ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΚΡΥΠΤΟΓΡΑΦΙΑ

(2021 – 2022)

2η Σειρά Ασκήσεων

Ονοματεπώνυμο:

- Χρήστος Τσούφης

Αριθμός Μητρώου:

- 031 17 176

Στοιχεία Επικοινωνίας:

- el17176@mail.ntua.gr
- chris99ts@gmail.com

1η Άσκηση

Αποδείξτε ότι (p − 1)! ≡ −1 (mod p), όπου p πρώτος αριθμός.

Λύση:

Έστω το πολυώνυμο $f(x) = (x-1)(x-2)\dots\big(x-(p-1)\big)$ με ρίζες 1, 2, …, p – 1.

Έστω επίσης, το πολυώνυμο $g(x) = x^{p-1} - 1$ για το οποίο θα ισχύει ότι $g(x) \bmod p$ θα έχει κι αυτό ρίζες 1, 2, … p – 1 από Μικρό Θεώρημα Fermat.

Έστω ακόμη, το πολυώνυμο $h(x) = f(x) - g(x)$ το οποίο θα ισούται με μηδέν όταν λαμβάνει τις τιμές x = 1, 2, …, p – 1.

Επίσης, σημειώνεται ότι θα είναι τάξης p – 2 αφού οι μεγιστοβάθμιοι όροι αλληλοαναιρούνται οπότε μπορεί να έχει μέχρι και p – 2 διαφορετικές ρίζες.

Επομένως, θα πρέπει το h(x) να είναι το μηδενικό πολυώνυμο οπότε ο σταθερός όρος θα πρέπει να ισούται με το μηδέν και άρα $(p-1)! - 1 \equiv 0 \bmod p$ αφού ο όρος $(p-1)!$ περιέχει όλους τους διαιρέτες του κ.

2η Άσκηση

Να βρείτε όλες τις υποομάδες της ομάδας $\mathbb{Z}_{29}^*$. Εξηγήστε αναλυτικά με ποιον τρόπο σκεφτήκατε και τι δοκιμές κάνατε.

Λύση:

Οι γεννήτορες της ομάδας $\mathbb{Z}_{29}^*$ είναι οι εξής: 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27.

Για την εύρεση όλων των γνήσιων υποομάδων, αρκεί να βρεθούν οι ομάδες που παράγουν τα στοιχεία που δεν είναι γεννήτορες.

Τάξη 1 → 1: {1}

Τάξη 2 → 28: {1, 28}

Τάξη 4 → 12, 17: {1, 12, 17, 28}

Τάξη 7 → 7, 16, 20, 23, 24, 25: {1, 7, 16, 20, 23, 24, 25}

Τάξη 14 → 4, 5, 6, 9, 13, 22: {1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28}

3η Άσκηση

Υπολογίστε το $25^{-1}\ mod\ 77$ *χωρίς αριθμομηχανή, χρησιμοποιώντας μόνο εμπειρικές παρατηρήσεις και το Κινέζικο Θεώρημα Υπολοίπων (CRT). Μπορείτε να βρείτε και 2ο τρόπο, χωρίς χρήση του CRT;*

Λύση:

Υπολογισμός με το Κινέζικο Θεώρημα Υπολοίπων (CRT):

Είναι γνωστό ότι η ομάδα $\mathbb{Z}_{77}$ είναι ισομορφική με το καρτεσιανό γινόμενο $\mathbb{Z}_7 \times \mathbb{Z}_{11}$. Επομένως, μπορεί να υπολογιστεί ο αντίστροφος του 25 από τις μικρότερες ομάδες. Έτσι, θα ισχύει ότι:

$$25^{-1}\ (\mathrm{mod}\ 77) \equiv \left(25^{-1}\ (\mathrm{mod}\ 7), 25^{-1}\ (\mathrm{mod}\ 11)\right) \equiv \left((5^2)^{-1}\ (\mathrm{mod}\ 7), (5^2)^{-1}\ (\mathrm{mod}\ 11)\right)$$
$$\equiv \left(5^{-1} \cdot 5^{-1}\ (\mathrm{mod}\ 7), 5^{-1} \cdot 5^{-1}\ (\mathrm{mod}\ 11)\right) \equiv \left(3 \cdot 3\ (\mathrm{mod}\ 7), 9 \cdot 9\ (\mathrm{mod}\ 11)\right)$$
$$\equiv \left(2\ (\mathrm{mod}\ 7), 4\ (\mathrm{mod}\ 11)\right)$$

Οπότε, με δοκιμές μπορεί να βρεθεί ότι ο αντίστροφος του $5\ (\mathrm{mod}\ 7)$ και $(\mathrm{mod}\ 11)$ θα είναι:

$$5^{-1} \equiv 3(\mathrm{mod}\ 7)\ \&\ 5^{-1} \equiv 9(\mathrm{mod}\ 11)$$

Συνεπώς, ο αντίστροφος του 25 θα είναι:

$$5^{-1} \cdot 5^{-1} \equiv 3 \cdot 3 \equiv 2\ (\mathrm{mod}\ 7)$$
$$5^{-1} \cdot 5^{-1} \equiv 9 \cdot 9 \equiv 4\ (\mathrm{mod}\ 11)$$

