ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ
ΣΗΜΕΙΩΣΕΙΣ #6

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

1. Το πρόβλημα του διακριτού λογαρίθμου

Στο μάθημα αυτό θα δούμε κάποιους αλγόριθμους για υπολογισμό διακριτών λογάριθμων. Θυμίζουμε ότι στο πρόβλημα του διακριτού λογάριθμου (**DL**), μας δίνεται μια ομάδα G, ένα στοιχείο $g \in G$ τάξης $n > 1$ και κάποιο $y \in \langle g \rangle$ και θέλουμε να υπολογίσουμε το μικρότερο μη αρνητικό ακέραιο x τέτοιο ώστε $y = g^x$. Αρχικά θα περιγράψουμε δύο αλγόριθμους που μπορούν να εφαρμοστούν σε οποιαδήποτε ομάδα G. Τέτοιους αλγόριθμους τους ονομάζουμε γενικούς. Είναι φανερό ότι το x μπορεί να βρεθεί αν υπολογίσουμε με τη σείρα τα g^k για $k = 0, 1, 2, \ldots, n-1$, και σε κάθε βήμα να συγκρίνουμε το g^k με το y. Όταν είναι ίσα έχουμε βρει το x. Ο αλγόριθμος αυτός ονομάζεται συχνά και τετριμμένος και χρειάζεται $O(n \log n)$ πράξεις στη G. Στις επόμενες παραγράφους θα περιγράψουμε αλγόριθμους που βελτιώνουν το φράγμα αυτό.

2. Ο αλγοριθμος Baby-step/Giant-step

Ο αλγόριθμος αυτός είναι του D. Shanks. Έστω ότι μας δίνεται το $g \in G$ τάξης n (γνωστής) και το $y \in \langle g \rangle = \{g^k \mid 0 \leq k \leq n-1\}$. Θέλουμε να υπολογίσουμε το $0 \leq x \leq n-1$ τέτοιο ώστε $y = g^x$.

Έστω $1 < q < n$ ένας ακέραιος. Τότε γράφοντας την εξίσωση της διαίρεσης με υπόλοιπο του x (που δεν ξέρουμε) με το q έχουμε

$$x = q \cdot i_0 + j_0, \quad \text{με } 0 \leq i_0 < \frac{n}{q} \text{ και } 0 \leq j_0 < q.$$

Φυσικά τα i και j δεν τα ξέρουμε. Όμως ξέρουμε ότι υπάρχουν και ότι αν υπολογίσουμε τα i_0 και j_0 θα έχουμε υπολογίσει το x. Αυτό θα κάνουμε. Γράφουμε

$$\begin{aligned} g^x = y &= g^{qi_0+j_0} \iff \\ yg^{-j_0} &= g^{gi_0}. \end{aligned}$$

Η τελευταία εξίσωση υποδεικνύει τον ακόλουθο αλγόριθμο.

(1) Υπολόγισε τα $u = g^{-1}$ και $w = g^q$.
(2) Για $j = 0, 1, \ldots, \lfloor n/q \rfloor$ υπολόγισε το yu^j και αποθήκευσε τα (yu^j, j).

(3) Για $i = 0, 1, \ldots, q-1$ υπολόγισε το w^i και για κάθε μία τιμή που υπολογίζεις, κοίτα αν το w^i είναι το πρώτο μέλος κάποιου ζεύγους που έχεις υπολογίσει στο βήμα (2).
(4) Οταν βρείς το i_0 τέτοιο ώστε $w^{i_0} = yu^{j_0}$, απάντησε $x = qi_0 + j_0$.

