Циклическая свёртка. Циркулянты

При умножении многочленов A и B степеней n и m обычно находят степень двойки такую, что она будет не меньше, чем $n+m$. Так мы гарантируем, что многочлен, который мы найдём будет иметь достаточно высокую степень. Давайте теперь подумаем о том, что будет если мы всё-таки применим эту процедуру для умножения двух многочленов степени $n-1$, при этом использую дискретное преобразование Фурье размера n.

Такое умножение однозначно задаст некоторый многочлен степени $n-1$. Определим его свойства. Мы вычисляли его значения в точках ω_n^k. Они все (и только они) удовлетворяют уравнению $x^n = 1$. Рассмотрим формальное умножение многочленов, в котором мы в посчитанном произведении заменяем $x^n \to 1, x^{n+1} \to x, \ldots, x^{2n-1} \to x^{n-1}$.

1. (1б) Покажите, что так мы получим остаток от деления многочлена $A(x)B(x)$ на $x^n - 1$.

После такого умножения мы всегда остаёмся в классе многочленов степени не выше $n-1$ и значения, которые мы получим, рассматривая многочлены A и B в точках ω_n^k и считая их покомпонентное произведение, будут соответствовать значениям многочлена, полученного применением данной процедуры к $A(x)B(x)$. Значит, в силу единственности интерполяционного многочлена это он и будет. Рассмотрим это с точки зрения остатков:

Как мы увидели раньше, при интерполяции мы применяем китайскую теорему об остатках. Это значит, что если мы рассматривали значения в точках x_i, то мы сначала переходили к остаткам от деления на $(x - x_i)$:

$$A(x) \pmod{x - x_i},\ B(x) \pmod{x - x_i}$$

А затем покомпонентно умножали и восстанавливали по КТО, то есть, в итоге мы получаем:

$$P(x) \equiv A(x) \cdot B(x) \left(\bmod \prod_{i=1}^{n} (x - x_i) \right)$$

В нашем случае получаем $\prod\limits_{i=0}^{n-1} (x - \omega_n^i) = x^n - 1$. Умножение многочленов по такому модулю называют *циклической свёрткой*. Её можно записать в следующем виде:

$$c_k = \sum_{i+j \equiv k} a_i b_j$$

В отличие от классической свёртки, здесь под $i+j \equiv k$ мы подразумеваем равенство $\pmod n$.

2. (2б) Найдите циклическую свёртку многочленов $A(x) = 1+2x+3x^2+4x^3$ и $B(x) = 1+x+x^2+x^3$ по определению и с помощью преобразования Фурье. Убедитесь, что они совпадают.

Наконец, заметим, что есть взаимооднозначеное соответствие между циклическими свёртками и умножением на так называемые циклические матрицы. Это такие матрицы, что каждая следующая строка в ней является циклическим сдвигом предыдущей:

$$\begin{pmatrix} a_0 & a_{n-1} & a_{n-2} & \ldots & a_1 \\ a_1 & a_0 & a_{n-1} & \ldots & a_2 \\ a_2 & a_1 & a_0 & \ldots & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \ldots & a_0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

Такие матрицы также называют *циркулянтами*. Из схемы выше непосредственно видно соответствие между циклической свёрткой c_k многочленов a_i и b_j и умножением вектор-стобца b_j

на матрицу, первой строкой которой являются коэффициенты a_i. Такое представление позволяет быстро умножать на циклические матрицы (за $O(n \log n)$, если она задана первой строкой), а также решать уравнения с циклическими матрицами (если те имеют размер 2^k). Можно просто считать циклические свёртки соответствующих многочленов, а для решения систем – делить полученные значения многочлена $C(x)$ на значения многочлена $A(x)$.

3. (2б) Используя дискретное преобразование Фурье, найдите решение системы линейных уравнений $Cx = b$, где C – циркулянтная матрица, порождённая вектором-столбцом $(1, 2, 4, 8)^t$, а $b^t = (16, 8, 4, 2)$.

4. (1б) Предложите способ посчитать циклическую свёртку $A(x)$ и $B(x)$ за $O(n \log n)$, где n – степени многочленов. При этом n, возможно, не является степенью двойки.

