Ομάδες & 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. Να δείξετε ότι το σύνολο των συμβολοσειρών μήκους 2 bit ("00","10","01","11",), με πράξη το XOR κατά συντεταγμένη, αποτελεί ομάδα.

3. Να δείξετε ότι η παραπάνω ομάδα είναι μεταθετική αλλά όχι κυκλική.

4. Να υπολογίσετε το $123^{2021} \mod 23$.

5. Να υπολογίσετε (προσεγγιστικά) το $\log_{10}(1234567890123456789012345678890)$ καθώς και το $\log_2(1234567890123456789012345678890)$. 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.