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 $\frac{1}{2}$;

   Λύση: Έστω $\Pr[b_A = 1] = p$ και $\Pr[b_B = 1] = q$.

   Από τον πίνακα αληθείας της αποκλειστικής διάζευξης έχουμε ότι $\Pr[b = 1] = \Pr[b_A = 1 \wedge b_B = 0] + \Pr[b_A = 0 \wedge b_B = 1]$. Άρα: $\Pr[b = 1] = p \cdot (q-1) + (p-1) \cdot q = p \cdot q - p + p \cdot q - q = 2p \cdot q - p - q$.

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

   Λύση Ελέγχουμε ότι οι ιδιότητες της ομάδας ισχύουν:

   - Έστω ένα ζεύγος συμβολοσειρών "ab", "cd". Το αποτέλεσμα της πράξης μεταξύ τους θα είναι "ef" όπου $e = a$ XOR c και $f = b$ XOR d. Με έλεγχο του πίνακα τιμών της XOR επιβεβαιώνουμε ότι το XOR δύο bits είναι bit, οπότε θα ισχύει ότι το e και το f είναι bits.
   - Η μεταθετικότητα της ομάδας προκύπτει από το ότι το XOR είναι μεταθετικό, και η ιδιότητα διατηρείται κάνοντας πράξεις ανα συντεταγμένη (όπως παραπάνω)
   - Υπάρχει ουδέτερο στοιχείο και είναι το "00", αφού ισχύει ότι a XOR $0 = a$, και η ιδιότητα διατηρείται κάνοντας πράξεις ανα συντεταγμένη (όπως παραπάνω).

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

   Λύση

   - Η μεταθετικότητα της ομάδας προκύπτει από το ότι το XOR είναι μεταθετικό.
   - Η ομάδα δεν είναι κυκλική: για κάθε συμβολοσειρά bits ισχύει ότι το XOR με τον εαυτό της παράγει μηδενικά. Άρα κάθε στοιχείο έχει τάξη το πολύ 2 $neq4$, οπότε δεν υπάρχει στοιχείο που να παράγει την ομάδα.

4. Να υπολογίσετε το $123^{2020} \mod 23$.

   Λύση: Στη βάση εργαζόμαστε modulo 23 και, αφού ο p είναι πρώτος, λόγω του ΜΘF στον εκθέτη εργαζόμαστε modulo $23 - 1 = 22$. Άρα έχουμε $123^{2020} \equiv 8^{2020} \equiv 8^{40} \equiv 8^{18} \mod 23$. Συνεχίζουμε γράφοντας $8^{18} \equiv 2^{54} \equiv 2^{10} \equiv 32^2 \equiv 9^2 \equiv 81 - 69 \equiv 12 \mod 23$

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

   Λύση: Το 12345678901234567890123456789 0 γράφεται: $1 \cdot 10^{29} + 2 \cdot 10^{28} + \ldots + 9 \cdot 10^1 + 0 \approx 10^{29}$, άρα ο λογαριθμός του με βάση το 10 είναι περίπου 29. Για το λογάριθμο με βάση το 2 εφαρμόζουμε τον τύπο αλλαγής βάσης όπου $log_b(a) = log_c(a) \cdot log_c(b)$, άρα έχουμε $\log_2(12345678901234567890123456789 0) \approx 29 \cdot 3.3 = 95.7$. (Ο κανονικός υπολογισμός δίνει τιμή περίπου 96.64).

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

   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 $b, G \leq S$.

   Έπειτα, ξαναγράφουμε την εξίσωση ως $g^{S \cdot B} \equiv h \cdot g^{-b}$. 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.

Λύση:

Παρατήρηση. Εμείς μπορούμε είτε να εξετάσουμε την τάξη του 2 πριν αρχίσουμε τους υπολογισμούς, είτε να τους κάνουμε γνωρίζοντας ότι ενδεχομένως δε θα προκύψει λύση. Για να ελέγξουμε την τάξη μπορούμε να δοκιμάσουμε τους διαιρέτες του 36: 2,3,4,6,9,12,18. Για συντομία, αρκεί να επιβεβαιώσουμε ότι $2^{12} \equiv 100 \equiv 26 \neq 1 \mod 37$ και $2^{18} \equiv -1 \neq 1 \mod 37$. (Οι πράξεις αναλυτικότερα βρίσκονται παρακάτω).

Αφού το 37 είναι πρώτος, η ομάδα μας έχει τάξη 36. Έστω x ο ζητούμενος λογάριθμος, τότε ο x θα γράφεται ως $b + G \cdot 6$ με $b, G \leq 5$. Οπότε θέλουμε να λύσουμε την εξίσωση $2^{b+6G} = 5 \mod 37$, ή ισοδύναμα: $2^b = 5 \cdot 2^{(-6)\cdot G}$.

