ДЗ 10
(криптография и теория чисел)

Владимир Латыпов
donrumata03@gmail.com

Содержание

4 Двумерные пластины

Сделаем теперь двумерное преобразование Фурье: заведём виртуальные переменные, а не реальные:

- сопоставим точке i, j на пластине степень x^{i+2nj} многочлена.
- произведём одномерное преобразование Фурье над полученным многочленом.
- восстановим «двумерные» коэфициенты:

$$[x^{i+2nj}]C = \sum_{i+2nj=k_1+k_2+2n(l_1+l_2)} a_{k_1,l_1} b_{k_2,l_2} = \sum_{k_1=0}^{i} \sum_{l_1=0}^{j} a_{k_1,l_1} b_{i-k_1,j-l_1}$$

$\longrightarrow$ Научились перемножать двумерные многочлены за $O(n^2 \log n)$ (так как преобразовании Фурье над $2n^2$ членами).

Теперь

- развернём вторую пластину по обеим осям,
- два раза (или один) посчитаем скалярное произведение
- найдём те позиции, где оказался ноль

5 Расстояние Хэмминга

6 Периоды

Лемма 6.1: Характеристическое свойство периода p строки s: $s[p...) = s[...n-p)$, то есть проверяем одним махом, что $\forall i : s[i] = s[i+p]$.

Тогда проверим это для всех p, посчитав такие скалярные произведения для всех сдвигов:

- Количество позиций, где $s > s'$, где в s : „?“ $\to$ „0“, а в в s' : „?“ $\to$ „1“
- Количество позиций, где $s < s'$, аналогично.

Те сдвиги, где оба условия выполнены, являются периодами.

7 Троичный DFFT

$p = 3^k q + 1$, подразумевается, что подобрано простое число такого вида для $n = 3^k$ — многочлены такой длины хотим преобразовывать.

Возьмём $\omega = g^{\frac{p-1}{n}} = q$, тогда будет

$$\underbrace{\underbrace{\omega^0}_{=1}\underbrace{\omega^1 \ldots}_{\neq 1}}_{n-1 \text{ штук}}$$

Заметим, что

$$A(x) = \underbrace{A_{\equiv_3 0}(x^3)}_{\approx \frac{n}{3}} + x\underbrace{A_{\equiv_3 1}(x^3)}_{\approx \frac{n}{3}} + x^2\underbrace{A_{\equiv_3 2}(x^3)}_{\approx \frac{n}{3}}$$

Тогда посчитаем 3 преобразования с ω^3 и $\frac{n}{3}$ и

```
for i in 0..n / 3 - 1
  f_i = f'_i + omega^i f''i + omega^(2i) f'''
  f_(i + n/3) = f'_i + omega^(i + n/3) f''i + (omega^(i + n/3))^2 f'''
  f_(i + 2 n/3) = f'_i + omega^(i + 2 n/3) f''i + (omega^(i + 2 n/3))^2 f'''
```