Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Δημήτριος Μπάκας
Αθανάσιος Ταουσάκος

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

12 Νοεμβρίου 2012

1 Κινέζικο Θεώρημα Υπολοίπων (Chinese Remainder Theorem)

Έστω το παρακάτω σύστημα εξισώσεων:
$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$\vdots$
$x \equiv a_i \pmod{m_i}$
$\vdots$
$x \equiv a_k \pmod{m_k}$
όπου $\forall i, j, gcd(m_i, m_j) = 1$ έχει μοναδική λύση στο δακτύλιο $\mathbb{Z}_{m_1 \cdot ... \cdot m_k}$.
Ισοδυναμα, μπορούμε να πούμε οτι το σύστημα έχει άπειρες λύσεις και αν s_1, s_2 δύο λύσεις του, ισχύει $s_1 \equiv s_2 \pmod{m}$.

Παράδειγμα:
$m_1 = 3$
$m_2 = 5$
$m_3 = 7$
Τότε υπάρχει μοναδική λύση στο $\mathbb{Z}_{105}$.

Απόδειξη:
$M = m_i \cdot ..... \cdot m_k$
Έστω $M_i = \frac{M}{m_i} = m_1 \cdot ... \cdot (m_i - 1) \cdot (m_i + 1) \cdot ... \cdot m_k$
Ισχύει πως $gcd(M_i, m_i) = 1$
Άρα $\exists N_i$ τέτοιο ώστε $N_i \cdot M_i \equiv 1 \pmod{m_i}$ για κάθε i.
Παρατηρούμε επίσης ότι για κάθε $j \neq i : N_i \cdot M_i \equiv 0 \pmod{m_j}$
Έστω

$$y = \sum_{i=1}^{k} N_i \cdot M_i \cdot a_i$$

Η y είναι λύση του συστήματος. Πράγματι,
$\forall i : y = (N_1 \cdot M_1 \cdot a_1 + ... + N_i \cdot M_i \cdot a_i + ... + N_k \cdot M_k \cdot a_k) \equiv a_i \pmod{m_i}$.

Για την μοναδικότητα τώρα έχουμε:
Έστω s_1, s_2 δυο διαφορετικές λύσεις ώστε $\forall i : s_1 \equiv s_2 \equiv a_i \pmod{m_i}$
Γνωρίζουμε όμως ότι αν $a \equiv b \pmod{n}$ και $a \equiv b \pmod{m}$ με $gcd(m, n) = 1$, τότε $a \equiv b \pmod{mn}$
Άρα $s_1 \equiv s_2 \pmod{m}$ οπότε μοναδική λύση.

Παράδειγμα:
$x \equiv 2 \pmod{3}$
$x \equiv 1 \pmod{5}$
$x \equiv 0 \pmod{7}$

Τότε $x \equiv 56 \pmod{105}$ αφού:
$M_1 = 35, M_2 = 21, M_3 = 15$
$N_1 = 2^{-1} = 2 \pmod 3$
$N_2 = 1 \pmod 5$
$N_3 = 1 \pmod 7$

$Y \equiv (2 \cdot 35 \cdot 2 + 21 \cdot 1 \cdot 1 + 0) \pmod{105} \equiv 161 \pmod{105}$
$\equiv 1 \cdot 105 + 56 \pmod{105} \equiv 56 \pmod{105}$

Το Κινέζικο Θεώρημα Υπολοίπων συνεπάγεται έναν ισομορφισμό του $\mathbb{Z}_M$:
$\mathbb{Z}_M \cong \mathbb{Z}_{m1} \times \mathbb{Z}_{m2} \times ... \times \mathbb{Z}_{mk}$

2 Τετραγωνικά Υπόλοιπα (Quadratic Residues)

Το 2 είναι τετραγωνικό υπόλοιπο $modulo 7$ διότι $3^2 = 9 \equiv 2 \pmod 7$ αλλά και $4^2 = 16 \equiv 2 \pmod 7$.
Η τετραγωνική ισοτιμία $x^2 \equiv 2 \pmod 7$ έχει λοιπόν 2 λύσεις.

