ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ
ΣΗΜΕΙΩΣΕΙΣ #5

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

1. Υπολογισμοι στην ομαδα $(\mathbb{Z}/p\mathbb{Z})^*$

Έστω πρώτος p. Το σύνολο $(\mathbb{Z}/p\mathbb{Z})$ εφοδιασμένο με πρόσθεση και πολλαπλασιασμό «modulo p» είναι σώμα. Το $(\mathbb{Z}/p\mathbb{Z})^*$ είναι η πολλαπλασιαστική ομάδα του σώματος και είναι κυκλική. Αυτό προκύπτει από την παρακάτω γενική πρόταση.

Πρόταση 1.1. *Κάθε πεπερασμένη υποομάδα της πολλαπλασιαστικής ομάδας ενός σώματος είναι κυκλική.*

Επομένως υπάρχει $g \in (\mathbb{Z}/p\mathbb{Z})^*$ που γεννά την ομάδα, που έχει δηλαδή τάξη $p-1$. Στόχος μας εδώ είναι να απαντήσουμε στις παρακάτω ερωτήσεις:

(1) Δεδομένου ενός στοιχείου $g \in (\mathbb{Z}/p\mathbb{Z})^*$, είναι το g γεννήτορας;
(2) Να βρεθεί ένας γεννήτορας της ονάδας $(\mathbb{Z}/p\mathbb{Z})^*$.

Και τις δύο ερωτήσεις θα τις απαντήσουμε δεδομένης της ανάλυσης της τάξης $p-1$ σε πρώτους παράγοντες.

2. Ελεγχος ταξης στοιχειου

Έστω πεπερασμένη κυκλική ομάδα G τάξης $n = q_1^{a_1} \cdots q_t^{a_t}$. Υποθέτουμε ότι τα $q_1, \ldots, q_t$ και $a_1, \ldots, a_t$ είναι γνωστά. Ο αλγόριθμος στηρίζεται στο παρακάτω λήμμα.

Λήμμα 2.1. *Έστω G πεπερασμένη κυκλική ομάδα τάξης $n = q_1^{a_1} \cdots q_t^{a_t}$ και $g \in G$. Αν $g^{n/q_j} \neq 1$ τότε $q_i^{a_j} | \mathrm{ord}(g)$.*

Απόδειξη. Έστω $s = \mathrm{ord}(g)$. Τότε το s είναι διαιρέτης του n, οπότε είναι της μορφής $s = q_1^{b_1} \cdots q_t^{b_t}$ με $0 \leq b_i \leq a_i$ για $1 \leq i \leq t$. Ας υποθέσουμε ότι το $q_j^{a_j}$ δεν διαιρεί το s. Αυτό σημαίνει ότι $b_j \leq a_j - 1$. Όμως τότε

$$\frac{n}{q_j} = q_1^{a_1} \cdots q_{j-1}^{a_{j-1}} q_j^{a_j - 1} q_{j+1}^{a_{j+1}} \cdots q_t^{a_t}$$

το οποίο είναι πολλαπλάσιο του s. Συνεπώς $g^{n/q_j} = 1$, άτοπο. □

Πρόταση 2.2. *Έστω G πεπερασμένη κυκλική ομάδα τάξης $n = q_1^{a_1} \cdots q_t^{a_t}$ και $g \in G$. $g^{n/q_j} \neq 1$ για $1 \leq i \leq t$ αν και μόνο αν $\mathrm{ord}(g) = n$.*

