

---

---

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ - ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ  
Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών  
και Πληροφορικής

## Κρυπτογραφία

Συμπληρωματικές σημειώσεις

Πάτρα, Μάρτιος 2010

---

---

## Περιεχόμενα

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Εισαγωγή στην θεωρία αριθμών</b>                             | <b>3</b>  |
| 1.1      | Βασικές έννοιες . . . . .                                       | 3         |
| 1.2      | Αριθμητικές πράξεις με υπόλοιπα . . . . .                       | 11        |
| <b>2</b> | <b>Πρωτόκολλα δημοσίου κλειδιού</b>                             | <b>28</b> |
| 2.1      | Δημιουργία και ανταλλαγή κλειδιών . . . . .                     | 32        |
| 2.2      | Το πρωτόκολλο δημοσίου κλειδιού RSA . . . . .                   | 33        |
| 2.3      | Το πρωτόκολλο δημοσίου κλειδιού του Rabin . . . . .             | 36        |
| 2.4      | Το πρωτόκολλο δημοσίου κλειδιού του El Gamal . . . . .          | 40        |
| <b>3</b> | <b>Ελεγχος πρώτων αριθμών</b>                                   | <b>43</b> |
| 3.1      | Πιθανοτικοί αλγόριθμοι . . . . .                                | 44        |
| 3.2      | Ο ντετερμινιστικός αλγόριθμος . . . . .                         | 48        |
| <b>4</b> | <b>Εφαρμογές της κρυπτογραφίας</b>                              | <b>51</b> |
| 4.1      | Σχήματα διαμοίρασης μυστικού και πρωτόκολλα δέσμευσης . . . . . | 51        |
| 4.2      | Εκλογές, δημοπρασίες και οικονομικές συναλλαγές . . . . .       | 53        |

# 1 Εισαγωγή στην θεωρία αριθμών

Στην ενότητα αυτή παρουσιάζουμε με συντομία κάποιες βασικές έννοιες της στοιχειώδους θεωρίας αριθμών, σχετικά με το σύνολο  $Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$  των ακεραίων και το σύνολο  $N = \{0, 1, 2, \dots\}$  των φυσικών αριθμών. Επιπλέον, θα περιγράψουμε ορισμένους αλγορίθμους που μας επιτρέπουν να εκτελέσουμε σε πολυωνυμικό χρόνο κάποιες βασικές πράξεις, όπως η επίλυση γραμμικών εξισώσεων, η εύρεση τετραγωνικών ριζών, κλπ.

## 1.1 Βασικές έννοιες

### Διαιρετότητα και διαιρέτες

Θα ξεκινήσουμε παρουσιάζοντας κάποιους ορισμούς σχετικά με την διαίρεση. Το γεγονός ότι ένας ακέραιος διαιρεί κάποιον άλλο είναι πολύ σημαντικό στην θεωρία αριθμών. Θα συμβολίζουμε με  $d|a$  το ότι  $a = kd$  για κάποιον ακέραιο  $k$ , ενώ προφανώς ισχύει πως κάθε ακέραιος διαιρεί το 0. Αν ισχύει πως  $a > 0$  και επιπλέον ότι  $d|a$ , τότε ισχύει επίσης ότι  $|d| \leq |a|$ . Θα λέμε ότι ο ακέραιος  $a$  είναι πολλαπλάσιο του  $d$  αν ισχύει ότι  $d|a$ , ενώ αν ο  $d$  δεν διαιρεί τον  $a$ , τότε αυτό το συμβολίζουμε με  $d \nmid a$ .

Συνεχίζοντας, λέμε ότι ο ακέραιος  $d$  είναι διαιρέτης ενός ακεραίου  $a$  αν ισχύει ότι  $d|a$  και  $d \geq 0$ . Επειδή, αν  $d|a$  τότε ισχύει και ότι  $-d|a$ , μπορούμε χωρίς βλάβη της γενικότητας να θεωρήσουμε ότι οι διαιρέτες είναι μη αρνητικοί ακέραιοι, έχοντας κατά νου ότι για κάθε διαιρέτη υπάρχει ένας αρνητικός αριθμός που επίσης διαιρεί τον  $a$ . Στην συνέχεια του κειμένου επομένως, θα ασχοληθούμε μόνο με θετικούς διαιρέτες. Ισχύει λοιπόν πως ένας διαιρέτης του  $a$  είναι τουλάχιστον ίσος με 1 αλλά όχι μεγαλύτερος από  $|a|$ . Για παράδειγμα, οι διαιρέτες του 18 είναι οι 1, 2, 3, 6 και 9.

Κάθε ακέραιος  $a$  διαιρείται από τους τετριμμένους διαιρέτες 1 και  $a$ , ενώ οι μη-τετριμμένοι διαιρέτες του  $a$  καλούνται και *παράγοντες* του  $a$ . Για παράδειγμα, οι παράγοντες του 12 είναι οι 2, 3, 4 και 6.

### Θεώρημα της διαίρεσης, υπόλοιπα και modular ισοδυναμίες

Αν θεωρήσουμε έναν ακέραιο  $n$ , τότε μπορούμε να χωρίσουμε το σύνολο των ακεραίων σε 2 ξένα μεταξύ τους υποσύνολα. Το ένα αποτελείται από εκείνους τους ακεραίους που είναι πολλαπλάσια του  $n$  και το δεύτερο από αυτούς που δεν είναι πολλαπλάσια του  $n$ . Μπορούμε να επεκτείνουμε αυτή την ιδέα και να διαμερίσουμε το δεύτερο υποσύνολο με βάση το υπόλοιπο της διαίρεσης με τον  $n$ . Το επόμενο θεώρημα συνοψίζει την παραπάνω ιδέα.

**Θεώρημα 1.** Για κάθε ακέραιο  $a$  και κάθε θετικό ακέραιο  $n$ , υπάρχουν μοναδικοί ακέραιοι  $q$  και  $r$ , τέτοιοι ώστε  $0 \leq r < n$  και  $a = qn + r$ .

Ο αριθμός  $q = \lfloor a/n \rfloor$  είναι το ηλίκο της διαίρεσης, ενώ ο  $r = a \bmod n$  το υπόλοιπο. Ισχύει ότι  $n|a$  αν και μόνο αν  $a \bmod n = 0$ .

Μπορούμε επομένως να χωρίσουμε τους ακέραιους αριθμούς σε ομάδες με βάση το υπόλοιπο της διαίρεσης τους με το  $n$ . Η κλάση ισοδυναμίας modulo  $n$  που ορίζεται με βάση τον ακέραιο  $a$  είναι η  $[a]_n = \{a + kn : k \in \mathbf{Z}\}$ . Για παράδειγμα,  $[3]_7 = \{\dots, -11, -4, 3, 10, 17, \dots\}$ , ενώ η ίδια ομάδα μπορεί να συμβολιστεί και ως  $[-4]_7$  ή  $[10]_7$ . Μπορούμε επίσης να συμβολίσουμε το γεγονός πως  $a \in [b]_n$  και ως  $a \equiv b \pmod{n}$ . Το σύνολο όλων αυτών των κλάσεων ισοδυναμίας είναι το  $\mathbf{Z}_n = \{[a]_n : 0 \leq a \leq n-1\}$ , ενώ εναλλακτικά μπορεί να συμβολιστεί ως  $\mathbf{Z}_n = \{0, 1, 2, \dots, n-1\}$  με την κατανόηση ότι το 0 συμβολίζει το  $[0]_n$ , το 1 συμβολίζει το  $[1]_n$  κλπ. Γενικότερα, προτιμάμε να συμβολίζουμε κάθε κλάση με βάση το μικρότερο μη-αρνητικό στοιχείο της, δεν πρέπει όμως να ξεχνάμε πως κάθε τέτοιος αριθμός συμβολίζει μια κλάση αριθμών, οι οποίοι είναι άπειροι στο πλήθος. Έτσι, μια αναφορά στον αριθμό  $-1$  ως μέλος του  $\mathbf{Z}_n$  είναι στην πραγματικότητα μια αναφορά στην κλάση ισοδυναμίας  $[n-1]_n$ , καθώς  $-1 \equiv n-1 \pmod{n}$ .

### Κοινοί διαιρέτες και μέγιστοι κοινοί διαιρέτες

Αν ο ακέραιος  $d$  είναι διαιρέτης του  $a$  και επίσης διαιρεί και τον  $b$ , τότε λέμε ότι ο  $d$  είναι κοινός διαιρέτης των  $a$  και  $b$ . Για παράδειγμα, οι διαιρέτες του 20 είναι οι 1, 2, 4, 5, 10 και 20, συνεπώς οι κοινοί διαιρέτες του 18 και του 20 είναι οι 1 και 2. Ισχύει γενικότερα πως ο αριθμός 1 είναι κοινός διαιρέτης οποιουδήποτε ζεύγους ακεραίων.

Μια σημαντική ιδιότητα ενός κοινού διαιρέτη είναι ότι αν  $d|a$  και  $d|b$ , τότε ισχύει επίσης  $d|(a+b)$  και  $d|(a-b)$ . Γενικότερα, ισχύει η πολύ σημαντική ιδιότητα ότι αν  $d|a$  και  $d|b$ , τότε

$$d|(ax + by), \tag{1}$$

για οποιουδήποτε ακεραίους  $x$  και  $y$ . Με άλλα λόγια, ο  $d$  διαιρεί οποιονδήποτε γραμμικό συνδυασμό των  $a$  και  $b$ . Επίσης, αν  $a|b$ , τότε είτε  $|a| \leq |b|$  ή  $b = 0$ , που συνεπάγεται ότι αν  $a|b$  και  $b|a$ , τότε  $a = \pm b$ .

Ο μέγιστος κοινός διαιρέτης δύο ακεραίων  $a$  και  $b$ , όπου δεν ισούνται και οι δύο με το μηδέν, είναι ο μεγαλύτερος από τους κοινούς διαιρέτες των  $a$  και  $b$  και συμβολίζεται ως  $\gcd(a, b)$ . Για παράδειγμα,  $\gcd(18, 20) = 2$ ,  $\gcd(11, 13) = 1$  και  $\gcd(0, 19) = 19$ . Αν οι  $a$  και  $b$  δεν είναι και

οι δύο μηδέν, τότε ο  $\gcd(a, b)$  είναι ένας ακέραιος μεταξύ του 1 και του  $\min(|a|, |b|)$ . Ορίζουμε ότι  $\gcd(0, 0) = 0$ , προκειμένου οι ακόλουθες στοιχειώδεις σχέσεις να ισχύουν πάντοτε.

$$\begin{aligned}\gcd(a, b) &= \gcd(b, a), \\ \gcd(a, b) &= \gcd(-a, b), \\ \gcd(a, b) &= \gcd(|a|, |b|), \\ \gcd(a, 0) &= |a|, \\ \gcd(a, ka) &= |a|, \quad \forall k \in \mathbf{Z}\end{aligned}$$

Το ακόλουθο θεώρημα παρέχει έναν διαφορετικό ορισμό του  $\gcd(a, b)$ , καθώς κι έναν έμμεσο τρόπο εύρεσής του.

**Θεώρημα 2.** Για οποιουδήποτε ακεραίους  $a$  και  $b$ , όπου δεν ισούνται και οι δύο με το μηδέν, ο  $\gcd(a, b)$  είναι ο ελάχιστος θετικός ακέραιος του συνόλου  $\{ax + by : x, y \in \mathbf{Z}\}$  των γραμμικών συνδυασμών των  $a$  και  $b$ .

Απόδειξη. Έστω  $s$  η τιμή του μικρότερου θετικού γραμμικού συνδυασμού των  $a$  και  $b$  και έστω  $s = ax + by$  για κάποια  $x, y \in \mathbf{Z}$ . Έστω επίσης  $q = \lfloor a/s \rfloor$ , το πηλίκο δηλαδή της διαίρεσης του  $a$  με το  $s$ . Τότε ισχύει ότι

$$\begin{aligned}a \bmod s &= a - qs \\ &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy),\end{aligned}$$

και επομένως ο  $a \bmod s$ , ο οποίος είναι ακέραιος αριθμός, είναι επίσης γραμμικός συνδυασμός των  $a$  και  $b$ . Επειδή όμως  $a \bmod s < s$ , έχουμε ότι  $a \bmod s = 0$ , καθώς ο  $s$  είναι ο μικρότερος θετικός γραμμικός συνδυασμός. Συνεπώς,  $s|a$  και για τον ανάλογο λόγο ισχύει ότι  $s|b$ . Επομένως, ο  $s$  είναι κοινός διαιρέτης των  $a$  και  $b$ , οπότε  $\gcd(a, b) \geq s$ . Από προηγούμενη ιδιότητα συνεπάγεται ότι  $\gcd(a, b)|s$ , καθώς ο  $\gcd(a, b)$  διαιρεί τα  $a$  και  $b$  και ο  $s$  είναι γραμμικός συνδυασμός αυτών των δύο ακεραίων. Επειδή  $\gcd(a, b)|s$  και  $s > 0$ , έχουμε ότι  $\gcd(a, b) \leq s$ . Συνδυάζοντας το ότι  $\gcd(a, b) \geq s$  και  $\gcd(a, b) \leq s$ , προκύπτει πως  $\gcd(a, b) = s$ . Καταλήγουμε λοιπόν ότι ο  $s$  είναι ο μέγιστος κοινός διαιρέτης των  $a$  και  $b$ . □

**Πόρισμα 3.** Για οποιουδήποτε ακεραίους  $a$  και  $b$ , αν  $d|a$  και  $d|b$  τότε  $d|\gcd(a, b)$ .

Απόδειξη. Ισχύει καθώς ο  $\gcd(a, b)$  είναι γραμμικός συνδυασμός των  $a$  και  $b$ . □

**Πόρισμα 4.** Για όλους τους ακεραίους  $a, b$  και για κάθε μη-αρνητικό ακέραιο  $n$ , ισχύει ότι

$$\gcd(an, bn) = n \gcd(a, b).$$

Απόδειξη. Αν  $n = 0$ , τότε προφανώς ισχύει η σχέση, ενώ αν  $n > 0$ , τότε ο  $\gcd(an, bn)$  είναι ο ελάχιστος θετικός εκπρόσωπος του συνόλου  $\{anx + bny\}$  και ισούται με  $n$  φορές τον ελάχιστο θετικό εκπρόσωπο του συνόλου  $\{ax + by\}$ . □

**Πόρισμα 5.** Για όλους τους θετικούς ακεραίους  $n, a$  και  $b$ , αν  $n|ab$  και  $\gcd(a, n) = 1$ , τότε  $n|b$ .

### Πρώτοι και σύνθετοι αριθμοί

Στην συνέχεια θα ασχοληθούμε με τους πρώτους αριθμούς, στις ιδιότητες των οποίων βασίζονται αρκετά πρωτόκολλα κρυπτογραφίας. Ένας ακέραιος  $a > 1$  λέγεται πρώτος αριθμός (ή απλούστερα, πρώτος) όταν οι μόνοι διαιρέτες του είναι οι τετριμμένοι διαιρέτες 1 και  $a$ . Σημειώνουμε πως ο αριθμός 2 είναι ο μόνος ζυγός πρώτος αριθμός, καθώς όλοι οι μεγαλύτεροι ζυγοί αριθμοί διαιρούνται από αυτόν. Ένας ακέραιος μεγαλύτερος του 1 που δεν είναι πρώτος, λέγεται σύνθετος αριθμός. Ο αριθμός 1 δεν είναι ούτε πρώτος ούτε σύνθετος, όπως επίσης ο αριθμός 0 καθώς και όλοι οι αρνητικοί αριθμοί.

Δύο ακέραιοι  $a$  και  $b$  ονομάζονται σχετικά πρώτοι αν ο μόνος κοινός τους διαιρέτης είναι το 1, δηλαδή αν  $\gcd(a, b) = 1$ . Για παράδειγμα, οι 5 και 6 είναι σχετικά πρώτοι, καθώς οι διαιρέτες του 5 είναι οι 1 και 5, ενώ οι διαιρέτες του 6 είναι οι 1, 2, 3 και 6. Το ακόλουθο θεώρημα δηλώνει ότι αν δύο ακέραιοι είναι σχετικά πρώτοι με έναν αριθμό  $p$ , τότε και το γινόμενό τους είναι ένας ακέραιος σχετικά πρώτος με τον  $p$ .

**Θεώρημα 6.** Για οποιουδήποτε ακεραίους  $a, b$  και  $p$ , αν  $\gcd(a, p) = 1$  και  $\gcd(b, p) = 1$ , τότε  $\gcd(ab, p) = 1$ .

Απόδειξη. Προκύπτει από το Θεώρημα 2 ότι υπάρχουν ακέραιοι  $x, y, x'$  και  $y'$ , τέτοιοι ώστε  $ax + py = 1$  και  $bx' + py' = 1$ . Πολλαπλασιάζοντας αυτές τις δύο σχέσεις, έχουμε ότι  $ab(xx') + p(ybx' + y'ax + pyy') = 1$ . Προκύπτει λοιπόν ότι ο αριθμός 1 είναι θετικός γραμμικός συνδυασμός των  $ab$  και  $p$ , οπότε το Θεώρημα 2 αρκεί για να ολοκληρωθεί η απόδειξη. □

Επιπλέον, θα λέμε πως οι ακέραιοι  $n_1, n_2, \dots, n_k$  είναι σχετικά πρώτοι ανά δύο αν  $\gcd(n_i, n_j) = 1$  για  $i \neq j$ .

## Μοναδική παραγοντοποίηση

Ένα απλό αλλά σημαντικό γεγονός για την διαίρεση με πρώτους είναι το ακόλουθο.

**Θεώρημα 7.** Για όλους τους πρώτους  $p$  και όλους τους ακεραίους  $a, b$ , αν  $p|ab$  τότε  $p|a$  ή  $p|b$  (ή και τα δύο).

Απόδειξη. Υποθέτουμε πως  $p|ab$  αλλά  $p \nmid a$  και  $p \nmid b$ . Συνεπώς,  $\gcd(a, p) = 1$  και  $\gcd(b, p) = 1$ , καθώς οι μόνοι διαιρέτες του  $p$  είναι το 1 και ο  $p$ , και από την υπόθεση ο  $p$  δεν διαιρεί ούτε τον  $a$  ούτε τον  $b$ . Από το Θεώρημα 6 προκύπτει ότι  $\gcd(ab, p) = 1$ , κάτι που είναι αντίθετο με την υπόθεση ότι  $p|ab$ , αφού από το ότι  $p|ab$  συνεπάγεται πως  $\gcd(ab, p) = p$ . Αυτή η αντίφαση ολοκληρώνει την απόδειξη.  $\square$

Μια σημαντική συνέπεια του Θεωρήματος 7 είναι το ότι κάθε ακέραιος μπορεί να παραγοντοποιηθεί σε πρώτους αριθμούς με μοναδικό τρόπο.

**Θεώρημα 8.** (Θεώρημα μοναδικής παραγοντοποίησης) Ένας σύνθετος αριθμός  $a$  μπορεί να γραφεί με μοναδικό τρόπο ως γινόμενο της μορφής  $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ , όπου ο  $p_i$  είναι πρώτος,  $p_1 < p_2 < \dots < p_r$  και ο  $e_i$  είναι θετικός ακέραιος.

**Μέγιστος κοινός διαιρέτης** Σε αυτή την ενότητα, περιγράφουμε έναν πολυωνυμικό αλγόριθμο που πρωτοπαρουσιάστηκε από τον Ευκλείδη για την εύρεση του μέγιστου κοινού διαιρέτη δύο ακεραίων. Η ανάλυση του χρόνου εκτέλεσης του αλγορίθμου αποκαλύπτει μια ενδιαφέρουσα σύνδεση με την ακολουθία των αριθμών Fibonacci, η οποία αποτελεί το χειρότερο στιγμιότυπο που μπορεί να δοθεί ως είσοδος.

Στην συνέχεια, θα ασχοληθούμε μόνο με μη-αρνητικούς ακεραίους. Αυτός ο περιορισμός δικαιολογείται, καθώς έχουμε ήδη διατυπώσει πως  $\gcd(a, b) = \gcd(|a|, |b|)$ .

Πριν προχωρήσουμε στην παρουσίαση του αλγορίθμου του Ευκλείδη, παρατηρούμε πως μία εναλλακτική μέθοδος για τον υπολογισμό του μέγιστου κοινού διαιρέτη  $\gcd(a, b)$  δύο ακεραίων  $a$  και  $b$  βασίζεται στην μοναδική παραγοντοποίηση αυτών των ακεραίων. Ας υποθέσουμε πως  $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$  και  $b = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}$ , όπου χρησιμοποιούμε και μηδενικούς εκθέτες προκειμένου το σύνολο των πρώτων  $p_1, p_2, \dots, p_r$  να είναι το ίδιο για τα  $a$  και  $b$ . Τότε, έχουμε  $\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_r^{\min(e_r, f_r)}$ .

Το πρόβλημα με την παραπάνω μέθοδο είναι πως μέχρι στιγμής οι καλύτεροι αλγόριθμοι για την παραγοντοποίηση δεν ολοκληρώνουν την εκτέλεσή τους σε πολυωνυμικό χρόνο, συνεπώς δεν

υπάρχει η δυνατότητα να χρησιμοποιηθούν για να δώσουν έναν αποδοτικό αλγόριθμο για το πρόβλημα της εύρεσης του μέγιστου κοινού διαιρέτη.

Ο αλγόριθμος του Ευκλείδη βασίζεται στο ακόλουθο θεώρημα.

**Θεώρημα 9.** Για κάθε μη-αρνητικό ακέραιο  $a$  και κάθε θετικό ακέραιο  $b$ ,

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

*Απόδειξη.* Θα δείξουμε ότι οι  $\gcd(a, b)$  και  $\gcd(b, a \bmod b)$  διαιρούν ο ένας τον άλλον, επομένως πρέπει να ισούνται (καθώς και οι δύο είναι μη-αρνητικοί ακέραιοι).

Πρώτα, θα δείξουμε πως  $\gcd(a, b) \mid \gcd(b, a \bmod b)$ . Αν ορίσουμε  $d = \gcd(a, b)$ , τότε  $d \mid a$  και  $d \mid b$ . Ισχύει  $(a \bmod b) = a - qb$ , όπου  $q = \lfloor a/b \rfloor$ . Επειδή ο  $(a \bmod b)$  είναι γραμμικός συνδυασμός των  $a$  και  $b$ , έχουμε ότι  $d \mid (a \bmod b)$ . Επομένως, επειδή  $d \mid b$  και  $d \mid (a \bmod b)$ , από το Πρόσχημα 3 προκύπτει ότι  $d \mid \gcd(b, a \bmod b)$ , ή ισοδύναμα, ότι  $\gcd(a, b) \mid \gcd(b, a \bmod b)$ .

Το να δείξουμε ότι  $\gcd(b, a \bmod b)$  γίνεται σχεδόν με τον ίδιο τρόπο. Αν ορίσουμε  $d = \gcd(b, a \bmod b)$ , τότε  $d \mid b$  και  $d \mid (a \bmod b)$ . Επειδή,  $a = qb + (a \bmod b)$ , όπου  $q = \lfloor a/b \rfloor$ , έχουμε ότι ο  $a$  είναι γραμμικός συνδυασμός των  $b$  και  $(a \bmod b)$ . Συμπεραίνουμε λοιπόν ότι  $d \mid a$ . Επειδή  $d \mid b$  και  $d \mid a$ , καταλήγουμε ότι  $d \mid \gcd(a, b)$  (από το Πρόσχημα 3), ή ισοδύναμα, ότι  $\gcd(b, a \bmod b) \mid \gcd(a, b)$ .

Αρκεί να συνδυάσουμε το ότι  $\gcd(a, b) \mid \gcd(b, a \bmod b)$  και το ότι  $\gcd(b, a \bmod b) \mid \gcd(a, b)$  για να ολοκληρωθεί η απόδειξη. □

### Ο αλγόριθμος του Ευκλείδη

Ο ακόλουθος αλγόριθμος πρωτοπαρουσιάστηκε στα *Στοιχεία* (περίπου το 300 π.Χ.), αν και πιθανόν να ήταν γνωστός από παλιότερα. Μπορεί να εκφραστεί ως ένα αναδρομικό πρόγραμμα βασισμένο απευθείας στο Θεώρημα 9. Οι αριθμοί  $a$  και  $b$  που δίνονται ως είσοδος είναι αυθαίρετοι μη-αρνητικοί ακέραιοι.

