Εξέταση Θεωρίας Αριθμών

27 Ιανουαρίου 2003

1. Για m, n ακεραίους $n > m$, ορίζεται το $\binom{n}{m} = \frac{n!}{m!(n-m)!}$. Δείξτε ότι το $\binom{n}{m}$ είναι ακέραιος.

2. Να υπολογίσετε τον μέγιστο κοινό διαιρέτη των αριθμών 234 και 71 και να εφραστεί σαν γραμμικός συνδιασμός αυτών. Στην συνέχεια να λυθεί η
$$71x \equiv 1 \mod 234$$
και η
$$142x \equiv 2 \mod 468.$$

3. Να βρεθούν οι αριθμοί x που όταν διαιρεθούν με το 3 αφήνουν υπόλοιπο 2, όταν διαιρεθούν με το 5 αφήνουν υπόλοιπο 3 και όταν διαιρεθούν με το 7 αφήνουν υπόλοιπο 2.

4. Να οριστεί η συνάρτηση ϕ του Euler. Να δείξετε ότι είναι πολλαπλασιαστική και ότι
$$\phi(p^k) = p^k - p^{k-1}.$$

5. Να διατυπώσετε το «μικρό» θεώρημα του Fermat. Αν p, q είναι πρώτοι αριθμοί, διαφορετικοί μεταξύ τους, να αποδειχτεί ότι
$$p^{q-1} + q^{p-1} \equiv 1 \mod pq.$$

6. Να οριστεί η τάξη ενός αριθμού modulo m. Να οριστεί η πρωταρχική ρίζα modulo m, και ο δείκτης ενός αριθμού ως προς μια πρωταρχική ρίζα. Αν w, u είναι δύο αρχικές ρίζες modulo p, όπου p πρώτος αριθμός, να αποδειχτεί ότι ισχύει
$$\mathrm{ind}_u a \equiv \mathrm{ind}_{\mathrm{w}} a \cdot \mathrm{ind}_u w \mod (p-1).$$

7. Να εξετάσετε αν η ισοδυναμία
$$x^2 \equiv 23 \mod 5231,$$
έχει λύσεις. Δίνεται ότι ο αριθμός 5231 είναι πρώτος.

Καλή Επιτυχία