ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

1η Σειρά Ασκήσεων

Υπολογιστική Κρυπτογραφία

Ανδρέας Στάμος

Αριθμός μητρώου: 03120***

Διεύθυνση ηλεκτρονικού ταχυδρομείου: stamos.aa@gmail.com

9ο Εξάμηνο — 2024-2025

Περιεχόμενα

1 Άσκηση 1: Affine Cipher

1.1 Περιγραφή κρυπτοσυστήματος

Το σύστημα κρυπτογραφεί χωριστά, και με την σειρά, κάθε χαρακτήρα του plaintext.

Υποθέτουμε ότι το κείμενο αποτελείται μόνο από πεζούς λατινικούς χαρακτήρες.

Έστω x_i ο αύξων αριθμός στο λατινικό αλφάβητο του i-οστού χαρακτήρα του plaintext.

Το κλειδί ορίζεται να είναι ένας ζεύγος αριθμών (a, b) ώστε $\gcd(a, b) = 1$ (a, b σχετικά πρώτοι).

Η κρυπτογράφηση του x_i είναι:

$$y_i = ENC(x_i) = ax_i + b \mod 26$$
$$x_i = DEC(y_i) = a^{-1}(y_i - b) \mod 26$$

Παρατηρούμε ότι δεν θα είχε νόημα να ορίσουμε κλειδιά εκτός του $\{0 \cdots 25\}$ διότι θα ήταν ισοδύναμα με τα υπόλοιπά τους ως προς 26.

Επίσης παρατηρούμε ότι η ιδιότητα $\gcd(a, b) = 1$ είναι αναγκαία ώστε η αποκρυπτογράφηση να μπορεί να επιστρέψει το αρχικό κείμενο.

1.2 Ερώτημα α: Κρυπτανάλυση

1.2.1 Chosen Plaintext Attack (CPA)

Ζητούμε το κρυπτοκείμενο y_0, y_1 των χαρακτήρων:

$$x_0 = \texttt{'z'} = 26 \equiv 0 \mod 26$$
$$x_1 = \texttt{'a'} = 1 \equiv 1 \mod 26$$

Είναι:

$$y_0 \equiv a \cdot 0 \mod 26 \equiv a \mod 26$$
$$y_1 \equiv a \cdot 1 + b \mod 26 \equiv y_0 + b \mod 26 \iff b = y_1 - y_0 \mod 26$$

Όλα τα κλειδιά $a' \equiv a \mod 26$ και $b' \equiv b \mod 26$ είναι ισοδύναμα (ίδια κρυπτογράφηση και αποκρυπτογράφηση). Συνεπώς διαθέτουμε ένα κλειδί για το σύστημα, το:

$$(a, b) = (y_0, y_1 - y_0)$$

.

1.2.2 Χαλάρωση των περιορισμών — Known Plaintext Attack (KPA)

Έστω το κρπτοκείμενο y_0, y_1 δύο χαρακτήρων x_0, x_1 με $x_0 \neq x_1$.

Είναι:

$$y_0 \equiv ax_0 + b \mod 26$$
$$y_1 \equiv ax_1 + b \mod 26$$

Συνεπώς:

$$y_1 \equiv ax_1 + y_0 - ax_0 \mod 26 \iff y_1 - y_0 \equiv a(x_1 - x_0) \mod 26 \tag{1.1}$$

Αν $gcd(x_1 - x_0, 26) = 1$ τότε απευθείας έχουμε βρει το κλειδί:

$$a \equiv (y_1 - y_0)(x_1 - x_0)^{-1} \mod 26$$
$$b \equiv y_0 - ax_0 \mod 26$$

Από τους $26 \cdot 25 = 650$ συνδυασμούς για τα (x_0, x_1) (τα αρχικά μηνύματα υποθέτουμε διαφορετικά, αλλιώς δεν έχει νόημα), οι 312 (48%) δίνουν $x_1 - x_0$ σχετικά πρώτο με το 26. Οπότε έχουμε σημαντική βελτίωση σε σχέση με την προηγούμενη CPA.

Θα το χαλαρώσουμε ακόμα παραπάνω.

Έστω ότι $d = gcd(x_1 - x_0, 26) > 1$.

Αν $d \nmid (y_1, y_0)$ τότε η σχέση 1.1 είναι αδύνατη, γεγονός που είναι άτοπο αφού τα y_1, y_0 είναι έγκυρα κρυπτοκείμενα.

Άρα:

$$\frac{y_1 - y_0}{d} \equiv a\frac{x_1 - x_0}{d} \mod \frac{26}{d} \iff a \equiv \frac{y_1 - y_0}{d}(\frac{x_1 - x_0}{d})^{-1} \mod \frac{26}{d} \tag{1.2}$$

Στο σημείο αυτό θα μπορούσαμε να πούμε ότι έχουμε περιορίσει τις τιμές των (a, b) οπότε κάνουμε μια brute force attack ελέγχοντας με frequencies αν πετύχουμε έγκυρο plaintext. Αλλά ας το προσπεράσουμε αυτό.

Έστω ότι $d > 1$ και ότι έχουμε και ένα τρίτο ζεύγος plaintext, ciphertext (x_2, y_2).

Προφανώς, έστω ότι $x_2 \neq x_1$, $x_2 \neq x_0$ (αλλιώς φυσικά δεν κερδίσαμε τίποτα).

Αν κάποια διαφορά $x_2 - x_1$ ή $x_2 - x_0$ είναι σχετικά πρώτη με το 26 εφαρμόζουμε το προηγούμενο για το αντίστοιχο ζεύγος.

Έστω ότι μία από τις δύο αυτές διαφορές, έστω χωρίς βλάβη της γενικότητας η $x_2 - x_0$ (όμοια για την άλλη) δίνει $\gcd(x_2 - x_0, 26) = d' > 1$.

Υποθέτουμε αρχικά $d' \neq d$.

Το 26 έχει διαιρέτες το $2, 13, 26$, οπότε τα d, d' έχουν κάποια από αυτές τις τιμές. Ωστόσο:

$$\gcd(x_i - x_j, 26) = 26 \iff x_i - x_j \equiv 0 \mod 26 \iff x_i = x_j \mod 26$$

Αλλά $0 \leq x_i, x_j \leq 25$ οπότε $\gcd(x_i - x_j, 26) = 26 \iff x_i = x_j$, που έχουμε υποθέσει ότι δεν το έχουμε. (δεν έχει νόημα να μελετάμε τέτοια περίπτωση)

Άρα αφού υποθέσαμε $d' \neq d$ τότε $(d, d') = (2, 13)$ ή $(d', d) = (13, 2)$.

Εφαρμόζοντας την σχέση 1.2 λαμβάνουμε:

$$\begin{aligned} a &\equiv \frac{y_1 - y_0}{d}(\frac{x_1 - x_0}{d})^{-1} \mod \frac{26}{d} \\ a &\equiv \frac{y_2 - y_0}{d}(\frac{x_2 - x_0}{d})^{-1} \mod \frac{26}{d'} \end{aligned} \tag{1.3}$$

Με βάση τα προηγούμενα είναι $(\frac{26}{d}, \frac{26}{d'}) \in \{(2, 13), (13, 2)\}$.

Συνεπώς, με βάση το Κινέζικο Θεώρημα Υπολοίπων, το σύστημα έχει μια μοναδική λύση $a \mod 26$ (την βρίσκουμε εύκολα με εκτεταμένο αλγόριθμο Ευκλείδη).

Έχοντας βρει το a προσδιορίζουμε άμεσα $b \equiv y_1 - ax_0 \mod 26$, οπότε κρπυταναλύσαμε το σύστημα.

Απομένει η περίπτωση $d' = d$, δηλαδή η περίπτωση όπου:

$$d = \gcd(x_1 - x_0, 26) = \gcd(x_2 - x_0, 26) = \gcd(x_2 - x_1, 26) > 1 \tag{1.4}$$

Οι περιπτώσεις αυτές είναι ακόμα πιο μειωμένες από πριν.

Πιο συγκεκριμένα με ένα script Python (παρακάτω γίνεται μαθηματική ανάλυση με κλειστό τύπο αντί brute force αναζήτηση) βρίσκουμε ότι από $26 \cdot 25 \cdot 24$ διαφορετικές 3άδες ζευγών μόλις 3432 (22%) δίνουν διαφορές που να έχουν όλες ίδιο GCD με το 26 και αυτό το GCD να είναι και > 1.

Θα δώσουμε μια ανάλυση για n διαφορετικά ζεύγη κρυπτοκειμένων. Προφανώς για $n = 26$ θα μπορούμε να βρούμε το κλειδί με 100% επιτυχία, αφού έχουμε κρυπτοσύστημα αντικατάστασης και θα έχουμε βρει το κρυπτοκείμενο όλων των χαρακτήρων.

Για να μην μπορούμε να βρούμε το κλειδί με n ζεύγη, πρέπει οι διαφορές ανά δύο των plaintexts να δίνουν όλες τον ίδιο GCD με το 26, έστω d, και μάλιστα $d > 1$.

Διακρίνουμε περιπτώσεις:

d=26 Η περίπτωση αυτή αποκλείεται αφού $\gcd(x - y, 26) = 26 \iff x \equiv y \mod 26$ που αποκλείεται διότι $x \neq y$ από υπόθεση.

d=13 Είναι: $\gcd(x - y, 26) = 13 \implies x \equiv y \mod 13$. Όμως $x \neq y$ και $x, y \in \{0 \cdots 25\}$. Άρα πρέπει $y = x + 13$, $x \in \{0 \cdots 12\}$. Συνεπώς αποκλείεται $n \geq 3$ διότι έχουμε πάντα έναν αριθμό ≤ 13 και έναν > 13.

Για αυτές τιμές ισχύει επίσης $\gcd(x - y, 26) = 13$. Άρα πετυχαίνουμε $d = 13$ μόνο για $n = 2$ ζεύγη και αυτά είναι ακριβώς 12 υποσύνολα τιμών plaintexts τα $\{(0, 13), \cdots, (12, 25)\}$.

d=2 Για να είναι $\gcd(x-y, 26) = 2$ πρέπει $x-y$ άρτιος. Επίσης αρκεί $x-y$ άρτιος, διότι τότε $\gcd(x-y, 26) \in \{2, 13, 26\}$ αλλά το 26 δείξαμε πριν αδύνατο.

Ο $x-y$ είναι άρτιος αν και μόνο αν οι x, y είναι και οι δύο άρτιοι ή και οι δύο είναι περιττοί. Άρα είτε όλα τα plaintexts είναι άρτια είτε όλα είναι περιττά.

Στο $\{0 \cdots 25\}$ υπάρχουν 13 άρτιοι και 13 περιττοί. Άρα τέτοια υποσύνολα υπάρχουν μόνο για $n <= 13$! Για $n \leq 13$ υπάρχουν $2 \cdot \binom{13}{n}$ υποσύνολα του $\{0 \cdots 25\}$ τέτοια ώστε οι αριθμοί του να είναι όλοι άρτιοι ή όλοι περιττοί.

Αρχικά, συμπεραίνουμε ότι για **για $n \geq 14$ ζεύγη είναι σίγουρο ότι θα βρούμε τουλάχιστον δύο διαφορές που να δώσουν διαφορετικό GCD, οπότε η λύση με το Κινεζικό Θεώρημα Υπολοίπων θα λειτουργήσει**

Ας δούμε όμως και για $n \leq 13$.

