Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

---

# Υπολογιστική Κρυπτογραφία
# 2η Σειρά Ασκήσεων

*Προθεσμία παράδοσης: 17/11/2016*

9 Νοεμβρίου 2016

## 1η Άσκηση

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

## 2η Άσκηση

Βρείτε τις λύσεις της εξίσωσης $39x \equiv 13 \cdot (1 + \alpha\mu_{20}) \pmod{143}$.

## 3η Άσκηση

Δώστε όλες τις υποομάδες των $\mathbb{Z}_a$ και $\mathbb{Z}_b^*$ όπου $a = 5 + \alpha\mu_3$ και $b = 9 + \alpha\mu_5$.

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

## 5η Άσκηση

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

## 6η 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.

## 7η Άσκηση

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

## 8η Άσκηση

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

## 9η Άσκηση

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

## 10η Άσκηση

Έστω ότι υπάρχει ακέραιος $n_0$ τέτοιος ώστε να ισχύουν $\gcd(p^{ab}, ab) = p$ για κάθε πρώτο $p \leq n_0$ και $\gcd(p^{ab}, ab) = 1$ για κάθε πρώτο $p > n_0$. Δείξτε ότι $\gcd(a,b) = 1$.

## 11η Άσκηση

Συμπληρώστε τις λεπτομέρειες της απόδειξης του Θεμελιώδους Θεωρήματος της Αριθμητικής (βλ. διαφάνεια #7 στην ενότητα 'Εισαγωγή στη Θεωρία Αριθμών').

## 12η 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 $n$.

## 13η Άσκηση

Υπολογίστε τα $(\frac{19}{61}), (\frac{17}{31}), (\frac{107}{117})$ χρησιμοποιώντας μόνο το θεώρημα τετραγωνικής αντιστροφής καθώς και άλλες ιδιότητες των συμβόλων, χωρίς χρήση παραγοντοποίησης (εκτός με το 2).

## 14η 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').

## 15η Άσκηση

Έστω $\mathbb{Z}_p^*$ με $p$ πρώτο και $g$ ένας γεννήτορας, $p, g$ γνωστά.

1. Αν $d$ ένας ακέραιος που διαιρεί το $p-1$, βρείτε με αποδοτικό τρόπο ένα στοιχείο $b$ του $\mathbb{Z}_p^*$ τάξης $d$ (δηλαδή $d$ ο μικρότερος ακέραιος με $b^d \equiv 1 \pmod{p}$)
2. Πόσα στοιχεία τάξης $d$ υπάρχουν μέσα στο $\mathbb{Z}_p^*$;
3. Πόσους γεννήτορες έχει η κυκλική υποομάδα που παράγει ένα στοιχείο $b$ τάξης $d$;
4. Πόσες κυκλικές υποομάδες τάξης $d$ υπάρχουν στο $\mathbb{Z}_p^*$;
5. Αν μας δώσουν ένα στοιχείο $h$, την τάξη του $d$ και ένα τυχαίο στοιχείο $a$, πως μπορούμε να δούμε αν το $a$ ανήκει στην υποομάδα που παράγει το $h$ σε πολυωνυμικό χρόνο;

*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').