Обоснуем формально связь циклических матриц с преобразованием Фурье. Пусть $\mathcal{F}$ — матрица дискретного преобразования Фурье:

$$\mathcal{F} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-1} & \omega^{-2} & \dots & \omega \end{pmatrix}$$

5. (2б) Покажите, что если мы умножим циклическую матрица A на $\mathcal{F}$, то получим:

$$A\mathcal{F} = \begin{pmatrix} A(1) & A(\omega) & A(\omega^2) & \dots & A(\omega^{-1}) \\ A(1) & \omega A(\omega) & \omega^2 A(\omega^2) & \dots & \omega^{-1} A(\omega^{-1}) \\ A(1) & \omega^2 A(\omega) & \omega^4 A(\omega^2) & \dots & \omega^{-2} A(\omega^{-1}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A(1) & \omega^{-1} A(\omega) & \omega^{-2} A(\omega^2) & \dots & \omega A(\omega^{-1}) \end{pmatrix}$$

Где $A(x)$ – некоторый многочлен. Выпишите явно, какой многочлен имеется в виду.

Таким образом, столбцы $\mathcal{F}$ являются собственными векторами любой циклической матрицы A, а собственными числами выступают значения многочлена $A(x)$ в корнях степени n из единицы.

1°. (4б) Формализуйте алгоритм решения систем с циркулянтной матрицей с помощью дискретного преобразования Фурье. Рассмотрите случаи когда некоторые значения выходят нулевыми.

Преобразование Фурье в кольце вычетов $\mathbb{Z}_n$

Как было сказано выше, помимо комплексных корней из единицы, можно рассматривать корни из единицы в каком-нибудь поле. В данном случае нас интересуют поля остатков по модулю простых чисел. Известно, что в любом таком поле есть образующий элемент – такое число, что его степени пробегают все элементы, кроме нуля.

Значит, для любого простого p в поле остатков от деления на него есть корень g степени $p-1$ из единицы. Если при этом $(p-1) = c \cdot 2^k$, то g^c будет корнем степени 2^k, что позволяет применять метод Кули-Тьюки. Отсюда следует, что нас интересуют числа вида $p = c \cdot 2^k + 1$.

6. (8б)

1. Найдите примитивный корень восьмой степени в поле $\mathbb{Z}_{41}$.
2. Вычислите ДПФ многочленов $A(x) = 3x + 2,\ B(x) = x^2 + 1$ в поле $\mathbb{Z}_{41}$.
3. Пусть A – матрица дискретного преобразования Фурье длины n, ω_n – соответствующий первообразный корень степени n в поле $\mathbb{Z}_p$. Докажите, что $(A^{-1})_{ij} \equiv n^{-1} \cdot (\omega^{-1})^{ij} \pmod{p}$.
4. С помощью БПФ найдите произведения $A(x),\ B(x)$ из второго пункта в поле $\mathbb{Z}_{41}$.

Применения FFT

Свёртки и корреляции

Большая часть применений преобразования Фурье использует то, что оно позволяет быстро считать произведение двух многочленов $A(x) = \sum\limits_{i=0}^{n} a_i x^i$ и $B(x) = \sum\limits_{j=0}^{m} b_j x^j$, то есть, такой многочлен $C(x) = \sum\limits_{k=0}^{n+m} c_k x^k$, что:

$$c_k = \sum_{i+j=k} a_i b_j = \sum_j a_{k-j} b_j$$

Такая последовательность c_k называется *свёрткой* последовательностей a_i и b_j. Для упрощения обозначений, будем считать, что a_i и b_j на самом деле финитные последовательности, т.е. если мы обратимся к коэффициенту, номер которого находится за пределами определённых, то будем считать, что он равен нулю.

Введём обозначение $B^r(x) = x^m B(x^{-1})$, где $m = \deg B$. Так мы задали многочлен, чья последовательность коэффициентов развёрнута относительно многочлена B. То есть, $b^r_j = b_{m-j-1}$. Если мы рассмотрим свёртку $A(x)$ и $B^r(x)$, мы получим *корреляцию* последовательностей $A(x)$ и $B(x)$, т.е. многочлен $\widetilde{C}(x)$:

$$\widetilde{c_k} = \sum_{i+(m-j-1)=k} a_i b_j = \sum_j a_{j+k-(m-1)} b_j$$

Её смысл в том, что $\widetilde{c_k}$ равен скалярному произведению последовательностей a и b при том, что a рассматривается, начиная с элемента $k-(m-1)$.

