Συναρτήσεις & Κέρματα

1. Η Πέππα και η Σούζυ έχουν δύο κέρματα, ένα σωστά φτιαγμένο (με πιθανότητα να φέρει 1 ίση με $p = \frac{1}{2}$), και ένα ελατωματικό, με πιθανότητα να φέρει 1 ίση με πιθανότητα $q \neq \frac{1}{2}$. Δυστυχώς, καθώς έπαιζαν, τα δύο κέρματα μπλέχτηκαν ώστε δεν μπορούν πλέον να ξεχωρίσουν ποιό είναι ποιό. Υπάρχει τρόπος ώστε να διεξάγουν ρίψεις ώστε το αποτέλεσμα να είναι ίσο με 1 με πιθανότητα ακριβώς $\frac{1}{2}$;

2. Σε μία συσκευή υπάρχει μια γεννήτρια τυχαίων αριθμών η οποία σε κάθε κλήση επιστρέφει ένα τυχαίο bit. Στις προδιαγραφές της συσκευής, η γεννήτρια επιστρέφει 1 με πιθανότητα $\frac{1}{2}$.

   Δυστυχώς, για λόγους κόστους, ο Βασίλης προμηθεύτηκε συσκευές Β΄ διαλογής, στις οποίες η γεννήτρια επιστρέφει 1 με πιθανότητα $\frac{1}{2} + \delta$, όπου $0 < \delta < \frac{1}{2}$.

   (α΄) Ο Βασίλης πιστεύει ότι μπορεί να βελτιώσει την συμπεριφορά της γεννήτριας εάν κάθε φορά που χρειάζεται ένα bit καλεί τη γεννήτρια δύο φορές και κάνει XOR τα αποτελέσματα. Εξηγήστε τι σημαίνει «βελτιώσει» τη συμπεριφορά, και εξετάστε (αυστηρά) αν η διαίσθηση του Βασίλη είναι σωστή.

3. Στο παράδειγμα που εξετάσαμε στο μάθημα, θεωρήσαμε ότι αρκεί μονάχα η Αλίκη να χρησιμοποιήσει σχήμα δέσμευσης για το μηνυμά της –αφού μιλάει πρώτη, ενώ ο Βασίλης δεν χρειάζεται.

   Ο Βασίλης προτείνει για λόγους συμμετρίας να στέλνει και αυτός μια δέσμευση αντί για το αρχικό μήνυμα του, και αναλόγως να προστεθεί ένας τέταρτος γύρος στον οποίο «ανοίγει» τη δεσμευσή του.

   Είναι ασφαλής η παραλλαγή του Βασίλη;

   Υπόδειξη. Θεωρήστε ότι η Αλίκη κερδίζει το παιχνίδι όταν το αποτέλεσμα είναι 1.

   Σημείωση. Ακόμα δεν έχουμε δει αυστηρά τη σύνταξη ενός σχήματος δέσμευσης, οπότε μπορείτε να χρησιμοποιήσετε ένα απλουστευμένο υποθετικό σχήμα όπου το $Com(a) \to (c, r)$ παράγει μια δέσμευση c στην τιμή a και μια απόδειξη r, ενώ το $Ver(a, c, r) \to \{0, 1\}$ ελέγχει εάν πράγματι το c περιέχει το a με βάση το r.

4. Να υπολογίσετε το $123^{2022} \mod 23$.

5. Να υπολογίσετε (προσεγγιστικά) το $\log_{10}(12345678901234567890123456789 0)$ καθώς και το $\log_2(12345678901234567890123456789 0)$. Δίνεται ότι $\log_2(10) \approx 3.3$

6. Να υπολογίσετε το $\log_2 5 \mod 37$. Χρησιμοποιείστε τον αλγόριθμο Baby step, Giant step, ο οποίος δίνεται παρακάτω.

   Στον αλγόριθμο Baby step, Giant step, θέλουμε να λύσουμε την εξίσωση $g^x = h \mod p$ «σπάζοντας» τον άγνωστο λογάριθμο $0 \leq x < p - 1$ σε $x = b + S \cdot G$, όπου $S = \lceil \sqrt{(p-1)} \rceil$ και $b, G \leq S$.

   Για να το κάνουμε αυτό, ξαναγράφουμε την εξίσωση ως $g^{S \cdot B} \equiv h \cdot g^{-b}$, με αγνώστους το B και το b. Έτσι, μπορούμε να εξαντλήσουμε όλες τις περιπτώσεις, με $2S$ υπολογισμούς (και $O(n \log n)$ συγκρίσεις για ταξινόμιση), αντί τους $p - 1 = S^2$ υπολογισμούς της προφανούς λύσης.

   Παρατήρηση. Επειδή το 37 είναι πρώτος και $37 - 1 = 36$, η τάξη της πολλαπλασιαστικής ομάδας του $\mathbb{Z}_{37}^*$ είναι 36. Η τάξη του 2 ξέρουμε ότι διαιρεί το 36 και άρα υπάρχουν πολλές μη τετριμμένες περιπτώσεις για την τάξη του. Σε περίπτωση που η τάξη του 2 δεν είναι 36, τότε δεν παράγει όλη την ομάδα, άρα ενδέχεται το 5 να μην εμφανιστεί ως δυναμή του, και ο ζητούμενος λογάριθμος να μην υπάρχει.