L04. Вычисления в конечных полях и кольцах

Для факторизации полиномов $f(x) \in Z_p[x]$ над конечными полями Z_p нам потребуется знакомство с техникой вычислений в фактор-кольцах полиномиальных колец.

Пусть задан полином

$$f(x) = \sum_{i=0}^{n} a_i x^i \in Z_p[x], \quad a_n = 1,$$

будем обозначать

$$Z_{p,f(x)}[x] = Z_p[x]/(f(x)Z_p[x])$$

фактор-кольцо $Z_p[x]$ по главному идеалу $(f(x))Z_p[x]$, порожденному полиномом $f(x)$.

□ Как известно, в том случае, когда f(x) не раскладывается на простые множители, $Z_{p,f(x)}[x]$ является полем характеристики p, которое содержит p^n элементов. Оно называется полем Галуа. Обозначается $\mathbf{F}_{p^k}$.

□ В 1893 году Элиаким Гастингс Мур доказал, что любое конечное поле изоморфно некоторому полю Галуа.

Eliakim Hastings Moore, 26.01.1862-30.12.1932, заведовал кафедрой математики в чикагском университете, который расположен в городке Шампен-Урбана. Там же находится сегодня и Wolfram Inc., создатель Mathematica.

Так как фактор-кольцо –это кольцо, образованное классами смежности по некоторому идеалу, то принято операции в фактор-кольцах выполнять с помощью представителей классов смежности. Например, в качестве представителей элементов Z_7 можно взять числа 0,1,..,6. Важно, чтобы в этом моножестве было ровно по одному представителю из каждого класса смежности.

Естественно взять в качестве представителей кольца $Z_{p,f(x)}[x]$ множество полиномов из $Z_p[x]$, у которых степени не превосходят $n-1$. Тогда, для любого полинома процедура вычисления представителя его класса смежности сводится к нахождению остатка от деления на полином $f(x)$.

При вычислениях в фактор-кольце $Z_{p,f(x)}[x]$ используются его представители в $Z_p[x]$. И каждый раз результат вычислений «приводится к его представителю» путем вычисления остатка от деления на $f(x)$.

В случае разреженных полиномов, когда число мономов m полинома $g(x)$ значительно меньше его степени d, $m << d$, операция деления полиномов оказыватся достаточно дорогой. Она требует примерно $\sim dn$ операций вычитания и умножения в поле Z_p и еще некоторое число делений. Поэтому пользуются более дешевым способом, который требует mn операций сложения и умножения.

Пусть $g(x) = \sum_{i=0}^{d} b_i x^i \in Z_p[x]$. Вычислим для каждого монома x^i его образ (т.е. его представителя) в $Z_p[x]$ при гомоморфизме $Z_p[x] -> Z_{p,f(x)}[x]$: $x^i -> W_i(x) = \sum_{j=0}^{n-1} w_{i,j} x^j$.

Можно, например, просто найти для каждого i остаток от деления x^i на $f(x)$:

$$W_i(x) = \mathbf{remainder}(x^i, f(x)). \qquad (1)$$

Однако, более «экономно» сразу вычислить представителей всех мономов, начиная с младших, и сохранить их в некотором массиве.

Для всех $i = 1, 2, .., n-1$ очевидно получим: $x^i - - > W_i(x) = x^i$.

Для $i = n$ получим

$$x^n - > W_n(x) = x^n - f(x) = -\sum_{i=0}^{n-1} a_i x^i.$$

Для каждого $i > n$ и найдем

$$x^{k+1} - > W_{k+1}(x) = xW_k(x) = \sum_{j=0}^{n-1} w_{k,j} x^{j+1} = w_{k,n-1} W_n(x) + \sum_{j=0}^{n-2} w_{k,j} x^{j+1} \qquad (2)$$

Это требует только n операций умножения и столько же пераций сложения в Z_p.
Составим таблицу всех полиномов $W_k(x)$ для $k <= (n-1)p$ и сохраним.
Теперь вычисление представителя для полинома g можно выполнить так:

$$g(x) = \sum_{i=0}^{d} b_i x^i - > \sum_{i=0}^{d} b_i W_i(x). \qquad (3)$$

Если в полиноме $g(x)$ имеется m мономов, то потребуется nm операций умножения и столько же сложения. Отметим, что и для плотных полиномов число операций не превышает $n(d+1)$, где d - это степень полинома g.

