Длинная арифметика

Дискретный анализ 2012/13

Андрей Калинин, Татьяна Романова

16 февраля 2013 г.

Классические алгоритмы

- Сложение
- Вычитание
- Умножение
- Деление

Быстрое умножение

- Алгоритм Карацубы

Литература

- Дональд Кнут, «Искусство программирования», том 2, «Получисленные алгоритмы», 3-е издание. Глава 4.3, «Арифметика многкратной точности», стр. 304–335.

База

- Целые числа представляются в системе счисления по основанию b, не превышающему машинное слово.
- В наличии:
  1. Сложение и вычитание одноразрядных целых чисел с получением одноразрядного результата и разряда переноса.
  2. Перемножение двух одноразрядных чисел с получением двухразрядного результата.
  3. Деление двухразрядного целого числа на одноразрядное, дающее одноразрядное частное и одноразрядный остаток.
- Считаем числа неотрицательными.

Раздел

Задача

Дано:

- $u = (u_{n-1} \dots u_1 u_0)_b$
- $v = (v_{n-1} \dots v_1 v_0)_b$

Нужно найти число

$$w = u + v$$

в представлении

$$w = (w_n w_{n-1} \dots w_1 w_0)_b.$$

Здесь w_n — разряд переноса, равный 0 или 1.

Алгоритм сложения

1 $k \leftarrow 0$
2 **for** $j \leftarrow 0$ **to** $n-1$
3 $\quad w_j \leftarrow (u_j + v_j + k) \mod b$
4 $\quad k \leftarrow \lfloor (u_j + v_j + k)/b \rfloor$
5 $w_n \leftarrow k$

Раздел

Задача

Дано:

- $u = (u_{n-1} \dots u_1 u_0)_b$
- $v = (v_{n-1} \dots v_1 v_0)_b$
- $u \geq v$

Нужно найти число

$$w = u - v$$

в представлении

$$w = (w_{n-1} \dots w_1 w_0)_b.$$

Алгоритм вычитания

1 $k \leftarrow 0$
2 **for** $j \leftarrow 0$ **to** $n-1$
3 $\quad w_j \leftarrow (u_j - v_j + k) \mod b$
4 $\quad k \leftarrow \lfloor (u_j - v_j + k)/b \rfloor$

В конце алгоритма $k = 0$, по начальному предположению $u \geq v$.

Раздел

Задача

Дано:

- $u = (u_{m-1} \dots u_1 u_0)_b$
- $v = (v_{n-1} \dots v_1 v_0)_b$

Нужно найти число

$$w = u \times v$$

в представлении

$$w = (w_{m+n-1} \dots w_1 w_0)_b.$$

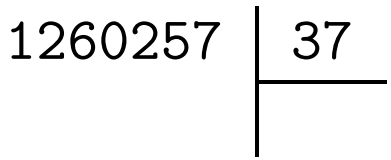
Алгоритм умножения

```
1  (w_{m-1}, w_{m-2}, ..., w_0) ← (0, 0, ..., 0)
2  for j ← 0 to n − 1
3      if v_j ≠ 0
4          k ← 0
5          for i ← 0 to m − 1
6              t ← u_i × v_j + w_{i+j} + k
7              w_{i+j} ← t mod b
8              k ← ⌊t/b⌋
9          w_{j+m} ← k
```

Алгоритм работает за $O(nm)$, есть значительно более быстрые алгоритмы.

Раздел

Пример деления столбиком



Пример деления столбиком

1260257	37
111	3
15	

Пример деления столбиком

1260257	37
111	3
150	

Пример деления столбиком

1260257	37
111	34
150	
148	
2	

Пример деления столбиком

1260257	37
111	340
150	
148	
22	

Пример деления столбиком

1260257	37
111	340
150	
148	
225	

Пример деления столбиком

1260257	37
111	3406
150	
148	
225	
222	
3	

Пример деления столбиком

```
1260257 | 37
111     | 3406
 150
 148
   225
   222
     37
```

Пример деления столбиком

1260257	37
111	34061
150	
148	
225	
222	
37	
37	
0	

Пример деления столбиком

```
1260257 | 37
--------+-----
111     | 34061
 150
 148
   225
   222
     37
     37
      0
```

Самое сложноформализуемое в этом алгоритме — определение следующего разряда частного.