EUCLID( $a, b$ )

1 αν  $b = 0$

2 τότε επίστρεψε  $a$

3 αλλιώς επίστρεψε EUCLID( $b, a \bmod b$ )



Για παράδειγμα, αν εκτελέσουμε τον παραπάνω αλγόριθμο για να βρούμε τον μέγιστο κοινό διαιρέτη του 30 και του 21, έχουμε

$$\begin{aligned} \text{EUCLID}(20, 15) &= \text{EUCLID}(15, 5) \\ &= \text{EUCLID}(5, 0) \\ &= 5. \end{aligned}$$

Στον παραπάνω υπολογισμό υπάρχουν δύο αναδρομικές κλήσεις του αλγορίθμου του Ευκλείδη (EUCLID). Η ορθότητα του αλγορίθμου πηγάζει από το Θεώρημα 9 και το γεγονός ότι αν ο αλγόριθμος επιστρέφει  $a$  στην γραμμή 2, τότε  $b = 0$ , επομένως  $\text{gcd}(a, b) = \text{gcd}(a, 0) = a$ . Ο αλγόριθμος δεν καλείται αναδρομικά επ' άπειρον, καθώς το δεύτερο όρισμα μειώνεται σε κάθε αναδρομική κλήση και είναι πάντοτε μη-αρνητικός ακέραιος. Συνεπώς, ο αλγόριθμος του Ευκλείδη τερματίζει πάντοτε με το σωστό αποτέλεσμα.

### Χρόνος εκτέλεσης του αλγορίθμου

Στην παράγραφο αυτή θα εξετάσουμε ποιος είναι ο χρόνος εκτέλεσης του αλγορίθμου στην χειρότερη περίπτωση. Θα τον εκφράσουμε σε συνάρτηση με το μέγεθος των  $a$  και  $b$ . Υποθέτουμε, χωρίς βλάβη της γενικότητας, ότι  $a > b \geq 0$ . Αυτή η υπόθεση μπορεί να αιτιολογηθεί από την παρατήρηση πως αν  $b > a \geq 0$ , τότε ο  $\text{EUCLID}(a, b)$  θα κάνει αμέσως αναδρομική κλήση στον  $\text{EUCLID}(b, a)$ . Με άλλα λόγια, αν το πρώτο όρισμα είναι μικρότερο από το δεύτερο, τότε η πρώτη αναδρομική κλήση εναλλάσει την σειρά των ορισμάτων. Παρομοίως, αν  $b = a > 0$ , ο αλγόριθμος τερματίζει μετά από μια αναδρομική κλήση, αφού  $a \bmod b = 0$ .

Ο συνολικός χρόνος εκτέλεσης είναι ανάλογος με τον αριθμό των αναδρομικών κλήσεων και δηλώνεται στο ακόλουθο Λήμμα.

**Λήμμα 10.** Αν  $a > b \geq 1$  και η κλήση του αλγορίθμου  $\text{EUCLID}(a, b)$  προκαλεί  $k \geq 1$  αναδρομικές κλήσεις, τότε  $a \geq F_{k+2}$  και  $b \geq F_{k+1}$ .

Το ακόλουθο θεώρημα προκύπτει ως άμεσο πόρισμα του παραπάνω λήμματος.

**Θεώρημα 11.** Για κάθε ακέραιο αριθμό  $k \geq 1$ , αν  $a > b \geq 1$  και  $b < F_{k+1}$ , τότε ο αλγόριθμος  $\text{EUCLID}(a, b)$  προκαλεί λιγότερες από  $k$  αναδρομικές κλήσεις.

Επειδή μπορούμε να προσεγγίσουμε τον  $k$ -οστό όρο της ακολουθίας Fibonacci  $F_k$  ως  $\phi^k / \sqrt{5}$ , όπου  $\phi^k$  είναι η 'χρυσή τομή', ο αριθμός των αναδρομικών κλήσεων είναι  $O(\log b)$ . Συνεπάγεται

ότι αν ο αλγόριθμος εκτελεσθεί με δύο ορίσματα των  $\beta$  bits, τότε θα χρειαστούν  $O(\beta)$  αριθμητικές πράξεις και  $O(\beta^3)$  πράξεις σε bits (υποθέτουμε πως ο πολλαπλασιασμός και η διαίρεση δύο αριθμών με  $\beta$  bits απαιτούν  $O(\beta^2)$  πράξεις με bits).

**Ο γενικευμένος αλγόριθμος του Ευκλείδη** Σε αυτή την ενότητα θα δούμε πώς μπορούμε να τροποποιήσουμε τον αλγόριθμο του Ευκλείδη ώστε να αποκομίζουμε περισσότερη πληροφορία. Πιο συγκεκριμένα, τροποποιούμε τον αλγόριθμο έτσι ώστε να υπολογίζονται οι ακέραιοι  $x$  και  $y$  που ικανοποιούν την σχέση  $d = \gcd(a, b) = ax + by$ . Σημειώνουμε ότι οι  $x$  και  $y$  μπορεί να είναι και μη-θετικοί ακέραιοι και θα μας φανούν χρήσιμοι για τον υπολογισμό του πολλαπλασιαστικού αντιστρόφου. Ο αλγόριθμος EXTENDED-EUCLID δέχεται ως όρισμα ένα ζευγάρι μη-αρνητικών ακεραίων και επιστρέφει μια τριάδα της μορφής  $(d, x, y)$  που ικανοποιεί την σχέση  $d = \gcd(a, b) = ax + by$ .

EXTENDED-EUCLID( $a, b$ )

1 αν  $b = 0$

2 τότε επίστρεψε  $a$

3  $(d', x', y') \leftarrow \text{EXTENDED-EUCLID}(b, a \bmod b)$

4  $(d, x, y) \leftarrow (d', y', x') \lfloor a/b \rfloor y'$

5 επίστρεψε  $(d, x, y)$

Ο παραπάνω αλγόριθμος βασίζεται στον αλγόριθμο του Ευκλείδη. Αρχικά, η γραμμή 1 είναι ισοδύναμη με τον έλεγχο 'αν  $b = 0$ ' στην γραμμή 1 του EUCLID. Αν  $b = 0$ , τότε ο EXTENDED-EUCLID επιστρέφει όχι μόνο  $d = a$  στην γραμμή 2, αλλά και τους συντελεστές  $x = 1$  και  $y = 0$ , ώστε να ισχύει  $a = ax + by$ . Αν  $b \neq 0$ , ο EXTENDED-EUCLID πρώτα υπολογίζει το  $(d', x', y')$  έτσι ώστε  $d' = \gcd(b, a \bmod b)$  και

$$d' = bx' + (a \bmod b)y' \quad (2)$$

Στον EUCLID, σε αυτή την περίπτωση έχουμε ότι  $d = \gcd(a, b) = d' = \gcd(b, a \bmod b)$ . Για να πάρουμε  $x$  και  $y$  ώστε  $d = ax + by$ , ξαναγράφουμε την ισότητα 2 χρησιμοποιώντας το ότι  $d' = d$ .

$$\begin{aligned} d &= bx' + (a - \lfloor a/b \rfloor b)y' \\ &= ay' + b(x' - \lfloor a/b \rfloor y'). \end{aligned}$$

Συνεπώς, θέτοντας  $x = y'$  και  $y = x' - \lfloor a/b \rfloor y'$  ικανοποιείται η εξίσωση  $d = ax + by$  και αποδεικνύεται η ορθότητα του αλγορίθμου EXTENDED-EUCLID.

Επειδή ο αριθμός των αναδρομικών κλήσεων που γίνονται στον EXTENDED-EUCLID είναι ίσος με τον αριθμό των αναδρομικών κλήσεων που γίνονται στον EUCLID, ο χρόνος εκτέλεσης του EXTENDED-EUCLID διαφέρει από αυτόν του EUCLID κατά έναν σταθερό παράγοντα, δηλαδή, για  $a > b > 0$  ο αριθμός των αναδρομικών κλήσεων είναι  $O(\log b)$ .

## 1.2 Αριθμητικές πράξεις με υπόλοιπα

Στην συνέχεια θα παρουσιάσουμε ορισμένους βασικούς αλγόριθμους που χρησιμοποιούνται στην αριθμητική με υπόλοιπα. Μπορεί κανείς να θεωρήσει την αριθμητική όταν δουλεύουμε με υπόλοιπα ως την κανονική αριθμητική με ακέραιους αριθμούς, μόνο που όταν δουλεύουμε modulo κάποιο ακέραιο αριθμό  $n$ , αντικαθιστούμε κάθε αποτέλεσμα  $x$  με κάποιο στοιχείο από το σύνολο  $\{0, 1, \dots, n-1\}$  που είναι ισοδύναμο με το  $x \bmod n$ . Αυτή η ανεπίσημη θεώρηση είναι αρκετή προκειμένου να περιγράψει κανείς τις πράξεις της πρόσθεσης, της αφαίρεσης και του πολλαπλασιασμού. Για να δώσουμε έναν πιο επίσημο ορισμό, πρέπει πρώτα να περιγράψουμε την έννοια της ομάδας (group).

**Πεπερασμένες ομάδες** Μια ομάδα  $(S, \oplus)$  είναι ένα σύνολο  $S$  συνδεδεμένο με έναν δυαδικό τελεστή  $\oplus$  που ορίζεται στο  $S$  για το οποίο ισχύουν οι ακόλουθες ιδιότητες:

1. Κλειστότητα: Για κάθε  $a, b \in S$ , ισχύει  $a \oplus b \in S$ .
2. Ύπαρξη ουδέτερου στοιχείου: Υπάρχει ένα στοιχείο  $e \in S$ , που καλείται *ουδέτερο στοιχείο* του συνόλου, τέτοιο ώστε  $a \oplus e = e \oplus a = a$  για κάθε  $a \in S$ .
3. Προσεταιριστικότητα: Για όλα τα  $a, b, c \in S$ , ισχύει  $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ .
4. Ύπαρξη αντιστρόφου: Για κάθε  $a \in S$ , υπάρχει ένα μοναδικό στοιχείο, που καλείται *αντίστροφος* του  $a$ , έτσι ώστε  $a \oplus b = b \oplus a = e$ .

Για παράδειγμα, μπορεί κανείς να θεωρήσει την γνώριμη ομάδα  $(Z, +)$  των ακεραίων  $Z$  για την πράξη της πρόσθεσης: το 0 είναι το ουδέτερο στοιχείο και ο αντίστροφος του  $a$  είναι ο  $-a$ . Αν μια ομάδα  $(S, \oplus)$  ικανοποιεί την ιδιότητα της αντιμεταθετικότητας  $a \oplus b = b \oplus a$  για όλα τα  $a, b \in S$ , τότε καλείται *αβελιανή ομάδα*, ενώ αν για μια ομάδα  $(S, \oplus)$ , ισχύει ότι  $|S| < \infty$ , τότε καλείται *πεπερασμένη ομάδα*.

**Ομάδες που ορίζονται από την πρόσθεση και τον πολλαπλασιασμό με υπόλοιπα**  
 Μπορούμε να σχηματίσουμε δύο πεπερασμένες αβελιανές ομάδες χρησιμοποιώντας τις πράξεις της πρόσθεσης και του πολλαπλασιασμού modulo  $n$ , όπου  $n$  είναι ένας θετικός ακέραιος. Αυτές οι ομάδες βασίζονται στις κλάσεις ισοδυναμίας των ακεραίων modulo  $n$ , που ορίστηκαν στο προηγούμενο κεφάλαιο.

Για να ορίσουμε μια ομάδα στο  $Z_n$  πρέπει να έχουμε κατάλληλες δυαδικές πράξεις, τις οποίες μπορούμε τις αποκτήσουμε τροποποιώντας κατάλληλα τις συνηθισμένες πράξεις της πρόσθεσης και του πολλαπλασιασμού. Είναι εύκολο να ορίσουμε την πρόσθεση και τον πολλαπλασιασμό για το  $Z_n$ , επειδή η κλάση ισοδυναμίας δύο ακεραίων προσδιορίζει με μοναδικό τρόπο την κλάση ισοδυναμίας του αθροίσματος ή του γινομένου τους. Δηλαδή, αν  $a \equiv a' \pmod{n}$  και  $b \equiv b' \pmod{n}$ , τότε

$$a + b \equiv a' + b' \pmod{n},$$

$$ab \equiv a'b' \pmod{n}.$$

Συνεπώς, ορίζουμε την πρόσθεση και τον πολλαπλασιασμό modulo  $n$ , με αντίστοιχους συμβολισμούς  $+_n$  και  $\cdot_n$ , ως εξής:

$$[a]_n +_n [b]_n = [a + b]_n, \quad (3)$$

$$[a]_n \cdot_n [b]_n = [ab]_n. \quad (4)$$

Παρατηρούμε πως η αφαίρεση μπορεί να οριστεί με παρόμοιο τρόπο στο  $Z_n$  ως  $[a]_n -_n [b]_n = [a - b]_n$ , αλλά η περίπτωση της διαίρεσης είναι περισσότερο περίπλοκη και θα εξεταστεί αργότερα. Τα παραπάνω δικαιολογούν την συνήθη πρακτική να χρησιμοποιούμε τον μικρότερο μη-αρνητικό ακέραιο κάθε κλάσης ισοδυναμίας ως αντιπρόσωπό της όταν κάνουμε πράξεις στο  $Z_n$ . Οι πράξεις της πρόσθεσης, της αφαίρεσης και του πολλαπλασιασμού γίνονται με ορίσματα τους αντιπροσώπους των κλάσεων ισοδυναμίας και στην συνέχεια κάθε αποτέλεσμα  $x$  αντικαθίσταται από τον αντιπρόσωπο της κλάσης (δηλαδή από το  $x \pmod{n}$ ).

Χρησιμοποιώντας τον παραπάνω ορισμό της πρόσθεσης modulo  $n$ , ορίζουμε την ομάδα πρόσθεσης modulo  $n$  ως  $(Z_n, +_n)$ . Το μέγεθος της ομάδας είναι  $|Z_n| = n$ .

**Θεώρημα 12.** Η ομάδα  $(Z_n, +_n)$  είναι πεπερασμένη και αβελιανή.

Χρησιμοποιώντας τον ορισμό του πολλαπλασιασμού modulo  $n$ , ορίζουμε την ομάδα πολλαπλασιασμού modulo  $n$  ως  $(Z_n^*, \cdot_n)$ . Τα στοιχεία αυτής της ομάδας είναι το σύνολο  $Z_n^*$  των ακεραίων του

$Z_n$  που είναι σχετικά πρώτοι με το  $n$ :

$$Z_n^* = \{[a]_n \in Z_n : \gcd(a, n) = 1\}.$$

Για να δούμε ότι το σύνολο  $Z_n^*$  είναι καλώς ορισμένο, παρατηρούμε ότι για  $0 \leq a < n$ , ισχύει ότι  $a \equiv (a+kn) \pmod{n}$  για όλους τους ακεραίους  $k$ . Συνεπώς, από το ότι  $\gcd(a, n) = 1$  συνεπάγεται πως  $\gcd(a+kn, n) = 1$  για όλους τους ακεραίους  $k$ . Επειδή  $[a]_n = \{a+kn : k \in \mathbb{Z}\}$ , το σύνολο  $Z_n^*$  είναι καλώς ορισμένο. Ένα παράδειγμα τέτοιας ομάδας είναι το

$$Z_{12}^* = \{1, 5, 7, 11\},$$

όπου η πράξη του πολλαπλασιασμού γίνεται modulo 12.

**Θεώρημα 13.** Η ομάδα  $(Z_n^*, \cdot_n)$  είναι πεπερασμένη και αβελιανή.

Ως ένα παράδειγμα υπολογισμού πολλαπλασιαστικού αντιστρόφου, υποθέτουμε πως  $a = 5$  και  $n = 11$ . Τότε ο EXTENDED-EUCLID( $a, n$ ) επιστρέφει  $(d, x, y) = (1, -2, 1)$ , έτσι ώστε  $1 = 5 \cdot (-2) + 11 \cdot 1$ . Συνεπώς, το  $-2$  (δηλαδή το  $9 \pmod{11}$ ) είναι πολλαπλασιαστικός αντίστροφος του  $5 \pmod{11}$ .

Όταν δουλεύουμε με τις ομάδες  $(Z_n, +_n)$  και  $(Z_n^*, \cdot_n)$  στην συνέχεια του κειμένου, θα συνεχίσουμε την συνήθη πρακτική να χρησιμοποιούμε τον εκπρόσωπο μιας κλάσης ισοδυναμίας για να συμβολίσουμε την κλάση, καθώς και τα  $+$  και  $\cdot$  για να συμβολίσουμε τα  $+_n$  και  $\cdot_n$ . Επιπλέον, θα μετατρέπουμε τις ισοδυναμίες modulo  $n$  σε εξισώσεις στο  $Z_n$ . Για παράδειγμα, οι ακόλουθες δύο προτάσεις είναι ισοδύναμες:

$$ax \equiv b \pmod{n}$$

$$[a]_n \cdot_n [x]_n = [b]_n.$$

Επιπλέον, μερικές φορές θα αναφερόμαστε στην ομάδα  $(S, \oplus)$  απλώς ως  $S$ , όταν η πράξη υπονοείται από τα συμφραζόμενα. Επομένως, θα αναφερόμαστε στις ομάδες  $(Z_n, +_n)$  και  $(Z_n^*, \cdot_n)$  ως  $Z_n$  και  $Z_n^*$  αντίστοιχα.

Ο πολλαπλασιαστικός αντίστροφος ενός στοιχείου  $a$  συμβολίζεται με  $(a^{-1} \pmod{n})$ . Η διαίρεση modulo  $n$  ορίζεται από την εξίσωση  $a/b \equiv ab^{-1} \pmod{n}$ . Για παράδειγμα, στο  $Z_{12}^*$  έχουμε ότι  $7^{-1} \equiv 7 \pmod{12}$ , αφού  $7 \cdot 7 \equiv 49 \equiv 1 \pmod{12}$ , και έτσι  $2/7 \equiv 2 \cdot 7 \equiv 2 \pmod{12}$ .

Σε αντίθεση με το σύνολο  $Z_n$  όπου ισχύει ότι  $|Z_n| = n$ , για το σύνολο  $Z_n^*$  τα πράγματα δεν είναι τόσο απλά και χρειάζεται να ορίσουμε μια νέα ποσότητα για να περιγράψουμε το πλήθος των

στοιχείων του. Ο αριθμός λοιπόν των ακεραίων στο  $Z_n^*$  συμβολίζεται με  $\phi(n)$ . Αυτή η συνάρτηση, γνωστή και ως *συνάρτηση  $\phi$  του Euler*, ικανοποιεί την σχέση

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \quad (5)$$

όπου το  $p$  διατρέχει όλους τους πρώτους αριθμούς που διαιρούν το  $n$ , ενώ αν το  $n$  είναι πρώτος τότε συμπεριλαμβάνεται και αυτό. Διαισθητικά, αρχίζουμε από μια λίστα των  $n$  υπολοίπων  $\{0, 1, \dots, n-1\}$  και για κάθε πρώτο  $p$  που διαιρεί το  $n$ , διαγράφουμε όλα τα πολλαπλάσια του  $p$  από την λίστα. Για παράδειγμα, εφόσον οι πρώτοι διαιρέτες του 12 είναι το 2 και το 3

$$\begin{aligned} \phi(12) &= 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) \\ &= 12\left(\frac{1}{2}\right)\left(\frac{2}{3}\right) \\ &= 4, \end{aligned}$$

το οποίο επαληθεύεται από τους προηγούμενους υπολογισμούς μας για την σύσταση του  $Z_{12}^*$ . Αν ο  $p$  είναι πρώτος αριθμός, τότε  $Z_p^* = \{1, 2, \dots, p-1\}$  και

$$\phi(p) = p - 1, \quad (6)$$

ενώ αν ο  $n$  είναι σύνθετος, τότε  $\phi(n) < n - 1$ .

**Υποομάδες** Αν το  $(S, \oplus)$  είναι ομάδα, υπάρχει ένα σύνολο  $S' \subseteq S$  και το  $(S', \oplus)$  είναι επίσης ομάδα, τότε το  $(S', \oplus)$  καλείται υποομάδα του  $(S, \oplus)$ . Για παράδειγμα, οι ζυγοί ακεραίοι αριθμοί αποτελούν υποομάδα των ακεραίων για την πράξη της πρόσθεσης. Το ακόλουθο θεώρημα δηλώνει πως αρκεί να ισχύει η πράξη της κλειστότητας για να είναι ένα υποσύνολο υποομάδα.

**Θεώρημα 14.** *Αν το  $(S, \oplus)$  είναι μια πεπερασμένη ομάδα και το  $S'$  είναι οποιοδήποτε μη-κενό υποσύνολο του  $S$ , τέτοιο ώστε  $a \oplus b \in S'$  για κάθε  $a, b \in S'$ , τότε το  $(S', \oplus)$  είναι υποομάδα του  $(S, \oplus)$*

Για παράδειγμα, το σύνολο  $\{0, 2, 4, 6\}$  αποτελεί υποομάδα του  $Z_8$ , καθώς είναι μη-κενό και ισχύει η ιδιότητα της κλειστότητας για την πράξη της πρόσθεσης. Το ακόλουθο θεώρημα περιγράφει ένα χρήσιμο περιορισμό για το μέγεθος μιας υποομάδας.

**Θεώρημα 15.** *(Θεώρημα του Lagrange) Αν το  $(S, \oplus)$  είναι μια πεπερασμένη ομάδα και το  $(S', \oplus)$  είναι υποομάδα του  $(S, \oplus)$ , τότε το  $|S'|$  είναι μη-τετριμμένος διαιρέτης του  $|S|$ .*

Μια υποομάδα  $S'$  μιας ομάδας  $S$  καλείται *κανονική* υποομάδα αν  $S' \neq S$ . Το ακόλουθο πόρισμα θα φανεί χρήσιμο κατά την ανάλυση του ελέγχου Miller-Rabin για το αν ένας αριθμός είναι πρώτος ή όχι.

**Πόρισμα 16.** Αν το  $S'$  είναι κανονική υποομάδα μιας πεπερασμένη ομάδας  $S$ , τότε  $|S'| \leq |S|/2$ .

**Υποομάδες που προκύπτουν από στοιχείο** Το θεώρημα 14 μας δίνει έναν τρόπο να δημιουργούμε μια υποομάδα μιας πεπερασμένη ομάδας  $(S, \oplus)$ : διαλέγουμε ένα στοιχείο  $a$  και επιλέγουμε όλα τα στοιχεία που μπορούν να δημιουργηθούν από το  $a$  χρησιμοποιώντας την πράξη της ομάδας. Πιο συγκεκριμένα, ορίζουμε το  $a^{(k)}$  για  $k \geq 1$  ως

$$a^{(k)} = \bigoplus_{1 \leq i \leq k} \underbrace{a \oplus a \oplus \dots \oplus a}_k.$$

Για παράδειγμα, αν  $a = 2$  για την ομάδα  $Z_6$ , η ακολουθία  $a^{(1)}, a^{(2)}, \dots$  είναι  $2, 4, 0, 2, 4, 0, \dots$

Στην ομάδα  $Z_n$ , έχουμε  $a^{(k)} = ka \pmod n$  και στην ομάδα  $Z_n^*$  έχουμε  $a^{(k)} = a^k \pmod n$ . Η υποομάδα που προκύπτει από το  $a$  συμβολίζεται με  $\langle a \rangle$  ή  $(\langle a \rangle, \oplus)$  και ορίζεται ως  $\langle a \rangle = \{a^{(k)} : k \geq 1\}$ , ενώ θα λέμε ότι το στοιχείο  $a$  δημιουργεί την υποομάδα  $\langle a \rangle$ .

Εφόσον, το  $S$  είναι πεπερασμένη ομάδα, το  $\langle a \rangle$  είναι πεπερασμένη υποομάδα του  $S$ , που πιθανόν να περιέχει όλα τα στοιχεία του  $S$ . Επειδή, από την προσεταιριστικότητα του  $\oplus$  προκύπτει ότι  $a^{(i)} \oplus a^{(j)} = a^{(i+j)}$ , ισχύει η κλειστότητα για το  $\langle a \rangle$  και από το θεώρημα 14, το  $\langle a \rangle$  είναι υποομάδα του  $S$ . Για παράδειγμα, μερικές υποομάδες στο  $Z_6$  είναι οι

$$\begin{aligned} \langle 0 \rangle &= \{0\} \\ \langle 1 \rangle &= \{0, 1, 2, 3, 4, 5\} \\ \langle 2 \rangle &= \{0, 2, 4\}. \end{aligned}$$

Παρομοίως, για το  $Z_7^*$ , οι πρώτες υποομάδες είναι οι

$$\begin{aligned} \langle 1 \rangle &= \{1\} \\ \langle 2 \rangle &= \{1, 2, 4\} \\ \langle 3 \rangle &= \{1, 2, 3, 4, 5, 6\}. \end{aligned}$$

Η τάξη του  $a$  (για την ομάδα  $S$ ) ορίζεται ως ο ελάχιστος θετικός ακέραιος για τον οποίο  $a^{(t)} = e$  και συμβολίζεται ως  $\text{ord}(a)$ .

