Тема 4. Умножение чисел

С. Б. Гашков, И. С. Сергеев

Стандартный (машинный) метод умножения основан на известном школьном приеме: один из множителей последовательно умножается на разряды другого, соответствующим образом сдвинутые результаты записываются друг под другом и затем складываются. Умножение чисел 26 и 21 в этой интерпретации будет выглядеть так:

					1	1	0	1	0
					1	0	1	0	1
					1	1	0	1	0
				0	0	0	0	0	
			1	1	0	1	0		
		0	0	0	0	0			
	1	1	0	1	0				
1	0	0	0	1	0	0	0	1	0

Сложность умножения n-разрядных чисел этим способом, как легко проверить, составляет по порядку n^2 операций. Квадратичный порядок сложности казался естественным для умножения до 1961 г., когда А. А. Карацуба предложил метод, в основе которого лежит идея «деления пополам»: представим $2n$-разрядные числа a и b в виде $a_1 2^n + a_0$ и $b_1 2^n + b_0$ соответственно, где $a_i, b_i < 2^n$. Тогда произведение ab согласно формуле

$$ab = a_1 b_1 2^{2n} + ((a_1 + a_0)(b_1 + b_0) - a_1 b_1 - a_0 b_0)2^n + a_0 b_0$$

можно свести к трем умножениям чисел вдвое меньшей длины. Рекурсивное применение этого приема в конечном счете приводит к оценке сложности $O(n^{\log_2 3})$, где $\log_2 3 < 1,585$.

В 1963 г. А. Л. Тоом обобщил прием Карацубы, сведя умножение kn-разрядных чисел к $2k - 1$ умножениям $(n + O(1))$-разрядных, что

позволило получить новую оценку сложности умножения в виде $c^{\sqrt{\log n}}n$. В основе метода Тоома лежит идея интерполяции: перехода от кодирования многочлена набором его коэффициентов к кодированию набором значений в определенных точках. Развитие идеи интерполяции привело в конце 60-х гг. к появлению быстрых алгоритмов умножения при помощи ДПФ. Подробно рассмотрим метод Шёнхаге—Штрассена, опубликованный в 1971 г. и остававшийся асимптотически наилучшим известным способом умножения вплоть до 2007 г.

1 Арифметика в кольце вычетов по модулю числа Ферма

Рассмотрим кольцо $\mathbb{Z}_{2^{2^n}+1}$. Пусть элементы этого кольца представляются 2^{n+1}-разрядными числами, а операции с ними производятся по модулю $2^{2^{n+1}} - 1 = (2^{2^n} - 1)(2^{2^n} + 1)$. Вычету $\overline{a} \in \mathbb{Z}_{2^{2^n}+1}$ в таком представлении может соответствовать любое из чисел

$$\{a + b(2^{2^n} + 1) \mid b \in \mathbb{Z}\} \cap \{0, \ldots, 2^{2^{n+1}} - 1\}.$$

Далее для простоты изложения в качестве элементов кольца вычетов будем использовать числа-представители эквивалентных классов (по модулю $2^{2^n} + 1$).

Заметим, что двойка является примитивным корнем степени 2^{n+1} в кольце $\mathbb{Z}_{2^{2^n}+1}$. Действительно, $2^{2^{n+1}} \equiv 1$, а $2^{2^n} - 1$ не является делителем нуля в силу взаимной простоты чисел $2^{2^n} \pm 1$.

Лемма 1. *Любая из операций сложения, вычитания и умножения на 2^k в кольце $\mathbb{Z}_{2^{2^n}+1}$ выполняется со сложностью $O(2^n)$.*

Доказательство. Действительно, умножение на степень двойки реализуется простым циклическим сдвигом разрядов числа-элемента кольца. Сложность циклического сдвига можно принять равной нулю, если исходить из схемной модели вычислений, либо $O(2^n)$ в случае программной реализации.

