Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία
3η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 18/11/2017

16 Νοεμβρίου 2017

1η Άσκηση

Αποδείξτε ότι αν a,b είναι περιττοί ακέραιοι, τότε ισχύει ότι $16 \mid a^4 + b^4 - 2$.

2η Άσκηση

Να λύσετε το σύστημα εξισώσεων:

$$x \equiv 1 + \alpha\mu_{25} \pmod{A}$$
$$x \equiv 1 + \alpha\mu_{40} \pmod{B}$$
$$x \equiv 1 + \alpha\mu_{55} \pmod{C}$$

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

3η Άσκηση

Έστω G ομάδα με την ακόλουθη ιδιότητα: από κάθε τρία διακριτά στοιχεία της G, τουλάχιστον δύο από αυτά αντιμετατίθενται. Δείξτε ότι η G είναι αβελιανή. Ισχύει το ίδιο αν αντικατασταθεί η λέξη "τρία"με την "τέσσερα";

4η Άσκηση

Αποδείξτε ότι $(p-1)! = -1 \pmod{p}$, όπου p πρώτος αριθμός. Αποδείξτε ότι αν $gcd(a,p) = 1$ τότε $\prod_{j=1}^{p-1} j \equiv \prod_{i=1}^{p-1} ai \pmod{p}$, όπου p πρώτος αριθμός και a ακέραιος.

5η Άσκηση

Δείξτε ότι μια ομάδα G με n στοιχεία είναι κυκλική αν και μόνο αν υπάρχει $x \in G$ τέτοιο ώστε $ord(x) = n$.

6η Άσκηση

Έστω m ένας σύνθετος ακέραιος. Δείξτε ότι τουλάχιστον $\sqrt{m}$ στοιχεία του $\mathbb{Z}_m$ δεν έχουν πολλαπλασιαστικό αντίστροφο.

7η Άσκηση

Δείξτε ότι $gcd(2^s - 1, 2^t - 1) = 1$ αν και μόνο αν $gcd(s, t) = 1$.

8η Άσκηση

Έστω $n = pq$ και έστω ότι γνωρίζετε έναν ακέραιο k που είναι πολλαπλάσιο του $p - 1$ αλλά όχι του $q - 1$. Βρείτε αποδοτικό πιθανοτικό αλγόριθμο παραγοντοποίησης του n.

9η Άσκηση

Σχεδιάστε αλγόριθμο επαναλαμβανόμενου τετραγωνισμού (για ύψωση σε δύναμη $a^b \bmod p$) υποθέτοντας ότι ο εκθέτης b δίνεται σε δυαδική μορφή. Χρησιμοποιήστε τα ψηφία του εκθέτη από το περισσότερο προς το λιγότερο σημαντικό (από 'αριστερά προς τα δεξιά').

Σημείωση: Στις παραπάνω ασκήσεις $\alpha\mu_x = AM \bmod x$, όπου ΑΜ ο αριθμός μητρώου σας.

Συμβουλή: Ακόμη και αν συνεργαστείτε για την επίλυση μιας άσκησης, ή βρείτε τη λύση της στο δίκτυο ή σε βιβλία, θα ωφεληθείτε αν γράψετε την απάντησή σας ατομικά (προσπαθήστε να την αναπαραγάγετε 'εκ του μηδενός').