Η ορθότητα του αλγόριθμου είναι φανερή από όσα είπαμε παραπάνω. Πόσες πράξεις στη G κάνει ο αλγόριθμος; Έχουμε $O(\log q)$ πράξεις στο βήμα (1), $O(\lfloor n/q \rfloor \log(n/q))$ πράξεις στο βήμα (2) και $O(q \log q)$ πράξεις στο βήμα (3). Συνολικά έχουμε $O(q \log q + (n/q)\log(n/q))$ πράξεις. Θυμηθείτε ότι έχουμε ακόμη την ελευθερία να επιλέξουμε το q. Αν δούμε το $q + n/q$ σαν συνάρτηση του q, ελαχιστοποιήται για $q = \sqrt{n}$. Βέβαια το q πρέπει να είναι ακέραιος, οπότε επιλέγουμε το q να είναι ένας ακέραιος κοντά στο $\sqrt{n}$, για παράδειγμα το $\lfloor \sqrt{n} \rfloor$. Τότε ο αριθμός των βημάτων του αλγορίθμου είναι $O(\sqrt{n} \log n)$.

3. Ο αλγοριθμος των Pohlig και Hellman

Ο στόχος του αλγορίθμου των Pohlig και Hellman είναι διαφορετικός από αυτόν του Baby-step/Giant-step. Στόχος είναι να ανάγουμε τον υπολογισμό ενός διακριτού λογαρίθμου στην ομάδα $\langle g \rangle$ στο υπολογισμό πολλών διακριτών λογαρίθμων σε υποομάδες της $\langle g \rangle$. Για να το πετύχουμε αυτό χρειάζεται να γνωρίζουμε την ανάλυση του n σε πρώτους παράγοντες. Ας υποθέσουμε λοιπόν ότι η ανάλυση αυτή είναι $n = p_1^{t_1} \cdots p_r^{t_r}$. Αν καταφέρουμε να υπολογίσουμε $0 \leq a^{(i)} < p_i^{t_i}$ για $i = 1, \ldots, r$ τέτοια ώστε $x \equiv a^{(i)} \pmod{p^{t_i}}$ τότε μπορούμε να βρούμε το x από τις παραπάνω σχέσεις με το Κινέζικο Θεώρημα Υπολοίπων. Άρα μένει να δείξουμε πώς μπορούν να υπολογιστούν τα $a^{(i)}$. Έστω ότι $n = mp^t$ με $(m, p) = 1$. Αν $y_0 = y^m$, $g_0 = g^m$, τότε $y_0 = g_0^x$ και g_0 είναι στοιχείο τάξης p^t. Αν $0 \leq a < p^t$ είναι ο διακριτός λογάριθμος του y_0 ως προς τη βάση g_0, τότε $x \equiv a \pmod{p^t}$.

Αν γράψουμε το a στη βάση p, έχουμε

$$a = a_0 + a_1 p + \cdots + a_{t-1} p^{t-1}, \quad 0 \leq a_i < p, \text{ για } \ i = 0, 1, \ldots, t-1.$$

Θέλουμε να υπολογίσουμε τα $a_0, a_1, \ldots, a_{t-1}$. Έχουμε

$$y_0 = g_0^a \ \Rightarrow y_0^{p^{t-1}} = \left(g_0^{p^{t-1}}\right)^a$$

και θέτοντας $h_0 = y_0^{p^{t-1}}$, $g_1 = g_0^{p^{t-1}}$, έχουμε

$$h_0 = g_1^{a_0 + a_1 p + \cdots + a_{t-1} p^{t-1}} = g_1^{a_0},$$

διότι η τάξη του g_1 είναι p. Από τα δεδομένα μπορούμε να υπολογίσουμε τα $h_0 = y^{n/p}$ και $g_1 = g^{n/p}$. Στη συνέχεια υπολογίζουμε το διακριτό λογάριθμο του h_0 ως προς τη βάση g_1. Το αποτέλεσμα είναι το a_0.

