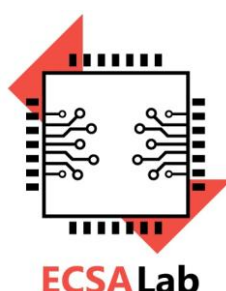


**Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών
Υπολογιστών του
Πανεπιστημίου Πελοποννήσου**

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



Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος

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 $ac \equiv (db) \pmod{n}$.

ΛΥΣΗ:

Ξέρουμε ότι ισχύει $a \equiv b \pmod{n}$ αν και μόνο αν $n|(b-a)$.

Άρα έχουμε $a \equiv b \pmod{n} \rightarrow n|(b-a) \rightarrow b-a=in$.

Όμοια αν $c \equiv d \pmod{n} \rightarrow d-c=jn$.

Προσθέτουμε κατά μέλη και έχουμε

$$(b-a)+(d-c)=in+jn \rightarrow (b+d)-(a+c)=(i+j)n \rightarrow (a+c) \equiv (b+d) \pmod{n}$$

Επίσης έχουμε $a \equiv b \pmod{n} \rightarrow b-a=in$ (1). Και $c \equiv d \pmod{n} \rightarrow d-c=jn$ (2).

Πολλαπλασιάζουμε την (1) με c και έχουμε $cb-ca=cin$ (3)

Πολλαπλασιάζουμε την (2) με b και έχουμε $bd-bc=bjn$ (4)

Και τέλος προσθέτουμε κατά μέλη τις (3) και (4) και έχουμε $cb-ca+bd-bc=cin+bjn \rightarrow db-ca=(ci+bj)n \rightarrow ac \equiv (db) \pmod{n}$

2) Να υπολογίσετε τον Μέγιστο Κοινό Διαιρέτη μεταξύ των αριθμών 354448 και 233456.

ΛΥΣΗ:

Για οποιονδήποτε μη αρνητικό ακέραιο a και οποιονδήποτε θετικό ακέραιο b , ισχύει: $\gcd(a, b) = \gcd(b, a \bmod b)$.

Επίσης ισχύει $a \bmod n = \begin{cases} a, & \text{αν } n = 0 \\ a - \lfloor a/n \rfloor n, & \text{διαφορετικά} \end{cases}$

Άρα έχουμε, $\gcd(354448, 233456) =$
 $\gcd(233456, 354448 \bmod 233456) =$
 $\gcd(233456, 120992) =$
 $\gcd(120992, 233456 \bmod 120992) =$
 $\gcd(120992, 112464) =$
 $\gcd(112464, 120992 \bmod 112464) =$
 $\gcd(112464, 8528) =$
 $\gcd(8528, 112464 \bmod 8528) =$
 $\gcd(8528, 112464 - \lfloor 112464/8528 \rfloor 8528) =$
 $\gcd(8528, 1600)$
 $= \dots =$
 $\gcd(0, 16) = 16$

3) Κάνοντας χρήση της μεθόδου του επαναλαμβανόμενου τετραγωνισμού – και – πολλαπλασιασμού υπολογίστε το $5^{11} \bmod 2005$.

ΛΥΣΗ:

Έχουμε $5^{11} \bmod 2005 = 5 (5^2) (5^8) \bmod 2005$.

Έπειτα δημιουργούμε έναν πίνακα

$$5 \bmod 2005 = 5$$

$$5^2 \bmod 2005 = 25$$

$$5^4 \bmod 2005 = 25^2 \bmod 2005 = 625$$

$$5^8 \bmod 2005 = 625^2 \bmod 2005 = 1655$$

$$\text{Άρα, } 5^{11} \bmod 2005 = 5 \times 25 \times 1655 \bmod 2005 = 360$$

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 $12345x + 11111y = 1$.

