Laboratorium ochrony danych

Ćwiczenie nr 1

Temat ćwiczenia: Ciała skończone proste

Cel dydaktyczny: Poznanie metod generowania ciał skończonych prostych oraz zasad rachowania w tych systemach algebraicznych, badanie właściwości ciał i wielomianów nad ciałami.

Wprowadzenie teoretyczne

W kryptografii oraz w technice kodowania stosuje się alfabety o skończonej liczbie elementów. Z reguły liczba elementów stosowanego alfabetu równa jest albo liczbie pierwszej, albo potędze liczby pierwszej. Dzięki temu zastosowany alfabet można uważać za strukturę algebraiczną, która nazywa się ciałem skończonym lub inaczej ciałem Galois.

Ciało skończone *GF*(*p*) jest to system algebraiczny, złożony ze zbioru liczb A={0,1,...,*p*-1} oraz z operacji dodawania i mnożenia modulo *p*, które można wykonywać na tych liczbach. Taki system spełnia wszystkie aksjomaty ciał, tzn.:

- zbiór {0,1,...,*p*-1} wraz z operacją dodawania modulo *p* jest przemienną grupą addytywną, z elementem neutralnym 0,
- zbiór {0,1,...,*p*-1} wraz z operacją mnożenia modulo *p* jest przemienną grupą multyplikatywną, z elementem neutralnym 1,
- mnożenie jest rozdzielne względem dodawania, czyli dla każdego *a*, *b* i *c* należących do {0,1,..., *p*-1} spełniona jest zależnośc $\forall a,b,c \in A \quad a \cdot (b+c) = (b+c) \cdot a = a \cdot b + a \cdot c$.

Skończone ciała proste można skonstruować dla zbiorów liczbowych o liczbie elementów równej liczbie pierwszej *p*. Ciała takie oznaczamy symbolem $GF(p)$. Elementami ciała prostego są liczby: 0, 1, 2, ..., $p-1$. Działania w ciałach prostych są takie same jak działania arytmetyczne z operacją modulo *p*. Ciało proste jest więc ciałem reszt modulo *p*. Sumę *S* i iloczyn *P* dwóch elementów ciała prostego *a* i *b* określają zależności:

$$S \equiv a + b \pmod{p},$$

$$P \equiv a \cdot b \pmod{p}.$$

W *GF*(*p*) każdy element ma element do siebie przeciwny, a każdy element niezerowy ma multyplikatywną odwrotność, dzięki czemu w ciele *p*-elementowym można też odejmować, dzielić, potęgować i wyciągać pierwiastki. Wobec tego nad ciałem *GF*(*p*) mają sens takie obliczenia, jak rozwiązywanie rownań liniowych i nieliniowych, dodawanie, mnożenie i odwracanie macierzy, wszystkie operacje na wielomianach, itp.

Element przeciwny ciała obliczamy za pomocą aksjomatu

$$\forall a \in A \quad \exists b \in A \quad a + b = b + a = 0,$$

a element odwrotny ciała obliczamy za pomocą aksjomatu

$$\forall a \in A \quad \exists b \in A \quad a \cdot b = b \cdot a = 1.$$

Jako przykład wieloelementowego skończonego ciała prostego przyjmijmy ciało $GF(7)$. Elementami ciała $GF(7)$ są liczby: 0, 1, 2, 3, 4, 5, 6.

Tabliczki dodawania i mnożenia ciała $GF(7)$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Do badania ciał skończonych używa się funkcji Eulera. Funkcja Eulera $\varphi(n)$ określa liczbę liczb naturalnych w zbiorze {1, 2, ..., *n*–1} względnie pierwszych z *n*. Na przykład $\varphi(8)=4,$ gdyż w zbiorze liczb mniejszych od 8 tylko 1, 3, 5 i 7 są względnie pierwsze z 8. Liczby względnie pierwsze nie mają żadnego wspólnego podzielnika oprócz 1. Funkcja Eulera dla liczby pierwszej *p* jest równa $p-1$, gdyż wszystkie liczby mniejsze od *p* są względnie pierwsze z *p*.

Aby znaleźć wartość funkcji Eulera liczby złożonej *n*, rozkładamy ją na iloczyn potęg liczb pierwszych

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_m^{e_m}.$$

Wartość funkcji Eulera dla takiej liczby złożonej wylicza się ze wzoru

$$\varphi(n) = \prod_{i=1}^{m} p_i^{e_i-1}(p_i - 1).$$

P r z y k ł a d .
Obliczenie funkcji Eulera liczby złożonej.
$n = 2646 = 2 \cdot 3^3 \cdot 7^2$, $\varphi(2646) = 1 \cdot 3^2 \cdot 2 \cdot 7 \cdot 6 = 756.$

Niezerowe elementy ciała charakteryzuje rząd multyplikatywny. *Rzędem multyplikatywnym* dowolnego elementu ciała *a* jest najmniejsza liczba całkowita *e* taka, że

$$a^e = 1.$$

Na przykład rzędem multyplikatywnym elementu 5 ciała $GF(7)$ jest 6, ponieważ $5^6 = 1 \pmod 7$. Rząd mutyplikatywny elementu ciała $GF(p)$ jest dzielnikiem $p-1$.
Elementy ciała $GF(7)$ mają następujące rzędy multyplikatywne:
element 1 – rząd multyplikatywny 1,
elementy 2 i 4 – rząd multyplikatywny 3,
elementy 3 i 5 – rząd multyplikatywny 6,
element 6 – rząd multyplikatywny 2.
Elementy ciała $GF(p)$ mające rząd multyplikatywny równy $p-1$ nazywamy *elementami pierwotnymi* ciała. Liczbę elementów pierwotnych *n* ciała $GF(p)$ można określić z zależności

$$n = \varphi(p-1),$$

gdzie φ jest funkcją Eulera.

