Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

Κρυπτογραφία

1ο Set Ασκήσεων

Διδάσκουσα: Ελισάβετ Κωνσταντίνου
Μάρτιος 2018

Αυλακιώτης Χρήστος
321/2012015

Ζήτημα 1 (0.8 μονάδες) Υπολογίστε τα αποτελέσματα των παρακάτω πράξεων στο $\mathbb{Z}_{28}$: a+b, a-b, 2ab, a/b, 4b/a, b/5 όπου a = 15 και b =

Απάντηση

15 = 15mod28
και 18 = 18mod28

- a+b
  (15+18)mod28 = 5
  Άρα a+b = (15+18)mod28 $\equiv$ 5mod28

- a-b
  (15-18)mod28 = 25
  Άρα a-b = (15-18)mod28 $\equiv$ 25mod28

- 2ab
  (15 $\times$ 18)mod28 = 25
  Άρα a-b = (15-18)mod28 $\equiv$ 25mod28

- a/b
  Για να ορίζεται η πράξη πρεπει το b να είναι αντιστρέψιμο. gcd(18,28)=2 άρα δεν είναι αντιστρέψιμο και συνεπώς ηπράξη δεν ορίζεται.

- 4b/a
  Για να ορίζεται η πράξη πρεπει το a να είναι αντιστρέψιμο. gcd(15,28)=1 άρα είναι αντιστρέψιμο και συνεπώς η πράξη ορίζεται. Άρα υπάρχει $15^{-1} \equiv$ 15mod28. Διότι 15 $\times$ 15 $\equiv$ 1mod28. Άρα 4b/a = 4 $\times$ 18 $\times$ 15 = 1080 $\equiv$ 1052mod28

- b/5
  Για να ορίζεται η πράξη πρεπει το 5 να είναι αντιστρέψιμο. gcd(5,28)=1 άρα είναι αντιστρέψιμο και συνεπώς η πράξη ορίζεται. Άρα υπάρχει $5^{-1} \equiv$ 17mod28. Διότι 5 $\times$ 17 $\equiv$ 1mod28. Άρα b/5 = 18 $\times$ 17 = 306 $\equiv$ 288mod28

Ζήτημα 2 (0.8 μονάδες) Από ποια στοιχεία αποτελείται το σύνολο $\mathbb{Z}_{42}$ και από ποια το $\mathbb{Z}^*{}_{42}$;

Απάντηση

Το $\mathbb{Z}_{42}$ αποτελείται απο τα στοιχεία {0,1 ... 41}. Η πολλαπλασιαστική ομάδα αποτελείται απο τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_{42}$. Δηλαδή $\mathbb{Z}^*{}_{42}$ = {1,5,11,13,17,19,23,25,29,31,37,41}

Ζήτημα 3 (0.9 μονάδες) Έστω ότι συμβολίζουμε με X το σύνολο των ρητών αριθμών που είναι μεγαλύτεροι του 1. Αν ορίσουμε ως πράξη επί του X την a*b -> a^{lnb} για κάθε a και b στο X, τότε το σύνολο X αποτελεί ομάδα; Αν ναι, είναι αντιμεταθετική;

Απάντηση

Για να αποτελεί το X ομάδα θα πρέπει η πράξη * να έχει τις εξείς ιδιότητες:

1. x*(y*z) = (x*y)*z για κάθε x,y,z $\in$ X.
2. Υπάρχει g $\in$ X τέτοιο ώστε για κάθε x $\in$ X να ισχύει x*g = x = g*x.

3. Για κάθε x ∈ X υπάρχει ένα x' ∈ X τέτοιο ώστε x*x' = g = x'*x.

1. $x^{(lny^{lnz})}$ = $(x^{lny})^{lnz}x$ ⇔ $x^{lnz \times lny}$ = $(lny \times x)^{lnz}$ ⇔ $lnx^{lnz \times lny}$ = $ln(lny \times x)^{lnz}$ ⇒ lnz × lny × lnx = lnz × lny × lnx όπου ισχύει.
2. χ^{lng} = x = g^{lnx}
   - χ^{lng} = x ⇔ lnx^{lng} = lnx ⇒ lng×lnx = lnx
   - g^{lnx} = x ⇔ lng^{lnx} = lnx ⇒ lnx×lng = lnx

   Ισχύει για g = e.
3. $x^{lnx'}$ = e = x'^{lnx} $x^{lnx'}$ = e ⇔ $lnx^{lnx'}$ = lne ⇔ lnx' × lnx = 1 ⇔ lnx' = $\frac{1}{lnx}$ ⇔ x' = $e^{\frac{1}{lnx}}$.
   Αρα για κάθε χ ∈ X το συμμετρικό του στοιχείο είναι το $e^{\frac{1}{lnx}}$

Για να είναι και αντιμεταθετική θα πρέπει a*b = b*a ⇒ a^{lnb} = b^{lna} ⇔ lna^{lnb} = lnb^{lna} ⇔ lnb × lna = lna × lnb όπου ισχύει. Άρα η ομάδα X είναι και αντιμεταθετική.