Рассмотрим свёртки и корреляции на примере. Пусть $A(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4$, $B(x) = b_0 + b_1 x + b_2 x^2$.

$$\begin{aligned}
c_0 &= b_2 \cdot 0 + b_1 \cdot 0 + b_0 \cdot a_0 + 0 \cdot a_1 + 0 \cdot a_2 + 0 \cdot a_3 + 0 \cdot a_4 + 0 \cdot 0 + 0 \cdot 0,\\
c_1 &= 0 \cdot 0 + b_2 \cdot 0 + b_1 \cdot a_0 + b_0 \cdot a_1 + 0 \cdot a_2 + 0 \cdot a_3 + 0 \cdot a_4 + 0 \cdot 0 + 0 \cdot 0,\\
c_2 &= 0 \cdot 0 + 0 \cdot 0 + b_2 \cdot a_0 + b_1 \cdot a_1 + b_0 \cdot a_2 + 0 \cdot a_3 + 0 \cdot a_4 + 0 \cdot 0 + 0 \cdot 0,\\
c_3 &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot a_0 + b_2 \cdot a_1 + b_1 \cdot a_2 + b_0 \cdot a_3 + 0 \cdot a_4 + 0 \cdot 0 + 0 \cdot 0,\\
c_4 &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot a_0 + 0 \cdot a_1 + b_2 \cdot a_2 + b_1 \cdot a_3 + b_0 \cdot a_4 + 0 \cdot 0 + 0 \cdot 0,\\
c_5 &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot a_0 + 0 \cdot a_1 + 0 \cdot a_2 + b_2 \cdot a_3 + b_1 \cdot a_4 + b_0 \cdot 0 + 0 \cdot 0,\\
c_6 &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot a_0 + 0 \cdot a_1 + 0 \cdot a_2 + 0 \cdot a_3 + b_2 \cdot a_4 + b_1 \cdot 0 + b_0 \cdot 0.
\end{aligned}$$

Теперь посмотрим на корреляцию, т.е., на свертку $A(x)$ с $B^r(x) = b_2 + b_1 x + b_0 x^2$.

$$\begin{aligned}
\widetilde{c_0} &= b_0 \cdot 0 + b_1 \cdot 0 + b_2 \cdot a_0 + 0 \cdot a_1 + 0 \cdot a_2 + 0 \cdot a_3 + 0 \cdot a_4 + 0 \cdot 0 + 0 \cdot 0,\\
\widetilde{c_1} &= 0 \cdot 0 + b_0 \cdot 0 + b_1 \cdot a_0 + b_2 \cdot a_1 + 0 \cdot a_2 + 0 \cdot a_3 + 0 \cdot a_4 + 0 \cdot 0 + 0 \cdot 0,\\
\widetilde{c_2} &= 0 \cdot 0 + 0 \cdot 0 + b_0 \cdot a_0 + b_1 \cdot a_1 + b_2 \cdot a_2 + 0 \cdot a_3 + 0 \cdot a_4 + 0 \cdot 0 + 0 \cdot 0,\\
\widetilde{c_3} &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot a_0 + b_0 \cdot a_1 + b_1 \cdot a_2 + b_2 \cdot a_3 + 0 \cdot a_4 + 0 \cdot 0 + 0 \cdot 0,\\
\widetilde{c_4} &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot a_0 + 0 \cdot a_1 + b_0 \cdot a_2 + b_1 \cdot a_3 + b_2 \cdot a_4 + 0 \cdot 0 + 0 \cdot 0,\\
\widetilde{c_5} &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot a_0 + 0 \cdot a_1 + 0 \cdot a_2 + b_0 \cdot a_3 + b_1 \cdot a_4 + b_2 \cdot 0 + 0 \cdot 0,\\
\widetilde{c_6} &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot a_0 + 0 \cdot a_1 + 0 \cdot a_2 + 0 \cdot a_3 + b_0 \cdot a_4 + b_1 \cdot 0 + b_2 \cdot 0.
\end{aligned}$$

Визуально мы прикладываем последовательность b к a и считаем скалярные произведения.