Ετοιμάζουμε τις δυνάμεις του 2^6.

- Για $G = 0$ έχουμε $2^{6G} \equiv 1 \mod 37$
- Για $G = 1$ έχουμε $2^{6G} \equiv 64 \equiv -10 \equiv 27 \mod 37$ (Αφαιρούμε το $37 \cdot 2 = 74$ για να πάρουμε -10. Ως αποτέλεσμα κρατάμε το 26 που είναι ο αντιπρόσωπος της κλάσσης, αλλά όποτε εξυπηρετεί στις πράξεις το υπολογίζουμε και ως -10).
- Για $G = 2$ έχουμε $2^{6G} \equiv 64^2 \equiv (-10)^2 \equiv 100 \equiv -11 \equiv 26 \mod 37$ (Αρχίζουμε θεωρώντας στο 26 ως -10 για ευκολία στις πράξεις. Μετά αφαιρούμε $3 \cdot 37 = 111$.)
- Για $G = 3$ έχουμε $2^{6G} \equiv -10 \cdot (-11) \equiv 110 \equiv -1 \equiv 36 \mod 37$
- Για $G = 4$ έχουμε $2^{6G} \equiv -10 \cdot -1 \equiv 10 \mod 37$
- Για $G = 5$ έχουμε $2^{6G} \equiv -11 \cdot -1 \equiv 11 \mod 37$

Για να υπολογίσουμε τα πολλαπλάσια του 2^{-1}, πρώτα εκτελούμε την αντιστροφή: είτε υψώνουμε στην 35η είτε χρησιμοποιούμε ευκλείδια διαίρεση. Με την Ευκλείδια διαίρεση, έχουμε:

$$\begin{aligned} 37 &= 18 \cdot 2 + 1 \\ 1 &= 37 + (-18) \cdot 2 \\ 1 &\equiv 0 + (-18) \cdot 2 \mod 37 \end{aligned}$$

Άρα, ο αντίστροφος του 2 είναι ο $-18 \equiv 19$ και συνεχίζουμε με τις δυνάμεις του 19.

- Για $b = 0$ έχουμε $19^b \equiv 1 \mod 37$
- Για $b = 1$ έχουμε $19^b \equiv 19 \mod 37$
- Για $b = 2$ έχουμε $19^b \equiv 19 \cdot 19 \equiv 361 \equiv 361 - 370 \equiv -9 \equiv 28 \mod 37$.
- Για $b = 3$ έχουμε $19^b \equiv 19 \cdot (-9) \equiv -171 \equiv 185 - 171 \equiv 14 \mod 37$. (Χρησιμοποιούμε το ότι $37 \cdot 5 = 185$).
- Για $b = 4$ έχουμε $19^b \equiv (-9) \cdot (-9) \equiv 81 \equiv 81 - 74 \equiv 7 \mod 37$.
- Για $b = 5$ έχουμε $19^b \equiv (14) \cdot (-9) \equiv 148 - 126 \equiv 22 \mod 37$. (Χρησιμοποιούμε το ότι $37 \cdot 4 = 148$)

Έπειτα, πολλαπλασιάζουμε τις δυνάμεις του 19 επί 5.

- Για $b = 0$ έχουμε $5 \cdot 19^b \equiv 5 \mod 37$
- Για $b = 1$ έχουμε $5 \cdot 19^b \equiv 5 \cdot 19 \equiv 95 - 74 \equiv 21 \mod 37$
- Για $b = 2$ έχουμε $5 \cdot 19^b \equiv 5 \cdot 28 \equiv 140 - 111 \equiv 29 \mod 37$.
- Για $b = 3$ έχουμε $5 \cdot 19^b \equiv 5 \cdot 14 \equiv 70 - 37 \equiv 33 \mod 37$.
- Για $b = 4$ έχουμε $5 \cdot 19^b \equiv 5 \cdot 7 \equiv 35 \mod 37$.
- Για $b = 5$ έχουμε $5 \cdot 19^b \equiv 5 \cdot 22 \equiv 110 - 74 \equiv 36 \mod 37$.

Συγκρίνοντας τις λίστες, βλέπουμε ότι για $G = 3, b = 5$ έχουμε και στις δύο, την τιμή 36. Δηλαδή:

$$2^{18} \equiv 5 \cdot 2^{-5} \mod 37 \quad \text{οπότε,}$$
$$2^{23} \equiv 5 \mod 37$$