Άρα, σύμφωνα με το CRT, υπάρχει μοναδικός αριθμός που να αφήνει υπόλοιπο 2 με το 7 και υπόλοιπο 4 με το 11. Αυτός ο αριθμός θα είναι το 37 και μπορεί να προκύψει είτε εμπειρικά είτε με βάση τον τύπο:

$$\sum_{i=0}^{k} N_i \cdot M_i \cdot a_i$$
$$M = \prod_{i=0}^{k} m_i\ ,\ M_i = \frac{M}{m_i}, N_i \cdot M_i \equiv 1\ (\mathrm{mod}\ m_i)$$

Εναλλακτικά, εκμεταλλευόμενοι την εξής ιδιότητα:

$$a \equiv b \bmod n \wedge a \equiv b \bmod m \Leftrightarrow a \equiv b \bmod m \cdot n$$

Μπορεί να γίνει ο εξής υπολογισμός:

$$a \equiv 25^{-1} \bmod 77 \Leftrightarrow a \equiv 25^{-1} \bmod 7 \wedge a \equiv 25^{-1} \bmod 11 \Leftrightarrow$$
$$a \equiv 4^{-1} \bmod 7 \wedge a \equiv 3^{-1} \bmod 11 \Leftrightarrow a \equiv 2 \bmod 7 \wedge a \equiv 4 \bmod 11$$

Επιπλέον, $M_1 = 11, N_1 = 2, M_2 = 7, N_1 = 8$

Οπότε $a \equiv 11 \cdot 2 \cdot 2 + 7 \cdot 8 \cdot 4 \equiv 268 \equiv 37 \bmod 77$.

Υπολογισμός χωρίς το Κινέζικο Θεώρημα Υπολοίπων (CRT):

Μια πρώτη προσέγγιση θα ήταν να σκεφτεί κανείς ότι αναζητά έναν αριθμό α που να ισχύει ότι:

$$a \cdot 25 \equiv 1 \bmod 77 \Rightarrow a \cdot 25 = 77 \cdot k + 1 \Rightarrow a = \frac{77 \cdot k + 1}{25}$$

Συνεπώς, αναζητείται ένας ακέραιος k που να επαληθεύει την σχέση. Οπότε, με δοκιμές, για k = 12 προκύπτει α = 37.

Εναλλακτικά, θα μπορούσε να παρατηρήσει κανείς ότι οι αριθμοί 25 και 7 είναι σχετικά πρώτοι μεταξύ τους.

Έτσι, μπορεί κανείς να υπολογίσει τον αντίστροφο από τον Επεκτεταμένο Αλγόριθμο του Ευκλείδη.

Άρα, μπορούν να βρεθούν δυο αριθμοί m, n ∈ $\mathbb{Z}$ που να ικανοποιούν τη σχέση 25·m + 77·n = 1.

Σύμφωνα με τον Αλγόριθμο του Ευκλείδη, ο Μέγιστος Κοινός Διαιρέτης δύο αριθμών a, b υπολογίζεται από το τελευταίο μη μηδενικό υπόλοιπο gcd(a, b) = r_k ως εξής:

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

...

$$r_{k-1} = q_{k+1} r_k + 0$$

Συνεπώς, για α = 77 και b = 25, προκύπτει:

$$77 = 3 \cdot 25 + 2$$

$$25 = 12 \cdot 2 + 1$$

$$2 = 2 \cdot 1$$

Έτσι, αρχίζοντας από την τελευταία σχέση και με διαδοχικές αντικαταστάσεις, μπορούν να υπολογιστούν οι αριθμοί m, n ∈ $\mathbb{Z}$ ως εξής:

$$1 = 25 - 12 \cdot 2 \xrightarrow{2=77-3\cdot 25} 1 = 25 - 12 \cdot (77 - 3 \cdot 25) \Rightarrow -12 \cdot 77 + 37 \cdot 25 = 1$$

Οπότε, ο αντίστροφος του 25 είναι το 37.

4η Άσκηση

(α) *Να δείξετε ότι κάθε υποομάδα μιας κυκλικής ομάδας είναι επίσης κυκλική.*

(β) *Πόσες υποομάδες έχει η ομάδα* $U(\mathbb{Z}_{4872961})$*;*

Λύση:

(α) Έστω G μια κυκλική ομάδα με γεννήτορα g. Έστω, επίσης, μια υποομάδα της G.

Αν H = {e}, τότε θα είναι κυκλική με γεννήτορα το e.

Αν H ≠ {e}, τότε κάθε στοιχείο της h ∈ H μπορεί να γραφεί ως κάποια δύναμη του γεννήτορα της G. Έστω $h = g^m$ για κάποιο m ∈ ℤ.

Έστω, ακόμη, το σύνολο A, με όλες τις θετικές δυνάμεις του γεννήτορα g που ανήκουν στην H:

$$A = \{k \in \mathbb{N} | g^k \in H\} \subseteq \mathbb{N}$$

Αξίωμα Φυσικών Αριθμών: Κάθε μη κενό υποσύνολο του ℕ έχει ελάχιστο στοιχείο.

Επομένως, από το παραπάνω αξίωμα, αν s είναι το ελάχιστο στοιχείο του A, τότε το $a^s \in H$ θα είναι γεννήτορας της H.