**Θεώρημα 17.** Για κάθε πεπερασμένη ομάδα  $(S, \oplus)$  και κάθε  $a \in S$ , η τάξη ενός στοιχείου ισούται με το μέγεθος της υποομάδας που δημιουργεί, ή αλλιώς  $\text{ord}(a) = |\langle a \rangle|$ .

**Πόρισμα 18.** Η ακολουθία  $a^{(1)}, a^{(2)}, \dots$  είναι περιοδική με περίοδο  $t = \text{ord}(a)$ , δηλαδή  $a^{(i)} = a^{(j)}$  αν και μόνο αν  $i \equiv j \pmod{t}$ .

Σύμφωνα με το παραπάνω πόρισμα, μπορούμε να ορίσουμε το  $a^{(0)}$  ως  $e$  και το  $a^{(i)}$  ως  $a^{(i \bmod t)}$ , όπου  $t = \text{ord}(a)$  για κάθε ακέραιο  $i$ .

**Πόρισμα 19.** Αν το  $(S, \oplus)$  είναι πεπερασμένη ομάδα με ουδέτερο στοιχείο το  $e$ , τότε για κάθε  $a \in S$  ισχύει ότι  $a^{(|S|)} = e$ .

**Επίλυση γραμμικών εξισώσεων** Σε αυτή την ενότητα θα ασχοληθούμε με την επίλυση εξισώσεων της μορφής

$$ax \equiv b \pmod{n}, \quad (7)$$

όπου  $a > 0$  και  $n > 0$ . Υπάρχουν αρκετές εφαρμογές αυτού του προβλήματος: για παράδειγμα θα το χρησιμοποιήσουμε ως μέρος της διαδικασίας εύρεσης κλειδιών στο πρωτόκολλο RSA. Υποθέτουμε ότι μας δίνουν τους αριθμούς  $a, b$  και  $n$  και πρέπει να βρούμε τις τιμές του  $x$  modulo  $n$  που ικανοποιούν την εξίσωση 7. Μπορεί να υπάρχουν καμία, μία ή και περισσότερες τέτοιες λύσεις.

Έστω  $\langle a \rangle$  η υποομάδα του  $Z_n$  που δημιουργείται από το στοιχείο  $a$ . Επειδή  $\langle a \rangle = \{a^{(x)} : x > 0\} = \{ax \bmod n : x > 0\}$ , η εξίσωση 7 έχει λύση αν και μόνο αν  $b \in \langle a \rangle$ . Το θεώρημα του Lagrange μας λέει ότι το  $|\langle a \rangle|$  πρέπει να είναι διαιρέτης του  $n$ . Το ακόλουθο θεώρημα παρέχει έναν ακριβή χαρακτηρισμό του  $\langle a \rangle$ .

**Θεώρημα 20.** Για οποιουδήποτε θετικούς ακραίους  $a$  και  $n$ , αν  $d = \text{gcd}(a, n)$ , τότε

$$\langle a \rangle = \langle d \rangle = \{0, d, 2d, \dots, ((n/d) - 1)d\}, \quad (8)$$

στο  $Z_n$  και συνεπώς  $|\langle a \rangle| = n/d$ .

**Απόδειξη.** Αρχίζουμε αποδεικνύοντας πως  $d \in \langle a \rangle$ . Υπενθυμίζουμε ότι ο EXTENDED-EUCLID( $a, n$ ) παράγει ακραίους  $x'$  και  $y'$  τέτοιους ώστε  $ax' + ny' = d$ . Συνεπώς,  $ax' \equiv d \pmod{n}$  οπότε  $d \in \langle a \rangle$ .



Επειδή,  $d \in \langle a \rangle$  έπεται ότι κάθε πολλαπλάσιο του  $d$  ανήκει στο  $\langle a \rangle$ , μιας και κάθε πολλαπλάσιο ενός πολλαπλάσιου του  $a$  είναι με την σειρά του πολλαπλάσιο του  $a$ . Άρα, το  $\langle a \rangle$  περιέχει κάθε στοιχείο από το σύνολο  $\{0, d, 2d, \dots, ((n/d) - 1)d\}$ . Επομένως,  $\langle d \rangle \subseteq \langle a \rangle$ .

Θα δείξουμε τώρα πως  $\langle a \rangle \subseteq \langle d \rangle$ . Αν  $m \in \langle a \rangle$ , τότε  $m = ax \pmod n$  για κάποιον ακέραιο  $x$  και συνεπώς  $m = ax + ny$  για κάποιον ακέραιο  $y$ . Όμως,  $d|a$  και  $d|n$  και επομένως  $d|m$  από την εξίσωση 1. Άρα,  $m \in \langle d \rangle$ .

Συνδυάζοντας τα παραπάνω αποτελέσματα, καταλήγουμε ότι  $\langle a \rangle = \langle d \rangle$ . Για να δείξουμε πως  $|\langle a \rangle| = n/d$ , παρατηρούμε ότι υπάρχουν ακριβώς  $n/d$  πολλαπλάσια του  $d$  ανάμεσα στο 0 και το  $n - 1$ , συμπεριλαμβανομένων των άκρων.  $\square$

**Πόρισμα 21.** Η εξίσωση  $ax \equiv b \pmod n$  λύνεται ως προς το  $x$  αν και μόνο αν  $\gcd(a, n) | b$ .

**Πόρισμα 22.** Η εξίσωση  $ax \equiv b \pmod n$  έχει είτε  $d$  διαφορετικές λύσεις modulo  $n$ , όπου  $d = \gcd(a, n)$ , είτε δεν έχει καμία λύση.

*Απόδειξη.* Αν η  $ax \equiv b \pmod n$  έχει λύση, τότε  $b \in \langle a \rangle$ . Από το Θεώρημα 17,  $\text{ord}(a) = |\langle a \rangle|$  και επομένως συνεπάγεται ότι η ακολουθία  $ai \pmod n$ , για  $i = 0, 1, \dots$ , είναι περιοδική με περίοδο  $|\langle a \rangle| = n/d$ . Αν  $b \in \langle a \rangle$ , τότε το  $b$  εμφανίζεται ακριβώς  $d$  φορές στην ακολουθία  $ai \pmod n$ , για  $i = 0, 1, \dots, n - 1$ , αφού το block μήκους  $n/d$  με τιμές  $\langle a \rangle$  επαναλαμβάνεται ακριβώς  $d$  φορές όσο αυξάνεται το  $i$  από 0 σε  $n - 1$ . Οι δείκτες  $x$  των  $d$  θέσεων για τις οποίες  $ax \pmod n = b$  είναι οι λύσεις της εξίσωσης  $ax \equiv b \pmod n$ .  $\square$

**Θεώρημα 23.** Έστω  $d = \gcd(a, n)$  και  $d = ax' + ny'$  για κάποιους ακεραίους  $x'$  και  $y'$  (όπως υπολογίζονται για παράδειγμα από τον EXTENDED-EUCLID). Αν  $d | b$ , τότε η εξίσωση  $ax \equiv b \pmod n$  έχει ως μία από τις λύσεις τις την τιμή  $x_0$ , όπου

$$x_0 = x'(b/d) \pmod n.$$

*Απόδειξη.* Ισχύει ότι

$$\begin{aligned} ax_0 &\equiv ax'(b/d) \pmod n \\ &\equiv d(b/d) \pmod n \\ &\equiv b \pmod n, \end{aligned}$$

και συνεπώς το  $x_0$  είναι λύση για το  $ax \equiv b \pmod n$ .  $\square$

**Θεώρημα 24.** Έστω ότι η εξίσωση  $ax \equiv b \pmod{n}$  επιλύεται (δηλαδή  $d|b$ , όπου  $d = \gcd(a, n)$ ), και πως το  $x_0$  είναι μια λύση για την εξίσωση. Τότε, η εξίσωση έχει ακριβώς  $d$  διαφορετικές λύσεις modulo  $n$ , που δίνονται από την σχέση  $x_i = x_0 + i(n/d)$  για  $i = 0, 1, \dots, d - 1$ .

Απόδειξη. Αφού  $n/d > 0$  και  $0 \leq i(n/d) \leq n$  για  $i = 0, 1, \dots, n - 1$ , οι τιμές  $x_0, x_1, \dots, x_{d-1}$  είναι όλες διαφορετικές modulo  $n$ . Εφόσον το  $x_0$  είναι λύση της εξίσωσης  $ax \equiv b \pmod{n}$ , έχουμε  $ax_0 \pmod{n} = b$ . Συνεπώς, για  $i = 0, 1, \dots, d - 1$ , έχουμε

$$\begin{aligned} ax_i \pmod{n} &= a(x_0 + in/d) \pmod{n} \\ &= (ax_0 + ain/d) \pmod{n} \\ &= ax_0 \pmod{n} \\ &= b, \end{aligned}$$

και επομένως το  $x_i$  είναι επίσης λύση. Από το πόρισμα 22, υπάρχουν ακριβώς  $d$  λύσεις, οπότε αυτές είναι οι  $x_0, x_1, \dots, x_{d-1}$ . □

Ός τώρα έχουμε παρουσιάσει το απαραίτητο μαθηματικό υπόβαθρο που χρειάζεται για να λύσουμε την εξίσωση  $ax \equiv b \pmod{n}$ , ο ακόλουθος αλγόριθμος υπολογίζει όλες τις λύσεις για την εξίσωση. Οι είσοδοι  $a$  και  $n$  είναι αυθαίρετοι θετικοί ακέραιοι, ενώ το  $b$  είναι ένας αυθαίρετος ακέραιος.

MODULAR-LINEAR-EQUATION-SOLVER( $a, b, n$ )

1  $(d, x', y') \leftarrow \text{EXTENDED-EUCLID}(a, n)$

2 αν  $d|b$

3 τότε  $x_0 \leftarrow x'(b/d) \pmod{n}$

4 για  $i \leftarrow 0$  μέχρι  $d - 1$

5 τύπωσε  $(x_0 + i(n/d)) \pmod{n}$

6 αλλιώς τύπωσε 'δεν υπάρχει λύση'

Ως ένα παράδειγμα της λειτουργίας του παραπάνω αλγορίθμου, ας εξετάσουμε την εξίσωση  $6x \equiv 3 \pmod{21}$ , όπου  $a = 6, b = 3, n = 21$ . Καλώντας τον EXTENDED-EUCLID στην γραμμή 1, παίρνουμε  $(d, x, y) = (3, -3, 1)$ . Επειδή  $3|3$ , εκτελούνται οι γραμμές 3-5 και στην γραμμή 3 υπολογίζουμε το  $x_0 = (-3)(1) \pmod{21} = 18$ , ενώ ο βρόχος στις γραμμές 4-5 τυπώνει τις δύο λύσεις 4 και 11.

Ο MODULAR-LINEAR-EQUATION-SOLVER εκτελεί  $O(\log n + \gcd(a, n))$  αριθμητικές πράξεις, καθώς ο EXTENDED-EUCLID χρειάζεται  $O(\log n)$  αριθμητικές πράξεις και κάθε επανάληψη του βρόχου απαιτεί σταθερό αριθμό από αριθμητικές πράξεις.

Τα ακόλουθα πορίσματα του Θεωρήματος 24 παρουσιάζουν ιδιαίτερο ενδιαφέρον.

**Πόρισμα 25.** Για κάθε  $n > 1$ , αν  $\gcd(a, n) = 1$ , τότε η εξίσωση  $ax \equiv b \pmod{n}$  έχει μοναδική λύση modulo  $n$ .

Αν  $b = 1$ , μια συνηθισμένη περίπτωση με ιδιαίτερο ενδιαφέρον, το  $x$  που αναζητάμε είναι πολλαπλασιαστικός αντίστροφος του  $a$  modulo  $n$ .

**Πόρισμα 26.** Για κάθε  $n > 1$ , αν  $\gcd(a, n) = 1$ , τότε η εξίσωση  $ax \equiv 1 \pmod{n}$  έχει μοναδική λύση modulo  $n$ , αλλιώς δεν υπάρχει λύση.

Το πόρισμα 26 μας επιτρέπει να χρησιμοποιήσουμε τον συμβολισμό  $(a^{-1} \pmod{n})$  για να αναφερθούμε στον πολλαπλασιαστικό αντίστροφο του  $a$  modulo  $n$ , όταν τα  $a$  και  $n$  είναι πρώτοι μεταξύ τους. Αν  $\gcd(a, n) = 1$ , τότε μια λύση για την εξίσωση  $ax \equiv 1 \pmod{n}$  είναι ο ακέραιος  $x$  που επιστρέφεται από τον EXTENDED-EUCLID, καθώς η εξίσωση

$$\gcd(a, n) = 1 = ax + ny$$

υπονοεί ότι  $ax \equiv 1 \pmod{n}$ . Συνεπώς, μπορούμε να υπολογίσουμε το  $(a^{-1} \pmod{n})$  αποδοτικά χρησιμοποιώντας τον EXTENDED-EUCLID.

**Κινέζικο θεώρημα υπολοίπων** Στους πρώτους αιώνες μ.Χ. ο Κινέζος μαθηματικός Sun Tzu ασχολήθηκε κι έλυσε το πρόβλημα της εύρεσης εκείνων των ακεραίων  $x$  που αφήνουν υπόλοιπο 2, 3 και 2 όταν διαιρεθούν με το 3, 5 και το 7 αντίστοιχα. Μια τέτοια λύση είναι το  $x = 23$ : όλες οι λύσεις έχουν την μορφή  $23 + 105k$  για αυθαίρετους ακεραίους  $k$ . Το 'Κινέζικο θεώρημα των υπολοίπων' παρέχει μια αντιστοιχία ανάμεσα σε ένα σύστημα εξισώσεων modulo ενός συνόλου σχετικά πρώτων υπολοίπων (για παράδειγμα 3, 5 και 7) και μιας εξίσωσης modulo το γινόμενο τους (για παράδειγμα το 105).

Το Κινέζικο θεώρημα των υπολοίπων έχει δύο σημαντικές χρήσεις. Έστω ένας ακέραιος  $n$  που παραγοντοποιείται ως  $n = n_1 n_2 \dots n_k$ , όπου οι παράγοντες  $n_i$  είναι ανα δύο πρώτοι μεταξύ τους. Αρχικά, το θεώρημα είναι ένα περιγραφικό 'δομικό θεώρημα' που περιγράφει την δομή του  $Z_n$  ως παρόμοια με αυτή του καρτεσιανού γινομένου  $Z_{n_1} \times Z_{n_2} \times \dots \times Z_{n_k}$ , με πρόσθεση και πολλαπλασιασμό

modulo  $n_i$  για το  $i$ -οστό συστατικό. Επιπλέον, αυτή η περιγραφή μπορεί να χρησιμοποιηθεί ώστε να σχεδιαστούν αποδοτικοί αλγόριθμοι, καθώς είναι αποδοτικότερο να εφαρμοστούν σε καθένα από τα  $Z_{n_i}$  παρά να εφαρμοστούν modulo  $n$ .

**Θεώρημα 27.** (Κινέζικο θεώρημα των υπολοίπων) Έστω  $n = n_1 n_2 \cdots n_k$ , όπου τα  $n_i$  είναι ανά δύο πρώτα μεταξύ τους. Θεωρούμε τις αντιστοιχίες

$$a \leftrightarrow (a_1, a_2, \dots, a_k), \quad (9)$$

όπου  $a \in Z_n$ ,  $a_i \in Z_{n_i}$  και  $a_i = a \pmod{n}$  για  $i = 1, 2, \dots, k$ . Τότε, η αντιστοιχία (9) είναι μια '1-1' αντιστοιχία ανάμεσα στο  $Z_n$  και στο καρτεσιανό γινόμενο  $Z_{n_1} \times Z_{n_2} \times \dots \times Z_{n_k}$ . Οι λειτουργίες που εφαρμόζονται στα στοιχεία του  $Z_n$  μπορούν ισοδύναμα να εφαρμοστούν στις αντίστοιχες  $k$ -άδες με το να εφαρμόζονται ανεξάρτητα σε κάθε αντίστοιχο σύστημα συντεταγμένων. Αυτό σημαίνει πως αν

$$a \leftrightarrow (a_1, a_2, \dots, a_k)$$

$$b \leftrightarrow (b_1, b_2, \dots, b_k),$$

τότε

$$(a + b) \pmod{n} \leftrightarrow ((a_1 + b_1) \pmod{n_1}, \dots, (a_k + b_k) \pmod{n_k}),$$

$$(a - b) \pmod{n} \leftrightarrow ((a_1 - b_1) \pmod{n_1}, \dots, (a_k - b_k) \pmod{n_k}),$$

$$(ab) \pmod{n} \leftrightarrow ((a_1 b_1) \pmod{n_1}, \dots, (a_k b_k) \pmod{n_k}).$$

*Απόδειξη.* Η μετάβαση από την μία αναπαράσταση στην άλλη είναι αρκετά απλή. Από το  $a$  στο  $(a_1, a_2, \dots, a_k)$  απαιτούνται μόνο  $k$  διαιρέσεις. Ο υπολογισμός του  $a$  από τα  $(a_1, a_2, \dots, a_k)$  είναι περισσότερο πολύπλοκος και επιτυγχάνεται ως ακολούθως. Αρχικά, ορίζουμε το  $m_i = n/n_i$  για  $i = 1, 2, \dots, k$ : άρα το  $m_i$  είναι το γινόμενο όλων των  $n_j$  που είναι διαφορετικά από το  $n_i$ . Ακολούθως, ορίζουμε το

$$c_i = m_i(m_i^{-1} \pmod{n_i}) \quad (10)$$

για  $i = 1, 2, \dots, k$ . Η εξίσωση 10 είναι πάντοτε καλώς ορισμένη: επειδή τα  $m_i$  και  $n_i$  είναι πρώτοι μεταξύ τους (από το Θεώρημα 6), το Πρόσμημα 26 εγγυάται ότι υπάρχει το  $(m_i^{-1} \pmod{n_i})$ . Τέλος,

μπορούμε να υπολογίσουμε το  $a$  ως συνάρτηση των  $a_1, a_2, \dots, a_k$  ως εξής:

$$a \equiv (a_1c_1 + a_2c_2 + \dots + a_kc_k) \pmod{n}. \quad (11)$$

Θα δείξουμε τώρα ότι η εξίσωση 11 εγγυάται πως  $a \equiv a_i \pmod{n_i}$  για  $i = 1, 2, \dots, k$ . Παρατηρούμε ότι αν  $j \neq i$ , τότε  $m_j \equiv 0 \pmod{n_i}$ , το οποίο υπονοεί ότι  $c_j \equiv m_j \equiv 0 \pmod{n_i}$ . Παρατηρούμε επίσης ότι  $c_i \equiv 1 \pmod{n_i}$ , από την εξίσωση 10. Έχουμε έτσι την χρήσιμη αντιστοιχία

$$c_i \leftrightarrow (0, 0, \dots, 0, 1, 0, \dots, 0)$$

ένα διάνυσμα που έχει παντού 0 εκτός από την  $i$ -οστή συντεταγμένη, όπου υπάρχει 1· επομένως τα  $c_i$  σχηματίζουν κατά κάποιον τρόπο μια 'βάση' για την αναπαράσταση. Για κάθε  $i$  έχουμε

$$\begin{aligned} a &\equiv a_i c_i \pmod{n_i} \\ &\equiv a_i m_i (m_i^{-1} \pmod{n_i}) \pmod{n_i} \\ &\equiv a_i \pmod{n_i}, \end{aligned}$$

το οποίο είναι αυτό που θέλαμε να αποδείξουμε. Η μέθοδος υπολογισμού του  $a$  από τα  $a_i$  παράγει ένα  $a$  που ικανοποιεί τους περιορισμούς  $a \equiv a_i \pmod{n_i}$  για  $i = 1, 2, \dots, k$ . Η αντιστοιχία είναι '1-1', αφού μπορούμε να μεταβούμε και προς τις δύο κατευθύνσεις.  $\square$

Τα επόμενα πορίσματα θα χρησιμοποιηθούν αργότερα.

**Πόρισμα 28.** Αν τα  $n_1, n_2, \dots, n_k$  είναι πρώτοι μεταξύ τους και  $n = n_1 n_2 \dots n_k$  τότε για όλους τους ακέραιους  $a_1, a_2, \dots, a_k$ , το σύστημα εξισώσεων  $x \equiv a_i \pmod{n_i}$  για  $i = 1, 2, \dots, k$  έχει μοναδική λύση modulo  $n$  για τον άγνωστο  $x$ .

**Πόρισμα 29.** Αν τα  $n_1, n_2, \dots, n_k$  είναι πρώτοι μεταξύ τους και  $n = n_1 n_2 \dots n_k$ , τότε για όλους τους ακέραιους  $x$  και  $a$ ,

$$x \equiv a \pmod{n}$$

για  $i = 1, 2, \dots, k$  αν και μόνο αν

$$x \equiv a \pmod{n}.$$

Ως παράδειγμα μιας εφαρμογής του Κινέζικου θεωρήματος των υπολοίπων, ας υποθέσουμε ότι έχουμε δύο εξισώσεις

$$\begin{aligned} a &\equiv 2 \pmod{5} \\ a &\equiv 3 \pmod{13}, \end{aligned}$$

έτσι ώστε  $a_1 = 2, n_1 = m_2 = 5, a_2 = 3$  και  $n_2 = m_1 = 13$ , και θέλουμε να υπολογίσουμε το  $a \pmod{65}$ , μιας και  $n = 65$ . Επειδή  $13^{-1} \equiv 2 \pmod{5}$  και  $5^{-1} \equiv 8 \pmod{13}$ , έχουμε

$$c_1 = 13(2 \pmod{5}) = 26,$$

$$c_2 = 5(8 \pmod{13}) = 40,$$

και

$$a \equiv 2 \cdot 26 + 3 \cdot 40 \pmod{65}$$

$$\equiv 52 + 120 \pmod{65}$$

$$\equiv 42 \pmod{65}.$$

Συνεπώς, μπορούμε να δουλεύουμε modulo  $n$  απευθείας ή να δουλέψουμε στην μετασχηματισμένη αναπαράσταση χρησιμοποιώντας βολικούς ξεχωριστούς υπολογισμούς modulo  $n_i$ .

**Ύψωση ενός στοιχείου σε δύναμη** Όπως είναι λογικό να εξετάσουμε τα πολλαπλάσια ενός αριθμού  $a$  modulo  $n$ , είναι επίσης λογικό να εξετάσουμε την ακολουθία των δυνάμεων του  $a$  modulo  $n$ , όπου  $a \in Z_n^*$ :

$$a^0, a^1, a^2, a^3, \dots,$$

modulo  $n$ . Δεικτοδοτώντας από το 0, η μηδενική τιμή αυτής της ακολουθίας είναι  $a^0 \pmod{n}$ , και η  $i$ -οστή τιμή είναι το  $a^i \pmod{n}$ . Για παράδειγμα οι δυνάμεις του 2 modulo 7 είναι

|                |   |   |   |   |   |   |   |   |   |   |    |    |     |
|----------------|---|---|---|---|---|---|---|---|---|---|----|----|-----|
| $i$            | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | ... |
| $2^i \pmod{7}$ | 1 | 2 | 4 | 1 | 2 | 4 | 1 | 2 | 4 | 1 | 2  | 4  | ... |

ενώ οι δυνάμεις του 3 modulo 7 είναι

|                |   |   |   |   |   |   |   |   |   |   |    |    |     |
|----------------|---|---|---|---|---|---|---|---|---|---|----|----|-----|
| $i$            | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | ... |
| $3^i \pmod{7}$ | 1 | 3 | 2 | 6 | 4 | 5 | 1 | 3 | 2 | 6 | 4  | 5  | ... |

Σε αυτήν την ενότητα, έστω  $\langle a \rangle$  η υποομάδα του  $Z_n^*$  που δημιουργείται από το  $a$  με επαναλαμβανόμενους πολλαπλασιασμούς, και έστω  $\text{ord}_n(a)$  η τάξη του  $a$  στο  $Z_n^*$ . Για παράδειγμα,  $\langle 2 \rangle = \{1, 2, 4\}$  στο  $Z_7^*$  και  $\text{ord}_7(2) = 3$ . Χρησιμοποιώντας το ότι η συνάρτηση  $\phi$  του Euler ισούται με το μέγεθος του  $Z_n^*$  καθώς και το Πόρισμα 19 οδηγούμαστε στα ακόλουθα θεωρήματα.

