L05. ФАКТОРИЗАЦИЯ ПОЛИНОМОВ ОДНОЙ ПЕРЕМЕННОЙ В КОНЕЧНОМ ПОЛЕ.

АЛГОРИТМ БЕРЛЕКАМПА.

Нам потребуется несколько фактов из теории чисел и теории конечных полей. Пусть p простое число и Z_p – конечное поле.

Т Е О Р Е М А 1. (О биномиальных коэффициентах.)

$$\binom{p}{k} = 0 \textbf{ mod } p \quad \forall\{k : 0 < k < p\}. \qquad (1)$$

Д О К А З А Т Е Л Ь С Т В О.

$$\binom{p}{k} = \frac{p(p-1)..(p-k+1)}{1..(k-1)k} = 0 \textbf{ mod } p,$$

так как p – простое число и $0 < k < p$.

Т Е О Р Е М А 2. (О биноме Ньютона в Z_p.)

$$(a+b)^p = a^p + b^p. \qquad (2)$$

Д О К А З А Т Е Л Ь С Т В О. Сводится к формуле бинома Ньютона и подстановке (1).

С Л Е Д С Т В И Е 1.

$$(a_1 + a_2 + .. + a_s)^p = a_1^p + a_1^p + .. + a_s^p. \qquad (3)$$

Д О К А З А Т Е Л Ь С Т В О.
$(a_1 + a_2 + .. + a_s)^p =$
$= ((a_1 + a_2 + .. + a_{s-1})^p + (a_s)^p = ((a_1 + a_2 + .. + a_{s-2})^p + a_{s-1}^p + a_s^p = .. = a_1^p + a_1^p + .. + a_s^p.$

Т Е О Р Е М А 3. (Малая теорема Ферма.)

$$\forall a \in Z_p : \quad a^p = a \qquad (5)$$

Д О К А З А Т Е Л Ь С Т В О.
Для p=0 утверждение очевидно. Пусть $b = a + 1$,тогда $b^p = (a+1)^p = a^p + 1^p = a + 1 = b$.

С Л Е Д С Т В И Е 2.

$$(\sum_{i=0}^{n} a_i x^i)^p = \sum_{i=0}^{n} a_i x^{pi}. \qquad (6)$$

Д О К А З А Т Е Л Ь С Т В О.
По Следствию 1 теоремы 2 получим $(\sum_{i=0}^{n} a_i x^i)^p = \sum_{i=0}^{n} a_i^p x^{pi}$.
По теореме Ферма получим $\sum_{i=0}^{n} a_i^p x^{pi} = \sum_{i=0}^{n} a_i x^{pi}$.

Т Е О Р Е М А 4. (Безу. Для Евклидовых колец полиномов).
Остаток от деления полинома $f(x)$ на двучлен $(x - a)$ равен $f(a)$.
Д О К А З А Т Е Л Ь С Т В О.
Можно разделить $f(x)$ на $(x - a)$ с остатком $r(x)$. Получим

$$f(x) = q(x)(x-a) + r(x).$$

Здесь $\textbf{degree}(r(x)) < \textbf{degree}(x - a) = 1$ и выполняется равенство $f(a) = r(a)$. Следовательно,

$r(x)$ - это постоянная и она равна $f(a)$.

С Л Е Д С Т В И Е 3.

Если a – корень полинома $f(x)$, то $f(x)$ делится на двучлен $x - a$.

Т Е О Р Е М А 5. (Лагранж. Основная теорема о разложении многочлена $x^p - x \in Z_p[x]$.)

$$x^p - x = x(x-1)(x-2)..(x-p+1).$$

Д О К А З А Т Е Л Ь С Т В О.

По теореме Ферма числа $0, 1, .., p-1$ являются корнями полинома $x^p - x$. По теореме Безу $x^p - x$ делится на $(x - a)$ $\forall a \in Z_p$.

Так как эти p двучленов не имеют общих делителей, то $x^p - x$ делится на их произведение $x(x-1)(x-2)..(x-p+1)$. Произведение – это полином степени p со сташим коэффициентом 1. Следовательно, при делении на него полинома $x^p - x$, получим в частном 1.

Т Е О Р Е М А 6. (Берлекампа)

[Elwyn R. Berlekamp. Factoring polynomials over finite fields. Bell System Technical J. V.46 (1967), 1853-1859.]