Έστω ένα τυχαίο στοιχείο της H, το οποίο γράφεται ως g^n, n ∈ ℤ. Τότε:

$$n = q \cdot s + r \Rightarrow g^n = g^{s \cdot q} \cdot g^r \Rightarrow g^r = g^{n - q \cdot s} \Rightarrow g^r = g^n \cdot (g^s)^{-q}, \text{για } 0 \leq r \leq s$$

Οπότε, λόγω της κλειστότητας της υποομάδας θα ισχύει ότι $g^n \in H$, $(g^n)^{-q} \in G$ άρα και $g^r \in H$.

Εφόσον, το ελάχιστο στοιχείο του A είναι το s και επειδή 0 ≤ r ≤ s, θα πρέπει r = 0 και τελικά n = q·s.

Συνεπώς, κάθε στοιχείο του H μπορεί να γραφεί ως κάποια δύναμη του g^s.

Οπότε, το g^s είναι γεννήτορας της H και τελικά η H είναι κυκλική.

(β) Η ομάδα $U(\mathbb{Z}_{4872961})$ είναι ισόμορφη με την $\mathbb{Z}^*_{4872961}$ αφού ο αριθμός 4872961 είναι πρώτος.

Η ομάδα $\mathbb{Z}^*_{4872961}$ είναι κυκλική τάξης 4872960.

Από το Θεώρημα του Lagrange είναι γνωστό ότι η τάξη της υποομάδας διαιρεί την τάξη της ομάδας. Η απόδειξη φαίνεται στην Άσκηση όπου δείχνεται ότι για κάθε διαιρέτη d υπάρχει ακριβώς μια ομάδα).

Συνεπώς, θα έχει 180 υποομάδες.

5η Άσκηση

Υλοποιήστε τον έλεγχο πρώτων αριθμών Fermat σε πρόγραμμα (απαιτείται να υποστηρίζονται πράξεις μεγάλων αριθμών, χιλιάδων ψηφίων). Εφαρμόστε τον για να ελέγξετε τους παρακάτω

αριθμούς:

67280421310721, 170141183460469231731687303715884105721, $2^{2281}-1$, $2^{9941}-1$, $2^{19939}-1$

Λύση:

Ο κώδικας που υλοποιεί την παραπάνω συνάρτηση επισυνάπτεται στο zip αρχείο που υποβλήθηκε.

Επεξήγηση:

Για την εύρεση των πρώτων χρησιμοποιήθηκε το Μικρό Θεώρημα Fermat και αγνοήθηκε η ύπαρξη των αριθμών Carmichale.

Συμπέρασμα:

Από τον κώδικα προκύπτει ότι οι αριθμοί 67280421310721, $2^{2281}-1$, $2^{9941}-1$ είναι πρώτοι (επιστρέφει True) ενώ οι αριθμοί 170141183460469231731687303715884105721, $2^{19939}-1$ δεν είναι πρώτοι (επιστρέφει False).

6η Άσκηση

Στο ηλιακό σύστημα του πλανήτη Ραττατάκ υπάρχουν κάτι πολύ περίεργες λευκές τρύπες, τις οποίες οι Ραττατακιανοί χρησιμοποιούν για τις μετακινήσεις τους. Οι αξιολάτρευτες κατά τα άλλα αυτές λευκές τρύπες έχουν η καθεμιά ένα διαφορετικό αριθμό-αναγνωριστικό αναλόγως με το πόσο αδύναμες ή δυνατές είναι ως προς την ικανότητά τους να επιφέρουν τηλεμεταφορά στον χώρο αλλά και στον χρόνο. Επίσης, ο χρόνος μέσα σε αυτές κυλάει (μα και φυσικά!) με διαφορετικό τρόπο από ό,τι στον "έξω" κόσμο, και συγκεκριμένα, για μια λευκή τρύπα με αναγνωριστικό έστω M και απόσταση έστω Z που ο Ραττατακιανός επιθυμεί να τηλεμεταφερθεί, η λευκή τρύπα τον καθυστερεί για μια (πολύ μικρή!) χρονική διάρκεια:

$$2^{1998000^{100^{10}}} mod\ 10^M \quad \text{"πλεξοδευτερόλεπτα"}$$

Καλείστε να βοηθήσετε έναν μικρό Ραττατακιανό, γράφοντας ένα κομψό και αποδοτικό πρόγραμμα, κατά προτίμηση σε γλώσσα C ή Python που με είσοδο τους αριθμούς , θα υπολογίζει πόσο χρόνο θα χρειαστεί (σε πλεξοδευτερόλεπτα) για το ταξίδι του στον χωροχρόνο.

Αιτιολογήστε τη σκέψη σας πίσω από το πρόγραμμα και ως παράδειγμα, υπολογίστε τα πλεξοδευτερόλεπτα που θα χρειαστεί ο μικρούλης για την λευκή τρύπα M = 3 σε απόσταση Z = 548

Λύση:

Ο κώδικας που υλοποιεί την παραπάνω συνάρτηση επισυνάπτεται στο zip αρχείο που υποβλήθηκε.

Βλ. [13]

Επεξήγηση:

Χρησιμοποιήθηκε ο τύπος:

$$x^n \equiv x^{\varphi(m)+[n \bmod \varphi(m)]} (\bmod m)$$

Συμπέρασμα:

Τα αποτελέσματα φαίνονται στο ipynb αρχείο για τις διάφορες τιμές των Z, M.