ПРИМЕР.

Приготовим таблицу представителей для $x, x^2, .., x^{20}$ при $f = x^4 + 3x - 2$ по формуле (2):
$SPACE = Z[x];$
$n = 4; p = 7; N = 21; W = \mathbf{O}_N; W = (w_i);$
$i = 1; five = 5; one = 1;$
$out:$

1

По формуле (2) нам требуется выделить старший коэффициент $w_{k,n-1}$ и умножить его на полином $W_n(x)$.

Следовательно потребуется функция **leadingCoeff**(f) для выделения старшего коэффициента у полинома

и функция **degree**(f) для определения старшей степени у полинома.

Если **degree**$(W_k) < n-1$, то $w_{k,n-1} = 0$, а если **degree**$(W_k) = n-1$, то $w_{k,n-1} =$ **leadingCoeff**(W_k).
А для вычисления суммы $\sum_{j=0}^{n-2} w_{k,j} x^{j+1}$ мы вычислим xW_k и вычтем старший моном $lc * x^n$.

$SPACE = Zp32[x]; MOD32 = 7;$
$f = x^4 + 3x - 2; deg =$ **degree**(f); запомним степень полинома f, чтобы потом с ней сравнивать
$w_1 = x; w_2 = x^2; w_3 = x^3$; это первые искомы образы для степеней, меньше, чем deg
$D = x^4 - f; w_4 = D; T = D;$
$for(i = one; i < five; i = i+1)\{b = [i, w_i];$ **print**$(b); \}$ распечатаем их, включая и W_{deg}
$for(i = five; i \le N; i = i+1)\{$
  $if($**degree**$(T) == deg - 1)\{lc =$ **leadingCoeff**$(T); \} else\{\ lc = 0; \}$
  $T = lcD + xT - lcx^n;\ w_i = T;$
  $b = [i, T];$ **print**$(b);$
$\}$
COMMENT: $W_{k+1}(x) = w_{k,n-1} W_n(x) + \sum_{j=0}^{n-2} w_{k,j} x^{j+1}$ формула (2).

$out:$

$b = [1, x]$
$b = [2, x^2]$
$b = [3, x^3]$
$b = [4, -3x + 2]$
$b = [5, -3x^2 + 2x]$
$b = [6, -3x^3 + 2x^2]$
$b = [7, 2x^3 + 2x + 1]$
$b = [8, 2x^2 - 5x + 4]$
$b = [9, 2x^3 - 5x^2 + 4x]$
$b = [10, -5x^3 + 4x^2 + x + 4]$
$b = [11, 4x^3 + x^2 + 5x - 3]$
$b = [12, x^3 + 5x^2 - x + 1]$
$b = [13, 5x^3 - x^2 - 2x + 2]$
$b = [14, -x^3 - 2x^2 + x + 3]$
$b = [15, -2x^3 + x^2 - x - 2]$
$b = [16, x^3 - x^2 + 4x - 4]$
$b = [17, -x^3 + 4x^2 + 2]$
$b = [18, 4x^3 - 2x + 5]$
$b = [19, -2x^2 + 1]$
$b = [20, -2x^3 + x]$
$b = [21, x^2 - x - 4]$

Теперь можно отобразить любой полином, который имеет степень не больше 21.
Пусть например полином имеет мономы со степенью кратной 7. Запишем степени в вектор K:

$SPACE = Z[x];$
$K = \mathbf{O}_4; K = (k_i);$
$for(j = 1; j \leq n; j = j + 1)\{k_j = (j - 1) \cdot 7;\}$
$K;$
$out:$

$[0, 7, 14, 21]$

Соответствующие этим степеням полиномы W_u запишем в виде плотных векторов v_u из 4 компонент.