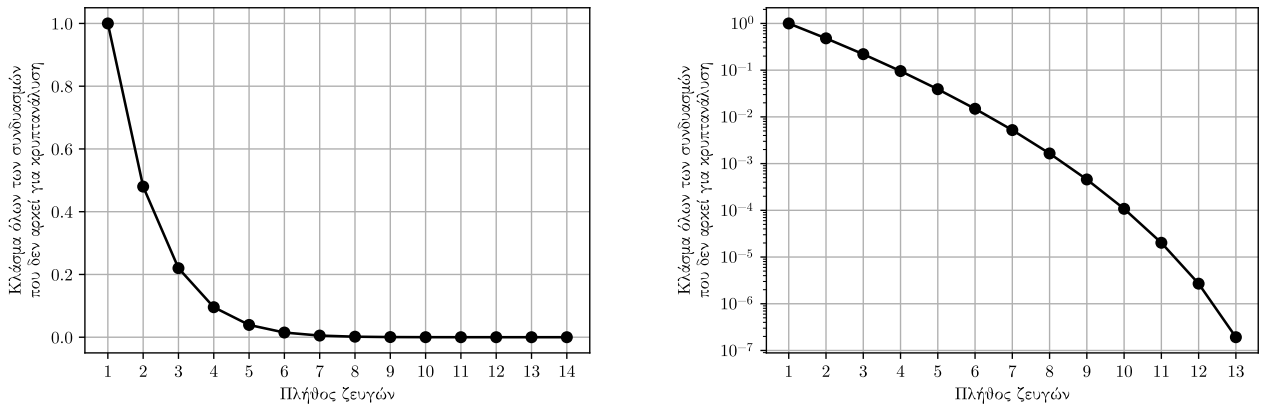
Από όλους τους $\binom{26}{n}$ συνδυασμούς που μπορούν να μας δοθούν, αδυνατούμε να λύσουμε μόνο πλήθος συνδυασμών:

$$2 \cdot \binom{13}{k} + \begin{cases} 13 & n = 2 \\ 0 & n = 0 \end{cases} \tag{1.5}$$

Το ποσοστό των συνδυασμών (ως κλάσμα) που δεν μπορούμε να λύσουμε για τις διάφορες τιμές του n φαίνεται στον πίνακα 1 και στο γράφημα του σχήματος 1.

n	Κλάσμα συνδυασμών ζευγών που δεν κρυπταναλύονται
1	1.0000
2	0.4800
3	0.2200
4	0.0957
5	0.0391
6	0.0149
7	0.0052
8	0.0016
9	4.6e-04
10	1.1e-04
11	2.0e-05
12	2.7e-06
13	1.9e-07
14	0.0e+00

Πίνακας 1: Affine Cipher: Κλάσμα όλων των συνδυασμών ζευγών (plaintext, ciphertext) που δεν αρκούν για κρυπτανάλυση για τα διάφορα πλήθη n των ζευγών



(α′) Γραμμική κλίμακα

(β′) Λογαριθμική κλίμακα

Σχήμα 1: Affine Cipher: Κλάσμα όλων των συνδυασμών ζευγών (plaintext, ciphertext) που δεν αρκούν για κρυπτανάλυση για τα διάφορα πλήθη n των ζευγών

1.3 Ερώτημα β: Διπλή Κρυπτογράφηση

Μελετάμε την ασφάλεια διπλής κρυπτογράφησης με διαφορετικά κλειδιά, δηλαδή:

$$ENC'(((a_1, b_1), (a_2, b_2)), m) = ENC((a_2, b_2), ENC((a_1, b_1), m)) \tag{1.6}$$

Για plaintext x λαμβάνουμε από το 1ο επίπεδο κρυπτογράφησης:

$$y_1 \equiv a_1 x + b_1 \mod 26 \tag{1.7}$$

Για plaintext y_1 λαμβάνουμε από το 2ο επίπεδο κρυπτογράφησης:

$$y_2 \equiv a_2 y_1 + b_2 \mod 26 \equiv a_2 a_1 x + a_2 b_1 + b_1 \mod 26 \tag{1.8}$$

Έστω το κλειδί:

$$(a', b') = (a_2 a_1, a_2 b_1 + b_1) \tag{1.9}$$

Είναι τότε: $y_2 \equiv a'x + b' \mod 26$, οπότε:

$$ENC'(((a_1, b_1), (a_2, b_2)), m) = ENC((a', b'), m) \tag{1.10}$$

Άρα ένας κακόβουλος χρήστης μπορεί απλά να αναζητήσει το κλειδί (a', b') σαν να ήταν το απλό Affine Cipher και να αποκρυπτογραφήσει με αυτό το κλειδί το κείμενο. Όλες οι τακτικές κρυπτανάλυσης που μπορεί να υπάρχουν για το απλό Affine Cipher εφαρμόζουν συνεπώς αυτούσιες και στο διπλό Affine Cipher, συμπεριλαμβανομένης και της εξαντλητικής αναζήτησης.

TL;DR δεν κερδίσαμε σε ασφάλεια.

2 Άσκηση 2: Κρυπτανάλυση συστήματος Vigenere σε ciphertext-only attack

2.1 Εύρεση μήκους κλειδιού

Χρησιμοποιήθηκε ο έλεγχος Index of Coincidence για τον υπολογισμό των πιθανότερων μηκών κλειδιού.

Πιο συγκεκριμένα έστω μια συμβολοσειρά N χαρακτήρων και έστω ότι ο i-οστός χαρακτήρας του αλφαβήτου εμφανίζεται f_i φορές. Αν επιλέξουμε τυχαία δύο διαφορετικούς χαρακτήρες, η πιθανότητα να είναι ίδιοι είναι (επιλέγω έναν χαρακτήρα με f_i επιλογές και μετά τον επιλέγω ξανά με $f_i - 1$ επιλογές):

$$IC = \sum_{i=1}^{26} \frac{f_i \cdot (f_i - 1)}{N \cdot (N-1)} \tag{2.1}$$

Αν θεωρήσουμε p_i την πιθανότητα του i-οστού συμβόλου, στην μέση περίπτωση (αν οι χαρακτήρες επιλέγονται ανεξάρτητα) θα έχουμε $f_i = N \cdot p_i$.

Συνεπώς:

$$\bar{IC} = \sum_{i=1}^{26} \frac{Np_i \cdot (Np_i - 1)}{N \cdot (N-1)} = \frac{N}{N-1} \sum_{i=1}^{26} p_i^2 - \frac{1}{N-1} \approx \sum_{i=1}^{26} p_i^2 \tag{2.2}$$

Η τιμή $\sum_{i=1}^{26} p_i^2$ υπολογίστηκε, με βάση την κατανομή χαρακτήρων σε αγγλικό κειμένων[1], σε 0.0655.

Έτσι, για αν βρούμε το μήκος κλειδιού, δοκιμάζουμε τα μήκη κλειδιών του $\{1 \cdots \text{άνω φράγμα}\}$, υπολογίζουμε τις παραπάνω εκφράσεις, και επιλέγουμε την τιμή κλειδιού που δίνει την ελάχιστη (απόλυτη τιμή) διαφοράς αυτών.

Σχετικά με το άνω φράγμα αναζήτησης, όσο το κλειδί πλησιάζει το μέγεθος του κειμένου, το κρυπτοσύστημα τείνει προς το one-time pad, οπότε είναι λογικό ότι δυσκολεύει η κρυπτανάλυση. Πιο συγκεκριμένα, η στατιστική ανάλυση που εκτελούμε, δεν θα μπορεί να λειτουργήσει λόγω μη ικανοποιητικού δείγματος. Το άνω φράγμα, τίθεται προκειμένου να μπορούμε να πάρουμε ένα ικανοποιητικό δείγμα όλων των χαρακτήρων. Έτσι θέτουμε άνω φράγμα αναζήτησης το $\left\lceil \frac{\text{μήκος κειμένου}}{30} \right\rceil$.

2.2 Εύρεση κλειδιού, δεδομένου του μήκους του

Με δεδομένο το μήκος κλειδιού, για κάθε σύνολο χαρακτήρων που κρυπτογραφείται με το ίδιο shift, έχουμε πρακτικά κρυπτογράφηση τύπου Καίσαρα. Εκτελέστηκε στατιστική ανάλυση για την εύρεση του shift. Πιο συγκεκριμένα υπολογίστηκε αρχικά η κατανομή χαρακτήρων στο κρυπτοκείμενο. Έπειτα, για όλα τα 26 shifts, έγιναν αντίστοιχα 26 κυκλικά shifts της κατανομής χαρακτήρων. Υπολογίστηκε για κάθε μία κατανομή η απόσταση Kullback-Leibler από την γνωστή κατανομή των λατινικών χαρακτήρων στην αγγλική γλώσσα. Επιλέχθηκε το shift που δίνει ελάχιστη τέτοια απόσταση. Για γνωστή κατανομή P (εδώ η κατανομή χαρακτήρων της Αγγλικής Γλώσσας) η απόσταση Kullback-Leibler δίνεται από την σχέση:

$$D_{\mathrm{KL}}(P \parallel Q) = \sum_{x \in \mathcal{X}} P(x) \ \log\left(\frac{P(x)}{Q(x)}\right) \tag{2.3}$$

2.3 Προγραμματιστική Υλοποίηση

Η υλοποίηση έγινε στην συναρτησιακή γλώσσα προγραμματισμού **Haskell**. Έγινε profiling χρονικών επιδόσεων του κώδικα, και βρέθηκε πως ο υπολογισμός των "στηλών" ήταν σημαντικό σημείο καθυστέρησης. Έτσι το σημείο αυτό έχει βελτιστοποιηθεί με χρήση του "προστακτικού" ST monad.

Το κρυπτοσύστημα Vigenere γενικά έχει οριστεί για λατινικό αλφάβητο και όχι για κενά, σημεία στίξης, κ.λπ. Έτσι εκτελούμε όλη την ανάλυση παραλείποντας τους χαρακτήρες αυτούς, και έπειτα απλά τους προσθέτουμε στο κείμενο εκ νέου.

Δίνεται ο κώδικας Haskell παρακάτω:

```
1 import Data.Char (chr, isAlpha, ord)
2 import Data.List (group, minimumBy, sort, sortBy, transpose)
3 import Data.Ord (comparing)
```

[1] https://en.wikipedia.org/wiki/Letter_frequency

```haskell

import Control.Monad
import Control.Monad.ST
import qualified Data.Vector as V
import qualified Data.Vector.Mutable as MV

import Text.Printf (printf)

english_props :: [Double]
english_props =
  [ 0.08167082
  , 0.01492015
  , 0.02782028
  , 0.04253043
  , 0.12702127
  , 0.02228022
  , 0.0201502
  , 0.06094061
  , 0.0696607
  , 0.00153002
  , 0.00772008
  , 0.0402504
  , 0.02406024
  , 0.06749067
  , 0.07507075
  , 0.01929019
  , 0.00095001
  , 0.0598706
  , 0.06327063
  , 0.09056091
  , 0.02758028
  , 0.0097801
  , 0.02360024
  , 0.00150002
  , 0.0197402
  , 0.00074001
  ]

calc_freqs :: String -> [Int]
calc_freqs s =
  let counts =
        map (\xs -> (ord (head xs) - ord 'a', length xs)) $ group (sort s)
      go [] n = repeat 0
      go l@((i, val):xs) n
        | n < i = 0 : go l (n + 1)
        | otherwise = val : go xs (n + 1)
   in take 26 $ go counts 0

calc_props :: String -> [Double]
calc_props s =
  let freqs = calc_freqs s
   in map (\x -> fromIntegral x / fromIntegral (sum freqs)) freqs

smoothing :: Double
smoothing = 1e-10

distribution_dist :: [Double] -> [Double] -> Double
{-kl_div ps qs =
        let qs_smooth = map (max smoothing) qs
        in
        sum $ map (\(p,q) -> p * log (p/q)) $ zip ps qs_smooth
```

```haskell
-}
distribution_dist expected observed =
  foldl' (+) 0 $ zipWith metric expected observed
  where
    metric e o = e * log (e / (max o smoothing))

ceasar :: String -> (Char, String)
ceasar cipher =
  let props = calc_props cipher
      shifts = take 26 (iterate (\(x:xs) -> xs ++ [x]) props)
      offset =
        snd
          $ minimumBy
              (comparing (\(qs, _) -> distribution_dist english_props qs))
          $ zip shifts [0 ..]
   in ( chr (ord 'a' + offset)
      , map
          (\c ->
             if isAlpha c
               then (chr $ (ord c - ord 'a' - offset) `mod` 26 + ord 'a')
               else c)
          cipher)

ic :: String -> Double
ic s =
  fromIntegral (sum $ map (\f -> f * (f - 1)) (calc_freqs s))
    / fromIntegral (length s * (length s + 1))

strips :: [a] -> Int -> [[a]]
--strips l k  = [ [x | (x,i) <- zip l [0..], i `mod` k == j] | j <- [0..k-1] ]
strips l k =
  runST $ do
    vec <- MV.replicate k id
    let go [] _ = return ()
        go (x:xs) i = do
          let idx = i `mod` k
          currDList <- MV.read vec idx
          MV.write vec idx (currDList . (x :))
          go xs (i + 1)
    go l 0
    frozenVec <- V.freeze vec
    return $ map ($ []) (V.toList frozenVec)

try_keylen :: String -> Int -> Double
try_keylen s k =
  let cols = strips s k
      ave_ic = (sum (map ic cols)) / (fromIntegral k)
      len = fromIntegral $ length s
   in abs (ave_ic - 0.0655)

vigenere_keylens :: String -> Int -> [Int]
vigenere_keylens s ub = sortBy (comparing (try_keylen s)) [1 .. ub]

decrypt_vigenere :: String -> Int -> (String, String)
decrypt_vigenere s keylen =
  let cols = strips s keylen
      plain_key = map ceasar cols
      plain = concat $ transpose $ map snd plain_key
      key = map fst plain_key
   in (key, plain)

```

```haskell
reconstruct :: String -> String -> String
reconstruct (c:cs) ps
  | not (isAlpha c) = c : (reconstruct cs ps)
reconstruct (_:cs) (p:ps) = p : (reconstruct cs ps)
reconstruct _ _ = []

main :: IO ()
main = do
  cipher <- getContents
  let cipher' = filter isAlpha cipher
      keylens = take 5 $ vigenere_keylens cipher' (length cipher' `div` 30)
      plains = [decrypt_vigenere cipher' keylen | keylen <- keylens]
      printResult (key, plain) = do
        putStrLn
          $ key
              ++ " "
              ++ reconstruct cipher plain
              ++ " "
              ++ (printf "%.4f" (ic plain))
  mapM_ printResult plains
```

Για την μεταγλώττιση, θα χρειαστεί η εγκατάσταση της βιβλιοθήκης Vector.

