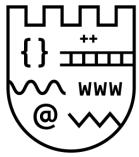
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Σχολή Θετικών Επιστημών



ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Εργασία στο μάθημα της Κρυπτογραφίας

Καλαθάς Μάνος - ΑΕΜ:101

7 Φεβρουαρίου 2022

Περιεχόμενα

1 ΄Ασκηση 1.3

Ξεκινάω και ελέγχω για όλες τις τιμές του εκθέτη το αποτέλεσμα της έκφρασης $g^{ab} \mod 677$ και τυπώνω τις τιμές του εκθέτη που δίνουν αποτέλεσμα 1.

2 ΄Ασκηση 2.4

Υπολογίζω αρχικά την τιμή του modulo και πραγματοποιώ γρήγορη ύψωση σε δύναμη για να υπολογίσω τους τρεις παράγοντες modulo την τιμή που βρήκαμε, χρησιμοποιώντας την ιδιότητα $a \cdot b \mod c = a \mod c \cdot b \mod c$ και τους πολλαπλασιάζω με τον αλγόριθμο Karatsuba.

3 ΄Ασκηση 3.1

Υποθέτω ότι οι αριθμοί της μορφής $4n+3$, $n \in \mathbb{Z}$ είναι τέλεια τετράγωνα. Μπορούν άρα να γραφούν ως:

$$4n + 3 = x^2$$

Το πρώτο μέρος της εξίσωσης είναι ένας περιττός αριθμός άρα και τα x^2, x είναι και αυτοί περιττοί, άρα: $x = 2k + 1$, $k \in \mathbb{Z}$. Αντικαθιστώντας στην αρχική εξίσωση έχω ότι:

$$4n+3 = (2k+1)^2 \iff 4n+3 = 4k^2+4k+1 \iff 4k^2+4k-4n = 2 \iff 2(k^2+k-n) = 1 \quad k, n \in \mathbb{Z}$$

Καταλήξαμε λοιπόν σε άτοπο άρα και η αρχική υπόθεση είναι λανθασμένη.

Για το δεύτερο ερώτημα, αρκεί να αποδείξω ότι όλοι οι αριθμοί 11,111,1111 μπορούν να γραφούν σαν 4n+3 και από την παραπάνω απόδειξη προκύπτει ότι οι αριθμοί που εξετάζουμε δεν μπορεί να είναι τέλεια τετράγωνα. Παρατηρώ ότι

μπορώ να γράψω 111 = 100 + 11, 1111 = 1000 + 11, 11111 = 10000 + 11 κ.ο.κ. Έστω ότι επιλέγω χ έναν τυχαίο όρο από την ακολουθία, ισχύει ότι:

$$x \equiv 11 \pmod{100} \iff x = 100 \cdot k + 11 \iff x = 4(25 \cdot k) + 11 \iff x \equiv 11 \pmod{4} \iff x \equiv 3 \pmod{4} \tag{3.1}$$

Από τον ορισμό του modulo έχω $\chi = 4n + 3, n \in \mathbb{Z}$ Ο.Ε.Δ.

4 ΄Ασκηση 3.4

Έστω ότι το 2^m είναι άθροισμα διαδοχικών ακέραιων αριθμών τότε μπορώ να το γράψω σαν:

$$2^m = a_i + \ldots + a_k = ka_i + \frac{k(k+1)}{2} = \frac{2 \cdot k \cdot a_i + k^2 + k}{2} \iff 2^{m+1} = k(2 \cdot a_i + k + 1)$$

Αλλά ο όρος 2^{m+1} αποτελείται μόνο από ζυγούς παράγοντες άρα πρέπει και το δεύτερο μέρος της εξίσωσης να ικανοποιεί την ίδια ιδιότητα. Εξετάζω δύο περιπτώσεις:

- Ο k είναι περιττός, άρα αυτομάτως καταλήγουμε σε άτοπο.
- Ο k είναι ζυγός, επομένως και το $2 \cdot a_i + k + 1$ είναι ένας άρτιος αριθμός συν ένα, άρα και περιττός που οδηγεί πάλι σε άτοπο.

Το 2^m επομένως δεν μπορεί να είναι άθροισμα διαδοχικών ακέραιων αριθμών.

