Εθνικο Μετσοβιο Πολυτεχνειο

Σχολη Ηλεκτρολογων Μηχανικων & Μηχανικων Υπολογιστων

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Θανάσης Ανδρεου

Διδάσκοντες:
Στάθης Ζαχος
Άρης Παγουρτζης

5 Δεκεμβρίου 2011

Μικρό Θεώρημα Fermat

Από τις σημειώσεις [Ζάχος]: Κεφάλαιο 6, σελίδα 155.

Άσκηση 6.44: *Αν ο πρώτος p δε διαιρεί τον a και $n \equiv m \pmod{(p-1)}$ τότε $a^n \equiv a^m \pmod{p}$*

$$\begin{aligned} (p-1)|(n-m) \Rightarrow \\ \exists k \in \mathbb{Z} : n = k(p-1)+m \Rightarrow \\ a^n \equiv a^{k(p-1)+m} \pmod{p} \Rightarrow \\ a^n \equiv a^m \pmod{p} \end{aligned}$$

Ιδιότητα

$$\begin{aligned} \forall a \not\equiv 0 \pmod{p}, \forall n \in \mathbb{Z}_+, \\ a^n \equiv a^{n \underline{\bmod} (p-1)} \pmod{p} \end{aligned}$$

Ιδιότητα

$$\begin{aligned} \forall a \in \mathbb{Z}, gcd(a,m) = 1, \forall n \in \mathbb{Z}_+, \\ a^n \equiv a^{n \underline{\bmod} \phi(m)} \pmod{m} \end{aligned}$$

Κινέζικο Θεώρημα Υπολοίπων (Chinese Remainder Theorem)

Από τις σημειώσεις [Ζάχος]: Κεφάλαιο 6, σελίδα 156.

Το CRT συνεπάγεται έναν ισομορφισμό του $\mathbb{Z}_M$:
$\mathbb{Z}_M \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times ... \times \mathbb{Z}_{m_k}$

Τετραγωνικά Υπόλοιπα, Ο νομος Τετραγωνικής Αμοιβαιότητας

Από τις σημειώσεις [Ζάχος]: Κεφάλαιο 6, σελίδα 157.

Πρόταση 6.48 *Η εξίσωση $x^2 \equiv a \pmod{p}$ έχει λυση αν και μόνο αν $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Απόδειξη

$$\mathbb{Z}_p^* = \{g^1, g^2, ..., g^{p-1}(=1)\}$$

" $\Rightarrow$ " Έστω x_0 μια λύση, τότε $\exists k$

$$x_0 \equiv g^k \pmod{p} \Rightarrow$$
$$a \equiv {x_0}^2 \equiv g^{2k} \pmod{p} \Rightarrow$$
$$a^{\frac{p-1}{2}} \equiv g^{k(p-1)} \pmod{p} \Rightarrow \text{(Fermat)}$$
$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

" $\Leftarrow$ " Έστω $a \equiv g^b \pmod{p}$

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Rightarrow$$
$$g^{b\frac{p-1}{2}}$$

Έστω $b = 2\lambda + 1$, τότε

$$g^{(2\lambda+1)(\frac{p-1}{2})} \equiv 1 \pmod{p} \Rightarrow$$
$$g^{\lambda(p-1)} g^{(\frac{p-1}{2})} \equiv 1 \pmod{p}$$

Αυτό μας λέει ότι η τάξη του g είναι $\frac{p-1}{2}$.
Όμως το g είναι γεννήτορας και η τάξη του είναι $p-1$, άρα άτοπο, άρα

$$b = 2\lambda \Rightarrow$$
$$a \equiv g^{2\lambda} = (g^\lambda)^2 \Rightarrow$$

$\exists$ λύση: $g^\lambda \pmod{p}$

Παρατήρησεις

- Τα τετραγωνικά υπόλοιπα είναι οι άρτιες δυνάμεις του γεννήτορα.
- Το πλήθος των τετραγωνικών υπολοίπων είναι $\frac{p-1}{2}$.
- Για pq έχουμε $\frac{p-1}{2}\frac{q-1}{2}$ τετραγωνικά υπόλοιπα.

