Υπολογιστική Κρυπτογραφία
2η Σειρά Ασκήσεων

Μαραβίτσας Παναγιώτης
Α.Μ: 03116206

26 Νοεμβρίου 2020

Περιεχόμενα

Άσκηση 1

Καταρχάς, μια υποομάδα της $\mathbb{Z}_{29}^*$ είναι η τετριμμένη υποομάδα $< 1 >= \{1\}$. Στη συνέχεια γνωρίζουμε ότι η $\mathbb{Z}_{29}^*$ είναι κυκλική αφού ο αριθμός 29 είναι πρώτος οπότε αναζητούμε κάποιο γεννήτορα. Έστω g $\in U(\mathbb{Z}_{29})$. Αν το g είναι γεννήτορας τότε ισχύει πως $g^{|\mathbb{Z}_{29}^*|} = g^{28} = 1 \pmod{29}$ ενώ για κάθε $d \in U(\mathbb{Z}_{29})$ τέτοιο ώστε $d|28$ και $d < 28$ ισχύει πως $g^d \neq 1 \pmod{29}$. Επομένως προσπαθούμε με δοκιμές να εντοπίσουμε κάποιον αριθμό που ικανοποιεί τα παραπάνω. Έτσι προκύπτει πως το 2 είναι γεννήτορας της $\mathbb{Z}_{29}^*$. Έχοντας εντοπίσει έναν γεννήτορα μπορούμε εύκολα να βρούμε γεννήτορες για όλες τις υπόλοιπες υποομάδες. Συγκεκριμένα εκμεταλλευόμαστε το γεγονός πως αν g γεννήτορας μιας ομάδας G, τότε το στοιχείο g^r είναι γεννήτορας μίας ομάδας με $\frac{|G|}{gcd(r,|G|)}$ στοιχεία. Έτσι για την εύρεση γεννήτορα μιας υποομάδας με k (πρέπει ο k να διαιρεί το $|G|$) στοιχεία αρκεί να βρούμε κάποιο r τέτοιο ώστε $gcd(r, |G|) = \frac{|G|}{k}$. Για παράδειγμα έστω ότι ψάχνουμε κάποιο γεννήτορα της υποομάδας με 7 στοιχεία στην ομάδα $\mathbb{Z}_{29}^*$. Τότε το στοιχείο $2^4 \pmod{29}$ είναι γεννήτορας αφού $gcd(4, 28) = 4 = \frac{28}{7}$ και προκύπτει η υποομάδα $H = \{2^{4i} | i \in \mathbb{Z}\}$. Ομοίως προκύπτουν και οι υπόλοιπες υποομάδες. Συγκεντρωτικά έχουμε:

- 1 στοιχείο: $< 1 >= \{1\}$
- 2 στοιχεία: $< 28 >= \{1, 28\}$
- 4 στοιχεία: $< 12 >= \{1, 12, 17, 28\}$
- 7 στοιχεία: $< 16 >= \{1, 7, 16, 20, 23, 24, 25\}$
- 14 στοιχεία: $< 4 >= \{1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28\}$
- 28 στοιχεία: $< 2 >= \{1, 2, ..., 28\}$

Άσκηση 2

1ος τρόπος

Από το κινέζικο θεώρημα υπολοίπων έχουμε ότι:

$$\mathbb{Z}_{77}^* \cong \mathbb{Z}_7^* \times \mathbb{Z}_{11}^*$$

Αν f είναι αυτός ο ισομορφισμός τότε:

$$f(25) = (25 \bmod 7, 25 \bmod 11) = (4, 3)$$

Τώρα είναι εύκολο να δούμε ποιος είναι ο αντίστροφος αφού:

$$(4,3)^{-1} = (4^{-1} \bmod 7, 3^{-1} \bmod 11) = (2, 4)$$

Ο υπολογισμός του $f^{-1}((4,3))$ μπορεί να γίνει εύκολα. Αρκεί να λύσουμε το σύστημα:

$$x = 2 \pmod 7$$
$$x = 4 \pmod{11}$$

Η λύση μπορεί να βρεθεί μέσω του κινέζικου θεωρήματος υπολοίπων. Συγκεκριμένα: $M_1 = 11, M_2 = 7, N_1 = 2, N_2 = 8, a_1 = 2, b_2 = 4$. Η λύση του συστήματος τελικά είναι:

$$y = \sum_{i=1}^{2} N_i M_i a_i = 37 \pmod{77}$$

2ος τρόπος

Ο αντίστροφος μπορεί να βρεθεί και μέσω του επεκτεταμένου αλγορίθμου του Ευκλείδη. Συμβολίζουμε κάθε βήμα της εκτέλεσης του αλγορίθμου με ένα tuple $(x, y, x_1, x_2, y_1, y_2)$, έτσι ώστε σε κάθε βήμα ισχύει πως $x = 25x_1 + 77x_2$ και $y = 25y_1 + 77y_2$. Υπολογίζοντας το gcd(25,77) με τον επεκτεταμένο αλγόριθμο του Ευκλείδη έχουμε πως:

$$(25, 77, 1, 0, 0, 1) \vdash (25, 2, 1, 0, -3, 1) \vdash (1, 2, 37, -12, -3, 1) \vdash (1, 0, 37, -12, -77, 25)$$

Επομένως προκύπτει:

$$1 = 37 \cdot 25 - 12 \cdot 77 \implies 1 = 37 \cdot 25 \pmod{77}$$

Άρα ο 37 είναι ο αντίστροφος του 25 (mod 77).