Πρόταση:
Έστω p πρώτος αριθμός και $a \in \mathbb{Z}_p^*$.
Η τετραγωνική ισοτιμία $x^2 \equiv a \pmod p$ έχει είτε 0 είτε 2 λύσεις στο $\mathbb{Z}_p$.

Απόδειξη:
Έστω y λύση της εξίσωσης, τότε και η $-y$ θα είναι λύση.
Επίσης, αν $y \equiv -y \pmod p$, τότε $2y \equiv 0 \pmod p \Rightarrow y \equiv 0 \pmod p$, οπότε για τιμές διάφορες του 0, έχουμε οτι $y \neq -y \pmod p$.
Για 2 λύσεις y, y' ισχύει οτι:
$y^2 \equiv y'^2 \pmod p \Rightarrow p|y^2 - y'^2 \Rightarrow p|(y - y')(y + y') \Rightarrow p|(y - y') \vee p|(y + y')$
$\Rightarrow y \equiv y' \pmod p \vee y \equiv -y' \pmod p$

Πρόταση:
Έστω p, q πρώτοι.
Η τετραγωνική ισοτιμία $x^2 \equiv a \pmod{pq}$ έχει είτε 0 είτε 4 λύσεις στο $\mathbb{Z}_{pq}$.

Απόδειξη:
$x^2 \equiv a \pmod{pq} \Rightarrow pq|(x^2 - a) \Rightarrow p|x^2 - a$ και $q|x^2 - a$
άρα $x^2 \equiv a \pmod p$ και $x^2 \equiv a \pmod q$.
Συνεπώς η λύση της εξίσωσης είναι ισοδύναμη με τη λύση των δυο εξισώσεων $x^2 \equiv a \pmod p$ και $x^2 \equiv a \pmod q$. Έστω ότι η πρώτη έχει λύσεις τις $x_1, -x_1$

και η δεύτερη τις $x_2, -x_2$. Για κάθε έναν απο τους συνδυασμούς αυτών των λύσεων (που είναι 4) προκύπτει μια διαφορετική λύση για την εξίσωση, απο το σύστημα $x \equiv \pm x_1 \pmod{p}, x \equiv \pm x_2 \pmod{q}$. Η ύπαρξη μοναδικής λύσης στο Z_{pq} αυτού του συστήματος προκύπτει απο το κινέζικο θεώρημα υπολοίπων.

Για p πρώτο,
$p \equiv 1 \pmod{4}$: πιθανοτικός αλγόριθμος
$p \equiv 3 \pmod{4}$: $\pm a^{\frac{p+1}{4}}$ είναι οι 2 λύσεις.
Άρα όταν το a είναι τετραγωνικό υπόλοιπο $modulop$
$(\pm a^{\frac{p+1}{4}})^2 = a^{\frac{p+1}{2}} \equiv a^{p-1} \cdot a \equiv a \pmod{p}$
Ισχυει διότι $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ αν και μόνο αν το a είναι τετραγωνικό υπόλοιπο $modulop$.

Πρόταση:
Η εξίσωση $x^2 \equiv a \pmod{p}$ έχει λύση αν και μόνο αν $a^{\frac{p-1}{2}} \equiv 1(\pmod{p})$.

Απόδειξη:
Η $\mathbb{Z}_p^*$ είναι κυκλική με γεννήτορα g.
"$\Rightarrow$" : Έστω $a \equiv g^b \pmod{p}$.
$a^{\frac{p-1}{2}} \equiv g^{b \cdot \frac{p-1}{2}} \equiv 1 \pmod{p}$
Θα πρέπει $b \cdot \frac{p-1}{2} | p-1 \Rightarrow 2|b$.
Αν θεωρήσουμε $b = 2k+1$, τότε $g^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, το οποίο είναι άτοπο.