7η Άσκηση

Ο τελεστής $\uparrow\uparrow$ *ορίζεται ως εξής*

$$\alpha \uparrow\uparrow (n+1) = a^{a\uparrow\uparrow n} \; με \; a \uparrow\uparrow 1 = a$$

Για παράδειγμα $3 \uparrow\uparrow 4 = 3^{3^{3^3}} = 3^{3^{27}} = 3^{7625597484987}$

Να φτιάξετε ένα κομψό και αποδοτικό πρόγραμμα, προτιμώμενα σε γλώσσα C ή Python, το οποίο να υπολογίζει τα τελευταία 17 ψηφία του αριθμού $1707 \uparrow\uparrow 1783$.

Σημείωση: ο ζητούμενος υπολογισμός μπορεί να γίνει σε χρόνο λιγότερο από 3 sec σε υπολογιστή 'κανονικών' προδιαγραφών χρησιμοποιώντας μεταβλητές τύπου long (ακέραιους 64-bit).

Λύση:

Ο κώδικας που υλοποιεί την παραπάνω συνάρτηση επισυνάπτεται στο zip αρχείο που υποβλήθηκε.

Επεξήγηση:

Για την υλοποίηση χρησιμοποιήθηκε το γεγονός ότι η βάση πρέπει να είναι σχετικά πρώτη με το 2 και το 5 καθώς, από το Θεώρημα του Euler ισχύει ότι:

$$a^{\varphi(m)} \equiv 1 \bmod m$$

Όμως, $\gcd(a, m) = 1$ και $m = 2^k \cdot 5^n$.

Συμπέρασμα:

Από τον κώδικα προκύπτει ότι τα τελευταία 17 ψηφία του $1707 \uparrow\uparrow 1783$ είναι '70080500540924243'.

8η Άσκηση

Έστω $\mathbb{Z}_p^*$ με p πρώτο και g ένας γεννήτορας, p, g γνωστά.

1. *Αν d ένας ακέραιος που διαιρεί το $p-1$, βρείτε με αποδοτικό τρόπο ένα στοιχείο b του $\mathbb{Z}_p^*$ τάξης d (δηλαδή d ο μικρότερος ακέραιος με $b^d \equiv 1(mod\ p)$).*

2. *Πόσα στοιχεία τάξης d υπάρχουν μέσα στο $\mathbb{Z}_p^*$;*

3. *Πόσους γεννήτορες έχει η κυκλική υποομάδα που παράγει ένα στοιχείο b τάξης d;*

4. *Πόσες κυκλικές υποομάδες τάξης d υπάρχουν στο $\mathbb{Z}_p^*$;*

5. *Αν μας δώσουν ένα στοιχείο h, την τάξη του d και ένα τυχαίο στοιχείο a, πώς μπορούμε να δούμε αν το a ανήκει στην υποομάδα που παράγει το h σε πολυωνυμικό χρόνο;*

Λύση:

1. Έστω $\mathbb{Z}_p^*$ με p πρώτο και g ένας γεννήτορας. Ο όρος $b = g^{\frac{p-1}{d}}$ με $\frac{p-1}{d} \in \mathbb{Z}$ ικανοποιεί την σχέση $b^d \equiv 1(\mathrm{mod}\ p)$ αφού είναι γνωστό για τον γεννήτορα g ότι ισχύει $g^{p-1} \equiv 1\ (\mathrm{mod}\ p)$ και $p-1$ η τάξη του. Οπότε, θα ισχύει ότι $g^{\left(\frac{p-1}{d}\right)^d} \equiv 1\ (\mathrm{mod}\ p)$.

Έστω, $d > l$, δηλαδή $g^{\left(\frac{p-1}{d}\right)^l} \equiv 1\ \mathrm{mod}\ p$.

Τότε, $l \cdot \frac{p-1}{d} < p-1$, το οποίο είναι άτοπο αφού η τάξη του g είναι $p-1$.

Επομένως, ο όρος $g^{\frac{p-1}{d}}$ θα είναι τάξης d.

Εναλλακτικά, αυτό μπορεί να δειχθεί και ως εξής.

Από το Θεώρημα του Euler ισχύει ότι αν δύο αριθμοί a, p είναι σχετικά πρώτοι μεταξύ τους, δηλαδή gcd(a, p) = 1, τότε:

$$x \equiv y\ (\mathrm{mod}\ \varphi(p)) \Leftrightarrow a^x \equiv a^y (\mathrm{mod}\ p)$$

Οπότε, το στοιχείο b είναι τάξης $x < d$, δηλαδή $b^x \equiv 1(\mathrm{mod}\ p)$.

Επιπλέον, ισχύει ότι $b^d \equiv 1(\mathrm{mod}\ p)$ και τότε θα πρέπει $x \equiv d(\mathrm{mod}\ p-1)$ το οποίο είναι άτοπο αφού $x < d < p-1$.

Συνεπώς, το b θα είναι τάξης d.

2. 1ος Τρόπος Επίλυσης:

Όλα τα στοιχεία τάξης d ικανοποιούν την εξίσωση: $x^d \equiv 1 (\mathrm{mod}\ p)$

Από το Θεμελιώδες Θεώρημα της Άλγεβρας είναι γνωστό ότι αυτή η εξίσωση θα έχει το πολύ d ρίζες.