Παρατίθεται το αρχείο `vigenere.cabal` για να διευκολυνθεί η μεταγλώττιση από τον αναγνώστη:

```
cabal-version:      3.0
name:               vigenere
version:            0.1.0.0
license:            GPL-3.0-only
license-file:       LICENSE
author:             Andreas Stamos
maintainer:         stamos.aa@gmail.com
build-type:         Simple
extra-doc-files:    CHANGELOG.md

common warnings
    ghc-options: -Wall

executable vigenere
    import:           warnings
    main-is:          Main.hs
    build-depends:    base ^>=4.20.0.0, vector
    hs-source-dirs:   app
    default-language: Haskell2010
    ghc-prof-options: -fprof-auto -rtsopts

```

2.4 Αποτελέσματα εξόδου

Παραθέτουμε μόνο το πιθανότερο αποτέλεσμα εξόδου (για λόγους συντομίας). Η εκτέλεση του προγράμματος δίνει και τα 5 πιθανότερα αποτελέσματα, όπως ζητείται.

Το κλειδί βρέθηκε: `ietzschenietzschen`

Το αποκρυπτογράφημενο κείμενο (plain text) βρέθηκε:

```
hen zarathustra was thirty years old, he left his home and the lake of his home, and went into
the mountains. there he enjoyed his spirit and solitude, and for ten years did not weary of
it. but at last his heart changed,-and rising one morning with the rosy dawn, he went before
the sun, and spake thus unto it: thou great star! what would be thy happiness if thou hadst
not those for whom thou shinest! for ten years hast thou climbed hither unto my cave: thou
wouldst have wearied of thy light and of the journey, had it not been for me, mine eagle,
and my serpent. but we awaited thee every morning, took from thee thine overflow and blessed
thee for it. lo! i am weary of my wisdom, like the bee that hath gathered too much honey; i
```

need hands outstretched to take it. i would fain bestow and distribute, until the wise have once more become joyous in their folly, and the poor happy in their riches. therefore must i descend into the deep: as thou doest in the evening, when thou goest behind the sea, and givest light also to the nether-world, thou exuberant star! like thee must i go down, as men say, to whom i shall descend. bless me, then, thou tranquil eye, that canst behold even the greatest happiness without envy! bless the cup that is about to overflow, that the water may flow golden out of it, and carry everywhere the reflection of thy bliss! lo! this cup is again going to empty itself, and zarathustra is again going to be a man. thus began zarathustra's down-going

Ο δείκτης σύμπτωσης του plain text υπολογίστηκε: 0.0692.

3 Άσκηση 3: Ιδιότητες τέλειας μυστικότητας

3.1 Ισοπίθανα κλειδιά

Αν οι χώροι κλειδιών, μηνυμάτων και κρυπτοκειμένων είναι ισοπληθείς, τότε από το Θεώρημα που υπάρχει στις διαφάνειες πρέπει όλα τα κλειδιά να είναι ισοπίθανα για να έχουμε τέλεια μυστικότητα.

Όμως, μπορούν οι χώροι αυτοί να είναι ανισοπληθείς μεταξύ τους (φυσικά τηρώντας το $\mathcal{M} \leq \mathcal{K} \leq \mathcal{C}$) και τα κλειδιά να μην είναι ισοπίθανα, όμως να έχουμε τέλεια μυστικότητα.

Παρουσιάζουμε παράδειγμα ύπαρξης. Δίνουμε μια παραλλαγή του one-time pad.

Πιο συγκεκριμένα, έστω:

- $\mathcal{M} = \{0,1\}^N$
- $\mathcal{K} = \{0,1,2\}^N$
- $\mathcal{C} = \{0,1,2,3\}^N$
- $y_i = ENC_k(x_i) = (x_i + k_i \mod 2) \mid \text{NonDeterministic}(0,2)$
- $x_i = DEC_k(y_i) = y_i + k_i \mod 2$

Όπου NonDeterministic$(0,2)$ θεωρούμε μια επιλογή μεταξύ των αριθμών 0, 2 που αποτιμάται αυθαιρέτως σε οποιαδήποτε τιμή.

(το $\mid$ σημαίνει bitwise or)

Θεωρούμε $p_k(0) = 0.25$, $p_k(1) = 0.5$, $p_k(2) = 0.25$.

Με άλλα λόγια, έχουμε προσθέσει στο κλειδί ένα δεύτερο bit που η συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης απλά απορρίπτουν.

Επίσης, έχουμε προσθέσει σε κάθε σύμβολο κρυπτοκειμένου ένα ακόμα bit που επίσης απορρίπτεται στην αποκρυπτογράφηση.

Αυτά ισχύουν διότι γενικά αν $a = a_1 \cdot 2 + a_0$ και $b = b_1 \cdot 2 + b_0$ τότε $a + b \equiv a_0 + b_0 \mod 2$.

Με άλλα λόγια, το σύστημα είναι ισοδύναμο με το κλασικό one-time pad (που δουλεύει bit-bit) αν θεωρήσουμε το LSB bit όλων των συμβόλων.

Πράγματι, $p_k(LSB = 0) = p_k(0) = p_k(2) = 0.5$ και $p_k(LSB = 1) = p_k(1) = 0.5$.

Αν και η απόδειξη αυτή θεωρούμε επαρκεί παρέχουμε και μια σύντομη απόδειξη με βάση τον ορισμό της τέλειας μυστικότητας.

Ισχύει λόγω των προηγούμενων ότι $\mathbb{P}[M = x|C = 3] = \mathbb{P}[M = x|C = 1]$ και $\mathbb{P}[M = x|C = 2] = \mathbb{P}[M = x|C = 0]$. Όμως επειδή $x = (y\&1) \oplus (k\&1)$ και επειδή, όμως δείξαμε πριν οι (δύο) τιμές του $k\&1$ είναι ισοπίθανες, τότε για δεδομένο $y\&1$ τα x είναι ισοπίθανα. Με άλλα λόγια $\mathbb{P}[M = x|C = y] = \mathbb{P}[M = x]$ είτε $y\&1 = 0$ είτε $y\&1 = 0$. Άρα το σύστημα έχει τέλεια μυστικότητα.

3.2 Ισοδύναμες συνθήκες Τέλειας Μυστικότητας

Επαναλαμβάνουμε τον ορισμό της Τέλειας Μυστικότητας για λόγους πληρότητας.

Ορισμός 3.1. *Έστω $\mathcal{M}$ το σύνολο των μηνυμάτων και $\mathcal{C}$ το σύνολο των κρυπτοκειμένων.*

Έστω τυχαίες μεταβλητές M, C που αναπαριστούν το μήνυμα και το κρυπτοκείμενο.

Έστω $\mathcal{K}$ το σύνολο των κλειδιών και έστω επιπλέον K τυχαία μεταβλητή που αναπαριστά το κλειδί.

Οι τυχαίες μεταβλητές M, C, K, από τον ορισμό του κρυπτοσυστήματος, πρέπει να ικανοποιούν την σχέση:

$$C = Enc_K(M) \tag{3.1}$$

Ορισμός 3.2. *Ένα σύστημα κρυπτογράφησης λέγεται τέλεια μυστικό αν για κάθε κατανομή πιθανότητας πάνω στο σύνολο $\mathcal{M}$, για κάθε στοιχείο $m \in \mathcal{M}$ και για κάθε στοιχείο $c \in \mathcal{C}$, τέτοιο ώστε $\mathbb{P}[C = c] > 0$, ισχύει ότι:*

$$\mathbb{P}[M = m|C = c] = \mathbb{P}[M = m] \tag{3.2}$$

Θα αποδείξουμε το παρακάτω θεώρημα (**ερώτημα i της εκφώνησης**).

Θεώρημα 3.1. *Ένα κρυπτοσύστημα είναι τέλεια μυστικό αν και μόνο αν για κάθε $x \in \mathcal{M}$, με $\mathbb{P}[x] > 0$ και για κάθε $y \in \mathcal{C}$ ισχύει ότι:*

$$\mathbb{P}[C = y] = \mathbb{P}[C = y | M = x] \tag{3.3}$$

Η υπόθεση $\mathbb{P}[x] > 0$ απαιτείται ώστε η δεσμευμένη πιθανότητα να είναι ορισμένη.

Απόδειξη. Αρχικά δείχνουμε ότι αν το κρυπτοσύστημα είναι τέλεια ασφαλές, τότε ισχύει η παραπάνω σχέση.

Έστω στοιχείο $m \in \mathcal{M}$. Είναι:

$$\mathbb{P}[C = y|M = x] \cdot \mathbb{P}[M = x] = \mathbb{P}[M = x|C = y] \cdot \mathbb{P}[C = y] \overset{\text{τέλεια ασφάλεια}}{=} \mathbb{P}[M = x] \cdot \mathbb{P}[C = y] \overset{\mathbb{P}[M=x]>0}{\Rightarrow} \mathbb{P}[C = y|M = x] = \mathbb{P}[C = y]$$

Αντίστροφα, έστω ότι ισχύει η παραπάνω σχέση. Θα δείξουμε ότι το σύστημα είναι τέλεια ασφαλές.

Διακρίνουμε περιπτώσεις.

Αν $\mathbb{P}[M = x] = 0$ τότε ισχύει άμεσα ότι $0 = \mathbb{P}[M = x] = \mathbb{P}[M = x|C = y]$.

Αν $\mathbb{P}[M = x] > 0$ τότε ισχύει η σχέση της υπόθεσης.

Η τέλεια ασφάλεια ορίζεται αν $\mathbb{P}[C = y] > 0$, οπότε το υποθέτουμε.

Τότε:

$$\mathbb{P}[M = x|C = y] \cdot \mathbb{P}[C = y] \overset{\mathbb{P}[M=x]>0}{=} \mathbb{P}[C = y|M = x] \cdot \mathbb{P}[M = x] = \mathbb{P}[C = y] \cdot \mathbb{P}[M = x] \overset{\mathbb{P}[C=y]>0}{\Rightarrow} \mathbb{P}[M = x|C = y] = \mathbb{P}[M = x]$$

Άρα το σύστημα είναι τέλεια ασφαλές. □

Θα αποδείξουμε το παρακάτω θεώρημα (**ερώτημα ii της εκφώνησης**).

Θεώρημα 3.2. *Ένα κρυπτοσύστημα είναι τέλεια μυστικό αν και μόνο αν για κάθε $x_1, x_2 \in \mathcal{M}$, με $\mathbb{P}[M = x_1] > 0$, $\mathbb{P}[M = x_2] > 0$, για κάθε $y \in \mathcal{C}$ ισχύει ότι:*

$$\mathbb{P}[C = y|M = x_1] = \mathbb{P}[C = y|M = x_2] \tag{3.4}$$

Η υπόθεση $\mathbb{P}[M = x_1] > 0$, $\mathbb{P}[M = x_2] > 0$ απαιτείται ώστε η δεσμευμένη πιθανότητα να είναι ορισμένη.

Απόδειξη. Αρχικά δείχνουμε ότι αν το κρυπτοσύστημα είναι τέλεια ασφαλές, τότε ισχύει η παραπάνω σχέση.

Από το θεώρημα 3.1 λαμβάνουμε:

$$\begin{aligned} \mathbb{P}[C = y] &= \mathbb{P}[C = y|M = x_1] \\ \mathbb{P}[C = y] &= \mathbb{P}[C = y|M = x_2] \end{aligned} \tag{3.5}$$

Συνεπώς ισχύει ότι: $Pr[C = y|M = x_1] = Pr[C = y|M = x_2]$.

Αντίστροφα, έστω ότι ισχύει η παραπάνω σχέση.

Διακρίνουμε περιπτώσεις.

Αν $\mathbb{P}[M = x] = 0$ τότε ισχύει άμεσα ότι $0 = \mathbb{P}[M = x] = \mathbb{P}[M = x|C = y]$.