"$\Leftarrow$" : Αφού το a είναι τετραγωνικό υπόλοιπο $\pmod{p}$, τότε $\exists$k $\in Z_p^*$: $k^2 \equiv a \pmod{p}$.
Άρα $a^{\frac{p-1}{2}} \equiv k^{p-1} \equiv 1 \pmod{p}$.

Παρατήρηση:
Η παραπάνω πρόταση μπορεί να γενικευτεί ως εξής:
Αν $gcd(a,m) = 1$ τότε $\exists x : x^n \equiv a \pmod{m}$ αν και μόνο αν $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$ όπου $d = gcd(n, \varphi(m))$.

Πρόταση:
Για το $\mathbb{Z}_p$ γνωρίζουμε πως ακριβώς τα μισά του στοιχεία είναι τετραγωνικά υπόλοιπα ενώ τα υπόλοιπα είναι τετραγωνικά μη υπόλοιπα.

Έστω g γεννήτορας του $\mathbb{Z}_p^*$, τότε τα g^2, g^4, g^{p-1} είναι τετραγωνικά υπόλοιπα ενώ τα g, g^3, g^5, g^{p-2} είναι τετραγωνικά μη υπόλοιπα.

Παρατηρήσεις:
•Τα τετραγωνικά υπόλοιπα είναι οι άρτιες δυνάμεις του γεννήτορα.

•Το πλήθος των τετραγωνικών υπολοίπων είναι $\frac{p-1}{2}$.
•Για pq έχουμε $\frac{p-1}{2} \cdot \frac{q-1}{2}$ τετραγωνικά υπόλοιπα.

3 Σύμβολο Legendre

Το σύμβολο Legendre για έναν αριθμό $a \in \mathbb{Z}_p$ ορίζεται ως εξής:

$$(\frac{a}{p}) = \begin{cases} 1 & \text{εάν } \exists x \in \mathbb{Z}_p : x^2 \equiv a \pmod{p} \\ -1 & \text{εάν } \nexists x \in \mathbb{Z}_p : x^2 \equiv a \pmod{p} \\ 0 & \text{εάν } p \mid a \end{cases}$$

Αν $(\frac{a}{p}) = 1$, τότε το a το ονομάζουμε και τετραγωνικό υπόλοιπο $modulo p$.
Αν $(\frac{a}{p}) = -1$, τότε το a το ονομάζουμε και τετραγωνικό μη υπόλοιπο $modulo p$.

Πρόταση

1. $m \equiv n \pmod{p} \Rightarrow (\frac{m}{p}) = (\frac{n}{p})$
2. $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$
3. $(\frac{a}{p}) \cdot (\frac{b}{p}) = (\frac{a \cdot b}{p})$

Λήμμα Gauss
Αν το πλήθος των στοιχείων του συνόλου $A = \{a, 2 \cdot a, ..., \frac{p-1}{2} \cdot a\} \pmod{p}$ που είναι μεγαλύτερα του $\frac{p}{2}$ το συμβολίσουμε με μ, τότε ισχυει ότι $(\frac{a}{p}) = (-1)^{\mu}$.

Πρόταση

1. $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{εάν } p \equiv 1 \pmod{4} \\ -1 & \text{εάν } p \equiv 3 \pmod{4} \end{cases}$
2. $(\frac{2}{p}) = \begin{cases} 1 & \text{εάν } p \equiv 1 \pmod{8} \vee p \equiv 7 \pmod{8} \\ -1 & \text{εάν } p \equiv 3 \pmod{8} \vee p \equiv 5 \pmod{8} \end{cases}$

Νόμος Τετραγωνικής Αντιστροφής

$$(\frac{p}{q}) = \begin{cases} -(\frac{q}{p}) & \text{εάν } p \equiv q \equiv 3 \pmod{4} \\ (\frac{q}{p}) & \text{αλλιώς} \end{cases}$$

Για παράδειγμα: $(\frac{5}{7}) = (\frac{7}{5}) = (\frac{2}{5}) = -1$

Παρατήρηση:
Ο συγκεκριμένος νόμος είναι εξαιρετικά χρήσιμος για τον υπολογισμό μιας τιμής καθώς είναι ταχύτερος από την ύψωση σε δύναμη.