Ζήτημα 4 (2.5 μονάδες) Φτιάξτε ένα πρόγραμμα που να υλοποιεί το CRT (σε όποια γλώσσα προγραμματισμού επιθυμείτε). Θα χρειαστεί να υλοποιήσετε επίσης τον επεκταμένο αλγόριθμο του Ευκλείδη. Εφαρμόστε το πρόγραμμά σας για να βρείτε την λύση στο εξής πρόβλημα: 7 ληστές προσπαθούν να μοιραστούν ένα κιβώτιο με μπάρες χρυσού. Στη μοιρασιά περισσεύουν 6 μπάρες. Στον τσακωμό που ακολουθεί ένας ληστής σκοτώνεται. Οι υπόλοιποι 6 ληστές προσπαθούν να μοιραστούν τις μπάρες χρυσού, όμως τώρα περισσεύουν 2 μπάρες. Στον τσακωμό που ακολουθεί σκοτώνεται ακόμα ένας. Οι υπόλοιποι 5 τελικά καταφέρνουν να μοιραστούν εξίσου τις μπάρες χρυσού. Να βρεθεί το ελάχιστο πλήθος μπαρών χρυσού που είχαν οι ληστές.

Απάντηση

Έφτιαξα ένα πρόγραμμα σε Python όπου υλοποιεί το CRT χρησιμοποιώντας τον αλγόριθμο του Ευκλείδη για την εύρεση του πολλαπλασιαστικού αντιστρόφου ενός ακεραίου. Με εκτέλεση του προγράμματος με τις παραμέτρους του προβλήματος του ζητήματος βρίσκεται η λύση η οποία είναι 20. Ο κώδικας του προγράμματος:

```
def crt(n, a):
    N = reduce(lambda a, b: a * b, n)
    sum = 0
    for n_i, a_i in zip(n, a):
        N_i = N  / n_i
        sum += a_i * mulinv(N_i, n_i) * N_i

    return sum % N

#Modular multiplicative inverse
# returns x where (a * x) % b == 1
def mulinv(b, n):
    g, x, y = egcd(b, n)
    if g == 1:
        return x % n

#O epektetamenos Algorithmos toy Eukleidi
```

```python
# return (g, x, y) a*x + b*y = gcd(x, y)
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, x, y = egcd(b % a, a)
        return (g, y - (b // a) * x, x)


if __name__ == '__main__':
    n = [ 6, 7]
    a = [ 2, 6]
    print crt(n, a)
```

Ζήτημα 5 (1 μονάδα) Βρείτε τα αποτελέσματα των πράξεων 7^{345} mod 15, 48^{322} mod 25 και 2^{69} mod 71.

Απάντηση

- 7^{345} mod 15
  Το $7 \in \mathbb{Z}^*{}_{15}$ άρα με το θεώρημα του Euler έχω: φ(15)=8 άρα $7^8 \equiv 1 \text{mod} 15$
  Συνεπώς το $7^{345} \equiv 7^{8\times 48+1} \equiv (7^8)^{48} \times 7^1 \equiv 1^{48} \times 7^1 \equiv 7 \equiv 7 \text{mod} 15$

- 48^{322} mod 25
  Το $48 \notin \mathbb{Z}^*{}_{25}$ άρα το μετατρέπω σε $2^{322}\times 24^{322}$ όπου τα 2, $24 \in \mathbb{Z}^*{}_{25}$ και με το θεώρημα του Euler έχω: φ(25)=20 άρα $2^{20} \equiv 1 \text{mod} 25 \equiv 24^{20}$
  Συνεπώς το $48^{345} \equiv 48^{20\times 16+2} \equiv 2^{20\times 16+2} \times 24^{20\times 16+2} \equiv (2^{20})^{16} \times 2^2 \times (24^{20})^{16} \times 24^2 \equiv 1^{16} \times 2^2 \times 1^{16} \times 24^2 \equiv 2304 \equiv 4 \text{mod} 25$

- 2^{69} mod 71
  $2^{69} = 2^{70} \times 2^{-1}$. Απο το μικρό θεώρημα του Fermat ξέρω πως $2^{70} \equiv 1 \text{mod} 71$.
  Άρα $2^{69} \text{mod} 71 \equiv 2^{-1} \text{mod} 71 \equiv \frac{1}{2} \text{mod} 71$

Ζήτημα 6 (1 μονάδα) Βρείτε την τάξη των ακεραίων 9 και 13 στο $\mathbb{Z}^*{}_{34}$. Είναι κάποιος από τους αριθμούς αυτούς γεννήτορας του $\mathbb{Z}^*{}_{34}$? Αν όχι, μπορείτε να βρείτε έναν γεννήτορα της ομάδας?

Απάντηση
Τα στοιχεία 7, $9 \in \mathbb{Z}^*{}_{34}$ άρα η τάξη τους είναι ίση με $\varphi(34) = 16$ και συνεπώς είναι και τα δύο γεννήτορες του $\mathbb{Z}^*{}_{34}$

Ζήτημα 7 (1 μονάδα). Αποδείξτε ότι 9^{1980} - $7^{1980} \equiv 0 \text{mod} 130$.

Απάντηση
Τα 7, 9 είναι γεννήτορες του $\mathbb{Z}^*{}_{130}$ και τάξη τους είναι $\varphi(130) = 48$.
Άρα 9^{1980} - $7^{1980} \equiv 1 \text{mod} 130$ - $1 \text{mod} 130 \equiv 0 \text{mod} 130$