  με

$$\frac{2275}{25} \bar{n}_1 = 91 \bar{n}_1 = 1 \pmod{25} \Rightarrow 16 \bar{n}_1 = 1 \pmod{25},$$

$$\frac{2275}{7} \bar{n}_2 = 325 \bar{n}_2 = 1 \pmod{7} \Rightarrow 3 \bar{n}_2 = 1 \pmod{7},$$

$$\frac{2275}{13} \bar{n}_3 = 175 \bar{n}_3 = 1 \pmod{13} \Rightarrow 6 \bar{n}_3 = 1 \pmod{13}.$$

Η πρώτη έχει λύση  $\bar{n}_1 = 11$

Η δεύτερη έχει λύση  $\bar{n}_2 = 5$

Η τρίτη έχει λύση  $\bar{n}_3 = 11$

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

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

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



**Παράδειγμα 1.7** (Κουκουβίνος - Παπαϊωάννου, 2007: 43): Έστω ότι θέλουμε να βρούμε το  $7^{-1} \pmod{65}$ .

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

Το Κινέζικο θεώρημα δίνει

$$x = 3 \pmod{5} \Rightarrow x = 3$$

$$x = 3 \pmod{13} \Rightarrow x = 2$$

$$\text{Άρα θα λύσουμε το } \left(\frac{65}{5}\right)y_1 = 13y_1 = 1 \pmod{5} \Rightarrow y_1 = 2 \quad \text{και}$$

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

$$\text{Άρα } x_0 = \frac{65}{5}x_1y_1 + \frac{65}{13}x_2y_2 = 13 \cdot 3 \cdot 2 + 5 \cdot 2 \cdot 8 = 78 + 80 =$$

$$= 158 = 28 \pmod{65}.$$

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

Αναφέρουμε ότι το πρόβλημα του Sun Tsu αποδίδεται και στον σύγχρονό του (1<sup>ος</sup> αιώνας μ.Χ.) Νικόμαχο τον Γερασινό, έναν Έλληνα μαθηματικό που έγραψε την Αριθμητική Εισαγωγή. (Η Γέρασα ήκμασε τους πρώτους αιώνες μ.Χ. βρίσκεται στην Ιορδανία βόρεια του Αμμάν).

#### 1.4 Ισοδυναμίες Δευτέρου Βαθμού

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

έχουμε μία κυκλική ομάδα.

Ο ακέραιος  $g$  ονομάζεται αρχική ή πρωταρχική ρίζα  $\text{mod } p$ .

**Παράδειγμα 1.8** (Κουκουβίνος - Παπαϊωάννου, 2007: 44-45): Γνωρίζουμε ότι  $\varphi(10)=4$  και  $\{r_1=1, r_2=3, r_3=7, r_4=9\}$  περιορισμένο σύνολο υπολοίπων  $\text{mod } 10$ .

Πράγματι από τον ορισμό έχουμε

- i)  $\text{MK}\Delta(r_i, 10)=1 \quad \forall 1 \leq i \leq 4$ .
- ii)  $r_i \neq r_j \text{ mod } 10$  οπότε  $i \neq j$ .
- iii) κάθε αριθμός  $n$  με  $(n, 10)=1$  αντιστοιχεί σ' έναν  $r_i$ , ήτοι  $n \equiv r_i \text{ mod } 10$  για ένα μόνο  $i$ .

Παρατηρούμε ότι	$3^1=3=3 \text{ mod } 10$	$7^1=7=7 \text{ mod } 10$
	$3^2=9=9 \text{ mod } 10$	$7^2=49=9 \text{ mod } 10$
	$3^3=27=7 \text{ mod } 10$	$7^3=343=3 \text{ mod } 10$
	$3^4=81=1 \text{ mod } 10$	$7^4=2401 \text{ mod } 10$

δηλαδή τα σύνολα  $\{3^1, 3^2, 3^3, 3^4\}$  και  $\{7^1, 7^2, 7^3, 7^4\}$  αποτελούν περιορισμένα σύνολα υπολοίπων  $\text{mod } 10$ .

Το παράδειγμα αυτό σε συνδυασμό με την παρατήρηση ότι  $4=\varphi(10)$  είναι ο ελάχιστος ακέραιος  $h$  με την ιδιότητα  $g^h \equiv 1 \text{ mod } 10$  όταν  $g=3, 7$  μας οδηγεί στον ορισμό:

**Ορισμός 1.9** (Κουκουβίνος - Παπαϊωάννου, 2007: 45): Αν  $h$  είναι ο μικρότερος θετικός ακέραιος τέτοιος ώστε  $a^h \equiv 1 \text{ mod } m$  τότε λέμε ότι ο  $a$  ανήκει στον εκθέτη  $h$  modulo  $m$ .

**Θεώρημα 1.10** (Κουκουβίνος X.-Παπαϊωάννου A., 2007: 45): Μία ικανή και αναγκαία συνθήκη για να ισχύει  $a^b \equiv 1 \text{ mod } m$  για κάποιον ακέραιο  $b$  είναι η  $\text{MK}\Delta(a, m)=1$ .

**Απόδειξη:** Έστω  $\text{MK}\Delta(a, m)=d$ . Αν  $d|a$  και  $d|m$  τότε ο  $d$  διαιρεί την διαφορά τους  $a^b - \text{πολ}m=1$  ήτοι  $d|1$  άρα  $d=1$ .

**Αντίστροφα** αν  $\text{MK}\Delta(a, m)=1$  τότε  $a^{\varphi(m)} \equiv 1 \text{ mod } m$  από το θεώρημα του Euler οπότε  $b=\varphi(m)$ .

**Θεώρημα 1.11** (Κουκουβίνος - Παπαϊωάννου, 2007: 45): Αν ο  $a$  ανήκει στον εκθέτη  $h$  modulo  $m$  και  $a^r = 1 \pmod{m}$  τότε  $h|r$ .

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

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

**Ορισμός 1.12** (Κουκουβίνος - Παπαϊωάννου, 2007: 45): Αν ο ακέραιος  $g$  ανήκει στον εκθέτη  $\varphi(m) \pmod{m}$  τότε ο  $g$  ονομάζεται **αρχική ή πρωταρχική ρίζα**  $\pmod{m}$ .

**Θεώρημα 1.13** (Κουκουβίνος - Παπαϊωάννου, 2007: 45-46): Αν ο  $g$  είναι αρχική ρίζα  $\pmod{m}$  τότε οι δυνάμεις του  $g$  δηλαδή  $g, g^2, \dots, g^{\varphi(m)}$  είναι όλες μη ισοδύναμες  $\pmod{m}$  και αποτελούν ένα περιορισμένο σύνολο υπολοίπων  $\pmod{m}$ .

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

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

**Παράδειγμα 1.9** (Κουκουβίνος - Παπαϊωάννου, 2007: 46): Θα δείξουμε ότι δεν υπάρχουν πρωταρχικές ρίζες  $\pmod{8}$ . Έστω  $g$  μία τέτοια, αφού  $\varphi(8)=4$  η  $g$  θα ανήκει στον εκθέτη  $4 \pmod{8}$ . Από το θεώρημα 3.1 έχουμε  $\text{ΜΚΔ}(g,8)=1$  άρα  $g=1 \pmod{8}$  ή  $3 \pmod{8}$  ή  $5 \pmod{8}$  ή  $7 \pmod{8}$ .

Πράγματι  $1^4 = 1 \pmod{8}$                       αφού  $\varphi(8)=4$   
 $3^4 = 1 \pmod{8}$   
 $5^4 = 1 \pmod{8}$   
 $7^4 = 1 \pmod{8}$

όμως δεν είναι πρωταρχική ρίζα διότι **και**  $1^2 = 1 \pmod{8}$   
 $3^2 = 1 \pmod{8}$   
 $5^2 = 1 \pmod{8}$

$$7^2 = 1 \pmod{8}$$

άρα η  $g$  δεν ανήκει στον εκθέτη  $4 \pmod{8}$  άρα δεν υπάρχουν πρωταρχικές ρίζες  $\pmod{8}$ .

Ακολουθώς θα βρούμε έναν απλό τύπο για το πλήθος των αμοιβαία μη ισοδύναμων πρωταρχικών ριζών  $\pmod{8}$ .

**Θεώρημα 1.14** (Κουκουβίνος - Παπαϊωάννου, 2007: 46-47): Αν ο  $a$  ανήκει στον εκθέτη  $h \pmod{m}$  και  $\text{ΜΚΔ}(k, h) = d$  τότε ο  $a^k$  ανήκει στον εκθέτη  $h/d \pmod{m}$ .

**Απόδειξη:** Έστω ότι ο  $a^k$  ανήκει στον εκθέτη  $j \pmod{m}$ . Τότε  $a^{kj} = 1 \pmod{m}$ , άρα  $h|kj$ .

Θέτω  $h/d = h_1$  και  $k/d = k_1$  τότε η σχέση  $h|k \cdot j$  γίνεται  $h_1|k_1 j$ .

Και αφού  $\text{ΜΚΔ}(h, k) = d \Rightarrow \text{ΜΚΔ}(h_1, k_1) = 1$  οπότε η  $h_1|k_1 j$  δίνει  $h_1|j$ .

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

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

**Πόρισμα 1.15** (Κουκουβίνος - Παπαϊωάννου, 2007: 47): Αν  $g$  μια πρωταρχική ρίζα  $\pmod{m}$  τότε η  $g^r$  είναι επίσης μία πρωταρχική ρίζα  $\pmod{m}$  αν και μόνο αν  $\text{ΜΚΔ}(r, \varphi(m)) = 1$ .

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

$$\frac{\varphi(m)}{\text{ΜΚΔ}(r, \varphi(m))}$$

που ισούται με  $\varphi(m)$  αν και μόνο αν  $\text{ΜΚΔ}(r, \varphi(m)) = 1$ .

**Θεώρημα 1.16** (Κουκουβίνος - Παπαϊωάννου, 2007: 47): Αν υπάρχει κάποια πρωταρχική ρίζα  $\pmod{m}$  τότε το πλήθος των αμοιβαία μη ισοδύναμων πρωταρχικών ριζών είναι  $\varphi(\varphi(m))$ .

**Απόδειξη:** Έστω  $g$  μία πρωταρχική ρίζα  $\pmod{m}$ . Αλλά (Θ3.3) οι  $g, g^2, \dots, g^{\varphi(m)}$  είναι αμοιβαία μη ισοδύναμες και αποτελούν ένα περιορισμένο σύνολο υπολοίπων  $\pmod{m}$ . Από το προηγούμενο πόρισμα η  $g^r$  είναι πρωταρχική ρίζα αν και μόνο αν  $\text{ΜΚΔ}(r, \varphi(m)) = 1$ .

Όμως από τον ορισμό της συνάρτησης του Euler υπάρχουν  $\varphi(\varphi(m))$  αριθμοί στο διάστημα  $[1, \varphi(m)]$  σχετικά πρώτοι προς τον  $\varphi(m)$ .