Ας υποθέσουμε τώρα ότι έχουμε υπολογίσει τα $a_0, \ldots, a_{i-1}$ και θέλω να υπολογίσω το a_i. Έχουμε

$$y_0 = g_0^{a_0+a_1p+\cdots+a_{i-1}p^{i-1}+a_ip^i+\cdots+a_{t-1}p^{t-1}},$$

οπότε

$$y_0 g_0^{-a_0-a_1p-\cdots-a_{i-1}p^{i-1}} = g_0^{a_ip^i+\cdots+a_{t-1}p^{t-1}}.$$

Υψώνοντας στην p^{t-i-1} και τα δύο μέλη, έχουμε

$$h_i = g_1^{a_i},$$

όπου $h_i = (y_0 g_0^{-a_0-a_1p-\cdots-a_{i-1}p^{i-1}})^{p^{t-i-1}}$. Κάναμε και πάλι χρήση του γεγονότος ότι η τάξη του g_1 είναι p. Από τα προηγούμενα βήματα, έχουμε υπολογίσει τα $a_0, \ldots, a_{i-1}$, οπότε μπορούμε να υπολογίσουμε το h_i και στη συνέχεια το διακριτό λογάριθμο του h_i ως προς τη βάση g_1. Το αποτέλεσμα είναι το a_i.

Η πολυπλοκότητα του αλγορίθμου μπορεί να υπολογιστεί ως εξής. Για να υπολογίσουμε κάθε ένα από τα ψηφία a_i απαιτούνται $O(\log n)$ πράξεις στην ομάδα καθώς και ο υπολογισμός ενός διακριτού λογαρίθμου σε μια ομάδα τάξης p. Με τον αλγόριθμο Baby-Step/Giant-Step αυτό μπορεί να γίνει με $O(\sqrt{p}\log p)$ πράξεις στην ομάδα. Συνεπώς, για να υπολογίστουν όλα τα ψηφία του $x \mod p_i^{t_i}$ απαιτούνται $O(t_i\sqrt{p_i}\log p_i)$ πράξεις στην ομάδα. Για να υπολογιστεί ο x modulo $p_i^{t_i}$ για $i = 1, \ldots, r$ απαιτούνται $O\left(\sum_{i=1}^r t_i\sqrt{p_i}\log p_i\right)$ πράξεις. Καθώς $n \geq p_i^{t_i}$ για κάθε $1 \leq i \leq r$, η παραπάνω ποσότητα φράσεται από την $O\left(\log n \sum_{i=1}^r \sqrt{p_i}\right)$. Είναι εύκολο να δει κανείς ότι $r \leq \log n/\log 2$. Αν $p = \max\{p_1, \ldots, p_r\}$, τότε ένα άνω φράγμα για τον αριθμό των πράξεων που απαιτεί ο αλγόριθμος είναι

$$O\left(\sqrt{p}\,(\log n)^2\right).$$

Το δίδαγμα είναι ότι ο υπολογισμός ενός διακριτού λογαρίθμου σε μια κυκλική ομάδα τάξης n μπορεί πάντα να αναχθεί στον υπολογισμό διακριτών λογαρίθμων σε υποομάδες πρώτης τάξης. Αν θέλουμε το πρόβλημα να είναι δύσκολο, πρέπει να σιγουρευτούμε ότι το n διαιρείται από κάποιο μεγάλο πρώτο. Για παράδειγμα, αν ο μόνος διαθέσιμος αλγόριθμος είναι αυτός των Pohlig και Hellman, και θέλουμε ο υπολογισμός του διακριτού λογαρίθμου να απαιτεί περίπου 2^{100} πράξεις στην ομάδα, τότε πρέπει να επιλέξουμε μια ομάδα τάξης n, όπου το n διαιρείται από κάποιο πρώτο μεγέθους περίπου 2^{200} (δηλαδή να έχει πρώτο διαιρέτη με 200 περίπου bits).

Παράδειγμα 3.1. Ας πούμε για παράδειγμα, ότι $p = 2^t + 1$ είναι πρώτος και θέλουμε να υπολογίζουμε διακριτούς λογάριθμους στην ομάδα $\mathbb{F}_p^\times$. Η τάξη της ομάδας είναι $n = p - 1 = 2^t$, που μπορεί να παραγοντοποιηθεί πολυ εύκολα. Χρησιμοποιώντας τον αλγόριθμο των Pohlig και Hellman μπορούμε να λύσουμε το πρόβλημα σε χρόνο $O(\sqrt{2}\log^2 n) = O(\log^2 p)$. Δηλαδή το πρόβλημα λύνεται σε πολυωνυμικό χρόνο. Αν θέλουμε να βασίσουμε ένα σύστημα ElGamal στην

ομάδα $\mathbb{F}_p^\times$ πρέπει να επιλέξουμε το p έτσι ώστε το $p-1$ να έχει μεγάλο πρώτο διαιρέτη.

