Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Εθνικό Μετσόβιο Πολυτεχνείο
Ροή Λ, 9ο εξάμηνο

Υπολογιστική Κρυπτογραφία

Δεύτερη σειρά ασκήσεων

Σπουδαστής
Παπασκαρλάτος Αλέξανδρος (Α.Μ.: 03111097)

Ημερομηνία Υποβολής: 2 Νοεμβρίου 2019

Οι κώδικες που ζητούνται βρίσκονται σε ξεχωριστά αρχεία.
Σε αυτή τη σειρά, τα ζητούμενα προγράμματα υλοποιήθηκαν σε python, καθώς η python διαχειρίζεται εύκολα μεγάλους αριθμούς.

Άσκηση 1

Δίνεται πως το κρυπτοσύστημα διαθέτει τέλεια μυστικότητα για την ομοιόμορφη κατανομή πιθανότητας πάνω στα αρχικά κείμενα.

Λοιπόν, η πιθανότητα εμφάνισης ενός κρυπτοκειμένου είναι ανεξάρτητη από το αρχικό κείμενο.

Επομένως, η αλλαγή της κατανομής πιθανότητας στα αρχικά κείμενα, δεν επηρεάζει την πιθανότητα εμφάνισης ενός κρυπτοκειμένου.
$\forall x \in M, y \in C,$ τα ενδεχόμενα το αρχικό κείμενο να είναι το x και το κρυπτοκείμενο να είναι το y, είναι ανεξάρτητα.

Συνεπώς, το κρυπτοσύστημα διατηρεί την ιδιότητα της τέλειας μυστικότητας ακόμα και στην περίπτωση που ένα από τα αρχικά κείμενα εμφανίζεται με πιθανότητα 1/2, ενώ τα υπόλοιπα με πιθανότητα $1/2(|M| - 1)$.

Άσκηση 2

Ισχύει $(p-1)! \equiv -1 \pmod p$, όπου p πρώτος αριθμός

Απόδειξη

Περίπτωση: p = 2

Είναι $(p-1)! \equiv (2-1)! \equiv 1! \equiv 1 \equiv -1 \pmod 2$

Άρα ισχύει στην περίπτωση που p=2

Περίπτωση: p > 2

Καθώς ο p είναι πρώτος και $p \neq 2$, ο p είναι περιττός και άρα ο p-1 είναι άρτιος.

Επίσης, για κάθε τέτοιο p, $1 \not\equiv p-1 \pmod p$.

Κάθε στοιχείο α στο Z^*_p έχει αντίστροφο α^{-1} στο Z^*_p καθώς το Z^*_p είναι κυκλική ομάδα.

Επίσης, η εξίσωση $x^2 \equiv 1 \pmod p$ έχει ακριβώς δύο λύσεις στο Z^*_p καθώς ο p είναι πρώτος. Είναι οι λύσεις: $x_1 \equiv 1 \pmod p$ και $x_2 \equiv -1 \equiv p-1 \pmod p$.

Συνεπώς, όλα τα υπόλοιπα στοιχεία του Z^*_p μπορούν να χωριστούν σε δυάδες αντιστρόφων, δηλαδή (α, α^{-1}), (β, β^{-1}) κοκ.
Έχουμε p-3 τέτοια στοιχεία (αφού εξαιρέσαμε τα 1, p-1), οπότε προκύπτουν (p-3)/2 τέτοιες δυάδες.

Καθώς κάθε τέτοια δυάδα δίνει γινόμενο 1 (mod p) εάν πολλαπλασιάσουμε τα δύο επιμέρους στοιχεια της, προκύπτει:

$(p-1)! \equiv 1 \cdot (p-1) \cdot (\alpha_1 \cdot \alpha_1^{-1}) \cdot (\alpha_2 \cdot \alpha_2^{-1}) \cdot \ldots \cdot (\alpha_{(p-3)/2} \cdot \alpha_{(p-3)/2}) \equiv 1 \cdot (p-1) \cdot 1 \cdot 1 \cdot 1 \cdot \ldots \cdot 1 \equiv$
$\equiv p-1 \equiv -1 \pmod p$

Οπότε αποδείξαμε το ζητούμενο για p > 2.