**Θεώρημα 30.** (Θεώρημα του Euler) Για όλους τους ακεραίους  $n > 1$ ,

$$a^{\phi(n)} \equiv 1 \pmod{n}, \forall a \in Z_n^*.$$

**Θεώρημα 31.** (Θεώρημα του Fermat) Αν ο  $p$  είναι πρώτος αριθμός, τότε

$$a^{\phi(p)} \equiv 1 \pmod{p}, \forall a \in Z_p^*.$$

Απόδειξη. Από την εξίσωση 6,  $\phi(p) = p - 1$  αν ο  $p$  είναι πρώτος. □

Η τελευταία σχέση ισχύει για κάθε στοιχείο στο  $Z_p$  εκτός από το 0, εφόσον  $0 \notin Z_p^*$ . Από την άλλη, για κάθε  $a \in Z_p$ , ισχύει ότι  $a^p \equiv a \pmod{p}$  αν ο  $p$  είναι πρώτος.

Αν  $\text{ord}_n(g) = |Z_n^*|$  τότε κάθε στοιχείο του  $Z_n^*$  είναι δύναμη του  $g$  modulo  $n$ , και λέμε ότι το  $g$  είναι 'ρίζα' (primitive root) ή 'δημιουργός' (generator) του  $Z_n^*$ . Για παράδειγμα, το 3 είναι ρίζα modulo 7 αλλά το 2 δεν είναι ρίζα modulo 7. Αν το  $Z_n^*$  έχει ρίζα, τότε λέμε ότι η ομάδα  $Z_n^*$  είναι κυκλική.

**Θεώρημα 32.** Οι τιμές του  $n > 1$  για τις οποίες το  $Z_n^*$  είναι κυκλική ομάδα είναι οι  $2, 4, p^e$  και  $2p^e$ , για κάθε πρώτο  $p > 2$  και όλους τους θετικούς ακέραιους  $e$ .

Αν το  $g$  είναι ρίζα του  $Z_n^*$  και το  $a$  είναι στοιχείο του  $Z_n^*$ , τότε υπάρχει ένα  $z$  τέτοιο ώστε  $g^z \equiv a \pmod{n}$ . Αυτό το  $z$  το καλούμε διακριτό λογάριθμο του  $a$  όταν δουλεύουμε modulo  $n$  για την βάση  $g$ .

**Θεώρημα 33.** (Θεώρημα του διακριτού λογαρίθμου) Αν το  $g$  είναι ρίζα του  $Z_n^*$ , τότε η εξίσωση  $g^z \equiv g^y \pmod{n}$  ισχύει αν και μόνο αν ισχύει η εξίσωση  $x \equiv y \pmod{\phi(n)}$ .

Απόδειξη. Έστω ότι  $x \equiv y \pmod{\phi(n)}$ . Τότε,  $x = y + k\phi(n)$  για κάποιον ακέραιο  $k$ . Γί αυτόν τον λόγο

$$\begin{aligned} g^x &\equiv g^{y+k\phi(n)} \pmod{n} \\ &\equiv g^y \cdot (g^{\phi(n)})^k \pmod{n} \\ &\equiv g^y \cdot 1^k \pmod{n} \\ &\equiv g^y \pmod{n} \end{aligned}$$

Από την άλλη πλευρά, έστω  $g^x \equiv g^y \pmod{n}$ . Επειδή η ακολουθία των δυνάμεων του  $g$  δημιουργεί κάθε στοιχείο του  $\langle g \rangle$  και  $|\langle g \rangle| = \phi(n)$ , από το Πρόγραμμα 18 συνεπάγεται ότι η ακολουθία των δυνάμεων του  $g$  είναι περιοδική με περίοδο  $\phi(n)$ . Συνεπώς, αν  $g^x \equiv g^y \pmod{n}$  τότε πρέπει και  $x \equiv y \pmod{\phi(n)}$ . □

**Ύψωση σε δύναμη με επαναλαμβανόμενο τετραγωνισμό** Μια πράξη που συναντάται συχνά στην θεωρία αριθμών είναι η ύψωση ενός αριθμού σε μια δύναμη modulo κάποιον άλλο αριθμό· μια πράξη που είναι γνωστή και ως *ύψωση παρουσία υπολοίπου* (modular exponentiation). Για την ακρίβεια, αυτό που αναζητούμε είναι ένας αποδοτικός τρόπος να υπολογίσουμε το  $a^b \bmod n$ , όπου τα  $a$  και  $b$  είναι μη-αρνητικοί ακέραιοι και το  $n$  είναι θετικός ακέραιος. Η ύψωση παρουσία υπολοίπου είναι μια σημαντική πράξη σε πολλές μεθόδους που ελέγχουν αν ένας αριθμός είναι πρώτος ή όχι, καθώς και στο πρωτόκολλο RSA. Η μέθοδος του *επαναλαμβανόμενου τετραγωνισμού* λύνει αυτό το πρόβλημα αποδοτικά, χρησιμοποιώντας την δυαδική αναπαράσταση του  $b$ .

Έστω  $\langle b_k, b_{k-1}, \dots, b_1, b_0 \rangle$  η δυαδική αναπαράσταση του  $b$ . Αυτό σημαίνει ότι η δυαδική αναπαράσταση έχει μήκος  $k + 1$  bits, το  $b_k$  είναι το πιο σημαντικό bit, ενώ το  $b_0$  είναι το λιγότερο σημαντικό bit. Ο ακόλουθος αλγόριθμος υπολογίζει το  $a^c \bmod n$ , καθώς το  $c$  αυξάνεται με διπλασιασμούς και προσθέσεις από 0 σε  $b$ .

MODULAR-EXPONENTIATION( $a, b, n$ )

1  $c \leftarrow 0$

2  $d \leftarrow 1$

3 έστω  $\langle b_k, b_{k-1}, \dots, b_1, b_0 \rangle$  η δυαδική αναπαράσταση του  $b$

4 για  $i \leftarrow k$  μέχρι 0

5      $c \leftarrow 2c$

6      $d \leftarrow (d \cdot d) \bmod n$

7     αν  $b_i = 1$

8         τότε  $c \leftarrow c + 1$

9          $d \leftarrow (d \cdot a) \bmod n$

επίστρεψε  $d$

Η ύψωση στο τετράγωνο στην γραμμή 6 εξηγεί γιατί η μέθοδος αυτή ονομάζεται 'επαναλαμβανόμενος τετραγωνισμός'. Για παράδειγμα, αν  $a = 7, b = 560$  και  $n = 561$ , ο αλγόριθμος υπολογίζει μια ακολουθία τιμών modulo 561, όπως φαίνονται παρακάτω. Η ακολουθία των εκθετών που χρησιμοποιούνται φαίνεται στην γραμμή με δείκτη  $c$ . Η μεταβλητή  $c$  δεν είναι αναγκαία για την εκτέλεση του αλγορίθμου, αλλά συμπεριλαμβάνεται γιατί βοηθάει στην κατανόηση και την ανάλυσή του.



|       |   |    |     |     |     |     |     |     |     |     |
|-------|---|----|-----|-----|-----|-----|-----|-----|-----|-----|
| $i$   | 9 | 8  | 7   | 6   | 5   | 4   | 3   | 2   | 1   | 0   |
| $b_i$ | 1 | 0  | 0   | 0   | 1   | 1   | 0   | 0   | 0   | 0   |
| $c$   | 1 | 2  | 4   | 8   | 17  | 35  | 70  | 140 | 280 | 560 |
| $d$   | 7 | 49 | 157 | 526 | 160 | 241 | 298 | 166 | 67  | 1   |

Ο αλγόριθμος είναι σχεδιασμένος έτσι ώστε να ισχύουν τα ακόλουθα:

1. Η τιμή του  $c$  είναι ίδια με το πρόθεμα  $\langle b_k, b_{k-1}, \dots, b_1, b_0 \rangle$  της δυαδικής αναπαράστασης του  $b$  και
2.  $d = a^c \pmod n$

Αν οι είσοδοι  $a, b$  και  $n$  είναι αριθμοί με  $\beta$  bits, τότε ο συνολικός αριθμός των αριθμητικών πράξεων που απαιτούνται είναι  $O(\beta)$  και ο συνολικός αριθμός των πράξεων σε bits είναι  $O(\beta^3)$ .

**Τετραγωνικά υπόλοιπα και εύρεση τετραγωνικών ριζών** Στην παράγραφο αυτή θα εξετάσουμε το πρόβλημα της επίλυσης της εξίσωσης

$$x^2 = a \pmod n, \quad (12)$$

με άλλα λόγια το πρόβλημα της εύρεσης τετραγωνικών ριζών.

Καταρχάς, τονίζουμε ότι η παραπάνω εξίσωση ενδέχεται να μην έχει καν κάποια λύση. Οι ακέραιοι  $a$  για τους οποίους η εξίσωση (12) έχει κάποια λύση ονομάζονται *τετραγωνικά υπόλοιπα* (quadratic residues) modulo  $a$ , ενώ αυτοί για τους οποίους δεν υπάρχει λύση ονομάζονται *τετραγωνικά μη-υπόλοιπα* (quadratic non-residues). Στην συνέχεια, διακρίνουμε δύο περιπτώσεις που ορίζονται από το αν ο  $n$  είναι πρώτος ή σύνθετος.

Στην περίπτωση που είναι πρώτος, τότε, ακολουθώντας την σύμβαση να συμβολίζουμε τους πρώτους αριθμούς με  $p$ , προκύπτει η ισοδυναμία  $x^2 = a \pmod p$ . Ένα βασικό αποτέλεσμα που σχετίζεται με τα τετραγωνικά υπόλοιπα modulo έναν πρώτο αριθμό είναι το κριτήριο του Euler.

**Θεώρημα 34.** Ένας ακέραιος  $a$  στο διάστημα  $1 \leq a \leq p - 1$  είναι τετραγωνικό υπόλοιπο modulo έναν περιττό πρώτο αριθμό  $p$  αν και μόνο αν

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

Αν συμβολίσουμε με  $Q_p$  (αντίστοιχα, με  $\overline{Q}_p$ ) το σύνολο των τετραγωνικών υπολοίπων (αντίστοιχα, των τετραγωνικών μη-υπολοίπων) όταν δουλεύουμε modulo έναν πρώτο αριθμό  $p$ , τότε

ισχύει ότι  $|Q_p| = |\overline{Q}_p| = |Z_p^*| = (p-1)/2$ , με άλλα λόγια ακριβώς οι μισοί ακέραιοι στο  $Z_p^*$  είναι τετραγωνικά υπόλοιπα modulo  $p$ . Για παράδειγμα, όταν  $p = 13$  τότε  $Q_{13} = \{1, 3, 4, 9, 10, 12\}$  και  $\overline{Q}_{13} = \{2, 5, 6, 7, 8, 11\}$ , γιατί  $1^6 = 1 \pmod{13}$ ,  $2^6 = 12 \pmod{13}$  κοκ.

Στην περίπτωση που ο  $n$  είναι σύνθετος αριθμός τέτοιος ώστε  $n = pq$ , όπου  $p, q$  πρώτοι αριθμοί, τότε ένας ακέραιος  $a \in Z_n^*$  είναι τετραγωνικό υπόλοιπο modulo  $n$  αν και μόνο αν είναι τετραγωνικό υπόλοιπο τόσο modulo  $p$  όσο και modulo  $q$ . Επομένως, ισχύει ότι  $|Q_n| = |Q_p||Q_q| = (p-1)(q-1)/4$  και  $|\overline{Q}_q| = 3(p-1)(q-1)/4$ . Για παράδειγμα, αν  $n = 21$ , τότε  $Q_{21} = \{1, 4, 16\}$  και  $\overline{Q}_{21} = \{2, 5, 8, 10, 11, 13, 17, 19, 20\}$ .

Στην συνέχεια θα ασχοληθούμε με το πρόβλημα της εύρεσης της τετραγωνικής ρίζας ενός τετραγωνικού υπολοίπου, με άλλα λόγια με τον υπολογισμό ενός  $x \in Z_n^*$  τέτοιου ώστε  $x^2 = a \pmod{n}$ , όταν γνωρίζουμε ότι  $a \in Q_n$ . Κάνουμε πάλι την διάκριση σχετικά με το αν ο  $n$  είναι πρώτος ή σύνθετος.

Έστω λοιπόν ότι δουλεύουμε modulo έναν πρώτο αριθμό  $p$  και μάλιστα υποθέτουμε ότι ισχύει  $p \equiv 3 \pmod{4}$ . Για την εύρεση της λύσης χρησιμοποιούμε το ακόλουθο λήμμα.

**Λήμμα 35.** *Αν ο  $p$  είναι πρώτος αριθμός της μορφής  $4k - 1$  και το  $a$  είναι τετραγωνικό υπόλοιπο modulo  $p$ , τότε οι λύσεις της εξίσωσης*

$$x^2 = a \pmod{p}$$

δίνεται από την σχέση

$$x = \pm a^k \pmod{p}.$$

Απόδειξη. Επειδή γνωρίζουμε πως το  $a$  είναι τετραγωνικό υπόλοιπο modulo  $p$ , το κριτήριο του Euler δίνει

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

Επειδή  $k = \frac{1}{4}(p+1)$ , έχουμε πως

$$\begin{aligned} a^{\frac{1}{4}(p+1)} a^{\frac{1}{4}(p+1)} &= a^{\frac{1}{2}(p+1)} = a^{\frac{1}{2}(p-1)} a \\ &= a \pmod{p}. \end{aligned}$$

□

Στην περίπτωση που δουλεύουμε modulo έναν σύνθετο  $n = pq$ , όπου  $p, q$  πρώτοι αριθμοί τέτοιοι ώστε  $p \equiv q \equiv 3 \pmod{4}$ , τότε ακολουθούμε τα ακόλουθα βήματα.

1. Αρχικά πρέπει να βρούμε τις λύσεις  $(r, -r)$  της ισοδυναμίας  $x^2 = a \pmod{p}$ .
2. Υπολογίζουμε αντιστοίχως τις λύσεις  $(s, -s)$  της ισοδυναμίας  $x^2 = a \pmod{q}$ .
3. Υπολογίζουμε  $c, d$  τέτοια ώστε  $cp + dq = 1$ . Σημειώνουμε πως αυτό είναι εφικτό χρησιμοποιώντας τον αλγόριθμο EXTENDED-EUCLID αφού  $\gcd(p, q) = 1$ .
4. Υπολογίζουμε τα  $x = rdq + scp \pmod{n}$  και  $y = rdq - scp \pmod{n}$ .
5. Επιστρέφουμε ως λύσεις τους αριθμούς  $(\pm x, \pm y)$ .

Παρατηρούμε ότι ο παραπάνω αλγόριθμος βασίζεται στην γνώση της παραγοντοποίησης του  $n$ . Γενικότερα, ισχύει το ισχυρότερο αποτέλεσμα ότι το πρόβλημα της εύρεσης τετραγωνικών ριζών modulo  $n$  όταν  $n = pq$  είναι υπολογιστικά ισοδύναμο με το πρόβλημα της παραγοντοποίησης του  $n$  στους πρώτους παράγοντες  $p$  και  $q$ . Αν έχουμε έναν πολυωνυμικό αλγόριθμο για το πρόβλημα της παραγοντοποίησης, τότε τον χρησιμοποιούμε για να βρούμε τα  $p, q$  και στην συνέχεια εκτελούμε τον παραπάνω αλγόριθμο για να βρούμε τις τετραγωνικές ρίζες. Για την αντίθετη κατεύθυνση, έστω ότι έχουμε έναν πολυωνυμικό αλγόριθμο  $\mathcal{A}(a, n)$  που επιστρέφει κάποια τετραγωνική ρίζα του  $a$  modulo  $n$ . Τότε αρκεί να διαλέξουμε ένα  $x \in \mathbb{Z}_n^*$ , να υπολογίσουμε το  $a = x^2 \pmod{n}$  και να εκτελέσουμε τον  $\mathcal{A}(a, n)$  και έστω  $y$  η επιστρεφόμενη τετραγωνική ρίζα. Αν  $y = \pm x \pmod{n}$ , τότε αποτύχαμε και πρέπει να δοκιμάσουμε πάλι διαλέγοντας κάποια διαφορετική τιμή για το  $x$ , αλλιώς ο  $\gcd(x - y, n)$  είναι παράγοντας του  $n$ , είτε ο  $p$  είτε ο  $q$ .

Ένας αριθμός  $x$  καλείται *μη τετριμμένη τετραγωνική ρίζα του 1*, όταν δουλεύουμε modulo  $n$  αν επαληθεύει την εξίσωση  $x^2 \equiv 1 \pmod{n}$  αλλά είναι διαφορετικός από τις δύο τετριμμένες ρίζες:  $1$  ή  $-1 \pmod{n}$ . Για παράδειγμα το 6 είναι μη-τετριμμένη τετραγωνική ρίζα του 1 modulo 35. Το ακόλουθο πόρισμα θα μας φανεί χρήσιμο για να αποδείξουμε την ορθότητα του ελέγχου Miller-Rabin για το αν ένας αριθμός είναι πρώτος ή όχι.

**Πόρισμα 36.** *Αν υπάρχει μη-τετριμμένη ρίζα του 1 modulo  $n$ , τότε ο  $n$  είναι σύνθετος αριθμός.*

## 2 Πρωτόκολλα δημοσίου κλειδιού

Στην ενότητα αυτή αφού ορίσουμε τι είναι τα πρωτόκολλα δημοσίου κλειδιού και κάνουμε μια σύγκριση ανάμεσα στα πρωτόκολλα δημόσιου και ιδιωτικού κλειδιού, στην συνέχεια παρουσιάζουμε ορισμένα πρωτόκολλα δημοσίου κλειδιού, δίνοντας ιδιαίτερη έμφαση στο πρωτόκολλο RSA.

Ένα σύστημα δημοσίου κλειδιού μπορεί να χρησιμοποιηθεί για να κρυπτογραφηθούν τα μηνύματα που δύο οντότητες θέλουν να ανταλλάξουν κατά την επικοινωνία τους. Ο στόχος είναι να μην μπορεί κάποιος που κρυφακούει το κανάλι επικοινωνίας να καταλάβει το περιεχόμενο του, ενώ ένα σύστημα δημοσίου κλειδιού επιτρέπει επίσης στον αποστολέα να επισυνάψει στο μήνυμα μια 'ψηφιακή υπογραφή' που δεν γίνεται να πλαστογραφηθεί. Μια τέτοια υπογραφή μπορεί να θεωρηθεί ως το ηλεκτρονικό αντίστοιχο της χειρόγραφης υπογραφής σε ένα κείμενο γραμμένο σε χαρτί. Μπορεί εύκολα να επαληθευθεί από οποιονδήποτε διαβάζει το κείμενο, αλλά δύσκολα μπορεί κάποιος να την πλαστογραφήσει, επιπλέον, αν αλλάξει έστω κι ένα bit από το κείμενο, η υπογραφή χάνει την εγκυρότητά της. Επομένως, παρέχει έναν τρόπο να πιστοποιείται τόσο η ταυτότητα του χρήστη-αποστολέα, όσο και το περιεχόμενο του μηνύματος.

Σε ένα σύστημα δημοσίου κλειδιού, κάθε συμμετέχον μέρος έχει ένα δημόσιο κλειδί και ένα μυστικό κλειδί. Κάθε κλειδί περιέχει ένα κομμάτι πληροφορίας. Είναι σύνηθες τα συμμετέχοντα μέρη που επιθυμούν να χρησιμοποιήσουν κρυπτογραφικές μεθόδους κατά την επικοινωνία τους να καλούνται με τα ονόματα Alice και Bob. Συμβολίζουμε με  $P_A, S_A$  τα κλειδιά της Alice και με  $P_B, S_B$  τα κλειδιά του Bob.

Κάθε συμμετέχων δημιουργεί το δικό του δημόσιο και μυστικό κλειδί και φροντίζει έτσι ώστε το μυστικό κλειδί να μην το μάθει κανείς άλλος, αλλά μπορεί να ανακοινώσει το δημόσιο σε οποιονδήποτε ή και να το δημοσιοποιήσει σε όλους. Στην πραγματικότητα, η δεύτερη επιλογή είναι προτιμότερη και συνήθως υπάρχει ένας δημόσιος κατάλογος που περιέχει δημόσια κλειδιά διαφόρων χρηστών, έτσι ώστε να διευκολύνεται η εύρεση του δημόσιου κλειδιού κάποιου χρήστη.

Το δημόσιο και το μυστικό κλειδί καθορίζουν κάποιες συναρτήσεις-μετασχηματισμούς εφαρμόζονται σε οποιοδήποτε μήνυμα. Έστω  $\mathcal{D}$  το σύνολο όλων των επιτρεπτών μηνυμάτων. Για παράδειγμα, το  $\mathcal{D}$  μπορεί να είναι το σύνολο όλων των ακολουθιών με πεπερασμένο αριθμό από bits. Στον αρχικό, και απλούστερο, ορισμό της κρυπτογραφίας δημοσίου κλειδιού, απαιτείται το δημόσιο και το μυστικό κλειδί να καθορίζουν συναρτήσεις '1-1' από το  $\mathcal{D}$  στον εαυτό του. Η συνάρτηση που αντιστοιχεί στο δημόσιο κλειδί  $P_A$  της Alice συμβολίζεται με  $P_A()$  και η συνάρτηση που αντιστοιχεί

στο μυστικό κλειδί  $S_A$  με  $S_A()$ . Οι συναρτήσεις  $P_A()$  και  $S_A()$  είναι λοιπόν μεταθέσεις του  $\mathcal{D}$ . Υποθέτουμε ότι οι  $P_A()$  και  $S_A()$  μπορούν να υπολογισθούν αποδοτικά, δεδομένων των αντίστοιχων κλειδιών  $P_A$  και  $S_A$ .

Το δημόσιο κλειδί και το μυστικό κλειδί κάθε χρήστη αποτελούν ‘ζευγάρι’ υπό την έννοια ότι ορίζουν συναρτήσεις που η μία είναι αντίστροφη της άλλης, δηλαδή

$$M = S_A(P_A(M)), \quad (13)$$

$$M = P_A(S_A(M)), \quad (14)$$

για οποιοδήποτε μήνυμα  $m \in \mathcal{D}$ . Αν μετασχηματίσουμε επιτυχώς το  $M$  με τα δύο κλειδιά  $P_A$  και  $S_A$ , με οποιαδήποτε σειρά, θα πρέπει να καταλήξουμε και πάλι στο αρχικό μήνυμα  $M$ .

Σε ένα σύστημα δημοσίου κλειδιού είναι σημαντικό να μην μπορεί κανείς παρά μόνο η Alice να υπολογίσει την συνάρτηση  $S_A()$  σε κάποιο λογικό χρονικό διάστημα. Η ιδιωτικότητα της ηλεκτρονικής επικοινωνίας που κρυπτογραφείται και στέλνεται στην Alice και η αυθεντικότητα της ψηφιακής υπογραφής της Alice στηρίζονται στην υπόθεση ότι μόνο η Alice μπορεί να υπολογίσει την  $S_A()$ . Αυτή η προϋπόθεση εξηγεί γιατί η Alice πρέπει να κρατήσει μυστικό το  $S_A$ : αν δεν το κάνει, τότε χάνει την μοναδικότητά της ως χρήστης και το σύστημα δημοσίου κλειδιού δεν μπορεί να την ‘προστατεύσει’. Η υπόθεση ότι μόνο η Alice μπορεί να υπολογίσει την  $S_A()$  πρέπει να ισχύει ακόμα κι αν κανένας γνωρίζει το  $P_A$  και μπορεί σε λογικό χρονικό διάστημα να υπολογίσει την  $P_A()$ , που είναι αντίστροφη της  $S_A()$ . Η μεγάλη δυσκολία στον σχεδιασμό ενός πρακτικού συστήματος δημοσίου κλειδιού είναι το πώς θα δημιουργηθεί ένα πρωτόκολλο που επιτρέπει την δημοσιοποίηση της  $P_A()$ , χωρίς να μπορεί να βρεθεί η αντίστροφη συνάρτηση  $S_A()$ .

Σε ένα σύστημα δημοσίου κλειδιού, η κρυπτογράφηση γίνεται ως εξής: υποθέτουμε ότι ο Bob θέλει να στείλει στην Alice ένα μήνυμα  $M$  με τέτοιο τρόπο έτσι ώστε οποιοσδήποτε κρυφακούει το κανάλι επικοινωνίας να μην μπορεί να καταλάβει τι είναι το μήνυμα. Το πρωτόκολλο δουλεύει ως εξής:

- Ο Bob βρίσκει το δημόσιο κλειδί  $P_A$  της Alice (είτε από κάποιον δημόσιο κατάλογο είτε απευθείας από την Alice).
- Ο Bob υπολογίζει το κρυπτογραφημένο μήνυμα  $C = P_A(M)$  που αντιστοιχεί στο μήνυμα  $M$  και στέλνει το  $C$  στην Alice.