Арифметические прогрессии длины 3. Пусть есть n сундуков. Часть из них содержит сокровище, а часть является мимиками. Мы знаем про каждый сундук, является ли он мимиком. Нужно узнать, сколько есть троек $i < k < j$ таких, что сундуки на номерах i, j и k – мимики, и при этом $j - k = k - i$, т.е. их номера образуют арифметическую прогрессию длины 3.

Пусть a_i равно 1 если сундук мимик и 0 если нет. Рассмотрим свёртку этой последовательности самой с собой.

$$c_k = \sum_{i+j=k} a_i a_j \implies c_{2k} = \sum_{j-k=k-i} a_i a_j$$

Значит, ответом будет $\sum\limits_{k=0}^{n-1} a_k(c_{2k} - 1)$. Мы вычитаем единицу, чтобы не учитывать $i = k = j$.

Можно получить альтернативную форму ответа, введя концепт индикаторной функции:

$$\delta(x) = \begin{cases} 1, x = 0, \\ 0, x \neq 0 \end{cases}$$

Нам нужно посчитать $\sum\limits_{i=0}^{n-1}\sum\limits_{j=0}^{n-1}\sum\limits_{k=0}^{n-1} a_i a_j a_k \delta(i + j - 2k)$. Индикаторную функцию на множестве $\mathbb{Z}_n$ можно выразить через корни из единицы: $\delta(x) = \frac{1}{n}\sum\limits_{t=0}^{n-1} \omega_n^{tx}$. Значит, нам нужно посчитать следующую сумму:

$$\frac{1}{n}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1}\sum_{t=0}^{n-1} a_i a_j a_k \omega_n^{t(i+j-2k)} =$$

$$= \frac{1}{n}\sum_{t=0}^{n-1}\left(\sum_{i=0}^{n-1} a_i \omega_n^{(-2t)i}\right)\left(\sum_{i=0}^{n-1} a_i \omega_n^{ti}\right)^2 =$$

$$= \frac{1}{n}\sum_{t=0}^{n-1} [\mathrm{DFT}_n(A)]_{-2t} [\mathrm{DFT}_n(A)]_t^2$$

То есть, ответ можно выразить непосредственно через элементы преобразования Фурье. Заметим, что индикаторную функцию мы ввели над $\mathbb{Z}_n$, значит, на самом деле мы посчитаем количество арифметических прогрессий таких что $i + j = 2k \pmod n$. Чтобы решить эту проблему, нужно взять достаточно большой n, дополнив последовательность нулями, тогда $i + j$ не будет превосходить n и ответ будет такой же, как если бы мы рассматривали только целые числа.

Попарные суммы. Пусть у нас есть два набора предметов A и B, предметы могут иметь вес от 0 до n. Мы знаем a_i и b_i – сколько предметов веса i есть в обоих наборах. Нужно для каждого $0 \leq k \leq 2n$ узнать, сколько есть способов выбрать по одному предмету из набора, чтобы их суммарный вес был равен k.

Если мы захотим взять предмет веса i из A и веса j из B, будет $a_i \cdot b_j$ способов сделать это. Отсюда следует, что ответ выражается по той же формуле, что свёртка последовательностей:

$$c_k = \sum_{i+j=k} a_i \cdot b_j$$

2°. (4б) Вам дано число в двоичной записи $a_0 + a_1 \cdot 2 + \cdots + a_{n-1} \cdot 2^{n-1}$. Предложите алгоритм, работающий за время $O(n \log^2 n)$, который переведёт это число в десятичную систему, т.е. представит в виде $b_0 + b_1 \cdot 10 + \ldots b_{m-1} \cdot 10^{m-1}$. Считайте, что арифметические операции с числами, не превышающими n^2 могут выполняться за $O(1)$.

