Лекція 18. Скінченні поля.

Побудова скінченних полів

Поле, яке має скінченну кількість елементів, називають скінченним полем або полем Галуа. Наведена далі теорема дає повний опис (ізоморфну класифікацію) скінченних полів.

Теорема 7. (a) Будь-яке скінченне поле має p^n елементів, де p – просте число, а n – натуральне число.
(b) Для фіксованих простого числа p та натурального числа n існує (і, з точністю до ізоморфізму, лише одне) поле, яке має p^n елементів.

Теорема 7 є екзистенціальною теоремою, тобто теоремою про існування скінченних полів. Така теорема не дає ніяких вказівок про те, як збудувати скінченне поле з потрібною кількістю елементів. Тому далі описуємо, як отримати бажане поле. Скінченні поля з точністю до ізоморфізму будують наступним чином.

Скінченне поле з p елементів ізоморфне кільцю $\mathbf{Z}_p$ цілих чисел за модулем простого числа p.

Скінченне поле з p^n елементів отримуємо таким чином. Розглядаємо кільце многочленів $\mathbf{Z}_p[x]$ від однієї змінної x над полем $\mathbf{Z}_p$. Беремо в цьому кільці многочлен $f(x)$ степеня n, який є нерозкладним над $\mathbf{Z}_p$. Зауважимо, що для будь-яких простого числа p та натурального числа n принаймні один такий нерозкладний многочлен існує. Позначимо через $(f(x))$ ідеал, який складається з елементів, що діляться на $f(x)$. Тоді фактор-кільце $\mathbf{Z}_p[x]/(f(x))$ є бажаним полем, яке має p^n елементів. Виконання операцій над елементами цього поля здійснюється за двома модулями: за модулем числа p і за модулем многочлена $f(x)$. Часто це позначається наступним чином: $(mod\ f(x),\ p)$.

Далі деталізовано опис скінченного поля $GF(2^8)$.

Хоча з точністю до ізоморфізму є лише одне скінченне поле $GF(2^8)$ із $2^8 = 256$ елементів, проте його елементи можна зображати по-різному. Відображення елементів впливає на складність реалізації. У стандарті, який розглядаємо, використано таке загальноприйняте відображення. Байт із бітами $a_7a_6a_5a_4a_3a_2a_1a_0$ розглядають як поліном від деякої формальної змінної x із коефіцієнтами з множини $\{0,1\}$:

$$a(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0.$$

Наприклад, байтові з шістнадцятковим значенням 5A (двійковим значенням 01011010) відповідає многочлен

$$0\cdot x^7 + 1\cdot x^6 + 0\cdot x^5 + 1\cdot x^4 + 1\cdot x^3 + 0\cdot x^2 + 1\cdot x + 0 = x^6 + x^4 + x^3 + x\ .$$

Для елементів $a(x)$, $b(x)$ поля $GF(2^8)$ додавання задають так:

$$c(x) = a(x) + b(x) = c_7x^7 + c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0.$$

де $c_i = a_i \oplus b_i$, $i = 0, 1, \ldots, 7$. Тобто сума двох поліномів – це поліном, коефіцієнти якого дорівнюють сумі за модулем 2 відповідних коефіцієнтів доданків.

Отже, додавання двох байтів виконується побітово. Наприклад, B1 + 8F = 3E. У двійковій формі це виглядає так:

$$\begin{array}{r} 1011\ 0001 \\ \underline{1000\ 1111} \\ 0011\ 1110, \end{array}$$

а у вигляді многочленів -

$$(x^7 + x^5 + x^4 + 1) + (x^7 + x^3 + x^2 + x + 1) = x^5 + x^4 + x^3 + x^2 + x.$$

Множина означених поліномів із операцією додавання утворює абелеву групу.

Щоб задати множення в полі $GF(2^8)$, треба зафіксувати якийсь нерозкладний многочлен степеня 8 з коефіцієнтами із поля $\mathbf{Z}_2=\{0,1\}$, яке має 2 елементи. Нерозкладність многочлена означає, що аналогічно до випадку цілих чисел, він ділиться лише сам на себе й на одиницю. Таких многочленів степеня 8 є декілька. Один із многочленів, який вважають стандартним, виглядає так:

$$f(x) = x^8 + x^4 + x^3 + x + 1.$$

Його шістнадцяткове значення дорівнює 11B.

Два елементи поля $GF(2^8)$ множать за модулем многочлена $f(x)$. Це означає таке. Спочатку два многочлени множать як звичайні многочлени (додавання добутків коефіцієнтів виконується за модулем 2). Потім отриманий проміжний результат зводять за модулем многочлена $f(x)$. Для цього його ділять на $f(x)$ і як остаточний результат беруть залишок від ділення – поліном, степінь якого не перевищує 7.