- Όταν η Alice λάβει το κρυπτογραφημένο μήνυμα  $C$ , χρησιμοποιεί το μυστικό της κλειδί  $S_A$  για να ανακτήσει το αρχικό μήνυμα  $M = S_A(C)$ .

Επειδή οι  $S_A()$  και  $P_A()$  είναι αντίστροφες συναρτήσεις, η Alice μπορεί να υπολογίσει το μήνυμα  $M$  από το  $C$ . Επειδή μόνο η Alice μπορεί να υπολογίσει την  $S_A()$ , είναι ταυτόχρονα και η μόνη που μπορεί να υπολογίσει το  $M$  από το  $C$ . Η κρυπτογράφηση του  $M$  με την  $P_A()$  προστατεύει το περιεχόμενο του μηνύματος και δεν επιτρέπει την ανάγνωσή του, παρά μόνο στην Alice.

Οι ψηφιακές υπογραφές είναι επίσης εύκολο να υλοποιηθούν με αυτόν τον ορισμό του συστήματος δημοσίου κλειδιού. Σημειώνουμε πως υπάρχουν κι άλλες μέθοδοι να προσεγγιστεί το πρόβλημα δημιουργίας ψηφιακών υπογραφών, αλλά δεν θα μας απασχολήσουν στην παρούσα ενότητα. Υποθέτουμε ότι η Alice θέλει να απαντήσει στον Bob με ένα μήνυμα  $M'$  που έχει υπογραφεί ψηφιακά, οπότε προκύπτουν τα ακόλουθα.

- Η Alice υπολογίζει την ψηφιακή της υπογραφή  $\sigma$  για το μήνυμα  $M'$  χρησιμοποιώντας το μυστικό κλειδί  $S_A$  και την σχέση  $\sigma = S_A(M')$ .
- Η Alice στέλνει το ζεύγος μηνύματος-υπογραφής  $(M', \sigma)$  στον Bob.
- Όταν ο Bob λάβει το  $(M', \sigma)$ , μπορεί να επιβεβαιώσει ότι προέρχεται από την Alice χρησιμοποιώντας το δημόσιο κλειδί της Alice για να επαληθεύσει την σχέση  $M' = P_A(\sigma)$ . Υποθέτουμε ότι το  $M'$  περιέχει το όνομα της Alice, ώστε ο Bob να ξέρει ποιο δημόσιο κλειδί να χρησιμοποιήσει. Αν η σχέση επαληθευτεί, τότε ο Bob μπορεί να συμπεράνει ότι το μήνυμα  $M'$  περιέχει όντως την ψηφιακή υπογραφή της Alice. Αν δεν επαληθευτεί, τότε ο Bob μπορεί να συμπεράνει είτε ότι το μήνυμα είτε η ψηφιακή υπογραφή 'πειράχτηκαν' κατά την μετάδοση. Αυτό μπορεί να οφείλεται σε λάθος του καναλιού μετάδοσης, μπορεί όμως και να έγινε απόπειρα πλαστογράφησης της υπογραφής ή απόπειρα τροποποίησης του μηνύματος.

Επειδή η ψηφιακή υπογραφή προσφέρει ταυτόχρονα ταυτοποίηση του αποστολέα που υπογράφει και πιστοποίηση του περιεχομένου του μηνύματος, είναι ανάλογη με την χειρόγραφη υπογραφή σε ένα κείμενο που υπάρχει στο χαρτί.

Μια σημαντική ιδιότητα της ψηφιακής υπογραφής είναι ότι μπορεί να επιβεβαιωθεί από οποιονδήποτε που έχει πρόσβαση στο δημόσιο κλειδί του αποστολέα. Ένα υπογεγραμμένο μήνυμα μπορεί να επιβεβαιωθεί από έναν χρήστη και μετά να μεταβιβαστεί σε άλλους χρήστες, οι οποίοι ακολουθώντας

μπορούν να επιβεβαιώσουν την υπογραφή. Για παράδειγμα, το μήνυμα μπορεί να είναι μια ηλεκτρονική επιταγή από την Alice για τον Bob. Αφού ο Bob επαληθεύσει την ψηφιακή υπογραφή της Alice, μπορεί να δώσει την επιταγή στην τράπεζά του, η οποία μπορεί επίσης να επαληθεύσει την υπογραφή της Alice και να προβεί στην αντίστοιχη συναλλαγή.

Σημειώνουμε ότι ως τώρα θεωρούμε ότι το μήνυμα δεν έχει κρυπτογραφηθεί, μεταδίδεται όπως είναι και δεν προστατεύεται από κάποιον που παρακολουθεί το κανάλι επικοινωνίας. Συνθέτοντας το πρωτόκολλο της κρυπτογράφησης με αυτό της ψηφιακής υπογραφής, μπορούμε να δημιουργήσουμε μηνύματα που είναι ταυτόχρονα κρυπτογραφημένα και υπογεγραμμένα. Ο αποστολέας πρώτα επισυνάπτει την ψηφιακή υπογραφή στο τέλος του μηνύματος και ακολούθως κρυπτογραφεί το ζεύγος μηνύματος-υπογραφής με το δημόσιο κλειδί του παραλήπτη. Ο παραλήπτης, αφού λάβει το μήνυμα, αποκρυπτογραφεί με το μυστικό του κλειδί για να αποκτήσει το ζεύγος μηνύματος υπογραφής και στην συνέχεια επαληθεύει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα. Η αντίστοιχη διαδικασία σε έγγραφη επικοινωνία θα ήταν να υπογράψει ο αποστολέας το έγγραφο και στην συνέχεια να το βάλει σε κλειστό φάκελο που θα ανοιχθεί μόνο από τον παραλήπτη.

**Σύγκριση με πρωτόκολλα ιδιωτικού κλειδιού** Η βασική διαφορά μεταξύ των πρωτοκόλλων δημοσίου κλειδιού και ιδιωτικού κλειδιού είναι ότι στα πρώτα δεν υπάρχει η απαίτηση το κλειδί που χρησιμοποιείται για την κρυπτογράφηση ενός μηνύματος να είναι ίδιο με αυτό που χρησιμοποιείται για την αποκρυπτογράφηση. Το γεγονός αυτό επιτρέπει την δημοσιοποίηση του κλειδιού που χρησιμοποιείται για την κρυπτογράφηση, με τον σημαντικό περιορισμό ότι θα πρέπει να μην είναι εφικτό να χρησιμοποιηθεί αυτή η γνώση ώστε να προκύψει το κλειδί της αποκρυπτογράφησης, το οποίο αποκαλείται και *μυστικό κλειδί*. Αντίθετα, στα πρωτόκολλα ιδιωτικού κλειδιού τα δύο αυτά κλειδιά ταυτίζονται και γι' αυτό πρέπει να παραμείνουν μυστικά.

Μία πρώτη συνέπεια είναι ότι ένα πρωτόκολλο δημοσίου κλειδιού στο οποίο συμμετέχουν  $N$  χρήστες απαιτεί  $N$  κλειδιά (στην πραγματικότητα απαιτεί  $N$  ζεύγη της μορφής δημόσιο κλειδί - μυστικό κλειδί), ενώ ένα αντίστοιχο πρωτόκολλο ιδιωτικού κλειδιού απαιτεί  $\binom{n}{2} = \frac{n(n-1)}{2}$  κλειδιά, καθώς πρέπει να δημιουργηθεί ένα κλειδί για κάθε ζεύγος χρηστών. Από την άλλη πλευρά, τα πρωτόκολλα ιδιωτικού κλειδιού είναι αρκετά ταχύτερα από τα αντίστοιχα δημοσίου κλειδιού.

## 2.1 Δημιουργία και ανταλλαγή κλειδιών

Ενώ στα πρωτόκολλα δημοσίου κλειδιού είναι εύκολο να βρει κανείς το κλειδί με το οποίο πρέπει να κρυπτογραφήσει το μήνυμα προς κάποιον συγκεκριμένο αποστολέα (εφόσον αυτός το δημοσιοποιεί), στα πρωτόκολλα ιδιωτικού κλειδιού γεννάται το ερώτημα του πώς δύο χρήστες θα συμφωνήσουν σε ένα συγκεκριμένο κλειδί. Η πηγή του προβλήματος είναι ότι μέχρι να οριστικοποιηθεί κάποιο κλειδί το κανάλι επικοινωνίας είναι ανασφαλές, επομένως οποιοδήποτε μήνυμα μεταξύ αυτών των δύο χρηστών μπορεί να αναγνωσθεί από όλους όσους έχουν πρόσβαση στο κανάλι. Με άλλα λόγια, αντιμετωπίζουμε το πρόβλημα της δημιουργίας ενός ασφαλούς κλειδιού με χρήση ενός ανασφαλούς καναλιού επικοινωνίας.

Στην συνέχεια, παρουσιάζουμε με συντομία την λύση που προτάθηκε το 1976 από τους Whitfield Diffie και Martin Hellman για το συγκεκριμένο πρόβλημα. Υποθέτουμε ότι έχουμε ένα σύνολο  $U$  από  $N$  χρήστες κι έστω  $u_i$  ο  $i$ -οστός χρήστης. Αρχικά, θα πρέπει όλοι αυτοί οι χρήστες να συμφωνήσουν σε έναν μεγάλο πρώτο αριθμό  $p$  (θα πρέπει να είναι πολύ μεγαλύτερος από το πλήθος των χρηστών) καθώς και ένα δημιουργό-στοιχείο  $g \in Z_p^*$ . Επιπλέον, κάθε χρήστης  $u_i$  πρέπει να δημιουργήσει τυχαία ένα στοιχείο  $a_i \in Z_p^*$  και να υπολογίσει το  $A_i = g^{a_i} \bmod p$ . Αν τώρα δύο χρήστες  $u_i$  και  $u_j$  θέλουν να δημιουργήσουν ένα ιδιωτικό κλειδί ώστε να μπορούν στην συνέχεια να επικοινωνούν, τότε αρκεί ο  $u_i$  να στείλει το  $A_i$  στον  $u_j$  και ο  $u_j$  το  $A_j$  στον  $u_i$ . Στην συνέχεια, ο  $u_i$  υπολογίζει το  $A_j^{a_i} \bmod p = (g^{a_j} \bmod p)^{a_i} \bmod p = g^{a_i a_j} \bmod p$  και αντίστοιχα ο  $u_j$  να υπολογίσει το  $A_i^{a_j} \bmod p = (g^{a_i})^{a_j} \bmod p = g^{a_i a_j} \bmod p$ . Παρατηρούμε ότι τελικά οι δύο χρήστες  $u_i$  και  $u_j$  έχουν υπολογίσει την ίδια ποσότητα, η οποία αποτελεί και το ιδιωτικό κλειδί για το συγκεκριμένο ζεύγος χρηστών.

Το πρωτόκολλο των Diffie και Hellman βασίζεται στο πρόβλημα του διακριτού λογαρίθμου, με άλλα λόγια στο ότι ενώ είναι εύκολο δοθέντων των  $p, g$  και  $a_i$  να υπολογιστεί το  $A_i = g^{a_i} \bmod p$ , είναι υπολογιστικά δύσκολο να αντιστραφεί αυτή η πράξη και δοθέντων των  $p, g$  και  $A_i$  να βρεθεί το συγκεκριμένο  $a_i$ .

Ολοκληρώνουμε αυτή την παράγραφο με ένα παράδειγμα κι έστω ότι οι χρήστες έχουν συμφωνήσει στον πρώτο αριθμό  $p = 71$  και στο δημιουργό στοιχείο  $g = 7$ . Δύο χρήστες  $u_1$  και  $u_2$  διαλέγουν τυχαία από έναν αριθμό από το  $Z_{71}^*$  κι έστω  $a_1 = 5$  και  $a_2 = 12$ . Τότε ισχύει ότι  $A_1 = g^{a_1} \bmod p = 7^5 \bmod 71 = 51$  και  $A_2 = g^{a_2} \bmod p = 7^{12} \bmod 71 = 4$ . Επομένως, αφού οι συγκεκριμένοι χρήστες ανταλλάξουν τα παραπάνω μηνύματα, υπολογίζει ο  $u_1$  το  $4^5$



$\text{mod } 71 = 30$  και ο  $u_2$  το  $51^{12} \text{ mod } 71 = 30$ . Συνεπώς, το ιδιωτικό κλειδί που θα πρέπει να χρησιμοποιούν οι  $u_1$  και  $u_2$  για την μεταξύ τους επικοινωνία είναι ο αριθμός 30. Σημειώνουμε ότι για τον υπολογισμό της ύψωσης σε δύναμη οι χρήστες πρέπει να χρησιμοποιήσουν τον αλγόριθμο MODULAR-EXPONENTIATION που παρουσιάσαμε στην Ενότητα 1.2.

## 2.2 Το πρωτόκολλο δημοσίου κλειδιού RSA

Το πρωτόκολλο δημοσίου κλειδιού RSA βασίζεται στην μεγάλη διαφορά ανάμεσα στην ευκολία εύρεσης μεγάλων πρώτων αριθμών και την δυσκολία παραγοντοποίησης του γινομένου δύο μεγάλων πρώτων αριθμών. Στην ενότητα 3 περιγράφεται μια αποδοτική διαδικασία για την εύρεση μεγάλων πρώτων αριθμών.

Κάθε χρήστης δημιουργεί το δημόσιο και το μυστικό κλειδί με την ακόλουθη διαδικασία.

1. Επιλέγει τυχαία δύο μεγάλους πρώτους αριθμούς  $p$  και  $q$  έτσι ώστε  $p \neq q$ . Οι πρώτοι αριθμοί υποθέτουμε ότι είναι 512 bits ο καθένας.
2. Υπολογίζει το  $n = pq$ .
3. Επιλέγει έναν μικρό περιττό ακέραιο  $e$  ο οποίος είναι σχετικά πρώτος με το  $\phi(n)$ , το οποίο ισούται με  $(p-1)(q-1)$ .
4. Υπολογίζει το  $d$ , το οποίο είναι το πολλαπλασιαστικό αντίστροφο του  $e$  modulo  $\phi(n)$ . Το Πρόγραμμα 26 εγγυάται ότι το  $d$  υπάρχει και είναι μοναδικό. Για να υπολογίσει το  $d$  από τα  $e$  και  $\phi(n)$  μπορεί να ακολουθήσει την μέθοδο της ενότητας 1.2.
5. Δημοσιοποιεί το ζεύγος  $P = (e, n)$ , το οποίο είναι το δημόσιο RSA κλειδί του.
6. Κρατά μυστικό το ζεύγος  $S = (d, n)$ , το οποίο είναι το μυστικό RSA κλειδί του.

Σε αυτή την μέθοδο, το πεδίο  $\mathcal{D}$  είναι το σύνολο  $Z_n$ . Ο μετασχηματισμός ενός μηνύματος  $M$  που σχετίζεται με το δημόσιο κλειδί  $P = (e, n)$  είναι ο

$$P(M) = M^e \pmod{n}. \quad (15)$$

Ο μετασχηματισμός του κρυπτογραφημένου μηνύματος  $C$  που σχετίζεται με το μυστικό κλειδί  $S = (d, n)$  είναι ο

$$S(C) = C^d \pmod{n}. \quad (16)$$

Αυτές οι δύο εξισώσεις εφαρμόζονται και για την κρυπτογράφηση και για την υπογραφή. Για να υπογράψει το μήνυμα, ο χρήστης εφαρμόζει το μυστικό του κλειδί στο 'καθαρό' μήνυμα, αντί για το κρυπτογραφημένο. Για να επαληθεύσει μια υπογραφή, ο παραλήπτης εφαρμόζει το δημόσιο κλειδί του αποστολέα στην υπογραφή, αντί για το μήνυμα.

Οι πράξεις για την δημιουργία του δημόσιου και του μυστικού κλειδιού μπορούν να γίνουν χρησιμοποιώντας την διαδικασία MODULAR-EXPONENTIATION όπως αυτή παρουσιάστηκε στην ενότητα 1.2. Για την ανάλυση του χρόνου εκτέλεσης των πράξεων αυτών, υποθέτουμε ότι το δημόσιο κλειδί  $(e, n)$  και το μυστικό κλειδί  $(d, n)$  ικανοποιούν τις σχέσεις  $\log e = O(1)$ ,  $\log d \leq \beta$  και  $\log n \leq \beta$ . Τότε, η χρήση ενός δημόσιου κλειδιού απαιτεί  $O(1)$  modular πολλαπλασιασμούς και  $O(\beta^2)$  πράξεις σε bits. Η χρήση ενός μυστικού κλειδιού απαιτεί  $O(\beta)$  modular πολλαπλασιασμούς και  $O(\beta^3)$  πράξεις σε bits.

**Θεώρημα 37.** Οι εξισώσεις 15 και 16 ορίζουν αντίστροφους μετασχηματισμούς στο  $Z_n$  που ικανοποιούν τις σχέσεις 13 και 14.

Απόδειξη. Από τις εξισώσεις 15 και 16, έχουμε ότι για κάθε  $M \in Z_n$

$$P(S(M)) = S(P(M)) = M^{ed} \pmod{n}.$$

Επειδή τα  $e$  και  $d$  είναι πολλαπλασιαστικοί αντίστροφοι modulo  $\phi(n) = (p-1)(q-1)$ ,

$$ed = 1 + k(p-1)(q-1)$$

για κάποιον ακέραιο  $k$ . Τότε όμως, αν  $M \not\equiv 0 \pmod{p}$ , τότε έχουμε

$$\begin{aligned} M^{ed} &\equiv M(M^{p-1})^{k(q-1)} \pmod{p} \\ &\equiv M(1)^{k(q-1)} \pmod{p} \\ &\equiv M \pmod{p}. \end{aligned}$$

Επίσης,  $M^{ed} \equiv M \pmod{p}$  αν  $M \equiv 0 \pmod{p}$ . Συνεπώς,

$$M^{ed} \equiv M \pmod{p}$$

για κάθε  $M$ . Παρομοίως,

$$M^{ed} \equiv M \pmod{q}$$

για κάθε  $M$ . Οπότε, από το Πρόγραμμα 29 για το Κινέζικο θεώρημα των υπολοίπων, έχουμε

$$M^{ed} \equiv M \pmod{n}$$

για κάθε  $M$ . □

Η ασφάλεια του πρωτοκόλλου RSA βασίζεται σε μεγάλο βαθμό στο ότι είναι υπολογιστικά δύσκολη η παραγοντοποίηση μεγάλων ακεραίων. Αν ένας 'αντίπαλος' μπορεί να παραγοντοποιήσει το  $n$  σε ένα δημόσιο κλειδί, τότε μπορεί να αποκτήσει το μυστικό κλειδί από το δημόσιο κλειδί, χρησιμοποιώντας την γνώση των παραγόντων  $p$  και  $q$ , με τον ίδιο τρόπο που ο δημιουργός του δημοσίου κλειδιού τους χρησιμοποίησε. Επομένως, αν είναι υπολογιστικά εύκολη η παραγοντοποίηση μεγάλων ακεραίων, τότε είναι υπολογιστικά εύκολο να παραβιαστεί το πρωτόκολλο RSA. Η αντίθετη πρόταση δεν έχει αποδειχθεί, συνεπώς μια απόδειξη ότι η παραγοντοποίηση είναι υπολογιστικά δύσκολη δεν θα αποδείκνυε ότι το RSA είναι ασφαλές. Μπορούμε όμως, μετά από σχεδόν 30 χρόνια ερευνητικών προσπαθειών, να πούμε ότι ο ευκολότερος τρόπος να παραβιαστεί η ασφάλεια του RSA είναι μέσω της παραγοντοποίησης μεγάλων ακεραίων. Επιλέγοντας τυχαία δύο αριθμούς των 512 bits και πολλαπλασιάζοντάς τους, μπορεί κανείς να δημιουργήσει ένα δημόσιο κλειδί που δεν μπορεί να 'σπάσει' σε λογικό χρόνο με βάση την παρούσα τεχνολογική κατάσταση. Καταλήγοντας, αν δεν επέλθει κάποια δραστηρή αλλαγή και πρόοδος στην θεωρία αριθμών, το πρωτόκολλο RSA είναι ασφαλές, όταν υλοποιείται προσεχτικά.

Επιγραμματικά, πιθανοί τρόποι ώστε να παραβιαστεί η ασφάλεια του πρωτοκόλλου RSA είναι οι ακόλουθοι:

- Μέσω παραγοντοποίησης του  $n$ : Προφανώς, αν ο αντίπαλος βρει τα  $p$  και  $q$  για τα οποία  $n = pq$ , τότε μπορεί να βρει το  $\phi(n) = (p - 1)(q - 1)$  και το μυστικό κλειδί  $d$ .
- Μέσω υπολογισμού του  $\phi(n)$ : Αν το  $\phi(n)$  είναι γνωστό, τότε μπορεί να υπολογιστεί το  $d$ . Είναι εύκολο όμως να δούμε πως η γνώση του  $\phi(n)$  οδηγεί στην παραγοντοποίηση του  $n$ . Αυτό συμβαίνει λόγω των σχέσεων  $p + q = n - \phi(n) + 1$ ,  $(p - 1)^2 = (p + q)^2 - 4n$  και  $q = \frac{1}{2}[(p + q) - (p - q)]$ .

Για λόγους ευκολίας και ταχύτητας, αρκετά συχνά χρησιμοποιείται στην πράξη ένα υβριδικό σχήμα που περιέχει και γρήγορα πρωτόκολλα που δεν βασίζονται σε δημόσια κλειδιά. Σε ένα τέτοιο υβριδικό σύστημα, τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση είναι ίδια. Αν η Alice θέλει να στείλει ένα μήνυμα  $M$  στον Bob, επιλέγει τυχαία ένα

κλειδί  $K$  και κρυπτογραφεί με γρήγορο τρόπο το  $M$  χρησιμοποιώντας το  $K$ , οπότε έχει υπολογίσει το κρυπτογραφημένο μήνυμα  $C$ . Το  $C$  είναι ίδιου μεγέθους με το  $M$ , αλλά το  $K$  είναι αρκετά μικρό σε μέγεθος. Στην συνέχεια, κρυπτογραφεί το  $K$  με βάση το δημόσιο κλειδί του Bob. Επειδή, το  $K$  είναι μικρό σε μέγεθος, ο υπολογισμός του  $P_B(K)$  γίνεται γρήγορα (πολύ γρηγορότερα από ότι θα χρειαζόταν για να υπολογιστεί το  $P_B(M)$ ). Ακολούθως, μεταδίδει το  $(C, P_B(K))$  στον Bob, ο οποίος αποκρυπτογραφεί το  $P_B(K)$  για να πάρει το  $K$ , το οποίο το χρησιμοποιεί για να αποκρυπτογραφήσει το μήνυμα  $C$  για να πάρει το αρχικό μήνυμα  $M$ .

Μια παρόμοια υβριδική προσέγγιση χρησιμοποιείται για την γρήγορη δημιουργία ψηφιακών υπογραφών. Το RSA συνδυάζεται με μια δημόσια *one-way hash function*  $h$ : μια συνάρτηση που μπορεί να υπολογιστεί εύκολα αλλά για την οποία είναι υπολογιστικά αδύνατο να βρεθούν δύο μηνύματα  $M$  και  $M'$  τέτοια ώστε  $h(M) = h(M')$ . Η τιμή  $h(M)$  είναι ένα μικρό (ας πούμε 160 bits) 'αποτύπωμα' του μηνύματος  $M$ . Αν η Alice θέλει να υπογράψει το μήνυμα  $M$ , εφαρμόζει πρώτα την  $h$  στο  $M$  για να πάρει το  $h(M)$ , το οποίο υπογράφει με το μυστικό της κλειδί. Ακολούθως, στέλνει στον Bob το  $(M, S_A(h(M)))$ . Ο Bob μπορεί να επαληθεύσει την υπογραφή υπολογίζοντας το  $h(M)$  και επαληθεύοντας ότι αν εφαρμόσει το  $P_A$  στο  $S_A(h(M))$  που έλαβε θα πάρει το  $h(M)$ . Επειδή είναι υπολογιστικά αδύνατο να δημιουργηθούν δύο μηνύματα με το ίδιο αποτύπωμα, είναι υπολογιστικά αδύνατο να αλλοιωθεί ένα υπογεγραμμένο μήνυμα και να παραμείνει αναλλοίωτη η ψηφιακή υπογραφή.