Пусть $f(x)$ и $\phi(x)$ – полиномы в кольце $Z_p[x]$ и пусть $\phi(x)$ удовлетворяет тождеству

$$\phi(x)^p - \phi(x) = 0 \ \mathbf{mod} \ f(x). \qquad (7)$$

тогда любой простой делитель $f(x)$ явлется делителем некоторого полинома $\phi(x) + \lambda$ $(\lambda \in Z_p)$.

Если $f(x) = \prod_{j=0}^{m} u_j$ – разложение на простые множители с с кратностью 1 полинома $f(x)$, то каждое решение (7) является решением системы из следующих m уравнений при некотором наборе чисел $\mu_i \in Z_p$

$$\phi(x) = \mu_i \ \mathbf{mod} \ u_i(x), \quad i = 1, 2, .., m, \qquad (8)$$

Наоборот, каждое решение системы (8) является решением (7).

Д О К А З А Т Е Л Ь С Т В О.

По условию найдется многочлен $q(x)$ такой, что

$$\phi(x)^p - \phi(x) = q(x)f(x)$$

а по теореме 5 отсюда следует равенство:

$$\phi(x)(\phi(x) - 1)(\phi(x) - 2)..(\phi(x) - p + 1) = q(x)f(x). \qquad (9)$$

Из этого равенства следует, что каждый простой делитель u_j полинома $f(x) = \prod_{j=0}^{m} u_j$ является делителем некоторого полинома вида $\phi(x) - \lambda$. Пусть $(\phi(x) - \mu_i)$ имеет делитель u_i, следовательно $\phi(x) = \mu_i \ \mathbf{mod} \ u_i$ и выполняется (8).

С другой стороны, пусть выполняется (8) при некотором наборе чисел μ_i. Если некоторые числа μ_i повторяются,например, $\mu_i = \mu_j$, то $(\phi(x) - \mu_i)$ делится на оба простых делителя u_i и u_j, поэтому он делится на их произведение. Следовательно каждый полином u_i делит некоторый полином в левой части (9), а так как u_i взаимно простые, то левая часть (9) делится на $f(x)$. Следовательно, выполняется (7).

Матричный алгоритм решения уравнения $\phi(\mathbf{x})^{\mathbf{p}} - \phi(\mathbf{x}) = \mathbf{0} \ \mathbf{mod} \ \mathbf{f}(\mathbf{x})$

Нужно решить однородное уравнение степени p в факторкольце $Z_{p,f(x)}$.

Так как у искомого полинома $\phi(x)$ степень менше степени $f()$, то он может иметь не более n коэффициентов. Будем располагать эти коэффициенты в векторе V из n компонент. Построим матрицу Q преобразования полинома $\phi(x)^p$ в факторкольцо $Z_{p,f(x)}$:

$$Q = \begin{pmatrix} q_{1,1} & q_{1,2} & \dots & q_{1,n} \\ q_{2,1} & q_{2,2} & \dots & q_{2,n} \\ q_{n,1} & q_{n,2} & \dots & q_{n,n} \end{pmatrix},$$

$$x^{pj} - - > W_j(x) = \sum_{i=0}^{n-1} q_{n-i,j} x^i = q_{1,j} x^{n-1} + q_{2,j} x^{n-2} + .. + q_{n,j} x^0$$

$$< - - > [q_{1,j}, q_{2,j}, ..., q_{n-1,j}]^T.$$

Задача свелась к решению матричного уравнения

$$QV - V = 0, \quad V \in (Z_p)^n. \qquad (10)$$

Как известо, решением является ядро оператора $Q - I$.
$SPACE = Z[x]; one = 1; zero = 0;$
Например, для поля Z_p
$p = 7$ и для полинома
$f = x^4 + 3x - 2$степени
$n = 4$ мы нашли, матрицу
$Q = \begin{pmatrix} 0 & -1 & 2 & 0 \\ 1 & -2 & 0 & 0 \\ -1 & 1 & 2 & 0 \\ -4 & 3 & 1 & 1 \end{pmatrix};$
$out:$

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

$SPACE = Zp32[x]; MOD32 = 7;$
$Q_p = \mathbf{toNewRing}(Q);$
Найдем ядро оператора
$B = Q_p - \mathbf{I}_{4,4};$
$ker = \mathbf{kernel}(B);$
И проверим произведение B*ker:
$Check = B \cdot ker; \mathbf{print}(B, ker, Check)$
$out:$

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

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

$$Check = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

R^n; A: $R^n - - - > R^n$

$X \in R^n$ $A * X = 0$ $A(X+Y) = 0$; $A(\lambda X) = 0$;
out:
0

Каждому базисному вектору ядра ker, соответствует один полином - решение. Последнему вектору соответтвует решение, которое является константой, поэтому мы его не берем.