Σύμβολο Legendre

Από τις σημειώσεις [Ζάχος]: Κεφάλαιο 6, σελίδα 159.

Επιπρόσθετες ιδιότητες

- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, p$ πρώτος > 2.
- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}, p, q$ πρώτοι > 2. (Νόμος τετραγωνικής αντιστροφής)

Το κρυπτοσύστημα RSA

Από τις σημειώσεις [Ζάχος]: Κεφάλαιο 8, σελίδα 201.

Απόδειξη: *Η συνάρτηση D είναι αντίστροφη της E και για κάθε $x \in \mathbb{Z}_N^* \setminus U(\mathbb{Z}_N^*)$.*

$D(E(x)) = x^{ed} \underline{\text{mod}} N \equiv x^{1+k(p-1)(q-1)} \pmod N$

Έστω ότι $x \equiv 0 \pmod p, x \not\equiv 0 \pmod q$. (Το αντίστροφο είναι συμμετρικο).

$$x^{ed} \underline{\text{mod}} N \equiv \begin{cases} x^{1+k(p-1)(q-1)} \pmod q (1) \\ 0 \pmod p (2) \end{cases}$$

$(1) \Rightarrow 0 \equiv x \pmod p$.

$(2) \Rightarrow x^{1+(k(p-1))(q-1)} \equiv x \pmod q$.

Και από CRT $\Rightarrow$
$x^{ed} \underline{\text{mod}} N = x$

Κρυπτανάλυση του RSA και Παραγοντοποίηση

RSA-BREAK: given (y, e, N) find $x \in \mathbb{Z}_N$: $x^e \underline{\text{mod}} N = y$.

RSA-BREAK $\leq^p d -$ computation $\equiv^{RP} \phi(N)$ computation $\equiv^P$ factoring
(Αποδεικνύεται ότι αν μπορούσαμε να βρούμε τον εκθέτη d θα μπορούσαμε να βρούμε και το factoring με πιθανότικό αλγόριθμο).

RP: prop[correct answer] $\geq 1 - \frac{1}{2^{p(n)}}$
n : input size

p : polyonymial

Επίθεση Κοινού Γινομένου

Έχουμε κοινό N και

$$e_A, d_A : e_A d_A \equiv 1 \pmod{\phi(N)}$$

$$e_B, d_B : e_B d_B \equiv 1 \pmod{\phi(N)}$$

Ο B γνωρίζει e_A, d_B, e_B και θέλει να βρεί το d_A
Έστω ο B διαβάζει $y = x^{e_A} \underline{\text{mod}} N$
Όμως διαθέτει:

$$e_B d_B = 1 + k\phi(N)$$

, για κάποιο k
$g_0 = e_B d_B - 1 = k\phi(N)$

- Άν $gcd(g_0, e_A) = 1$,
  τότε θα μπορούσε ο B να υπολογίσει κάποιο $e_A {d_A}' \equiv 1 \pmod{g_0} \Rightarrow$
  ${e_A d_A}' = 1 + \lambda k\phi(N) \Rightarrow y^{{d_A}'} \equiv x \pmod{N}$
- Αν $gcd(g_0, e_A) \neq 1$,
  διαιρούμε με ένα $a|g_0$ και $gcd(a, e_A) = 1$. Άρα,
  $g_i = k'\phi(N) \Rightarrow gcd(e_A, g_i) = 1 \Rightarrow e_A d''_A \equiv 1 \pmod{g_i}$

Επομένως, δεν πρέπει να χρησιμοποιούμε κοινό γινόμενο.

Βιβλιογραφία

1. [Ζάχος]: Ε. Ζάχος, «Σημειώσεις στη Θεωρία Αριθμων και την Κρυπτογραφία», 2007