**Παράδειγμα 1.9** (Κουκουβίνος - Παπαϊωάννου, 2007: 47): Αν  $m=10$  το Θεώρημα 3.6 λέει ότι έχουμε  $\varphi(\varphi(10))=\varphi(4)=2$  αμοιβαία μη ισοδύναμες πρωταρχικές ρίζες  $\text{mod } 10$ . Από το παράδειγμα 3.1 έχουμε ότι οι δύο είναι οι 3 και 7 με  $3 \neq 7 \text{ mod } 10$ .

Το Θεώρημα 3.7 είναι ειδική περίπτωση ενός γενικότερου θεωρήματος που υπολογίζει τις πρωταρχικές ρίζες  $\text{mod } p$ . Συγκεκριμένα θα δείξουμε ότι για κάθε πρώτο  $p$  υπάρχουν πρωταρχικές ρίζες  $\text{mod } p$ .

**Θεώρημα 1.17** (Κουκουβίνος - Παπαϊωάννου, 2007: 47-48): Για κάθε πρώτο  $p$ , υπάρχουν πρωταρχικές ρίζες  $\text{mod } p$ .

**Απόδειξη:** Θεωρούμε το περιορισμένο σύνολο υπολοίπων  $1, 2, \dots, p-1 \text{ mod } p$ . Συμβολίζω με  $N(h)$  το πλήθος των ακεραίων αυτών που ανήκουν στον εκθέτη  $h \text{ mod } p$ .

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

Επίσης γνωρίζουμε ότι κάθε στοιχείο ενός περιορισμένου συνόλου διαφόρων ανήκει σε κάποιο εκθέτη  $h \text{ mod } p$ . Άρα

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

Θα δείξουμε τώρα ότι  $N(h)=0$  ή  $\varphi(h)$ . Αν κανένας ακέραιος δεν ανήκει στο  $h \text{ mod } p$  τότε προφανώς  $N(h)=0$ . Αν  $a$  ανήκει στο  $h \text{ mod } p$  η εξίσωση

$$x^h = 1 \text{ mod } p \text{ έχει το πολύ } h \text{ μη ισοδύναμες λύσεις,}$$

όμως οι  $h$  αριθμοί  $a, a^2, \dots, a^h$  είναι αμοιβαία μη ισοδύναμες λύσεις της εξίσωσης άρα η  $x^h = 1 \text{ mod } p$  έχει ακριβώς  $h$  λύσεις. Άρα κάθε της λύση θα είναι ισοδύναμη με τον  $a^r$  για κάποιο  $r$ . Από το Πρόσχημα 3.5 ο  $a^r$  ανήκει στο  $h$  αν και μόνο αν  $\text{M.K.}\Delta.(r,h)=1$ . Άρα μεταξύ των αριθμών  $a, a^2, \dots, a^h$  υπάρχουν ακριβώς  $\varphi(h)$  αριθμοί που ανήκουν στον  $h \text{ mod } p$ . Άρα  $N(h)=\varphi(h)$  εδώ.

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

$$\sum_{d \mid n} \varphi(d) = n:$$

$$p-1 = \sum_{h \mid p-1} N(h) < \sum_{h \mid p-1} \varphi(h) = p-1 \text{ άτοπο.}$$

Άρα  $N(h)=\varphi(h)$  για όλα τα  $h$  που διαιρούν το  $p-1$ . Άρα  $\varphi(p-1)$  ακέραιοι ανήκουν στον εκθέτη  $p-1 \pmod{p}$  δηλαδή υπάρχουν  $\varphi(p-1)$  πρωταρχικές ρίζες  $\pmod{p}$ .

Υπενθυμίζουμε ότι αν  $p$  πρώτος  $\varphi(p)=p-1$ .

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

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

Για  $p=8, p=15$  δεν υπάρχουν πρωτ. ρίζες.

**Παράδειγμα 1.10** (Κουκουβίνος - Παπαϊωάννου, 2007: 49): Έστω  $p=5$ . Ένα περιορισμένο σύνολο υπολοίπων είναι το  $\{1,2,3,4\}$ . Από το Θ3.7 υπάρχουν πρωταρχικές ρίζες  $\pmod{5}$ . Άρα από το Θ3.6 θα υπάρχουν  $\varphi(\varphi(5))=\varphi(4)=2$  αμοιβαία μη ισοδύναμες πρωταρχικές ρίζες  $\pmod{5}$ .

Έχουμε	$2^1=2 \pmod{5}$	και	$3^1=3 \pmod{5}$
	$2^2=4 \pmod{5}$		$3^2=4 \pmod{5}$
	$2^3=3 \pmod{5}$		$3^3=2 \pmod{5}$
	$2^4=1 \pmod{5}$		$3^4=1 \pmod{5}$

Άρα οι ρίζες 2 και 3 είναι πρωταρχικές ρίζες  $\pmod{5}$ .

### 1.5 Τετραγωνικά Υπόλοιπα

**Ορισμός 1.18** (Κουκουβίνος - Παπαϊωάννου, 2007: 49): Έστω ο πρώτος  $p$  και  $\text{ΜΚΔ}(a,p)=1$ . Αν  $p \nmid a$  και η εξίσωση  $x^2=a \pmod{p}$  έχει λύση λέμε ότι ο  $a$  είναι τετραγωνικό υπόλοιπο  $\pmod{p}$ .

**Παράδειγμα 1.11** (Κουκουβίνος - Παπαϊωάννου, 2007: 49): Έστω  $p=7$ . Οι αριθμοί 1, 4, 9 είναι τέλεια τετράγωνα και δεν διαιρούνται με τον 7. Άρα είναι τετραγωνικά υπόλοιπα  $\pmod{7}$ . Αλλά και όλοι οι ακέραιοι που είναι ισοδύναμοι με τα τετράγωνα

αυτά mod7 είναι επίσης τετραγωνικά υπόλοιπα mod7 όπως οι 2, 11 κοκ. Ο 49 όμως αν και τέλειο τετράγωνο δεν είναι τετραγωνικό υπόλοιπο mod7 διότι  $7 \mid 49$ .

Το κριτήριο του Euler μας λέει πότε ακριβώς ένας αριθμός  $a$  είναι τετραγωνικό υπόλοιπο mod $p$ .

**Θεώρημα (Κριτήριο του Euler) 1.19** (Κουκουβίνος - Παπαϊωάννου, 2007: 50):

Έστω  $a \neq 0$ ,  $p > 0$  πρώτος και  $(a, p) = 1$

Ο αριθμός  $a$  είναι τετραγωνικό υπόλοιπο mod $p$  αν και μόνο αν  $a^{\frac{p-1}{2}} = 1 \pmod{p}$ .

**Απόδειξη:** Έστω ότι ο  $a$  είναι τετραγωνικό υπόλοιπο mod $p$  και έστω  $x$  ακέραιος με  $x^2 = a \pmod{p}$ .

Αφού  $p \nmid a \Rightarrow p \nmid x$  ήτοι  $\text{MK}\Delta(x, p) = 1$  άρα

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

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

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

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

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

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

Αν λοιπόν  $x=g^s$  έχουμε:  $x^2 = g^{2s} = g^r = a \pmod{p}$ .

Ένα πολύ χρήσιμο πόρισμα είναι το εξής

**Πόρισμα 1.20** (Κουκουβίνος - Παπαϊωάννου, 2007: 50): Έστω  $g$  μία πρωταρχική ρίζα mod $p$  και έστω  $\text{MK}\Delta(a, p) = 1$ . Έστω  $r$  ακέραιος με  $g^r = a \pmod{p}$ . Τότε ο  $r$  είναι ζυγός αν και μόνο αν το  $a$  είναι τετραγωνικό υπόλοιπο mod $p$ .

**Παράδειγμα 1.12** (Κουκουβίνος - Παπαϊωάννου, 2007: 50-51):

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

b)  $a=3$   $p=11$   $3^5 = 243 = 1 \pmod{11}$  άρα ο 3 είναι τετραγ. υπόλοιπο mod5.

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

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

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

$$\begin{cases} 1 \text{ αν ο } b \text{ είναι τετραγωνικό υπόλοιπο} \\ 0 \text{ αν } ob = \text{πολ}p \\ -1 \text{ στις άλλες περιπτώσεις} \end{cases}$$

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

ισοδυναμία  $x^2 = b \pmod{p}$  έχει λύση.

**Ιδιότητες:**

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

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

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

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

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

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

**Παράδειγμα 1.13** (Κουκουβίνος - Παπαϊωάννου, 2007: 51):

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

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

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

**Θεώρημα 1.21** (Κουκουβίνος - Παπαϊωάννου, 2007: 52): Αν  $p$  μονός πρώτος

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



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

**Απόδειξη:** Έστω  $p$  μονός πρώτος. Θα προσδιορίσω τα  $a$  με  $1 \leq a \leq p-1$  που είναι λύσεις της ισοδ.  $x^2 = a \pmod{p}$ .

Αλλά  $x^2 \equiv (p-x)^2 \pmod{p}$ .

[Πράγματι  $x^2 - (p-x)^2 = x^2 - p^2 + 2px - x^2 = \text{πολ}p$ ]. Τα τετράγωνα των αριθμών στα σύνολα  $\left\{1, 2, \dots, \frac{p-1}{2}\right\}$  και  $\left\{\frac{p+1}{2}, \frac{p+1}{2}+1, \dots, p-1\right\}$  είναι ισοδύναμα κατά ζεύγη [όχι με την σειρά που αναγράφονται].

Άρα εξετάζω μόνο για τις τιμές του  $x$  με  $1 \leq x \leq \frac{p-1}{2}$ .

Αλλά τα τετράγωνα των αριθμών στο σύνολο  $\left\{1, 2, \dots, \frac{p-1}{2}\right\}$  είναι όλα μη ισοδύναμα  $\pmod{p}$  διότι αλλιώς η  $x^2 = a \pmod{p}$  θα είχε 4 μη ισοδύναμες  $\pmod{p}$  λύσεις, πράγμα που αντίκειται στο θεώρημα του Lagrange: «Το πλήθος των μη ισοδύναμων λύσεων της ισοδυναμίας  $f(x) \equiv 0 \pmod{p}$  ποτέ δεν υπερβαίνει τον βαθμό  $f(x)$ ». Άρα τα  $\frac{p-1}{2}$  Q.R.  $\pmod{p}$  είναι ακριβώς οι αριθμοί  $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ .

**Παράδειγμα 1.14** (Κουκουβίνος - Παπαϊωάννου, 2007: 52-54):

α) Τα QR του 19 είναι αριθμοί της μορφής  
b, 19-b

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

$$8^2 = 7 \pmod{9}$$

$$11^2 = 121 = 7 \pmod{9}$$

$$9^2 = 5 \pmod{9}$$

$$10^2 = 100 = 5 \pmod{9}$$

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

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

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

$$2^2 = 4 \pmod{31} = 29^2$$

$$3^2 = 9 \pmod{31} = 28^2$$

$$4^2 = 16 \pmod{31} = 27^2$$

$$5^2 = 25 \pmod{31} = 26^2$$

$$6^2 = 5 \pmod{31} = 25^2$$

$$7^2 = 18 \pmod{31} = 24^2$$

$$8^2 = 2 \pmod{31} = 23^2$$

$$9^2 = 19 \pmod{31} = 22^2$$

$$10^2 = 7 \pmod{31} = 21^2$$

$$11^2 = 28 \pmod{31} = 20^2$$

$$12^2 = 20 \pmod{31} = 19^2$$

$$13^2 = 14 \pmod{31} = 18^2$$

$$14^2 = 10 \pmod{31} = 17^2$$

$$15^2 = 8 \pmod{31} = 16^2$$

$$\begin{aligned}
\gamma) \quad 1^2 &= 1 \pmod{29} = 28^2 & \text{QR}_{29} &= \{1,4,5,6,7,9,13,16,20,22,23,24,25,28\} \\
2^2 &= 4 \pmod{29} = 29^2 & \text{QNR}_{29} &= \{2,3,8,10,11,12,14,15,17,18,19,21,26,27\} \\
3^2 &= 9 \pmod{29} = 28^2 \\
4^2 &= 16 \pmod{29} = 27^2 \\
5^2 &= 25 \pmod{29} = 26^2 \\
6^2 &= 7 \pmod{29} = 25^2 \\
7^2 &= 20 \pmod{29} = 24^2 \\
8^2 &= 6 \pmod{29} = 23^2 \\
9^2 &= 23 \pmod{29} = 22^2 \\
10^2 &= 13 \pmod{29} = 21^2 \\
11^2 &= 5 \pmod{29} = 20^2 \\
12^2 &= 28 \pmod{31} = 19^2 \\
13^2 &= 24 \pmod{31} = 18^2 \\
14^2 &= 22 \pmod{31} = 17^2
\end{aligned}$$

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

Προηγούμενα εξετάζουμε ένα λήμμα:

**Λήμμα 1.22** (Κουκουβίνος - Παπαϊωάννου, 2007: 54): Αν  $p$  μονός πρώτος και  $(a,p)=1$  τότε είτε

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

**Απόδειξη:** Αφού  $p$  πρώτος και  $(a,p)=1$  από το θεώρημα του Fermat ισχύει  $a^{p-1} \equiv 1 \pmod{p}$  ή  $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$

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

Οπότε είτε  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$  είτε  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

**Θεώρημα (Κριτήριο του Euler) 1.23** (Κουκουβίνος – Παπαϊωάννου, 2007: 54-55):

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

**Απόδειξη:** Έστω μονός πρώτος  $p$  με  $(a,p)=1$  και  $1 \leq r \leq p-1$ . Αφού η ισοδυναμία  $rx \equiv a \pmod{p}$  έχει μοναδική λύση [(αφού  $(r,p)=1$ ] υπάρχει ακριβώς ένα στοιχείο  $s$  με  $1 \leq s < p-1$  έτσι ώστε  $rs \equiv a \pmod{p}$  [το στοιχείο  $s$  είναι η λύση της ισοδυναμίας].

**Περίπτωση 1:** Αν  $a$  είναι QNR  $\pmod{p}$  τότε  $\left(\frac{a}{p}\right) \equiv -1$  οπότε για τον  $s$  θα είναι

$r \neq s$  διότι αν  $r = s$ ,  $r^2 \equiv a \pmod{p}$  ήτοι  $a \text{ QR} \pmod{p}$  και τα στοιχεία του  $\{1, 2, \dots, p-1\}$

μπορούν να γίνουν ζεύγη  $r_i, s_i$  έτσι ώστε  $r_i \cdot s_i \equiv a \pmod{p}$   $i=1, 2, \dots, \frac{p-1}{2}$ .

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

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

Από Fermat  $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$  άρα

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

**1.6 Το σύμβολο του Jacobi** (Κουκουβίνος - Παπαϊωάννου, 2007: 100-101):

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

n. Για ακέραιους  $a$  έχουμε:

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

**Παρατηρήσεις:**

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

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

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

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

## 1.7 Πρωταρχικές Ρίζες

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

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

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

**Θεώρημα 1.24** (Κουκουβίνος - Παπαϊωάννου, 2007: 120): Αν  $\text{ord}_n(a) = k$  τότε

$$a^h = 1 \pmod n \text{ αν και μόνο αν } k | h.$$

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

Αντίστροφα αν  $k | h$  τότε  $kt = h$  και αφού  $\text{ord}_n(a) = k$  τότε

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

Το επόμενο θεώρημα μας δίνει την  $ord_n(a^m)$  αν γνωρίζουμε την  $ord_n(a)$ .

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

**Απόδειξη:** Έστω  $ord_n(a) = k$ ,

$$ord_n(a^m) = r,$$

$$\text{ΜΚΔ}(m, k) = d \Rightarrow m = bd, k = cd \text{ με } \text{ΜΚΔ}(b, c) = 1$$

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

Αφού  $ord_n(a) = k$  έχουμε  $(a^{mr}) = (a^m)^r = 1 \pmod n$ . Από το θεώρημα 4.1 έχουμε  $k | mr$  ήτοι  $cd | (bd)r \Rightarrow c | br$ . Αφού όμως  $(c, b) = 1 \Rightarrow c | r$ . (2)

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

Το Θεώρημα 4.1 λέει ότι η τάξη κάθε στοιχείου modulo έναν πρώτο είναι διαιρέτης του  $p-1$ . Το Θεώρημα 4.2 λέει επιπλέον ότι αν  $d$  διαιρέτης του  $p-1$  υπάρχουν  $\varphi(d)$  μη ισοδύναμοι ακέραιοι mod  $p$  που έχουν τάξη  $d$ .

**Παράδειγμα 1.15** (Κουκουβίνος - Παπαϊωάννου, 2007: 121): Για  $p = 17$ , ο 8 είναι διαιρέτης του  $p - 1 = 16$ .

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

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

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

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

Άμεσα πορίσματα των δύο αυτών θεωρημάτων είναι τα:

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

Έχουμε ένα κριτήριο πιστοποίησης πρώτων για τους αριθμούς Fermat που προτάθηκε τον 19<sup>ο</sup> αιώνα από τον Γάλλο J. Pepin.

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

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

Ο QRL δίνει  $\left(\frac{3}{F_n}\right) \cdot \left(\frac{F_n}{3}\right) = 1$  αφού  $F_n = 1 \pmod 4$  αλλά

$\left(\frac{3}{F_n}\right) \cdot \left(\frac{F_n}{3}\right) = \left(\frac{3}{F_n}\right) \cdot \left(\frac{2}{3}\right) = \left(\frac{3}{F_n}\right) \cdot (-1)^{\frac{9-1}{8}} = \left(\frac{3}{F_n}\right) \cdot (-1)$ . Άρα  $\left(\frac{3}{F_n}\right) = -1$  και από το

κριτήριο του Euler  $3^{\frac{F_n-1}{2}} = -1 \pmod{F_n}$

**Αντίστροφα:** Έστω  $3^{\frac{F_n-1}{2}} = -1 \pmod{F_n}$ . Έστω  $p$  πρώτος διαιρέτης του  $F_n$  (άρα ο

$F_n$  όχι πρώτος) οπότε  $3^{\frac{F_n-1}{2}} = -1 \pmod p$  (αφού  $p \nmid F_n$ ). Τετραγωνίζοντας έχουμε  $3^{F_n-1} = 1 \pmod p$ . Αν  $\text{ord}_p(3) = m$  από το θεώρημα 4.1  $m \mid F_n - 1$  ήτοι (ορισμός αριθμών Fermat)  $m \mid 2^{2^n}$ . Άρα  $m = 2^r$  με  $0 \leq r \leq 2^n$ . Έστω  $r = 2^n - s$  με  $s > 0$ .

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

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

Άρα  $s = 0$  και το 3 έχει τάξη  $m = 2^r = 2^{2^n} \pmod p$ . Από το θεώρημα 4.1  $2^{2^n} \mid p-1$  άρα  $2^{2^n} \leq p-1$  που γίνεται αν προσθέσω την μονάδα  $F_n \leq p$ . αν  $p$  πρώτος διαιρέτης του  $F_n \Rightarrow F_n = p$  ήτοι  $F_n$  πρώτος.

Οι πρώτοι πέντε αριθμοί Fermat είναι

$$\text{για } n = 0 \quad F_0 = 2^{2^0} + 1 = 3$$

$$n = 1 \quad F_1 = 2^{2^1} + 1 = 5$$

$$n = 2 \quad F_2 = 2^{2^2} + 1 = 17$$

$$n = 3 \quad F_3 = 2^{2^3} + 1 = 257$$

$$n = 4 \quad F_4 = 2^{2^4} + 1 = 65.537$$

$$n = 5 \quad F_5 = 2^{2^5} + 1 = 4.294.967.297 = 641 \cdot 6.700.417 .$$

Ο Fermat έκανε την εικασία ότι  $F_n$  πρώτος για κάθε  $n$  αλλά ο Euler έδειξε ότι ο  $F_5$  παραγοντοποιείται. Σήμερα είναι γνωστό ότι  $F_n$  σύνθετος για  $5 \leq n \leq 23$  αλλά δεν γνωρίζουμε τι γίνεται για  $F_n$  με  $n \geq 24$ .

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

Δηλαδή για κάθε ακέραιο  $r$  με  $1 < q \leq n-1$  και με  $\text{MKΔ}(q, n) = 1$  υπάρχει  $k$  με  $q^k = r$ . Στην περίπτωση αυτή ο  $q$  βοηθά στο να βρίσκουμε την τάξη των στοιχείων του περιορισμένου συνόλου υπολοίπων αλλά και τα  $QR$  και  $QNR$  του  $n$ .

Ονομάζουμε ένα φυσικό  $q$  **πρωταρχική** (ή αρχική) **ρίζα** αν  $\text{ord}_n(q) = \varphi(n)$ . Θα δείξουμε ότι οι πρωταρχικές ρίζες του  $n$  παράγουν το περιορισμένο σύνολο υπολοίπων  $\pmod n$ .

**Θεώρημα 1.27** (Κουκουβίνος - Παπαϊωάννου, 2007: 124): Αν ο  $q$  είναι πρωταρχική ρίζα του  $n$  τότε τα  $q, q^2, \dots, q^{\varphi(n)}$  αποτελούν ένα περιορισμένο σύνολο υπολοίπων  $\pmod n$ .



**Απόδειξη:** Αφού  $q$  πρωταρχική ρίζα  $\Rightarrow \text{ord}_n(q) = \varphi(n)$  οπότε  $\text{MK}\Delta(q, n) = 1$ . Άρα  $\text{MK}\Delta(q^i, n) = 1$  για  $i = 1, 2, \dots, \varphi(n)$ . Άρα τα  $q, q^2, \dots, q^{\varphi(n)}$  είναι  $\varphi(n)$  το πλήθος φυσικοί μη ισοδύναμοι μεταξύ τους. Πράγματι αν  $q^i = q^j \pmod n$  με  $1 \leq i < j \leq \varphi(n)$  τότε από το δεύτερο πόρισμα  $i = j \pmod{\varphi(n)}$  οπότε  $\varphi(n) \mid j - i$ . Άτοπο διότι  $0 < j - i < \varphi(n)$ , οπότε οι δυνάμεις του  $q, q^2, \dots, q^{\varphi(n)}$  αποτελούν ένα περιορισμένο σύνολο υπολοίπων  $\pmod n$ .

