Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Καλογερόπουλος Παναγιώτης

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

29 Οκτωβρίου 2012

1 Εισαγωγή Στη Θεωρία Αριθμών

Ορισμός 1. *Για $a, b \in \mathbb{Z}$ θα λέμε ότι ο "α διαιρεί τον b" αν υπάρχει $c \in \mathbb{Z}$ τέτοιο ώστε $b = ac$. Συμβολικά γράφουμε $a|b$.*

Παρατήρηση 1. *Θα λέμε ότι ο α δεν διαιρεί τον b και θα συμβολίζουμε με $a \nmid b$ αν $\forall c \in \mathbb{Z}$, $b \neq ca$.*

Πρόταση 1. *Για κάθε $a, b \in \mathbb{Z}$:*

1. $a|a$, $1|a$ *και* $a|0$.
2. $0|a$ *ανν* $a = 0$.
3. $a|b$ *και* $b|c$ *τότε* $a|c$.
4. $a|b$ *και* $b|a$ *τότε* $a = \pm b$.
5. *αν* $a|b$ *τότε* $a|bc$.
6. *αν* $a|b$ *και* $a|c$ *τότε* $a|(xb + yc) \forall x, y \in \mathbb{Z}$.
7. *αν* $a|b$ *και* $b \geq 0$ *τότε* $a \leq b$.

Απόδειξη. Άσκηση.

Παρατήρηση 2. *Η διαιρετότητα στους $\mathbb{N}$ είναι μια σχέση μερικής διάταξης.*

Ορισμός 2. *Ο a θα λέγεται γνήσιος διαιρέτης του b αν $a|b$ και $0 < a < |b|$.*

Ορισμός 3. *Ο a θα λέγεται μη τετριμμένος διαιρέτης του b αν $a|b$ και $1 < a < |b|$.*

Ορισμός 4. *Ο $p > 1$ θα λέγεται πρώτος αριθμός αν μοναδικοί διαιρέτες του είναι ο 1 και ο p.*

Θεώρημα 1. ***Ακέραιας διαίρεσης με υπόλοιπο***
Για κάθε $a, b \in \mathbb{Z}$ με $b > 0$ υπάρχουν μοναδικά q (quotient), r (remainder) ($q, r \in \mathbb{Z}$) τέτοια ώστε:

$$a = qb + r \qquad \text{και} \qquad 0 \leq r < b$$

Απόδειξη.
Θεωρούμε το σύνολο

$$S = \{a - xb | x \in \mathbb{Z}, a - xb \geq 0\}$$

Το S είναι μη κενό (για παράδειγμα το $x = -|a| \in S$) συνεπώς έχει ελάχιστο στοιχείο r. Υπάρχει $q \in \mathbb{Z}$ τέτοιο ώστε

$$a - qb = r \Rightarrow a = qb + r \qquad \text{και} \qquad 0 \leq r < b$$

Έστω $q', r' \in \mathbb{Z}$ τέτοια ώστε

$$a = q'b + r' \qquad \text{και} \qquad 0 \leq r' < b,$$

τότε

$$0 \leq |r' - r| < b \text{ διότι } 0 \leq r < b \text{ και } 0 \leq r' < b$$

Επίσης,

$$qb + r = q'b + r' \Rightarrow (q - q')b = (r' - r) \Rightarrow |q - q'|b = |r' - r|.$$

Αν $q \neq q'$ τότε $b \leq |r' - r|$, άτοπο. Συνεπώς $q = q'$ και τότε $r = r'$.

Θεώρημα 2. *Έστω $a, b \in \mathbb{Z}$ και $d = gcd(a, b)$. Τότε:*
a) *υπάρχουν $k, \lambda \in \mathbb{Z}$ τέτοια ώστε $d = ka + \lambda b$.*
b) *κάθε κοινός διαιρέτης d' των a, b είναι μικρότερος του d.*

Απόδειξη.
Για να δείξουμε την ύπαρξη έστω,

$$S = \{xa + yb | x, y \in \mathbb{Z}, xa + yb \geq 0\}$$

Το S είναι μη κενό (διότι για παράδειγμα περιέχει το $b^2 = 0a + bb$) και συνεπώς έχει ελάχιστο στοιχείο d με $d = ka + \lambda b$.Θα δείξουμε ότι $d|a$. Έστω πως $d \nmid a$. Τότε υπάρχουν $q, r \in \mathbb{Z}$ τέτοια ώστε

$$a = qd + r \qquad 0 < r < d$$

Όμως,

$$r = a - qd = a - q(ka + \lambda b) = (1 - qk)a + (-\lambda q)b$$

και φυσικά $r \in S$ και $0 < r < d$, άτοπο. Ομοίως $d|b$.