Сопоставление образцов

Пусть у вас есть строки s и t. Вы хотите найти все вхождения s в t. Рассмотрим два подхода:

1. Пусть алфавит – Σ. Тогда можно рассмотреть каждый символ алфавита в отдельности. Рассмотрим последовательности A' и B', в которых вхождения текущего символа c заменены на 1, а остальные – на 0. Теперь мы можем посчитать корреляцию A' и B' и узнать для каждой позиции в A, сколько есть мест, где, начиная с этой позиции символы A и B совпадают и равны c. Просуммировав это по всем $c \in \Sigma$, мы узнаем, в каких позициях имеет место точное совпадение, т.е. число таких символов равно $|B|$.

2. Можно посмотреть на это с другой стороны – мы хотим найти такие позиции k, что

$$\sum_{i=0}^{m-1}(a_{k+i}-b_i)^2 = \sum_{i=0}^{m-1}(a_{k+i}^2+b_i^2) - 2\sum_{i=0}^{m-1}a_{k+i}b_i = 0$$

   Суммы квадратов мы можем посчитать отдельно, а суммы $a_{k+i}b_i$ могут быть посчитаны как корреляция.

Первый подход менее практичный, но зато он позволяет быстро считать расстояние Хемминга от B до каждой подстроки A. Второй, с другой стороны, может быть посчитан асимптотически быстрее и позволяет точно узнать среднеквадратичное отклонение подстрок A от B.

Теперь можно рассмотреть модификацию алгоритма, которая позволяет быстро находить вхождения одной строки в другую если в них есть “джокеры”, т.е. символы, которым можно сопоставить произвольный. Обычно они обозначаются знаком “?”.

7. (2б) Покажите, что описанную задачу можно решить если вместо джокеров поставить в строки нули и искать позиции k такие что нулю равна изменённая сумма:

$$\sum_{i=0}^{m-1} a_{i+k}b_i(a_{i+k}-b_i)^2 = 0$$

Предложите алгоритм, находящий все такие позиции за $O(n \log n)$.

Интерполяция многочленов

Теперь, умея умножать многочлены, научимся интерполировать их в произвольных точках.

Обратный ряд

Если свободный член многочлена P не равен нулю, у него есть обратный ряд Q такой что $P \cdot Q = 1$. Приведём процедуру, позволяющую последовательно удваивать число известных коэффициентов в нём. Для этого будем строить последовательность приближений Q_n такую что $P \cdot Q_n \equiv 1 \pmod{x^{2^n}}$. Базой будет служить $Q_0 = P(0)^{-1}$. Указанное выше равенство можно переписать в виде:

$$P \cdot Q_n \equiv 1 + x^{2^n} \cdot R \pmod{x^{2^{n+1}}}$$

Взяв $Q_{n+1} = Q_n + x^{2^n} \cdot T$, получим:

$$P \cdot Q_{n+1} \equiv 1 + x^{2^n} \cdot (R + P \cdot T) \pmod{x^{2^{n+1}}}$$

Нам нужно, чтобы справа был только 1, значит,

$$R + P \cdot T \equiv 0 \pmod{x^{2^n}} \implies T \equiv -R \cdot P^{-1} \equiv -R \cdot Q_n \pmod{x^{2^n}}$$

Отсюда следует, что:

$$x^{2^n} \cdot T \equiv -x^{2^n} \cdot R \cdot Q_n \equiv (1 - P \cdot Q_n) \cdot Q_n \pmod{x^{2^{n+1}}}$$

Это даёт нам искомое выражение:

$$Q_{n+1} = Q_n \cdot (2 - P \cdot Q_n) \pmod{x^{2^{n+1}}}$$

3°. (1б) Покажите, что первые m коэффициентов обратного ряда можно вычислить за $O(m \log m)$.

Взятие остатка по модулю

Теперь научимся представлять многочлены в виде:

$$A(x) = D(x) \cdot B(x) + R(x), \deg R(x) < \deg B(x)$$

Пусть $\deg A = n, \deg B = m$, тогда $\deg D = n - m$. Коэффициенты при $x^m, \ldots, x^n$ у R равны нулю в силу ограничения на степень $\deg R < m$. Тогда для нахождения $D(x)$ будет удобно "развернуть" многочлены и взять остаток по модулю x^{n-m}, чтобы R не мешало. Введём обозначения:

$$A^r(x) = x^n A(x^{-1}),\ B^r(x) = x^m B(x^{-1}),\ D^r(x) = x^{n-m} D(x^{-1}),\ R^r(x) = x^n R(x^{-1})$$

4°. (2б) Покажите, что $A^r(x) = D^r(x) \cdot B^r(x) + R^r(x)$.

