Модулярное деление и вычисление обратного элемента по модулю степени двойки

Еникеев Р.Р.

Казанский (Приволжский) федерельный университет

Обратный элемент для d по модулю p это такое число d^{-1}, которое удовлетворяет равенству

$$d * d^{-1} \equiv 1 \pmod{p}.$$

Для его существования необходимо, чтобы d было взаимно простым с p.

Модулярное деление $\frac{e}{d} \bmod p$ определяется как $e * d^{-1} \bmod p$.

Введение

k-арный алгоритм

k-арный алгоритм для вычисления НОД $u > v > 0$ состоит из:

- Шаг редукции

$$u = |a * u + b * v|/k,$$

где $a, |b| \leq \sqrt{k} : a * u + b * v \equiv 0 \pmod{k}$ при $k = 2^{2W}$. Для нахождения a и b вычисляется $u/v \bmod k$

- Операция dmod определяется как $u = |u - c * v|/2^W$, где $c = u/v \bmod 2^W$.

Эти две операции выполняются поочередно, в результате чего длина обоих чисел уменьшается на W.

Вычисление модулярного деления по модулю 2^W и 2^{2W} является важнейшей задачей в k-арном алгоритме.

Расширенный алгоритм Евклида

Для любых двух чисел u и v существуют такие числа x и y (коэффициенты Безу), что выполняется:

$$u * x + v * y = \text{НОД}(u, v).$$

Для вычисления этих коэффициентов используется расширенный алгоритм Евклида (РАЕ).

Для взаимно простых чисел коэффиценты Безу являются также и обратными элементами по модулю, т. е.

$$x = u^{-1} \bmod v, y = v^{-1} \bmod u.$$

Для получения $v^{-1} \bmod \beta^n$ необходимо запустить этот метод, передав в качестве параметров $v \bmod \beta^n$ и β^n (β — основание системы счисления).

Итеративное вычисление модулярного деления

Вычисление $u/v \mod \beta^n$ модулярного деления по m цифр (обобщение MODIV):

Algorithm 1 Алгоритм модулярного деления MODIV

$v' := v^{-1} \mod \beta^m$
$i := t := 0$
while $i < n$ **do**
  $v_i := v' * u \mod \beta^m$
  $t := v_i * \beta^i + t$
  $u := (u - v_i * v)/\beta^m$
  $i := i + m$
return $t \mod \beta^n$

Передав $u = 1$, можно найти обратный элемент $v^{-1} \mod \beta^n$.

Рекурсивное вычисление обратного элемента

Рекурсивная формула для вычисления обратного элемента, которая выполняется для любых взаимно простых чисел v и β:

$$v^{-1} = (2 - v * v') * v' \mod \beta^2, \qquad \text{где } v' = v^{-1} \mod \beta.$$

Алгоритм:

- Вычислить $v^{-1} \mod \beta^m$
- Использовать формулу $\lceil \log_\beta n/m \rceil$ раз
- Вернуть $v^{-1} \mod \beta^n$

Вычисления по модулю степени двойки

Случай $\beta = 2$:

- Деление/умножение на 2^m реализуется с помощью сдвига вправо/влево.
- при $n = W$ и $n = 2 * W$ можно воздержаться от нахождения остатка от деления на 2^i
- PAE необходимо запустить с параметрами v и 2^W, но из-за того, что максимальное значение, которое может храниться в памяти, равняется $2^W - 1$, первый шаг нам нужно провести вручную, исходя из того, что $\lfloor 2^W / v \rfloor = \lfloor (2^W - 1)/v \rfloor$.

Начальный шаг вычислений

В предыдущих алгоритмах необходимо вычисление обратного элемента $v^{-1} \bmod 2^m$ на начальном этапе. Мы рассматриваем следующие способы:

- Без дополнительной памяти
  - $v^{-1} \bmod 2^m = v \bmod 2^m$ при m равным 1, 2 или 3.
  - $m = 4$ вычисление начального шага можно выполнить с помощью следующей формулы $((v \ll 1 \,\hat{}\, v)\&4) \ll 1 \,\hat{}\, v$
- С дополнительной памятью: таблица, которая содержит значения $v^{-1} \bmod 2^m$ для всех нечетных $0 < v < 2^m$.

Исследования

Относительное время работы алгоритмов для $\beta = 2$ и $N = 64$

Алгоритм	Время в зависимости от m							
	1	2	3	4	5–7	8	9–15	16
PAE	142							
MODIV_B	63	46	32	22	—			
MODIV_C	—			22	17–13	10.5	10.4–5.3	4.7
Recur_B	-	2.6	-	1.96	—			
Recur_C	—			1.9	—	1.4	—	1

B— без памяти, C— с памятью

Спасибо за внимание!