5 ΄Ασκηση 3.25

Έστω ότι ο $\sqrt{p}$ είναι ρητός, τότε $\sqrt{p} = \frac{q}{n}, \iff p = \frac{q^2}{n^2} \iff n^2 p = q^2 \quad q, n \in \mathbb{N}$
Από το θεμελιώδες θεώρημα αριθμητικής έχω:

$$\chi = p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$$

Τα τέλεια τετράγωνα, επομένως και τα q^2, n^2 έχουν άρτιο αριθμό πρώτων στην παραγοντοποίηση τους. Στον όρο $n^2 \cdot p$ το p είτε είναι παράγοντας του n ή όχι και αντιστοίχως εμφανίζεται συνολικά $\#p = 1$ ή $\#p = 2\kappa + 1, k \in \mathbb{N}$ φορές στο πρώτο μέρος της εξίσωσης που είναι ένας περιττός αριθμός άρα καταλήγουμε σε άτοπο. Επομένως ο p δεν μπορεί να είναι ρητός.

6 ΄Ασκηση 3.28

Χρησιμοποιώ τον εκτεταμένο αλγόριθμο του Ευκλείδη, βρίσκω αρχικά τον gcd(540,315):

$$540 = 315 + 225$$
$$315 = 225 + 90$$
$$225 = 2 \cdot 90 + 45$$
$$90 = 2 \cdot 45$$

Και μετά τους παράγοντες Bezout:

$$45 = 225 - 2 \cdot 90 = 225 - 2(315 - 225) =$$
$$= -2 \cdot 315 + 3 \cdot 225 = -2 \cdot 315 + 3(540 - 315) = 3 \cdot 540 - 5 \cdot 315$$

΄Αρα α=3 και β=-5 και ισχύει

$$3 \cdot 540 - 5 \cdot 315 = 45$$

7 ΄Ασκηση 3.30

Ισχύει gcd(a,b)=1 άρα $ax + by = 1$ και οι a,b είναι πρώτοι μεταξύ τους:

1. Με την λογική, ο μέγιστος κοινός διαιρέτης του c και του b θα είναι ο ίδιος με αυτόν του ac και b αφού οι a και b είναι πρώτοι μεταξύ τους και άρα το a δεν προσθέτει κάποιο διαιρέτη για να αλλάξει το αποτέλεσμα. Διατυπώνοντας το μαθηματικά, έστω ότι έχουμε:

$$gcd(ac, b) = p \Rightarrow p|ac \wedge p|b \Rightarrow p|c \wedge p|b \Rightarrow p|gcd(c, b) \Rightarrow p|q$$
$$gcd(c, b) = q \Rightarrow q|c \wedge q|b \Rightarrow q|ac \wedge q|b \Rightarrow q|gcd(ac, b) \Rightarrow q|p$$

   Για το βήμα $p|ac \Rightarrow p|c$, χρειάζεται να ξέρουμε ότι gcd(p,a)=1 κάτι που ισχύει διότι ο p θα είναι είτε ένα είτε κάποιος διαιρέτης του b αλλά οι a και b είναι πρώτοι μεταξύ τους άρα και κανένας διαιρέτης του p δεν θα διαιρεί τον α. Από τις δύο προηγούμενες προτάσεις επομένως, ισχύει ότι $p = q \Rightarrow gcd(ac, b) = gcd(c, b)$ Ο.Ε.Δ.

2. Έστω gcd(a+b, a-b) = g, τότε:

$$g|a + b \Rightarrow gx = a + b$$
$$g|a - b \Rightarrow gy = a - b$$

Προσθέτοντας και αφαιρώντας κατά μέλη έχουμε:

$$g(x+y) = 2a \Rightarrow g|2a$$
$$g(x-y) = 2b \Rightarrow g|2b$$

Όμως οι a,b είναι πρώτοι μεταξύ τους οπότε δεν έχουν κοινό διαιρέτη, άρα πρέπει το g να είναι είτε ένα ή δύο διότι αλλιώς το g θα διαιρούσε και τα a,b κάτι αδύνατο. Αν a,b περιττοί τότε οι a+b,a-b είναι ζυγοί αριθμοί και χρησιμοποιώντας το προηγούμενο εύρημα καταλήγουμε στο ότι ο μέγιστος κοινός διαιρέτης τους είναι το 2.