Αν $\mathbb{P}[M = x] > 0$.

Έστω ένα στοιχείο $x_0 \in \mathcal{M}$. Ισχύει ότι:

$$\mathbb{P}[C = y] = \sum_{x' \in \mathcal{M}, \mathbb{P}[M=x']>0} \mathbb{P}[C = y|M = x'] \cdot \mathbb{P}[M = x'] = \sum_{x' \in \mathcal{M}, \mathbb{P}[M=x']>0} \mathbb{P}[C = y|M = x_0] \cdot \mathbb{P}[M = x'] = \mathbb{P}[C = y|M = x_0] \cdot \sum_{x' \in \mathcal{M}, \mathbb{P}[M=x']>0} \mathbb{P}[M = x'] = \mathbb{P}[C = y|M = x_0] \cdot 1 = \mathbb{P}[C = y|M = x]$$

Από το θεώρημα 3.1 λαμβάνουμε ότι το σύστημα είναι τέλεια ασφαλές. □

4 Άσκηση 4: Πειραγμένο One-Time Pad

Υποθέτουμε τροποποιημένη εκδοχή του One-Time Pad ώστε: $\mathcal{K} = 0, 1^\lambda \setminus 0^\lambda$ και υποθέτουμε ότι η τυχαία μεταβλητή K έχει κατανομή ομοιόμορφη πάνω σε αυτό το $\mathcal{K}$.

Είναι: $|\mathcal{K}| = 2^\lambda - 1 < 2^\lambda = |\mathcal{M}|$. Συνεπώς το σύστημα δεν είναι τέλεια ασφαλές.

Το τελευταίο βασίζεται στο παρακάτω γνωστό θεώρημα, που αποδεικνύουμε ξανά για λόγους πληρότητας.

Θεώρημα 4.1. *Αν ένα κρυπτοσύστημα είναι τέλεια ασφαλές, τότε* $|\mathcal{K}| \geq |\mathcal{M}|$.

Απόδειξη. Έστω ότι $|\mathcal{K}| < |\mathcal{M}|$.

Έστω ένα κρυπτοκείμενο $c \in \mathcal{C}$.

Έστω το σύνολο $A(c) = \{m \in \mathcal{M} \mid \exists k \in \mathcal{K},\ c = Enc_k(m)\}$.

Είναι $|A(c)| \leq |\mathcal{K}|$.

Αφού $|K| < |\mathcal{M}|$ τότε $|A(c)| < |\mathcal{M}|$.

Συνεπώς υπάρχει ένα στοιχείο $m \in \mathcal{M}$ τέτοιο ώστε $m \notin A(c)$.

Υποθέτω μια κατανομή πιθανότητας στο $\mathcal{M}$ που δίνει $\mathbb{P}[M = m] > 0$.

Τότε $\mathbb{P}[M = m|C = y] = 0$, αλλά $\mathbb{P}[M = m] > 0$.

Αν το σύστημα είναι τέλεια ασφαλές, θα ίσχυε $\mathbb{P}[M = m|C = y] = \mathbb{P}[M = m]$ για κάθε κατανομή πιθανότητας στο $\mathcal{M}$, οπότε και αυτή που ορίσαμε. Άτοπο.

Άρα $|\mathcal{K}| \geq |\mathcal{M}|$. □

5 Άσκηση 5: Πολλαπλασιαστικό One-Time Pad

Ορισμός 5.1 (Πολλαπλασιαστικό One-Time Pad)**.** *Έστω ένας πρώτος αριθμός p.*

Έστω:

$$\begin{gathered}\mathcal{M} = \mathcal{K} = \mathcal{C} = \mathbb{Z}_p^* = 1, \cdots, p-1 \\ Enc_k(m) = (k \cdot m) \mod p\end{gathered} \tag{5.1}$$

Αρχικά επειδή το $\mathbb{Z}_p^*$ είναι ομάδα ισχύει ότι

$$Enc_k(m) = (k \cdot m) \mod p \in \mathcal{C} = \mathbb{Z}_p^*$$

.

Αφού $k \in \mathbb{Z}_p^*$ ορίζεται ο πολλαπλασιαστικός του αντίστροφος k^{-1}.

Ορίζεται τότε η **συνάρτηση αποκρυπτογράφησης**:

$$Dec_k(c) = k^{-1} \cdot y \mod p \tag{5.2}$$

Ισχύει ότι:

$$Dec_k(Enc_k(m)) = k^{-1} \cdot k \cdot m \mod p = m \mod p = m$$

Συνεπώς το σύστημα κρυπτογράφησης είναι **ορθό**, δηλαδή η αποκρυπτογράφηση ενός κρυπτογραφημένου μηνύματος δίνει το αρχικό μήνυμα για κάθε αρχικό μήνυμα.

Το σύστημα είναι τέλεια ασφαλές, επειδή η ομάδα $(\mathbb{Z}_p^*, *)$ είναι ισομορφική με την ομάδα $(\mathrm{Z}_{p-1}, +)$. Το αποδεικνύουμε ακριβέστερα.

Αρχικά αποδεικνύουμε το παρακάτω λήμμα.

Λήμμα 5.1. *Ένα σύστημα είναι τέλεια ασφαλές αν και μόνο αν για κάθε $m_1, m_2 \in \mathcal{M}$ και για κάθε $c \in \mathcal{C}$ ισχύει ότι:*

$$\mathbb{P}[c = Enc_K(m_1)] = \mathbb{P}[c = Enc_K(m_2)]. \tag{5.3}$$

υπενθυμίζεται ότι το K έχει οριστεί ως τυχαία μεταβλητή

Απόδειξη. Για κάθε $m \in \mathcal{M}$ ισχύει ότι:

$$\mathbb{P}[C = c | M = m] = \mathbb{P}[Enc_K(M) = c | M = m] = \mathbb{P}[Enc_K(m) = c | M = m] \overset{K, M \text{ανεξάρτητες}}{=} \mathbb{P}[[]Enc_K(m) = c] \tag{5.4}$$

Συνεπώς ισχύει:

$$\mathbb{P}[c = Enc_K(m_1)] = \mathbb{P}[c = Enc_K(m_2)] \iff \mathbb{P}[C = c | M = m_1] = \mathbb{P}[C = c | M = m_2] \tag{5.5}$$

Συνεπώς από το θεώρημα 3.2 ισχύει ότι η σχέση του λήμματος είναι ισοδύναμη με τέλεια ασφάλεια. □

Αποδεικνύουμε τώρα ότι **Πολλαπλασιαστικό One-Time Pad είναι τέλεια ασφαλές**.

Θεώρημα 5.1. *Το Πολλαπλασιαστικό One-Time Pad είναι τέλεια ασφαλές.*

Απόδειξη. Αφού η $(\mathbb{Z}_p^*, \otimes)$ είναι ισομορφική με την $(\mathbb{Z}_{p-1}, \oplus)$ έστω $\phi : \mathbb{Z}_{p-1} \mapsto \mathbb{Z}_p^*$ ένας ισομορφισμός τους.

Ισχύει δηλαδή για κάθε για κάθε $a, b \in \mathbb{Z}_{p-1}$:

$$\phi(a \oplus b) = \phi(a) \otimes \phi(b)$$

Ορίζουμε τον εξής συμβολισμό για λόγους απλότητας. Για κάθε σύμβολο S, το S' ορίζεται ως $\phi^{-1}(S)$.

Τότε στο Πολλαπλασιαστικό One-Time Pad, για κάθε $m \in \mathcal{M}$ και για κάθε $c \in C$:

$$\begin{gathered}\mathbb{P}[c = Enc_K(m)] = \mathbb{P}[c = m_1 \otimes K] = \\ \mathbb{P}[\phi(c') = \phi(m') \otimes \phi(K')] = \mathbb{P}[\phi(c') = \phi(m' \oplus K')] = \\ \mathbb{P}[c' = m' \oplus K'] = \mathbb{P}[c' = Enc^+_{K'} m']\end{gathered} \tag{5.6}$$

όπου Enc^+ συμβολίζουμε την συνάρτηση κρυπτογράφησης του προσθετικού One-Time Pad.

Έστω $m_1, m_2 \in \mathcal{M}$ και $c \in \mathcal{C}$.

Κατά τα γνωστά το προσθετικό One-Time Pad είναι τέλεια ασφαλές.

Συνεπώς από το λήμμα 5.1:

$$\mathbb{P}[c' = Enc^{+}_{K'}(m'_1)] = \mathbb{P}[c' = Enc^{+}_{K'}(m'_2)]$$

Τότε:

$$\mathbb{P}[c = Enc_K(m_1)] \overset{\text{σχέση } 5.6}{=} \mathbb{P}[c' = Enc^{+}_{K'}(m'_1)] = \mathbb{P}[c' = Enc^{+}_{K'}(m'_2)] \overset{\text{σχέση } 5.6}{=} \mathbb{P}[c = Enc_K(m_2)]$$

Συνεπώς από το λήμμα 5.1 το Πολλαπλασιαστικό One-Time Pad είναι τέλεια ασφαλές. □

6 Άσκηση 6: Ιδιότητες πρώτων

6.1 Ερώτημα 1: Αν $2^n - 1$ πρώτος, τότε n πρώτος

Θεώρημα 6.1. *Έστω $n \in \mathbb{N}$. Αν ο αριθμός $2^n - 1$ είναι πρώτος, τότε ο n είναι πρώτος.*

Απόδειξη. Έστω ότι ο n είναι σύνθετος. Τότε υπάρχουν $a \geq 2$, $b \geq 2$ ώστε $n = a \cdot b$.

Τότε:

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1) \cdot ((2^a)^{b-1} + (2^a)^{b-2} + \cdots 1)$$

Είναι: $a \geq 2 \Rightarrow 2^a - 1 \geq 3$. Επίσης επειδή $2^a > 1$ και $b > 1$ είναι $2^a < (2^a)^b \Rightarrow 2^a - 1 < 2^n - 1$.

Άρα βρήκαμε παράγοντα του $2^n - 1$ που είναι διάφορος του 1 και του $2^n - 1$, οπότε ο $2^n - 1$ δεν είναι πρώτος. Άτοπο. □

6.2 Ερώτημα 2: Αριθμοί $2^p - 1$

6.2.1 Ερώτημα i

Θεώρημα 6.2. *Έστω ένας περιττός πρώτος αριθμός p και $M_p = 2^p - 1$.*

Ισχύει ότι: $M_p \equiv 1 \mod p$

Απόδειξη. Το 2 είναι σχετικά πρώτο με τον πρώτο p, αφού ο p περιττός (δηλαδή αφού $p \neq 2$).

Τότε από Μικρό Θεώρημα Fermat: $2^{p-1} \equiv 1 \mod p$.

Άρα:

$$M_p \equiv 2^p - 1 \equiv 2 \cdot 2^{p-1} - 1 \equiv 2 \cdot 1 - 1 \equiv 1 \mod p$$

□

6.2.2 Ερώτημα ii

Θεώρημα 6.3. *Έστω ένας περιττός πρώτος αριθμός p και $M_p = 2^p - 1$.*

Ισχύει ότι: $p \mid \phi(M_p)$.

Απόδειξη. Ισχύει ότι: $2^p \equiv 1 \mod M_p$.

Άρα: $ord_{M_p}(2) \mid p$.

Όμως ο p είναι πρώτος. Άρα είτε $ord_{M_p}(2) = 1$ είτε $ord_{M_p}(2) = p$.

Αν $ord_{M_p}(2) = 1$, τότε $2 \equiv 1 \mod M_p$, που είναι αδύνατο διότι $p > 2 \Rightarrow M_p = 2^p - 1 > 3 > 1$.

Άρα: $ord_{M_p}(2) = p$.

Από το θεώρημα Lagrange, η τάξη ενός στοιχείου διαιρεί την τάξη της ομάδας. (αναφερόμαστε στην ομάδα $U(\mathbb{Z}_{M_p})$.)

Συνεπώς είναι $ord_{M_p}(2) \mid \phi(M_p)$, οπότε $p \mid \phi(M_p)$. □

6.3 Ερώτημα 3

Θεώρημα 6.4. *Έστω p,q δύο διαφορετικοί πρώτοι. Ισχύει ότι: $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$*

Απόδειξη. Από Μικρό Θεώρημα Fermat ισχύουν:

$$\begin{aligned} q^{p-1} &\equiv 1 \pmod{p} \\ p^{q-1} &\equiv 1 \pmod{q} \end{aligned}$$

Επίσης:

$$\begin{aligned} p^{q-1} &\equiv 0 \pmod{p} \\ q^{p-1} &\equiv 0 \pmod{q} \end{aligned}$$

Άρα:

$$\begin{aligned} p^{q-1} + q^{p-1} &\equiv 1 \pmod{p} \\ p^{q-1} + q^{p-1} &\equiv 1 \pmod{q} \end{aligned} \tag{6.1}$$

Από το Κινέζικο Θεώρημα Υπολοίπων το σύστημα εξισώσεων 6.1 (θεωρώντας το $p^{q-1}+q^{p-1}$ ως άγνωστο) έχει λύση και κάθε λύση είναι ισοϋπόλοιπη ως προς pq.