Рассмотрим операцию сложения чисел $x, y \in [0, \ldots, 2^{2^{n+1}} - 1]$. Положим $z' = x + y \leq 2(2^{2^{n+1}} - 1)$; обозначим через z'_1 старший 2^{n+1}-й разряд числа z' (нумерация с нуля), а через z'_0 — число, получаемое из z' удалением этого разряда. Тогда число

$$z = z'_0 + z'_1 = z' - z'_1(2^{2^{n+1}} - 1) = (x + y) \bmod \left(2^{2^{n+1}} - 1\right)$$

в кольце $\mathbb{Z}_{2^{2^n}+1}$ представляет сумму $x+y$. Ясно, что сложность вычисления z по порядку совпадает со сложностью обычного сложения 2^{n+1}-разрядных чисел и составляет, следовательно, $O(2^n)$.

Вычитание может быть сведено к умножению на 2^{2^n} и сложению в силу тождества $x - y \equiv x + 2^{2^n} y \bmod (2^{2^n}+1)$. Лемма доказана.

Следствие 1. *Пусть $k \le n+1$. Сложность ДПФ порядка 2^k над кольцом $\mathbb{Z}_{2^{2^n}+1}$ составляет $O(k2^{n+k})$.*

Помимо арифметических операций, следует остановиться еще на двух. Первая состоит в вычислении канонического представителя класса вычетов — числа из $[0, \ldots, 2^{2^n}]$ — по некоторому представлению, что эквивалентно операции приведения по модулю $2^{2^n}+1$. Пусть $x = u + v2^{2^n}$, где $0 \le u, v < 2^{2^n}$. Тогда

$$x \bmod (2^{2^n}+1) = \begin{cases} u - v, & u \ge v, \\ 2^{2^n} + 1 + u - v, & u < v. \end{cases}$$

Ясно, что вычисления по этой формуле сводятся к вычитаниям и сложениям и могут быть выполнены со сложностью $O(2^n)$.

Лемма 2. *Пусть $0 \le \xi \le 2^{2^n}$, $0 \le \eta < 2^k$ и $k \le 2^n$. Тогда нахождение числа $z \in [0, \ldots, 2^k(2^{2^n}+1) - 1]$ по остаткам ξ и η от деления соответственно на $2^{2^n}+1$ и 2^k может быть реализовано со сложностью $O(2^n)$.*

Доказательство. Число z можно вычислить по формуле

$$z = \xi + \left((\eta - \xi) \bmod 2^k\right)\left(2^{2^n}+1\right)$$

со сложностью $O(2^n)$. Несложно проверить, что z находится в условленных пределах и имеет заданные остатки от деления на $2^{2^n}+1$ и 2^k. Лемма доказана.

2 Метод Шёнхаге—Штрассена

Умножение N-разрядных чисел можно выполнить при помощи алгоритма умножения в кольце $\mathbb{Z}_{2^{2^m}+1}$, где $2^m \ge 2N$. В методе Шёнхаге—Штрассена умножение в кольце $\mathbb{Z}_{2^{2^m}+1}$ сводится к умножениям в кольце

$\mathbb{Z}_{2^{2^n}+1}$, где $n = \lceil (m+1)/2 \rceil$. Выделяются случаи нечетного и четного m. Рассмотрим более подробно первый случай.

Итак, пусть $m = 2n-1$. Перемножаемые 2^{m+1}-разрядные числа (элементы кольца $\mathbb{Z}_{2^{2^m}+1}$) обозначим через a и b. Разобьем их на блоки длины 2^{n-1}:

$$a = \sum_{i=0}^{2^{n+1}-1} a_i 2^{i2^{n-1}}, \quad b = \sum_{i=0}^{2^{n+1}-1} b_i 2^{i2^{n-1}}, \quad 0 \le a_i, b_i < 2^{2^{n-1}}.$$