Έστω ένα τυχαίο σημείο $\alpha \in \mathbb{Z}_p^*$ τάξης d, το οποίο πάντα υπάρχει.

Τα στοιχεία $\alpha^2, \alpha^3, \ldots, \alpha^d = 1$, d στο πλήθος, είναι επίσης λύσεις της εξίσωσης και είναι διακεκριμένα μεταξύ τους αφού το στοιχείο α είναι τάξης d κι έτσι, δεν υπάρχουν κι άλλα στοιχεία που να την ικανοποιούν.

Για την εύρεση όσων είναι τάξης d αρκεί να δειχθεί ότι τα στοιχεία α^k είναι τάξης d, αν και μόνο αν, οι k, d είναι σχετικά πρώτοι μεταξύ τους.

Απόδειξη:

Ευθύ:

Το α^k είναι τάξης d. Έστω ότι τα k, d έχουν κοινό παράγοντα $q > 1$ τέτοιο ώστε $k = k' \cdot q$, $d = d' \cdot q$. Τότε, $(a^k)^{d'} \equiv 1 (\mathrm{mod}\ p)$, αφού $(a^k)^{d'} \equiv \alpha^{k \cdot d'} \equiv a^{k' \cdot q \cdot d'} \equiv 1$ με το α να είναι τάξης d και επιπλέον να ισχύει ότι $d \mid k' \cdot q \cdot d'$.

Αντίστροφο:

Οι k, d είναι σχετικά πρώτοι μεταξύ τους. Για το στοιχείο α^k υπάρχει $n \in \mathbb{Z}$ τέτοιο ώστε $(a^k)^m \equiv a^{km} \equiv 1 (\mathrm{mod}\ p)$. Αφού το α είναι τάξης d, το d διαιρεί το km οπότε $d \mid km \xrightarrow{\gcd(\kappa,\delta)=1} d \mid m$. Επίσης, είναι γνωστό ότι $(a^k)^d \equiv 1 (\mathrm{mod}\ p) \Rightarrow d \mid m$. Οπότε, α^k είναι επίσης τάξης d.

Υπάρχουν φ(d) αριθμοί σχετικά πρώτοι με το d οπότε και φ(d) στοιχεία τάξης d.

2ος Τρόπος Επίλυσης:

Χρησιμοποιώντας τα πορίσματα των ερωτημάτων 3 & 4 θα προκύψει η απάντηση.

- Είναι γνωστό ότι η κυκλική υποομάδα τάξης d έχει φ(d) γεννήτορες.
  Επιπλέον, αποδείχθηκε ότι υπάρχει μόνο μια κυκλική υποομάδα τάξης d.
  Επομένως, αφού όλα τα στοιχεία τάξης d παράγουν μια υποομάδα και επειδή υπάρχει μόνο μια κυκλική υποομάδα τάξης d θα ισχύει ότι όλα τα στοιχεία τάξης d είναι γεννήτορες αυτής της ομάδας και άρα είναι το πολύ φ(d).

- Έστω στοιχείο x τάξης d. Τότε, για στοιχείο x^n η τάξη του θα είναι $\frac{d}{\gcd(d,n)}$.
  Επομένως, για όλα τα n όπου gcd(d, n) = 1, η τάξη του στοιχείου x^n είναι d. Οπότε, τα στοιχεία τάξης d είναι τουλάχιστον φ(d).

Συνεπώς, συνδυάζοντας τα παραπάνω αποτελέσματα προκύπτει ότι υπάρχουν ακριβώς φ(d) στοιχεία τάξης d.

3. Ισχύει ότι ένα στοιχείο x τάξης d είναι γεννήτορας της ομάδας που δημιουργεί. Οπότε, για ένα στοιχείο x^n η τάξη του θα είναι $\frac{d}{\gcd(d,n)}$. Επίσης, μια υποομάδα που παράγει ένα στοιχείο b τάξης d $\langle b = g^{\frac{p-1}{d}} \rangle = \{b, b^2, b^3, \dots, b^d = 1\}$ θα έχει επίσης τάξη d. Συνεπώς, θα υπάρχουν φ(d) στοιχεία τάξης d και έτσι, φ(d) γεννήτορες.

4. <u>1ος Τρόπος Επίλυσης</u>:

Χρησιμοποιώντας το Θεώρημα Κυκλικών Ομάδων προκύπτει ότι θα υπάρχει μόνο μια υποομάδα τάξης d.

Έστω το στοιχείο $g^{\frac{p-1}{d}}$ για το οποίο είναι γνωστό ότι έχει τάξη d. Η υποομάδα που παράγει αυτό το στοιχείο θα είναι η: l, $g^{1\cdot\frac{p-1}{d}}$, $g^{2\cdot\frac{p-1}{d}}$, $g^{3\cdot\frac{p-1}{d}}$, …, $g^{(d-1)\cdot\frac{p-1}{d}}$ που έχει d στοιχεία οπότε θα είναι τάξης d.

Έστω επίσης, το στοιχείο g^m που παράγει και αυτός υποομάδα τάξης d. Η τάξη του m είναι $\frac{p-1}{\gcd(p-1,m)}$. Όμως, επειδή m | p – 1, η τάξη του είναι τελικά $\frac{p-1}{m} = d \Rightarrow m = \frac{p-1}{d}$.