Όμως το 1 είναι λύση του συστήματος. Επίσης όμως και το $p^{q-1}+q^{p-1}$ είναι λύση του συστήματος.

Άρα είναι: $p^{q-1}+q^{p-1} \equiv 1 \pmod{pq}$. □

6.4 Ερώτημα 4

Θεώρημα 6.5. *Έστω $p > 2$ πρώτος αριθμός. Ισχύει ότι:*

$$\sum_{\beta \in \mathbb{Z}_p^*} \beta = \sum_{\beta \in \mathbb{Z}_p^*} \beta^{-1} \equiv 0 \pmod{p}$$

Απόδειξη. Είναι: $\mathbb{Z}_p^* = 1, \cdots, p-1$.

Άρα:

$$\sum_{\beta \in \mathbb{Z}_p^*} \beta = 1 + \cdots + p - 1 = \frac{(p-1)(p-1+1)}{2} = \frac{p(p-1)}{2}$$

Αφού $p > 2$ τότε p περιττός. Συνεπώς ο $p-1$ είναι άρτιος, οπότε ο $\dfrac{p-1}{2}$ ακέραιος.

Άρα: $\sum\limits_{\beta \in \mathbb{Z}_p^*} \beta = p \cdot \dfrac{p-1}{2}$

Άρα:

$$\sum_{\beta \in \mathbb{Z}_p^*} \beta \equiv 0 \pmod{p}$$

Απομένει να δείξουμε ότι: $\sum\limits_{\beta \in \mathbb{Z}_p^*} \beta = \sum\limits_{\beta \in \mathbb{Z}_p^*} \beta^{-1}$

Πράγματι επειδή το $\mathbb{Z}_p^*$ είναι ομάδα σε κάθε στοιχείο $x \in \mathbb{Z}_p^*$ αντιστοιχεί μοναδικός αντίστροφος $x^{-1} \in \mathbb{Z}_p^*$.

Δύο διαφορετικά στοιχεία δεν μπορούν να έχουν ίδιο αντίστροφο, διότι τότε αυτός ο αντίστροφος θα είχε δύο αντιστρόφους.

Συνεπώς όλα τα β^{-1} είναι διαφορετικά μεταξύ τους, οπότε η απεικόνιση $\beta \mapsto \beta^{-1}$ είναι μια μετάθεση του συνόλου $\mathbb{Z}_p^*$.

Συνεπώς:

$$\sum_{\beta \in \mathbb{Z}_p^*} \beta^{-1} = \sum_{\beta \in \mathbb{Z}_p^*} \beta$$

Τελικά:

$$\sum_{\beta \in \mathbb{Z}_p^*} \beta = \sum_{\beta \in \mathbb{Z}_p^*} \beta^{-1} \equiv 0 \pmod{p}$$

□

6.5 Ερώτημα 5

Θεώρημα 6.6. *Έστω ακέραιος $n > 2$. Ο n είναι πρώτος αν και μόνο αν:*

$$(n-1)! \equiv -1 \pmod{n}$$

Απόδειξη. Έστω ότι ο n είναι πρώτος. Θα δείξουμε ότι ισχύει η σχέση.

Αφού ο n είναι πρώτος ορίζεται η πολλαπλασιαστική ομάδα $\mathbb{Z}_n^*$. Το $(n-1)!$ είναι το γινόμενο όλων των στοιχείων της ομάδας αυτής.

Για κάθε αριθμό $x \in \mathbb{Z}_n^*$ ορίζεται ο $x^{-1} \in \mathbb{Z}_n^*$.

Αν $x = x^{-1} \pmod{n}$ τότε: $x^2 = 1 \pmod{n}$, οπότε επειδή ο n είναι πρώτος ισχύει ότι: $x \equiv \pm 1 \pmod{n}$.

Άρα τα μόνα στοιχεία του $\mathbb{Z}_n^*$ που έχουν αντίστροφο τον εαυτό τους είναι το 1 και το $n-1$.

Συνεπώς στο γινόμενο $(n-1)! = 1 \cdot 2 \cdot ... \cdot (n-2) \cdot (n-1)$, όλοι αριθμοί εκτός του 1 και του $n-1$ έχουν και τον αντίστροφο τους στο γινόμενο αυτό. Επειδή η ομάδα είναι αβελιανή, μπορώ να αναδιατάξω τα στοιχεία στο γινόμενο ώστε όλοι οι αριθμοί να είναι δίπλα με τον αντίστροφό τους, οπότε στο γινόμενο το ζεύγος τους να δίνει $1 \pmod{n}$.

Άρα: $(n-1)! \equiv 1 \cdot (n-1) \pmod{n} = -1 \pmod{n}$.

Αντίστροφα, έστω ότι ισχύει η σχέση. Θα δείξουμε ότι ο n είναι πρώτος.

Έστω ότι ο n είναι σύνθετος. Τότε έχει έναν διαιρέτη d τέτοιο ώστε $2 \leq d \leq n-1$. Ισχύει ότι: $d \equiv 0 \pmod{n}$. Ο διαιρέτης αυτός είναι κάποιο πολλαπλασιαστέος του γινόμενου $(n-1)! = 1 \cdot ... \cdot (n-1)$.

Συνεπώς $(n-1)! \equiv 0 \pmod{n}$ που είναι άτοπο. Άρα ο n είναι πρώτος. □

7 Άσκηση 7: Ιδιότητες αβελιανών ομάδων

7.1 Ερώτημα 1: Τάξη του Γινομένου Στοιχείων σε Πεπερασμένες Αβελιανές Ομάδες

Αποδεικνύουμε το θεώρημα απευθείας για κάθε πεπερασμένη αβελιανή ομάδα G, οπότε ισχύει και την $U(\mathbb{Z}_n)$.

Θεώρημα 7.1. *Έστω πεπερασμένη αβελιανή ομάδα G. Για κάθε $a \in G$, $b \in G$ είναι* $\operatorname{ord}(ab) = \operatorname{ord}(a) \cdot \operatorname{ord}(b)$ *αν και μόνο αν* $\gcd(\operatorname{ord}(a), \operatorname{ord}(b)) = 1$.

Απόδειξη. Αρχικά:

$$(ab)^{\operatorname{lcm}(\operatorname{ord}(a),\operatorname{ord}(b))} \overset{G \text{ αβελιανή}}{=} (a^{\operatorname{ord}(a)})^k b^{\operatorname{ord}(b)})^l = ee = e$$

όπου $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) = k \cdot \operatorname{ord}(a) = l \cdot \operatorname{ord}(b)$.

Άρα:

$$\operatorname{ord}(ab) \mid \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) \tag{7.1}$$

Ισχύει ότι:

$$e = e^{\operatorname{ord}(a)} = \left((ab)^{\operatorname{ord}(ab)}\right)^{\operatorname{ord}(a)} \overset{G \text{ αβελιανή}}{=} a^{\operatorname{ord}(ab)\operatorname{ord}(a)} b^{\operatorname{ord}(ab)\operatorname{ord}(a)} = (a^{\operatorname{ord}(a)})^{\operatorname{ord}(ab)} b^{\operatorname{ord}(ab)\operatorname{ord}(a)} = b^{\operatorname{ord}(ab)\operatorname{ord}(a)}$$

Άρα $\operatorname{ord}(b) \mid \operatorname{ord}(ab)\operatorname{ord}(a)$.

Όμοια λαμβάνουμε ότι $\operatorname{ord}(a) \mid \operatorname{ord}(ab)\operatorname{ord}(b)$.

Έστω ότι $\operatorname{ord}(a)$ και $\operatorname{ord}(b)$ είναι σχετικά πρώτοι. Θα δείξουμε ότι $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$.

Αφού οι $\operatorname{ord}(a)$ και $\operatorname{ord}(b)$ είναι σχετικά πρώτοι και αφού $\operatorname{ord}(b) \mid \operatorname{ord}(ab) \mid \operatorname{ord}(a)$, τότε $\operatorname{ord}(b) \mid \operatorname{ord}(ab)$.

Όμοια $\operatorname{ord}(a) \mid \operatorname{ord}(ab)$,

Συνεπώς $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) \mid \operatorname{ord}(ab)$.

Αφού $\operatorname{ord}(a)$ και $\operatorname{ord}(b)$ είναι σχετικά πρώτοι τότε $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) = \operatorname{ord}(a)\operatorname{ord}(b)$.

Συνεπώς $\operatorname{ord}(a)\operatorname{ord}(b) \mid \operatorname{ord}(ab)$.

Όμως από την σχέση 7.1: $\operatorname{ord}(ab) \mid lcm(\operatorname{ord}(a), \operatorname{ord}(b)) = \operatorname{ord}(a)\operatorname{ord}(b)$.

Άρα: $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$.

Αντίστροφα, έστω ότι $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$. Θα δείξω ότι $\operatorname{ord}(a)$ και $\operatorname{ord}(b)$ είναι σχετικά πρώτοι.

Από την σχέση 7.1 είναι:

$$\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b) \mid \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$$

Αφού $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) \leq \operatorname{ord}(a)\operatorname{ord}(b)$ τότε $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) = \operatorname{ord}(a)\operatorname{ord}(b)$.

Αφού ισχύει η τελευταία σχέση τότε $\operatorname{ord}(a)$ και $\operatorname{ord}(b)$ είναι σχετικά πρώτοι.[2] □

Πόρισμα 7.1. *Έστω $a \in U(\mathbb{Z}_n)$ τάξης k και $b \in U(\mathbb{Z}_n)$ τάξης m. Ο αριθμός ab έχει τάξη nm αν και μόνο αν $gcd(k, m) = 1$.*

Απόδειξη. Η $U(\mathbb{Z}_n)$ είναι μια πεπερασμένη αβελιανή ομάδα. Συνεπώς το συμπέρασμα προκύπτει άμεσα από το θεώρημα 7.1. □

[2] $\operatorname{lcm}(a,b) \cdot \gcd(a,b) = \operatorname{ord}(a)\operatorname{ord}(b) \Rightarrow \gcd(a,b) = 1$

7.2 Ερώτημα 2: Η τάξη ενός στοιχείου διαιρεί την μέγιστη τάξη στοιχείου

Δείχνουμε αρχικά το παρακάτω λήμμα.

Λήμμα 7.1. *Έστω ομάδα G.*

Έστω στοιχείο a με τάξη $\operatorname{ord}(a)$. Για κάθε n, m ώστε $\operatorname{ord}(a) = n \cdot m$ στοιχείο $a' = a^n$ έχει τάξη m.

Απόδειξη. Ισχύει ότι: ${a'}^m = a^{nm} = a^{\operatorname{ord}(a)} = e$.

Άρα $\operatorname{ord}(a') \mid m$.

Επίσης: $a^{n \cdot \operatorname{ord}(a')} = {a'}^{\operatorname{ord}(a')} = e$. Άρα $\operatorname{ord}(a) = (n \cdot m) \mid (n \cdot \operatorname{ord}(a'))$.

Συνεπώς: $m \mid \operatorname{ord}(a')$.

Αφού και $\operatorname{ord}(a') \mid m$, τότε $\operatorname{ord}(a') = m$. □

Προχωράμε στην απόδειξη του κύριου θεωρήματος.

Θεώρημα 7.2. *Έστω πεπερασμένη αβελιανή ομάδα G.*

Έστω στοιχείο m που έχει την μέγιστη τάξη στοιχείου, δηλαδή στοιχείο $m \in G$ τέτοιο ώστε για κάθε στοιχείο $x \in G$ ισχύει ότι $\operatorname{ord}(m) \geq \operatorname{ord}(x)$.

Για κάθε στοιχείο $a \in G$ ισχύει ότι $\operatorname{ord}(a) \mid \operatorname{ord}(m)$.

Απόδειξη. Έστω ότι $\operatorname{ord}(a) \nmid \operatorname{ord}(m)$.

Θεωρούμε την ανάλυση σε πρώτους παράγοντες των αριθμών $\operatorname{ord}(a)$ και $\operatorname{ord}(m)$.

Αφού $\operatorname{ord}(a) \nmid \operatorname{ord}(m)$ τότε υπάρχει ένας πρώτος p έτσι ώστε η μέγιστη δύναμη (έστω i) του p που διαιρεί τον $\operatorname{ord}(a)$ είναι μεγαλύτερη από την μέγιστη δύναμη (έστω j) του p που διαιρεί τον $\operatorname{ord}(m)$. (φυσικά μπορεί $j = 0$.)