Τελικά, ισχύει $\forall$ p prime, $(p-1)! \equiv -1 \pmod p$

Άσκηση 3

Είναι $x \equiv 25^{-1} \pmod{77}$

1ος τρόπος: Υπολογισμός με χρήση CRT

Είναι $25\,x \equiv 1 \pmod{77}$ και $77 = 7 \cdot 11$

Συνεπώς, ισχύουν τα κάτωθι:

- $25\,x \equiv 1 \pmod 7$
  $21\,x + 4\,x \equiv 1 \Leftrightarrow 4\,x \equiv 1 \Leftrightarrow x \equiv 4^{-1} \Leftrightarrow x \equiv 2 \pmod 7$

- $25\,x \equiv 1 \pmod{11}$
  $22\,x + 3\,x \equiv 1 \Leftrightarrow 3\,x \equiv 1 \Leftrightarrow x \equiv 3^{-1} \Leftrightarrow x \equiv 4 \pmod{11}$

Είναι $M = 77 = 7 \cdot 1$, $M_1 = M / 7 = 11$
$M_2 = M / 11 = 7$

Και $N_1 \equiv M_1^{-1} \pmod 7 \equiv 11^{-1} \equiv 2 \pmod 7$
$N_2 \equiv M_2^{-1} \pmod{11} \equiv 7^{-1} \equiv 8 \pmod{11}$

i	Eq	b_i	M_i	N_i	$b_i \cdot M_i \cdot N_i$
1	$x \equiv 2 \pmod 7$	2	11	2	44
2	$x \equiv 4 \pmod{11}$	4	7	8	224

Επομένως, $x \equiv \Sigma(b_i \cdot M_i \cdot N_i) \equiv 44 + 224 \equiv 268 \equiv 37 \pmod{77}$
Πράγματι, $25 \cdot 37 \equiv 925 \equiv 12 \cdot 77 + 1 \equiv 1 \pmod{77}$

2ος τρόπος: Επεκτεταμένος αλγόριθμος του Ευκλείδη

Είναι gcd(77, 25) = 1.
Επομένως, $\exists\ \kappa, \lambda \in Z$, $77\,\kappa + 25\,\lambda = 1$
Άρα, $25\,\lambda \equiv -77\kappa + 1 \equiv 1 \pmod{77} \Leftrightarrow \lambda \equiv 25^{-1} \pmod{77}$.
Θα υπολογίσουμε το λ, χρησιμοποιώντας τον επεκτεταμένο αλγόριθμο του Ευκλείδη.
$77 = 3 \cdot 25 + 2$
$25 = 12 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$

$1 = 25 - 12 \cdot 2 = 25 - 12\,(77 - 3 \cdot 25) = 36 \cdot 25 + 25 - 12 \cdot 77 = 37 \cdot 25 - 12 \cdot 77$
Συνεπώς, $\lambda = 37 \Rightarrow 25^{-1} \equiv 37 \pmod{77}$

3ος τρόπος: Θεώρημα του Euler

Είναι gcd(25, 77) = 1 $\Rightarrow 25^{\varphi(77)} \equiv 1 \pmod{77}$
$\varphi(77) = 77\,(1 - 1/7)\,(1 - 1/11) = 77\,(6/7)\,(10/11) = 60$
Άρα $25^{60} \equiv 1 \Leftrightarrow 25 \cdot 25^{59} \equiv 1 \Leftrightarrow 25^{59} \equiv 25^{-1} \pmod{77}$
Και $25^{59} \equiv 37 \pmod{77}$

Άσκηση 4

Έστω $a \in \cup (Z_n)$ τάξης k και $b \in \cup (Z_n)$ τάξης m.
Ισχύει πως $ab \in \cup (Z_n)$ έχει τάξη km, αvv gcd(k, m) =1

Απόδειξη

⇒ (Ισχύει πως το ab έχει τάξη km)

Block άτοπο: Έστω gcd(k, m) > 1

- Εφόσον gcd(k, m) > 1, οι k, m δεν είναι σχετικά πρώτοι.
- $\exists\ t \in Z, t > 1,\ \ t \mid k\ \wedge\ t \mid m$
- $\exists\ c, d\ \exists\ Z,\quad k = c \cdot t\ \wedge\ m = d \cdot t$
- Είναι $(ab)^{c\,d\,t} \equiv a^{c\,d\,t}\, b^{c\,d\,t} \equiv (a^{c\,t})^{d}\, (b^{d\,t})^{c} \equiv a^{k\,d}\, b^{m\,c} \equiv 1^{d}\, 1^{c} \equiv 1$
- Συνεπώς, η τάξη του ab είναι το πολύ $c \cdot d \cdot t$.
- Όμως, $k \cdot m = c \cdot t \cdot d \cdot t = (c \cdot d \cdot t) \cdot t > c \cdot d \cdot t$