Απόδειξη. Αν $\mathrm{ord}(g) = n$ είναι φανερό ότι $g^{n/q_j} \neq 1$ για $1 \leq i \leq t$. Θα δείξουμε την αντίθετη κατεύθυνση. Έστω, λοιπόν, ότι $g^{n/q_j} \neq 1$ για $1 \leq i \leq t$. Από το λήμμα προκύπτει ότι $q_i^{a_i} | \mathrm{ord}(g)$ για $1 \leq i \leq t$. Ακόμη $(q_i^{a_i}, q_j^{a_j}) = 1$ για $i \neq j$. Οπότε $\prod_{i=1}^t q_i^{a_i} | \mathrm{ord}(g)$. Επίσης, από το Θεώρημα του Lagrange $\mathrm{ord}(g) | \prod_{i=1}^t q_i^{a_i} = n$. Άρα $\mathrm{ord}(g) = \prod_{i=1}^t q_i^{a_i} = n$. □

Σύμφωνα με την τελευταία πρόταση, για να ελέγξουμε αν ένα δεδομένο στοιχείο g γεννά την ομάδα G, αρκεί να ελέγξουμε αν $g^{n/q_i} \neq 1$ για $1 \leq i \leq t$. Αυτός είναι ο αλγόριθμος! Ας μετρήσουμε τώρα τις πράξεις (στην ομάδα) που χρειάζεται ο αλγόριθμος. Χρειάζεται t υψώσεις σε δύναμη. Κάθε ύψωση μπορεί να γίνει με $O(\log n)$ πράξεις στην ομάδα. Άρα τελικά χρειάζονται $O(t \log n)$ πράξεις. Δείτε τώρα ότι $n = q_1^{a_1} \cdots q_t^{a_t} \geq 2 \cdots 2 = 2^t$ οπότε $t \log 2 \leq \log n$. Συνολικά, λοιπόν, ο αλγόριθμος μας κάνει $O((\log n)^2)$ πράξεις στην ομάδα.

Παράδειγμα 2.3. Έστω ο πρώτος $p = 101$. Θα ελέγξουμε αν ο $a = 2$ είναι γεννήτορας της ομάδας $(\mathbb{Z}/p\mathbb{Z})^*$. Κατ' αρχάς χρειαζόμαστε την παραγοντοποίηση $p - 1 = 2^2 5^2$. Σύμφωνα με την Πρόταση 2.2 θα χρειαστεί να κάνουμε δύο ελέγχους. Βλέπουμε ότι $2^{(p-1)/2} \equiv 2^{50} \equiv -1 \pmod{p}$ και $2^{(p-1)/5} \equiv 2^{20} \equiv 95 \pmod{p}$. Άρα η τάξη του 2 είναι $p - 1$ και το 2 γεννά την ομάδα.

3. Εύρεση γεννήτορα

Έστω πεπερεασμένη κυκλική ομάδα G τάξης n και γεννήτορας $g \in G$. Τότε $G = \{g^t \ : \ 0 \leq t \leq n-1\}$. Ποιά από τα στοιχεία τα στοιχεία της G είναι γεννήτορες; Η απάντηση δίνεται από την παρακάτω πρόταση.

Πρόταση 3.1. *Έστω πεπερεασμένη κυκλική ομάδα G τάξης n και γεννήτορας $g \in G$. Η τάξη του στοιχείου g^t είναι $n/(n,t)$.*

Απόδειξη. Ας ονομάσουμε $s = \mathrm{ord}(g^t)$. Επίσης ας είναι $d = (n,t)$, $n = dn_1$, $t = dt_1$. Βλέπουμε ότι $(n_1, t_1) = 1$. Θα δείξουμε ότι $s = n_1$.

Έχουμε

$$(g^t)^{n_1} = g^{tn_1} = g^{t_1 n} = 1,$$

οπότε $s | n_1$.