<u>2ος Τρόπος Επίλυσης</u>:

Στο $\mathbb{Z}_p^*$ υπάρχει μια ομάδα τάξης d. Έστω η υποομάδα που παράγει το στοιχείο b τάξης d:

$$\langle b = g^{\frac{p-1}{d}} \rangle = \{b, b^2, b^3, \dots, b^d = 1\}$$

Έστω, επίσης, μια υποομάδα της $\mathbb{Z}_p^*$ η $H = \{h_1, \dots, h_d\}$ τάξης d. Κάθε στοιχείο της H μπορεί να γραφτεί ως κάποια δύναμη του g. Άρα $h_i = g^k$, $k \in \mathbb{Z}$.

Από το Θεώρημα Lagrange, είναι γνωστό ότι η τάξη του στοιχείου διαιρεί τη τάξη της ομάδας. Άρα $g^{k\cdot d} \equiv 1 (\mathrm{mod}\ p)$. Αφού το g είναι γεννήτορας, θα έχει τάξη p – 1 οπότε το k·d διαιρεί το p – 1. Έτσι,

$$k \cdot d = c \cdot (p-1) \Rightarrow k = c \cdot \frac{p-1}{d}, \text{οπότε για το } h_i \text{ θα ισχύει } h_i = g^k = g^{c\frac{p-1}{d}} = \left(g^{\frac{p-1}{d}}\right)^c = b^c$$

Συνεπώς, κάθε στοιχείο της d μπορεί να γραφεί ως δύναμη του b οπότε η H και η ⟨b⟩ είναι ίδιες.

5. Έστω ένα στοιχείο α. Το α θα ανήκει στην ομάδα που ορίζει το h εάν η τάξη του r διαιρεί το h. Εάν αυτή η υποομάδα περιέχει έστω και ένα στοιχείο l τάξης r, τότε θα τα περιέχει όλα αφού σε αυτή την υποομάδα το l ορίζει μια υποομάδα τάξης r που θα πρέπει να ταυτίζεται με αυτή της αρχικής ομάδας καθώς είναι μοναδική. Επιπλέον, φαίνεται πως η υποομάδα του h περιέχει το στοιχείο $h^{\frac{d}{r}}$ και ισχύει ότι $h^{r\cdot\frac{d}{r}} \equiv 1 \bmod p$. Για r > n, $h^{l\cdot\frac{d}{r}} \equiv 1 \bmod p$. Όμως, $l \cdot \frac{d}{r} < d$ που είναι άτοπο αφού η τάξη του h είναι d.

Συνεπώς, για τον έλεγχο για το αν το α ανήκει ή όχι στην υποομάδα του h αρκεί να εξεταστεί αν ισχύει ότι $\alpha^d \equiv 1 \bmod p$.

9η Άσκηση

1. *Έστω $a \in U(\mathbb{Z}_n)$ τάξης k και $b \in U(\mathbb{Z}_n)$ τάξης m. Αποδείξτε ότι ο αριθμός $a \cdot b \in U(\mathbb{Z}_n)$ έχει τάξη $k \cdot m$ αν και μόνο αν $gcd(k, m) = 11$. Ισχύει η ιδιότητα για οποιαδήποτε (πεπερασμένη) αβελιανή ομάδα;*

2. *Να δείξετε ότι σε μια (πεπερασμένη) αβελιανή ομάδα η τάξη κάθε στοιχείου διαιρεί την μέγιστη τάξη (μεταξύ όλων των στοιχείων της ομάδας).*

Υπόδειξη: μπορεί να σας φανεί χρήσιμη η διαδικασία απόδειξης του ερωτήματος (6.1).

3. *Έστω μια (πεπερασμένη) αβελιανή ομάδα που έχει την εξής ιδιότητα: έχει το πολύ μία υποομάδα για κάθε πιθανή τάξη (παρατήρηση: σε γενικές ομάδες, είναι δυνατόν αυτό να μην συμβαίνει, δηλαδή να υπάρχουν δύο υποομάδες διαφορετικές μεταξύ τους με την ίδια όμως τάξη). Να δείξετε ότι είναι κυκλική.*

4. *Χρησιμοποιώντας το θεώρημα Lagrange της θεωρίας αριθμών που μπορείτε να λάβετε ως δεδομένο, ότι δηλαδή αν g είναι ένα μη-σταθερό πολυώνυμο βαθμού d με συντελεστές στο $\mathbb{Z}_p^*$ τότε το πολυώνυμο αυτό έχει το πολύ d ρίζες στο $\mathbb{Z}_p^*$, να δείξετε ότι η ομάδα $\mathbb{Z}_p^*$ είναι κυκλική για κάθε πρώτο p.*

Λύση:

1. *Ευθύ*:

Έστω $\gcd(k, m) = l$.

Τότε, θα ισχύει ότι $(a \cdot b)^{k \cdot m} \equiv a^{k \cdot m} b^{k \cdot m} \equiv 1 \bmod n$.

Έστω επίσης, l για το οποίο θα ισχύει ότι $(a \cdot b)^l \equiv 1 \bmod n$ με $l < k \cdot m$.

Τότε, $l \mid k \cdot m$.

Όμως, $(a \cdot b)^{l^m} \equiv a^{l \cdot m} b^{l \cdot m} \equiv a^{l \cdot m} 1 \equiv 1 \bmod n$.