Για την μοναδικότητα. Έστω d' τέτοιο ώστε $d'|a$ και $d'|b$. Τότε $a = c_1 d'$ και $b = c_2 d'$ οπότε $d = ka + \lambda b = kc_1 d' + \lambda c_2 d' = (kc_1 + \lambda c_2)d'$. Συνεπώς, $d'|d \Rightarrow d' \leq d$.

Παρατήρηση 3. *Το S είναι ιδεώδες με γεννήτορα τον d, $S =< d >$.*

Πόρισμα 1. *Αν $gcd(a, b) = 1$ τότε υπάρχουν $\kappa, \lambda \in \mathbb{Z}$ τέτοια ώστε $\kappa a + \lambda b = 1$.*

Πρόταση 2. *Αν $c|ab$ και $gcd(a, c) = 1$ τότε $c|b$.*

Απόδειξη
Εφόσον $gcd(a, c) = 1$ υπάρχουν $\kappa, \lambda \in \mathbb{Z}$ τέτοια ώστε $\kappa c + \lambda a = 1 \Rightarrow \kappa cb + \lambda ab = b \Rightarrow c|b$.

Πρόταση 3. *Αν p πρώτος αριθμός και $p|ab$ τότε $p|a$ ή $p|b$.*

Απόδειξη
Αν $gcd(p, a) = p$ τότε $p|a$. Αν $gcd(p, a) = 1$ εφόσον $p|ab$ από Πρόταση 2 $p|b$.

Θεώρημα 3. ***Θεμελιώδες Θεώρημα Αριθμητικής***
Κάθε ακέραιος αριθμός $n, n > 1$ μπορεί να γραφτεί με μοναδικό τρόπο (αν αγνοήσουμε τη σειρά των παραγόντων) ως πεπερασμένο γινόμενο πρώτων αριθμών.

Απόδειξη.
Υποθέτουμε ότι

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

και χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $p_1 \leq p_2 \leq \ldots \leq p_r$ και $q_1 \leq q_2 \leq \ldots \leq q_s$. Αρκεί να δείξουμε ότι $r = s$ και $p_i = q_i, i = 1, \ldots, r$.
Για $n = 2$ το Θεώρημα ισχύει. Υποθέτουμε ότι ισχύει για κάθε ακέραιο $k < n$ και θα δείξουμε ότι ισχύει για τον n. Αν ο n είναι πρώτος τότε το Θεώρημα προφανώς ισχύει. Αν ο n δεν είναι πρώτος τότε $r > 1$ και $s > 1$. Επειδή $p_1|q_1 q_2 \cdots q_s$ και $q_1|p_1 p_2 \cdots p_r$ θα έχουμε $p_1 = q_i$ για κάποιο i και $q_1 = p_j$ για κάποιο j. Όμως, $p_1 \leq p_j = q_1$ και $q_1 \leq q_i = p_1$. Έχουμε $p_1 = q_1, 1 < \frac{n}{p_1} < n$ και $\frac{n}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s$. Από την υπόθεση της επαγωγής $r - 1 = s - 1$ και $p_i = q_i, i = 2, \ldots, r$. Τελικά $r = s$ και $p_i = q_i, i = 1, \ldots, r$.

2 Το κρυπτοσύστημα Σακιδίου

Ορισμός 5. *Κλασικά κρυπτοσυστήματα ή κρυπτοσυστήματα ιδιωτικού κλειδιού ή συμμετρικά κρυπτοσυστήματα.*

Ένα συμμετρικό κρυπτοσύστημα αποτελείται από τα ακόλουθα: :

- Ένα χώρο μηνυμάτων (plaintext) $\mathcal{M}$.
- Ένα χώρο κωδικοποιημένων μηνυμάτων (ciphertext) $\mathcal{C}$.
- Ένα χώρο κλειδιών $\mathcal{K}$.
- Ένα αποδοτικό αλγόριθμο κωδικοποίησης $Enc : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$.
- Ένα αποδοτικό αλγόριθμο αποκωδικοποίησης $Dec : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$.
- Ένα αποδοτικό αλγόριθμο δημιουργίας κλειδιών $\mathcal{G} : \mathbb{N} \to \mathcal{K}$.

πρέπει επίσης να ικανοποιεί την ακόλουθη σχέση

$$\text{Για όλα τα } m \in \mathcal{M} \text{ και } k \in \mathcal{K}, Dec_K(Enc_K(m)) = m.$$

Το βασικό πρόβλημα στα κρυπτοσυστήματα αυτά είναι η ανταλλαγή του κλειδιού.

