ΤΗΛ 511: Θεωρία Αριθμών και Κρυπτογραφία
Εαρινό Εξάμηνο 2024
Σχολή Ηλεκτρολόγων Μηχ/κών και Μηχ/κών Υπολογιστών
Πολυτεχνείο Κρήτης

Εργασία 2

Τετάρτη 19/6/2024 (updated)

Διδάσκων: Γεώργιος Καρυστινός

1. Problem 5.4.2 from the book.

2. Problem 6.12.6 from the book.

3. Problem 6.12.7 from the book.

4. Έστω η ομάδα $\langle \mathbb{Z}_n; * \rangle$, με $n > 0$ και $a * b = r_n[a + b]$. Θεωρούμε ένα $a \in \mathbb{Z}_n$ και το σύνολο $G = \{a^n : \ n \in \mathbb{Z}\}$, όπου $a^0 = 0$, για $n > 0$ έχουμε $a^n = \underbrace{a * a * \ldots * a}_{n}$ και $a^{-n} = (a^{-1})^n$, και a^{-1} είναι το αντίθετο στοιχείο του a.

   (α′) Δείξτε ότι το $\langle G; * \rangle$ είναι αντιμεταθετική ομάδα.

   (β′) Δείξτε ότι $G = \mathbb{Z}_n$ αν και μόνο αν $(a, n) = 1$.

5. Έστω το σύνολο $S = \{0, 1, 2, 3\}$ με πράξεις "$+$" και "$\cdot$" ορισμένες ως εξής. Η πράξη "$+$" ορίζεται ως κανονική πρόσθεση modulo 4. Για την πράξη "$\cdot$", ισχύουν τα εξής.
   (α) $0 \cdot a = 0$, για κάθε $a \in S$.
   (β) $1 \cdot a = a$, για κάθε $a \in S$.
   (γ) $2 \cdot 2 = 3$, $3 \cdot 3 = 2$, $2 \cdot 3 = 1$.
   (δ) $a \cdot b = b \cdot a$, για κάθε $a, b \in S$.
   Είναι σώμα το $<S, +, \cdot>$ και γιατί;

6. α) Για το σώμα $\mathbb{Z}_7$, γράψτε τον πίνακα αληθείας της πρόσθεσης και του πολλαπλασιασμού.
   β) Στην ακέραια περιοχή $\mathbb{Z}_7[x]$, διαιρέστε το $4+6x+2x^2+5x^3+x^4$ με το $1+2x+3x^2$ και βρείτε το πηλίκο και το υπόλοιπο. Εξηγήστε σε ποιο σημείο της διαίρεσης απαιτείται να είναι σώμα ο αρχικός δακτύλιος $\mathbb{Z}_7$.

7. Δείξτε ότι το πολυώνυμο $1 + x^3 + x^5 \in \mathbb{Z}_2[x]$ είναι ανάγωγο στο $\mathbb{Z}_2[x]$.

8. α) Για το σώμα $\mathbb{Z}_3$, γράψτε τον πίνακα αληθείας της πρόσθεσης και του πολλαπλασιασμού.
   β) Δείξτε ότι το πολυώνυμο $1 + x^2 \in \mathbb{Z}_3[x]$ είναι ανάγωγο στο $\mathbb{Z}_3[x]$.
   γ) Κατασκευάστε ένα σώμα με 9 στοιχεία χρησιμοποιώντας το ανάγωγο πολυώνυμο $1 + x^2 \in \mathbb{Z}_3[x]$.

9. Υλοποιήστε τη συνάρτηση `[g,s,t]=ext_euc_alg_int(a,b)` που επιτελεί τον Ευκλείδειο Αλγόριθμο στους ακεραίους `a` και `b`. Η έξοδος `g` είναι το `(a,b)` και οι συντελεστές `s` και `t` είναι τ.ώ. `a*s+b*t=g`.

10. Υλοποιήστε τις παρακάτω συναρτήσεις.
    `z=sumZp(x,y,p)` που υπολογίζει το `x+y` στο $\mathbb{Z}_p$,

z=difZp(x,y,p) που υπολογίζει το x-y στο $\mathbb{Z}_p$,
z=oppZp(x,p) που υπολογίζει το -x στο $\mathbb{Z}_p$,
z=mulZp(x,y,p) που υπολογίζει το x*y στο $\mathbb{Z}_p$,
z=convZp(x,y,p) που υπολογίζει τη συνέλιξη των x και y στο $\mathbb{Z}_p$,
z=invZp(x,p) που υπολογίζει το αντίστροφο του x στο $\mathbb{Z}_p$,
z=divZp(x,y,p) που υπολογίζει το x/y στο $\mathbb{Z}_p$.
Σε όλες τις περιπτώσεις, το p είναι πρώτος και τα x και y είναι διανύσματα ίδιου μήκους (εκτός από τις συναρτήσεις mulZp και divZp όπου το y είναι βαθμωτό και τη συνάρτηση invZp όπου το x είναι βαθμωτό). Τα στοιχεία των x και y ανήκουν στο $\mathbb{Z}_p$.

11. Υλοποιήστε τη συνάρτηση [c,d]=mydeconv(a,b,p) η οποία διαιρεί το πολυώνυμο $a(x)$ με το πολυώνυμο $b(x)$. Η είσοδος της συνάρτησης θα είναι τα διανύσματα a και b που αποτελούνται από τους συντελεστές των πολωνύμων $a(x)$ και $b(x)$, αντίστοιχα, και ο ακέραιος p. Η έξοδος της συνάρτησης θα είναι τα διανύσματα c και d που αποτελούνται από τους συντελεστές των πολωνύμων $c(x)$ και $d(x)$ τα οποία αποτελούν το πηλίκο και το υπόλοιπο, αντίστοιχα, της διαίρεσης.

    Επίσης, υλοποιήστε τη συνάρτηση [g,s,t]=ext_euc_alg_poly(a,b,p) που επιτελεί τον Ευκλείδειο Αλγόριθμο στα πολυώνυμα $a(x)$ και $b(x)$. Η είσοδος της συνάρτησης θα είναι τα διανύσματα a και b που αποτελούνται από τους συντελεστές των πολωνύμων $a(x)$ και $b(x)$, αντίστοιχα, και ο ακέραιος p. Η έξοδος της συνάρτησης θα είναι τα διανύσματα g, s, και t που αποτελούνται από τους συντελεστές των πολωνύμων $g(x)$, $s(x)$, και $t(x)$, αντίστοιχα, τ.ώ. $a(x)s(x) + b(x)t(x) = g(x)$ όπου $g(x) = (a(x), b(x))$. Σημειώστε ότι τα $g(x)$, $s(x)$, και $t(x)$ θα πρέπει να είναι κανονικοποιημένα ώστε το $g(x)$ να είναι μονικό.

    Αν το p είναι πρώτος, τότε όλα τα πολυώνυμα και όλες οι πράξεις είναι στην ακέραια περιοχή $\mathbb{Z}_p[x]$. Διαφορετικά, το p θα πρέπει να είναι μηδέν και σε αυτήν την περίπτωση όλα τα πολυώνυμα και όλες οι πράξεις είναι στην ακέραια περιοχή $\mathbb{R}[x]$.