Άσκηση 3

α

Έστω κυκλική ομάδα G με γεννήτορα g. Έστω H υποομάδα της G.
Αν $H =< e >$, τότε η H είναι κυκλική. Έστω $H \neq< e >$ και i ο ελάχιστος θετικός ακέραιος ώστε $g^i \in H$. Θα δείξουμε ότι $H = \{g^{ik}|k \in \mathbb{Z}\}$. Έστω κάποιο $h \in H$. Αφού $h \in H$, $H \leq G$ και G κυκλική τότε υπάρχει κάποιο j τέτοιο ώστε $h = g^j$. Από τον αλγόριθμο της διαίρεσης έχουμε:

$$\exists q, r \in \mathbb{Z} : j = qi + r, r < i$$

Όμως τότε για το στοιχείο h έχουμε:

$$h = g^j = g^{qi+r} = (g^i)^q g^r \implies g^r = (g^i)^{-q} h$$

Αφού $g^i, h \in H$, τότε $g^r \in H$, όμως ο i ήταν ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $g^i \in H$, άρα $r = 0$ και το τυχαίο στοιχείο h παράγεται από το g^i, άρα το g^i είναι γεννήτορας της H και η H είναι κυκλική.

β

Ο αριθμός 4872961 είναι πρώτος, συνεπώς η ομάδα $U(\mathbb{Z}_{4872961})$ είναι κυκλική με τάξη $|U(\mathbb{Z}_{4872961})| = 4872960$. Επίσης για κάθε d|4872960 υπάρχει μοναδική υποομάδα τάξης d, συνεπώς το πλήθος των υποομάδων ταυτίζεται με το πλήθος των διαιρετών του 4872960. Αν $N = \prod_{i=1}^{q} p_i^{a_i}$, όπου p_i πρώτος για κάθε i, τότε το πλήθος των διαιρετών του N είναι $\prod_{i=1}^{q}(a_i + 1)$. Παραγοντοποιώντας έχουμε ότι $4872960 = 2^8 \cdot 3^4 \cdot 5 \cdot 47$, όποτε η ομάδα $U(\mathbb{Z}_{4872961})$ έχει $(8+1)\cdot(4+1)\cdot(1+1)\cdot(1+1) = 180$ υποομάδες.

Άσκηση 4

Ο έλεγχος Fermat στηρίζεται στο γεγονός πως αν ο N είναι πρώτος αριθμός, τότε:

$$\forall a \in \mathbb{Z}_N : a^{N-1} = 1(\text{mod N})$$

Προκειμένου να αποδείξουμε την ορθότητα του αλγορίθμου εισάγουμε την έννοια των μαρτύρων, δηλαδή στοιχείων τα οποία δεν ικανοποιούν την παραπάνω σχέση (προφανώς υπάρχουν μόνο αν ο N δεν είναι πρώτος). Αποδεικνύεται εύκολα πως οι μη μάρτυρες αποτελούν υποομάδα του $\mathbb{Z}_N^*$. Αν για κάποιο N υπάρχει έστω και ένας μάρτυρας τότε η ομάδα των μη μαρτύρων αποτελεί γνήσια υποομάδα του $\mathbb{Z}_N^*$ και συνεπώς περιέχει το πολύ $\frac{N}{2}$ στοιχεία. Επομένως αν κάποιος αριθμός N δεν ανήκει στην κατηγορία των Carmichael Numbers, δηλαδή μη πρώτων αριθμών χωρίς μάρτυρες τότε η πιθανότητα να επιλέξουμε ένα τυχαίο στοιχείο $a \in \mathbb{Z}_N$ και να είναι μάρτυρας είναι τουλάχιστον $\frac{1}{2}$. Εκτελώντας λοιπόν τον έλεγχο Fermat t φορές, η πιθανότητα να μην διαλέξουμε τυχαία κάποιο μάρτυρα είναι το πολύ $\frac{1}{2^t}$, δηλαδή αμελητέα ως προς το t.

Τα αποτελέσματα για τους συγκεκριμένους αριθμούς είναι:

- 67280421310721: πρώτος
- 170141183460469231731687303715884105721: σύνθετος
- $2^{2281} - 1$: πρώτος
- $2^{9941} - 1$: πρώτος
- $2^{19939} - 1$: σύνθετος

Ο κώδικας επισυνάπτεται.

Άσκηση 5

Καταρχάς παρατηρούμε πως ο εκθέτης του αριθμού που πρέπει να υπολογίσουμε είναι υπερβολικά μεγάλος για να χρησιμοποιήσουμε επαναλαμβανόμενο τετραγωνισμό. Συνεπώς πρέπει να εκμεταλλευτούμε το θεώρημα του Euler, σύμφωνα με το οποίο αν οι αριθμοί α,m είναι σχετικά πρώτοι τότε:

$$a^{\phi(m)} \equiv 1 \text{ (mod m)}$$

Ένα άμεσο πόρισμα του παραπάνω θεωρήματος είναι πως αν οι αριθμοί α,m είναι σχετικά πρώτοι τότε:

$$a^n \equiv a^{n \bmod \phi(m)} \pmod{m}$$

Έχοντας χρησιμοποιήσει το θεώρημα αυτό, ο εκθέτης μπορεί εύκολα να υπολογιστεί με επαναλαμβανόμενους τετραγωνισμούς. Ο ζητούμενος υπολογισμός μπορεί να γραφτεί ως:

$$Z^{a^b} \bmod 10^M$$

όπου Z,M το input του χρήστη, $a = 1998000$, $b = 100^{10}$. Το πρόβλημα τώρα έγγυται στο γεγονός πως οι αριθμοί Z και 10^M μπορεί και να μην είναι σχετικά πρώτοι. Παρατηρούμε πως το πρόβλημα δημιουργείται μόνο αν το Z έχει ως παράγοντες τους αριθμούς 2,5. Έτσι μπορούμε να το γράψουμε ως

$$Z = 2^{a_1} 5^{a_2} c$$

με $a_1, a_2 \geq 0$ και $gcd(c, 10^M) = 1$ και να υψώσουμε τον κάθε όρο στη δύναμη a^b ξεχωριστά. Ο ζητούμενος υπολογισμός γίνεται λοιπόν:

$$(2^{a_1})^{a^b} (5^{a_2})^{a^b} c^{a^b} \bmod 10^M = 2^{a_1 a^b} 5^{a_2 a^b} c^{a^b} \bmod 10^M$$