Тогда

$$ab = \sum_{i=0}^{2^{n+1}-1} c_i 2^{i2^{n-1}} \bmod (2^{2^m}+1), \quad c_i = \sum_{\substack{\rho+\sigma \equiv i \bmod 2^{n+1} \\ 0 \le \rho, \sigma < 2^{n+1}}} a_\rho b_\sigma, \qquad (1)$$

поскольку

$$2^{(\rho+\sigma)2^{n-1}} \equiv 2^{(\rho+\sigma \bmod 2^{n+1})2^{n-1}} \bmod (2^{2^m}+1).$$

Очевидно, $0 \le c_i < 2^{n+1+2^n}$.

Если заметить, что

$$2^{2^n \cdot 2^{n-1}} = 2^{2^m} \equiv -1 \bmod (2^{2^m}+1),$$

то формулу (1) можно переписать в виде

$$ab = \sum_{i=0}^{2^n-1} (c_i - c_{i+2^n}) 2^{i2^{n-1}} \bmod (2^{2^m}+1) =$$

$$\sum_{i=0}^{2^n-1} \underbrace{(c_i - c_{i+2^n} + 2^{n+1+2^n})}_{z_i} 2^{i2^{n-1}} + \sum_{i=2^n}^{2^{n+1}-1} \underbrace{2^{n+1+2^n}}_{z_i} \cdot 2^{i2^{n-1}} \bmod (2^{2^m}+1) =$$

$$\sum_{i=0}^{2^{n+1}-1} z_i 2^{i2^{n-1}} \bmod (2^{2^m}+1).$$

Ясно, что $0 \le z_i < 2^{n+2+2^n}$. При $n \ge 2$ выполняется $n+2+2^n \le 2^{n+1}$, т.е. для записи числа z_i достаточно 2^{n+1} двоичных разрядов.

Процесс вычислений распадается на две части: вычисление z_i и восстановление ab. Рассмотрим эти части в обратном порядке.

2.1 Часть II. Восстановление произведения из z_i

Пусть

$$ab = \sum_{i=0}^{2^{n+1}-1} w_i 2^{i2^{n-1}}, \quad 0 \le w_i < 2^{2^{n-1}}.$$

По существу, задача состоит в вычислении блоков w_i по известным z_i. Произведение ab можно представить в виде суммы четырех слагаемых A_j:

$$A_j = \sum_{i=0}^{2^{n-1}-1} z_{4i+j} 2^{i2^{n+1}}, \quad j = 0, \ldots, 3.$$

Блоки z_i в каждом из этих слагаемых не пересекаются, поскольку имеют длину не более 2^{n+1}. Поскольку сложение в кольце $\mathbb{Z}_{2^{2^m}+1}$ имеет линейную сложность (см. лемму 1), получаем для сложности второй части оценку $O(2^m)$.

2.2 Часть I. Вычисление z_i

В силу $0 \le z_i < 2^{n+2}(2^{2^n}+1)$ для вычисления z_i достаточно вычислить остатки от деления z_i на числа 2^{n+2} и $2^{2^n}+1$ и затем воспользоваться леммой 2. Согласно лемме 2, сложность восстановления всех z_i равна $2^n O(2^n) = O(2^{2n})$. Оценим сложность вычисления $z_i \bmod 2^{n+2}$ и $z_i \bmod 2^{2^n}+1$.

а) *Вычисление* $z_i \bmod 2^{n+2}$.

Обозначим

$$\alpha_i = a_i \bmod 2^{n+2}, \qquad \beta_i = b_i \bmod 2^{n+2}$$

и положим

$$u = \sum_{i=0}^{2^{n+1}-1} \alpha_i 2^{i(3n+5)}, \qquad v = \sum_{i=0}^{2^{n+1}-1} \beta_i 2^{i(3n+5)}.$$

Тогда

$$uv = \sum_{i=0}^{2^{n+1}-1} \gamma_i 2^{i(3n+5)}, \qquad \gamma_i = \sum_{\rho+\sigma=i} \alpha_\rho \beta_\sigma.$$

При этом в сумме, выражающей uv, слагаемые не накладываются друг на друга в силу

$$\gamma_i < 2^{n+1}(2^{n+2})^2 = 2^{3n+5}.$$

Поэтому все γ_i могут быть восстановлены из uv с нулевой сложностью.