Με τη συμβολή των Diffie–Hellman (το 1976) προέκυψαν κρυπτοσυστήματα μονής κατεύθυνσης ή δημοσίου κλειδιού. Σ' ένα κρυπτοσύστημα δημοσίου κλειδιού υπάρχουν δύο κλειδιά το ένα που γίνεται δημόσιο και χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων και ένα ιδιωτικό για την αποκρυπτογράφηση. Σημαντικό είναι ότι η γνώση του δημοσίου κλειδιού δεν μπορεί εύκολα να μας οδηγήσει στην αποκρυπτογράφηση του κειμένου. Δηλαδή, ενώ η εφαρμογή του αλγόριθμου κρυπτογράφησης είναι εύκολη όταν είναι γνωστό το δημόσιο κλειδί η εύρεση του αλγόριθμου αποκρυπτογράφησης χωρίς τη γνώση του κλειδιού αποκρυπτογράφησης είναι υπολογιστικά δύσκολη (trapdoor function). Με απλά λόγια, κάποιος που μπορεί να κρυπτογραφήσει μια πληροφορία δεν μπορεί να χρησιμοποιήσει το δημόσιο κλειδί για να την αποκρυπτογραφήσει.

Ορισμός 6. ***trapdoor function***

Συναρτήσεις f που ο υπολογισμός της αντίστροφής συνάρτησης f^{-1} από την f είναι πρακτικά ανέφικτος αν δεν μας δοθεί κάποια περαιτέρω πληροφορία (στην συγκεκριμένη περίπτωση το ιδιωτικό κλειδί για την αποκρυπτογράφηση)

Το κρυπτοσύστημα Merkle - Hellman, είναι ένα κρυπτοσύστημα δημοσίου κλειδιού βασισμένο στο πρόβλημα του σακιδίου.

Το κρυπτοσύστημα Merkle - Hellman βασίζεται ουσιαστικά στο NP-complete πρόβλημα του αθροίσματος υποσυνόλων (Subset Sum).

Subset Sum Problem
Είσοδος:
Ένα σύνολο $A = \{a_1, a_2, \ldots, a_n\}$ και ένα $k \in \mathbb{N}$.

Έξοδος:

- Ένα $A' = \{a_{i_1}, a_{i_2}, \ldots, a_{i_m}\} \subseteq A$ τέτοιο ώστε $\sum_{j=1}^{m} a_{i_j} = k$.
- **Όχι** αν δεν υπάρχει τέτοιο υποσύνολο του A.

Παρατήρηση 4. *Αν το σύνολο A έχει n το πλήθος στοιχεία τότε τα δυνατά υποσύνολα του A είναι 2^n. Για n αρκετά μεγάλο η επίλυση του προβλήματος δεν είναι εύκολη.*

Ορισμός 7. *Ένα σύνολο $A = \{a_1, a_2, \ldots, a_n\}$ καλείται υπεραυξητικό (super increasing) αν $\forall i \leq n$ έχουμε $\quad a_i > \sum_{j=1}^{i-1} a_j$.*

Παράδειγμα 1. *Το $A = \{1, 3, 9, 20, 42, 88\}$ είναι υπεραυξητικό.*

Παρατήρηση 5. *Στα υπεραυξητικά σύνολα είναι "εύκολη" η λύση του Subset Sum Problem.*

Παράδειγμα 2. *Ας υποθέσουμε ότι θέλουμε να γράψουμε το 51 ως άθροισμα στοιχείων του $A = \{1, 3, 9, 20, 42, 88\}$.*

- ***Βήμα 1ο:*** *Προφανώς αποκλείω το 88.*
- ***Βήμα 2ο:*** *Πρέπει οπωσδήποτε να πάρω το 42 διότι διαφορετικά τα στοιχεία που απομένουν έχουν άθροισμα μικρότερο του 42.*
- ***Βήμα 3ο:*** *Απόμενουν 51-42=9.*
- ***Βήμα 4ο:*** *Παίρνω και το 9.*

Βασική Ιδέα του Merkle - Hellman Knapsack κρυπτοσυστήματος είναι να χρησιμοποιήσω ως δημόσιο κλειδί ένα καμουφλαρισμένο υπεραυξητικό διάνυσμα.

- Ξεκινώ με κάποιο υπεραυξητικό διάνυσμα A
- Επιλέγω $t, m : m > \sum a_i$ και $gcd(t, m) = 1$
- Υπολογίζω το $\mathrm{A}' = t \cdot \mathrm{A} \mod m$ και το δημοσιεύω.

