Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Αγαμέμνων Γιαννακόπουλος

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

2 Νοεμβριου 2012

1 Ασκήσεις στα Modulo

Άσκηση 1
Άν $gcd(a,n)=1$ τότε $\exists$ μοναδική λύση της $ax \equiv \text{mod} n$ στο $\mathbb{Z}_n$

ΛΥΣΗ

Άν $gcd(a,n)=1$ τότε $\exists$ λύση: $x \equiv a^{-1} \text{ mod } n$
Έστω x' κι άλλη λύση, τότε:

$ax \equiv \text{mod} n$ και $ax' \equiv \text{mod} n$

Άρα $a(x-x') \equiv 0 \text{ mod } n \Rightarrow n/a(x-x') \Rightarrow n/(x-x')$ (επειδή $gcd(a,n)=1$)
$\Rightarrow x=x'$.

Άσκηση 2
Έστω $gcd(a,n)=d$ τότε η $ax \equiv \text{mod} n$ έχει λύση $\Longleftrightarrow d/b$.

ΛΥΣΗ

$\Rightarrow$: Έστω x_0 μια λύση, τότε $ax_0 \equiv \text{mod} n \Rightarrow n/(ax_0-b) \Rightarrow d/b$.
$\Leftarrow$: Έστω οτι d/b, τότε $ax \equiv \text{mod} n \Leftrightarrow n/ax-b \Leftrightarrow \exists\, z : zn = ax-b$
$\Leftrightarrow \exists\, z : z\frac{n}{d} = a\frac{x}{d} - \frac{b}{d} \Leftrightarrow \frac{n}{d}/(\frac{a}{d}x - \frac{b}{d}) \Leftrightarrow \frac{a}{d}x \equiv \frac{b}{d} \text{ mod } \frac{n}{d}$
$\Leftrightarrow \exists x_0 \in \mathbb{Z}_{\frac{n}{d}} : \frac{a}{d}x_0 \equiv \frac{b}{d} \text{ mod } \frac{n}{d}$.
$\Leftrightarrow x_0 \equiv (\frac{a}{d})^{-1}(\frac{b}{d}) \text{ mod } \frac{n}{d}$.
Παρατηρούμε οτι υπάρχουν d λύσεις στο $\mathbb{Z}_n : x_0 + \frac{in}{d}$ με $0 \leqslant i \leqslant d$.

Λήμμα Απαλοιφής
$ax \equiv ax' \text{ mod } n \Rightarrow x \equiv x' \text{ mod } \left(\frac{n}{gcd(a,n)}\right)$.

Άσκηση 1.11 (από Παπαδημητρίου)
Δείξτε ότι $35 \mid \left(4^{1536} - 9^{4824}\right)$

ΛΥΣΗ

Παρατηρούμε πρώτα οτι $35 = 5 \cdot 7$
Δείχνωντας οτι το 5 και 7 διαιρεί το $4^{1536} - 9^{4824}$ θα έχουμε οτι και το 35 το διαιρεί.
Για το 7 έχουμε οτι:

$4^3 \equiv 1 \bmod 7 \Rightarrow 4^{1536} \equiv 1 \bmod 7$
$9^3 \equiv 1 \bmod 7 \Rightarrow 9^{4824} \equiv 1 \bmod 7$

Άρα $4^{1536} - 9^{4824} \equiv 0 \bmod 7$
Επίσης το τελευταίο ψηφίο του 4^{1536} είναι το 6 ενώ του 9^{4824} το 1.
Άρα $5/4^{1536} - 9^{4824}$ άρα $4^{1536} - 9^{4824} \equiv 0 \bmod 5$.
Προφανώς $4^{1536} - 9^{4824} \equiv 0 \bmod 35$.

Άσκηση 1.12 (από Παπαδημητρίου)
$(2^2)^{2006} \equiv\ ?\ \bmod 3$.

ΛΥΣΗ

Παρατηρούμε οτι $2^2 \equiv 1 \bmod 3$.
Άρα $\left(2^2\right)^{2006} = \left(\left(2^2\right)^2\right)^{1003} \equiv 1 \bmod 3$.