Τέλος, αναφέρουμε ότι η χρήση πιστοποιητικών (certificates) κάνει ευκολότερη την διανομή των δημοσίων κλειδιών. Για παράδειγμα, υποθέτουμε ότι υπάρχει μια έμπιστη αρχή  $T$ , της οποίας το δημόσιο κλειδί είναι γνωστό σε όλους. Η Alice μπορεί να τότε να πάρει ένα υπογεγραμμένο μήνυμα (πιστοποιητικό) από την  $T$ , το οποίο θα λέει ότι 'το δημόσιο κλειδί της Alice είναι το  $P_A$ '. Αυτό το πιστοποιητικό πιστοποιεί κατά κάποιον τρόπο τον εαυτό του, καθώς όλοι ξέρουν το  $P_T$ . Η Alice μπορεί να επισυνάψει το πιστοποιητικό σε κάθε υπογεγραμμένο μήνυμά της, οπότε ο παραλήπτης έχει στην διάθεσή του αμέσως το δημόσιο κλειδί με το οποίο θα επαληθεύσει την υπογραφή. Επειδή το κλειδί της είναι πιστοποιημένο από την  $T$ , ο παραλήπτης μπορεί να είναι σίγουρος ότι έχει στην διάθεσή του το πραγματικό δημόσιο κλειδί της Alice.

### 2.3 Το πρωτόκολλο δημοσίου κλειδιού του Rabin

Όπως προαναφέραμε στην συζήτηση για το πρωτόκολλο RSA, γνωρίζουμε ότι μπορεί να παραβιαστεί αν υπάρχει κάποιος αποδοτικός αλγόριθμος για το πρόβλημα της παραγοντοποίησης. Χρησι-

μοποιώντας όρους υπολογιστικής πολυπλοκότητας, αυτό μπορεί να αναπαρασταθεί ως

Παραβίαση  $RSA \propto$  Παραγοντοποίηση.

Δεν έχει αποδειχθεί όμως ότι το πρόβλημα RSA είναι υπολογιστικά τόσο δύσκολο όσο το πρόβλημα της παραγοντοποίησης.

Μια διαφορετική ιδέα, που επίσης βασίζεται στην θεωρία αριθμών, προτάθηκε από τον M. Rabin το 1979. Ο Rabin πρότεινε ένα πρωτόκολλο δημοσίου κλειδιού το οποίο είναι αποδεδειγμένα τόσο δύσκολο όσο το πρόβλημα της παραγοντοποίησης. Κάθε χρήστης επιλέγει ένα ζευγάρι  $(p, q)$  από διαφορετικούς πρώτους ακεραίους, το οποίο κρατάει μυστικό. Διαλέγει επίσης έναν ακέραιο  $B < N = pq$ .

Το δημόσιο κλειδί είναι το ζεύγος  $(B, N)$ .

Το μυστικό κλειδί είναι η παραγοντοποίηση  $(p, q)$  του  $N$ .

Η συνάρτηση κρυπτογράφησης  $e$  ενός μηνύματος  $M$ , όπου το  $M$  (αν είναι μεγάλο, μπορούμε να το χωρίσουμε σε τμήματα) αναπαρίσταται ως ένας ακέραιος στο διάστημα  $\{1, \dots, N - 1\}$ , είναι

$$e(M) = M(M + B) \pmod{N}.$$

Αν συμβολίσουμε το κρυπτογραφημένο μήνυμα με  $C$ , τότε το πρόβλημα της αποκρυπτογράφησης είναι να βρεθεί ένα  $M$  τέτοιο ώστε

$$M^2 + MB = C \pmod{N}. \quad (17)$$

Η κεντρική ιδέα του πρωτοκόλλου είναι η ακόλουθη.

**Λήμμα 38.** *Μια λύση για την ισοδυναμία*

$$x^2 + Bx = C \pmod{pq} \quad (18)$$

μπορεί να βρεθεί αν βρούμε τις λύσεις  $u$  και  $v$  για τις ισοδυναμίες

$$u^2 + Bu = C \pmod{p},$$

$$v^2 + Bv = C \pmod{q},$$

και ακεραίους  $a$  και  $b$  τέτοιους ώστε

$$a = 1 \pmod{p}, \quad a = 0 \pmod{q}, \quad b = 0 \pmod{p}, \quad b = 1 \pmod{q}. \quad (19)$$

Τότε έχουμε πως η σχέση  $x = au + bv$  ικανοποιεί την ισοδυναμία 18.

Απόδειξη. Κάνοντας αριθμητικές πράξεις και αντικαθιστώντας  $a = 1 + kp$  ή  $a = lq$  όπου χρειάζεται.

□

Συνεχίζουμε την παρουσίαση του πρωτοκόλλου με το ακόλουθο αποτέλεσμα.

**Λήμμα 39.** Αφού οι  $p$  και  $q$  είναι πρώτοι αριθμοί, οι ακέραιοι  $a$  και  $b$  που ικανοποιούν την σχέση 19 μπορούν να βρεθούν χρησιμοποιώντας τον EXTENDED-EUCLID σε χρόνο πολυωνυμικό ως προς το  $\log pq$ .

Απόδειξη. Εκτελούμε τον αλγόριθμο EXTENDED-EUCLID και βρίσκουμε τον μέγιστο κοινό διαιρέτη των  $p$  και  $q$ . Αφού είναι πρώτοι μεταξύ τους, καταλήγουμε σε μια σχέση σαν την  $1 = ep + fq$ . Η απόδειξη ολοκληρώνεται αν θέσουμε  $a = fq$  και  $b = ep$ .

□

Συνεπώς, η αποκρυπτογράφηση μπορεί να γίνει εύκολα αν μπορούμε να λύσουμε την ισοδυναμία modulo έναν πρώτο αριθμό. Το παραπάνω όμως μπορεί να γίνει ως εξής.

**Λήμμα 40.** Η επίλυση της

$$u^2 + Bu = C \pmod{p}$$

είναι ισοδύναμη με την επίλυση της

$$y^2 = C + (4^{-1})_p B^2 \pmod{p}, \quad (20)$$

όπου το  $(4^{-1})_p$  δηλώνει τον πολλαπλασιαστικό αντίστροφο του 4 modulo  $p$ .

Απόδειξη. Το  $(4^{-1})_p$  υπάρχει εφόσον ο  $p$  είναι πρώτος αριθμός και η σχέση 20 προκύπτει αν συμπληρώσουμε το ανάπτυγμα του τετραγώνου.

□

Εφόσον ο  $q$  είναι επίσης πρώτος, το Λήμμα 40 ισχύει και αν όπου  $p$  έχουμε το  $q$ , και συνεπώς έχουμε ανάγει το πρόβλημα της αποκρυπτογράφησης στο πρόβλημα της εύρεσης τετραγωνικών ριζών modulo κάποιον πρώτο αριθμό.

Συνδυάζοντας τα παραπάνω αποτελέσματα, αποδεικνύουμε την ακόλουθη πρόταση.

**Πόρισμα 41.** Αν οι πρώτοι αριθμοί  $p$  και  $q$  αφήνουν και οι δύο υπόλοιπο 3 modulo 4, τότε η διαδικασία της αποκρυπτογράφησης μπορεί να γίνει σε πολυωνυμικό χρόνο.

Απόδειξη. Ο παραλήπτης, ο οποίος γνωρίζει τους πρώτους παράγοντες  $p$  και  $q$  του  $n$ , γνωρίζει επίσης πως το κρυπτογραφημένο μήνυμα πρέπει να είναι τετραγωνικό υπόλοιπο και μπορεί να λύσει τις εξισώσεις modulo  $p$  και modulo  $q$  και να χρησιμοποιήσει τα Λήμματα 38 και 40 για να βρεί την λύση  $M$  της εξίσωσης 17.  $\square$

Στην πραγματικότητα, ο Rabin απέδειξε κάτι πιο ισχυρό από το πόρισμα 41. Αυτό που έδειξε είναι πως ακόμα κι αν οι αριθμοί  $p, q$  δεν ανήκουν σε αυτή την κατηγορία (δηλαδή δεν αφήνουν και οι δύο υπόλοιπο 3 modulo 4), τότε και πάλι οι εξισώσεις modulo  $p$  και modulo  $q$  μπορούν να λυθούν σε πολυωνυμικό χρόνο, χρησιμοποιώντας έναν πιθανοτικό αλγόριθμο. τον οποίον δεν θα παρουσιάσουμε εδώ.

Ανακεφαλαιώνοντας, για οποιουδήποτε πρώτους αριθμούς  $p$  και  $q$ , η διαδικασία της αποκρυπτογράφησης μπορεί να γίνει (είτε μέσω ντετερμινιστικού είτε μέσω πιθανοτικού αλγορίθμου) σε πολυωνυμικό χρόνο.

Για παράδειγμα, υποθέτουμε ότι η Alice έχει ως δημόσιο κλειδί το ζεύγος  $(B, N) = (2, 77)$ , ενώ το μυστικό της κλειδί είναι η παραγοντοποίηση  $(p, q) = (7, 11)$  του  $N$ . Αν το μήνυμα είναι το  $M = 3$ , τότε

$$C = M^2 + 2M = 15 \pmod{77}.$$

Για να αποκρυπτογραφήσει, η Alice θα πρέπει να λύσει τις

$$u^2 + 2u = 15 = 1 \pmod{7}$$

και

$$v^2 + 2v = 15 = 4 \pmod{11}.$$

Αυτές λύνονται, αν λύσει τις  $(u + 1)^2 = 2 \pmod{7}$  και  $(v + 1)^2 = 5 \pmod{11}$  για να πάρει τις τιμές  $u + 1 = \pm 2^2 = \pm 4 \pmod{7}$  και  $v + 1 = \pm 5^3 = \pm 4 \pmod{11}$ . Συνεπώς,

$$u = 3 \quad \text{ή} \quad 2, \quad v = 3 \quad \text{ή} \quad 6.$$

Ακολουθώντας, χρησιμοποιώντας τον αλγόριθμο EXTENDED-EUCLID παίρνει τις τιμές  $a = 22$  και  $b = -21$ , και η λύση στο

$$x^2 + 2x = 15 \pmod{77}$$

είναι η

$$x = \begin{pmatrix} 2 \cdot 22 - 3 \cdot 21 \\ 2 \cdot 22 - 6 \cdot 21 \\ 3 \cdot 22 - 3 \cdot 21 \\ 3 \cdot 22 - 6 \cdot 21 \end{pmatrix} \pmod{77}.$$

Αυτό σημαίνει πως η Alice έχει να διαλέξει ανάμεσα σε 4 πιθανά μηνύματα του αποστολέα, δηλαδή  $M_1 = 3, M_2 = 17, M_3 = 58, M_4 = 72$ .

Το παραπάνω παράδειγμα παρουσιάζει ένα από τα μειονεκτήματα του πρωτοκόλλου δημοσίου κλειδιού του Rabin, δηλαδή το ότι ο παραλήπτης πρέπει να διαλέξει ανάμεσα σε περισσότερα πιθανά αρχικά μηνύματα. Συνήθως, το πρόβλημα αυτό λύνεται από την ίδια την φύση του μηνύματος (αν δηλαδή γνωρίζουμε ότι το αρχικό μήνυμα ήταν μια πρόταση στα ελληνικά, τότε είναι απίθανο να υπάρχουν πάνω από ένα πιθανά μηνύματα που να έχουν νόημα στα ελληνικά). Ως ένα επιπλέον μέτρο ασφαλείας, μπορούμε να επιβάλουμε σε όλους τους χρήστες του πρωτοκόλλου να επαναλαμβάνουν π.χ. τα πρώτα 64 bits στο τέλος του μηνύματος. Τότε, ο παραλήπτης θα ελέγχει κάθε πιθανό μήνυμα για το αν έχει αυτή την ειδική μορφή.

Τέλος, θα κάνουμε μια σύντομη αναφορά σε ένα σύστημα ψηφιακών υπογραφών που χρησιμοποιεί το πρωτόκολλο του Rabin, για το οποίο θα υποθέσουμε ότι για όλους τους χρήστες ισχύει πως  $B = 0$ . Αν ο αποστολέας θέλει να αποστείλει ένα μήνυμα  $m$ , τότε υπολογίζει την τετραγωνική ρίζα  $s$  έτσι ώστε  $s^2 = m \pmod{n}$  και στέλνει στον παραλήπτη το μήνυμα  $(m, s)$ .

Ο παραλήπτης με την σειρά του, κοιτάζει το δημόσιο κλειδί  $n$  του αποστολέα και υπολογίζει το  $m' = s^2 \pmod{n}$ . Αν  $m' = m$  τότε αποδέχεται ότι το συγκεκριμένο μήνυμα όντως το έστειλε ο 'υποτιθέμενος' αποστολέας.

Ένα πιθανό πρόβλημα με το παραπάνω σύστημα ψηφιακών υπογραφών, είναι πως ένας κακόβουλος χρήστης μπορεί να επιλέξει ένα  $s \in Z_n^*$ , να υπολογίζει το  $m = s^2 \pmod{n}$  και ακολούθως να στείλει το  $(s, m)$ , το οποίο φυσικά ο παραλήπτης θα νομίζει ότι προέρχεται από τον αποστολέα με δημόσιο κλειδί  $n$ . Ευτυχώς, για την ασφάλεια του πρωτοκόλλου, η πιθανότητα το (τυχαίο)  $s$  να έχει κάποιο νόημα είναι πολύ μικρή.

## 2.4 Το πρωτόκολλο δημοσίου κλειδιού του El Gamal

Το πρωτόκολλο δημοσίου κλειδιού El Gamal προτάθηκε από τον Taher El Gamal το 1984 και βασίζεται στο πρωτόκολλο των Diffie και Hellman που περιγράψαμε νωρίτερα.

Οι χρήστες που πρόκειται να συμμετάσχουν στο πρωτόκολλο χρειάζεται να ακολουθήσουν τα



ακόλουθα βήματα για κάθε φάση του πρωτοκόλλου.

**Δημιουργία κλειδιού** Κάθε χρήστης επιλέγει έναν μεγάλο πρώτο αριθμό  $p$ , ένα δημιουργό στοιχείο  $g \in Z_p^*$  καθώς και ένα τυχαίο ακέραιο  $a$  τέτοιον ώστε  $2 \leq a \leq p-2$  και κατόπιν υπολογίζει το  $g^a \pmod p$ . Το δημόσιο κλειδί του χρήστη είναι η τριάδα  $(p, g, g^a \pmod p)$ , ενώ το μυστικό κλειδί είναι ο ακέραιος  $a$ .

**Κρυπτογράφηση** Αν ο χρήστης  $B$  θέλει να επικοινωνήσει με τον χρήστη  $A$  τότε πριν από όλα πρέπει να βρει το δημόσιο κλειδί  $P_A$  του  $A$  κι έστω  $P_A = (p, g, g^a \pmod p)$ . Ακολούθως, ο χρήστης  $B$  μετατρέπει το μήνυμα που θέλει να στείλει σε έναν αριθμό  $m$  στο διάστημα  $\{0, \dots, p-1\}$  και επιλέγει έναν τυχαίο ακέραιο  $k$  τέτοιον ώστε  $2 \leq k \leq p-2$ . Για να κρυπτογραφήσει το μήνυμα  $m$  χρειάζεται να υπολογίσει τις ποσότητες  $\gamma = g^k \pmod p$  και  $\delta = m(g^a)^k \pmod p$ , και τέλος στέλνει στον χρήστη  $A$  το μήνυμα  $c = (\gamma, \delta)$ .

**Αποκρυπτογράφηση** Ο  $A$ , αφού έχει λάβει το  $c$ , χρησιμοποιεί το μυστικό κλειδί  $a$  και υπολογίζει το  $\gamma^{p-1-a} \pmod p$ , για το οποίο ισχύει ότι  $\gamma^{p-1-a} = \gamma^{-a} = g^{-ak}$ . Τέλος, ανακτά το μήνυμα  $m$  υπολογίζοντας το  $(\gamma^{-a})\delta \pmod p$ , καθώς ισχύει ότι  $\gamma^{-a}\delta \equiv g^{-ak}mg^{ak} \equiv m \pmod p$ .

**Παράδειγμα** Υποθέτουμε ότι ο χρήστης  $A$  έχει διαλέξει τον πρώτο αριθμό  $p = 2357$ , το δημιουργό στοιχείο  $g = 2 \in Z_{2357}^*$  και τον ακέραιο  $a = 1751$ . Μπορεί συνεπώς να υπολογίσει το  $g^a \pmod p = 2^{1751} \pmod 2357 = 1185$  και το δημόσιο κλειδί του είναι  $P_A = (p = 2357, g = 2, g^a \pmod p = 1185)$ .

Αν ο χρήστης  $B$  θέλει να στείλει το μήνυμα  $m = 2035$ , επιλέγει ένα  $k = 1520$  και στην συνέχεια υπολογίζει τα  $\gamma = g^k = 2^{1520} \pmod 2357 = 1430$  και  $\delta = 2035 \cdot 1185^{1520} \pmod 2357 = 697$ . Επομένως, ο  $B$  στέλνει το μήνυμα  $c = (1430, 697)$  στον  $A$ .

Ο τελευταίος υπολογίζει τα  $\gamma^{p-1-a} = 1430^{605} \pmod 2357 = 872$  και  $m = 872 \cdot 697 \pmod 2357 = 2035$ , επομένως έχει καταφέρει να ανακτήσει το μήνυμα  $m$ .

**Υπογραφές El Gamal** Κατ' αρχάς, το στάδιο της δημιουργίας του δημόσιου κλειδιού  $P_A = (p, g, g^a)$  για τον χρήστη  $A$  είναι ίδιο όπως και στο πρωτόκολλο κρυπτογράφησης. Όταν ο  $A$  θέλει να στείλει ένα μήνυμα  $m$  στον  $B$ , αρχικά διαλέγει έναν τυχαίο ακέραιο  $k$  τέτοιον ώστε  $2 \leq k \leq p-2$

και  $\gcd(k, p-1) = 1$  και υπολογίζει τα  $r = g^k \pmod{p}$ ,  $k^{-1} \pmod{p-1}$  και  $s = k^{-1}\{h(m) - ar\} \pmod{p-1}$ . Η ψηφιακή υπογραφή του  $A$  για το μήνυμα  $m$  είναι το ζεύγος  $(r, s)$ .

Όταν ο παραλήπτης  $B$  πάρει το μήνυμα και την υπογραφή, αρχικά βρίσκει το δημόσιο κλειδί του αποστολέα και επιβεβαιώνει ότι  $1 \leq r \leq p-1$  αλλιώς απορρίπτει το μήνυμα. Στην συνέχεια, υπολογίζει τα  $v_1 = g^{ar} r^s \pmod{p}$ ,  $h(m)$  και  $v_2 = g^{h(m)} \pmod{p}$ . Αν ισχύει ότι  $v_1 = v_2$  τότε δέχεται το μήνυμα και την υπογραφή, αλλιώς τα απορρίπτει.

Για να αποδείξουμε ότι το συγκεκριμένο πρωτόκολλο ψηφιακής υπογραφής είναι σωστό, αρκεί να θεωρήσουμε την σχέση  $s = k^{-1}\{h(m) - ar\} \pmod{p-1}$ . Αν πολλαπλασιάσουμε και τα 2 μέλη με  $k$  τότε προκύπτει  $ks = \{h(m) - ar\} \pmod{p-1}$  και  $h(m) = ar + ks \pmod{p-1}$ . Αν υψώσουμε το δημιουργό στοιχείο  $g$  στα δύο μέλη, προκύπτει ότι  $g^{h(m)} = g^{ar+ks} \pmod{p}$  (από το Θεώρημα 33) και συνεπώς  $g^{h(m)} = (g^a)^r \cdot (g^k)^s = (g^a)^r \cdot (r)^s \pmod{p}$  και συνεπώς ισχύει ότι  $v_1 = v_2$ .

### 3 Ελεγχος πρώτων αριθμών

Σε αυτή την ενότητα, θα ασχοληθούμε με το πρόβλημα της εύρεσης μεγάλων πρώτων αριθμών. Αρχικά θα εξετάσουμε το ζήτημα της ‘πυκνότητας’ των πρώτων αριθμών, ακολούθως θα εξετάσουμε μια εύλογη προσέγγιση στο πρόβλημα του ελέγχου για το αν ένας μεγάλος αριθμός είναι πρώτος και θα παρουσιάσουμε έναν αποδοτικό πιθανοτικό αλγόριθμο ελέγχου που ανέπτυξαν ο Miller και ο Rabin. Τέλος, θα παρουσιάσουμε τον αλγόριθμο των Agrawal, Kayal και Saxena που το 2002 σε μια πολύ σημαντική εργασία για την θεωρία αριθμών παρουσίασαν έναν ντετερμινιστικό αλγόριθμο που επιλύει το πρόβλημα του ελέγχου σε πολυωνυμικό χρόνο. Θα δώσουμε μεγαλύτερη έμφαση στην παρουσίαση πιθανοτικών αλγορίθμων, καθώς είναι γρηγορότεροι και παρουσιάζουν ιδιαίτερο ενδιαφέρον για διδακτικούς λόγους.

**Πυκνότητα των πρώτων αριθμών** Σε πολλές εφαρμογές (όπως η κρυπτογραφία), χρειάζεται να βρούμε μεγάλους ‘τυχαίους’ πρώτους αριθμούς. Ευτυχώς, οι μεγάλοι πρώτοι δεν είναι πολύ σπάνιοι, οπότε σε εύλογο χρονικό διάστημα μπορούμε να ελέγξουμε τυχαίους μεγάλους αριθμούς μέχρι να βρεθεί κάποιος πρώτος. Η συνάρτηση κατανομής  $\pi(n)$  προσδιορίζει τον αριθμό των πρώτων αριθμών που είναι μικρότεροι ή ίσοι με το  $n$ . Για παράδειγμα,  $\pi(12) = 4$  αφού υπάρχουν 5 πρώτοι αριθμοί μικρότεροι ή ίσοι με το 12, οι οποίοι είναι οι 2, 3, 5, 7 και 11. Το θεώρημα των πρώτων αριθμών παρέχει μια χρήσιμη προσέγγιση για το  $\pi(n)$ .

**Θεώρημα 42.** (Θεώρημα πρώτων αριθμών)

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n/\ln n} = 1.$$

Μπορούμε να χρησιμοποιήσουμε το θεώρημα των πρώτων αριθμών για να εκτιμήσουμε την πιθανότητα ότι ένας τυχαία επιλεγμένος ακέραιος  $n$  να είναι πρώτος ως  $1/\ln n$ . Συνεπώς, θα πρέπει να εξετάσουμε περίπου  $\ln n$  τυχαία επιλεγμένους ακεραίους κοντά στο  $n$ , έτσι ώστε να βρούμε έναν πρώτο με ίδιο μέγεθος όπως το  $n$ . Για παράδειγμα, για να βρούμε έναν πρώτο με 512 bits, μπορεί να χρειαστεί να εξετάσουμε περίπου  $\ln 2^{512} \approx 355$  τυχαίους αριθμούς των 512 bits. Στην πραγματικότητα, θα πρέπει να εξετάσουμε τους μισούς, αν περιοριστούμε σε περιττούς ακεραίους.

Στο υπόλοιπο αυτής της ενότητας, θα ασχοληθούμε με το πρόβλημα του ελέγχου αν ένας μεγάλος περιττός ακέραιος είναι πρώτος ή όχι. Θα χρησιμοποιούμε την βολική υπόθεση ότι ο  $n$  παραγοντοποιείται σε πρώτους παράγοντες ως

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

όπου  $r \geq 1$ ,  $p_1, p_2, \dots, p_r$  είναι οι πρώτοι παράγοντες του  $n$  και οι  $e_1, e_2, \dots, e_r$  είναι θετικοί ακέραιοι. Ο  $n$  είναι πρώτος αν και μόνο αν  $r = 1$  και  $e_1 = 1$ .

Μια απλή προσέγγιση στο πρόβλημα του ελέγχου είναι η εξονυχιστική διαίρεση. Δοκιμάζουμε να διαιρέσουμε το  $n$  με κάθε ακέραιο  $2, 3, \dots, \lfloor \sqrt{n} \rfloor$ , εξετάζοντας μόνο το 2 και τους περιττούς ακεραίους. Είναι προφανές ότι ο  $n$  είναι πρώτος αν και μόνο αν κανένας από τους προαναφερόμενους ακεραίους δεν διαιρεί το  $n$ . Υποθέτοντας ότι κάθε διαίρεση απαιτεί σταθερό χρόνο, ο χρόνος εκτέλεσης της χειρότερης περίπτωσης είναι  $\Theta(\sqrt{n})$ , ο οποίος είναι εκθετικός ως προς το μήκος του  $n$ . Υπενθυμίζουμε ότι αν το  $n$  αναπαρίσταται στο δυαδικό αλφάβητο με  $\beta$  bits, τότε  $\beta = \lceil \log(n + 1) \rceil$  και επομένως  $\sqrt{n} = \Theta(2^{\beta/2})$ . Άρα, η δοκιμαστική διαίρεση δουλεύει καλά μόνο αν το  $n$  είναι μικρό ή τυχαίνει να έχει κάποιον μικρό πρώτο παράγοντα. Έχει το πλεονέκτημα πως δεν αποφαινεται μόνο για το αν ο  $n$  είναι πρώτος, αλλά επιστρέφει και έναν πρώτο παράγοντα στην αντίθετη περίπτωση.