3. Αρκεί να αποδείξω ότι $p = gcd(2^a - 1, 2^b - 1)$ είναι πρώτοι μεταξύ τους.Οι αριθμοί $2^a - 1, 2^b - 1$ είναι περιττοί άρα όλοι οι παράγοντες τους και επομένως και το p είναι περιττοί αριθμοί. Έχω ότι:

$$p|2^a - 1, \quad p|2^b - 1 \Rightarrow p|2^a - 2^b - 2, \quad p|2^a + 2^b$$

4. Από το προηγούμενο ερώτημα συμπεράναμε ότι άν $gcd(a, b) = 1 \Rightarrow gcd(2^a - 1, 2^b - 1) = 1$. Για το ζητούμενο αρκεί να αποδείξουμε ότι gcd(p, q) = 1 κάτι που ισχύει αφού όλοι οι πρώτοι αριθμοί είναι και πρώτοι με όλους τους άλλους ακέραιους άρα και $gcd(M_p, M_q) = 1$.

8 ΄Ασκηση 3.39

Για να βρούμε το άθροισμα τον θετικών διαιρετών ενός αριθμού ξεκινάμε από το 2 μέχρι την τιμή της ρίζας του και ελέγχουμε αν το υπόλοιπο της διαίρεσης είναι μηδέν. Σε αυτήν την περίπτωση κρατάμε τον διαιρέτη και το πηλίκο και τα προσθέτουμε στο άθροισμα των διαιρετών. Έπειτα, ελέγχουμε για κάθε ακέραιο στο διάστημα $[2, 10^7]$ αν ισχύει η ανισότητα $\sigma(n) > e^{\gamma} n \ln(\ln n)$, με τον μεγαλύτερο

αριθμό για τον οποίο αληθεύει να είναι ο 5040.

9 ΄Ασκηση 3.74

Έχουμε το σύστημα:

$$\begin{cases} 2x \equiv 1 \pmod 5 \\ 3x \equiv 9 \pmod 6 \\ 4x \equiv 1 \pmod 7 \\ 5x \equiv 9 \pmod{11} \end{cases}$$

Έστω ότι $n_1 = 1, n_2 = 9, n_3 = 1, n_4 = 9$ και $m_1 = 5, m_2 = 6, m_3 = 7, m_4 = 11$ άρα $M = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 2310$ και $M_1 = \frac{M}{m_1} = 462, M_2 = \frac{M}{m_2} = 385, M_3 = \frac{M}{m_3} = 330, M_4 = \frac{M}{m_4} = 210$, με όλα τα ζεύγη των m να είναι πρώτοι μεταξύ τους άρα μπορώ να εφαρμόσω το κινέζικο θεώρημα υπολοίπων. Επομένως έχω ότι:

$$x = \sum_{i=1}^{4} M_i v_i n_i = 462 \cdot v_1 \cdot 1 + 385 \cdot v_2 \cdot 9 + 330 \cdot v_3 \cdot 1 + 210 \cdot v_4 \cdot 9 \tag{9.1}$$

Βρίσκω τα $v_i = M_i^{-1} \pmod{m_i}$ από τον ευκλείδειο αλγόριθμο με τιμές $v_1 = 3, v_2 = 1, v_3 = 1, v_4 = 1$. Αντικαθιστώντας στην (6.1) έχουμε:

$$x = 462 \cdot 3 \cdot 1 + 385 \cdot 1 \cdot 9 + 330 \cdot 1 \cdot 1 + 210 \cdot 1 \cdot 9 = 7071 \pmod{2310} = 141 \tag{9.2}$$

10 ΄Ασκηση 4.41

Βρίσκω αρχικά τον αριθμό Fibonacci F_{104911} και αφού υλοποιήσω τον αλγόριθμο Miller-Rabin φτιάχνω μία συνάρτηση που να υπολογίζει γρήγορα μεγάλες δυνάμεις με modulo χρησιμοποιώντας την δεξιά προς τα αριστερά δυαδική μέθοδο και α-

ποδεικνύεται ότι ο αριθμός που ελέγχω είναι πράγματι πρώτος.