Każdy element niezerowy ciała generuje grupę cykliczną. Element pierwotny ciała generuje grupę multyplikatywną ciała. W tak utworzonej grupie będą wszystkie niezerowe elementy ciała. Elementy grupy multyplikatywnej o rzędzie multyplikatywnym większym od 1 i mniejszym od $p-1$ generują podgrupy multyplikatywne. Taka podgrupa zachowuje działania grupy.

Grupę cykliczną generowaną przez dowolny element ciała skończonego otrzymamy, biorąc kolejne potęgi tego elementu. Na przykkład element 5 ciała $GF(7)$ generuje grupę multyplikatywną: 5, 4, 6, 2, 3, 1, gdyż kolejne potęgi elementu 5 wynoszą: 5, $5\cdot5=4$, $4\cdot5=6$, $6\cdot5=2$, $2\cdot5=3$, $3\cdot5=1$. Podobnie element 2 generuje podgrupę trzyelementową: 2, 4, 1.

W teorii kodowania są szeroko wykorzystywane wielomiany nad ciałami skończonymi. Wielomian stopnia *m* nad ciałem *GF*(*q*) ma ogólną postać

$$p(x) = x^m + a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_1 x + a_0 \quad \text{nad } GF(q).$$

Przyrównując ten wielomian do zera, otrzymamy

$$x^m = -a_{m-1}x^{m-1} - a_{m-2}x^{m-2} - \ldots - a_1 x - a_0.$$

Zależność rekurencyjna stowarzyszona z tym wielomianem będzie

$$s_{j+m} = -a_{m-1}s_{j+m-1} - a_{m-2}s_{j+m-2} - \ldots - a_1 s_{j+1} - a_0 s_j, \; j = 0,1,2,3,\ldots$$

Działania należy tu wykonywać zgodnie z zasadami rachowania w ciele $GF(q)$. Gdy założymy ciąg początkowy o długości *m* elementów: $s_0, s_1, s_2, \ldots, s_{m-1}$, wówczas dla kolejnych wartości j można obliczyć z powyższej zależności elementy sekwencji okresowej. Okres wygenerowanej sekwencji okresowej zależy od typu wielomianu. W przypadku wielomianów pierwotnych sekwencja osiąga okres maksymalny. Okres maksymalny *M* dla wielomianu stopnia *m* nad ciałem $GF(q)$ wynosi

$$M = q^m - 1.$$

Wielomiany niepierwotne generują sekwencje o okresie mniejszym od *M*.

Niech wielomianem generującym sekwencję okresową będzie wielomian stopnia trzeciego nad ciałem $GF(2)$

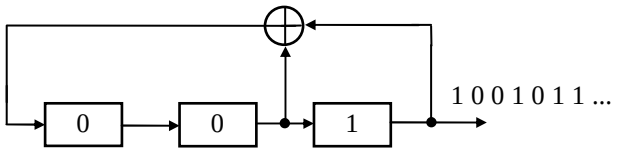
$$x^3 + x + 1 = 0.$$

Zależność rekurencyjna stowarzyszona z tym wielomianem ma postać

$$s_{j+3} = s_j + s_{j+1}, \qquad j = 0,1,2,3,\ldots$$

a wygenerowana sekwencja będzie: 1001011 1001011 ... .

Realizację zależności rekurencyjnej za pomocą układów logicznych pokazano na rysunku.



Generator binarnej sekwencji okresowej

Przebieg ćwiczenia

1. Wygenerować tabliczkę mnożenia i dodawania ciała *GF*(*p*), gdzie $p \leq 19$.
2. Wyznaczyć elementy przeciwne do elementów ciała *GF*(*p*), dla $p \leq 19$.
3. Wyznaczyć elementy odwrotne niezerowych elementów ciała *GF*(*p*), dla $p \leq 19$.
4. Wyznaczyć rząd multyplikatywny elementów ciała *GF*(*p*), dla $p \leq 19$.
5. Znaleźć elementy pierwotne ciała *GF*(*p*), dla $p \leq 19$.
6. Wygenerować sekwencję okresową dla wielomianu nad ciałem *GF*(*p*). Wykorzystać zależność rekurencyjną stowarzyszoną z wielomianem. Przetestować działanie programu dla wielomianów stopnia m (stopień dowolny – ograniczenie w postaci stałej w programie) o współczynnikach $a_0, a_1, a_2, \ldots, a_{m-1}$ i sekwencji początkowej $s_0, s_1, s_2, \ldots, s_{m-1}$ zadawanych przez użytkownika (np. wykonać testy dla wielomianów postaci $x^4 + x + 1$ nad *GF*(2) oraz $x^2 + x + 2$ nad *GF*(3).

Zadania rozwiązać w dowolnym języku programowania.