Έχουμε ότι $gcd(c, 10^M) = 1$, άρα

$$c^{a^b} \bmod 10^M = c^{a^b \bmod \phi(10^M)} \bmod 10^M$$

. Τώρα για τον υπολογισμό των άλλων δύο παραγόντων χρησιμοποιούμε την ιδιότητα:

$$x = y \bmod m \implies xz = yz \bmod mz$$

Έστω λοιπόν d ο ελάχιστος ακέραιος ώστε $gcd(\frac{2^{a_1 a^b}}{2^d}, \frac{M}{2^d}) = 1$ Τότε:

$$2^{a_1 a^b} \bmod 10^M = 2^d (2^{a_1 a^b - d} \bmod \frac{10^M}{2^d}) \bmod 10^M = 2^d (2^{(a_1 a^b - d) \bmod \phi(\frac{10^M}{2^d})} \bmod \frac{10^M}{2^d}) \bmod 10^M$$

Πλέον ο παραπάνω υπολογισμός μπορεί να γίνει εύκολα με επαναλαμβανόμενους τετραγωνισμούς και με ακριβώς όμοιο τρόπο μπορεί να υπολογιστεί και ο όρος $5^{a_2 a^b} \bmod 10^M$

Τελικά για M=3 και Z=548 ο Ρατταταkιανός θα χρειαστεί 376 πλεξοδευτερόλεπτα.

Ο κώδικας επισυνάπτεται.

Άσκηση 6

1.

Θα αποδείξουμε πως αν G είναι μια κυκλική ομάδα με $|G| = N$ και g είναι ένας γεννήτορας της G, τότε το στοιχείο g^r παράγει μια κυκλική υποομάδα τάξης $\frac{|N|}{gcd(r,N)}$. Έστω ότι η υποομάδα που παράγεται έχει τάξη k. Τότε ο N είναι ο ελάχιστος φυσικός αριθμός τέτοιος ώστε:

$$(g^r)^k = g^{rk} = e$$

. Τότε πρέπει $N|rk$. Έστω $m = gcd(r, N)$. Άρα έχουμε ότι το m είναι το ελάχιστο θετικό στοιχείο του συνόλου $\{\kappa r + \lambda N | \kappa, \lambda \in \mathbb{Z}\}$. Επομένως:

$$\exists \kappa, \lambda \in \mathbb{Z} : m = \kappa r + \lambda N$$

Αφού $m = gcd(r, N)$ έχουμε ότι

$$\kappa \frac{r}{m} + \lambda \frac{N}{m} = 1$$

Ψάχνουμε το ελάχιστο k ώστε $\frac{rk}{N} = \frac{k\frac{r}{m}}{\frac{N}{m}}$ να είναι ακέραιος. Από την παραπάνω σχέση οι αριθμοί $\frac{r}{m}$ και $\frac{N}{m}$ είναι σχετικά πρώτοι οπότε πρέπει $\frac{N}{m}|k$. Ο ελάχιστος αριθμός k ώστε να ισχύει η παραπάνω σχέση είναι $k = \frac{N}{m}$. Συνεπώς:

$$| < g^r > | = \frac{|G|}{gcd(r, |G|)}$$

Θέλουμε αποδοτικά να βρούμε ένα στοιχείο τάξης d, δηλαδή ένα γεννήτορα μιας κυκλικής υποομάδας με d στοιχεία. Χρησιμοποιώντας το παραπάνω ψάχνουμε κάποιο r τέτοιο ώστε:

$$\frac{p-1}{gcd(r, p-1)} = d \implies gcd(r, p-1) = \frac{p-1}{d}$$

Για $r = \frac{p-1}{d}$ η παραπάνω εξίσωση ικανοποιείται και συνεπώς το στοιχείο $g^{\frac{p-1}{d}}$ είναι ένα στοιχείο τάξης d.

2.

Η ομάδα $\mathbb{Z}_p^*$ είναι κυκλική συνεπώς αρκεί να βρούμε τα r για τα οποία η ομάδα $< g^r >$, όπου $g \in G$, είναι τάξης d. Από το προηγούμενο ερώτημα είδαμε ότι ένα στοιχείο $g^r \in \mathbb{Z}_p^*$ είναι τάξης d αν και μόνο αν:

$$gcd(r, p-1) = \frac{p-1}{d}$$

Προφανώς μας ενδιαφέρουν οι τιμές $0 \leq r < p-1$. Το σύνολο των πιθανών λύσεων είναι το:

$$\{\frac{\kappa(p-1)}{d}|0 \leq \kappa < d\}$$

Ισοδύναμα ψάχνουμε τα κ ώστε:

$$gcd(\frac{\kappa(p-1)}{d}, p-1) = \frac{p-1}{d}$$

Αυτό συνεπάγεται πως:

$$\exists u, v \in \mathbb{Z} : u\frac{\kappa(p-1)}{d} + v(p-1) = \frac{p-1}{d} \implies u\kappa + vd = 1 \implies gcd(\kappa, d) = 1$$

Συνεπώς υπάρχουν $\phi(d)$ τέτοια κ, οπότε το πλήθος των στοιχείων τάξης d στην ομάδα $\mathbb{Z}_p^*$ είναι $\phi(d)$.

