Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Προηγμένα Θέματα Αλγορίθμων

Αλγόριθμοι Δικτύων και Πολυπλοκότητα

Εαρινό εξάμηνο 2018-2019

(ΕΜΠ – ΑΛΜΑ)

Διδάσκοντες: Δ. Φωτάκης - Α. Παγουρτζής

3η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 27/6/2019 (κατά την εξέταση)

Η σειρά αυτή είναι ημιτελής. Θα ολοκληρωθεί σύντομα.

Άσκηση 1

Αποδείξτε ότι για πεπερασμένη ομάδα G και υποσύνολο $H \subseteq G$, H είναι υποομάδα της G αν και μόνο αν το H είναι κλειστό ως προς την πράξη της ομάδας.

Άσκηση 2

Αποδείξτε το Θεώρημα Lagrange. Ειδικότερα, αποδείξτε ότι για πεπερασμένη ομάδα G, και υποομάδα $H \subseteq G$, δύο (δεξιά) σύμπλοκα της H είτε ταυτίζονται είτε είναι ξένα μεταξύ τους, και έχουν ίδια πληθικότητα με την H.

Άσκηση 3

Bonus άσκηση (προαιρετική): `https://courses.corelab.ntua.gr/pluginfile.php/494/mod_resource/content/2/BONUS_CRYPTO.pdf`

Σημείωση: αγνοήστε την ημερομηνία παράδοσης που αναγράφεται στην εκφώνηση.

Άσκηση 4

Αποδείξτε ότι στην περίπτωση όπου $n = p^e, e > 1, p$ περιττός, ο έλεγχος Miller-Rabin επιτυγχάνει με πιθανότητα $> 1/2$. Συγκεκριμένα, αποδείξτε ότι για περισσότερα από τα μισά $b \in \mathbb{Z}_n : b^{n-1} \not\equiv 1 \pmod{n}$.

Υπόδειξη: θεωρήστε γνωστό το γεγονός ότι η ομάδα $U(\mathbb{Z}_n)$ είναι κυκλική για $n = p^e, e > 0, p$ περιττό.

Άσκηση 5

Διατυπώστε παραμετρικό αλγόριθμο για το πρόβλημα Dominating Set με παράμετρο το μέγεθος του κυρίαρχου συνόλου. Είναι ο αλγόριθμός σας FPT; Εξηγήστε. Αλλάζει κάτι αν θεωρήσουμε ως παράμετρο και τον μέγιστο βαθμό του γράφου εισόδου Δ;