Задача получения следующего разряда

Дано:

- $u = (u_n u_{n-1} \dots u_1 u_0)_b$
- $v = (v_{n-1} \dots v_1 v_0)_b$
- $u/v < b$ (или $(u_n u_{n-1} \dots u_0)_b < (v_{n-1} v_{n-2} \dots v_0)_b$)

Нужно найти число

$$q = \lfloor u/v \rfloor$$

Угадывание q

Положим

$$\hat{q} = \min\left(\left\lfloor \frac{u_n b + u_{n-1}}{v_{n-1}} \right\rfloor, b - 1\right)$$

Угадывание q

Положим

$$\hat{q} = \min\left(\left\lfloor \frac{u_n b + u_{n-1}}{v_{n-1}} \right\rfloor, b - 1\right)$$

Как это ни странно, такое приближение даёт хорошие результаты. Покажем это.

Теорема

$$\hat{q} = \min\left(\left\lfloor \frac{u_n b + u_{n-1}}{v_{n-1}} \right\rfloor, b-1\right) \geq q$$

Доказательство.

$$\hat{q} = b-1 \quad \Rightarrow \quad \hat{q} \geq q.$$

Теорема

$$\hat{q} = \min\left(\left\lfloor \frac{u_n b + u_{n-1}}{v_{n-1}} \right\rfloor, b-1\right) \geq q$$

Доказательство.

$\hat{q} = b - 1 \quad \Rightarrow \quad \hat{q} \geq q.$

$\hat{q} = \lfloor (u_n b + u_{n-1})/v_{n-1} \rfloor \quad \Rightarrow \quad \hat{q} v_{n-1} \geq u_n b + u_{n-1} - v_{n-1} + 1.$

Теорема

$$\hat{q} = \min\left(\left\lfloor \frac{u_n b + u_{n-1}}{v_{n-1}} \right\rfloor, b-1\right) \geq q$$

Доказательство.

$$\hat{q} = b-1 \quad \Rightarrow \quad \hat{q} \geq q.$$

$$\hat{q} = \lfloor (u_n b + u_{n-1})/v_{n-1} \rfloor \quad \Rightarrow \quad \hat{q} v_{n-1} \geq u_n b + u_{n-1} - v_{n-1} + 1.$$

$$\begin{aligned} u - \hat{q}v &\leq u - \hat{q} v_{n-1} b^{n-1} \\ &\leq u_n b^n + \cdots + u_0 - (u_n b^n + u_{n-1} b^{n-1} - v_{n-1} b^{n-1} + b^{n-1}) \\ &= u_{n-2} b^{n-2} + \cdots + u_0 - b^{n-1} + v_{n-1} b^{n-1} \\ &< v_{n-1} b^{n-1} \leq v \end{aligned}$$

Теорема

$$\hat{q} = \min\left(\left\lfloor \frac{u_n b + u_{n-1}}{v_{n-1}} \right\rfloor, b-1\right) \geq q$$

Доказательство.

$\hat{q} = b-1 \quad \Rightarrow \quad \hat{q} \geq q.$

$\hat{q} = \lfloor (u_n b + u_{n-1})/v_{n-1} \rfloor \quad \Rightarrow \quad \hat{q} v_{n-1} \geq u_n b + u_{n-1} - v_{n-1} + 1.$

$$\begin{aligned} u - \hat{q}v &\leq u - \hat{q} v_{n-1} b^{n-1} \\ &\leq u_n b^n + \cdots + u_0 - (u_n b^n + u_{n-1} b^{n-1} - v_{n-1} b^{n-1} + b^{n-1}) \\ &= u_{n-2} b^{n-2} + \cdots + u_0 - b^{n-1} + v_{n-1} b^{n-1} \\ &< v_{n-1} b^{n-1} \leq v \end{aligned}$$

$u - \hat{q}v < v \quad \Rightarrow \quad \hat{q} \geq q$ (т.к. $0 \leq u - qv < v$). $\square$

Насколько $\hat{q}$ больше q?

Преположим, что $\hat{q} \geq q + 3$. Тогда:

$$\hat{q} \leq \frac{u_n b + u_{n-1}}{v_{n-1}} = \frac{u_n b^n + u_{n-1} b^{n-1}}{v_{n-1} b^{n-1}} \leq \frac{u}{v_{n-1} b^{n-1}} < \frac{u}{v - b^{n-1}}$$

Насколько $\hat{q}$ больше q?