По построению,

$$c_i \equiv \gamma_i + \gamma_{i+2^{n+1}} \mod 2^{n+2},$$

следовательно,

$$z_i \equiv \gamma_i + \gamma_{i+2^{n+1}} - \gamma_{i+2^n} - \gamma_{i+3\cdot 2^n} \mod 2^{n+2}. \tag{2}$$

Окончательно, сложность вычисления всех $z_i \bmod 2^{n+2}$ можно оценить сложностью умножения $(3n+5)2^{n+1}$-разрядных чисел u и v плюс $O(n2^n)$ операций для реализации сложений-вычитаний (2). Умножение можно реализовать при помощи алгоритма умножения в кольце $\mathbb{Z}_{2^{2^{m'}}+1}$, где $m' = n + \lceil \log_2 n \rceil + 5$, т.к. $3n+5 \le 8n \le 2^{\lceil \log_2 n \rceil + 3}$.

б) *Вычисление* $z_i \bmod 2^{2^n}+1$.

При $0 \le i < 2^n$, учитывая, что $2^{2^n} \equiv 2^{-2^n} \equiv -1 \mod (2^{2^n}+1)$, запишем

$$\begin{aligned}
\hat{c}_i = 2^i(c_i - c_{i+2^n}) \equiv \\
\equiv \sum_{\substack{\rho+\sigma \equiv i \bmod 2^{n+1} \\ 0 \le \rho,\sigma < 2^{n+1}}} (2^\rho a_\rho)(2^\sigma b_\sigma) - 2^{-2^n} \sum_{\substack{\rho+\sigma \equiv i+2^n \bmod 2^{n+1} \\ 0 \le \rho,\sigma < 2^{n+1}}} (2^\rho a_\rho)(2^\sigma b_\sigma) \equiv \\
\equiv \sum_{\substack{\rho+\sigma \equiv i \bmod 2^{n} \\ 0 \le \rho,\sigma < 2^{n+1}}} (2^\rho a_\rho)(2^\sigma b_\sigma) \equiv \\
\equiv \sum_{\substack{\rho+\sigma \equiv i \bmod 2^{n} \\ 0 \le \rho,\sigma < 2^{n}}} (2^\rho a_\rho - 2^\rho a_{\rho+2^n})(2^\sigma b_\sigma - 2^\sigma b_{\sigma+2^n}) \mod (2^{2^n}+1).
\end{aligned}$$

Далее в этом пункте все вычисления выполняются по модулю $2^{2^n}+1$.

Положим

$$\hat{a}_i = 2^i(a_i - a_{i+2^n}), \qquad \hat{b}_i = 2^i(b_i - b_{i+2^n}).$$

Справедливо

$$\left(\sum_{i=0}^{2^n-1}\hat{a}_i x^i\right)\left(\sum_{i=0}^{2^n-1}\hat{b}_i x^i\right)=\sum_{i=0}^{2^{n+1}-1}\left(\sum_{\rho+\sigma=i}\hat{a}_\rho\hat{b}_\sigma\right)x^i\equiv$$
$$\equiv\sum_{i=0}^{2^n-1}\left(\sum_{\rho+\sigma\equiv i \bmod 2^n}\hat{a}_\rho\hat{b}_\sigma\right)x^i=\sum_{i=0}^{2^n-1}\hat{c}_i x^i \mod (x^{2^n}-1).$$