Οπότε, $k \mid l \cdot m$. Όμως, $k \nmid m$ οπότε $k \mid l$.

Ομοίως, προκύπτει ότι $m \mid l$.

Τελικά $k \cdot m \mid l$, δηλαδή $l = k \cdot m$.

Αντίστροφο:

Έστω $\gcd(k, m) \neq 1$.

Τότε, αυτό θα σημαίνει ότι έχουν έναν κοινό διαιρέτη n οπότε $k = c \cdot l$ και $m = d \cdot l$.

Όμως, για $c \cdot d \cdot l < k \cdot m$ ισχύει ότι $(a \cdot b)^{c \cdot d \cdot l} \equiv a^{c \cdot d \cdot l} b^{c \cdot d \cdot l} \equiv a^{k \cdot d} b^{m \cdot c} \equiv 1^d 1^c \equiv 1 \bmod n$ οπότε το $a \cdot b$ δεν είναι τάξης $k \cdot m$.

10η Άσκηση

Εξετάστε τη γεννήτρια ψευδοτυχαιότητας RC4. Αποδείξτε ότι το δεύτερο byte (κλειδί) εξόδου είναι ίσο με 0 με πιθανότητα περίπου ίση με 2^{-7}. Ξεκινήστε δείχνοντας ότι αν μετά τη φάση δημιουργίας κλειδιών (KSA) ισχύει για την μετάθεση P ότι P[2] = 0 και P[1] ≠ 2 τότε το δεύτερο byte εξόδου είναι ίσο με 0 με πιθανότητα 1.

Λύση:

Έστω μια γεννήτρια ψευδοτυχαιότητας RC4 με πίνακα μεταθέσεων P[0 … 255] που είναι αρχικοποιημένος ∀ i: P[i] = i.

Έστω P_i ο πίνακας μεταθέσεων μετά από i επαναλήψεις και j_i το j μετά από i επαναλήψεις.

Έστω, ακόμη, ο ακόλουθος τρόπος λειτουργίας της παραγωγής ψευδοτυχαίων byte (PRGA)

```
i = 0
j = 0
while next key needed:
    i = (i + 1)%256
    j = (j + P[i])%256
    swap (P[i], P[j])
    K0 = P[(P[i] + P[j])%256]
    return K0
```

Πρώτα, θα δειχθεί ότι αν μετά τη φάση δημιουργίας κλειδιών (KSA) ισχύει για την μετάθεση P ότι P[2] = 0 και P[1] ≠ 2 τότε το δεύτερο byte εξόδου είναι ίσο με 0 με πιθανότητα 1.

Για αυτό το λόγο θα αναλυθούν οι πρώτες επαναλήψεις του PRGA. Αρχικά είναι i = 0; j = 0.

- Με την είσοδο στο while loop, $i = i + 1 \xrightarrow{i=0} i = 1$ και $j = j + P[i] \xrightarrow[j=0]{i=1} j = P[1] = k \neq 2$. Μετά γίνεται swap(P[1], P[k] (≠ P[2])). Οπότε, P[1] = P[k] και P[k] = k. Οπότε στην πρώτη έξοδο, ανταλλάσσουν θέση το 1 με το k.
- Στο επόμενο loop είναι $i = i + 1 \xrightarrow{i=1} i = 2$ και $j = j + P[i] \xrightarrow[j=k]{i=2} j = k + P[2] \xrightarrow{P[2]=0} j = k$. Μετά γίνεται swap(P[2], P[k]). Οπότε, P[2] = k και P[k] = 0. Οπότε, ανταλλάσσουν θέση το 2 με το k. Πλέον, το μηδέν βρίσκεται στην θέση k και το k στην θέση 2. Επομένως, η δεύτερη έξοδος θα είναι P[(P[i]+P[j]) mod 256]. Εδώ, P[i] = P[2] = k και P[j] = P[k] = 0 οπότε K_0 = P[P[2] + P[k] mod 256] = P[P[2]] = P[k] = 0.

Όμως, αν P[2] ≠ 0, τότε η διαδικασία είναι τυχαία και η εμφάνιση οποιουδήποτε byte είναι ισοπίθανη. Οπότε,

$$\Pr[K_0 = 0] = \Pr[K_0 = 0 | P[2] = 0] \cdot \Pr[P[2] = 0] + \Pr[K_0 = 0 | P[2] \neq 0] \cdot \Pr[P[2] \neq 0] =$$

$$= (1 - 2^{-8}) \cdot 2^{-8} + 2^{-8} \cdot (1 - 2^{-8}) = 2 \cdot 2^{-8} - 2 \cdot 2^{-16} \approx 2 \cdot 2^{-8} = 2^{-7}$$

11η Άσκηση

Έστω F: $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ *ψευδοτυχαία συνάρτηση. Εξετάστε τις παρακάτω συναρτήσεις ως προς την ψευδοτυχαιότητα τους:*

1. $F_1(k,x) = F(k,x) \oplus x$

2. $F_2(k,x) = F(F(k,0^n),x)$

3. $F_3(k,x) = F(F(k,0^n),x)||F(k,x)$

Λύση:

1. Η F_1 μπορεί εύκολα να παρατηρήσει κανείς ότι δ είναι ψευδοτυχαία εξαιτίας της τυχαιότητας της F αφού, από την στιγμή που είναι γνωστό το x τότε αν μπορέσει να αποφανθεί κανείς για την έκβαση της F_1 τότε θα μπορέσει να αποφανθεί και για την F μέσω της πράξης $F_1 \oplus x = F$. Βέβαια, ο αντίπαλος δεν μπορεί να ξεχωρίσει αν η έξοδος είναι από την F ή από μια $f \leftarrow Func_n$.