Преположим, что $\hat{q} \geq q + 3$. Тогда:

$$\hat{q} \leq \frac{u_n b + u_{n-1}}{v_{n-1}} = \frac{u_n b^n + u_{n-1} b^{n-1}}{v_{n-1} b^{n-1}} \leq \frac{u}{v_{n-1} b^{n-1}} < \frac{u}{v - b^{n-1}}$$

Т.к. $q > (u/v) - 1$, то:

$$3 \leq \hat{q} - q < \frac{u}{v - b^{n-1}} - \frac{u}{v} + 1 = \frac{u}{v}\left(\frac{b^{n-1}}{v - b^{n-1}}\right) + 1$$

Насколько $\hat{q}$ больше q?

Преположим, что $\hat{q} \geq q + 3$. Тогда:

$$\hat{q} \leq \frac{u_n b + u_{n-1}}{v_{n-1}} = \frac{u_n b^n + u_{n-1} b^{n-1}}{v_{n-1} b^{n-1}} \leq \frac{u}{v_{n-1} b^{n-1}} < \frac{u}{v - b^{n-1}}$$

Т.к. $q > (u/v) - 1$, то:

$$3 \leq \hat{q} - q < \frac{u}{v - b^{n-1}} - \frac{u}{v} + 1 = \frac{u}{v}\left(\frac{b^{n-1}}{v - b^{n-1}}\right) + 1$$

Следовательно:

$$\frac{u}{v} > 2\left(\frac{v - b^{n-1}}{b^{n-1}}\right) \geq 2(v_{n-1} - 1)$$

Насколько $\hat{q}$ больше q?

Преположим, что $\hat{q} \geq q + 3$. Тогда:

$$\hat{q} \leq \frac{u_n b + u_{n-1}}{v_{n-1}} = \frac{u_n b^n + u_{n-1} b^{n-1}}{v_{n-1} b^{n-1}} \leq \frac{u}{v_{n-1} b^{n-1}} < \frac{u}{v - b^{n-1}}$$

Т.к. $q > (u/v) - 1$, то:

$$3 \leq \hat{q} - q < \frac{u}{v - b^{n-1}} - \frac{u}{v} + 1 = \frac{u}{v}\left(\frac{b^{n-1}}{v - b^{n-1}}\right) + 1$$

Следовательно:

$$\frac{u}{v} > 2\left(\frac{v - b^{n-1}}{b^{n-1}}\right) \geq 2(v_{n-1} - 1)$$

Поскльку $b - 4 \geq \hat{q} - 3 \geq q = \lfloor u/v \rfloor \geq 2(v_{n-1} - 1)$, то $v_{n-1} < \lfloor b/2 \rfloor$.

Теорема

Если $v_{n-1} \geq \lfloor b/2 \rfloor$, *то* $\hat{q} - 2 \leq q \leq \hat{q}$.

Теорема

Если $v_{n-1} \geq \lfloor b/2 \rfloor$, *то* $\hat{q} - 2 \leq q \leq \hat{q}$.

Следствия:

1. Условие теоремы не зависит от того, насколько велико b: подобранное частное $\hat{q}$ не отличается от истинного более чем на 2.

Теорема

Если $v_{n-1} \geq \lfloor b/2 \rfloor$, *то* $\hat{q} - 2 \leq q \leq \hat{q}$.

Следствия:

1. Условие теоремы не зависит от того, насколько велико b: подобранное частное $\hat{q}$ не отличается от истинного более чем на 2.
2. Любые входные данные можно преобразовать таким образом, чтобы выполнялось условие теоремы. Например, можно домножить u и v на $\lfloor b/(v_{n-1}+1) \rfloor$. Это не изменит значения u/v и не увеличит количество разрядов в v, при этом новое v_{n-1} станет достаточно велико.

Дополнительные условия

$\hat{r} = u_n b + u_{n-1} - \hat{q} v_{n-1}$. Предположим, что $v_{n-1} > 0$.

1. Если $\hat{q} v_{n-2} > b\hat{r} + u_{n-2}$, то $q < \hat{q}$.
2. Если $\hat{q} v_{n-2} \leq b\hat{r} + u_{n-2}$, то $\hat{q} = q$ или $q = \hat{q} - 1$.
3. Если $v_{n-1} \geq \lfloor b/2 \rfloor$ и $\hat{q} v_{n-2} \leq b\hat{r} + u_{n-2}$, но $\hat{q} \neq q$, то $u \bmod v \geq (1 - 2/b)v$, т.е. это событие происходит с вероятностью приблизительно равной $2/b$.

Задача длинного деления

Дано:

- $u = (u_{n+m-1}u_{n-1}\ldots u_1u_0)_b$
- $v = (v_{n-1}\ldots v_1v_0)_b$
- $v_{n-1} \neq 0$, $n > 1$.