Приведенная выкладка показывает, что для нахождения $\hat{c}_i$ можно воспользоваться ДПФ порядка 2^n. Вычисляем:

$$(a_0^*,\ldots,a_{2^n-1}^*)=\text{ДПФ}_{2^n,4}(\hat{a}_0,\ldots,\hat{a}_{2^n-1}),$$

$$(b_0^*,\ldots,b_{2^n-1}^*)=\text{ДПФ}_{2^n,4}(\hat{b}_0,\ldots,\hat{b}_{2^n-1}),$$

$$(\hat{c}_0,\ldots,\hat{c}_{2^n-1})=\text{ДПФ}_{2^n,4^{-1}}(a_0^*b_0^*,\ldots,a_{2^n-1}^*b_{2^n-1}^*).$$

Общая сложность вычислений в этом пункте складывается из $O(2^{2n})$ операций (вычисление $\hat{a}_i$, $\hat{b}_i$), $O(n2^{2n})$ операций (реализация ДПФ) и 2^n умножений в $\mathbb{Z}_{2^{2^n}+1}$.

2.3 Сложность метода умножения

Случай $m=2n-1$ расмотрен полностью. Случай $m=2n-2$ рассматривается аналогично, только числа a и b разбиваются на 2^n блоков длины 2^{n-1} и, в конечном счете, умножение в $\mathbb{Z}_{2^{2^m}+1}$ сводится к 2^{n-1} умножениям в $\mathbb{Z}_{2^{2^n}+1}$.

В итоге приходим к следующим рекуррентным соотношениям для сложности $\mu(m)$ умножения в $\mathbb{Z}_{2^{2^m}+1}$:

$$\mu(2n-1)\le 2^n\mu(n)+\mu(n+\lceil\log_2 n\rceil+5)+\gamma_0(n-1)2^{2n}, \tag{3}$$

$$\mu(2n-2)\le 2^{n-1}\mu(n)+\mu(n+\lceil\log_2 n\rceil+4)+\gamma_0(n-1)2^{2n-1} \tag{4}$$

при подходящей константе γ_0.

Покажем по индукции, что существует постоянная γ, такая, что

$$\mu(n)\le\gamma k2^{n+k} \tag{5}$$

при $n\le 2^k+1$.

Выберем произвольное $\epsilon \in (0, 1)$. Определим n_0 так, что для всех $n \geq n_0$ выполняется $(k+1)2^{k+7-n} < \epsilon$. Заметим, что при этом выполняется $n+k+6 < 2n-1$. Определим γ' так, чтобы при $n < n_0$ было справедливо $\mu(n) \leq \gamma' k 2^{n+k}$. Наконец, положим $\gamma = \max\{\gamma', \frac{\gamma_0}{1-\epsilon}\}$.

В основание индукции положим случай $n < n_0$, в котором соотношение (5) выполняется в силу определения γ. Проверим индуктивный переход при нечетном аргументе (3); четный случай (4) проверяется аналогично:

$$\begin{aligned}\mu(2n-1) &\leq 2^n \gamma k 2^{n+k} + \gamma(k+1)2^{n+2k+7} + \gamma_0 2^{2n+k} = \\ &= 2^{2n+k}\left(\gamma k + \gamma_0 + \gamma(k+1)2^{k+7-n}\right) \leq \\ &\leq 2^{2n+k}(\gamma k + (1-\epsilon)\gamma + \epsilon\gamma) \leq \gamma(k+1)2^{2n+k},\end{aligned}$$

что и требовалось доказать.

3 Заключение

Полученная оценка сложности умножения в кольце $\mathbb{Z}_{2^{2^n}+1}$ приводит к оценке $O(n \log n \log\log n)$ сложности умножения n-разрядных чисел. В 2007 г. М. Фюрер опубликовал новый метод умножения чисел с оценкой сложности $nc^{\log^* n} \log n$, где $\log^* n$ — сверхлогарифм, очень медленно растущая функция, определяемая из соотношения:

$$\lfloor \underbrace{\log \ldots \log}_{\log^* n} n \rfloor = 1.$$