4 Σύμβολο Jacobi

Με τη βοήθεια του συμβόλου του Legendre θα ορίσουμε το σύμβολο του Jacobi, που αποτελεί μία γενίκευση όταν ο διαιρέτης είναι σύνθετος.
Αν $n = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_k^{a_k}$ η ανάλυση σε γινόμενο πρώτων αριθμών ενός θετικού περιττού ακεραίου, τότε για κάθε ακέραιο m το σύμβολο **Jacobi** $(\frac{m}{n})$ ορίζεται ως εξής:

$$(\frac{m}{n}) = \prod_{i=1}^{k} (\frac{m}{p_i})^{a_i}$$

Για παράδεγμα: $(\frac{18}{35}) = (\frac{18}{7}) \cdot (\frac{18}{5})$

Για το σύμβολο Jacobi ισχύουν όλες οι προτάσεις που είπαμε για το σύμβολο Legendre, πλην της πρότασης 2.

Αν $(\frac{m}{n}) \neq 1$ τότε η ισοδυναμία $x^2 \equiv m \pmod{n}$ δεν έχει λύσεις.
(Ισχύει για Legendre και Jacobi).

Παρατήρηση:
Πρέπει να σημειωθεί ότι το σύμβολο Jacobi δεν χαρακτηρίζει απολύτως την ύπαρξη λύσεων της αντίστοιχης εξίσωσης $x^2 \equiv a(\pmod{n})$. Πράγματι είναι εύκολο να δούμε οτι αν αυτή η εξίσωση έχει λύσεις, το συμβολο Jacobi $(\frac{a}{n}) = 1$ αλλά δεν ισχύει το αντίστροφο.

5 Κρυπτοσυστημα RSA

Το κρυπτοσύστημα των Rivest, Shamir και Adlemann (RSA) που προτάθηκε το 1977 ήταν το πρώτο κρυπτοσύστημα δημοσίου κλειδιού.

Ορισμός

Το κρυπτοσύστημα RSA ορίζεται μέσα από τα παρακάτω βήματα:

1. Εύρεση πρώτων p, q με "αρκετά" ψηφία (π.χ. > 100)
2. Υπολογισμός $n = p \cdot q$ και $\varphi(n) = (p-1) \cdot (q-1)$

3. Επιλογή $e \in \mathbb{Z}_n^*$: gcd$(e, \varphi(n)) = 1$ (π.χ. $e > max(p, q)$)
4. Υπολογισμός $d : e \cdot d \equiv 1 \pmod{\varphi(n)}$ χρησιμοποιώντας τον Επεκτεταμένο Ευκλείδιο αλγόριθμο.

Ακολούθως, ο χρήστης δημοσιοποιεί το δημόσιο κλειδί του: (e, n) κρατώντας απόρρητο το ιδιωτικό κλειδί: (p, q, d) (ή και μόνο d όταν το n έχει υπολογιστεί από κάποια Έμπιστη Αρχή)

Κρυπτογράφηση: $c = enc(m) = m^e \underline{mod} n \quad m \in \mathbb{Z}_n$

Αποκρυπτογράφηση: $dec(c) = c^d \underline{mod} n$

Ορθότητα
$dec(m^e \underline{mod} n) \equiv (m^e)^d \equiv m^{k \cdot \varphi(n)+1} \equiv m \pmod{n}$
Αποδεικνύεται εύκολα για $m \in \mathbb{Z}_n^*$ αλλά ισχύει $\forall m \in \mathbb{Z}_n$.

