ΕΠΛ 232: Αλγόριθμοι και Πολυπλοκότητα

Κατ'οίκον Εργασία 4

Ημερομηνία Παράδοσης: 26/04/02

1. (α) Να προτείνετε δίκτυο σύγκρισης με n γραμμές και το ελάχιστο δυνατό βάθος το οποίο να επιστρέφει στην πρώτη του γραμμή το ελάχιστο στοιχείο και στην τελευταία του γραμμή το μέγιστο στοιχείο από το δεδομένο εισόδου του. Να αιτιολογήσετε την απάντησή σας.
   (β) Να προτείνετε και να σχεδιάσετε δίκτυο ταξινόμησης για 8 στοιχεία βασισμένο στον αλγόριθμο ταξινόμησης InsertionSort. Να γενικεύσετε το δίκτυό σας για n στοιχεία. Ποιο το μέγεθος και ποιο το βάθος του δικτύου σας;

2. (α) Να προτείνετε αποδοτικό παράλληλο αλγόριθμο ο οποίος, με δεδομένο εισόδου ένα γράφο, να υπολογίζει τα μήκη των βραχύτερων μονοπατιών για όλα τα ζεύγη κορυφών του γράφου. Ποιος ο χρόνος εκτέλεσης του αλγορίθμου σας;
   (β) Έχετε στη διάθεσή σας $n^3/\log n$ επεξεργαστές. Να προτείνετε παράλληλο αλγόριθμο ο οποίος να υπολογίζει το γινόμενο δύο $n \times n$ πινάκων σε χρόνο $O(\log n)$.

3. CLR, άσκηση 33.2-9, σελίδα 813.

4. (α) Έστω $n=863 \cdot 877=756851$, όπου 863 και 877 είναι πρώτοι αριθμοί, και $e=5$. Να υπολογίσετε την τιμή του $\phi(n)$ και τιμή d τέτοια ώστε $e \cdot d \equiv 1 \bmod \phi(n)$.
   (b) Είστε χρήστης ενός RSA κρυπτοσυστήματος με δημόσιο κλειδί $n=756851$ και $e=5$. Υποθέστε πως οι τιμές του Z_n γράφονται πάντα ως εξαψήφιοι αριθμοί (αν χρειάζεται επενδυμένοι με αρχικά μηδενικά, π.χ. το 12 γράφεται ως 000012). Τότε, μπορούμε να υποθέσουμε ότι τα στοιχεία του Z_n αντιπροσωπεύουν τριάδες γραμμάτων όπου $00 \leftrightarrow$A, $01 \leftrightarrow$B, $02 \leftrightarrow$C, …, $25 \leftrightarrow$Z, π.χ. 1719 = 001719 $\leftrightarrow$ ART. Να κρυπτογραφήσετε το μήνυμα ALGORITHM.