Домашнее задание №8

Гунаев Руслан, 776 группа

1 мая 2019 г.

1.

$$A(x)B(x) = P_1(x) + P_2(x) = C(x),$$

где $P_1(x)$ – многочлен порядка не выше, чем $n-1$, $P_2(x)$– многочлен порядка выше $n-1$. Произведем требуемую замену в многочлене $C(x)$, получим $C'(x) = P_1(x) + P_2'(x)$, где многочлен $P_2'(x)$– многочлен с теми же коэфициентами, что и $P_2(x)$, но порядка не выше $n-1$. Посмотрим разность этих многочленов.

$$C(x) - C'(x) = P_2(x) - P_2'(x) = \alpha_1(x^n - 1) + \alpha_2 x(x^n - 1) + \dots + \alpha_n x^{n-1}(x^n - 1) = P_2'(x)(x^n - 1)$$

Таким образом, получили, что $C(x)$ имеет тот же остаток что и $C'(x)$, но $C'(x)$ имеет порядок не выше $n-1$, а значит такой заменой мы получим остаток при делении исходного многочлена на $x^n - 1$.

2.

Найдем свертку по определению.

$$(1 + 2x + 3x^2 + 4x^3)(1 + x + x^2 + x^3 + x^4) = 1 + 3x + 6x^2 + 10x^3 + 9x^4 + 7x^5 + 4x^6$$

Сделаем замену степеней, как в первом номере, получим

$$A(x)B(x) = 10(1 + x + x^2 + x^3) \;\; mod \; x^n - 1$$

Найдем свертку с помощью быстрого преобразования Фурье. Сделаем прямое преобразование, потом разделим на $n = 4$ и развернем.

$$\omega_4 = i, \omega_2 = -1$$
$$A(\omega_4^0)B(\omega_4^0) = 40$$
$$A(\omega_4^1)B(\omega_4^1) = 0$$
$$A(\omega_4^2)B(\omega_4^2) = 0$$
$$A(\omega_4^3)B(\omega_4^3) = 0$$

$$P_0 = 40, P_1 = 0$$

$$P(\omega_4^k) = P_0(\omega_4^k) + \omega_4^k P_1(\omega_2^4)$$

Все коэффициенты равна 40. А значит свертка равна

$$C(x) = 10(1 + x + x^2 + x^3)$$

Многочлены равны.

3.

$$a = (1, 2, 4, 8)^T, b = (16, 8, 4, 2)^T$$

Обозначим искомый вектор за P. Найдем значения этого вектора в точках.

$$P(\omega_4^0) = B(\omega_4^0)/A(\omega_4^0) = 30/2 = 2$$
$$P(\omega_4^1) = B(\omega_4^1)/A(\omega_4^1) = (1 + 2i - 4 - 8i)^{-1}(16 + 8i - 4 - 2i) = \frac{6i - 8}{5}$$
$$P(\omega_4^2) = B(\omega_4^2)/A(\omega_4^2) = -2$$
$$P(\omega_4^1) = B(\omega_4^1)/A(\omega_4^1) = -\frac{8 + 6i}{5}$$

Применим обратное преобразование Фурье. Для этого сделаем прямое преобразование, затем разделим на $n = 4$ и развернем.

$$R_0(x) = 2 - 2x$$
$$R_1(x) = (6i - 8)/5 - (8 + 6i)x/5$$

$$R(\omega_4^k) = R_0(\omega_4^k) + \omega_4^k R_1(\omega_2^4)$$

В итоге получим, что искомый вектор равен

$$P = (-4/5, 8/5, 4/5, 2/5)^T$$

Это и будет ответом.

4.

Найдем $k : 2^{k-1} \leqslant n + 1 \leqslant 2^k$, тогда положим коэфициенты многочленов нулями при степенях больших n. Применим обратное преобразование Фурье, получим нужную асимптотику.

5.

Произведем умножение $AF = C$.

$$c_{kj} = \sum_{i=0}^{n-1} a_{k-i \ (mod \ n)} \omega^{ij} = \omega^{kj} \sum_{i=0}^{n-1} a_{k-i \ (mod \ n)} \omega^{j(i-k)} = \omega^{kj} A(\omega^j)$$

Чтобы равенство выполнялось, многочлен должен иметь следующий вид

$$A(x) = a_0 + a_{n-1}x + a_{n-2}x^2 + \ldots + a_1 x^{n-1}.$$

6.

1)

$$41 = 5 \cdot 2^3 + 1 \Rightarrow c = 5.$$

6–первообразный корень по модулю 41, значит $6^5 \equiv 27 \ (mod \ 41)$.

2)

Так как максимальная степень первого многочлена равна 1,а второго – 2, то нам достаточно знать примитивный корень 4 степени и второй, которые равны $27^2 \equiv 32 \ (mod\ 41)$ и $32^2 \equiv 40 \ (mod\ 41)$ соответственно.