Άτοπο, καθώς από υπόθεση, το ab έχει τάξη km
Επομένως, gcd(k,m) = 1

⇐ (Ισχύει πως gcd(k, m) = 1

Περίπτωση k = 1 ή m = 1

Χωρίς βλάβη της γενικότητας, θεωρούμε πως k = 1.
Τότε, $a^{k} \equiv 1 \Leftrightarrow a^{1} \equiv 1 \Leftrightarrow a \equiv 1$.
Έστω r η τάξη του ab, τότε $(ab)^{r} \equiv 1 \Leftrightarrow b^{r} \equiv 1$.
Το μικρότερο αποδεκτό r που να ικανοποιεί την άνωθι σχέση είναι η τάξη του b.
Δηλαδή, $r = m = 1 \cdot m = k \cdot m$.

Επομένως, ισχύει στην περίπτωση που k = 1 ή m = 1.

Περίπτωση k > 1 ∧ m > 1

Έστω r η τάξη του ab.
Block άτοπο: Έστω r = 1

- Είναι $(ab)^{r} \equiv 1 \Leftrightarrow (ab)^{1} \equiv 1 \Leftrightarrow ab \equiv 1$
- $ab \equiv 1 \Leftrightarrow (ab)^{k} \equiv 1 \Leftrightarrow a^{k}\, b^{k} \equiv 1 \Leftrightarrow 1 \cdot b^{k} \equiv 1 \Leftrightarrow b^{k} \equiv 1$
- Το b έχει τάξη m και $b^{k} \equiv 1$, άρα $m \mid k$

Άτοπο, καθώς gcd(m, k) = 1, δηλαδή τα m, k σχετικά πρώτα και m > 1.
Επομένως, **r > 1**.

Είναι $(ab)^{k\,m} \equiv a^{k\,m}\, b^{m\,k} \equiv 1^{m}\, 1^{k}$ ⇒ $\mathbf{(ab)^{k\,m} \equiv 1}$

Block άτοπο: Έστω $r \neq k \cdot m$ (*Ολόκληρη αυτή η σελίδα είναι ένα ενιαίο άτοπο)

- Είναι r η τάξη του ab με $r \neq k \cdot m$ και $(ab)^{k\,m} \equiv 1$. Άρα $r < k \cdot m$

  Subblock άτοπο (φωλιασμένο): Έστω $k \mid r$
  - $\exists\ t \in Z, t > 1,\ r = t \cdot k$
  - $(ab)^r \equiv 1 \Leftrightarrow a^r b^r \equiv 1 \Leftrightarrow a^{t\,k} b^r \equiv 1 \Leftrightarrow (a^k)^t b^r \equiv 1 \Leftrightarrow 1^t b^r \equiv 1 \Leftrightarrow b^r \equiv 1$
  - $b^r \equiv 1 \wedge$ τάξη του b είναι m, οπότε $m \mid r \Leftrightarrow m \mid t \cdot k$
  - $m \mid t \cdot k \wedge \gcd(k, m) = 1 \Rightarrow m \mid t$
  - $m \mid t \Rightarrow \exists\ c \in N^*,\quad t = c \cdot m$
  - $r = t \cdot k = c \cdot m \cdot k = c \cdot (k \cdot m)$, με $c \geq 1$
  - $r = c \cdot (k \cdot m) \geq k \cdot m$

  Άτοπο, καθώς από υπόθεση, $r < k \cdot m$
  Επομένως, $\mathbf{k \nmid r}$.

  Subblock άτοπο (φωλιασμένο): Έστω $r \mid k$
  - $r \mid k \Rightarrow \exists\ c\ \exists\ N^*,\ k = c \cdot r$
  - $(ab)^k \equiv (ab)^{c \cdot r} \equiv ((ab)^r)^c \equiv 1^c \equiv 1$
  - $(ab)^k \equiv 1 \Leftrightarrow a^k b^k \equiv 1 \Leftrightarrow b^k \equiv 1$
  - $b^k \equiv 1 \wedge$ η τάξη του b είναι m, οπότε $m \mid k$

  Άτοπο, καθώς $\gcd(k, m) = 1$ και $m > 1$.
  Επομένως, $\mathbf{r \nmid k}$.