Τότε: $\operatorname{ord}(a) = p^i \cdot \kappa$, $\operatorname{ord}(m) = p^j \cdot \lambda$, όπου οι κ, λ δεν έχουν παράγοντα τον p.

Έστω τα στοιχεία $a' = a^\kappa$, $m' = m^{p^j}$.

Από το λήμμα 7.1 είναι $\operatorname{ord}(a') = p^i$ και $\operatorname{ord}(m') = \lambda$.

Αφού $p \nmid \lambda$, τότε: $\gcd(\operatorname{ord}(a'), \operatorname{ord}(m')) = \gcd(p^i, \lambda) = 1$, δηλαδή οι $\operatorname{ord}(a')$, $\operatorname{ord}(m')$ είναι σχετικά πρώτοι.

Τότε από το θεώρημα 7.1, είναι $\operatorname{ord}(a'm') = \operatorname{ord}(a') \operatorname{ord}(m') = p^i \cdot \lambda \overset{i>j}{>} p^j \cdot \lambda = \operatorname{ord}(m)$.

Άρα το στοιχείο $x = a'm'$ έχει τάξη $\operatorname{ord}(x) > \operatorname{ord}(m)$ που είναι άτοπο, διότι το m έχει μέγιστη τάξη από όλα τα στοιχεία. □

8 Άσκηση 8: Ομάδα $\mathbb{Z}_p^*$

8.1 Ερώτημα 1: Αποδοτική εύρεση στοιχείου τάξης ίση με διαιρέτη του $p-1$

Έστω ότι δίνεται πρώτος αριθμός p και γεννήτορας g της ομάδας $\mathbb{Z}_p^*$.

Με είσοδο d διαιρέτη του $p-1$, θέλουμε να βρούμε αποδοτικά στοιχείο $b \in \mathbb{Z}_p^*$ τέτοιο ώστε $\text{ord}(b) = d$.

Έστω $d' = \dfrac{d}{p-1}$, $d' \in \mathbb{N}$ αφού $d \mid p-1$.

Τότε $\text{ord}(g) = p-1 = d \cdot d'$.

Έστω $b = g^{d'}$.

Από το λήμμα 7.1 είναι $\text{ord}(b) = d$.

Απαιτείται χρόνος $O(|d| \cdot |p|) = O\left(|p|^2\right)$ για τον υπολογισμό του d' και $O\left(|d'|^3\right) = O\left(|p|^3\right)$ για τον υπολογισμό του $b = g^{d'}$ (με επαναλαμβανόμενο τετραγωνισμό). Συνολικά ο υπολογισμός γίνεται σε χρόνο $O(|p|^3)$.

8.2 Ερώτημα 2: Πλήθος στοιχείων τάξης ίση με διαιρέτη του $p-1$

Θα αποδείξουμε ότι υπάρχουν $\phi(d)$ στοιχεία τάξης ίση με διαιρέτη d του $p-1$.

Το αποδεικνύουμε γενικότερα για κυκλικές ομάδες.

Ξεκινάμε με ένα λήμμα.

Λήμμα 8.1. *Έστω μια κυκλική ομάδα G τάξης n. Έστω ένας γεννήτορας της g.*

Για κάθε $k \in \mathbb{N}$ είναι:

$$\text{ord}\left(g^k\right) = \frac{n}{\gcd(n,k)} \tag{8.1}$$

Απόδειξη. Έστω $a = g^k$.

Το $\text{ord}(a)$ είναι ο μικρότερος αριθμός x τέτοιος ώστε: $a^x = e$.

Είναι: $a^x = g^{kx} = e$. Για να ισχύει ότι g^{kx} πρέπει και αρκεί $n \mid kx$.

Άρα αναζητούμε τον μικρότερο αριθμό x τέτοιο ώστε το kx να είναι πολλαπλάσιο του n.

Θεωρώντας την ανάλυση σε πρώτους παράγοντες των αριθμών k, x, n παρατηρούμε ότι ο μικρότερος τέτοιος αριθμός x έχει τις δυνάμεις πρώτων αριθμών που περιέχει ο n που δεν είναι κοινές στους k και n.

Ο $\gcd(n,k)$ περιέχει όλες τις κοινές δυνάμεις πρώτων του n και του k και μόνο αυτές.

Συνεπώς ο μικρότερος αριθμός x ώστε $n \mid kx$ είναι ο $x = \dfrac{n}{\gcd(n,k)}$.

Άρα:

$$\text{ord}(a) = \min_{x \in \mathbb{N}, n \mid kx} n = \frac{n}{\gcd(n,k)}$$

□

Συνεχίζουμε με το γενικότερο θεώρημα του ερωτήματος, αλλά για όλες τις κυκλικές ομάδες.

Θεώρημα 8.1. *Έστω μια κυκλική ομάδα G τάξης n.*

Για κάθε d διαιρέτη του n, υπάρχουν ακριβώς $\phi(d)$ πλήθος στοιχείων $b \in G$ με τάξη $\text{ord}(b) = d$.

Απόδειξη. Έστω $d' = \dfrac{d}{n}$, $d' \in \mathbb{N}$ αφού $d \mid n$. Είναι: $n = d \cdot d'$.

Αφού G κυκλική, έστω g γεννήτορας της G. Ισχύει ότι $\text{ord}(g) = n$.

Έστω στοιχείο $b \in G$. Αφού g γεννήτορας, τότε $b = g^k$ για μοναδικό $0 \le k < n$.

Από το λήμμα 8.1 είναι: $\text{ord}(b) = \text{ord}\left(g^k\right) = \dfrac{n}{\gcd(n,k)}$.

Άρα:

$$\text{ord}(b) = d \iff \frac{n}{\gcd(n,k)} = d' \iff \gcd(n,k) = \frac{n}{d} = d'$$

Αν $\gcd(n,k) = d'$ τότε $d' | k$, οπότε υπάρχει $c \in \mathbb{N}$ ώστε $k = cd'$. Είναι $k < n \Rightarrow cd' < dd' \Rightarrow c < d$.

Άρα[3]:

$$\begin{gathered}\operatorname{ord}(b) = d \iff \gcd(n,k) = d' \iff \\ \gcd(n,k) = d' \wedge k = cd' \wedge c < d \iff \\ \gcd(dd', cd') = d' \wedge k = cd' \wedge c < d \iff \\ \gcd(d,c) = 1 \wedge k = cd' \wedge c < d\end{gathered}$$

Με άλλα λόγια, κάθε στοιχείο $\operatorname{ord}(b) = d \in G$ γράφεται με μοναδικό τρόπο $b = g^k$, $0 \leq k < n$, και ισχύει ότι: $\operatorname{ord}(b) = d \iff \gcd(d,c) = 1 \wedge k = cd' \wedge c < d$.

Για διαφορετικά $0 \leq c < d'$ λαμβάνουμε διαφορετικά $k = cd'$, για τα οποία ισχύει ότι $0 \leq k < n$, οπότε για διαφορετικά c λαμβάνουμε και διαφορετικά στοιχεία b.

Οι αριθμοί c, με $0 \leq c < d$ τέτοιοι ώστε $\gcd(c,d) = 1$ (δηλαδή ώστε c και d σχετικά πρώτοι) είναι πλήθους $\phi(d)$. Κάθε τέτοιος αριθμός c αντιστοιχεί σε διαφορετικό στοιχείο b και κάθε τέτοιο στοιχείο έχει $\operatorname{ord}(b) = d$. Επίσης η ισοδυναμία εξασφαλίζει ότι και κάθε στοιχείο b με $\operatorname{ord}(b) = c$ δίνει και έναν αριθμό c από αυτούς που περιγράψαμε.

Συνεπώς υπάρχουν πλήθους ακριβώς $\phi(d)$ στοιχεία $b \in G$ τέτοια ώστε $\operatorname{ord}(b) = d$. □

Τελικά, προκύπτει το ζητούμενο του ερωτήματος ως απόρροια του θεωρήματος αυτού.

Πόρισμα 8.1. *Έστω ένας πρώτος p.*

Για κάθε d διαιρέτη του $p-1$, υπάρχουν ακριβώς $\phi(d)$ πλήθος στοιχείων $b \in \mathbb{Z}_p^*$ με τάξη $\operatorname{ord}(b) = d$.

Απόδειξη. Η ομάδα $\mathbb{Z}_p^*$ έχει τάξη $p-1$ και από γνωστό θεώρημα είναι κυκλική.

Συνεπώς, από το θεώρημα 8.1 ισχύει ότι για κάθε d διαιρέτη του $p-1$, υπάρχουν ακριβώς $\phi(d)$ πλήθος στοιχείων $b \in G$ με τάξη $\operatorname{ord}(b) = d$. □

8.3 Ερώτημα 3: Πλήθος γεννητόρων κυκλικής υποομάδας παραγόμενης από στοιχείο τάξης d

Ξεκινάμε με ένα λήμμα.

Λήμμα 8.2. *Έστω G κυκλική ομάδα τάξης d. Η G έχει ακριβώς $\phi(d)$ γεννήτορες.*

Απόδειξη. Οι γεννήτορες της G είναι ακριβώς τα στοιχεία της G που έχουν τάξη, την τάξη της ομάδας, δηλαδή d.

Ισχύει ότι $d \mid d$.

Άρα από το θεώρημα 8.1 υπάρχουν ακριβώς $\phi(d)$ στοιχεία της G με τάξη d.

Συνεπώς η G έχει ακριβώς $\phi(d)$ γεννήτορες. □

Συνεχίζουμε με το γενικότερο θεώρημα του ερωτήματος, αλλά για όλες τις ομάδες.

Θεώρημα 8.2. *Έστω G (πεπερασμένη) ομάδα.*

Για κάθε στοιχείο $b \in G$, αν το στοιχείο έχει τάξη $\operatorname{ord}(b) = d$, η κυκλική υποομάδα της G που παράγει το b, έχει ακριβώς $\phi(d)$ γεννήτορες.

Απόδειξη. Η κυκλική υποομάδα της G, έστω G', που παράγει το b έχει τάξη, την τάξη του στοιχείου b: $\operatorname{ord}(b) = d$.

Από το λήμμα 8.2 η G' έχει ακριβώς d γεννήτορες. □

[3] Αν $A \Rightarrow B$ τότε $A \iff A \wedge B$ καθώς η προς τα δεξιά κατεύθυνση ισχύει άμεσα και η προς τα αριστερά ισχύει λαμβάνοντας το αριστερό όρισμα του $\wedge$

8.4 Ερώτημα 4: Πλήθος κυκλικών υποομάδων της $\mathbb{Z}_p^*$ τάξης d

Θεώρημα 8.3. *Έστω G μια κυκλική ομάδα τάξης n.*

Για κάθε $d \in \mathbb{N}$, αν $d \mid n$, τότε υπάρχει μοναδική κυκλική υποομάδα της G τάξης d, ενώ αν $d \nmid n$ τότε δεν υπάρχει κυκλική υποομάδα της G τάξης d.

Απόδειξη. Αν $d \nmid n$ τότε δεν υπάρχει κυκλική υποομάδα της G τάξης d, διότι αν υπήρχε, από το Θεώρημα Lagrange, θα έπρεπε $d \mid n$.

Έστω ότι $d \mid n$. Από το θεώρημα 8.1 υπάρχει ακριβώς $\phi(d)$ στοιχεία της G με $\operatorname{ord}(()\, b) = d$.

Έστω ένα από αυτά τα στοιχεία, έστω b_0. Αφού $\operatorname{ord}(b_0) = d$ το d_0 παράγει μια κυκλική υποομάδα τάξης d.

Συνεπώς υπάρχει μια κυκλική υποομάδα της G τάξης d.

Θα δείξουμε ότι είναι μοναδική.

Έστω μια κυκλική υποομάδα G' της G τάξης d. Από το θεώρημα 8.2 η G' έχει ακριβώς $\phi(d)$ γεννήτορες.

Κάθε γεννήτορας g της G' είναι στοιχείο της G με τάξη, ως προς την G, d.

Δύο διαφορετικές κυκλικές υποομάδες G_1, G_2 της G, δεν μπορούν να έχουν κανέναν κοινό γεννήτορα, διότι αν είχαν, τότε αυτός ο γεννήτορας θα παρήγαγε και τις δύο ομάδες, οπότε η G_1, G_2 θα ήταν ίδιες.

Συνεπώς έστω ότι υπάρχουν k διαφορετικές κυκλικές υποομάδες τάξης d. Τότε όλες έχουν διαφορετικό σύνολο γεννητόρων, καθένα μέγεθος $\phi(d)$ και κάθε γεννήτορας κάθε υποομάδας είναι στοιχείο τάξης d της G.