Нужно найти числа q и r, такие, что:

$$u = v \times q + r, \quad 0 \leq r < v$$

в представлении

$$q = (q_m q_{m-1}\ldots q_0)_b, \quad r = (r_{n-1}\ldots r_1 r_0)_b$$

Алгоритм длинного деления

1 $d \leftarrow \lfloor b/(v_{n-1}+1) \rfloor$, $u \leftarrow u \times d$, $v \leftarrow v \times d$.
// В u может появиться дополнительный разряд (до $n+m$).
2 **for** $j \leftarrow m$ **downto** 0
3 $\hat{q} \leftarrow \lfloor (u_{j+n}b + u_{j+n-1})/v_{n-1} \rfloor$
4 $\hat{r} \leftarrow (u_{j+n}b + u_{j+n-1}) \mod v_{n-1}$
5 **while** $\hat{r} < b$ and $(\hat{q} = b$ or $\hat{q}v_{n-2} > b\hat{r} + u_{j+n-2})$
6 $\hat{q} \leftarrow \hat{q} - 1$, $\hat{r} \leftarrow \hat{r} + v_{n-1}$
7 $(u_{j+n} \dots u_j)_b \leftarrow (u_{j+n} \dots u_j)_b - \hat{q}(v_{n-1} \dots v_0)_b$
8 $q_j \leftarrow q$
9 **if** $(u_{j+n} \dots u_j)_b < 0$
10 $q_j \leftarrow q_j - 1$
11 $(u_{j+n} \dots u_j)_b \leftarrow (u_{j+n} \dots u_j)_b + (0v_{n-1} \dots v_0)_b$
// Перенос в разряд u_{j+n-1} игнорируется.
12 $r \leftarrow (u_{n-1} \dots u_0)_b / d$

Раздел

Можно ли быстрее, чем за n^2?

Допустим, есть

$$u = (u_{2n-1} \dots u_1 u_0)_2 = (U_1, U_0)_{2^n}, \quad v = (v_{2n-1} \dots v_1 v_0)_2 = (V_1, V_0)_{2^n}$$

Можно переписать:

$$u = 2^n U_1 + U_0, \quad v = 2^n V_1 + V_0$$

Тогда

$$uv = (2^{2n} + 2^n) U_1 V_1 + 2^n (U_1 - U_0)(V_0 - V_1) + (2^n + 1) U_0 V_0.$$

Можно ли быстрее, чем за n^2?

Допустим, есть

$$u = (u_{2n-1} \dots u_1 u_0)_2 = (U_1, U_0)_{2^n}, \quad v = (v_{2n-1} \dots v_1 v_0)_2 = (V_1, V_0)_{2^n}$$

Можно переписать:

$$u = 2^n U_1 + U_0, \quad v = 2^n V_1 + V_0$$

Тогда

$$uv = (2^{2n} + 2^n) U_1 V_1 + 2^n (U_1 - U_0)(V_0 - V_1) + (2^n + 1) U_0 V_0.$$

Т.е., операция умножения $2n$-битных чисел свелась к 3 операциям умножения n-битных чисел и нескольких операций сдвига и сложения.

Быстрое умножение

Этот подход можно использовать для рекурсивного процесса умножения. Допустим, $T(n)$ — время, затрачиваемое на выполнение умножения n-битных чисел. Тогда:

$$T(2n) \leq 3T(n) + cn$$
$$T(2^k) \leq c(3^k - 2^k), \qquad k \geq 1$$

То есть:

$$T(n) \leq T(2^{\lceil \lg n \rceil}) \leq c(3^{\lceil \lg n \rceil} - 2^{\lceil \lg n \rceil}) < 3c \cdot 3^{\lg n} = 3cn^{\lg 3}$$

Быстрое умножение

Этот подход можно использовать для рекурсивного процесса умножения. Допустим, $T(n)$ — время, затрачиваемое на выполнение умножения n-битных чисел. Тогда:

$$T(2n) \leq 3T(n) + cn$$
$$T(2^k) \leq c(3^k - 2^k), \qquad k \geq 1$$

То есть:

$$T(n) \leq T(2^{\lceil \lg n \rceil}) \leq c(3^{\lceil \lg n \rceil} - 2^{\lceil \lg n \rceil}) < 3c \cdot 3^{\lg n} = 3cn^{\lg 3}$$

Можно сократить операцию умножения до $n^{1.585}$