Επίσης,

$$1 = (g^t)^s = g^{ts},$$

οπότε $n | ts$. Άρα υπάρχει $\lambda \in \mathbb{Z}$ τέτοιο ώστε $ts = \lambda n$. Άρα $t_1 s = \lambda n_1$. Καθώς $(n_1, t_1) = 1$ προκύπτει ότι $n_1 | s$. Άρα τελικά $s = n_1$. □

Πρόταση 3.2. *Έστω πεπερεασμένη κυκλική ομάδα G τάξης n και γεννήτορας $g \in G$. Το σύνολο των γεννητόρων της G είναι το $\{g^t \ : \ 1 \leq t < n, \ (n,t) = 1\}$. Το πλήθος των γεννητόρων είναι $\phi(n)$.*

Απόδειξη. Από την προηγούμενη πρόταση προκύπτει ότι το σύνολο των στοιχείων της G που έχουν τάξη n είναι ακριβώς το $\{g^t \ : \ 1 \leq t < n, \ (n,t) = 1\}$. Το πλήθος των στοιχείων του συνόλου είναι $\phi(n)$. □

Βλέπουμε ότι αν επιλέξουμε ένα στοιχείο από την G τυχαία με ομοιόμορφη κατανομή (εφόσον φυσικά μπορούμε να το κάνουμε αυτό), τότε η πιθανότητα να επιλέξουμε γεννήτορα είναι $\phi(n)/n$. Άρα κατά μέσο όρο πρέπει να επιλέξουμε (τυχαία) $n/\phi(n)$ στοιχεία μέχρι να βρούμε γεννήτορα. Για να ελέγξουμε αν το εκάστοτε στοιχείο είναι ή όχι γεννήτορας χρησιμοποιούμε το τέστ της προηγούμενης εννότητας.

Πόσο μεγάλη μπορεί να γίνει η ποσότητα $n/\phi(n)$; Όχι πολύ μεγάλη, όπως δείχνει η παρακάτω πρόταση.

Πρόταση 3.3. *Υπάρχει σταθερά $A > 0$ τέτοια ώστε*

$$\frac{\phi(n)}{n} \geq \frac{A}{\log n}, \quad n \geq 2.$$

Απόδειξη. Υπολογίζουμε

$$\begin{aligned}
\frac{\phi(n)}{n} &= \prod_{p|n}\left(1-\frac{1}{p}\right) \\
&\geq \prod_{p\leq n}\left(1-\frac{1}{p}\right) \\
&= \exp\left(\log\left(\prod_{p\leq n}\left(1-\frac{1}{p}\right)\right)\right) \\
&= \exp\left(\sum_{p\leq n}\log\left(1-\frac{1}{p}\right)\right) \\
&\geq \exp\left(-\sum_{p\leq n}\frac{1}{p}\right)\exp\left(-\sum_{p\leq n}\frac{1}{p^2}\right),
\end{aligned}$$

όπου χρησιμοποιήσαμε ότι $\log(1-x) \geq -x - x^2$ για $x \in [0, 1/2]$. Η σειρά $\sum_{k=1}^{\infty} 1/k^2$ συγκλίνει σε κάποιο θετικό αριθμό B. Οπότε

$$\sum_{p\leq n}\frac{1}{p^2} \leq \sum_{p}\frac{1}{p^2} \leq \sum_{k=1}^{\infty}\frac{1}{k^2} = B.$$

Έχουμε λοιπόν,

$$\frac{\phi(n)}{n} \geq \exp(-B)\exp\left(-\sum_{p\leq n}\frac{1}{p}\right).$$

Στο σημείο αυτό χρειαζόμαστε το παρακάτω στοιχειώδες (αλλά όχι απλό) αποτέλεσμα. Υπάρχει σταθερά C τέτοια ώστε

$$\left|\sum_{p\leq n}\frac{1}{p} - \log\log n\right| \leq C, \quad n \geq 2.$$

Επομένως,

$$\sum_{p\leq n}\frac{1}{p} \leq \log\log n + C.$$

Χρησιμοποιώντας το παραπάνω αποτέλεσμα, έχουμε

$$\frac{\phi(n)}{n} \geq \exp(-B)\exp(-C)\exp(-\log\log n) = \frac{A}{\log n},$$

όπου $A = \exp(-B-C)$.

□