Το 1769 ο J. Lambert μελετώντας τα δεκαδικά αναπτύγματα του  $\frac{1}{p}$  ( $p$  πρώτος) απέδειξε το παρακάτω θεώρημα και ισχυρίστηκε ότι υπάρχουν πρωταρχικές ρίζες του  $p$  για κάθε πρώτο  $p$ . Ο Euler εισήγαγε τον όρο πρωταρχική ρίζα το 1773 και έδειξε ότι υπάρχουν  $\varphi(p - 1)$  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  $p - 1$ . Ο Gauss επίσης έδειξε το παρακάτω θεώρημα.

**Θεώρημα:** (Κουκουβίνος - Παπαϊωάννου, 2007: 124-125):

Υπάρχουν πρωταρχικές ρίζες  $\pmod n$  για  $n = 2, 4, p, p^k, 2p^k$  όπου  $p$  μονός πρώτος και  $k$  φυσικός.

**Θεώρημα (Lambert) 1.28** (Κουκουβίνος - Παπαϊωάννου, 2007: 125):

Αν  $p$  μονός πρώτος,  $h$  φυσικός και  $q$  πρώτος τέτοιος ώστε  $q^h \mid p - 1$  τότε υπάρχει φυσικός  $b$  με  $\text{ord}_p(b) = q^h$ .

**Απόδειξη:** Αφού  $p \geq 3$ , από το θεώρημα του Lagrange [Υπενθύμιση: το πλήθος των μη ισοδύναμων λύσεων της πολυωνυμικής εξίσωσης  $f(x) = 0 \pmod p$  δεν υπερβαίνει

το βαθμό του πολυωνύμου  $f(x)$ ] η εξίσωση  $x^q = 1 \pmod p$  έχει το πολύ  $\frac{p-1}{q}$

λύσεις όπου  $\frac{p-1}{q} \leq \frac{p-1}{2} \leq p-2$ . Άρα τουλάχιστον ένα στοιχείο, έστω το  $a$ , με

$1 \leq a \leq p-1$  και  $\text{MK}\Delta(a, p) = 1$  δεν είναι λύση. Άρα  $a^{\frac{p-1}{q}} \neq 1 \pmod p$ . Θέτουμε  $b = a^{\frac{p-1}{q}}$  και επίσης θέτουμε  $\text{ord}_p(b) = m$ . Ισχύει:  $b^{q^h} = a^{p-1} \pmod p = 1 \pmod p$  και το θεώρημα 4.1 λέει ότι  $m \mid q^h$ . Έστω ότι  $m < q^h$ . Αφού ο  $q$  πρώτος  $m \mid q^{h-1}$  άρα υπάρχει ακέραιος  $k$  με  $q^{h-1} = mk$ . Άρα

$$a^{\frac{p-1}{q}} = b^{q^{h-1}} \pmod p = b^{mk} = (b^m)^k = 1^k = 1 \pmod p \text{ άτοπο διότι } a^{\frac{p-1}{q}} \neq 1 \pmod p. \text{ Άρα } m = q^h = \text{ord}_p(b).$$

**Θεώρημα 1.29** (Κουκουβίνος - Παπαϊωάννου, 2007: 125-126): Δεν υπάρχουν πρωταρχικές ρίζες του  $2^n$  για  $n > 2$ .

**Απόδειξη:** Θα δείξουμε επαγωγικά ότι αν  $\text{MK}\Delta(a, 2^n) = 1$  για  $n > 2$ , τότε  $\text{ord}_{2^n}(a) = 2^{n-2}$ , άρα ο  $a$  δεν είναι πρωταρχική ρίζα του  $2^n$ .

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

Για  $n = 3$  και  $\text{MK}\Delta(a, 2^3) = 1$  είναι  $a = 1, 3, 5, 7 \pmod 8$ , αλλά ισχύει

$$\left. \begin{array}{l} 1^2 = 1 \pmod 8 \\ 3^2 = 1 \pmod 8 \\ 5^2 = 1 \pmod 8 \\ 7^2 = 1 \pmod 8 \end{array} \right\} \text{Άρα αν } \text{MK}\Delta(a, 8) = 1 \text{ τότε } \text{ord}_8(a) = 2 = 2^{3-2},$$

δηλαδή το θεώρημα ισχύει για  $n = 3$ .

Έστω λοιπόν  $k > 3$  και αν  $\text{MK}\Delta(m, 2^k) = 1$  για θετικό  $m$  τότε  $\text{ord}_{2^k}(m) = 2^{k-2}$  ήτοι

$$m^{2^{k-2}} = 1 \pmod{2^k} \text{ και } m^s \neq 1 \pmod{2^k} \text{ για } 1 \leq s < 2^{k-2}.$$

Έστω τώρα  $b$ :  $\text{MK}\Delta(b, 2^{k+1}) = 1$  οπότε και  $(b, 2^k) = 1$  και από την επαγωγική

υπόθεση  $\text{ord}_{2^k}(b) = 2^{k-2}$ . Δηλαδή υπάρχει ακέραιος  $r$  με  $b^{2^{k-2}} = 1 \pmod{2^k}$  ήτοι

$$b^{2^{k-2}} = 1 + r \cdot 2^k.$$

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

Υπάρχει ακέραιος  $s$  με  $b^s = 1 \pmod{2^{k+1}}$  και  $1 \leq s < 2^{k-1}$ ; όχι διότι τότε  $b^s = 1+t \cdot 2^{k+1} = 1+2t \cdot 2^k$  ήτοι  $b^s = 1 \pmod{2^k}$ . Άρα αν  $\text{MK}\Delta(b, 2^{k+1}) = 1 \Rightarrow \text{ord}_{2^{k+1}}(b) = 2^{k-1}$  και η επαγωγική απόδειξη ολοκληρώθηκε.

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

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

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

Τότε  $t_k = s_{t_{k-1}} \pmod p$  για  $1 \leq k \leq p-1$ .

Ο αλγόριθμος του Crelle δουλεύει διότι

$$a^{j-1} \cdot a = a^j \pmod p \quad (1 \leq i < j \leq p-1).$$

**Παράδειγμα 1.16** (Κουκουβίνος - Παπαϊωάννου, 2007: 127):

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

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

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

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

Άρα  $3^3 = 3 \cdot 9 = 10 \pmod{17}$ ,  $3^4 = 3 \cdot 10 = 13 \pmod{17}$ ,

Αφού η μικρότερη τιμή του  $k$   $1 \leq k \leq 16$  που δίνει  $3^k = 1 \pmod{17}$  είναι η  $k=16$  το 3 είναι πρωταρχική ρίζα του 17.

**Θεώρημα 1.30** (Κουκουβίνος - Παπαϊωάννου, 2007: 128): Αν  $p$  μονός πρώτος τότε υπάρχουν  $\phi(p-1)$  πρωτ. ρίζες  $\pmod p$ .

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

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

Αν λοιπόν  $q$  πρωτ. ρίζα του  $p$  υπάρχουν  $\varphi(p - 1)$  μη ισοδύναμες πρωτ. ρίζες του

$p$  που δίνονται από την:  $q_1^{a_1}, q_2^{a_2}, \dots, q_r^{a_{\varphi(p-1)}}$  όπου οι  $\varphi(p - 1)$  φυσικοί μικρότεροι του  $p - 1$  είναι πρώτοι προς τον  $p - 1$ .

**Παράδειγμα 1.17** (Κουκουβίνος - Παπαϊωάννου, 2007: 129): Οι πρωταρχικές ρίζες του 17 είναι  $\varphi(16) = 16 \cdot \frac{1}{2} = 8$ .

Είδαμε ότι το 3 είναι πρωταρχική ρίζα του 17.

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

**Παράδειγμα 1.18** (Κουκουβίνος - Παπαϊωάννου, 2007: 129): Υπολογίστε όλους τους φυσικούς που έχουν ακριβώς 1 πρωτ. ρίζα.

$\varphi(\varphi(m)) = 1$  συνεπάγεται  $\begin{cases} \text{είτε } \varphi(m) = 1 \Rightarrow m = 1 \\ \text{είτε } \varphi(m) = 2 \Rightarrow m = 2, 3, 4, 6. \end{cases}$

**Θεώρημα 1.31** (Κουκουβίνος - Παπαϊωάννου, 2007: 129-130): Αν  $q$  πρωταρχική ρίζα του  $p$  τα  $QR$  του  $p$  δίνονται από την παράσταση  $q^{2^k}$  και τα  $QNR$  από την

$$q^{2^{k-1}} \quad 0 \leq k \leq \frac{p-1}{2}.$$

**Απόδειξη:** Αν  $q$  πρωτ. ρίζα  $\pmod p$  με  $\text{ΜΚΔ}(q, p) = 1$  έχουμε:

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

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

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

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

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

$$1 \qquad 2$$

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

**Παράδειγμα 1.19:** (συνέχεια) (Κουκουβίνος - Παπαϊωάννου, 2007: 130):

Τα QR του 17 είναι λοιπόν

$$3^0 = 1, 3^2 = 9, 3^4 = 13, 3^6 = 15, 3^8 = 16, 3^{10} = 8, 3^{12} = 4, 3^{14} = 2, 3^{16} = 1.$$

**Θεώρημα 1.32** (Κουκουβίνος - Παπαϊωάννου, 2007: 130): Μία αναγκαία συνθήκη

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

**Απόδειξη:** Έστω  $\text{MK}\Delta(a, b) = 1$  και  $b$  λύση της  $x^m = a \pmod{p}$ . Από το θεώρημα του

$$\text{Fermat} \quad a^{\frac{p-1}{d}} = a^{\frac{(p-1)m}{md}} = b^{(p-1)\frac{m}{d}} = \left( b^{(p-1)} \right)^{\frac{m}{d}} = 1 \pmod{p}.$$

**Παράδειγμα 1.20** (Κουκουβίνος - Παπαϊωάννου, 2007: 130-131):

i) Η  $x^7 = 15 \pmod{29}$  δεν επιλύεται:

Έχω  $m = 7$ ,  $a = 15$ ,  $p = 29$ ,  $d = \text{MK}\Delta(7, 28) = 7$ .

$$15^4 \neq 1 \pmod{29} \text{ πράγματι } 15^4 = 50.625 = 10 \pmod{29}.$$

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

$$m = 16, a = 8, p = 73, d = \text{MK}\Delta(16, 72) = 8$$

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

Βρίσκω μία πρωτ. ρίζα του 73.

$$5^6 = 3 \pmod{73}, 5^{24} = 3^4 = 8 \pmod{73}$$

$$5^{72} = (5^{24})^3 = 8^3 = 1 \pmod{73} \text{ άρα } q=5.$$

Η εξίσωση  $5^s = 8 \pmod{73}$  έχει λύση  $s = 24$ . Η ρίζα είναι λοιπόν  $x = 5^6 = 3 \pmod{73}$ .

$$\text{Πράγματι } 3^{16} \pmod{73} = (3^4)^4 = 81^4 = 8^4 = 4096 = 8 \pmod{73}.$$

## ΚΕΦΑΛΑΙΟ 2

### ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΩΤΩΝ

#### 2.1 Το Θεώρημα του Fermat

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

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

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

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

**Ορισμός 2.1** (Κουκουβίνος - Παπαϊωάννου, 2007: 78): Ο  $a$ ,  $1 \leq a < n$ , ονομάζεται **F-μάρτυρας** για το  $n$  αν  $a^{n-1} \bmod n \neq 1$ .