3.

Ένα στοιχείο b τάξης d παράγει μια κυκλική υποομάδα με d στοιχεία. Επίσης:

$$\forall g \in <b> \exists r \in \{0, 1, \dots, d-1\} : b^r = g$$

Ψάχνουμε το πλήθος των $r \in \{0, 1, \dots, d-1\}$ ώστε $< b^r > = < b >$. Από το ερώτημα 1, ένα στοιχείο $b^r \in < b >$ παράγει μία κυκλική υποομάδα τάξης $\frac{d}{gcd(r,d)}$. Συνεπώς είναι γεννήτορας της ομάδας $< b >$ αν και μόνο αν $gcd(r, d) = 1$ και υπάρχουν $\phi(d)$ τέτοια r στο σύνολο $\{0, 1, \dots, d-1\}$. Άρα η κυκλική υποομάδα που παράγει ένα στοιχείο b τάξης d έχει $\phi(d)$ γεννήτορες.

4.

Από τα ερωτήματα 2,3 έχουμε τα εξής:

1. Το $\mathbb{Z}_p^*$ περιλαμβάνει ακριβώς $\phi(d)$ στοιχεία τάξης d.
2. Μια κυκλική υποομάδα που παράγεται από ένα στοιχείο τάξης d έχει ακριβώς $\phi(d)$ γεννήτορες.

Συνεπώς όλα τα στοιχεία τάξης d της ομάδας $\mathbb{Z}_p^*$ ανήκουν στην ίδια κυκλική υποομάδα, άρα παράγουν την ίδια (και προφανώς μοναδική) κυκλική υποομάδα τάξης d για κάθε $d|p-1$.

5.

Από το θεώρημα του Lagrange έχουμε πως για κάθε κυκλική ομάδα G τάξης n και κάθε στοιχείο $g \in G$, $ord(g)|n$ και $g^n = e$. Αν $h \in G$ και η ομάδα $< h >$ εχει τάξη d τότε για ένα τυχαίο στοιχείο $a \in G$, ισχύει ότι $a \in< h >$ αν και μόνο αν $a^d = 1$. Η μία κατεύθυνση ισχύει απο το παραπάνω. Για την άλλη κατεύθυνση υποθέτουμε ότι m είναι η τάξη του a, δηλαδή ο m είναι ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $a^m = e$. Επίσης γνωρίζουμε ότι $m|d$. Από το ερώτημα 2 γνωρίζουμε ότι τόσο η ομάδα G, όσο και η $< h >$ περιέχουν ακριβώς $\phi(m)$ στοιχεία τάξης m, συνεπώς $a \in< h >$.

Τελικά μπορούμε να βρούμε αν το a ανήκει στην υποομάδα που παράγεται από το h υπολογίζοντας (σε πολυωνυμικό χρόνο) αν $a^d = 1 \pmod p$

Η ύπαρξη αλγορίθμου πολυωνυμικού χρόνου έγγυται στο γεγονός ότι δίνεται η τάξη του h, καθώς και στο γεγονός ότι $h \in \mathbb{Z}_p^*$ αφού η $\mathbb{Z}_p^*$ είναι κυκλική. Σε διαφορετική περίπτωση θα μπορούσαν να υπάρχουν παραπάνω από μία υποομάδες τάξης d.

Άσκηση 7

1.

Ευθύ:
Έστω $d = gcd(k,m)$. Τότε:

$$a^{\frac{km}{d}} = (a^k)^{\frac{m}{d}} = 1,\ b^{\frac{km}{d}} = (b^m)^{\frac{k}{d}} = 1$$

Έστω c η τάξη του ab. Για το στοιχείο ab και χρησιμοποιώντας το γεγονός ότι η ομάδα $U(\mathbb{Z}_n)$ είναι αβελιανή έχουμε:

$$(ab)^{\frac{km}{d}} = a^{\frac{km}{d}} b^{\frac{km}{d}} = 1$$

Συμπερασματικά:

$$c | \frac{km}{gcd(k,m)} = lcm(k,m)$$

Αν λοιπόν $c = km$ τότε:

$$km | \frac{km}{gcd(k,m)} \implies gcd(k,m) = 1$$

Αντίστροφο:
Αφού η τάξη του ab είναι c και η $U(\mathbb{Z}_n)$ είναι αβελιανή έχουμε ότι:

$$(ab)^c = 1 \implies a^c b^c = 1 \implies (a^k)^c b^{kc} = 1 \implies b^{kc} = 1$$

Οπότε έχουμε πως:

$$m | kc \implies \frac{m}{d} | \frac{kc}{d}$$

Όμως:

$$\frac{m}{d} | \frac{kc}{d} \wedge gcd(\frac{m}{d}, \frac{k}{d}) = 1 \implies \frac{m}{d} | c$$

Ομοίως:

$$(ab)^c = 1 \implies a^c b^c = 1 \implies a^{mc}(b^m)^c = 1 \implies a^{mc} = 1$$

$$k | mc \implies \frac{k}{d} | \frac{mc}{d}$$

$$\frac{k}{d} | \frac{mc}{d} \wedge gcd(\frac{k}{d}, \frac{m}{d}) = 1 \implies \frac{k}{d} | c$$

Από τα παραπάνω έχουμε:

$$\frac{m}{d} | c \wedge \frac{k}{d} | c \wedge gcd(\frac{m}{d}, \frac{k}{d}) = 1 \implies \frac{km}{d^2} | c$$

Τελικά έχουμε καταλήξει στη σχέση:

$$\frac{km}{gcd^2(k,m)}|c|\frac{km}{gcd(k,m)}$$

Συνεπώς αν $gcd(k,m) = 1$, τότε η τάξη του ab είναι km, οπότε το αντίστροφο αποδείχτηκε.