Посчитаем ДПФ для первого многочлена.

$$A(1) = 3 + 2 = 5 \ (mod\ 41)$$
$$A(40) = 3 \cdot 40 + 2 = 40 \ (mod\ 41)$$

Аналогично для второго.

$$B(1) = 2 \ (mod\ 41)$$
$$B(32) = 0 \ (mod\ 41)$$
$$B(40) = 2 \ (mod\ 41)$$
$$B(32^3) = 0 \ (mod\ 41)$$

3)

Покажем, что матрица $B : (B)_{ij} = n^{-1}(\omega^{-1})^{ij}(mod\ p)$ обладает следующим свойством.

$$AB = E.$$

По определению

$$[AB]_{jj'} = n^{-1}\sum_{k=0}^{n-1}\omega^{k(j'-j)} = n^{-1}\sum_{k=0}^{n-1}\omega^{kt}$$

Заметим, что для целого $t > 0$, не кратного n, выполнено равенство

$$\sum_{k=0}^{n-1}(\omega^k)^t = 0$$

Докажем это.

$$\sum_{k=0}^{n-1}(\omega^k)^t = \frac{(\omega^k)^n - 1}{\omega^k - 1} = 0$$

Если $t = 0$, то очевидно такая сумма равна n.

Значит матрица B действительно является обратной.

4)

Полученный многочлен будет не выше четвертой степени. Сначала найдём обратный для четверки по модулю 41

$$4 \cdot 10 \equiv 40 \equiv -1(\text{mod } 41) \Rightarrow 4^{-1} \equiv -10 \equiv 31(\text{mod } 41)$$

.

Посчитаем значения произведений исходных многочленов в корнях четвертой степени из единицы ($\omega_4 = 32$).

$$A(\omega_4^0) \cdot B(\omega_4^0) = 10;\ A(\omega_4^1) \cdot B(\omega_4^1) = 0;\ A(\omega_4^2) \cdot B(\omega_4^2) = -2;\ A(\omega_4^3) \cdot B(\omega_4^3) = 0$$

Далее воспользуемся обратным преобразованием Фурье, чтобы восстановить коэффициенты исходного многочлена. $P_0(x) = 10 - 2x$; $P_1(x) = 0$. Тогда $a_k = P_0(\omega_2^{-k}) + \omega_4^{-k} P_1(\omega_2^{-k})$.

$$P_0(40^0) = 8;\ P_1(40^0) = 0;\ P_0(40^1) = 12;\ P_1(40^1) = 0$$

$$a_0 = 8/4 = 8 \cdot 31 = 2$$

$$a_1 = 12/4 = 12 \cdot 31 = 3$$

$$a_2 = 8/4 = 8 \cdot 31 = 2$$

$$a_3 = 12/4 = 12 \cdot 31 = 3$$

Итого $A(x) \cdot B(x) = 3x^3 + 2x^2 + 3x + 2$.

7.

В случае, когда в образец и текст могут входить «джокеры», то нам нужно вычислить суммы $B_i, i \in \overline{0, n-m}$, где $B_i = \sum\limits_{j=0}^{m-1} p_j t_{i+j} (t_{i+j} - p_j)^2$. При этом символу «?» соотвуетсвует ноль, а всем остальным положительные числа. Тогда данная сумма будет обнуляться тогда и только тогда, когда каждое ее слагаемое будет нулевым. Нулевым же слагаемое будет, если $p_j = 0$ (т. е. в образце на этой позиции стоит «джокер»), $t_{i+j} = 0$ (т. е. в тексте на этой позиции стоит «джокер») или $t_{i+j} = p_j$ (соответствующие символы в тексте и образце совпадают). Раскроем скобки и получим, что $B_i = \sum\limits_{j=0}^{m-1} (p_j^3 t_{i+j} - 2p_j^2 t_{i+j}^2 + p_j t_{i+j}^3)$. Теперь рассмотрим новые многочлены $T(x) = t_{n-1}^2 x_{n-1} + t_{n-2}^2 x_{n-2} + \ldots + t_0^2, Q(x) = t_{n-1} x_{n-1} + t_{n-2} x_{n-2} + \ldots + t_0, R(x) = t_{n-1}^3 x_{n-1} + t_{n-2}^3 x_{n-2} + \ldots + t_0^3$ и $P(x) = p_0^2 x^{m-1} + \ldots + p_{m-1}^2, S(x) = p_0^3 x^{m-1} + \ldots + p_{m-1}^3, W(x) = p_0 x^{m-1} + \ldots + p_{m-1}$, которые можно построить за линейное время. Каждый из многочленов степени не больше n. Найдем при помощи БПФ коэффициенты многочленов $K = TP, L = QS, M = RW$. Рассмотрим $k_{m-1+i} = p_0^2 t_i^2 + p_1^2 t_{i+1}^2 + \ldots + p_{m-1}^2 t_{m-1+i}^2 = \sum\limits_{j=0}^{m-1} p_j^2 t_{i+j}^2, l_{m-1+i} = \sum\limits_{j=0}^{m-1} p_j^3 t_{i+j}, m_{m-1+i} = \sum\limits_{j=0}^{m-1} p_j t_{i+j}^3$. Все эти коэффициенты мы посчитаем за $O(n \log n)$ при помощи БПФ. Тогда $B_i = l_{m-1+i} - 2k_{m-1+i} + m_{m-1+i}$. Таким образом, мы можем определить все значения B_i за требуемое время, затем сравнить их с нулем и выдать ответ о вхождении образца в тексте.