  Subblock άτοπο (φωλιασμένο): Έστω $\gcd(m, r) \neq 1$
  - $\gcd(m,r) \neq 1 \Rightarrow$ Τα m, r έχουν κοινό πρώτο παράγοντα, έστω p .
  - $\exists\ c, d \in N^*,\quad m = c \cdot p \wedge r = d \cdot p$
  - Είναι $(ab)^{c\,d\,p} \equiv ((a\,b)^{d\,p})^c \equiv (ab)^{r\,c} \equiv 1^c \equiv 1$
  - Είναι $(ab)^{c\,d\,p} \equiv 1 \Leftrightarrow a^{m\,d} b^{m\,d} \equiv 1 \Leftrightarrow a^{m\,d} 1^d \equiv 1 \Leftrightarrow a^{m\,d} \equiv 1$
  - $a^{m\,d} \equiv 1 \wedge$ η τάξη του a είναι k, οπότε $k \mid m \cdot d$
  - $k \mid m \cdot d \wedge \gcd(k, m) = 1 \Rightarrow k \mid d$
  - $k \mid d \Rightarrow k \mid d \cdot p \Rightarrow k \mid r$

  Άτοπο, καθώς $k \nmid r$, από προηγούμενο subblock άτοπο.
  Επομένως, **gcd(m, r) = 1**.

- $(ab)^{k\,m} \equiv 1 \wedge$ η τάξη του ab είναι r, οπότε $r \mid k \cdot m$
- $r \mid k \cdot m \wedge \gcd(m, r) = 1 \Rightarrow r \mid k$

Άτοπο, καθώς $r \nmid k$.
Επομένως, $\mathbf{r = k \cdot m}$

Τελικά αποδείξαμε πως το ab έχει τάξη k m σε κάθε περίπτωση.

Άσκηση 5

Έγραψα κώδικα python για έλεγχο πρώτων αριθμών Fermat.
Πρόκειται για το αρχείο Crypto_ex_2_5.py .

Σύμφωνα με το μικρό θεώρημα Fermat:
$\forall$prime p, $\forall a \in Z, p \nmid a : a^{p-1} \equiv 1 \pmod p$

Κατά τον έλεγχο ενός αριθμού p για primality σύμφωνα με το Fermat test, επιλέγουμε έναν τυχαίο αριθμό a και υπολογίζουμε το $a^{p-1} \pmod p$.
Εάν το αποτέλεσμα δεν είναι μονάδα, ο p είναι σύνθετος.
Διαφορετικά, δοκιμάζουμε με διαφορετικό a.
Εάν ο p είναι πρώτος, το αποτέλεσμα θα είναι μονάδα για οποιοδήποτε a και να διαλέξουμε.

Σημειώνω πως η ύψωση σε δύναμη modulo p γίνεται αποδοτικά με επαναλαμβανόμενο τετραγωνισμό.

Στο πρόγραμμά μου, δέχομαι πως ένας αριθμός είναι (μάλλον) πρώτος, αν περνάει το Fermat test με 30 τυχαίες τιμές για το a.

Λοιπόν, προκύπτει πως:
Το [67280421310721] είναι (μάλλον) πρώτος.
Το [170141183460469231731687303715884105721] δεν είναι πρώτος.
Το [$2^{2281} - 1$] είναι (μάλλον) πρώτος.
Το [$2^{9941} - 1$] είναι (μάλλον) πρώτος.
Το [$2^{19939} - 1$] δεν είναι πρώτος.

Γράφω πως οι αριθμοί που περνάνε τα τεστ είναι μάλλον πρώτοι και όχι σίγουρα, γιατί υπάρχει μια μικρή περίπτωση να είναι σύνθετοι,
είτε γιατί από υπερβολική ατυχία, παρότι δοκιμάσαμε 30 τιμές για το a, δεν έτυχε να επιλέξουμε έναν compositeness witness παρότι υπάρχουν τέτοιοι μάρτυρες,
ή γιατί το κόλπο ήταν στημένο και πρόκειται για αριθμό Carmichael, δηλαδή δεν υπάρχουν τέτοιοι μάρτυρες, οπότε ακόμα και αν το Fermat test ήταν εξονυχιστικό, δε θα μπορούσαμε να κρίνουμε το primality του αριθμού.