Στην απόδειξη χρησιμοποιήθηκε μόνο το γεγονός ότι η $U(\mathbb{Z}_n)$ είναι αβελιανή, συνεπώς ισχύει για κάθε πεπερασμένη αβελιανή ομάδα.

2.

Έστω πεπερασμένη αβελιανή ομάδα G με μέγιστη τάξη στοιχείου m, οπότε:

$$\forall g \in G : ord(g) <= m$$

όπου $ord(g)$ η τάξη του στοιχείου g. Έστω $a \in G$ ένα στοιχείο τάξης m. Τότε από το θεώρημα Lagrange έχουμε:

$$\forall g \in < a >: ord(g)|ord(a)$$

και προφανώς το ίδιο ισχύει για κάθε υποομάδα τάξης m.

Έστω ότι υπάρχει στοιχείο $b \in G$ με $ord(b) = r$, τέτοιο ώστε $r \nmid m$. Παραγοντοποιώντας τους αριθμούς r,m εχουμε:

$$m = \prod_i p_i^{m_i}, r = \prod_i p_i^{r_i}$$

όπου p_i πρώτοι και $m_i, r_i \geq 0$. Με βάση αυτή την παραγοντοποίηση δημιουργούμε τα σύνολα δεικτών:

$$I_1 = \{i : m_i \geq r_i\}, I_2 = \{i : m_i < r_i\}$$

Στη συνέχεια κατασκευάζουμε τους αριθμούς:

$$m' = \prod_{i \in I_1} p_i^{m_i}, r' = \prod_{i \in I_2} p_i^{r_i}$$

Από το ερώτημα 6.1 μπορούμε σε πολυωνυμικό χρόνο να κατασκευάσουμε στοιχεία a', b' με τάξεις m', r' αντίστοιχα. Τα στοιχεία αυτά είναι:

$$a' = a^{\frac{m}{m'}}, b' = b^{\frac{r}{r'}}$$

Επιπλέον είναι προφανές ότι $gcd(m', r') = 1$ συνεπώς από το προηγούμενο ερώτημα έχουμε ότι:

$$ord(a'b') = m'r' = \prod_{i \in I_1} p_i^{m_i} \prod_{i \in I_2} p_i^{r_i} = \prod_i p_i^{max(m_i, r_i)} = lcm(m, r)$$

Τέλος:

$$r \nmid m \implies lcm(m, r) > m \implies ord(a', b') > m$$

Έτσι καταλήγουμε σε άτοπο αφού $a'b' \in G$ και από υπόθεση m είναι η μέγιστη τάξη μεταξύ όλων των στοιχείων της G.

Άρα σε μια πεπερασμένη αβελιανή ομάδα η τάξη κάθε στοιχείου διαιρεί τη μέγιστη τάξη μεταξύ όλων των στοιχείων της ομάδας.

3.

Λήμμα:

Έστω κυκλική ομάδα G με n στοιχεία. Τότε από το θεώρημα Lagrange:

$$\forall g \in G : ord(g)|n$$

Κάθε κυκλική ομάδα τάξης n περιέχει ακριβώς μία υποομάδα τάξης d για κάθε $d|n$ και απο το ερώτημα 6.2 υπάρχουν ακριβώς $\phi(d)$ στοιχεία τάξης d. Από τα παραπάνω συνεπάγεται:

$$\sum_{d|n} \phi(d) = n$$

Χρησιμοποιώντας την παραπάνω σχέση μπορούμε πλέον να δείξουμε το ζητούμενο. Έστω πεπερασμένη αβελιανή ομάδα G με n στοιχεία. Τότε οι πιθανές τάξεις των υποομάδων της G είναι το σύνολο των διαιρετών του n. Κάθε στοιχείο είναι γεννήτορας της ελάχιστης κυκλικής υποομάδας που το περιέχει, έστω τάξης d, και για αυτή την υποομάδα υπάρχουν ακριβώς $\phi(d)$ γεννήτορες όπως έχουμε ήδη δειξει. Συμβολίζουμε με c_d το πλήθος των κυκλικών υποομάδων τάξης d. Έτσι προκύπτει πως:

$$n = \sum_{d|n} c_d \phi(d) \leq \sum_{d|n} \phi(d) = n$$

όπου η ανισότητα προκύπτει από την υπόθεση πως υπάρχει το πολύ μία υποομάδα για κάθε $d|n$. Η ισότητα στην παραπάνω σχέση ικανοποιείται μόνο όταν $\forall d|n : c_d = 1$ συνεπώς $c_n = 1$ και υπάρχει κυκλική υποομάδα τάξης n

4.

Έστω m η μέγιστη τάξη μεταξύ όλων των στοιχείων της ομάδας $\mathbb{Z}_p^*$. Επιπλέον η ομάδα $\mathbb{Z}_p^*$ είναι αβελιανή οπότε από το ερώτημα 7.2 έχουμε:

$$\forall g \in \mathbb{Z}_p^* : ord(g)|m \implies g^m = 1$$

Έστω ότι η ομάδα $\mathbb{Z}_p^*$ δεν είναι κυκλική. Τότε $m < p - 1$. Αν $f(x) = g^m - 1$, τότε από το θεώρημα Lagrange της θεωρίας αριθμών η εξίσωση $f(x) = 0 \pmod{p}$ έχει το πολύ m ρίζες στο $\mathbb{Z}[x]$. Έτσι καταλήγουμε σε άτοπο αφού όπως δείχτηκε προηγούμενως η εξίσωση αυτή έχει τουλάχιστον $p - 1$ ρίζες.

