ΚΡΥΠΤΟΓΡΑΦΙΑ

24 Απριλίου 2012

Πρώτο σύνολο ασκήσεων

Στις παρακάτω ασκήσεις, το $\alpha\mu_x$ αναφέρεται στο υπόλοιπο της διαίρεσης του αριθμού μητρώου σας με τον αριθμό x.

1. (10%) Δώστε όλες τις υποομάδες των Z_a και Z_b^*, όπου $a = 4 + \alpha\mu_3$ και $b = 6 + \alpha\mu_5$.

2. (15%) Βρείτε τις λύσεις της εξίσωσης $16x = 8 \cdot (1 + \alpha\mu_{20}) \pmod{168}$.

3. (15%) Λύστε το σύστημα εξισώσεων

$$\begin{aligned} x &= (1 + \alpha\mu_{10}) \pmod{\text{A}} \\ x &= (1 + \alpha\mu_{30}) \pmod{\text{B}} \\ x &= (1 + \alpha\mu_{40}) \pmod{\Gamma}, \end{aligned}$$

   όπου $A = 11 + 6\alpha\mu_2$, $B = 31 + 4\alpha\mu_2$, και $\Gamma = 41 + 6\alpha\mu_2$.

4. (10%) Είναι ομάδα το σύνολο Z_n εφοδιασμένο με την πράξη του πολλαπλασιασμού; Τεκμηριώστε την απάντησή σας.

5. (10%) Έστω m ένας σύνθετος ακέραιος. Δείξτε ότι τουλάχιστον $\sqrt{m}$ στοιχεία του Z_m δεν έχουν πολλαπλασιαστικό αντίστροφο.

6. (10%) Έστω ότι υπάρχει ακέραιος n_0 τέτοιος ώστε να ισχύουν $gcd(p^{ab}, ab) = p$ για κάθε πρώτο $p \leq n_0$ και $gcd(p^{ab}, ab) = 1$ για κάθε πρώτο $p > n_0$. Δείξτε ότι $gcd(a, b) = 1$.

7. (15%) Αποδείξτε ότι $(p-1)! = -1 \pmod{\text{p}}$, όπου ο p είναι πρώτος αριθμός.

8. (15%) Δείξτε ότι ισχύει $7^n + 9^n = 0 \pmod{11}$ όταν $n = 5 \pmod{10}$.

Παράδοση: Πέμπτη, 03/05/2012, 15.00