Συνεπώς η G έχει $k \cdot \phi(d)$ στοιχεία τάξης d.

Όμως από το θεώρημα 8.1 (εφαρμόστηκε και παραπάνω), η G έχει ακριβώς $\phi(d)$ στοιχεία τάξης d.

Συνεπώς $k \leq 1$, δηλαδή υπάρχει το πολύ μια κυκλική υποομάδα της G τάξης d.

Τελικά, η G έχει μια κυκλική υποομάδα τάξης d και αυτή είναι μοναδική. □

Προχωράμε στο ζητούμενο του ερωτήματος.

Πόρισμα 8.2. *Έστω p πρώτος.*

Για κάθε $d \in \mathbb{N}$, αν $d \mid p-1$, τότε υπάρχει μοναδική κυκλική υποομάδα της $\mathbb{Z}_p^*$ τάξης d, ενώ αν $d \nmid n$ τότε δεν υπάρχει κυκλική υποομάδα της $\mathbb{Z}_p^*$ τάξης d.

Απόδειξη. Η $\mathbb{Z}_p^*$ είναι κυκλική ομάδα (από γνωστό θεώρημα) και έχει τάξη $p-1$.

Συνεπώς το συμπέρασμα προκύπτει άμεσα από το θεώρημα 8.3. □

8.5 Ερώτημα 5: Αποδοτικός έλεγχος συμμετοχής στοιχείου κυκλικής ομάδας σε υποομάδα γνωστού γεννήτορα και τάξης

Δίνουμε γενικότερη λύση για κυκλικές ομάδες G.

Έστω κυκλική ομάδα G και ένα στοιχείο της $h \in G$ με τάξη $\operatorname{ord}(h) = d$.

Θέλουμε να εξετάσουμε αποδοτικά, δοθέντος h και d, αν ένα στοιχείο $a \in G$ ανήκει στην κυκλική υποομάδα που παράγει το h.

Υπολογίζουμε το a^d. Αν $a^d = e$ (στην $\mathbb{Z}_p^*$ αν $a^d \equiv 1 \pmod p$) απαντάμε πως ανήκει στην κυκλική υποομάδα που παράγει το h, αλλιώς απαντάμε πως δεν ανήκει.

Ο υπολογισμός γίνεται σε χρόνο $O(|p|^3)$ με επαναλαμβανόμενο τετραγωνισμό.

Αποδεικνύουμε την ορθότητα του αλγορίθμου.

Θεώρημα 8.4. *Έστω κυκλική ομάδα G και ένα στοιχείο της $h \in G$ με τάξη $\operatorname{ord}(h) = d$.*

Κάθε στοιχείο $a \in G$ ανήκει στην κυκλική υποομάδα G' που παράγει το h, αν και μόνο αν $a^d = e$.

Απόδειξη. Έστω ότι το a ανήκει στην κυκλική υποομάδα G' που παράγει το h.

Η G' έχει τάξη την τάξη του h, δηλαδή $\operatorname{ord}(h) = d$.

Τότε: $a^d = e$.

Αντίστροφα, έστω ότι $a^d = e$. Θα δείξω ότι $a \in G'$.

Αφού $a^d = e$, τότε $\text{ord}\,(a)\,|d$.

Η G' έχει τάξη d. Συνεπώς από το θεώρημα 8.3 υπάρχει ακριβώς μια κυκλική υποομάδα G'' της G' τάξης $\text{ord}\,(a)$.

Η G'' είναι υποομάδα της G', που είναι υποομάδα της G. Συνεπώς η G'' είναι μια κυκλική υποομάδα τάξης $\text{ord}\,(a)$ της G.

Έστω η κυκλική υποομάδα G''' της G που παράγει το a, τάξης $\text{ord}\,(a)$. Είναι $a \in G'''$.

Από το Θεώρημα Lagrange το $\text{ord}\,(a)$ διαιρεί την τάξη της ομάδας G.

Συνεπώς από το θεώρημα 8.3 η κυκλική υποομάδα τάξης $\text{ord}\,(a)$ είναι μοναδική, οπότε η G''' και η G'' ταυτίζονται.

Άρα $a \in G''$. Όμως $G'' \subseteq G'$. Συνεπώς $a \in G'$. □

9 Άσκηση 9: Προγραμματιστική Υλοποίηση ελέγχου Miller-Rabin

9.1 Υλοποίηση

```haskell
module MillerRabin
  ( isPrime
  ) where

import Control.Monad
import System.Random.Stateful

modexp :: Integer -> Integer -> Integer -> Integer
modexp b e m =
  let aux _ 0 acc = acc
      aux b1 e1 acc =
        let acc' =
              if odd e1
                then (b1 * acc) `mod` m
                else acc
         in aux ((b1 * b1) `mod` m) (e1 `div` 2) acc'
   in aux b e 1

isPrime_pass :: Integer -> Integer -> Bool
isPrime_pass n b
  | modexp b (n - 1) n /= 1 = False
  | otherwise =
    let t = go (n - 1)
        go x
          | even x = go (x `div` 2)
          | otherwise = x
        aux 1 = False
        aux bt'
          | bt' == (n - 1) = True
          | otherwise = aux ((bt' * bt') `mod` n)
        bt = modexp b t n
     in if bt == 1 || bt == n - 1
          then True
          else aux bt

isPrime :: Integer -> Int -> Bool
isPrime 1 _ = False
isPrime n checks =
  let randomexp gen = do
        bs <- replicateM checks $ uniformRM (1, n - 1) gen
        return (all (isPrime_pass n) bs)
      pureGen = mkStdGen 42
   in runStateGen_ pureGen randomexp
```

9.2 Testbench

Επιλέχθηκε πλήθος 10 passes στον έλεγχο Miller Rabin. (αυτό δίνει πιθανότητα αποτυχίας $4^{-10} \approx 10^{-6}$)

Ελέγχθηκε η ορθότητα για όλους τους αριθμούς $\{1 \cdots 10000\}$.

Ελέγχθηκε η ορθότητα για αριθμούς Mersenne με εκθέτες 3217, 4253, 4423, 9689.

Ελέγχθηκε η ορθότητα για αριθμούς της μορφής $2_i - 1$ με εκθέτες 1234, 4567, 9876, 5432, που με βάση πληροφορίες από το Διαδίκτυο, δεν δίνουν αριθμούς Mersenne, οπότε δεν είναι πρώτοι.

Τέλος ελέγχθηκε η ορθότητα για τους αριθμούς που δίνονται στην εκφώνηση, και ελέγχθηκε με πληροφορίες από το Διαδίκτυο, ότι οι απαντήσεις είναι ορθές.

Ειδικότερα, ελέγχθηκαν οι αριθμοί:

1. $67280421310721 \in \mathbb{P}$
2. $170141183460469231731687303715884105 7 \notin \mathbb{P}$
3. $2^{1001} - 1 \notin \mathbb{P}$
4. $2^{2281} - 1 \in \mathbb{P}$ (αριθμός Mersenne)
5. $2^{9941} - 1 \in \mathbb{P}$ (αριθμός Mersenne)

Οι έλεγχοι μπορούν να επανεκτελέστουν με την εντολή: `cabal test`.

Παρατίθεται ο κώδικας Haskell για το Testbench.

```haskell
module Main (main) where

import System.Exit (exitFailure)
import MillerRabin (isPrime)

isqrt :: Integer -> Integer
isqrt n
    | n < 2 = n
    | otherwise = aux 1 n
  where
    aux l r
        | r < l = r
        | m*m > n = aux l (m-1)
        | otherwise = aux (m+1) r
      where
        m = (l+r) `div` 2


isPrime_oracle :: Integer -> Bool
isPrime_oracle n
  | n <= 1 = False
  | n == 2 = True
  | even n = False
  | otherwise = null [x | x <- [3,5.. isqrt n], n `mod` x == 0]

checks :: Int
checks = 10

test :: Integer -> IO ()
test n =
  let p = isPrime n checks
      p' = isPrime_oracle n
  in
  if p == p' then return () else do
     putStrLn $ "isPrime " ++ show n ++ " = " ++ show p ++ " , isPrime_oracle " ++ show n ++
  ↪  " = " ++ show p'
     exitFailure

mersennes :: [Integer]
mersennes = [ 2^p-1 | p <- [3217, 4253, 4423, 9689] ]
nonmersennes :: [Integer]
nonmersennes = [ 2^i-1 | i <- [1234, 4567, 9876, 5432] ]

test_big :: Bool -> Integer -> IO ()
test_big is n =
  let p = isPrime n checks
  in
  if p == is then return () else do
     putStrLn $ "(the following is (/is not) a prime), isPrime " ++ show n ++ " = " ++ show p
```

```
      exitFailure


main :: IO ()
main = do
  mapM_ test [1..10000]
  putStrLn "Checked all numbers from 1 to 10000."

  mapM_ (test_big True) mersennes
  putStrLn "Checked some bigint mersenne primes."

  mapM_ (test_big False) nonmersennes
  putStrLn "Checked some bigint, mersenne-like non-primes (2^i-1)."

  test_big True 67280421310721
  putStrLn "Checked 67280421310721, found correctly it is a prime."

  test_big False 170141183460469231731687303715884105 7
  putStrLn "Checked 170141183460469231731687303715884105 7, found correctly it is not a
   ↪  prime."

  test_big False (2^1001 - 1)
  putStrLn "Checked 2^1001 - 1, found correctly it is not a prime."

  test_big True (2^2281 - 1)
  putStrLn "Checked 2^2281 - 1, found correctly it is a prime."

  test_big True (2^9941 - 1)
  putStrLn "Checked 2^9941 - 1, found correctly it is a prime."

```

9.3 Αρχείο `.cabal`

Παρατίθεται το αρχείο `millerrabin.cabal` για να διευκολυνθεί η μεταγλώττιση από τον αναγνώστη:

```
cabal-version:      3.0
name:               millerrabin
version:            0.1.0.0
-- synopsis:
-- description:
license:            GPL-3.0-only
license-file:       LICENSE
author:             Andreas Stamos
maintainer:         stamos.aa@gmail.com
-- copyright:
build-type:         Simple
extra-doc-files:    CHANGELOG.md
-- extra-source-files:

common warnings
    ghc-options: -Wall

library
    import:           warnings
    exposed-modules:  MillerRabin
    -- other-modules:
    -- other-extensions:
    build-depends:    base ^>=4.20.0.0, random
    hs-source-dirs:   src
    default-language: Haskell2010

```

```
test-suite millerrabin-test
    import:           warnings
    default-language: Haskell2010
    -- other-modules:
    -- other-extensions:
    type:             exitcode-stdio-1.0
    hs-source-dirs:   test
    main-is:          Main.hs
    build-depends:
        base ^>=4.20.0.0,
        millerrabin

```

10 Bonus Άσκηση: Το παιχνίδι του σιδεροθρόνου

10.1 Βοηθητικά Θεωρήματα: Αναγωγή σε πρόβλημα θεωρίας ομάδων

Έστω A το σύνολο των ανθρώπων. Είναι $|A| = 2^{19} - 1$.

Κάθε άνθρωπος τραυματίστηκε με κάποιο μαχαίρι από κάποιον άλλο. Υποθέτουμε, πως η εκφώνηση υπονοεί ότι αυτός ο κάποιος είναι και μοναδικός, δηλαδή πως αν ένας άνθρωπος με ένα μαχαίρι τραυματίσει έναν δεύτερο, τότε τον δεύτερο με το ίδιο μαχαίρι δεν τραυματίζει κανείς άλλος. Η παράγραφος της εκφώνησης για τις τριάδες ανθρώπων, αναφέρεται σε αυτόν που τραυματίζει σαν να είναι ένας, οπότε από αυτό, υποθέτουμε πως η προηγούμενη μοναδικότητα είναι πράγματι στις υποθέσεις.

Με βάση το προηγούμενο ορίζεται η συνάρτηση f : (τραυματιζόμενος, μαχαίρι) $\mapsto$ άνθρωπος που τραυματίζει. Επειδή τα μαχαίρια έχουν έναν μοναδικό ιδιοκτήτη, και κάθε άνθρωπος έχει ακριβώς ένα μαχαίρι (συνάρτηση $1-1$ και επί μεταξύ μαχαιριών και ανθρώπων), ορίζεται και η συνάρτηση f'τραυματιζόμενος, ιδιοκτήτης μαχαιριού $\mapsto$ άνθρωπος που τραυματίζει. Η συνάρτηση αυτή έχει τύπου $f' : A \times A \mapsto A$, δηλαδή είναι μια διμελής πράξη στο A. Θα την συμβολίζουμε infix ως: τραυματιζόμενος $\otimes$ ιδιοκτήτης μαχαιριού $=$ άνθρωπος που τραυματίζει.