Άσκηση 8

Για να υπολογίσουμε τα τελευταία 17 ψηφία του αριθμού $1707 \uparrow\uparrow 1783$, αρκεί να υπολογίσουμε το $1707 \uparrow\uparrow 1783 \bmod 10^{17}$. Ορίζουμε τη συνάρτηση:

$$\begin{cases} f(x,0) = \phi(x) \\ f(x,y) = \phi(f(x,y-1)) \end{cases}$$

Ο υπολογισμός $a \uparrow\uparrow n \bmod \mathrm{m}$ μπορεί να γίνει πολύ εύκολα αν ισχύει:

$$\forall x \in \{0,1,\ldots,n-2\} : gcd(a, f(m,x)) = 1$$

Σε αυτή την περίπτωση ο υπολογισμός γίνεται μέσω της αναδρομικής συνάρτησης:

$$\begin{cases} solve(a,1,m) = n \bmod \mathrm{m} \\ solve(a,n,1) = 0 \\ solve(a,n,m) = a^{solve(a,n-1,\phi(m))} \bmod \mathrm{m} \end{cases}$$

η οποία χρησιμοποιεί διαδοχική εφαρμογή του θεωρήματος του Euler αναδρομικά ώστε να μειώσει τους εκθέτες αρκετά και να είναι δυνατός ο υπολογισμός μέσω διαδοχικών τετραγωνισμών. Η συνθήκη που παρουσιάστηκε παραπάνω ικανοποιείται για τον υπολογισμό $1707 \uparrow\uparrow 1783 \bmod 10^{17}$ οπότε χρησιμοποιώντας τα παραπάνω προκύπτει πως $1707 \uparrow\uparrow 1783 \bmod 10^{17} = 70080500540924243$

Σε περίπτωση που ζητηθεί ο υπολογισμός $a \uparrow\uparrow n \bmod m$ και δεν ικανοποιείται η συνθήκη που δώσαμε ο υπολογισμός είναι πιο περίπλοκος αφού απαιτείται να παραγοντοποιήσουμε το a και στην συνέχεια να ακολουθήσουμε ακριβώς την ίδια διαδικασία με την άσκηση 5 αναδρομικά.

Ο κώδικας περιλαμβάνει και τις 2 περιπτώσεις και επισυνάπτεται.

Άσκηση 9

Θα ξεκινήσουμε την απόδειξη δείχνοντας ότι μετά τη φάση δημιουργίας των κλειδιών, αν ισχύει για τη μετάθεση ότι $P[2] = 0$ και $P[1] \neq 2$ τότε το δεύτερο byte εξόδου είναι ίσο με 0 με πιθανότητα 1.

Έστω λοιπόν ότι για την αρχική μετάθεση έχουμε $P[2] = 0$, $P[1] \neq 2$. Συμβολίζουμε με P_i τη μετάθεση που προκύπτει μετά την i-οστή επανάληψη
$i = 0, j = 0$
1η επανάληψη:
$i := 1$
$j := P[1]$
$P_1[1] := P[P[1]]$
$P_1[P[1]] = P[1]$
$\forall x \neq 1, P[1] : P_1[x] = P[x]$
2η επανάληψη:
$i := 2$
$j := P[1] + P_1[2] = P[1]$
$P_2[2] = P_1[P[1]] = P[1]$
$P_2[P[1]] = P_1[2] = 0$
$\forall x \neq 2, P[1] : P_2[x] = P_1[x]$
Άρα το δεύτερο byte εξόδου είναι:
$K_0 = P_2[P_2[2] + P_2[P[1]]] = K_0 = P_2[P[1] + 0] = 0$

Το παραπάνω συμβαίνει με πιθανότητα:

$$Pr[P[2] = 0 \wedge P[1] \neq 2] = Pr[P[2] = 0]Pr[P[1] \neq 2|P[2] = 0] = \frac{1}{256}\frac{254}{255} \approx 2^{-8} = Pr[P[2] = 0]$$

Αν $Pr[zero]$ η πιθανότητα το δεύτερο byte εξόδου να είναι 0 τότε από το νόμο του Bayes έχουμε:

$$Pr[zero] = Pr[zero|P[2] = 0]Pr[P[2] = 0] + Pr[zero|P[2] \neq 0]Pr[P[2] \neq 0]$$

Χρησιμοποιώντας τις προσεγγίσεις που έγιναν παραπάνω έχουμε ότι $Pr[zero|P[2] = 0] = 1$ και $Pr[P[2] = 0] = 2^{-8}$. Επιπλέον $Pr[P[2] \neq 0] = \frac{255}{256} \approx 1$ Τέλος υποθέτουμε πως αν $P[2] \neq 0$ η έξοδος ακολουθεί ομοιόμορφη κατανομή οπότε $Pr[zero|P[2] \neq 0] = 2^{-8}$

Τελικά αντικαθιστώντας στην παραπάνω σχέση βρίσκουμε ότι:

$$Pr[zero] \approx 2^{-8} + 2^{-8} = 2^{-7}$$

Άσκηση 10

1.