Στην ενότητα αυτή ενδιαφερόμαστε μόνο να μάθουμε αν ένας αριθμός  $n$  είναι πρώτος: αν ο  $n$  είναι σύνθετος δεν μας ενδιαφέρει να βρούμε την παραγοντοποίησή του σε πρώτους παράγοντες. Είναι μάλλον ενδιαφέρον το ότι είναι ευκολότερο να απαντηθεί αν ένας αριθμός είναι πρώτος από το να βρεθεί η παραγοντοποίησή του αν είναι σύνθετος.

### 3.1 Πιθανοτικοί αλγόριθμοι

**Έλεγχος ψευδοπρώτων** Θα εξετάσουμε τώρα μια μέθοδο για έλεγχο πρώτων αριθμών που 'σχεδόν δουλεύει' και είναι αρκετά καλή στις περισσότερες περιπτώσεις. Αργότερα, θα εκλεπτύνουμε την μέθοδο ώστε να μην έχει κάποιο μειονέκτημα. Έστω  $Z_n^+$  το σύνολο των μη-μηδενικών στοιχείων του  $Z_n$ :

$$Z_n^+ = \{1, 2, \dots, n - 1\}.$$

Αν ο  $n$  είναι πρώτος, τότε  $Z_n^+ = Z_n^*$ .

Λέμε ότι ο  $n$  είναι ψευδοπρώτος με βάση  $a$  αν ο  $n$  είναι σύνθετος και

$$a^{n-1} \equiv 1 \pmod{n}. \quad (21)$$

Από το θεώρημα του Fermat (Θεώρημα 31) συνεπάγεται ότι αν ο  $n$  είναι πρώτος, τότε το  $n$  ικανοποιεί την εξίσωση (21) για κάθε  $a$ . Συνεπώς, αν μπορέσουμε να βρούμε κάποιο  $a$  για το οποίο το  $n$  δεν ικανοποιεί την εξίσωση, τότε μπορούμε να αποφανθούμε με βεβαιότητα ότι το  $n$  είναι σύνθετος ακέραιος. Το αντίθετο ισχύει σχεδόν πάντα, επομένως έχουμε ένα αρκετά καλό κριτήριο για το αν ένας αριθμός είναι πρώτος ή όχι. Δοκιμάζουμε να δούμε αν το  $n$  ικανοποιεί την εξίσωση (21) για

$a = 2$ . Αν όχι, τότε λέμε ότι το  $n$  είναι σύνθετος. Αλλιώς, υποθέτουμε ότι το  $n$  είναι πρώτος (όταν στην πραγματικότητα το μόνο που ξέρουμε είναι πως το  $n$  είναι είτε πρώτος είτε ψευδοπρώτος με βάση  $a$ ).

Ο ακόλουθος αλγόριθμος γενικεύει την παραπάνω διαδικασία για να ελέγξει το  $n$ . Χρησιμοποιεί τον αλγόριθμο MODULAR-EXPONENTIATION από την ενότητα 1.2. Η είσοδος  $n$  υποθέτουμε ότι είναι κάποιος περιττός ακέραιος μεγαλύτερος του 2.

PSEUDOPRIME( $n$ )

1 αν MODULAR-EXPONENTIATION( $2, n - 1, n$ )  $\neq 1 \pmod n$

2     τότε επίστρεψε ΣΥΝΘΕΤΟΣ \\σίγουρα

3     αλλιώς επίστρεψε ΠΡΩΤΟΣ \\ελπίζουμε

Αυτός ο αλγόριθμος μπορεί να κάνει λάθη, αλλά μόνο ενός είδους. Αν δηλαδή πει πως ο  $n$  είναι σύνθετος, τότε είναι οπωσδήποτε σύνθετος. Αν όμως πει πως ο  $n$  είναι πρώτος, τότε μπορεί να κάνει λάθος αν ο  $n$  είναι ψευδοπρώτος με βάση το  $a$ .

Πόσο συχνά μπορεί να γίνει ένα τέτοιο λάθος; Ευτυχώς, κάτι τέτοιο συμβαίνει σπάνια. Υπάρχουν μόνο 22 τιμές του  $n$  μικρότερες από 10,000 για τις οποίες κάνει λάθος: οι πρώτες 4 είναι οι 341, 561, 645 και 1105. Μπορεί να αποδειχθεί ότι η πιθανότητα ότι ο αλγόριθμος κάνει λάθος για έναν τυχαία επιλεγμένο αριθμό των  $\beta$  bits τείνει στο 0 καθώς  $\beta \rightarrow \infty$ . Χρησιμοποιώντας ακριβέστερους υπολογισμούς, μπορούμε να δείξουμε ότι ένας αριθμός των 512 bits, για τον οποίο ο αλγόριθμος αποφασίζει ότι είναι πρώτος, έχει πιθανότητα μικρότερη από 1 στις  $10^{20}$  να είναι ψευδοπρώτος βάσης 2 και ένας τυχαία επιλεγμένος αριθμός με 1024 bits, για τον οποίο ο αλγόριθμος λέει ότι είναι πρώτος, έχει πιθανότητα μικρότερη από 1 στις  $10^{41}$  να είναι ψευδοπρώτος βάσης 2. Επομένως, αν μια εφαρμογή απλώς χρειάζεται έναν μεγάλο πρώτο αριθμό, είναι προτιμότερο να ακολουθήσουμε τον παραπάνω αλγόριθμο ο οποίος στην πράξη δουλεύει. Αν όμως ο αριθμός που εξετάζουμε δεν είναι τυχαία επιλεγμένος, τότε είναι αναγκαία μια καλύτερη προσέγγιση.

Δυστυχώς, δεν μπορούμε να γλυτώσουμε από τα λάθη, αλλάζοντας απλώς την βάση  $a$  για την εξίσωση 21, για παράδειγμα έστω πως  $a = 3$ , γιατί υπάρχουν σύνθετοι ακέραιοι  $n$  που ικανοποιούν την 21 για όλα τα  $a$ . Αυτοί οι ακέραιοι είναι γνωστοί ως αριθμοί Carmichael. Οι πρώτοι τρεις αριθμοί Carmichael είναι το 561, 1105 και 1729. Είναι αρκετά σπάνιοι: για παράδειγμα υπάρχουν μόνο 255 μικρότεροι του 100,000,000. Ακολούθως, θα δείξουμε πώς μπορούμε να βελτιώσουμε τον αλγόριθμο, έτσι ώστε οι αριθμοί Carmichael να μην αποτελούν πρόβλημα.

**Έλεγχος Miller-Rabin για πρώτους** Ο έλεγχος Miller-Rabin για το αν ένας αριθμός είναι πρώτος ή όχι αποφεύγει τα μειονεκτήματα της προηγούμενης μεθόδους με τις ακόλουθες αλλαγές

- Δοκιμάζει διάφορες τυχαία επιλεγμένες τιμές για την βάση  $a$  αντί για μόνο μία.
- Καθώς υπολογίζει τις υψώσεις σε δύναμη, εξετάζει αν βρεθεί μια μη-τετριμμένη τετραγωνική ρίζα του 1 modulo  $n$ . Αν ναι, τότε σταματάει και αποφαινεται πως ο αριθμός είναι σύνθετος. Το πόρισμα 36 εξηγεί γιατί συμβαίνει αυτό.

Στην συνέχεια, παρουσιάζουμε τον αλγόριθμο που εξετάζει αν μία συγκεκριμένη τιμή του  $a$  είναι 'μάρτυρας' για το ότι ο  $n$  είναι σύνθετος αριθμός, καθώς και κάποια σχόλια για την λειτουργία του.

WITNESS( $a, n$ )

1  $n - 1 = 2^t u$

2  $x_0 \leftarrow \text{MODULAR-EXPONENTIATION}(a, u, n)$

3 για  $i \leftarrow 1$  μέχρι  $t$

4  $x_i \leftarrow x_{i-1}^2 \pmod n$

5 αν  $x_i = 1$  και  $x_{i-1} \neq \pm 1$

6 τότε επιστρέψε ΑΛΗΘΕΣ

7 αν  $x_i \neq 1$

8 τότε επιστρέψε ΑΛΗΘΕΣ

9 επιστρέψε ΨΕΥΔΕΣ

Ο αλγόριθμος WITNESS υπολογίζει το  $a^{n-1} \pmod n$  υπολογίζοντας πρώτα την τιμή  $x_0 = a^u \pmod n$  στην γραμμή 2, υψώνοντας μετά το αποτέλεσμα στο τετράγωνο  $t$  φορές στην σειρά (γραμμές 3-6). Με αναγωγή στο  $i$ , η ακολουθία  $x_0, x_1, \dots, x_t$  των τιμών που υπολογίζονται ικανοποιεί την σχέση  $x_i \equiv a^{2^i u} \pmod n$  για  $i = 0, 1, \dots, t$ , οπότε  $x_t \equiv a^{n-1} \pmod n$ . Όποτε εκτελείται η γραμμή 4, ο βρόχος μπορεί να τερματιστεί πρόωρα αν στις γραμμές 5-6 ανακαλυφθεί μια μη-τετριμμένη τετραγωνική ρίζα του 1. Αν αυτό συμβεί, ο αλγόριθμος τερματίζει και επιστρέφει 'ΑΛΗΘΕΣ'. Οι γραμμές 7-8 επιστρέφουν 'ΑΛΗΘΕΣ' αν η τιμή που υπολογίστηκε για το  $x_t \equiv a^{n-1} \pmod n$  διαφέρει από το 1, για τον ίδιο λόγο που επιστρέφει 'ΑΛΗΘΕΣ' και ο αλγόριθμος PSEUDOPRIME. Τέλος, στην γραμμή 9 επιστρέφεται η τιμή 'ΨΕΥΔΕΣ', αν ο αλγόριθμος δεν έχει τερματίσει νωρίτερα.

Θα δείξουμε τώρα πως αν ο WITNESS( $a, n$ ) επιστρέφει 'ΑΛΗΘΕΣ', τότε ο  $n$  είναι σύνθετος.

Αν ο WITNESS επιστρέψει 'ΑΛΗΘΕΣ' στην γραμμή 8, τότε έχει ανακαλύψει ότι  $x_t = a^{n-1} \pmod n \neq 1$ . Αν ο  $n$  ήταν πρώτος, τότε από το θεώρημα του Fermat θα πρέπει να ισχύει  $a^{n-1} \equiv 1 \pmod n$  για όλα τα  $a \in Z_n^+$ . Συνεπώς, ο  $n$  δεν μπορεί να είναι πρώτος και η σχέση  $a^{n-1} \pmod n \neq 1$  είναι η απόδειξη γι' αυτό.

Αν ο WITNESS επιστρέψει 'ΑΛΗΘΕΣ' στην γραμμή 6, τότε έχει ανακαλύψει ότι το  $x_{i-1}$  είναι μη-τετριμμένη τετραγωνική ρίζα του 1 modulo  $n$ , αφού  $x_{i-1} \not\equiv \pm 1 \pmod n$  ενώ  $x_i \equiv x_{i-1}^2 \equiv 1 \pmod n$ . Το πόρισμα 36 δηλώνει πως μόνο αν ο  $n$  είναι σύνθετος μπορεί να υπάρχει μη-τετριμμένη τετραγωνική ρίζα του 1 modulo  $n$ , επομένως καταλήγουμε στο ότι ο  $n$  είναι σύνθετος.

Έτσι, ολοκληρώνεται η απόδειξη για την ορθότητα του WITNESS. Αν η κλήση WITNESS( $a, n$ ) επιστρέψει 'ΑΛΗΘΕΣ', τότε ο  $n$  είναι σίγουρα σύνθετος, κι αυτό μπορεί να αποδειχθεί για τα δεδομένα  $a$  και  $n$ .

Προχωράμε τώρα στην παρουσίαση του αλγορίθμου MILLER-RABIN που βασίζεται στο WITNESS. Υποθέτουμε και πάλι ότι το  $n$  είναι περιττός ακέραιος μεγαλύτερος από 2.

MILLER-RABIN( $n, s$ )

1 για  $j \leftarrow 1$  μέχρι  $s$

2      $a \leftarrow \text{RANDOM}(1, n - 1)$

3             αν WITNESS( $a, n$ )

4                     τότε επίστρεψε ΣΥΝΘΕΤΟΣ \ \ ελπίζουμε

5 επίστρεψε ΠΡΩΤΟΣ \ \ σίγουρα

Ο αλγόριθμος MILLER-RABIN είναι μια πιθανοτική αναζήτηση για μια απόδειξη ότι ο  $n$  είναι σύνθετος. Ο κύριος βρόχος διαλέγει  $s$  τυχαίες τιμές του  $a$  από το  $Z_n^+$ . Αν κάποιο από τα  $a$  είναι μάρτυρας, τότε ο MILLER-RABIN αποφαινεται 'ΣΥΝΘΕΤΟΣ' στην γραμμή 4. Μια τέτοια απόφαση είναι πάντοτε σωστή, από το γεγονός ότι ο αλγόριθμος WITNESS είναι σωστός. Αν δεν βρεθεί κανένας μάρτυρας σε αυτές τις  $s$  δοκιμές, τότε ο MILLER-RABIN υποθέτει πως αυτό συμβαίνει γιατί δεν υπάρχει κανένας μάρτυρας και συνεπώς ο  $n$  είναι πρώτος. Θα δείξουμε παρακάτω ότι αυτή η απόφαση είναι πιθανότατα σωστή αν το  $s$  είναι αρκετά μεγάλο, αλλά υπάρχει μια μικρή πιθανότητα να ήμαστε άτυχοι κατά την επιλογή των  $a$  και να υπάρχει κάποιος μάρτυρας.

Για παράδειγμα, έστω  $n$  ο αριθμός Carmichael 561, έτσι ώστε  $n-1 = 560 = 2^4 \cdot 35$ . Υποθέτοντας ότι επιλέγουμε  $a = 7$ , ξέρουμε ότι ο WITNESS υπολογίζει το  $x_0 \equiv a^{35} \equiv 241 \pmod{561}$  και υπολογίζει την ακολουθία  $X = \langle 241, 298, 166, 67, 1 \rangle$ . Άρα, ανακαλύψαμε μια μη-τετριμμένη

τετραγωνική ρίζα του 1, αφού  $a^{280} \equiv 67 \pmod{n}$  και  $a^{560} \equiv 1 \pmod{n}$ . Επομένως, το  $a = 7$  είναι μάρτυρας για το ότι ο  $n$  είναι σύνθετος, ο WITNESS επιστρέφει 'ΑΛΗΘΕΣ' και ο MILLER-RABIN επιστρέφει 'ΣΥΝΘΕΤΟΣ'. Αν ο  $n$  αποτελείται από  $\beta$  bits, ο MILLER-RABIN απαιτεί  $O(s\beta)$  αριθμητικές πράξεις και  $O(s\beta^3)$  πράξεις με bits, καθώς ασυμπτωτικά απαιτεί όση δουλειά χρειάζεται για  $s$  υψώσεις σε δύναμη.

**Ανάλυση της πιθανότητας λάθους του ελέγχου Miller-Rabin** Αν ο MILLER-RABIN αποφανθεί ότι ο  $n$  είναι πρώτος, τότε υπάρχει μια μικρή πιθανότητα ότι έχει κάνει λάθος. Σε αντίθεση με τον PSEUDOPRIME, αυτή η πιθανότητα λάθους είναι ανεξάρτητη από το  $n$ : δεν υπάρχουν άσχημες εισδοδοί για τον αλγόριθμο αυτό. Εξαρτάται όμως από το μέγεθος του  $s$  και τις τυχαίες επιλογές για τα διάφορα  $a$ . Επιπλέον, επειδή κάθε έλεγχος είναι αυστηρότερος από έναν απλό έλεγχο για αν ισχύει η σχέση (21), μπορούμε να ελπίζουμε ότι η πιθανότητα λάθους είναι μικρή για έναν τυχαίο ακέραιο  $n$ . Το ακόλουθα θεωρήματα παρέχουν την απάντηση.

**Θεώρημα 43.** *Αν το  $n$  είναι περιττός σύνθετος ακέραιος, τότε ο αριθμός των μαρτύρων για αυτό το γεγονός είναι τουλάχιστον  $3(n-1)/4$ .*

**Θεώρημα 44.** *Για κάθε περιττό ακέραιο  $n > 2$  και κάθε θετικό ακέραιο  $s$ , η πιθανότητα ότι ο αλγόριθμος Miller-Rabin( $n, s$ ) κάνει λάθος είναι το πολύ  $4^{-s}$ .*

Συνεπώς, αν θέσουμε  $s = 50$  τότε έχουμε ένα πολύ ικανοποιητικό επίπεδο ασφάλειας για τις περισσότερες πιθανές εφαρμογές. Αν αυτό που θέλουμε είναι να βρούμε κάποιον μεγάλο πρώτο αριθμό και εφαρμόσουμε τον αλγόριθμο Miller-Rabin σε τυχαία επιλεγμένους μεγάλους ακεραίους, τότε ακόμα και μια μικρή τιμή του  $s$  (έστω  $s = 3$ ) στις περισσότερες περιπτώσεις θα δώσει καλά αποτελέσματα. Αυτό σημαίνει πως για έναν τυχαία επιλεγμένο περιττό ακέραιο  $n$ , ο αναμενόμενος αριθμός των μη-μαρτύρων είναι αρκετά μικρότερος του  $(n-1)/4$ .

### 3.2 Ο ντετερμινιστικός αλγόριθμος

Τέλος, παρουσιάζουμε τον πρώτο ντετερμινιστικό αλγόριθμο που αποφαινεται για το αν ένας δεδομένος αριθμός είναι πρώτος ή όχι χωρίς να στηρίζεται σε κάποια αναπόδεικτη υπόθεση (όπως π.χ. η Υπόθεση του Riemann).

Ο αλγόριθμος βασίζεται στο ακόλουθο Λήμμα.



**Λήμμα 45.** Έστω  $a \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ , με  $n \geq 2$  και  $\gcd(a, n) = 1$ . Τότε ο  $n$  είναι πρώτος αριθμός αν και μόνο αν

$$(X + a)^n \equiv X^n + a \pmod{n}.$$

Απόδειξη. Για  $0 < i < n$ , ο συντελεστής του  $x^i$  στην έκφραση  $((X + a)^n - (X^n + a))$  είναι  $\binom{n}{i} a^{n-i}$ .

Έστω ότι ο  $n$  είναι όντως πρώτος αριθμός. Τότε, ισχύει ότι  $\binom{n}{k} \equiv 0 \pmod{n}$  και συνεπώς όλοι οι συντελεστές είναι ίσοι με 0.

Έστω ότι ο  $n$  είναι σύνθετος και ας θεωρήσουμε έναν πρώτο  $q$  που να είναι παράγοντας του  $n$  και έστω ότι  $q^k | n$ . Τότε, ο  $q^k$  δεν διαιρεί το  $\binom{n}{k}$  και είναι σχετικά πρώτος με το  $a^{n-q}$  και επομένως ο συντελεστής του  $X^q$  δεν είναι ισοδύναμος με μηδέν (modulo  $n$ ). Επομένως, η έκφραση  $((X + a)^n - (X^n + a))$  δεν είναι πάντοτε ισοδύναμη με μηδέν (modulo  $\mathbb{Z}_n$ ) στο  $\mathbb{Z}_n$ .  $\square$

Το παραπάνω Λήμμα είναι στην ουσία ένας απλός έλεγχος για το αν ένας αριθμός  $n$  είναι πρώτος. Αρκεί να διαλέξουμε έναν ακέραιο  $a$  και να ελέγξουμε αν ισχύει η ισοδυναμία. Το μειονέκτημα είναι ότι χρειάζεται χρόνος  $\Omega(n)$  γιατί στην χειρότερη περίπτωση χρειάζεται να υπολογίσουμε  $n$  συντελεστές στο αριστερό μέλος της ισοδυναμίας. Μία απλή μέθοδος για να μειώσουμε τον αριθμό των συντελεστών είναι να βρούμε την τιμή και των δύο μελών της ισοδυναμίας όταν δουλεύουμε modulo ένα πολυώνυμο της μορφής  $X^r - 1$  για μια κατάλληλα επιλεγμένη μικρή τιμή του  $r$ . Με άλλα λόγια, αρκεί να ελέγξουμε αν ισχύει η ακόλουθη ισοδυναμία

$$(X + a)^n \equiv X^n + a \pmod{X^r - 1, n}. \quad (22)$$

Από το Λήμμα 45 προκύπτει ότι όλοι οι πρώτοι αριθμοί ικανοποιούν την ισοδυναμία 22 για όλες τις τιμές των  $a, r$ . Από την άλλη πλευρά, παρουσιάζεται το πρόβλημα ότι υπάρχουν πλέον και σύνθετοι αριθμοί που ικανοποιούν την ισοδυναμία 22 για κάποιες τιμές των  $a, r$ . Μπορούμε όμως να δείξουμε ότι αν επιλέξουμε ένα κατάλληλο  $r$  τότε αν ικανοποιείται η 22 για αρκετά  $a$ , τότε ο  $n$  πρέπει να είναι δύναμη κάποιου πρώτου αριθμού. Ο αριθμός των  $a$  και η κατάλληλη τιμή του  $r$  φράσσονται από πάνω από ένα πολυώνυμο του  $\log n$ , οπότε καταλήγουμε σε έναν ντετερμινιστικό αλγόριθμο πολυωνυμικού χρόνου που αποκρίνεται για το αν ένας δεδομένος αριθμός είναι πρώτος.

Ακολούθως παρουσιάζουμε τον αλγόριθμο. Έστω ότι στην είσοδο έχουμε έναν ακέραιο  $n$  για τον οποίο θέλουμε να αποφανθούμε αν είναι πρώτος ή όχι.

1. Αρχικά, ο αλγόριθμος ελέγχει αν ισχύει  $n = a^b$  για κάποιον ακέραιο  $a \in \mathbb{N}$  και για  $b > 1$ , οπότε και επιστρέφει την απάντηση 'ΣΥΝΘΕΤΟΣ'.

2. Στην συνέχεια βρίσκει τον μικρότερο ακέραιο  $r$  για την οποίο ισχύει ότι  $\text{ord}_r(n) > \log^2 n$ , όπου θυμίζουμε ότι με  $\text{ord}_r(n)$  συμβολίζουμε την τάξη της υποομάδας που ορίζεται από το στοιχείο  $n$  όταν δουλεύουμε modulo  $r$ .
3. Ελέγχει αν  $1 \leq \text{gcd}(a, n) < n$  για κάποιο  $a \leq r$ , οπότε κι επιστρέφει την απάντηση 'ΣΥΝΘΕΤΟΣ'.
4. Ελέγχει αν ισχύει  $n \leq r$  οπότε κι επιστρέφει 'ΠΡΩΤΟΣ'.
5. Για τις τιμές του  $a$  από 1 ως  $\lfloor \sqrt{\phi(r)} \log n \rfloor$  ο αλγόριθμος ελέγχει αν  $(X + a)^n \not\equiv X^n + a \pmod{X^r - 1, n}$  οπότε κι επιστρέφει 'ΣΥΝΘΕΤΟΣ'.
6. Ο αλγόριθμος επιστρέφει την απάντηση 'ΠΡΩΤΟΣ'.

**Θεώρημα 46.** *Ο παραπάνω αλγόριθμος επιστρέφει 'ΠΡΩΤΟΣ' αν και μόνο αν ο  $n$  είναι πρώτος.*

Για την απόδειξη του παραπάνω θεωρήματος, θα χρειαστεί να αποδείξουμε ότι αν ισχύει το ένα σκέλος της πρότασης, τότε ισχύει οπωσδήποτε και το άλλο.

**Λήμμα 47.** *Αν ο  $n$  είναι πρώτος, τότε ο αλγόριθμος επιστρέφει 'ΠΡΩΤΟΣ'.*

*Απόδειξη.* Αν ο  $n$  είναι πρώτος, τότε τα βήματα 1 και 3 δεν θα επιστρέψουν σε καμία περίπτωση την απάντηση 'ΣΥΝΘΕΤΟΣ'. Από το Λήμμα 45 ο βρόχος επίσης δεν θα επιστρέψει 'ΣΥΝΘΕΤΟΣ'. Επομένως, ο αλγόριθμος θα επιστρέψει 'ΠΡΩΤΟΣ' είτε στην γραμμή 4 είτε στην γραμμή 6.  $\square$

Για την ολοκλήρωση της απόδειξης του Θεωρήματος 46 αρκεί να ισχύει το ακόλουθο Λήμμα, το οποίο παρατίθεται χωρίς απόδειξη.