Άσκηση 6

Έστω Z^*_p με p πρώτο και g ένας γεννήτορας, p, g γνωστά.

Στα κάτωθι, όλες οι ισοτιμίες αφορούν το mod p.
Οπότε, χάριν συντομίας, το (mod p) θα παραλείπεται στις ισοτιμίες, δηλαδή ∀ a, b,
η έκφραση $x \equiv y$ θα ισοδυναμεί με την $x \equiv y \pmod p$

1. Για d ακέραιο που διαιρεί το p-1, ένα στοιχείο b του Z^*_p με τάξη d είναι το $\mathbf{b \equiv g^{(p-1)/d}}$.

Απόδειξη

Καταρχάς, είναι $b^d \equiv g^{p-1} \equiv 1$, καθώς ο g είναι γεννήτορας, οπότε η τάξη του ισούται με την πληθικότητα του Z^*_p, δηλαδή p-1.

Block άτοπο : Έστω η τάξη του b είναι $k \neq d$

- Καθώς, $b^d \equiv 1$, πρέπει $k < d$.
- Επειδή η τάξη του b είναι k, ισχύει πως $b^k \equiv 1$.
- $a^k \equiv 1 \Leftrightarrow g^{k\,(p-1)\,/\,d} \equiv 1$
- Όμως, $k < d \Leftrightarrow k/d < 1 \Leftrightarrow (k/d)\,(p-1) < p-1$

Άτοπο, καθώς η τάξη του g είναι p-1.
Επομένως, η τάξη του $b = g^{(p-1)/d}$ είναι d.

2, 3, 4. Εάν δεχτούμε όσα αναφέρονται στις διαφάνειες του μαθήματος ως δεδομένη γνώση, τότε όλα είναι γνωστά από τη θεωρία:
Υπάρχει ακριβώς μία κυκλική υποομάδα τάξης d στο Z^*_p.
Η κυκλική υποομάδα τάξης d, που παράγει ένα στοιχείο τάξης d, έχει φ(d) γεννήτορες.
Συνεπώς, υπάρχουν ακριβώς φ(d) στοιχεία τάξης d στο Z^*_p.

Εάν ζητείται όντως να αποδείξω αυτές τις προτάσεις, και όχι να τις εκλάβω ως δεδομένες, έχουμε τα κάτωθι (για τα ερωτήματα 2, 3, 4):
Μου είναι πιο βολικό να απαντήσω πρώτα στα ερωτήματα (3), (4) και, έπειτα, στο (2).

3. Θδο πως μια ομάδα τάξης d έχει φ(d) γεννήτορες.
Έστω B μια ομάδα τάξης d και b ένας γεννήτορας.
Το b έχει τάξη d, $b^d \equiv 1$.
Έστω $m \in N$, $m \leq d$ και $\gcd(m, d) \neq 1$.
Καθώς $\gcd(m, d) \neq 1$, τα m, d δεν είναι σχετικά πρώτοι.
Συνεπώς, $\exists\ t, \mu, \delta \in N,\ t > 1\ \ m = \mu \cdot t, \qquad d = \delta \cdot t$
Για το στοιχείο $h = b^m$, ισχύει πως $h^\delta \equiv b^{m\,\delta} \equiv b^{\mu\,t\,\delta} \equiv (b^{\delta\,t})^\mu \equiv (b^d)^\mu \equiv 1^\mu \equiv 1$,
δηλαδή το $h = b^m$ έχει τάξη το πολύ $\delta < d$.
Επίσης, για κάθε $m \leq d$, προκύπτει κάποιο διαφορετικό στοιχείο b^m καθώς το b είναι γεννήτορας και $m \leq d$.
Επομένως, για κάθε $m \leq d$, με m μη σχετικά πρώτο με το d, το στοιχείο b^m δεν είναι γεννήτορας.