Έστω ότι η συνάρτηση $F_1(k,x)$ δεν είναι ψευδοτυχαία. Τότε υπάρχει PPT διαχωριστής $\mathcal{D}_1$ και μη αμελητέα συνάρτηση nnegl ώστε:

$$|Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}_1^{F_1(k,\cdot)}(1^n)=1]-Pr_{r\leftarrow Func_n}[\mathcal{D}_1^{r(\cdot)}(1^n)=1]|\geq nnegl(n)$$

Θα κατασκευάσουμε ένα διαχωριστή $\mathcal{D}$ ο οποίος μπορεί να ξεχωρίσει την F από μία τυχαία συνάρτηση. Ο $\mathcal{D}$ έχει μαντείο $\mathcal{O}$, το οποίο είναι είτε η συνάρτηση $F(k,x)$ με $k\leftarrow\{0,1\}^n$ είτε μία ομοιόμορφα επιλεγμένη συνάρτηση του $Func_n$. Ο διαχωριστής λειτουργεί ως εξής:

Ο $\mathcal{D}$ χρησιμοποιεί σαν υπορουτίνα τον $\mathcal{D}_1$ και έχει το ρόλο του μαντείου για αυτόν. Συγκεκριμένα όταν ο $\mathcal{D}_1$ ρωτάει το μαντείο του για κάποια συμβολοσειρά x, ο $\mathcal{D}$ ρωτάει το δικό του μαντείο για την ίδια συμβολοσειρά και επιστρέφει στον $\mathcal{D}$ τη συμβολοσειρά $\mathcal{O}(x)\oplus x$. Τελικά όταν ο $\mathcal{D}_1$ επιστρέφει 1, ο $\mathcal{D}$ επιστρέφει και αυτός 1, ενώ όταν ο $\mathcal{D}_1$ επιστρέφει 0, ο $\mathcal{D}$ επιστρέφει 0. Αν ισχύει ότι $\mathcal{O}(\cdot)=F(k,\cdot)$, τότε οι απαντήσεις που λαμβάνει ο $\mathcal{D}_1$ όταν ρωτάει το μαντείο είναι ίδιες με αυτές που θα λάμβανε αν είχε μαντείο $F_1(k,\cdot)$. Συνεπώς έχουμε ότι:

$$Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}^{F(k,\cdot)}(1^n)=1]=Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}_1^{F_1(k,\cdot)}(1^n)=1]]$$

Επίσης αν το μαντείο $\mathcal{O}(\cdot)$ είναι μία ομοιόμορφα επιλεγμένη συνάρτηση του $Func_n$ τότε η έξοδος του μαντείου θα είναι ομοιόμορφα κατανεμημένες συμβολοσειρές μήκους n. Όμως τότε η έξοδος του $\mathcal{O}(x)\oplus x$ θα είναι ομοιόμορφα κατανεμημένη ανεξαρτήτως της κατανομής του x οπότε ο $\mathcal{D}_1$ θα λαμβάνει ομοιόμορφα κατανεμημένες συμβολοσειρές. 'Ετσι προκύπτει πως:

$$Pr_{r'\leftarrow Func_n}[\mathcal{D}^{r'(\cdot)}(1^n)=1]=Pr_{r\leftarrow Func_n}[\mathcal{D}_1^{r(\cdot)}(1^n)=1]$$

Από τις παραπάνω σχέσεις παίρνουμε:

$$|Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}^{F(k,\cdot)}(1^n)=1]-Pr_{r'\leftarrow Func_n}[\mathcal{D}^{r'(\cdot)}(1^n)=1]|\geq nnegl(n)$$

το οποίο είναι άτοπο αφού η $F(k,x)$ είναι ψευδοτυχαία. Άρα αν η $F(k,x)$ είναι ψευδοτυχαία τότε και η $F_1(k,x)=F(k,x)\oplus x$ είναι ψευδοτυχαία.

2.

Έστω ότι υπάρχει PPT διαχωριστής $\mathcal{D}_1$ και μη αμελητέα συνάρτηση nnegl έτσι ώστε:

$$|Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}_1^{F_2(k,\cdot)}(1^n)=1]-Pr_{r\leftarrow Func_n}[D_1^{F(r(0^n),\cdot)}(1^n)=1]|\geq nnegl(n)$$

Θα κατασκευάσουμε διαχωριστή $\mathcal{D}$ ο οποίος μπορεί να διαχωρίσει την F από μία τυχαία συνάρτηση. Ο $\mathcal{D}$ διαθέτει μαντείο $\mathcal{O}$ που είναι είτε η $F(k,x)$ είτε μια ομοιόμορφα επιλεγμένη συνάρτηση του $Func_n$. Η λειτουργία του διαχωριστή παρουσιάζεται παρακάτω:

Ο $\mathcal{D}$ δίνει σαν είσοδο στο μαντείο του τη συμβολοσειρά 0^n. Έτσι θέτει $c := \mathcal{O}(0^n)$. Στη συνέχεια χρησιμοποιεί σαν υπορουτίνα τον $\mathcal{D}_1$. Επιπλέον ο $\mathcal{D}$ έχει το ρόλο του μαντείου για τον $\mathcal{D}_1$. Κάθε φορά που ο D_1 ρωτάει το μαντείο για μία συμβολοσειρά x, ο $\mathcal{D}$ του απαντάει με τη συμβολοσειρά $F(c,x)$. Τελικά όταν αν ο $\mathcal{D}_1$ επιστρέψει 1, τότε επιστρέφει 1 και ο $\mathcal{D}$, ενώ αν ο $\mathcal{D}_1$ επιστρέψει 0, επιστρέφει 0 και ο $\mathcal{D}$. Αν $\mathcal{O}(\cdot) = F(k,\cdot)$, τότε η απάντηση που δέχεται ο $\mathcal{D}_1$ είναι $F(F(k,0^n),x)$, ενώ αν $\mathcal{O}(\cdot)$ είναι ομοιόμορφη επιλεγμένη συνάρτηση τότε ο $\mathcal{D}_1$ δέχεται απάντηση $F(r(k,0^n),x)$, με $r \leftarrow Func_n$. Επομένως έχουμε:

$$Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}^{F(k,\cdot)}(1^n) = 1] = Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}_1^{F_2(k,\cdot)}(1^n) = 1]$$

$$Pr_{r\leftarrow Func_n}[\mathcal{D}^{r(\cdot)}(1^n) = 1] = Pr_{r\leftarrow Func_n}[\mathcal{D}_1^{F(r(0^n),\cdot)}(1^n) = 1]$$