**Λήμμα 48.** *Αν ο αλγόριθμος επιστρέψει 'ΠΡΩΤΟΣ', τότε ο  $n$  είναι πρώτος.*

## 4 Εφαρμογές της κρυπτογραφίας

Στην ενότητα αυτή θα εξετάσουμε κάποιες περισσότερο πρακτικές εφαρμογές της κρυπτογραφίας και των πρωτοκόλλων που παρουσιάσαμε στα προηγούμενα κεφάλαια. Θα παρουσιάσουμε κάποια πρωτόκολλα που επιτρέπουν την διαμοίραση κάποιου μυστικού στους χρήστες με τρόπο που δεν θα βλάπτει την ιδιωτικότητα του μυστικού, όπως και πρωτόκολλα που επιτρέπουν την δέσμευση των χρηστών σε συγκεκριμένες αποφάσεις και θα αποτρέπουν την υστερόβουλη αλλαγή τους. Τέλος, θα περιγράψουμε κάποιες εφαρμογές τους σε εκλογές, δημοπρασίες και μικροσυναλλαγές στο Διαδίκτυο.

### 4.1 Σχήματα διαμοίρασης μυστικού και πρωτόκολλα δέσμευσης

**Διαμοίραση μυστικού** Έστω ότι κάποιος κεντρικός χρήστης έχει στην διάθεσή του μια μυστική πληροφορία, της οποίας την δυαδική αναπαράσταση την συμβολίζουμε με  $S$ . Ο χρήστης θα ήθελε να μοιράσει την μυστική πληροφορία σε κάποιους άλλους χρήστες (έστω  $n$  το πλήθος τους) με τέτοιο τρόπο ώστε αν συνεργαστούν τουλάχιστον  $k$  από αυτούς να μπορούν να επανασυνθέσουν την πληροφορία. Στην αντίθετη περίπτωση, ο χρήστης θα ήθελε όχι μόνο να μην μπορούν να βρουν το  $S$ , αλλά και να μην έχουν μάθει κάτι περισσότερο για το  $S$  από ότι ήξεραν πριν καν γίνει η διαμοίρασή του. Για παράδειγμα, έστω ότι ο κεντρικός χρήστης έχει ως μυστικό την λέξη 'password' και την μοιράζει σε 4 χρήστες δίνοντας δύο γράμματα στον καθένα τους. Τότε, αν συνεργαστούν και οι 4 μπορούν να ανακτήσουν το  $S$ , αν όμως είναι λιγότεροι τότε ναι μεν δεν μπορούν να ανακτήσουν κατευθείαν την πληροφορία, έχουν όμως περισσότερη πληροφορία γι αυτό και επομένως τους είναι ευκολότερο να το βρουν δοκιμάζοντας όλες τις πιθανές λύσεις (υποθέτουμε ότι γνωρίζουν το μήκος της λέξης).

Εξετάζουμε αρχικά την περίπτωση όπου πρέπει να συνεργαστούν όλοι οι χρήστες προκειμένου να επανασυνθέσουν το μυστικό, με άλλα λόγια όταν  $k = n$ . Ο κεντρικός χρήστης εκτελεί τα ακόλουθα βήματα.

1. Αρχικά, διαλέγει έναν μεγάλο πρώτο αριθμό  $p$ , τέτοιον ώστε  $S < p$  και επομένως ισχύει ότι  $S \in Z_p^*$ .
2. Διαλέγει τυχαία  $a_i \in Z_p^*$  για  $i = 1, \dots, n - 1$  και δίνει το  $a_i$  στον  $i$ -οστό χρήστη.
3. Υπολογίζει το  $a_n = S - \sum_{i=1}^{n-1} a_i \pmod{n}$  και το δίνει στον  $n$ -οστό χρήστη.

Αν όντως συνεργαστούν και οι  $n$  χρήστες, τότε αρκεί να αθροίσουν τα  $a_i$  που κατέχουν για να επανασυνθέσουν το  $S$ , αφού ισχύει  $S = \sum_{i=1}^n a_i$ . Έστω ότι συνεργάζονται  $n - 1$  χρήστες κι έστω ότι δεν δέχεται ο  $n$ -οστός χρήστης να δώσει το  $a_n$ . Τότε, οι υπόλοιποι χρήστες προκειμένου να βρουν το  $S$  μπορούν να δοκιμάσουν να μαντέψουν το  $a_n \in Z_p^*$  και να εξετάσουν το  $S$  που θα προκύψει. Αυτό όμως είναι ισοδύναμο με το να μαντέψει κάποιος χρήστης από μόνος του ένα  $S \in Z_p^*$ , επομένως οι συνεργαζόμενοι χρήστες δεν έχουν αποκτήσει κάποια επιπρόσθετη πληροφορία από την συνεργασία.

Έστω τώρα η περίπτωση που αρκεί να συνεργαστούν  $k$  χρήστες, με  $k < n$ . Είναι προφανές ότι το προηγούμενο σχήμα δεν δουλεύει και χρειάζεται να σκεφτούμε κάτι περισσότερο εκλεπτυσμένο. Ο κεντρικός χρήστης εκτελεί τα ακόλουθα βήματα.

1. Αρχικά, διαλέγει έναν μεγάλο πρώτο αριθμό  $p$ , τέτοιον ώστε  $S < p$  κι επομένως ισχύει ότι  $S \in Z_p^*$ .
2. Διαλέγει τυχαία  $a_i \in Z_p^*$  για  $i = 1, \dots, k - 1$ .
3. Ορίζει την συνάρτηση  $f(x) = S + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1} \pmod{p}$ .
4. Τέλος, δίνει το  $f(i)$  στον  $i$ -οστό χρήστη.

Παρατηρούμε ότι στην ουσία έχουμε  $n$  εξισώσεις με  $k$  αγνώστους, τους  $S, a_1, a_2, \dots, a_{k-1}$ . Αν συνεργαστούν τουλάχιστον  $k$  χρήστες, τότε αρκεί να λύσουν ένα σύστημα  $k$  εξισώσεων με  $k$  αγνώστους και να υπολογίσουν το  $S$ . Στην αντίθετη περίπτωση, προκύπτει ένα σύστημα  $k - 1$  εξισώσεων με  $k$  αγνώστους, οπότε οι συνεργαζόμενοι χρήστες δεν μπορούν να υπολογίσουν το  $S$ , ούτε έχουν αποκομίσει κάποια επιπρόσθετη πληροφορία που τους διευκολύνει στον υπολογισμό του.

**Πρωτόκολλα δέσμευσης** Στην συνέχεια θα ασχοληθούμε με πρωτόκολλα δέσμευσης και εξετάζουμε το ακόλουθο παράδειγμα. Ας υποθέσουμε ότι η Alice και ο Bob έχουν πάρει διαζύγιο, μένουν πλέον σε διαφορετικές πόλεις και ψάχνουν έναν τρόπο να αποφασίσουν ποιος θα πάρει το αυτοκίνητο. Συμφωνούν στο να στρίψουν ένα κέρμα, αλλά ο Bob δεν θα ήθελε να διαλέξει ότι θα έρθει 'κορώνα' και να ακούσει την Alice να του ανακοινώνει από το τηλέφωνο ότι τελικά το αποτέλεσμα είναι 'γράμματα'. Θα θέλαμε λοιπόν να μπορεί ο Bob να διαλέξει ένα αποτέλεσμα χωρίς να το ανακοινώσει στην Alice και αυτή να ρίξει το κέρμα. Το επιθυμητό είναι το αποτέλεσμα που

διάλεξε ο Bob και το αποτέλεσμα που του ανακοίνωσε η Alice να μην μπορούν να αλλάξουν κατά την διάρκεια εκτέλεσης του πρωτοκόλλου.

Υπάρχουν αρκετά πρωτόκολλα που μπορεί να χρησιμοποιήσει κανείς σε τέτοιες περιπτώσεις, εμείς θα αρκεστούμε στην περιγραφή κάποιων απλών μεθόδων. Η μία από αυτές βασίζεται στο πρόβλημα του διακριτού λογαριθμού και η άλλη στο πρόβλημα της παραγοντοποίησης. Στην πρώτη, η Alice και ο Bob συμφωνούν σε έναν μεγάλο πρώτο αριθμό  $p$  και ένα δημιουργό στοιχείο  $g \in Z_p^*$ . Στην συνέχεια, η Alice επιλέγει τυχαία έναν ακέραιο  $a \in Z_p^*$ . Μπορεί πλέον να δει κανείς το πρόβλημα ως εξής: ο Bob καλείται να μαντέψει αν ο  $a$  είναι περιττός ή άρτιος αριθμός. Σημειώνουμε ότι οι μισοί ακέραιοι στο  $Z_p^*$  είναι περιττοί και οι άλλοι μισοί είναι άρτιοι. Επομένως, η Alice υπολογίζει το  $b = g^a \pmod{p}$  και το μεταδίδει στον Bob, ο οποίος έστω ότι αποφασίζει ότι ο  $a$  είναι περιττός. Τότε, η Alice καλείται να αποκαλύψει το  $a$  και αν είναι περιττός τότε κερδίζει ο Bob, ενώ στην αντίθετη περίπτωση το αυτοκίνητο το παίρνει η Alice. Παρατηρούμε ότι η Alice δεν μπορεί να πει ψέματα για την τιμή του  $a$  που έχει επιλέξει, καθώς μόνο ένα  $a \in Z_p^*$  έχει την ιδιότητα ότι  $b = g^a \pmod{p}$ . Επιπλέον, ο Bob δεν μπορεί να χρησιμοποιήσει την γνώση του  $b$  για να αποφασίσει σε ένα λογικό (πολυωνυμικό) χρονικό διάστημα αν ο  $a$  είναι περιττός ή όχι, καθώς αυτό θα σήμαινε ότι έχει κάποιον πολυωνυμικό αλγόριθμο για το πρόβλημα του διακριτού λογαριθμού.

Η δεύτερη μέθοδος βασίζεται, όπως προαναφέραμε, στο πρόβλημα της παραγοντοποίησης και είναι η ακόλουθη. Αρχικά, η Alice επιλέγει δύο μεγάλους πρώτους αριθμούς  $p$  και  $q$  τέτοιους ώστε και οι δύο να είναι ισοδύναμοι είτε με 3 modulo 4 είτε με 1 modulo 4. Υπολογίζει το  $n = pq$  και το ανακοινώνει στον Bob. Σημειώνουμε ότι όπως και να επιλέχθηκαν οι  $p$  και  $q$ , ισχύει ότι  $n = 1 \pmod{4}$ . Ο Bob καλείται πλέον να αποφασίσει (μέσα σε ένα σύντομο χρονικό διάστημα) αν οι  $p$  και  $q$  είναι ισοδύναμοι με 3 ή με 1 και στην συνέχεια η Alice του ανακοινώνει τα  $p$  και  $q$ . Αν ο Bob έχει επιλέξει σωστά τότε κερδίζει, αλλιώς κερδίζει η Alice. Σημειώνουμε πως η Alice δεν μπορεί να πει ψέματα, καθώς η μόνη δυνατή παραγοντοποίηση του  $n$  είναι οι πρώτοι αριθμοί  $p$  και  $q$ , ενώ ο Bob δεν μπορεί να εκμεταλλευτεί την γνώση του  $n$  για να βρει τα  $p$  και  $q$ , καθώς αυτό θα σήμαινε ότι υπάρχει πολυωνυμικός αλγόριθμος παραγοντοποίησης.

## 4.2 Εκλογές, δημοπρασίες και οικονομικές συναλλαγές

Σε αυτή την ενότητα παρουσιάζουμε μερικές εφαρμογές της κρυπτογραφίας που μας επιτρέπουν ορισμένες δραστηριότητες της καθημερινής, εκτός Διαδικτύου, ζωής να μπορούμε να τις πραγματοποιήσουμε και στο Διαδίκτυο. Θα παρουσιάσουμε τις βασικές ιδιότητες που πρέπει να

ικανοποιούν τα διάφορα πρωτόκολλα, χωρίς όμως να υπεισέλθουμε σε αναλυτική παρουσίαση πρωτοκόλλων.

**Εκλογές - ηλεκτρονικές ψηφοφορίες** Με τον όρο ηλεκτρονική ψηφοφορία εννοούμε την άσκηση του εκλογικού δικαιώματος με τη χρήση ηλεκτρονικών μεθόδων. Τα θεμελιώδη στοιχεία που συνθέτουν την ιδιαίτερη φύση της ηλεκτρονικής ψήφου και τη διαφοροποιούν σε μεγάλο βαθμό από τα υπάρχοντα συστήματα της εκλογικής διαδικασίας είναι η δυνατότητα άσκησης του εκλογικού δικαιώματος από απόσταση, χωρίς την αυτοπρόσωπη παρουσία του ψηφοφόρου στο εκλογικό τμήμα και η χρήση υπολογιστικού συστήματος και κατά συνέπεια αυτοματοποιημένων μεθόδων, για την οργάνωση και διεξαγωγή της όλης εκλογικής διαδικασίας. Η ρίψη μίας ηλεκτρονικής ψήφου μέσω του Διαδικτύου πρέπει να συνοδεύεται από επαρκείς εγγυήσεις ασφάλειας ότι η ταυτότητα του ψηφοφόρου δεν θα αποκαλυφθεί κατά τη διάρκεια της μεταφοράς και της επεξεργασίας της ψήφου, όπως επίσης και ότι το περιεχόμενό της δεν θα μεταβληθεί, λόγω μη αποτελεσματικής λειτουργίας του συστήματος ή εξαιτίας εκλογικής λαθροχειρίας. Με βάση τα παραπάνω, ηλεκτρονικό εκλογικό σύστημα ορίζεται το σύστημα εκείνο που είναι προορισμένο να εξυπηρετήσει τις ανάγκες διεξαγωγής μιας ηλεκτρονικής ψηφοφορίας.

Προκειμένου να σχεδιαστεί ένα σύστημα ηλεκτρονικής ψηφοφορίας το οποίο θα χρησιμοποιηθεί για εκλογές ευρείας κλίμακας είναι απαραίτητο να πληρούνται μερικές βασικές προϋποθέσεις:

- Δημοκρατικό: Μόνο οι ψηφοφόροι που έχουν δικαίωμα ψήφου μπορούν να ψηφίσουν, ενώ κανένας ψηφοφόρος δεν έχει το δικαίωμα να ψηφίσει πάνω από μία φορές
- Μυστικό: όλες ψήφοι παραμένουν μυστικές κατά τη διάρκεια υποβολής ψήφων και κανένας δεν είναι σε θέση να συνδέσει την ταυτότητα ενός ψηφοφόρου με την εκάστοτε ψήφο του
- Ακριβές: καμία ψήφος δεν μπορεί να αλλοιωθεί ή να καταμετρηθεί περισσότερες από μία φορές. Επίσης, καμία ψήφος δεν μπορεί να διαγραφεί από τις εκλογικές αρχές αλλά ούτε και από οποιουσδήποτε άλλους παράγοντες
- Προστατευόμενο από καταναγκασμό: ο ψηφοφόρος δεν κατέχει ούτε μπορεί να δημιουργήσει μια απόδειξη που να δείχνει το περιεχόμενο της ψήφου
- Ανθεκτικό: κάθε κακόβουλη συμπεριφορά από οποιονδήποτε παράγοντα μπορεί να αντιμετωπιστεί

- Αμερόληπτο: κανένας δεν είναι σε θέση να μάθει το αποτέλεσμα της εκλογικής διαδικασίας πριν την τελική καταμέτρηση των ψήφων. Συνεπώς, διασφαλίζεται ότι δεν θα επηρεαστούν οι τελευταίοι χρονικά ψηφοφόροι μέσω της ανακοίνωσης μιας εκτίμησης του αποτελέσματος και ότι δεν παρέχεται ένα πλεονέκτημα σε ένα συγκεκριμένο σύνολο οντοτήτων
- Ευκολία συμμετοχής των ψηφοφόρων
- Οικουμενικά επαληθεύσιμο: κάθε εξωτερικός παρατηρητής μπορεί να πειστεί για την ορθότητα των εκλογικών αποτελεσμάτων

**Δημοπρασίες** Είναι δύσκολο να καθορίσει κανείς πότε ακριβώς έγινε η πρώτη δημοπρασία στο Διαδίκτυο, είναι γνωστό όμως πως αυτές είχαν αρχίσει να διεξάγονται μέσω ηλεκτρονικού ταχυδρομείου και newsgroups ήδη από το 1988. Με την ραγδαία ανάπτυξη του Διαδικτύου κατά την δεκαετία του '90, ήταν αναπόφευκτο να χρησιμοποιηθεί αυτή η νέα τεχνολογία στις δημοπρασίες που διεξάγονταν online, οπότε και προέκυψε η ανάγκη για κρυπτογραφικά ασφαλή πρωτόκολλα δημοπρασίας.

Για να είναι ασφαλή τα πρωτόκολλα που χρησιμοποιούνται για δημοπρασίες στο Διαδίκτυο, χρειάζεται να ικανοποιούνται ορισμένες ιδιότητες που μερικές φορές είναι αλληλοσυγκρουόμενες, με αποτέλεσμα να μην υπάρχει κάποιο πρωτόκολλο που να τις ικανοποιεί όλες ταυτόχρονα. Στη συνέχεια αναφέρονται ορισμένες από αυτές τις ιδιότητες.

- Ορθότητα: Αν όσοι συμμετέχουν στη δημοπρασία φερθούν δίκαια τότε η σωστή νικητήρια τιμή και ο σωστός νικητής θα αναγνωριστούν και θα αναδειχθούν σύμφωνα πάντα με τους κανόνες της δημοπρασίας
- Δικαιοσύνη: Η δικαιοσύνη περιλαμβάνει ότι κανένας πλειοδότης δεν έχει καμιά πληροφορία για τις άλλες προσφορές πριν υποβάλλει την δική του. Η ιδιότητα αυτή περιλαμβάνεται επίσης και στην εμπιστευτικότητα. Επιπλέον, η δικαιοσύνη συνεπάγεται ότι αφού κάποιος πλειοδότης υποβάλλει την προσφορά του, τότε η προσφορά αυτή δεν μπορεί να μεταβληθεί και πως κανένας πλειοδότης δεν μπορεί να αρνηθεί την προσφορά του αφού την έχει υποβάλλει. Το γεγονός αυτό καλείται πολλές φορές και μη-απάρνηση της προσφοράς
- Ευρωστία: Η κακόβουλη συμπεριφορά οποιουδήποτε συμμετέχει στη δημοπρασία δεν θα πρέπει να θέτει σε κίνδυνο το σύστημα ή να οδηγεί σε λάθος αποτελέσματα. Η ευρωστία είναι

συμπληρωματική ιδιότητα της ορθότητας και εγγυάται ότι αν υπάρχει κάποιο τελικό αποτέλεσμα, τότε το αποτέλεσμα αυτό είναι το σωστό οποιαδήποτε αποτυχία ή επίθεση και να έχει συμβεί στο σύστημα

- **Εμπιστευτικότητα:** Οι δημοπράτες δεν θα πρέπει να γνωρίζουν την αξία των προσφορών μέχρι τη φάση του ανοίγματός τους. Για το λόγο ότι αν δεν συμβαίνει αυτό μπορούν να γίνουν κάποιες συνεργασίες με στόχο τα προσωπικά συμφέροντα κάποιων (ανάλογα και με το είδος και τους κανόνες της δημοπρασίας που διεξάγεται) και την τελική εξαπάτηση των τίμιων συμμετεχόντων
- **Ανωνυμία:** Οι ταυτότητες των πλειοδοτών που έχουν χάσει παραμένουν εμπιστευτικές μετά την αποκάλυψη του τελικού νικητή, έτσι ώστε να μην μπορούν να εκμεταλλευτούν κάποιοι την μη ανωνυμία με τους τρόπους που εξηγούνται στην επόμενη ιδιότητα
- **Μυστικότητα των προσφορών που έχασαν:** Οι προσφορές που δεν κέρδισαν τελικά τη δημοπρασία παραμένουν μυστικές, ακόμη και από τον ίδιο το δημοπράτη, μετά την αποκάλυψη του τελικού νικητή. Κι αυτό γιατί οι πλειοδότες που έχασαν είναι λογικό να μην επιθυμούν να συλλέγουν άλλοι τις εκτιμήσεις τους για τα προϊόντα, κάτι που μπορεί να θεωρηθεί παραβίαση των δικαιωμάτων τους, και μπορεί να τους φέρνει σε μειονεκτικότερη θέση σε κάποια άλλη δημοπρασία. Επιπλέον κάποιος πωλητής μπορεί να αποκτήσει κάποια πλεονεκτήματα όταν σε κάποια μελλοντική δημοπρασία θελήσει να πουλήσει ένα ίδιο ή παρόμοιο αντικείμενο
- **Δημόσια επαλήθευση:** Πρέπει όλοι οι συμμετέχοντες στη διαδικασία της δημοπρασίας, καθώς επίσης και ένας ουδέτερος παρατηρητής, να είναι ικανοί να επιβεβαιώσουν την εγκυρότητα των κρίσιμων διαδικασιών. Κρίσιμες διαδικασίες θεωρούνται αυτές που είναι ικανές να αλλάξουν το αποτέλεσμα της δημοπρασίας
- **Ευκολία - αποτελεσματικότητα :** Η δημοπρασία γίνεται με αλληλεπίδραση ανθρώπων. Οι κανόνες του πρωτοκόλλου που χρησιμοποιείται για τη διεκπεραίωσή της θα πρέπει να είναι αρκετά απλοί έτσι ώστε όσοι λαμβάνουν μέρος να μπορούν να τους κατανοήσουν και να τους ακολουθήσουν σε λογικό χρόνο

**Οικονομικές συναλλαγές** Με παρόμοιο τρόπο όπως και στις προηγούμενες δύο εφαρμογές, τα κρυπτογραφικά πρωτόκολλα βρήκαν μεγάλη εφαρμογή για την υλοποίηση μεθόδων που επιτρέπουν



την ασφαλή διεξαγωγή οικονομικών συναλλαγών μέσω του Διαδικτύου.

Στην συνέχεια αναφέρουμε ορισμένες από τις ιδιότητες που πρέπει να πληροί ένα πρωτόκολλο οικονομικών συναλλαγών.

- Χαμηλό κόστος συναλλαγής: το κόστος διενέργειας μιας συναλλαγής θα πρέπει να είναι όσο χαμηλό γίνεται. Ειδικότερα, σε περιπτώσεις όπου διακινούνται μικρά ποσά (μικροσυναλλαγές), αυτός ο παράγοντας είναι ο σημαντικότερος, καθώς δεν είναι επιθυμητό π.χ. για μια συναλλαγή του 1 ευρώ να υπάρχει πρόσθετη επιβάρυνση 0,5 ευρώ
- Ασφάλεια: τα πρωτόκολλα πρέπει να είναι ανθεκτικά σε επιθέσεις με στόχο τόσο το να διασφαλίζεται ότι η πιστοποίηση του χρήστη - αποστολέα όσο και η ακεραιότητα του μηνύματος. Επιπλέον, το πρωτόκολλο πρέπει να εξασφαλίζει ότι ένα μήνυμα (που αντιστοιχεί σε ηλεκτρονικό νόμισμα) δεν μπορεί να χρησιμοποιηθεί πάνω από μία φορά
- Ιδιωτικότητα: πρέπει να διασφαλίζεται ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε πληροφορία σχετικά με την ταυτότητα του αγοραστή. Σημειώνουμε ότι στα περισσότερα πρωτόκολλα, οι αγοραστές συμμετέχουν με ψευδώνυμα. Επιπλέον, από την στιγμή που θα ολοκληρωθεί η συναλλαγή, δεν πρέπει να υπάρχει η δυνατότητα να συνδεθεί κάποια αμοιβή με τον αγοραστή (όπως π.χ. δεν θέλουμε να μπορεί κάποιος έχοντας ένα χαρτονόμισμα να ξέρει ποιοι άλλοι το χρησιμοποίησαν κατά το παρελθόν)
- Δυνατότητα άμεσης επιβεβαίωσης

## Αναφορές

- [1] T.H. Cormen, C.E. Leiserson, R.L. Rivest and C. Stein. Introduction to Algorithms, Second Edition. MIT Press, 2001
- [2] D. Welsh. Codes and Cryptography. Carlendon Press, Oxford. 1995
- [3] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone. Handbook of Applied Cryptography. CRC Press, 2001.