$P = \mathbf{O}_n; P = (pol_i);$ Это массив pol для хранения всех найденных полиномов.

Транспонтруем ядро, чтобы выбирать строки и составлять из них полиномы.

$kerTR = ker^T; m = \mathbf{rowNumb}(kerTR) - 1;$ Это число базисных векторов в ядре минус 1.

$for(i = 1; i \le m; i = i+1)\{pol_i = \mathbf{vectorToPolynom}(\mathbf{takeRow}(kerTR, i)); \mathbf{print}(i, pol_i);\}$
$out:$

$i = 1$
$pol_i = x^3 - 2x^2 - 4x$

Получили ендинственный полином pol_1. Ищем НОД этого полинома с добавленными свободными членами у полинома f:

$f = x^4 + 3x - 2;$
$for(i = one; i \le p; i = i+1)\{I = \mathbf{toNewRing}(i); temp = pol_1 + I; gcd = \mathbf{GCD}(temp, f);$
$if(\neg(\mathbf{isOne}(gcd)))\{\mathbf{print}(temp, gcd);\}\}$
$out:$

$temp = x^3 - 2x^2 - 4x + 3$
$gcd = x^2 + x - 1$
$temp = x^3 - 2x^2 - 4x + 5$
$gcd = x^2 - x - 5$

Вот найдены искомые делители полинома $f = x^4 + 3x - 2$. Это
$a = x^2 + x - 1$ и
$b = x^2 - x - 5$. Можно сделать проверку
$sub = f - a \cdot b$
$out:$

0

Алгоритм Берлекампа

Для того, чтобы сформулировать алгоритм, необходимо знать еще одну теорему, которую пока приведем без доказательства.

Т Е О Р Е М А 7. (Батлера)

Размерность пространства ядра оператора $Q - I$ в поле Z_p равна числу простых делителей полинома $f \in Z_p[x]$.

Д О К А З А Т Е Л Ь С Т В О опубликовано в работе

M.C.R.Butler. On the Reductibility of Polynomials overa Finite Field. Quart. J.Math.V.5,No.1, 1954. 102-1
.

Из это теоремы следует, что алгоритм поиска простых делителей не надо начинать, если размерность ядра

$kernelSize$ равна 1, так как единственным простым делителем будет сам исходный полином f.

Из нее следует простой критерий остановки алгоритма: чило найденных простых делителей должно быть равно $kernelSize$.

Алгоритм факторизации полинома f степени n в простом поле Z_p

1) Построить матрицу Q отображения $u(x)^p$ по модулю $f(x)$, по заданным числам p, n и полиному $f(x)$.

2) Вычислить ядро оператора $Q - I$, его базис и его размерность $kernelSize$.

3) Если $kernelSize$=1, то полином f является неразложимым. Алгоритм завершается и возвращает f.

4) Каждый вектор из базиса ядра оператора соответствует одному полином в поле Z_p, который

является решением уравнения $u(x)^p = u(x) \textbf{ mod } f$. Запишем их в порядке возрастания степеней:

$$u_1, u_2, ..u_k, \quad k = kernelSize.$$

5) Для каждого из p полиномов $U_{1,j} = u_1 + j, \quad j = 0, 1, .., p - 1$ найдем $d_{1,j} = \mathbf{GCD}(f, U_{1,j})$. Все отличные от единицы полиномы $d_{1,j}$ являются делителями f.

6) Если получено $k = kernelSize$ делителей, то алгоритм завершается.

7) Если число делителей $k < kernelSize$, то повторяем шаг (5) для следующего по порядку

полинома $u_j \;\; j = 2, .., k$. Для полиномов $U_{i,j} = u_i + j, \quad j = 0, 1, .., p - 1$ находим $d_{i,j} = \mathbf{GCD}(f, U_{i,j})$. Так повторяем, пока не получим $k = kernelSize$ делителей полинома f.

END

$out:$

END

. Нужно придумать свой пример с составным полиномом и разложить полином на множители алгоритмом Берликампа факторизации полиномов в простом поле Z_p.

$out:$

2