ΛΥΣΗ:

Έχουμε αρχικά $\gcd(12345, 11111) = \gcd(11111, 12345 \bmod 11111) = \gcd(11111, 1234) = \gcd(1234, 11111 \bmod 1234) = \gcd(1234, 5) = \gcd(5, 1234 \bmod 5) = \gcd(5, 4) = \gcd(4, 5 \bmod 4) = \gcd(4, 1) = \gcd(1, 4 \bmod 1) = \gcd(1, 0) = 1$. Άρα έχουμε το ζεύγος $(a, b) = (1, 0)$ και ξεκινώντας από αυτό εκτελούμε, «προς τα πίσω», τον αλγόριθμο του Ευκλείδη στην ανεπτυγμένη μορφή του.

Άρα για $(a, b) = (1, 0)$ έχουμε $d \leftarrow 1, x \leftarrow 1, y \leftarrow 0$. Για $(a, b) = (4, 1)$ έχουμε

$$y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = 1 - \left\lfloor \frac{4}{1} \right\rfloor 0 = 1 \text{ και } x \leftarrow y' = 0. \text{ Όμοια για } (a, b) = (5, 4) \text{ έχουμε}$$

$$y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = 0 - \left\lfloor \frac{5}{4} \right\rfloor 1 = -1 \text{ και } x \leftarrow y' = 1. \text{ Για } (a, b) = (1234, 5) \text{ έχουμε}$$

$$y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = 1 - \left\lfloor \frac{1234}{5} \right\rfloor (-1) = 1 - (246)(-1) = 247 \text{ και } x \leftarrow y' = -1. \text{ Επίσης για}$$

$(a, b) = (11111, 1234)$ έχουμε

$$y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = (-1) - \left\lfloor \frac{11111}{1234} \right\rfloor (247) = (-1) - (9)(247) = -2224 \text{ και } x \leftarrow y' = 247.$$

Τελικά για το αρχικό ζεύγος $(a, b) = (12345, 11111)$ έχουμε,

$$y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = (247) - \left\lfloor \frac{12345}{11111} \right\rfloor (-2224) = 247 - (1)(-2224) = 2471 \text{ και}$$

$$x \leftarrow y' = -2224. \text{ Άρα οι ζητούμενοι ακέραιοι } x \text{ και } y \text{ για τους οποίους ισχύει}$$

$$12345x + 11111y = 1 \text{ είναι οι } x = -2224 \text{ και } y = 2471, \text{ δηλαδή ισχύει } \gcd$$

$$(12345, 11111) = 12345(-2224) + 11111(2471) = 1.$$

5) i) Να υπολογίσετε τον αντίστροφο του $3 \bmod (101)$ Με την βοήθεια του θεωρήματος Euler.

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

ΛΥΣΗ:

i) α) Από το θεώρημα Euler ο αντίστροφος του $3 \bmod (101)$ είναι:

$$3^{\phi(101)-1} \bmod(101) = 3^{99} \bmod(101). \text{ Επίσης ισχύει ότι, } 3^{99} = 3^{64} \times 3^{32} \times 3^2 \times 3.$$

Έπειτα δημιουργούμε τον πίνακα.

$$3 \bmod (101) = 3$$

$$3^2 \bmod (101) = 9$$

$$3^{32} \bmod (101) = 54$$

$$3^{64} \bmod (101) = (3^{32})^2 \bmod (101) = 54^2 \bmod (101) = 88$$

Άρα τελικά έχουμε $3^{99} \bmod (101) = 3 \times 9 \times 54 \times 88 \bmod (101) = 34 \equiv 34 \bmod (101)$.

Ισχύει $30^{70} \bmod (101) = 30^{64} \times 30^4 \times 30^2 \bmod (101)$.

Έπειτα δημιουργούμε τον πίνακα.

$$30^2 \bmod (101) = 900 \bmod (101) = 92$$

$$30^4 \bmod (101) = 81$$

$$30^{64} \bmod (101) = 88$$

Οπότε τελικά έχουμε, $30^{70} \bmod (101) = 88 \times 81 \times 92 \bmod (101) = 84 \equiv 84 \bmod (101)$.