Πανεπιστημιο Αιγαιου
Τμημα Μαθηματικων
83 200 Καρλοβασι
Σαμος

Καρλόβασι 12/02/2009

Θέματα στη Θεωρία Αριθμών

1. Να λυθεί η γραμμική ισοδυναμία $70x \equiv 16(\mathrm{mod} 41)$.

2. Ποιές απο τις παρακάτω προτάσεις αληθινές; Να δικαιολογήσετε την απάντησή σας.

(α) Σε ένα κινεζικό σύστημα είτε δεν έχουμε καμμία ακέραια λύση ή έχουμε άπειρες.

(β) Δεν είναι δυνατόν να υπάρχει ο αντίστροφος του 18 $(\mathrm{mod} 15)$

(γ) Αν ο $m > 2$ έχει μια αρχική ρίζα g τότε αναγκαστικά ισχύει $g^{\frac{\phi(m)}{2}} \equiv -1 \bmod m$ όπου ϕ είναι η συνάρτηση του Euler.

3. Να υπολογισθεί το $2^{602} \bmod 13$ με χρήση του κατάλληλου Θεωρήματος για την αποτελεσματική εύρεση των δυνάμεων που εμφανίζονται.

4. Να λυθεί η πολυωνυμική ισοτιμία

$$x^3 + 3x + 1 \equiv 0(\mathrm{mod} 75).$$

5. Ο διακριτός λογάριθμος έχει παρόμοιες ιδιότητες με τον κανονικό λογάριθμο. Χρησιμοποιώντας τις ιδιότητες που αυτός έχει και το γεγονός ότι το $g = 5$ είναι αρχική ρίζα $(\mathrm{mod} 18)$ να λύσετε την εκθετική ισοτιμία

$$7^x \equiv 13(\mathrm{mod} 18).$$

Χρόνος εξέτασης: 3 ώρες. Τα θέματα είναι ισοδύναμα.

Καλή επιτυχία!

Ο διδάξας

Χαράλαμπος Κορνάρος

Απαντήσεις: 1)$70^{-1} \equiv 17(\mathrm{mod} 41)$. Οπότε $x \equiv 17 \cdot 26 \equiv 26(\mathrm{mod} 41)$.
2)(α) ναί, (β) ναί, (γ) ναί.

3)$4(\bmod 13)$ με χρήση του Θεωρήματος του Fermat
4)Το σύστημα το αναλύουμε σε $x^3+3x+1 \equiv (\bmod 25)$ και $x^3+3x+1 \equiv (\bmod 3)$. Το πρώτο λύνεται δουλεύοντας κατά τα γνωστά με λύση $x \equiv 21(\bmod 25)$ και το δεύτερο εύκολα με δοκιμή $x \equiv 2(\bmod 3)$. Λύνοντας το κινεζικό σύστημα που προκύπτει παίρνουμε τελικά $x \equiv 71(\bmod 3)$
5) Έχουμε εύκολα $5^2 \equiv 7(\bmod 18)$ και $5^4 \equiv 13(\bmod 18)$. αντικαθιστώντας και παίρνοντας τα εκθετικά έχουμε $2x \equiv 4(\bmod \phi(18))$, οπότε $x \equiv 2$ ή $5(\bmod 6)$.