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

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

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

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

Γενικεύοντας έχουμε τον ορισμό:

**Ορισμός 2.2** (Κουκουβίνος - Παπαϊωάννου, 2007: 79): Για έναν (μονό) σύνθετο αριθμό  $n$  ένα στοιχείο  $1 \leq a \leq n - 1$  είναι F-ψεύτης αν  $a^{n-1} \bmod n = 1$ .

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

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

**Λήμμα 2.3** (Κουκουβίνος - Παπαϊωάννου, 2007: 79): α) Αν  $1 \leq a < n$  ικανοποιεί την  $a^r \bmod n = 1$  (για  $r \geq 1$ ) τότε  $a \in \square_n^*$ .

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

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

**Απόδειξη:** α)  $a^r \bmod n = 1$  για κάποιο  $r \geq 1 \Rightarrow a \cdot a^{r-1} \bmod n = 1 \Rightarrow a \in \square_n^*$ .

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

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

**Παράδειγμα 2.1** (Κουκουβίνος - Παπαϊωάννου, 2007: 80): Έστω  $n = 91 = 7 \cdot 13$ .

Έχουμε: 18 πολλαπλάσια του 7 και 13,

36 F-μάρτυρες και

36 F-ψεύτες στο  $\{1, 2, \dots, 90\}$ .

πολ7	7,14,21,28,35,42,49,56,63,70,77,84
πολ13	13,26,39,52,65,78
F-μάρτυρες στο $\square_{91}^*$	2,5,6,8,11,15,18,19,20,24,31,32,33,34,41,44,45,46,47,50,54,57,58,59,60,67,71,72,73,76,80,83,85,86,89



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

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

Αυτό μας οδηγεί στην πρώτη προσπάθεια πιθανοτικής πιστοποίησης πρώτου.

### Αλγόριθμος 1 (Fermat Test)

Είσοδος: Μονός φυσικός  $n \geq 3$

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

2. αν  $a^{n-1} \bmod n = 1$

3. τότε επιστροφή 1

4. αλλιώς επιστροφή 0

Η χρονική διάρκεια έχει ως εξής:

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

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

δίνει πιθανότητα  $\frac{34}{88} = \frac{17}{44}$ .

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

**Θεώρημα 2.4** (Κουκουβίνος - Παπαϊωάννου, 2007: 81-82): Αν  $n \geq 3$  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  $L_n^F = \{a \mid 1 \leq a < n \text{ με } a^{n-1} \bmod n = 1\}$  των F-ψευτών για το  $n$  είναι προφανώς υποσύνολο του  $\mathbb{Z}_n^*$ . Θα δείξουμε ότι είναι και υποομάδα της  $Z_n^*$ .

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

1.  $1 \in L_n^F$  που ισχύει διότι  $1^{n-1} = 1$  τετριμμένα.
2. Η  $L_n^F$  είναι κλειστή ως προς την πράξη πολλαπλασιασμός mod  $n$  (η πράξη της  $\mathbb{Z}_n^*$ ) διότι  $a^{n-1} \bmod n = 1$  και  $b^{n-1} \bmod n = 1$  συνεπάγεται  $(ab)^{n-1} = a^{n-1}b^{n-1} = 1 \cdot 1 = 1 \bmod n$ .

Αφού το  $Z_n^*$  από το Λήμμα 2.1 έχει τουλάχιστον ένα στοιχείο, το  $L_n^F$  είναι γνήσια υποομάδα του  $Z_n^*$ . Από το θεώρημα του Lagrange λοιπόν η τάξη του θα είναι γνήσιος διαιρέτης  $\varphi(n)$ , όπου  $\varphi(n) < n-1$  (διότι ο  $n$  σύνθετος), άρα  $L_n^F \leq \frac{n-2}{2}$ .

Άρα η πιθανότητα του μια τυχαία επιλογή από το  $\{2, \dots, n-2\}$  ανήκει στο

$$L_n^F - \{1, n-1\} \text{ είναι το πολύ } \frac{\frac{n-2}{2} - 2}{n-3} = \frac{n-6}{2(n-3)} < \frac{1}{2}.$$

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

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

## Αλγόριθμος 2 (Iterated Fermat Test)

### (Επαναληπτικό κριτήριο Fermat)

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

Διαδικασία: 1. Επαναλαμβάνω  $l$  φορές

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

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

4. επιστροφή 0

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

Αν ο  $n$  είναι σύνθετος και ισχύει το προηγούμενο θεώρημα (δηλαδή υπάρχει τουλάχιστον ένας F-μάρτυρας  $a$  με  $(a, n) = 1$ ) η πιθανότητα να επιλέξουμε F-ψεύτη

μετά από  $l$  δοκιμές γίνεται μικρότερη από  $\left(\frac{1}{2}\right)^l$ . Άρα για μεγάλα  $l$  η πιθανότητά

λάθους γίνεται όσο θέλουμε μικρή.

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

**Ορισμός 2.5** (Κουκουβίνος - Παπαϊωάννου, 2007: 83): Ένας μονός σύνθετος αριθμός  $n$  λέγεται αριθμός Carmichael αν  $a^{n-1} \bmod n = 1 \forall a \in Z_n^*$ . Ο μικρότερος αριθμός Carmichael είναι ο  $561 = 3 \cdot 11 \cdot 17$ .

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

Αν ένας αριθμός Carmichael  $n$  υποστεί το τεστ του Fermat η πιθανότητα να

πάρομε την λάθος απάντηση 0 είναι  $\frac{\varphi(n)-2}{n-3} > \frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$

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

Πχ. ο  $n = 651.693.055.693.681 = 72.931 \cdot 87.517 \cdot 102.103$  έχουμε

$$\frac{\varphi(n)}{n} > 0.99996.$$

Άρα χρειαζόμαστε καλλίτερα τεστ από το τεστ του Fermat.

Πρώτα όμως περιγράφουμε την βασική ιδιότητα των αριθμών Carmichael.

**Θεώρημα 2.6** (Κουκουβίνος - Παπαϊωάννου, 2007: 83): Αν ο  $n$  είναι αριθμός Carmichael, τότε ο  $n$  είναι γινόμενο τουλάχιστον τριών διαφορετικών πρώτων παραγόντων.

**Θεώρημα(Korcelt) 2.7** (Κουκουβίνος - Παπαϊωάννου, 2007: 85): Ένας περιττός

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

**Κατασκευή (J. Chernick 1939):** αν  $t$  ακέραιος τέτοιος ώστε  $n = (6t+1)(12t+1)(18t+1)$  από το παραπάνω θεώρημα είναι αριθμός Carmichael. Για  $t = 1$  έχω  $1729 = 7 \cdot 13 \cdot 19$  που είναι αριθμός Carmichael.

Ο Richard Pinch του πανεπιστημίου του Cambridge υπολόγισε τους 105.212 αριθμούς Carmichael τους μικρότερους του  $10^{15}$ .

## 2.2 Το Κριτήριο Miller Rabin και Solovay Strassen

**Ορισμός 2.8** (Κουκουβίνος - Παπαϊωάννου, 2007: 86): Έστω  $1 \leq a < n$ . Ο  $a$  ονομάζεται τετραγωνική ρίζα της μονάδας mod  $n$  αν  $a^2 \bmod n = 1$ .

Παρατηρούμε ότι ο 1 και ο  $n-1$  είναι πάντα τετραγωνικές ρίζες της μονάδας mod  $n$ . Πράγματι  $1^2 \bmod n = 1$ ,  $(n-1)^2 = (-1)^2 = 1 \bmod n$  αυτές είναι οι τετριμμένες ρίζες της μονάδας. Αν ο  $n$  είναι πρώτος δεν υπάρχουν άλλες ρίζες της μονάδας mod  $n$ .

**Λήμμα 2.9** (Κουκουβίνος - Παπαϊωάννου, 2007: 86): Αν  $p$  πρώτος και  $1 \leq a < p$  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  $p | (a+1)(a-1)$ .

Αφού ο  $p$  πρώτος

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

$$\text{ή } p | (a-1) \Rightarrow a-1 = kp \Rightarrow a = 1 \bmod p.$$

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

**Παράδειγμα 2.2** (Κουκουβίνος - Παπαϊωάννου, 2007: 86): Οι τετραγωνικές ρίζες του  $1 \bmod 91$  είναι 1, 27, 64 και 90.

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

**Πρόταση 2.10** (Κουκουβίνος - Παπαϊωάννου, 2007: 86-87): Έστω ο πρώτος  $p = 3 \text{ mod } 4$  και ο ακέραιος  $y$ . Έστω  $x = y^{\frac{p-1}{4}} \text{ mod } p$ .

1) Αν ο  $y$  έχει τετραγωνική ρίζα  $\text{mod } p$  τότε οι τετριμμένες ρίζες του  $y \text{ mod } p$  είναι  $\pm x$ .

2) Αν ο  $y$  δεν έχει τετριμμένες ρίζες  $\text{mod } p$  τότε ο  $-y$  έχει και οι τετριμμένες ρίζες του  $-y \text{ mod } p$  είναι  $\pm x$ .

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

Έστω  $y$  και  $-y$  τετράγωνα  $\text{mod } p$  ήτοι  $y = a^2, -y = b^2$  τότε  $-1 = \left(\frac{a}{b}\right)^2 \text{ mod } p$  αν

διαιρέσουμε κατά μέλη, ήτοι το  $-1$  είναι τετράγωνο  $\text{mod } p$ . Αλλά αφού  $p = 3 \text{ mod } 4$  τούτο είναι αδύνατο. Πράγματι αν  $p = 3 \text{ mod } 4$  η εξίσωση  $x^2 = -1 \text{ mod } p$  δεν έχει λύσεις διότι αν είχε, ήτοι αν υπήρχε τέτοιο  $x$ , τότε

$$(x^2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \text{ mod } p \Rightarrow$$

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

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

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

**Ορισμός 2.11** (Κουκουβίνος - Παπαϊωάννου, 2007: 91-92): Έστω  $n \geq 3$  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  $0 \leq i < k$ .  
Αν ο  $n$  σύνθετος και ο  $a$  δεν είναι A-μάρτυρας του  $n$ , τότε ο  $a$  λέγεται A-ψεύτης.