Для этого воспользуемся функцией $\mathbf{toVectorDence}(f, 4)$. Тут второй аргумент указывает, что необходимо получить в результате
вектор размера 4 или больше, но не меньше 4.

$V = \mathbf{O}_4; V = (v_i);$
$for(j = 2; j \leq n; j = j + 1)\{u = k_j; v_j = \mathbf{toVectorDence}(w_u, 4);\ \}$
$v_1 = [0, 0, 0, 1];\ V$
$out:$

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 2 & 0 & 2 & 1 \\ -1 & -2 & 1 & 3 \\ 0 & 1 & -1 & -4 \end{pmatrix}$$

Пусть имеется фиксированный разреженный полином с такими степенями.

$pol = 9x^{k_4} + 6x^{k_3} + 2x^{k_2} + 4x^{k_1};$

Составим плотный вектор из его коэффициентов.

Функция **toVectorSparce**(pol) возвращает вектор с четным числом компонент, в котором записаны все ненулевые коэффициенты,

а потом соответствующие степени. Нужно получиь только первую половину этого вектора.

$VEC = \mathbf{toVectorSparce}(pol); VEC = (vec_i);$
$L = \mathbf{O}_4; L = (l_i);$
$for(j = 1; j \leq n; j = j + 1)\{l_j = vec_j; \}$
$\mathbf{print}(pol, VEC, L)$
$out:$

$pol = 9x^{21} + 6x^{14} + 2x^7 + 4$
$VEC = [9, 6, 2, 4, 21, 14, 7, 0]$
$L = [9, 6, 2, 4]$

Теперь задача вычисления образа полинома pol сводится к умножению этого вектора L на матрицу M образов степенных полиномов:

$$pol -- > M * L.$$

Матрицу M надо составить так, чтобы ее столбцы были образованы в таком порядке:

$$M = [V_4, V_3, V_2, V_1].$$

Тогда первый коэффициент вектора L (полинома pol) будет умножаться на коэффициенты первого столбца V_4 , соответствующего W_{21},

второй – на коэффициенты втрого столбца V_3, соответствующего W_{14} и т.д. Построим эту матрицу.

$M = \mathbf{O}_{4,4}; M = (m_{i,j});$
$for(j = 1; j \leq n; j = j + 1)\{$
$\quad Z = v_{n+1-j}; Z = (z_i);$
$\quad for(i = 1; i \leq n; i = i + 1)\{m_{i,j} = z_i; \}\}M$
$out:$

$$\begin{pmatrix} 0 & -1 & 2 & 0 \\ 1 & -2 & 0 & 0 \\ -1 & 1 & 2 & 0 \\ -4 & 3 & 1 & 1 \end{pmatrix}$$

Теперь можно вычислить искомый образ полинома pol, путем умножения матрицы на вектор.

А потом сравнить результат с тем, который может быть получен путем вычисления остатка от деления

полинома pol на полином f в поле Z_p. Найдем для контроля их разность и получим нулевой вектор:

$SPACE = Zp32[x]; Lp = \mathbf{toNewRing}(L); pol_p = \mathbf{toNewRing}(pol);$
$Res = M \cdot\ Lp^T;$
$PRes = \mathbf{remainder}(pol_p, f);$
$Res2 = \mathbf{toVectorDence}(PRes);$
$Sub = Res2 - Res;\ \mathbf{print}(PRes, Res2, Res, Sub)$
$out:$

$PRes = 5x^3 - 3x^2 + x + 2$
$Res2 = [5, -3, 1, 2]$
$Res = [5, 4, 1, 2]$
$Sub = [0, 0, 0, 0]$