Με αντικατάσταση στην πρώτη σχέση παίρνουμε:

$$|Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}^{F(k,\cdot)}(1^n) = 1] - Pr_{r\leftarrow Func_n}[\mathcal{D}^{r(\cdot)}(1^n) = 1]| \geq nnegl(n)$$

το οποίο είναι άτοπο αφού η F είναι ψευδοτυχαία συνάρτηση. Επομένως για κάθε PPT αλγόριθμο $\mathcal{D}$ υπάρχει αμελητέα συνάρτηση $negl$ έτσι ώστε:

$$|Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}^{F_2(k,\cdot)}(1^n) = 1] - Pr_{r\leftarrow Func_n}[\mathcal{D}^{F(r(0^n),\cdot)}(1^n) = 1]| \leq negl(n)$$

Έστω $c \in \{0,1\}^n$. Τότε έχουμε ότι:

$$Pr_{r\leftarrow Func_n}[r(0^n) = c] = \frac{1}{2^n} = Pr_{k\leftarrow\{0,1\}^n}[k = c]$$

Προκύπτει λοιπόν άμεσα πως για κάθε PPT διαχωριστή $\mathcal{D}$:

$$Pr_{r\leftarrow Func_n}[\mathcal{D}^{F(r(0^n),\cdot)}(1^n) = 1] = Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}^{F(k,\cdot)}(1^n) = 1]$$

Τέλος η $F(k,x)$ είναι ψευδοτυχαία συνεπώς για κάθε PPT διαχωριστή $\mathcal{D}$ υπάρχει αμελητέα συνάρτηση $negl'$ ώστε:

$$Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}^{F(k,\cdot)}(1^n) = 1] = Pr_{r\leftarrow Func_n}[\mathcal{D}^{r(\cdot)}(1^n) = 1] \leq negl'(n)$$

Τελικά για κάθε πολυωνυμικό διαχωριστή $\mathcal{D}$:

$$\begin{aligned}
&|Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}^{F_2(k,\cdot)}(1^n) = 1] - Pr_{r\leftarrow Func_n}[\mathcal{D}^{r(\cdot)}(1^n) = 1]| \\
&\leq |Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}^{F_2(k,\cdot)}(1^n) = 1] - Pr_{r\leftarrow Func_n}[D_1^{F(r(0^n),\cdot)}(1^n) = 1]| \\
&+ Pr_{r\leftarrow Func_n}[D_1^{F(r(0^n),\cdot)}(1^n) = 1] - Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}^{F(k,\cdot)}(1^n) = 1] \\
&+ Pr_{k\leftarrow\{0,1\}^n}[\mathcal{D}^{F(k,\cdot)}(1^n) = 1] - Pr_{r\leftarrow Func_n}[\mathcal{D}^{r(\cdot)}(1^n) = 1] \leq negl(n)negl'(n)
\end{aligned}$$

Τελικά η συνάρτηση $F_2(k,x)$ είναι ψευδοτυχαία.

3.

Αν $x \in \{0,1\}^{2n}$ τότε συμβολίζουμε με $left(x)$ και $right(x)$ τα πρώτα και τα τελευταία n bits του x αντίστοιχα. Θα κατασκευάσουμε ένα PPT διαχωριστή $\mathcal{D}$ για την $F_3(k,x)$ ο οποίος διαθέτει μαντείο $\mathcal{O}$ το οποίο είναι είτε η $F_3(k,x)$ για ομοιόμορφα επιλεγμένο k είτε μία ομοιόμορφα επιλεγμένη συνάρτηση. Ο διαχωριστής λειτουργεί ως εξής:

1. Ρωτάει για την τιμή $q_1 = \mathcal{O}(0)$
2. Επιλέγει τυχαία κάποιο $x \in \{0,1\}^n$
3. Υπολογίζει την τιμή $F(right(q_1), x)$
4. Ρωτάει για την τιμή $q_2 = \mathcal{O}(x)$
5. Αν $left(q_2) = F(right(q_1), x)$ επιστρέφει 1, αλλιώς επιστρέφει 0

Αν το μαντείο $\mathcal{O}$ είναι η συνάρτηση $F_3(k,x)$ τότε:

$$Pr_{k \leftarrow \{0,1\}^n}[\mathcal{D}^{F_3(k,\cdot)}(1^n) = 1] = 1$$

Αν το μαντείο $\mathcal{O}$ είναι ομοιόμορφα επιλεγμένη συνάρτηση τότε:

$$Pr_{r \leftarrow Func_{n \to 2n}}[\mathcal{D}^{r(\cdot)}(1^n) = 1] = \frac{1}{2^n}$$

Συνεπώς καταλήγουμε πως:

$$|Pr_{k \leftarrow \{0,1\}^n}[\mathcal{D}^{F_3(k,\cdot)}(1^n) = 1] - Pr_{r \leftarrow Func_{n \to 2n}}[\mathcal{D}^{r(\cdot)}(1^n) = 1]| = 1 - \frac{1}{2^n}$$

που δεν είναι αμελητέα άρα η $F_3(k,x)$ δεν είναι ψευδοτυχαία.