Σχέση με Παραγοντοποίηση

Η κρυπτανάλυση ενός RSA μπορεί να αναχθεί σε παραγοντοποίηση (factoring).
Αν μπορούμε να αναλύσουμε σε πρώτους παράγοντες το n, τότε μπορούμε να υπολογίσουμε το $\varphi(n) = (p-1) \cdot (q-1)$. Στη συνέχεια βρίσκουμε αποδοτικά με τον Επεκτεταμένο Ευκλείδιο Αλγόριθμο ένα d ώστε $e \cdot d \equiv 1 \pmod{\varphi(n)}$. Τελικά, αποκρυπτογραφούμε το κρυπτοκείμενο y, με $x = y^d \pmod{n}$. Επομένως, η αντίστροφη της συνάρτησης RSA μπορεί να αναχθεί σε παραγοντοποίηση.

Αν υποθέσουμε πως γνωρίζω το $\varphi(n)$ τότε θα μπορούσα να υπολογίσω τα p, q από τις εξισώσεις:

n = p ·q
φ(n)=(p-1)·(q-1)
Άρα ο $\varphi(n) - COMPUTATION$ δεν μπορεί να είναι ευκολότερος από την παραγοντοποίηση του n.

RSA-BREAK $\leq^p FACTORING \leq^p \varphi(n) - COMPUTATION$

6 Επίθεση Κοινού Γινομένου

Η βασική υπόθεση εδώ είναι πως υπάρχει μία Έμπιστη Αρχή που διανέμει τόσο το γινόμενο n όσο και τα e_1, d_1 και e_2, d_2. Οι πρώτοι αριθμοί p, q είναι γνωστοί μόνο στην Έμπιστη Αρχή.

Με αυτό το σενάριο,υποθέτοντας πως είμαι ο χρήστης 1, μπορώ να βρώ **χωρίς παραγοντοποίηση του n** τον εκθέτη αποκρυπτογράφησης d_2 του χρήστη 2.
Ξέρω πως: $e_1 \cdot d_1 \equiv 1 \pmod{\varphi(n)} \Leftrightarrow \varphi(n)|(e_1 \cdot d_1 - 1)$
ή εναλλακτικά για κάποιο k ισχύει ότι:
$e_1 \cdot d_1 = k \cdot \varphi(n)$
Έστω a ο μέγιστος αριθμός για τον οποίο ισχύουν: $a|(e_1 \cdot d_1 - 1)$ και $(a, e_2) = 1$
επιπλέον ορίζω $t = \frac{e_1 \cdot d_1 - 1}{a}$
Θέτω $x_0 = gcd(e_2, \underbrace{e_1 \cdot d_1 - 1}_{g_0})$
και ορίζω επαγωγικά για $i \geq 1, \quad g_i = \frac{g_{i-1}}{h_{i-1}}, h_i = gcd(g_i, e_2)$
Για $h_i \geq 2$ ισχύει $g_{i+1} \geq g_i/2$ κάτι που σημαίνει πως μπορούμε να βρούμε το $h_i = 1$ σε γραμμικό χρόνο. Ο χρήστης 1 μπορεί με τον Επεκτεταμένο Ευκλείδιο Αλγόριθμο να υπολογίσει τα c, b έτσι ώστε:

$c \cdot a + b \cdot e_2 = 1$ (1)

Όμως αφού το $a|\varphi(n)$ προκύπτει: $b \cdot e_2 \equiv 1 \pmod{\varphi(n)})$
κι επομένως το $b \pmod{n}$ μπορεί να χρησιμοποιηθεί ως d_2.

Βιβλιογραφία

Zac12 : Σημειώσεις Ζάχου, ΕΜΠ, 2012.

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

Sho08 V. Shoup: A Computational Introduction to Number Theory and Algebra, 2nd edition, Cambridge University Press, 2008.

Tsa05 Π.Γ.Τσαγκάρης: Θεωρία Αριθμών, Συμμετρία, 2005.