11 ΄Ασκηση 4.46

Παράγω αρχικά με τη βοήθεια της βιβλιοθήκης random τυχαίους αριθμούς και θέτω το πρώτο και το τελευταίο δυαδικό στοιχείο τους ίσο με την μονάδα ώστε να είναι περιττοί και μήκους 2048 bit. Έστω p ένας τυχαίος αριθμός, θα ελέγξω στην περίπτωση που είναι πρώτος, αν και κάποιος από τους $q = 2*p+1, z = (p-1)/2$ είναι και αυτοί πρώτοι άρα και θα έχω ένα ζεύγος Sophie-Germain πρώτων. Ελέγχω πρώτα με ένα fermat test αν οι αριθμοί είναι πρώτοι λόγω υψηλότερης ταχύτητα και μετά επαληθεύω με το τεστ Miller-Rabin αξιωποιώντας και την ιδιότητα του lazy evaluation της python για καλύτερη απόδοση.

12 ΄Ασκηση 6.3

Εφόσον το N είναι μικρό μπορούμε να το παραγοντοποιήσουμε βρίσκοντας έτσι τους πρώτους p,q άρα και το φ(N). Έπειτα, από την ισοδυναμία $e \cdot d \equiv 1 \pmod{\varphi(N)}$ και έχοντας το e βρίσκουμε το ιδιωτικό κλειδί d και εύκολα αποκρυπτογραφούμε το μήνυμα καταλήγοντας στην έκφραση "welcowe to the real world".

13 ΄Ασκηση 6.5

Έστω $p = 5, q = 11, N = 55, c = 14$, τότε:

$$F^{-1}(sk, y) : x^2 \equiv 15 \pmod{55}$$

Λύνω το σύστημα:

$$\begin{cases} x^2 \equiv 4 \pmod 5 = 4 \\ x^2 \equiv 14 \pmod{11} = 3 \end{cases}$$

Η τετραγωνική ρίζα του $4 \pmod 5$ είναι το 2, ενώ του $3 \pmod{11}$ το 5, άρα λύνω το σύστημα:

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod{11} \end{cases}$$

Εφαρμόζω το Κινέζικο Θεώρημα αφού οι 5 και 11 είναι πρώτοι μεταξύ τους και έχω:

$$\begin{aligned} &m = 55, m_1 = 5, m_2 = 11, M_1 = \frac{m}{m_1} = 11, M_2 = \frac{m}{m_2} = 5, \\ &v_1 \equiv M_1^{-1} \pmod{m_1} = 1 \pmod 5, \\ &v_2 \equiv M_2^{-1} \pmod{m_2} = 9 \pmod{11} \end{aligned}$$

Άρα έχουμε τις τέσσερις πιθανές λύσεις που δίνονται από τον τύπο:

$$x \equiv (\pm 2 \cdot M_1 \cdot v_1 \pm 5 \cdot M_2 \cdot v_2) \pmod{55} = 23, \mathbf{12}, 22, 43$$

Αλλά ξέρουμε ότι ισχύει $m < 20$ άρα $m = 12$.

14 Άσκηση 7.2

Βρίσκω αρχικά το ιδιωτικό κλειδί με τιμή 20882 από την επίθεση Wiener. Στη συνέχεια, αποκρυπτογραφώ το μήνυμα που είναι σε μορφή base64 που μου δίνει ένα string. Αφού υποστεί επεξεργασία δίνεται μία σειρά από κρυπτογραφημένα με

RSA νούμερα τα οποία εύκολα μπορούμε να αποκρυπτογραφήσουμε αφού έχουμε το ιδιωτικό κλειδί από πριν, καταλήγοντας στο μήνυμα “ Just because you are a character doesn’t mean that you have character”.

15 ΄Ασκηση 10.1

Για την παραγωγή ενός ζεύγους δημόσιου/ιδιωτικού κλειδιού χρησιμοποιούμε την παρακάτω εντολή και ακολουθούμε τις οδηγίες που μας δίνονται:

```
gpg --gen-key
```

Για να δούμε όσα κλειδιά έχουμε στην διάθεση μας:

```
gpg --list-keys
```

Για να εξάγουμε ένα δημόσιο κλειδί ώστε να το διανέμουμε εκτελούμε την εντολή:

```
gpg --export recipient@gmail.com > pubkey.asc
```

Για να εισάγουμε το δημόσιο κλειδί που έχουμε λάβει από κάποιον άλλο κάνουμε:

```
gpg --import pubkey.asc
```

Για την κρυπτογράφηση ενός μηνύματος:

```
gpg --encrypt --recipient recipient@gmail.com message.txt
```

Για την αποκρυπτογράφηση ενός μηνύματος:

```
gpg --decrypt message.txt.gpg
```