ную запись некоторого числа x:

$$x = x_0 + x_1 10^1 + x_2 10^2 + \ldots + x_n 10^n,$$

где x_i – цифры. Не правда ли, это очень похоже на запись многочлена? Да и умножению в столбик чисел соответствует умножение в столбик многочленов. (Разница только в отсутствии переноса разрядов у многочленов.)

А нельзя ли два многочлена умножить быстрее, чем в столбик, используя меньшее число умножений коэффициентов? Оказывается, можно! Пусть $P(t)$ и $Q(t)$ – два многочлена степеней m и n соответственно. Тогда их произведение $P(t)Q(t)$ есть многочлен степени $m+n$. А он определяется своими значениями в $m+n+1$ точке. Например, в точках $0, \pm 1, \pm 2, \ldots, \pm(m+n)$. Поэтому, чтобы найти многочлен PQ, ищем значения P и Q в этих точках и перемножаем (получается $m+n+1$ умножение). Тем самым мы найдем значения PQ в $m+n+1$ точке, по которым восстанавливается PQ и находятся все его коэффициенты.

Например, пусть $P(t) = At + B$, $Q(t) = Ct + D$ – линейные двучлены. Их произведение – квадратный трехчлен $PQ(t) = (AC)t^2 + (BC + AD)t + (BD)$. Найдем его коэффициенты.

1. Находим $BD = P(0)Q(0)$ – первое умножение.

2. Находим $(A+B)(C+D) = P(1)Q(1)$ – второе умножение.

3. Находим $(B-A)(D-C) = P(-1)Q(-1)$ – третье умножение.

Беря полуразность выражений $(A+B)(C+D)$ и $(B-A)(D-C)$, находим второй коэффициент PQ, т.е. $BC + AD$, а вычитая BD из полусуммы $(A+B)(C+D)$ и $(B-A)(D-C)$, находим AC. И мы пришли почти что к формулам Карацубы![1]

Идея метода Карацубы – Тоома заключается в том, чтобы разбить запись $2n$-значных чисел $X = AB$, $Y = CD$ на блоки по n разрядов. Тем самым числа X и Y представляются в виде $At + B$ и $Ct + D$, где $t = 10^n$ для десятичной системы счисления (в общем случае $t = q^n$, q – основание системы счисления). А после этого можно перемножить полученные (линейные) многочлены.

Теперь ясно, как обобщить этот метод. Попробуем разбивать числа не на два, а на большее число блоков. Например, на три. Пусть $x_1 = \overline{A_1B_1C_1}$, $x_2 = \overline{A_2B_2C_2}$ – разбиение $3n$-значных чисел x_1, x_2 на блоки по n разрядов. Пусть $t = 10^n$. Тогда числа x_1, x_2 можно представить в виде $P(t) = A_1t^2 + B_1t + C_1$ и $Q(t) = A_2t^2 + B_2t + C_2$ соответственно. Будем действовать, как в предыдущем случае. Найдем произведение многочленов P и Q. Для этого найдем их значения в точках $0, \pm 1, \pm 2$ и перемножим. Получится 5 умножений k-значных чисел (и еще несколько сложений и умножений на 2 и 4). Далее, зная значения многочлена PQ в этих точках, найдем его коэффициенты. Они получаются путем умножения и деления на небольшие числа. Это требует не более 40 сложений (см. упражнение 1).

Таким образом, мы свели задачу умножения $3n$-разрядных чисел к пяти операциям для n-разрядных чисел и еще к операциям сложения, деления на маленькие числа и сдвига. Это дает оценку порядка $n^{\log_3 5}$ на число операций. В самом деле, пусть $3^k < n < 3^{k+1}$. Тогда $T(n)$ (число необходимых операций для умножения n-значных чисел) оценивается по порядку как

$$5^k = \left(3^k\right)^{\log_3 5} \approx n^{\log_3 5} \approx n^{1.3}.$$

Упражнения

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

4. Пусть e – фиксированное натуральное число.

а) Докажите, что алгоритм «умножения в столбик» n-значных чисел на число e имеет сложность порядка n. Его сложность можно оценить величиной $10k \cdot n$, где k – число разрядов в числе e.

б) Докажите, что алгоритм «деления в столбик» n-значных чисел на число e имеет сложность порядка n. Его сложность можно оценить величиной $10k \cdot n$, где k – число разрядов в числе e.

5. Покажите, что для нахождения произведения двух квадратных трехчленов с n-значными коэффициентами достаточно ограничиться $5n$-значными умножениями и $30n$ элементарными операциями.

6. Докажите рекуррентное неравенство

$$T(3n) \le 5T(n) + 30n.$$

Выведите из него асимптотическое неравенство

$$T(n) \ll n^{\log_3 5}.$$

Естественно, десятичную запись чисел можно разбивать не на три, а на большее число блоков. Проведем общее рассуждение. Пусть x и y – два $n(r+1)$-значных числа. Представим их в виде

$$x = 10^{rn}\xi_r + \ldots + 10^n\xi_1 + \xi_0,$$

$$y = 10^{rn}\eta_r + \ldots + 10^n\eta_1 + \eta_0$$

и положим

$$p(t) = \sum_{k=0}^{r} \xi_k t^k,\ q(t) = \sum_{k=0}^{r} \eta_k t^k,$$

$$s(t) = \sum_{k=0}^{2r} \varsigma_k t^k \Rightarrow xy = s\left(10^n\right).$$

В следующем пункте будет показано, что

Коэффициенты полинома $s(\cdot)$ вычисляются через линейные выражения от $2r+1$ чисел $\{p(k)q(k)\}_{k=0}^{2r}$, и это требует $C(r)n$ операций.

Таким образом, нахождение произведения $n(r+1)$-значных чисел требует $2r+1$ «больших умножений» $(n + D_r)$-значных чисел, где D_r – некоторая константа, зависящая от r, и $C(r)n$ элементарных операций.

Упражнение 7. Докажите, что константу D_r можно положить равной числу знаков в числе $r^{r+1} = r \cdot t^r$, $t = r$.

В итоге приходим к оценке

$$T((r+1)n) \le (2r+1)T(n + D_r) + cn.$$

Пусть

$$(r+1)^s \le n \le (r+1)^{s+1}.$$

Тогда легко видеть, что при некотором α_r имеет место неравенство

$$T(n) \le \alpha_r (2r+1)^s,$$

из которого вытекают асимптотические соотношения

$$T(n) \ll n^{\log_{r+1}(2r+1)} \ll n^{1+\log_{r+1} 2}.$$

Поскольку для любого наперед заданного ε при достаточно большом r верно неравество $r^\varepsilon > 3$, то $r^{1+\varepsilon} > 3r$. Теперь ясно, что можно выбрать такое r, что при достаточно больших n выполняется неравенство

$$T(n) < n^{1+\varepsilon}.$$

Мы получили такой результат:

Теорема (А.Тоом). *Для любого $\varepsilon > 0$ существует такая постоянная $c(\varepsilon)$ и такой метод умножения, что число элементарных операций $T(n)$, которые необходимо выполнить, чтобы умножить два n-разрядных числа, удовлетворяет оценке*

$$T(n) \le c(\varepsilon) n^{1+\varepsilon}.$$

Чтобы доказать теорему Тоома и построить алгоритм быстрого умно-

[1] *Разница только в том, что мы брали $(B-A)(D-C)$ – значение в (-1), а Карацуба вместо этого брал AC – коэффициент при главном члене на бесконечности.*