2. Η F_2 είναι ψευδοτυχαία αφού και η F είναι ψευδοτυχαία, εκτός κι αν βρεθεί κάποια πληροφορία για το κλειδί. Ωστόσο, για το $F(k, 0^n)$ ακόμα και να έχει κάποιος πρόσβαση στο Oracle της F, δεν μπορεί να πάρει πληροφορία για το κλειδί της F_2 από την στιγμή που δεν έχει καμία πληροφορία για το k.

Με άλλα λόγια, αν διατηρηθεί σταθερό το x δεν μπορεί να προκύψει κάποιο χρήσιμο αποτέλεσμα αφού αλλάζοντας το k, αλλάζει το κλειδί της εξωτερικής F, η οποία είναι ψευδοτυχαία. Από την άλλη, αν διατηρηθεί σταθερό το k ώστε πάντα να παίρνει η εξωτερική F ίδιο κλειδί, πάλι δεν είναι εύκολο να καταλάβει κανείς αν πρόκειται για την F_2 ή αν πρόκειται για μια f αφού αλλάζοντας το x αλλάζει με τυχαίο τρόπο η έξοδος.

3. Η F_3 δεν είναι ψευδοτυχαία. Έχοντας πρόσβαση στο Oracle της F και της F_3 και βάζοντας ως είσοδο το 0 στην F_3 εξασφαλίζεται ότι τα τελευταία n ψηφία γίνονται F(k, 0) το οποίο αποτελεί το κλειδί του πρώτου μισού. Συνεπώς, σε όλα τα υπόλοιπα loops γίνεται πρόβλεψη με πιθανότητα 1 για τα πρώτα n bits και έτσι:

$$\left|P\left[D^{F_k()}(1^n) = 1\right] - P\left[D^{F()}(1^n) = 1\right]\right| = 2^{-n} - 2^{-2n} = \frac{2^n - 1}{2^{2n}} \geq \text{negl}(2n)$$

Με άλλα λόγια, αν δοθεί πρώτα $F_3(k_0, 0^n)$ η έξοδος θα είναι $(F(k_0, 0^n), 0^n)||F(k_0, 0^n)$.

Αν όμως δοθεί $F_3(F(k_0, 0^n), 0^n)$ θα προκύψει ως έξοδος $(F(F(k_0, 0^n), 0^n), 0^n)||F(F(k_0, 0^n), 0^n))$.

Οπότε, τα n τελευταία bit της εξόδου θα είναι ίδια με τα πρώτα n bit της πρώτης εξόδου.

12η Άσκηση

Θεωρήστε την παραλλαγή του DES-X, με 2 κλειδιά k_1, k_2, όπου η κρυπτογράφηση ενός απλού κειμένου M γίνεται ως εξής:

$$Enc_{k_1,k_2}(M) = E_{k_1}(M \oplus k_2)$$

όπου E η συνάρτηση κρυπτογράφησης του DES.

Έχουμε περισσότερη ασφάλεια από τον κλασσικό DES στο παραπάνω σύστημα; Θεωρήστε ότι ο αντίπαλος έχει δυνατότητα KPA (διαθέτει αρκετά ζεύγη απλού κειμένου - κρυπτοκειμένου).

Λύση:

Έστω η συνάρτηση Dec(k, C) που αποκωδικοποιεί το κρυπτοκείμενο C που έχει κρυπτογραφηθεί με κλασσικό DES με κλειδί k.

Οπότε, θα ισχύει ότι $C = E_{k_1}(M \oplus k_2) \Rightarrow M \oplus k_2 = Dec(k_1, C) \Rightarrow k_2 = M \oplus Dec(k_1, C)$.

Επομένως, αρκεί να βρεθεί k_1 τέτοιο ώστε για δύο ζεύγη αρχικού κειμένου και κρυπτοκειμένου να δώσουν το ίδιο k_2.

Συνεπώς, το πρόβλημα ανάγεται σε Brute Force εύρεση του κλειδιού k_1 με δυο πράξεις ανά επανάληψη.

Άρα, η πολυπλοκότητα δεν αλλάζει σημαντικά στην Brute Force Approximation συγκριτικά με το κλασσικό DES.

Resources:

1. *Διαφάνειες Μαθήματος*
2. *https://theory.stanford.edu/~jvondrak/MATH233B-2017/lec3.pdf*
3. *Paul D. Humke: Lagrange's Theorem: Statement and Proof, April 5, 2012*
4. *Keith Conrad: Cosets and Lagrange's Theorem, The Miller-Rabin Test*
5. *Douglas R. Stinson, Maura B.Patterson. Cryptography Theory and Practice, Fourth Edition. CRC Press, 2019*
6. *Fomin, F.V., Kaski, P.: Exact exponential algorithms. Communications of the ACM 56(3), 80-88*
7. *https://cp-algorithms.com/algebra/phi-function.html*