Сложение и умножение

Рассмотрим простейший алгоритм сложения двух чисел столбиком. При применении этого алгоритма, например, к числам 1018 и 1105 – когда требуется сложить тысячу восемнадцать и тысячу сто пять в десятичной системе – на вход подается пара (1018, 1105) и мы поступаем так:

$$\begin{array}{r} 1 \\ +\begin{array}{r}1018\\1105\end{array} \\ \hline 2123 \end{array}$$

Произведено шесть элементарных операций по сложению однозначных чисел: 8 + 5 = 13 (три пишем, один «в уме»), 1 + 1 + 0 = 2, 0 + 1 = 1, и, наконец, 1 + 1 = 2. А меньше четырех и нельзя: ведь хоть по разу необходимо было употребить каждую цифру чисел.

А теперь умножим друг на друга два числа (в десятичной системе):

$$\begin{array}{r} \times\begin{array}{r}1011\\1101\end{array} \\ \hline 1011 \\ 0000 \\ 1011 \\ 1011 \\ \hline 1113111 \end{array}$$

Сколько операций мы совершили здесь? Элементарных умножений $4 \times 4 = 16$, и еще некоторое количество сложений. Из этого примера вытекает, что при умножении двух n-значных чисел столбиком нужно произвести n^2 элементарных умножений (n^2 раз заглянуть в таблицу умножения и заведомо не больше по порядку n^2 раз произвести элементарные сложения.)

Упражнение 1. Покажите, что алгоритм деления в столбик n-значного числа на m-значное требует по порядку величины mn элементарных операций (не менее mn и не более $10mn$).

А какова *сложность* процедуры умножения? Каково минимальное необходимое число элементарных операций?

Умножение столбиком известно многие столетия, едва ли еще не со времени выхода в свет «Алгебры» аль-Хорезми. Эта процедура, которую все изучали еще в начальных классах средней школы, выглядит как самый быстрый алгоритм: ведь каждая цифра одного числа должна вроде бы провзаимодействовать с каждой цифрой другого.

Тем не менее, всего тридцать семь лет назад московским математиком Анатолием Александровичем Карацубой (тогда 25-летним молодым ассистентом, а ныне он профессор МГУ, известный специалист по теории чисел) было совершено открытие, которого трудно было ожидать. Он обнаружил метод, куда более эффективный, чем умножение в столбик!

Метод Карацубы

Пусть x и y – два $2n$-значных десятичных числа:

$$x = \left(x_{2n-1}, \ldots, x_0\right),\ y = \left(y_{2n-1}, \ldots, y_0\right),$$

$$x_i, y_i = 0, 1, \ldots 9.$$

Представим их в виде

$$x = 10^n \xi_1 + \xi_0,\ y = 10^n \eta_1 + \eta_0, \quad (i)$$

где ξ_i, η_i – n-значные числа. Воспользовавшись тождеством

$$\left(\xi_1 - \xi_0\right)\left(\eta_0 - \eta_1\right) = $$
$$= -\xi_1\eta_1 - \xi_0\eta_0 + \xi_1\eta_0 + \xi_0\eta_1, \quad (ii)$$

получаем:

$$xy \overset{(i)}{=} \left(10^n \xi_1 + \xi_0\right)\left(10^n \eta_1 + \eta_0\right) \overset{(ii)}{=}$$
$$= \left(10^{2n} + 10^n\right)\xi_1\eta_1 +$$
$$+ 10^n\left(\xi_1 - \xi_0\right)\left(\eta_0 - \eta_1\right) + \left(10^n + 1\right)\xi_0\eta_0.$$

Мы свели задачу умножения $2n$-разрядных чисел к трем операциям для n-разрядных чисел $\xi_1\eta_1$, $\left(\xi_1 - \xi_0\right)\left(\eta_0 - \eta_1\right)$, $\xi_0\eta_0$ и еще к операциям сложения и сдвига.

На первый взгляд может показаться, что выигрыш по сравнению с обычным умножением незначителен – только $3/4$. Но ведь и сами n-значные числа мы будем умножать таким же образом! Поэтому множитель $3/4$ будет возникать при *каждом* удвоении числа разрядов. И, например, при умножении 1024-значных чисел накопится более чем десятикратный выигрыш.

Умножение Карацубы на n-значных числах будет эффективнее умножения в столбик по порядку величины в $C \cdot \left(\frac{3}{4}\right)^{\log_2 n}$ раз. Это дает оценку порядка $n^{\log_2 3} \approx n^{1.6}$ на число операций. В самом деле, пусть $2^k < n < 2^{k-1}$. Тогда $T(n)$ – число необходимых операций для умножения n-значных чисел – оценивается по порядку как $3^k = \left(2^k\right)^{\log_2 3} \approx n^{\log_2 3}$. Можно рассуждать и так. Из нашего построения вытекает рекуррентное неравенство

$$T(2n) \le 3T(n) + cn,$$

из которого легко выводится асимптотическое неравенство

$$T(n) \ll n^{\log_2 3}.$$

Упражнение 2. Проведите соответствующие рассуждения аккуратно.

Продемонстрируем метод Карацубы на примере умножения чисел, с которыми мы оперировали: $1101 \cdot 1011$.

Воспользовавшись тождеством $\left(a_1 - a_0\right)\left(b_0 - b_1\right) = -a_1b_1 - a_0b_0 + a_1b_0 + a_0b_1$, представим четырехзначные числа A и B в виде $A = 10^2 a_1 + a_0$ и $B = 10^2 b_1 + b_0$, где a_0, a_1, b_0, b_1 – двузначные числа. Тогда

$$AB = \left(10^2 a_1 + a_0\right)\left(10^2 b_1 + b_0\right) =$$
$$= \left(10^4 + 10^2\right)a_1b_1 +$$
$$+ 10^2\left(a_1 - a_0\right)\left(b_0 - b_1\right) + \left(10^2 + 1\right)a_0b_0.$$

Видно, что достаточно произвести всего три умножения двузначных чисел $a_1 \times b_1$, $\left(a_1 - a_0\right) \times \left(b_0 - b_1\right)$ и $a_0 \times b_0$, на каждое из которых мы затратим не больше четырех элементарных умножений, т.е. всего мы затратим 12 умножений вместо 16 (и некоторое количество сложений).

В нашем случае

$$a_1 = 11,\ a_0 = 1,\ b_1 = 10,\ b_0 = 11,$$

откуда

$$1101 \cdot 1011 =$$
$$= \left(10^2 \cdot 11 + 1\right) \cdot \left(10^2 \cdot 10 + 11\right) =$$
$$= \left(10^4 + 10^2\right) \cdot 11 \cdot 10 + 10^2 \cdot 10 \cdot 1 +$$
$$+ \left(10^2 + 1\right) \cdot 1 \cdot 11 = 1113111.$$

Числа и многочлены

Первоначально метод Карацубы выглядел трюком. Но в следующем, 1963 году студент механико-математического факультета МГУ Андрей Тоом (он был участником первой международной математической олимпиады 1959 года, где получил третью премию) осознал природу этого метода и нашел его замечательное обобщение.

В чем идея метода Карацубы и Тоома? Известно, что многие свойства чисел и многочленов очень похожи. Многие проблемы, связанные с уравнениями, сперва решались для многочленов. Посмотрим на десятич-