**Λήμμα 2.12** (Κουκουβίνος - Παπαϊωάννου, 2007: 92): Αν ο  $a$  A-μάρτυρας του  $n$  τότε ο  $n$  σύνθετος.

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

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

### Κριτήριο Miller-Rabin

Είσοδος: Μονός φυσικός  $n \geq 3$

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

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

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

4. αν  $b = 1$  ή  $b = n-1$  επιστροφή 0

5. επανάληψη  $k-1$  φορές

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

7. αν  $b = n-1$  επιστροφή 0

8. αν  $b = 1$  τότε επιστροφή 1

9. επιστροφή 1

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

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

Ένα πολύ βασικό κριτήριο συγγενές με τις τετραγωνικές ρίζες της μονάδας  $\text{mod } n$  είναι το εξής:

**Θεώρημα (Βασικό Κριτήριο Παραγοντοποίησης) 2.13** (Κουκουβίνος - Παπαϊωάννου, 2007: 93-94): Έστω ο φυσικός  $n$  και έστω ότι υπάρχουν φυσικοί  $x, y$  με  $x^2 - y^2 \text{ mod } n$  αλλά  $x \not\equiv \pm y \text{ mod } n$ . Τότε ο  $n$  είναι σύνθετος και ο  $d = \text{MK}\Delta(x - y, n)$  δίδει μη τετριμμένο παράγοντα του  $n$ .

**Απόδειξη:** Αν  $d = n$  τότε  $x = y \text{ mod } n$  που δεν ισχύει εξ υποθέσεως.

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

**Παράδειγμα 2.3** (Κουκουβίνος - Παπαϊωάννου, 2007: 94): Είναι  $12^2 = 2^2 \text{ mod } 35$  με  $12 \not\equiv \pm 2 \text{ mod } 35$ . Άρα 35 σύνθετος και  $\text{MK}\Delta(12 - 2, 35) = 5$  μη τετριμμένος παράγοντας του 35.

**2.3 Κριτήριο Miller-Rabin (αναλυτικά)** (Κουκουβίνος - Παπαϊωάννου, 2007: 94)

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

Αν  $b_1 \equiv -1 \text{ mod } n$  σταματάμε και λέμε ότι ο  $n$  είναι πιθανά πρώτος. Αλλιώς υπολογίζουμε το  $b_2 = b_1^2 \text{ mod } n$ . Αν  $b_2 \equiv 1 \text{ mod } n$  ο  $n$  σύνθετος, αν  $b_2 \equiv -1 \text{ mod } n$

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

**Παράδειγμα 2.4** (Κουκουβίνος - Παπαϊωάννου, 2007: 94-95) : Για  $n = 561$  είναι  $n-1 = 560 = 16 \cdot 35$ .

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

Έστω  $a = 2$ .

Τότε  $b_0 = 2^{35} = 263 \pmod{561}$ .

$$b_1 = 263^2 = 166 \pmod{561}.$$

$$b_2 = 166^2 = 67 \pmod{561}.$$

$$b_3 = 67^2 = 1 \pmod{561}.$$

Αφού  $b_3 \neq -1 \pmod n$  ο  $561$  σύνθετος με  $d = \text{MK}\Delta(66, 561) = 33$  μητετριμμένο παράγοντα του  $561$ .

Υπενθύμιση:  $561 = 3 \cdot 11 \cdot 17$ .

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

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

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

Μέχρι το  $10^{10}$  υπάρχουν  $455.052.511$  πρώτοι, υπάρχουν  $14.884$  ψευδοπρώτοι για την βάση  $2$  και  $3.291$  ισχυροί ψευδοπρώτοι για την βάση  $2$ . Άρα ο υπολογισμός  $2^{n-1} \pmod n$  (το κριτήριο του Fermat) θα αποτύχει να αναγνωρίσει έναν σύνθετο

στην περιοχή αυτή με πιθανότητα  $< \frac{1}{30.000}$  ενώ το κριτήριο του Miller Rabin με  $a$

$= 2$  αποτυγχάνει με πιθανότητα  $< \frac{1}{1000.000}$ . Ο πρώτος ισχυρός ψευδοπρώτος για

τις βάσεις  $2, 3, 5, 7$  είναι ο  $3.215.031.751$  ενώ για όλες τις πρώτες βάσεις τις  $< 200$  είναι ένας ισχυρός ψευδοπρώτος με  $337$  ψηφία.



**Ορισμός 2.14** (Κουκουβίνος - Παπαϊωάννου, 2007: 95-96): Αν  $a \in \mathbb{Z}$ ,  $m \geq 2$   $(a, m) = 1$  λέμε ότι ο  $a$  είναι τετραγωνικό υπόλοιπο (quadratic residue (QR))  $\pmod{m}$  αν  $a = x^2 \pmod{m}$  για  $x \in \mathbb{Z}$ .

**Παρατηρήσεις:**

- i)  $a \in QR$  είναι μία ιδιότητα όλων των αριθμών της κλάσης ισοδυναμίας του  $a$  οπότε δουλεύουμε στο  $\{1, \dots, m-1\}$ .
- ii)  $-1 = m-1 \pmod{m} \in \{1, \dots, m-1\}$
- iii) Οι αριθμοί  $a$  με  $(a, m) > 1$  δεν είναι ούτε τετραγωνικά υπόλοιπα ούτε μη

**Θεώρημα (Κριτήριο του Euler) 2.15** (Κουκουβίνος - Παπαϊωάννου, 2007: 97-98): Αν  $p$  μονός πρώτος τότε το QR είναι υποομάδα του  $\mathbb{Z}_p^*$  τάξης  $\frac{p-1}{2}$ . Επίσης

$$\text{αν } a \in \mathbb{Z}_p^* \text{ έχουμε } a^{\frac{p-1}{2}} = \begin{cases} 1, & \text{αν } a \in QR \\ -1 & \text{αν } a \notin QR \end{cases}$$

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

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

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

Η διαδικασία αυτή μας κάνει εύκολο τον υπολογισμό ριζών για τους μισούς περίπου πρώτους  $p$ . Αν  $p \geq 3$  είναι πρώτος και  $p+1 = \text{πολ}4$  (ήτοι  $p \equiv 3 \pmod{4}$ )

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

Τότε  $x = a^{\frac{p+1}{4}} = g^{i \frac{(p-1)}{2} + i} = \left(g^{\frac{p-1}{2}}\right)^i \cdot g^i = (-1)^i g^i$ , αλλά υψώνοντας στο τετράγωνο

$x^2 = (-1)^{2i} g^{2i} = 1 \cdot a = a$  ήτοι το  $x$  είναι τετραγωνική ρίζα (η άλλη είναι η  $p - x$ )

δηλαδή για να βρω το  $x$  από το  $a$  δεν χρειάζεται ο γεννήτορας  $g$ .

### Κριτήριο των Solovay-Strassen

Είσοδος: Μονός ακέραιος  $n \geq 3$

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

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

3. then return 1

4. else return 0.

Στην γραμμή 2 ο υπολογισμός του συμβόλου Jacobi  $\left(\frac{a}{n}\right)$  γίνεται από τον

αλγόριθμο και η εκθετοποίηση  $a^{\frac{n-1}{2}} \bmod n$  γίνεται με fast exponentiation,

Ο παραπάνω αλγόριθμος είναι  $O((\log n)^3)$ . Αν το  $n$  είναι πρώτος έχουμε σαν

έξοδο το 0 αν ο  $n$  είναι σύνθετος η πιθανότητα να πάρω στην έξοδο 0 είναι

μικρότερη της  $\frac{1}{2}$ .

## ΚΕΦΑΛΑΙΟ 3

### ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΑΚΕΡΑΙΩΝ

#### 3.1 Μέθοδος των Διαδοχικών Διαιρέσεων

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

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

**Παράδειγμα 3.1** (Πουλιάκης, 2006: 115-116): Θα παραγοντοποιήσουμε τον ακέραιο 225277. Έχουμε  $474 < \sqrt{225277} < 475$ . Οπότε, αν ο 225277 είναι σύνθετος θα έχει ένα πρώτο διαιρέτη  $< 474$ . Δοκιμάζοντας κάθε πρώτο αρχίζοντας από τον 3, βρίσκουμε ότι ο 13 διαιρεί τον 225277 και έτσι προκύπτει  $225277 = 13 \cdot 17329$ . Έχουμε  $131 < \sqrt{17329} < 132$ . Ομοίως, βρίσκουμε ότι ο 13 διαιρεί τον 17329 και επομένως  $225277 = 13^2 \cdot 1333$ . Τέλος, παίρνουμε  $1333 = 31 \cdot 43$ . Συνεπώς, η πρωτογενής ανάλυση του 225277 είναι  $225277 = 13^2 \cdot 31 \cdot 43$ .

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

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

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

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

### 3.2 Μέθοδος του Fermat και του Euler

Η πρώτη μέθοδος παραγοντοποίησης με την οποία θ' ασχοληθούμε είναι αρκετά παλιά και ανάγεται στον Fermat. Η ιδέα της μεθόδου βασίζεται στην παρακάτω πρόταση.

**Πρόταση 3.1** (Πουλάκης, 2006: 116-117): *Ας είναι  $n$  θετικός περιττός ακέραιος. Τότε υπάρχει μία αμφίεση μεταξύ των παραγοντοποιήσεων του  $n$  της μορφής  $n = ab$ , όπου  $a, b$  ακέραιοι  $a \geq b > 0$  και των παραστάσεων του  $n$  της μορφής  $t^2 - s^2$ , όπου  $s$  και  $t$  είναι ακέραιοι  $\geq 0$ . Η αμφίεση αυτή δίνεται από τις εξισώσεις:*

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

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

Απόδειξη: ας είναι  $n = ab$ , 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  $t = (a + b)/2$  και  $s = (a - b)/2$ , έχουμε  $n = t^2 - s^2$ . Αντιστρόφως, αν  $n = t^2 - s^2$ , όπου  $s$  και  $t$  είναι ακέραιοι  $\geq 0$ , τότε

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

Συνεπώς, οι αντιστοιχίες

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

και

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

δίνουν μία αμφίσηση μεταξύ των δύο τρόπων γραφής του  $n$ .

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

**Παράδειγμα 3.2** (Πουλάκης, 2006: 117-118): Θα παραγοντοποιήσουμε τον ακέραιο 670661. Έχουμε  $\sqrt{670661} = 818$ . Βρίσκουμε  $819^2 - 670661 = 10^2$ . Οπότε  $670661 = 829 \cdot 809$ .