Τώρα μένει να αποδείξουμε πως έχει ακριβώς φ(d) γεννήτορες.
Αρκεί να αποδείξουμε πως όλα τα στοιχεία που δεν εξετάσαμε πριν, είναι γεννήτορες.
Δηλαδή, πως για $m \in N$, $m \leq d$, $\gcd(m, d) = 1$, το $h = b^m$ είναι γεννήτορας.
Block άτοπο : Έστω ότι το προαναφερθέν $h = b^m$ δεν είναι γεννήτορας

- Καθώς το h δεν είναι γεννήτορας, το h έχει τάξη $r < d$.
- Είναι $h^r \equiv 1 \Leftrightarrow b^{m\,r} \equiv 1$
- $b^{m\,r} \equiv 1 \ \wedge$ η τάξη του b είναι d, οπότε $d \mid m \cdot r$
- $d \mid m \cdot r \ \wedge \ \gcd(d, m) = 1 \ \Rightarrow \ d \mid r \ \Rightarrow \ d \leq r$

Άτοπο, καθώς $r < d$.
Επομένως, το στοιχείο $h = b^m$ με $\gcd(m, d) = 1$ είναι γεννήτορας.

Τελικά, απέδειξα πως γεννήτορες της ομάδας B είναι όλα τα στοιχεία της μορφής $h = b^m$,
όπου $m \leq d$ σχετικά πρώτο με το d και b γεννήτορας της B, και μόνον αυτά.
Συνεπώς, η ομάδα τάξης d έχει ακριβώς φ(d) γεννήτορες.
(Θυμίζουμε πως μια υποομάδα τάξης d έχει d στοιχεία.)

4. Θδο πως το Z^*_p έχει μοναδική υποομάδα τάξης d.
Καταρχάς, από το ερώτημα (1) έχουμε δείξει πως υπάρχει στοιχείο τάξης d (το $b = g^{(p-1)\,/\,d}$), το οποίο αποτελεί και γεννήτορα ομάδας τάξης d.
Συνεπώς, υπάρχει μια υποομάδα τάξης d.

Τώρα, μένει να αποδείξουμε πως η υποομάδα αυτή είναι μοναδική.
Το g είναι γεννήτορας του Z^*_p (προφανώς με τάξη p-1), συνεπώς κάθε στοιχείο του Z^*_p έχει τη μορφή g^k για κάποιο k.
Επίσης, το στοιχείο $b = g^{(p-1)/d}$ είναι γεννήτορας τάξης d (από ερώτημα (1)).

Έστω το στοιχείο $h = g^k$ τάξης d. Ισχύουν τα κάτωθι:

- $h^d \equiv 1 \Leftrightarrow g^{k\,d} \equiv 1$.
- $g^{k\,d} \equiv 1 \ \wedge$ η τάξη του g είναι (p-1), οπότε $(p-1) \mid k \cdot d$.
- $\exists\ t \in N, \quad k \cdot d = t \cdot (p-1) \ \Leftrightarrow \ k = t \cdot (p-1) / d$
- $h = g^k = g^{t\,(p-1)\,/\,d} = b^t$

Συνεπώς, το στοιχείο h τάξης d, σίγουρα προκύπτει ως το στοιχείο $b = g^{(p-1)\,/\,d}$ υψωμένο σε κάποια δύναμη t, άρα σίγουρα ανήκει στην υποομάδα B τάξης d, που σχηματίζει το στοιχείο b ως γεννήτορας.
Επομένως, όλα τα στοιχεία τάξης d ανήκουν στην υποομάδα που σχηματίζει το στοιχειο b.
Επειδή, όλα αυτά τα στοιχεία έχουν τάξη ίση με την πληθικότητα της υποομάδας και ανήκουν στην υποομάδα, προφανώς σχηματίζουν την ίδια υποομάδα εάν χρησιμοποιηθούν ως γεννήτορες.
Δηλαδή, όλα τα στοιχεία τάξης d σχηματίζουν την ίδια υποομάδα.

Τελικά, το Z^*_p έχει μοναδική υποομάδα τάξης d.

2. Υπάρχει ακριβώς μία κυκλική υποομάδα τάξης d στο Z^*_p (από το ερώτημα (4)).
Η κυκλική υποομάδα τάξης d, που παράγει ένα στοιχείο τάξης d, έχει φ(d) γεννήτορες (από το ερώτημα (3)).
Συνεπώς, υπάρχουν ακριβώς φ(d) στοιχεία τάξης d στο Z^*_p.

