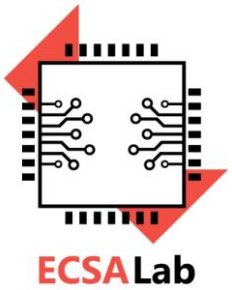
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

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 ≡ b (mod n) και c ≡ d (mod n) να δείξετε ότι (a+c) ≡ (b+d) (mod n) και ac ≡ (db) mod n.

ΛΥΣΗ:

Ξέρουμε ότι ισχύει a ≡ b (mod n) αν και μόνο αν n|(b-a).

Άρα έχουμε a ≡ b (mod n)→n|(b-a)→b-a=in.

Όμοια αν c ≡ d (mod n) →d-c=jn.

Προσθέτουμε κατά μέλη και έχουμε

(b-a)+(d-c)=in+jn→(b+d)-(a+c)=(i+j)n→ (a+c) ≡ (b+d) (mod n)

Επίσης έχουμε a ≡ b (mod n)→b-a=in (1). Και c ≡ d (mod n) →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→db-ca=(ci+bj)n→ ac ≡ (db) mod 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 mod b).

Επίσης ισχύει a mod 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 mod 233456)=

gcd(233456, 120992)=

gcd(120992, 233456 mod 120992)=

gcd(120992, 112464)=

gcd(112464, 120992 mod 112464)=

gcd(112464, 8528)=

gcd(8528, 112464 mod 8528)=

gcd(8528, 112464-⌞112464/8528⌟8528)=

gcd(8528, 1600)

=...=

gcd(0, 16)=16

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

ΛΥΣΗ:

Έχουμε 5^{11} mod 2005 = 5 (5^2) (5^8) mod 2005.

Έπειτα δημιουργούμε έναν πίνακα

5 mod 2005 = 5

5^2 mod 2005 = 25

5^4 mod 2005 = 25^2 mod 2005 = 625

5^8 mod 2005 = 625^2 mod 2005 = 1655

Άρα, 5^{11} mod 2005 = 5 x 25 x 1655 mod 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 mod 11111) = gcd(11111, 1234) = gcd(1234, 11111 mod 1234) = gcd(1234, 5) = gcd(5, 1234 mod 5) = gcd(5, 4) = gcd(4, 5 mod 4) = gcd(4, 1) = gcd(1, 4 mod 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 ← 1, x ← 1, y ← 0. Για (a, b) = (4, 1) έχουμε $y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = 1 - \left\lfloor \frac{4}{1} \right\rfloor 0 = 1$ και $x \leftarrow y' = 0$. Όμοια για (a, b) = (5, 4) έχουμε

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

$y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = 1 - \left\lfloor \frac{1234}{5} \right\rfloor (-1) = 1 - (246)(-1) = 247$ και $x \leftarrow y' = -1$. Επίσης για (a, b) = (11111, 1234) έχουμε

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

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

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

$x \leftarrow y' = -2224$. Άρα οι ζητούμενοι ακέραιοι x και y για τους οποίους ισχύει 12345x + 11111y = 1 είναι οι $x = -2224$ και $y = 2471$, δηλαδή ισχύει gcd (12345, 11111) = 12345(-2224) + 11111(2471) = 1.

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

ii) Να βρείτε το 30^{70} mod (101)

ΛΥΣΗ:

i) α) Από το θεώρημα Euler ο αντίστροφος του 3 mod (101) είναι: $3^{\phi(101)-1} \bmod(101) = 3^{99} \bmod(101)$. Επίσης ισχύει ότι, $3^{99}=3^{64}$ x 3^{32}x 3^2 x 3.

Έπειτα δημιουργούμε τον πίνακα.

3 mod (101) = 3

3^2 mod (101) = 9

3^{32} mod (101) = 54

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

Άρα τελικά έχουμε 3^{99} mod (101) = 3 x 9 x 54 x 88 mod (101) = 34 ≡ 34 mod (101).

Ισχύει 30^{70} mod (101) = 30^{64} x 30^4 x 30^2 mod (101).

Έπειτα δημιουργούμε τον πίνακα.

30^2 mod (101) = 900 mod (101)=92

30^4 mod (101) = 81

30^{64} mod (101) = 88

Οπότε τελικά έχουμε, 30^{70} mod (101) = 88 x 81 x 92 mod (101)= 84 ≡ 84 mod (101).