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

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

$$(t + s)(t - s) = kn.$$

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

Γενικότερα, αν βρούμε ακεραίους  $t$  και  $s$  με

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

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

**Παράδειγμα 3.3** (Πουλάκης, 2006: 118): Θα παραγοντοποιήσουμε τον ακέραιο 329345. Έχουμε  $\lfloor \sqrt{3 \cdot 329345} \rfloor = 993$ . θεωρούμε τις τιμές  $t = 994, \dots$  και παίρνουμε αμέσως  $994^2 - 3 \cdot 329345 = 1$ . Επομένως  $3 \cdot 329345 = 995 \cdot 993$ . Κατόπιν υπολογίζουμε τον μέγιστο κοινό διαιρέτη  $(329345, 995) = 995$ . Οπότε  $329345 = 331 \cdot 995$ . Παρατηρούμε ότι με την κλασσική μέθοδο του Fermat θα χρειαστεί να πάρουμε πολύ περισσότερες από μία τιμές για τον  $t$ .

**Παράδειγμα 3.4** (Κουκουβίνος - Παπαϊωάννου, 2007: 116): Για  $n = 931, k=31$ , διότι  $k^2 = 961 > 931$  και

$$31^2 - 931 = 30$$

$$32^2 - 931 = 93$$

$$33^2 - 931 = 158$$

$$34^2 - 931 = 225 = 15^2 = y^2.$$

Άρα  $y = 15, m = 3, x = k + m = 31 + 3 = 34$  και  $(34 - 15)(34 + 15) = 19 \cdot 49$ .

Όμως η διαδικασία αυτή στον αριθμό που ρώτησε ο Mersenne έχει  $m = 75.000$ .

*Βελτίωση της μεθόδου του Fermat αν  $n = a \cdot b$  και  $a \square b$ .*

Επιλέγω μικρό  $k$  και  $t = \lfloor \sqrt{kn} \rfloor + 1, \lfloor \sqrt{kn} \rfloor + 2, \dots$  και υπολογίζω  $t^2 - kn$  έως ότου

$t^2 - kn = s^2$  οπότε  $(t+s)(t-s) = kn$ . Έχω  $k < t-s < t+s < n$ . Άρα  $1 < \text{ΜΚΔ}(t \pm s, n) < n$  και οι  $t \pm s$  είναι γνήσιοι παράγοντες του  $n$ .

**Παράδειγμα 3.5 (Κουκουβίνος - Παπαϊωάννου, 2007: 117):** Έστω  $n = 329.345$ .

Θεωρώ  $k = 3$  και υπολογίζω  $\sqrt{3 \cdot 329.345} = 993, \dots$ . Όμως για  $t = 994$  έχω  $994^2 - 3 \cdot 329.345 = 988.036 - 988.035 = 1^2$  άρα

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

Υπολογίζω  $\text{ΜΚΔ}(329.345, 995) = \text{ΜΚΔ}(331 \cdot 995, 995) = 995$ .

Άρα  $329.345 = 331 \cdot 995$ .

Η απλή μέθοδος του Fermat θέλει πολύ περισσότερες δοκιμές.

### Μέθοδος Euler

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

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

ήτοι ο  $n$  παραγοντοποιείται.

Η παράσταση προκύπτει αν κάνω τις πράξεις στο 2<sup>ο</sup> μέλος.

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

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

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

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

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

$$a + c = kmr$$

$$a - c = ns$$

$$d + b = ms$$

$$d - b = nr.$$

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

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

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

$$\text{Άρα } 2N = \frac{2(k^2m^2r^2 + kn^2r^2 + km^2s^2 + n^2s^2)}{4} \text{ και συνεπώς}$$

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

**Παράδειγμα 3.7** (Κουκουβίνος - Παπαϊωάννου, 2007: 118-119): Θα παραγοντοποιήσουμε τον 34.889.

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

$$a + c = \overbrace{10}^k \cdot \overbrace{30}^{mr} \Rightarrow mr = 30, m = 10, r = 3$$

$$a - c = 14 = ns \Rightarrow s = 7.$$

$$d + b = 70 = ms$$

$$d - b = 6 = nr \Rightarrow n = 2$$

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



### 3.3 Ο αλγόριθμος παραγοντοποίησης του Dixon (1981)

**Ορισμός βάσης παραγοντοποίησης 3.3** (Κουκουβίνος - Παπαϊωάννου, 2007: 133): Είναι το σύνολο των διακεκριμένων πρώτων  $B = \{-1, p_1, \dots, p_h\}$  όπου προφανώς  $-1 \equiv n-1 \pmod{n}$ . Ο ακέραιος  $n$  καλείται **B-λείος** αν γράφεται σαν γινόμενο στοιχείων του  $B$ . Ο ακέραιος  $b$  λέγεται **B-προσαρμοσμένος ως προς τον φυσικό  $n$**

αν ο ακέραιος  $c$  με  $-\frac{n}{2} \leq c \leq \frac{n}{2}$  και  $b^2 = c \pmod{n}$  είναι B-λείος.

**Παράδειγμα 3.8** (Κουκουβίνος - Παπαϊωάννου, 2007: 133):

Έστω η βάση  $B = \{-1, 2, 3, 5, 7\}$ . Οι ακέραιοι  $40 = 2^3 \cdot 5$  και  $65 = 3^2 \cdot 7$  είναι B-λείοι.

Ισχύει  $59^2 = 40 \pmod{1147} \Rightarrow$  άρα ο  $b=59$ , για τον οποίο ισχύει  $b^2 = 40 \pmod{1147}$  και

$-\frac{1147}{2} \leq 40 \leq \frac{1147}{2}$ , είναι προσαρμοσμένος ως προς τον 1147.

Επίσης  $71^2 = 63 \pmod{2849}$  άρα ο  $b=71$  με  $71^2 = 63 \pmod{2849}$  και

$-\frac{2849}{2} \leq 63 \leq \frac{2849}{2}$  είναι προσαρμοσμένος ως προς τον 2849.

Παρατηρούμε ότι ο  $b$  είναι προσαρμοσμένος ως προς τον  $n$  αν το τετράγωνό του αναλύεται σε πρώτους παράγοντες της βάσης.

Το «ζουμί» του αλγορίθμου του Dixon είναι ότι παίρνουμε μία βάση που αποτελείται από μικρούς πρώτους (γι' αυτό βάλαμε το -1 αντί του  $n-1$ ) και φτιάχνουμε τετράγωνα που να γράφονται σαν γινόμενα μικρών πρώτων (το προσαρμοσμένος) και στοιχείων της βάσης (το λείος). Κάθε τέτοιο τετράγωνο δίνει μία γραμμή σ' έναν πίνακα στον οποίο καταχωρούνται οι εκθέτες των πρώτων αριθμών της βάσης. Αν πάρουμε περισσότερους τέτοιους αριθμούς από τα στοιχεία της βάσης ο προκύπτων πίνακας θα έχει  $\pmod{2}$  γραμμικές εξαρτήσεις μεταξύ των γραμμών. Οι γραμμικά εξαρτημένες γραμμές δίνουν  $x^2 = y^2 \pmod{n}$  (για διάφορα  $x, y$ ). Αν  $x \not\equiv \pm y \pmod{n}$  καταλήγουμε κατά τα γνωστά σε μη τετριμμένο παράγοντα του  $n$ .

### Αλγόριθμος Dixon

1. Επιλέγουμε φυσικό  $y$  και θεωρούμε την βάση  $B$  που σχηματίζουν οι πρώτοι παράγοντες  $p_1, p_2, \dots, p_{\pi(y)}$  που είναι  $\leq y$ .
2. Αν κανένας από τους πρώτους  $p_i$  δεν διαιρεί τον  $n$  βρίσκουμε ακεραίους  $b_i$ ,  $1 \leq b_i \leq n$   $i = 1, \dots, \pi(y) + 2$  που είναι  $B$ -προσαρμοσμένοι ως προς τον  $n$ .
3. Αν  $b_i^2 = (-1)^{a_{i0}} p_1^{a_{i1}} \dots p_{\pi(y)}^{a_{i\pi(y)}} \pmod n$  τότε αντιστοιχώ στο  $b_i$  το διάνυσμα  $u_i$  των εκθετών:  $u_i = (u_{i0}, u_{i1}, \dots, u_{i\pi(y)})$  του  $\square_2^{\pi(y)+1}$  θέτοντας  $u_{ij} = 0$  αν ο  $a_{ij}$  άρτιος και  $u_{ij} = 1$  αν ο  $a_{ij}$  περιττός [ $0, 1$  τα στοιχεία του  $\square_2$ ].
4. Υπολογίζω το υποσύνολο  $I$  του  $\{1, \dots, \pi(y) + 2\}$  με  $\sum_{i \in I} u_i = 0$  (δηλαδή τα γραμμικά εξαρτημένα  $\pmod 2$ ).
5. Υπολογίζω τα γινόμενα  $b = \prod_{i \in I} b_i$ ,  $c = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_{\pi(y)}^{\gamma_{\pi(y)}}$  όπου  $2\gamma_j = \sum_{i \in I} a_{ij}$ .  
Προσοχή: θέλω κάθε πρώτος της βάσης  $B$  να χρησιμοποιείται **άρτιο** πλήθος φορών.
6. Αν  $b \neq \pm c \pmod n$  υπολογίζω  $\text{MKΔ}(b+c, n)$  που δίνει μη τετριμμένο παράγοντα του  $n$ . Αν  $b = \pm c \pmod n$  υπολογίζω άλλο  $I \subset \{1, \dots, \pi(y) + 2\}$  ή άλλο  $y$  και επαναλαμβάνω την διαδικασία.

Παρατηρώ ότι στο βήμα 4 το πλήθος των διανυσμάτων  $u_i$   $i = 1, \dots, \pi(y) + 2$  είναι μεγαλύτερο από την διάσταση του διαν. χώρου  $\square_2^{\pi(y)+1}$  άρα τα διανύσματα είναι γραμμικά εξαρτημένα. Μπορώ λοιπόν με απαλοιφή να υπολογίσω το σύνολο  $I$ .

Από την κατασκευή των  $b, c$  έχουμε  $b^2 = c^2 \pmod n$  και αν  $b \neq \pm c \pmod n$  το βασικό λήμμα μας δίνει την παραγοντοποίηση του  $n$ .

Επίσης αφού οι πρώτοι  $p_1, p_2, \dots, p_{\pi(y)}$   $\nmid n$  έχουμε  $(b, n) = 1$ . Αν λοιπόν ο  $n$  έχει  $2^r$  πρώτους παράγοντες ( $r \geq 2$ ) τότε η πολυωνυμική ισοδυναμία  $x^2 = b^2 \pmod n$  έχει  $r$  λύσεις. Η πιθανότητα λοιπόν να έχω  $b \neq \pm c \pmod n$  ισούται με  $\frac{1}{2^{r-1}}$ .

Για την εύρεση ακεραίων  $b_i$  δοκιμάζουμε (όπως είδαμε στο παράδειγμα 5.2)

ακεραίους της μορφής  $\lfloor \sqrt{kn} \rfloor + j$ ,  $j=0,1,\dots$ ,  $k=1,2,\dots$ . Ο μικρότερος (κατ' απόλυτο τιμή ακέραιος) της κλάσης του τετραγώνου τέτοιων ακεραίων mod  $n$  είναι αρκετά μικρός και άρα έχει «μεγάλη» πιθανότητα να είναι B-προσαρμοσμένος ως προς τον  $n$ .