5. Έστω στοιχείο h τάξης d και H η υποομάδα που παράγει το h.
Τότε, για στοιχείο a, είναι:
$a^d \equiv 1 \Leftrightarrow a \in H$
Απόδειξη
$\Rightarrow$ (Ισχύει $a^d \equiv 1$)

Είναι $a^d \equiv 1$.

Εάν το a έχει τάξη d, τότε ανήκει στην H, καθώς η υποομάδα τάξης d είναι μοναδική.

Εάν το a έχει τάξη k, τότε το a ανήκει στη μοναδική υποομάδα τάξης k, έστω K.
Είναι $a^d \equiv 1$ $\wedge$ η τάξη του a είναι k, οπότε $k \mid d$.
Ισχύει $k \mid d$ και το στοιχείο $h^{d/k}$ έχει τάξη k (απόδειξη όμοια με το 6.1).
Συνεπώς το $h^{d/k}$ είναι γεννήτορας της K.
Επομένως, $\exists\ r \in N, r \le k,$ $(h^{d/k})^r \equiv a$.
Και $h^{r\ d/k} \equiv a$, άρα το a ανήκει στην H, καθώς σχηματίζεται από τον γεννήτορα h υψωμένο σε κάποια δύναμη $(r \cdot d / k)$.

Συνολικά, ισχύει σε κάθε περίπτωση.

$\Leftarrow$ (Ισχύει $a \in H$)

Είναι $a \in H$, άρα $\exists\ r \in N, r \le d,$ $a \equiv h^r$.
Οπότε είναι, $a^d \equiv h^{d\ r} \equiv 1^r \equiv 1$.

Άσκηση 7

Έγραψα κώδικα python ο οποίος υπολογίζει τα τελευταία 16 ψηφία του αριθμού 1707 ↑↑ 1783, όπου ο τελεστής ↑↑ ορίζεται ως εξής: $\alpha \uparrow\uparrow (n + 1) = \alpha^{\alpha \uparrow\uparrow n}$ με $\alpha \uparrow\uparrow 1 = \alpha$.
Πρόκειται για το αρχείο Crypto_ex_2_7.py .

Προκειμένου να βρούμε τα τελευταία 16 ψηφία του 1707 ↑↑ 1783, κάνουμε την πράξη $(1707 \uparrow\uparrow 1783) \bmod 10^{16}$.

Βασιζόμαστε στο θεώρημα του Euler:
$\forall a \in Z, \quad \gcd(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

Λοιπόν, για a, m σχετικά πρώτα, είναι:
$\forall\ k, r \in Z, \quad a^{k\,\varphi(m) + r} \equiv (a^{\varphi(m)})^k a^r \equiv 1 \cdot a^r \equiv a^r \pmod m$
Άρα $\forall\ d \in Z, \quad a^d \equiv a^{d \pmod{\varphi(m)}} \pmod m$.

Προφανώς, αν φ(m) = 1 (δηλαδή m=2), $a^d \equiv 1 \pmod m$, ανεξαρτήτως της τιμής του d.
Θυμίζω πως αναφερόμαστε σε a, m σχετικά πρώτα, άρα a περιττό.

Επίσης, γνωρίζουμε πως για σύνθετο n, $\phi(n) = n \prod_{p \mid n} (1 - (1/p))$.
Οπότε, $\varphi(10^{16}) = \varphi(2^{16}\, 5^{16}) = 10^{16} (1 - ½) (1 - ⅕) = 10^{16} \cdot ⅖ = 2^{17}\, 5^{15}$.
Μάλιστα, $\forall\ a, b \in N^*, \varphi(2^a\, 5^b) = 2^a\, 5^b \cdot ⅖ = 2^{a+1}\, 5^{b-1}$
Και $\forall\ a \in N^*, \quad \varphi(2^a) = 2^{a-1}$

Αξιοποιώντας τα παραπάνω (και το γεγονός πως το 2 και το 5 δεν είναι πρώτοι παράγοντες του 1707), έγραψα κώδικα που χρησιμοποιεί αναδρομή για να υπολογίσει το ζητούμενο.

Κατέληξα πως **$1707 \uparrow\uparrow 1783 \equiv 80500540924243 \pmod{10^{16}}$** .