Matematyka Dyskretna — Lista zadań 3

M. Michalski, 31.03.2021

Wielomiany nierozkładalne nad $\mathbb{Z}_2$

st. 1: $X, \quad X+1$

st. 2: X^2+X+1

st. 3: $X^3+X+1, \quad X^3+X^2+1$

st. 4: $X^4+X+1, \quad X^4+X^3+1, \quad X^4+X^3+X^2+X+1$

Wielomiany nierozkładalne nad $\mathbb{Z}_3$

st. 1: $X, \quad X+1, \quad X+2$

st. 2: $X^2+1, \quad X^2+X+2, \quad X^2+2X+2$

st. 3: $X^3+2X+1, \quad X^3+2X+2, \quad X^3+X^2+2, \quad X^3+X^2+X+2, \quad X^3+X^2+2X+1, \quad X^3+2X^2+1,$
$X^3+2X^2+X+1, \quad X^3+2X^2+2X+2$

1. Przedstaw następujące wielomiany w postaci iloczynu wielomianów nierozkładalnych:

a) Nad $\mathbb{F}_2$: $f(X)=X^4+X^2+X+1, \quad f(X)=X^5+X^3+X^2+X, \quad f(X)=X^{10}-X,$
$f(X)=X^5+X^2+X+1, \quad f(X)=X^7+1, \quad f(X)=X^7+X^4+X^2+X+1$

b) Nad $\mathbb{F}_3$: $f(X)=X^9-X, \quad f(X)=X^8+X^7+2X^6+X^2+X+2$

2. Wyznacz tabelki działań w następujących pierścieniach wielomianów. Które z tych pierścieni są ciałami?

(a) $\mathbb{F}_3[X]/(X^2+1)$
(b) $\mathbb{Z}_4[X]/(X^2+1)$
(c) $\mathbb{F}_2[X]/(X^2+1)$
(d) $\mathbb{F}_2[X]/(X^2+X+1)$
(e) $\mathbb{F}_2[X]/(X^3+X+1)$
(f) $\mathbb{F}_3[X]/(X^2+X+1)$
(g) $\mathbb{Z}_6[X]/(X^2-1)$

3. Napisz program w języku C, który realizuje funkcje wielomianowego kalkulatora. Pierwszym parametrem, o który prosi program jest podstawa modularna p. Gdy $p=0$, program operuje na wielomianach w $\mathbb{Z}[X]$, a w przeciwnym razie w $\mathbb{Z}_p[X]$. Wielomiany reprezentowane są jako tablice `int u[n]`, które przechowują ich współczynniki

$$u(X) \;=\; \texttt{u[n]}\,X^n \;+\; \texttt{u[n-1]}\,X^{n-1} \;+\; \cdots \;+\; \texttt{u[1]}\,X \;+\; \texttt{u[0]}\,.$$

Dodatkowo z każdym wielomianem związana jest zmienna `int su`, która przechowuje aktualny stopień wielomianu `u`, to jest $\max\{\texttt{k} \le \texttt{n} :\ \texttt{u[k]} \neq \texttt{0}\}$.

Kalkulator operuje rejestrem głównym — wielomianem `int w[n]`, w którym przechowywany jest wynik ostatnio wykonanej operacji. Program działa w pętli, prosząc użytkownika o podanie następnej operacji do wykonania na rejestrze:

— 0: zeruj rejestr
— 1: dodaj do rejestru
— 2: odejmij od rejestru
— 3: pomnóż rejestr
— 4: podziel rejestr (działanie to może być niewykonalne, gdy p nie jest liczbą pierwszą)
— 5: reszta z dzielenia rejestru (jak wyżej)
— 6: zapisz rejestr w pamięci `int a[n], b[n]` lub `c[n]`
— 7: odtwórz wartość rejestru z pamięci jak wyżej.

Np. operacja "pomnóż rejestr" prosi o podanie stopnia i współczynników wielomianu, przez który należy rejestr pomnożyć, przechowując je odp. w roboczej zmiennej `su` i tablicy `u[n]`, a następnie wywołuje funkcję mnożenia `c_mul(w, u, &sw, su, p)`. Wynik mnożenia, zredukowany (mod p) jeśli $p \neq 0$, trafia do rejestru `w`, a jego stopień `sw` podlega odpowiedniej aktualizacji. Funkcja ta ma przykładowo postać:

```
void c_mul(int r[], int s[], int *sr, int ss, int p){
int i, j, mx, st=*sr+ss;
int t[n];
   for (i=0; i<=st; ++i){ t[i]=0; }
   for (i=0; i<=*sr; ++i){
      for (j=0; j<=ss; ++j){ t[i+j]=t[i+j]+r[i]*s[j]; }
   }
   if (p!=0){
      mx=0;
      for (i=0; i<=st; ++i){
         r[i]=t[i]%p;
         if (r[i]!=0) {
            mx=i;
            if (r[i]<0) { r[i]+=p; }
         }
      }
      *sr=mx;
   }
   else {
      for (i=0; i<=st; ++i){
         r[i]=t[i];
      }
      *sr=st;
   }
}
```