Відомий алгоритм (так званий розширений алгоритм Евкліда), який для будь-яких многочленів $a(x)$, $b(x)$ без нетривіального спільного дільника дає змогу знайти такі многочлени $u(x)$, $v(x)$, що виконується рівність

$$a(x) \cdot u(x) + b(x) \cdot v(x) = 1.$$

Зокрема, приймемо $b(x) = f(x)$ та візьмемо як $a(x)$ довільний многочлен степеня не вище 7. Оскільки поліном $f(x)$ – нерозкладний, то поліноми $f(x)$ та $a(x)$ не мають відмінного від одиниці спільного дільника. Тоді знайдуться такі многочлени $u(x)$, $v(x)$, що

$$a(x) \cdot u(x) + f(x) \cdot v(x) = 1.$$

Отже, $a(x) \cdot u(x) = 1 \bmod f(x)$. Тобто елемент $a(x)$ має обернений елемент щодо означеної операції множення:

$$a^{-1}(x) = u(x) \bmod f(x).$$

Множина із 256 можливих многочленів з коефіцієнтами 0, 1 із означеними операціями додавання й множення утворює скінченне поле.

Як приклад, розглянемо множення в полі $GF(2^8)$: 74·B2 = E3. Для цього звичним способом множимо відповідні поліноми, виконуючи водночас додавання за модулем 2. Отримуємо

$$(x^6 + x^5 + x^4 + x^2) \cdot (x^7 + x^5 + x^4 + x) = x^{13} + x^{11} + x^{10} + x^7 + x^{12} + x^{10} + x^9 + x^6 + x^{11} + x^9 + x^8 + x^5 + x^9 + x^7 + x^6 + x^3 = x^{13} + x^{12} + x^9 + x^8 + x^5 + x^3.$$

Тепер зводимо отриманий поліном за модулем $f(x)$:

$$\begin{array}{ll} x^{13} + x^{12} + x^9 + x^8 + x^5 + x^3 & \mid \underline{x^8 + x^4 + x^3 + x + 1} \\ \underline{x^{13} + x^9 + x^8 + x^6 + x^5} & \mid x^5 + x^4 + 1 \\ x^{12} + x^6 + x^3 & \\ \underline{x^{12} + x^8 + x^7 + x^5 + x^4} & \\ x^8 + x^7 + x^6 + x^5 + x^4 + x^3 & \\ \underline{x^8 + x^4 + x^3 + x + 1} & \\ x^7 + x^6 + x^5 + x + 1. & \end{array}$$

Звідси

$$(x^{13} + x^{12} + x^9 + x^8 + x^5 + x^3) \bmod (x^8 + x^4 + x^3 + x + 1) = x^7 + x^6 + x^5 + x + 1.$$

У разі множення многочлена $a(x)$ на x на першому кроці маємо

$$a_7x^8 + a_6x^7 + a_5x^6 + a_4x^5 + a_3x^4 + a_2x^3 + a_1x^2 + a_0x.$$

Далі отриманий поліном треба звести за модулем $f(x)$. Якщо $a_7 = 0$, то нічого робити не треба. Якщо ж $a_7 = 1$, то ділення отриманого многочлена на $f(x)$ рівносильне додаванню до нього многочлена f (x). Звідси випливає, що множення на x (у шістнадцятковій системі на 02) у байтовому відображенні виглядає як зсув байта ліворуч на один розряд з можливим побітовим додаванням за модулем 2 отриманого байта з байтом 1B. У цьому разі множення на вищі степені x виконуємо послідовним застосуванням операції множення на x.

Наприклад, обчислимо значення $96 \cdot AB$:

$$96 \cdot 02 = 37;$$
$$96 \cdot 04 = 37 \cdot 02 = 6E;$$
$$96 \cdot 08 = 6E \cdot 02 = DC;$$
$$96 \cdot 10 = DC \cdot 02 = A3;$$
$$96 \cdot 20 = A3 \cdot 02 = 5D;$$
$$96 \cdot 40 = 5D \cdot 02 = BA;$$
$$96 \cdot 80 = BA \cdot 02 = 6F.$$

У результаті отримуємо

$$96 \cdot AB = 96 \cdot (01 \oplus 02 \oplus 08 \oplus 20 \oplus 80) = 96 \oplus 37 \oplus DC \oplus 5D \oplus 6F = 4F.$$