Исходя из этого следует, что $A^r(x) \equiv D^r(x) \cdot B^r(x) \pmod{x^{n-m+1}}$, так как $R^r(x) \equiv 0 \pmod{x^{n-m+1}}$.

Это позволяет в явном виде найти решение:

$$D^r(x) = A^r(x) \cdot [B^r(x)]^{-1} \pmod{x^{n-m+1}}$$

Вычисление многочлена в нескольких точках

Пусть теперь нам дан многочлен $P(x)$ степени n. Научимся вычислять его значения в точках $\{x_i\}_{i=0}^{n-1}$. Это значит, что нам нужно найти его остатки от деления на $(x - x_i)$. Для этого можно применить следующую рекурсивную процедуру:

1. Найдём $A = (x - x_0)(x - x_1) \ldots (x - x_{n/2})$ и $B = (x - x_{n/2+1})(x - x_{n/2+2}) \ldots (x - x_{n-1})$.
2. Посчитаем $P_1 = P \bmod A$, $P_2 = P \bmod B$ и запустимся рекурсивно с многочленами P_1, P_2 и точками, захваченными в A и B соответственно. База – многочлен степени 0, который надо вычислить в одной точке.

Мы сводим нашу задачу к двум подзадачам, размер которых в два раза меньше. При этом вычисление многочленов P_1 и P_2 занимает $O(n \log n)$ времени, поэтому общее время оценивается как:

$$T(n) = 2T\left(\frac{n}{2}\right) + O(n \log n) = O(n \log^2 n)$$

5°. (2б) В данном рассуждении содержится неточность. Найдите её и предложите, как её можно исправить, чтобы величина $O(n \log^2 n)$ всё ещё корректно оценивала процедуру.

Подсказка: Обратите внимание на нахождение A и B.

Интерполяция

Наконец, мы ввели все операции, которые нам понадобятся. Итак, пусть нам дан набор точек $\{(x_i, y_i)\}_{i=0}^{n-1}$, все x_i различны. Нужно найти многочлен $P(x)$ степени $n-1$, который проходит через все эти точки. Для этого по аналогии с вычислением многочлена воспользуемся идеей разделения задачи на две. Процедура:

1. Найдём $P_1(x)$ степени $n/2$ такой, что $P(x_i) = y_i$ для $x_i \leq n/2$.
2. Будем искать $P(x)$ в виде $P(x) = P_1(x) + Q(x) \cdot P_2(x)$, где $Q(x) = (x-x_0)(x-x_1)\dots(x-x_{n/2})$. Здесь $P_2(x)$ это многочлен степени $n - n/2$, такой что его значения в точках x_i для $i > n/2$ равны:
$$P_2(x_i) = \frac{P(x_i) - P_1(x_i)}{Q(x_i)} = \frac{y_i - P_1(x_i)}{Q(x_i)}$$

Таким образом, мы свели интерполяцию к вычислению многочленов $P_1(x)$ и $Q(x)$ в точках x_i. Итого:

$$T(n) = 2T\left(\frac{n}{2}\right) + O(n \log^2 n) = O(n \log^3 n)$$

1*. (3б) Пользуясь идеями из последних двух разделов, предложите быстрые алгоритмы для перехода:

$$x \equiv r \pmod{m} \Longleftrightarrow \begin{cases} x \equiv r_1 \pmod{m_1}, \\ x \equiv r_2 \pmod{m_2}, \\ \dots, \\ x \equiv r_n \pmod{m_n} \end{cases}$$

От представления числа как остатка по модулю m к представлению как набора остатков по модулям m_i. Считайте, что числа заданы последовательностями цифр, $\log m_i = O(\log n)$ и арифметические операции с числами, чья длина не превышает $\log n$ могут проводиться за $O(1)$.

Асимптотика должна быть $O(n \log^c n), c = \text{const}$.