**Παράδειγμα 3.9** (Κουκουβίνος - Παπαϊωάννου, 2007: 136-138): Θα παραγοντοποιήσω τον  $n = 93623 (= 373 \cdot 251)$ .

Θεωρώ την βάση  $B = \{-1, 2, 3, 5, 7, 11, 13\}$  με 7 στοιχεία άρα θα προσπαθήσω να βρω 8 B-προσαρμοσμένους ακεραίους ως προς τον  $n = 93623$ . Παρατηρώ ότι και τα 7 στοιχεία της  $B$  δεν διαιρούν τον  $n$ . Δοκιμάζω  $\lfloor \sqrt{kn} \rfloor + j$  με  $k, j=1,\dots,9$ .

Έχουμε:

$$\sqrt{n} \approx 305,9.. \text{ άρα αρχίζω με } b_1 : 306^2 = 93636 = 13 \pmod{n} \in B$$

$$\sqrt{2n} \approx 432, \dots \quad \text{ο } b_2 : 433^2 = 187.489 = 243 = 3^5 \pmod{n}, \quad 3 \in B$$

$$\sqrt{3n} < 530 \quad \text{ο } b_3 : 531^2 = 281.961 = 1092 = 2^2 \cdot 3 \cdot 7 \cdot 13 \in B$$

$$\text{και ο } b_4 : 537^2 = 288.369 = 7500 = 2^2 \cdot 3 \cdot 5^4 \in B$$

$$\sqrt{4n} < 612 \quad \text{και ο } b_5 : 612^2 = 374.544 = 52 = 2^2 \cdot 13 \in B$$

$\sqrt{5} < 750$  και δεν δίνει ανάλυση  $\in B$  κανέναν αριθμό στο διάστημα 750...759

$$\sqrt{6n} \approx 809, \dots \quad \text{και ο } b_6 : 809^2 = 654.481 = -880 = -2^4 \cdot 5 \cdot 11 \in B$$

$$\sqrt{7n} \approx 865, \dots \quad \text{και ο } b_7 : 866^2 = 749.956 = 972 = 2^2 \cdot 3^5 \in B$$

$$\sqrt{8n} \approx 917, \dots \quad \text{και ο } b_8 : 918^2 = 842.724 = 117 = 3^2 \cdot 13 \in B$$

οπότε έχω στο  $\mathbb{Z}_2^7$  τα 8 διανύσματα

$$u_1 = (0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1) \quad u_5 = (0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1)$$

$$u_2 = (0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0) \quad u_6 = (1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0)$$

$$u_3 = (0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1) \text{ το } 2^2 \text{ έδωσε } 0 \quad u_7 = (0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0)$$

$$u_4 = (0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0) \quad u_8 = (0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1)$$

Θεωρώ το γραμμικό ομογενές σύστημα  $x_1 \overline{u_1} + x_2 \overline{u_2} + \dots + x_8 \overline{u_8} = 0 \pmod{2}$ . Έχουμε

$$\left. \begin{array}{l} x_6 = 0 \\ x_2 + x_3 + x_4 + x_7 = 0 \\ x_3 = 0 \\ x_1 + x_3 + x_5 + x_8 = 0 \end{array} \right\} \text{mod } 2.$$

Μία λύση του συστήματος:

$$\begin{aligned} x_1 = x_5 = 1 \\ x_2 = x_3 = x_4 = x_6 = x_7 = x_8 = 0. \end{aligned}$$

Άρα το  $I = \{x_1, x_5\}$ . Θα υπολογίσω τα  $b, c$ .

$$b = \prod_{i \in I} b_i = b_1 b_5 = 306 \cdot 612 = 187.272.$$

$$c^2 = 13 \cdot 2^2 \cdot 13 \Rightarrow c^2 = 2^2 \cdot 13^2 \Rightarrow c = 26.$$

Αλλά  $187.272 = 26 \text{ mod } n$  [πράγματι  $187.272 - 26 = 187.246 = 2 \cdot 93623$ ] άρα δεν μπορούμε να υπολογίσουμε μη τετριμμένο παράγοντα  $n$ .

Βρίσκω άλλη λύση του συστήματος ήτοι την

$$\left. \begin{array}{l} x_2 = x_4 = 1 \\ x_1 = x_3 = x_5 = x_6 = x_7 = x_8 = 0 \end{array} \right\} I'$$

Τότε  $b = 433 \cdot 537 = 232.521$  και

$$c^2 = 3^5 \cdot 2^2 \cdot 3 \cdot 5^4 = 2^2 \cdot 3^6 \cdot 5^4 = (2 \cdot 3^3 \cdot 5^2)^2 \Rightarrow c = 2 \cdot 3^3 \cdot 5^2 = 1350.$$

Αλλά  $232.521 = 45.275 \text{ mod } n \Rightarrow b \neq \pm c \text{ mod } n$ .

Άρα  $\text{ΜΚΔ}(b+c, n) = (233.871, 93.623)$

$$\begin{array}{r} 233.871 \quad 93.623 \\ 46.625 \quad 93.623 \\ \hline 46.625 \quad 373 \\ \hline 0 \quad 373 \end{array}$$

$$46.625 \quad 93.623$$

$$46.625 \quad 373$$

$$0 \quad 373 \quad \text{Άρα } \text{ΜΚΔ} = 373.$$

Άρα  $93.623 = 373 \cdot 251$ .

Η πολυπλοκότητα του αλγορίθμου του Dixon με κατάλληλα μικρή βάση

παραγοντοποίησης δίνει χρόνο εκτέλεσης  $O\left(e^{c\sqrt{\log n \cdot \log \log n}}\right)$  άρα είναι υποεκθετικού

χρόνου.

### 3.4 Ο αλγόριθμος $p-1$ του John Pollard (1974)

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

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

Παρατηρούμε ότι ο  $p-1$  αλγόριθμος του Pollard που είδαμε όπως και ο αλγόριθμος των Pohlig – Hellman στηρίζεται στο προκαθορισμένο φράγμα  $B$  δηλαδή ουσιαστικά στην βάση  $B$  μικρών πρώτων αριθμών.

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

#### Ο αλγόριθμος $p-1$ του John Pollard

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

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

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

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

Οι άλλοι πρώτοι δίνουν εκθέτη 1.

2. Επιλέγουμε έναν ακέραιο  $a$  με  $1 < a < n$  και υπολογίζουμε  $\text{MKΔ}(a, n) = \delta$ .

Αρχίζω  $a=2$ ,  $a=3$  κοκ.

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

Αν  $\delta=1$  υπολογίζω τον  $\delta = \text{MKΔ}(a^k - 1, n)$ .

(βασικό βήμα του αλγ. όχι όμως πολύ πολύπλοκο)

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

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

**Παράδειγμα 3.10** (Κουκουβίνος - Παπαϊωάννου, 2007: 142-143):

1) Να παραγοντοποιηθεί ο  $n = 1.241.143$ .

Ας πάρουμε  $B = 13$ .

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

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

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

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

### 3.5 Ο αλγόριθμος Pollard Rho

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

**Ορισμός 3.4** (Κουκουβίνος - Παπαϊωάννου, 2007: 144): 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 3.5 (Παράδοξο των γενεθλίων (birthday paradox))** (Κουκουβίνος - Παπαϊωάννου, 2007: 144-145):

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

Από μαθηματικής άποψης, αν μια συνάρτηση  $f$  παράγει μία τιμή μεταξύ  $n$  διαφορετικών τιμών με την ίδια πιθανότητα και το  $n$  είναι αρκετά μεγάλο, τότε

υπολογίζοντας τη συνάρτηση για ένα πλήθος περίπου  $1,17 \sqrt{n}$  διαφορετικών εισόδων περιμένουμε να βρούμε ένα ζεύγος εισόδων  $x$  και  $x'$  ( $x \neq x'$ ) τέτοια ώστε  $f(x) = f(x')$ .

**Απόδειξη:** Θεωρούμε την ομάδα των ακεραίων  $\text{mod } n$ , δηλαδή το σύνολο  $\square_n = \{0, 1, 2, \dots, n-1\}$  με  $|\square_n| = n$ . Θα υπολογίσουμε την πιθανότητα να μην επιλεγθούν ίσα στοιχεία (όχι συγκρούσεις) σε μία τυχαία επιλογή  $k$  στοιχείων από το  $\square_n$ . Η πιθανότητα επιλογής ενός συγκεκριμένου στοιχείου είναι  $\frac{1}{n}$ . Η πρώτη μας επιλογή είναι αυθαίρετη. Η πιθανότητα η δεύτερη επιλογή να είναι διαφορετική από την πρώτη είναι  $\frac{n-1}{n} = 1 - \frac{1}{n}$ . Η πιθανότητα η τρίτη επιλογή να είναι διαφορετική από τις προηγούμενες είναι  $\frac{n-2}{n} = 1 - \frac{2}{n}$  κ.ο.κ.

Έτσι η πιθανότητα επιλογής  $k$  στοιχείων χωρίς συγκρούσεις είναι

$$\left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) \left(1 - \frac{3}{n}\right) \dots \left(1 - \frac{k-1}{n}\right) = \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right) \quad \text{όπως προκύπτει από την}$$

Πολλαπλασιαστική Αρχή.

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

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

Μία εκτίμηση της ζητούμενης πιθανότητας είναι η

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

Αν  $p$  είναι η πιθανότητα εύρεσης μίας σύγκρουσης τότε  $p \approx 1 - e^{-k(k-1)/2n}$

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

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



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

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

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

**Συνέχεια του αλγορίθμου Pollard Rho** (Κουκουβίνος - Παπαϊωάννου, 2007: 146):

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

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

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

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

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

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

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

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

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

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

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

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

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

## ΒΙΒΛΙΟΓΡΑΦΙΑ

- Πουλάκης Μ. Δημήτριος, Θεσσαλονίκη, *Κρυπτογραφία Η επιστήμη επικοινωνίας*, Εκδόσεις Ζήτη, 2009
- Κουκουβίνος Χ., Παπαϊωάννου Α., Αθήνα, *Κρυπτογραφία*, Εκδόσεις Ε.Μ.Π., 2007
- Lewand R., *Cryptological Mathematics*, the Mathematical Association of America, 2000
- Menezes A., van Oorschot P. Vanstone S., "Handbook of applied Cryptography", 1996.
- Rivest R.L., Shamir A., Adleman L.M., "a method for obtaining digital signatures and public key cryptosystems, Communications of the ACU", V.21 no 2, 1978
- Singh S., *Κώδικες και Μυστικά*, Τραυλός 2003 (ιστορική αναδρομή κρυπτολογίας)
- Smart N., *Cryptography: An introduction*, Mc Graw-Hill 2003
- Stinson D., "Cryptography. Theory and Practice", third ed., Chapman and Hall, 2006
- Trappe W. and Washington L. "Introduction to Cryptography with coding Theory", Pearson education international, 2006
- Ε. Ζάχος, «Εισαγωγή στη Θεωρία Αριθμών και την Κρυπτολογία», Ε.Π.Μ. 2005

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