Συνοπτικά,

- **Δημόσιο κλειδί:** το A'
- **Ιδιωτικό κλειδι:** $t^{-1} \mod m, A, m$

Έστω λοιπόν πως η Αλίκη θέλει να λάβει μια πληροφορία $b = (\ldots, 0, 1, \ldots)$ από τον Βασίλη. Για τον σκοπό αυτό η Αλίκη κατασκευάζει το σύνολο A' και το δημοσιεύει. Ο Βασίλης χρησιμοποιώντας το σύνολο κωδικοποιεί την πληροφορία.

$$b \to y = Enc_{\mathrm{A}'}(b) = \sum_{i=1}^{n} b_i a'_i$$

Η Αλίκη λαμβάνει ως απάντηση από τον Βασίλη έναν αριθμό τον οποίο και αποκωδικοποιεί ως εξής:

$$y \to Solve_{\mathrm{A}} \left[t^{-1} \cdot y \mod m \right]$$

όπου ο $Solve_{\mathrm{A}}$ είναι ένας αλγόριθμος επίλυσης του στιγμιοτύπου Subset Sum στο υπεραυξητικό διάνυσμα A, αναλυτικότερα...

$$Solve_{\mathrm{A}} \left[t^{-1} \left(\sum_{i=1}^{n} a'_i b_i \right) \mod m \right] =$$

$$Solve_{\mathrm{A}} \left[t^{-1} \left(\sum_{i=1}^{n} \left(t \cdot a_i \mod m \right) b_i \right) \mod m \right] =$$

$$Solve_{\mathrm{A}} \left[\left(\sum_{i=1}^{n} a_i b_i \right) \mod m \right] =$$

$$Solve_{\mathrm{A}}\left[\sum_{i=1}^{n} a_i b_i\right]$$

όπου η τελευταία ισότητα αληθεύει διότι $m > \sum_{i=1}^{n} a_i b_i$.

Παράδειγμα 3. *Έστω το υπεραυξητικό σύνολο* $A = \{1, 3, 5, 11\}$ *και* $m = 23, t = 7$. *Ο αντίστροφος του* $7 \mod 23$ *είναι ο* $10 \mod 23$. *Κατασκευάζω το* $A' = \{7, 21, 12, 8\}$ *(κάθε στοιχείο του* A' *προκύπτει από το* A, $a'_i \equiv ta_i \mod 23$*). Θα κωδικοποιήσουμε την ακολουθία* $b = (0110)$ *χρησιμοποιώντας το* A'.

$$enc_{A'}(0110) = 0 \cdot 7 + 1 \cdot 21 + 1 \cdot 12 + 0 \cdot 8 = 33.$$

Για την αποκωδικοποίηση, $8 = 10 \cdot 33 \mod 23$

$$Dec_{(A,t^{-1},m)} = Solve_A(8) = (0110)$$

όπου $Solve_{\mathrm{A}}$ ένας αλγόριθμος για να κατασκευάσουμε την ακολουθία b από το υπεραυξητικό σύνολο A.

Το Subset Sum πρόβλημα είναι ένα από τα NP-complete προβλήματα. Μεταξύ άλλων αυτό σημαίνει ότι δεν υπάρχει γνωστός αλγόριθμος που να το επιλύει σε πολυωνυμικό χρόνο. Αυτό φυσικά δεν αποκλείει την περίπτωση να υπάρχει αλγόριθμος που να επιλύει σε πολυωνυμικό χρόνο ειδικές περιπτώσεις του προβλήματος.

Γι' αυτό και το 1984 Ο **Shamir** έσπασε το κρυπτοσύστημα των Merkle – Hellman. Διαπίστωσε ότι δεν είναι απαραίτητος ο υπολογισμός των αρχικών m, t, A που χρησιμοποιήθηκαν. Αρκεί ο επιτιθέμενος να βρει m^*, t^* τέτοια ώστε να μπορεί να κατασκευαστεί κάποιο υπεραυξητικό σύνολο A^*.

Επίθεση στο κρυπτοσύστημα
Επιλέγω $t^* = 7, t^{*^{-1}} = 13, m^* = 15$. Κατασκευάζω νέο υπεραυξητικό σύνολο $\mathrm{A}'' = t^{*^{-1}} \cdot \mathrm{A}' \mod 15 = (1, 3, 6, 14)$.
$t^{*^{-1}} \cdot 33 \mod 15 = 9 \mod 15$.

$$9 = 0 \cdot 1 + 1 \cdot 3 + 1 \cdot 6 + 0 \cdot 14$$

Η ακολουθία που κωδικοποιήθηκε είναι η (0110).
Χωρίς να γνωρίζουμε το αρχικό υπεραυξητικό σύνολο, χωρίς να χρειάζεται να υπολογίσουμε το αρχικό υπεραυξητικό σύνολο, κατασκευάσαμε με κατάλληλα νέα t^*, m^* υπεραυξητικό σύνολο με τη χρήση του οποίου αποκωδικοποιήσαμε την πληροφορία.

Βιβλιογραφία

Zac12 : Σημειώσεις Ζάχου, ΕΜΠ, 2012.

Sti06 : D. Stinson: Cryptography: Theory and Practice, 3rd edition, CRC Press, 2005.