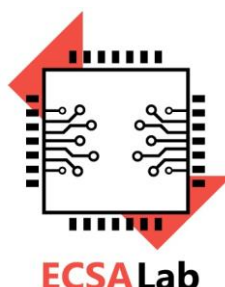


**Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών  
Υπολογιστών του  
Πανεπιστημίου Πελοποννήσου**

**Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και  
Εφαρμογών (ECSA Lab.)**



**Ασφάλεια Υπολογιστικών Συστημάτων**

Διδάσκων: Δρ. Παρασκευάς Κίτσος (Καθηγητής)

**Ασκήσεις στη θεματική ενότητα της Θεωρίας Αριθμών**

- 1) Αν ισχύουν οι παρακάτω σχέσεις  $a \equiv b \pmod{n}$  και  $c \equiv d \pmod{n}$  να δείξετε ότι  $(a+c) \equiv (b+d) \pmod{n}$  και  $ac \equiv (db) \pmod{n}$ .
- 2) Να υπολογίσετε τον Μέγιστο Κοινό Διαιρέτη μεταξύ των αριθμών 354448 και 233456.
- 3) Κάνοντας χρήση της μεθόδου του επαναλαμβανόμενου τετραγωνισμού – και – πολλαπλασιασμού υπολογίστε το  $5^{11} \pmod{2005}$ .
- 4) Χρησιμοποιήστε την ανεπτυγμένη μορφή του αλγορίθμου Ευκλείδη και αποδείξτε ότι  $\gcd(12345, 11111) = 1$ . Βρείτε τους ακεραίους  $x$  και  $y$  για τους οποίους ισχύει  $12345x + 11111y = 1$ . Ποιος είναι ο  $11111^{-1} \pmod{12345}$ .
- 5) i) Να υπολογίσετε τον αντίστροφο του  $3 \pmod{101}$ . α) Με την βοήθεια του θεωρήματος Euler β) Με την βοήθεια της ανεπτυγμένης μορφής του αλγορίθμου του Ευκλείδη.

ii) Να βρείτε το  $30^{70} \bmod (101)$