Παράδειγμα 3.2. Ας δούμε και ένα παράδειγμα υπολογισμού διακριτού λογάριθμου με τη μέθοδο Pohlig-Hellman. Ας είναι η ομάδα μας η $\mathbb{F}_{29}^\times$ και μας δίνονται τα $y = 10$ και $g = 3$. Βλέπουμε ότι η τάξη της ομάδας είναι $n = 29 - 1 = 28 = 2^2 \cdot 7$ και η τάξη του g είναι 28, δηλαδή $\langle g \rangle = \mathbb{F}_{29}^\times$. Θέλουμε να βρούμε $0 \leq x \leq 28$ τέτοιο ώστε $y = g^x$ δηλαδή $10 \equiv 3^x \pmod{29}$. Το x υπολογίζεται $\bmod$ 28.

Σύμφωνα με τον αλγόριθμο, θα υπολογίσω το $x \mod 2^2$ και $\mod 7$. Δηλαδή, θα υπολογίσω a και b τέτοια ώστε

$$\begin{aligned} x &\equiv a \pmod{2^2} \\ x &\equiv b \pmod{7}. \end{aligned}$$

Αρχικά υπολογίζω το a. Υπολογίζω

$$\begin{aligned} y_0 &= y^7 = 10^7 \equiv 17 \pmod{29}, \\ g_0 &= g^7 = 3^7 \equiv 12 \pmod{29}, \\ g_1 &= g_0^2 = 12^2 \equiv 28 \pmod{29}. \end{aligned}$$

Γράφω το a στη βάση 2, $a = a_0 + 2a_1$, με $0 \leq a_0, a_1 \leq 1$. Για το a_0 υπολογίζω:

$$h_0 = y_0^2 = 17^2 \equiv 28 \mod 29.$$

Καθώς $h_0 = g_1^1$, βλέπουμε ότι $a_0 = 1$. Στη συνέχεια, υπολογίζω:

$$h_1 = y_0 g_0^{-a_0} = 17 \cdot 12^{-1} \equiv 28 \mod 29,$$

και το διακριτό λογάριθμο του h_1 ως προς τη βάση g_1, που είναι και πάλι ίσος με 1. Άρα $a_1 = 1$. Συνεπώς $a = 1 + 2 = 3$.

Προχωρώ στον υπολογισμό του b. Καθώς στην ανάλυση $28 = 2^2 \cdot 7$ το 7 εμφανίζεται με εκθέτη 1, αρκει να υπολογίσω ένα μόνο ψηφίο, το ίδιο το b. Υπολογίζω

$$\begin{aligned} y_0 &= y^4 = 10^4 \equiv 24 \mod 29, \\ g_0 &= g^4 = 3^4 \equiv 23 \mod 29, \\ g_1 &= g_0. \end{aligned}$$

Επίσης, έχουμε $h_0 = y_0$. Έτσι έχουμε $h_0 = g_1^b$, δηλαδή

$$24 \equiv 12^b \pmod{29}.$$

Υπάρχουν 7 δυνατές επιλογές για το b (οι $b = 0, 1, \ldots, 6$), τις οποίες μπορώ να εξετάσω μια προς μία. Φυσικά θα μπορούσα να εφαρμόσω τον αλγόριθμο Baby-step/Giant-step. Σε κάθε περίπτωση, βρίσκω $b = 6$.

Έτσι έχω να λύσω το σύστημα

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 6 \pmod 7. \end{aligned}$$

Με τον αλγόριθμο για το Κινέζικο Θεώρημα Υπολοίπων, βρίσκω $x = 27$. Πραγματικά, μπορεί κανείς εύκολα να επαληθεύσει ότι $3^{27} = 10 \mod 29$.