Задачи по теме: быстрое умножение

А. Я. Канель-Белов, И. Митрофанов

February 13, 2010

1) Покажите, что алгоритм "деления в столбик с остатком" n-значного числа на m-значное требует не менее mn и не более $10mn$ элементарных операций, то есть имеет сложность порядка mn.

2) Пусть k – фиксированное натуральное число. Покажите, что сложность алгоритма "деления в столбик с остатком" n-значного числа на k равна n. Дайте оценку на число элементарных операций сверху.

3) Напишите на псевдокоде (или на другом удобном для Вас языке) текст программы, реализующей умножение двух натуральных чисел методом Карацубы.

4) $*$ Оцените число элементарных операций с цифрами, необходимых для умножения двух n-значных чисел методом Карацубы.

5) Выведите формулы для коэффициентов многочлена $R(t)$ четвёртой степени по значениям в точках $0, \pm 1, \pm 2$.

6) Покажите, что для вычисления произведения двух квадратных трёхчленов с n-значными коэффициентами достаточно ограничиться 5 n-значными умножениями и $30n$ элементарными операциями.

7) Пусть $T(n)$ – число элементарных операций, необходимых для умножения двух n-значных чисел. Докажите рекуррентное неравенство $T(3n) \leq 5T(n) + 30n$. Выведите из него асимптотическое неравенство $T(n) \ll n^{\log_3 5}$.

8) Докажите, что $\log_n(2n-1) \to 1$ при $n \to \infty$ и, более того, монотонно убывает при $n > 2$.

9) Сравните $\log_2 3$ и $\log_3 5$.

Задачи по теме: быстрое умножение-2

А. Я. Канель-Белов, И. Митрофанов

February 14, 2010

1) Пусть A, B, C – квадратные матрицы размера 2. Докажите, что $(A \times B) \times C = A \times (B \times C)$, то есть умножение матриц *ассоциативно*. Коммутативно ли оно, то есть всегда ли $A \times B = B \times A$?

2) * Попробуйте догадаться, как умножаются квадратные матрицы произвольного размера. Ассоциативно ли это умножение?

3) * Пусть A, B – матрицы размера $n \times n$. Докажите, что ранг произведения $A \times B$ не превосходит ранга матрицы A.

4) Решите предыдущую задачу для матриц 2×2.

5) Упростите выражение $\sum_{i=0}^{n} x_i^2 \frac{(x-x_0)\cdots\widehat{(x-x_i)}\cdots(x-x_n)}{(x_i-x_0)\cdots\widehat{(x_i-x_i)}\cdots(x_i-x_n)}$ при попарно неравных $x_1, \ldots, x_n$.

6) Проверьте корректность *алгоритма Штрассена* для умножения матриц второго порядка. Пусть

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix},$$

$$C = AB = \begin{pmatrix} c_{11} = a_{11}b_{11} + a_{12}b_{21} & c_{12} = a_{11}b_{12} + a_{12}b_{22} \\ c_{21} = a_{21}b_{11} + a_{22}b_{21} & c_{22} = a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

Рассмотрим величины $P_1 = (a_{11} + a_{22})(b_{11} + b_{22})$, $P_2 = (a_{11} + a_{22})b_{11}$, $P_3 = P_2 = a_{11}(b_{12} - b_{22})$, $P_4 = a_{22}(b_{21} + b_{22})$, $P_5 = (a_{11} + a_{12})b_{22}$, $P_6 = (a_{21} - a_{11})(b_{11} + b_{12})$, $P_7 = (a_{12} - a_{22})(b_{11} + b_{12})$

Тогда $c_{11} = P_1 + P_4 - P_5 + P_7$, $c_{12} = P_3 + P_5$, $c_{21} = P_2 + P_4$, $c_{22} = P_1 - P_2 + P_3 + P_6$.

Отметим, что в качестве коэффициентов a_{ij}, b_{ij}, c_{ij} могут стоять элементы произвольного *кольца* (множества, в котором определены операции умножения и сложения, связанные законом *дистрибутивности* т.е. $a(b+c) = ab+ac$ и $(b+c)a = ba+ca$), **в том числе матричные блоки произвольного размера** ибо матрицы образуют кольцо. Итерируя процедуру, можно получить алгоритм умножения матриц порядка 2^n за 7^n элементарных умножений.