Σκοπός είναι να δείξουμε ότι η $(A, \otimes)$ είναι ομάδα.

Συμβολίζουμε τον Καλικάτζαρο με $e \in A$.

Κάθε άνθρωπος αυτοτραυματίστηκε με το μαχαίρι του Καλικάτζαρου (συμπεριλαμβανομένου του Καλικάτζαρου). Συνεπώς:

$$\forall x, x \otimes e = x \tag{10.1}$$

Όλοι οι άνθρωποι, τραυματίστηκαν από όλα τα μαχαίρια. Αυτό ισχύει και για τον Καλικάτζαρο, δηλαδή όλοι οι άνθρωποι έχουν τραυματιστεί με κάποιο μαχαίρι από τον Καλικάτζαρο. Συνεπώς:

$$\forall x \exists x', x \otimes x' = e \tag{10.2}$$

Τέλος για κάθε τριάδα ανθρώπων (έστω $x, y, z \in A$), εκείνος που τραυμάτισε τον τρίτο (z) με το μαχαίρι αυτού που τραυμάτισε τον δεύτερο (y) με το μαχαίρι του πρώτου (x) – αυτός είναι ο $y \otimes x$ – είναι ο ίδιος με εκείνον που τραυμάτισε τον άνθρωπο που τραυμάτισε τον τρίτο (z) με το μαχαίρι του δεύτερου (y) – αυτός είναι ο $z \otimes y$, με το μαχαίρι του πρώτου (x). Ισοδύναμα:

$$\forall xyz, z \otimes (y \otimes x) = (z \otimes y) \otimes x \tag{10.3}$$

Αποδεικνύουμε το εξής θεώρημα:

Θεώρημα 10.1. *Έστω ένα σύνολο A, εφοδιασμένο με μια διμελή πράξη $\otimes : A \times A \mapsto A$.*

Έστω ότι ισχύουν τα εξής:

1. *Υπάρχει δεξιό ουδέτερο στοιχείο:*
$$\exists e \forall x,\ x \otimes e = x \tag{10.4}$$
2. *Υπάρχει δεξιός αντίστροφος:*
$$\forall x \exists x^{-1},\ x \otimes x^{-1} = e \tag{10.5}$$
, όπου το e είναι το ίδιο με πριν.
3. *Η πράξη είναι προσεταιριστική:*
$$\forall x \forall y \forall z,\ x \otimes (y \otimes z) = (x \otimes y) \otimes z \tag{10.6}$$

Τότε το $(A, \otimes)$ είναι ομάδα.

Απόδειξη. Λείπουν μόνο τα "ανάποδα" των υποθέσεων 10.4 και 10.5.

Για $x = e$ στην 10.4: $e \otimes e = e$.

Για κάθε $x \in A$, έστω το στοιχείο x^{-1} της υπόθεσης 10.5. Είναι: $x \otimes x^{-1} = e$.

Για το $x^{-1} \in A$, έστω το στοιχείο $\left(x^{-1}\right)^{-1}$ της υπόθεσης 10.5. Είναι: $x^{-1} \otimes \left(x^{-1}\right)^{-1} = e$.

Αντικαθιστώ την $x \otimes x^{-1} = e$ στην $e \otimes e = e$ (δεν αντικαθιστώ το πρώτο e):

$$e \otimes (x \otimes x^{-1}) = x \otimes x^{-1} \overset{10.6}{\Rightarrow}$$
$$(e \otimes x) \otimes x^{-1} = x \otimes x^{-1} \Rightarrow$$
$$((e \otimes x) \otimes x^{-1}) \otimes (x^{-1})^{-1} = (x \otimes x^{-1}) \otimes (x^{-1})^{-1} \overset{10.6}{\Rightarrow}$$
$$(e \otimes x) \otimes \left(x^{-1} \otimes (x^{-1})^{-1}\right) = x \otimes \left(x^{-1} \otimes (x^{-1})^{-1}\right) \overset{10.6}{\Rightarrow}$$
$$(e \otimes x) \otimes e = x \otimes e \overset{10.4}{\Rightarrow}$$
$$e \otimes x = e$$

Άρα:

$$e \otimes x = x \otimes e = x \tag{10.7}$$

Ισχύει επίσης:

$$x \otimes x^{-1} = e \Rightarrow$$
$$(x \otimes x^{-1}) \otimes (x^{-1})^{-1} = e \otimes (x^{-1})^{-1} \overset{10.6,\ 10.7}{\Rightarrow}$$
$$x \otimes \left(x^{-1} \otimes (x^{-1})^{-1}\right) = (x^{-1})^{-1} \Rightarrow$$
$$x \otimes e = (x^{-1})^{-1} \overset{10.7}{\Rightarrow}$$
$$x = (x^{-1})^{-1}$$

Τότε:

$$e = x^{-1} \otimes (x^{-1})^{-1} = x^{-1} \otimes x$$

Άρα:

$$x \otimes x^{-1} = x^{-1} \otimes x = e \tag{10.8}$$

Τελικά, αφού ισχύουν οι 10.7 (αριστερός και δεξιός ουδέτερος), 10.8 (αριστερός και δεξιός αντίστροφος) και 10.6 (προσεταιριστικότητα), η $(A, \otimes)$ είναι ομάδα. □

Επιστρέφοντας στην άσκηση, αφού ισχύουν οι 10.1 (ύπαρξη δεξιού ουδέτερου στοιχείου), 10.2 (ύπαρξη δεξιού αντιστρόφου) και 10.3 (προσεταιριστικότητα), με βάση το Θεώρημα 10.1, **το $(A, \otimes)$ είναι ομάδα!**

Είναι: $|A| = 2^{19} - 1$ και το $2^{19} - 1$ είναι πρώτος. (συγκεκριμένα είναι αριθμός Mersenne)

Αφού η ομάδα A έχει τάξη πρώτο αριθμό είναι κυκλική. Αυτό προκύπτει λόγω του επόμενου γνωστού θεωρήματος, που αποδεικνύουμε για λόγους πληρότητας.

Θεώρημα 10.2. *Έστω μια ομάδα G. Αν είναι $|G| \in \mathbb{P}$ τότε η G είναι κυκλική.*

Απόδειξη. Έστω ένα στοιχείο $x \in G$.

Έστω η κυκλική υποομάδα G' που παράγει το x.

Από το Θεώρημα Lagrange ο $|G'|$ διαιρεί τον $|G|$.

Άρα αφού $|G| \in \mathbb{P}$ τότε $|G'| = 1$ ή $|G'| = G$.

Αν υπάρχει έστω και ένα στοιχείο x ώστε $|G'| = |G|$, η G είναι κυκλική αφού το x την παράγει.

Έστω ότι δεν υπάρχει κανένα στοιχείο x ώστε $|G'| = |G|$, δηλαδή ότι για κάθε $x \in G$ η κυκλική υποομάδα G' που παράγει το x έχει τάξη 1, ισοδύναμα $x \otimes x = x$.

Όμως:

$$x \otimes x = x \Rightarrow x^{-1} \otimes x \otimes x = x^{-1} \otimes x \Rightarrow x = e$$

Δηλαδή για κάθε στοιχείο $x \in G$ είναι $x = e$. Οπότε $|G| = 1$.

Αν $|G| = 1$, τότε η G είναι κυκλική. Αλλιώς αν $|G| > 1$ άτοπο. □

10.2 Ερώτημα 1

Αφού η A είναι κυκλική, τότε είναι και αβελιανή, δηλαδή για κάθε $x, y \in A$ είναι: $x \otimes y = y \otimes x$.

Ισοδύναμα: *"Αν ένας άνθρωπος τραυμάτισε έναν άνθρωπο A με το μαχαίρι του B, τότε τραυμάτισε και τον B με του μαχαίρι του A!"*

Η Δρακομάνα τραυμάτισε τον Γιάννη τον Χιονιά με τον μαχαίρι του Τζοφραίου του Αντιπαθητικό.

(Γιάννης Χιονιάς $\otimes$ Τζοφραίος Αντιπαθητικός = Δρακομάνα)

Τότε ο Τζοφραίος ο Αντιπαθητικός τραυματίστηκε με το μαχαίρι του Γιάννη του Χιονιά από την Δρακομάνα.

(Τζοφραίος Αντιπαθητικός $\otimes$ Γιάννης Χιονιάς = Δρακομάνα)

10.3 Ερώτημα 2

Κάθε άνθρωπος, εκτός του Καλικάτζαρου, έχει έναν μοναδικό Θανάσιμο Εχθρό. Έστω η συνάρτηση $h : A - \{e\} \mapsto A$ που δίνει το Θανάσιμο Εχθρό κάθε ανθρώπου εκτός του Καλικάτζαρου.

Ο Καλικάντζαρος τραυμάτισε κάθε άνθρωπο με το μαχαίρι του Θανάσιμου Εχθρού του.

Άρα για κάθε $x \in A - \{e\}$: $x \otimes h(x) = e$. Ισοδύναμα:

$$h(x) = x^{-1} \tag{10.9}$$

Από αυτό προκύπτει και ότι: $h(h(x)) = h\left(x^{-1}\right) = \left(x^{-1}\right)^{-1} = x$ αν $h(x) \neq e$, δηλαδή:

"Αν ο θανάσιμος εχθρός ενός ανθρώπου A δεν είναι ο Καλικάτζαρος, τότε ο θανάσιμος εχθρός του θανάσιμου εχθρού του A είναι και πάλι ο άνθρωπος A."

Αυτό αναφέρεται στο ερώτημα ως να ισχύει από υπόθεση για την Δρακομάνα και τον Τζοφραίο τον Αντιπαθητικό, όμως δεν απαιτείται να το υποθέσουμε.

Η Δρακομάνα και ο Τζοφραίος ο Αντιπαθητικός είναι Θανάσιμοι Εχθροί.

Άρα: h(Τζοφραίος Αντιπαθητικός) = Δρακομάνα, δηλαδή:

$$\text{Τζοφραίος Αντιπαθητικός}^{-1} = \text{Δρακομάνα} \tag{10.10}$$

Από το ερώτημα 1:

$$\begin{gathered}\text{Γιάννης Χιονιάς} \otimes \text{Τζοφραίος Αντιπαθητικός} = \text{Δρακομάνα} \Rightarrow \\ \text{Δρακομάνα} \otimes \text{Τζοφραίος Αντιπαθητικός}^{-1} = \text{Γιάννης Χιονιάς} \Rightarrow \\ \text{Δρακομάνα} \otimes \text{Δρακομάνα} = \text{Γιάννης Χιονιάς}\end{gathered} \tag{10.11}$$

Συνεπώς, η Δρακομάνα τραυματίστηκε με το μαχαίρι της από τον Γιάννη τον Χιονιά.

10.4 Ερώτημα 3

Τον Γιάννη τον Χιονιά τραυμάτισε με το ίδιο του το μαχαίρι ο άνθρωπος (έστω A):

$$\text{A} = \text{Γιάννης Χιονιάς} \otimes \text{Γιάννης Χιονιάς} = \text{Γιάννης Χιονιάς}^2 \tag{10.12}$$

Τον Τζοφραίο τον Αντιπαθητικό τραυμάτισε με το ίδιο του το μαχαίρι ο άνθρωπος (έστω B):

$$\begin{gathered}B = \text{Τζοφραίος Αντιπαθητικός} \otimes \text{Τζοφραίος Αντιπαθητικός} = \text{Τζοφραίος Αντιπαθητικός}^2 \overset{10.10}{=} \\ \left(\text{Δρακομάνα}^{-1}\right)^2 = \text{Δρακομάνα}^{-2} = \\ \left(\text{Δρακομάνα}^2\right)^{-1} \overset{10.11}{=} \text{Γιάννης Χιονιάς}^{-1}\end{gathered} \tag{10.13}$$

Συνεπώς, ο άνθρωπος που χρησιμοποίησε το μαχαίρι του A, δηλαδή εκείνου που τραυμάτισε τον Γιάννη τον Χιονιά με το ίδιο του το μαχαίρι, για να τραυματίσει τον B, δηλαδή εκείνον που τραυμάτισε τον Τζοφραίο τον Αντιπαθητικό με τον εαυτό του είναι ο (έστω C):

$$C = A \otimes B = \text{Γιάννης Χιονιάς}^2 \otimes \text{Γιάννης Χιονιάς}^{-1} = \text{Γιάννης Χιονιάς} \tag{10.14}$$

Τελικά, δηλαδή, ο ζητούμενος άνθρωπος είναι **ο Γιάννης ο Χιονιάς**.

Κατάλογος Θεωρημάτων, Λημμάτων, Πορισμάτων