Тема 7. НОД многочленов

С. Б. Гашков, И. С. Сергеев

Рассматриваются классический бинарный и правосторонняя весрия асимптотически быстрого алгоритма НОД для многочленов над полем F. Первый имеет сложность $O(n^2)$, а второй $O(M(n)\log n)$. Эти оценки верны для схем или неветвящихся программ над арифметическим базисом, однако проще доказываются для ветвящихся программ. Можно проверить, что известный алгоритм Евклида имеет сложность $O(nM(n))$.

1 Бинарный алгоритм

Бинарный алгоритм НОД был предложен Штейном в 1961 г.

Бинарный алгоритм НОД многочленов.

Вход: многочлены $a, b \in F[x]$.

1. Если $\deg a < \deg b$, то НОД$\,(a,b) =$ НОД$\,(b,a)$.
2. Если $b = 0$, то НОД$\,(a,b) = a$.

   Пусть $a_0 = a \bmod x$, $b_0 = b \bmod x$.
3. Если $a_0 = b_0 = 0$, то НОД$\,(a,b) = x$НОД$\,(a/x, b/x)$;

   иначе, если $a_0 = 0, b_0 \neq 0$, то НОД$\,(a,b) =$ НОД$\,(a/x, b)$;

   иначе, если $b_0 = 0, a_0 \neq 0$, то НОД$\,(a,b) =$ НОД$\,(a, b/x)$;

   иначе, НОД$\,(a,b) =$ НОД$\,((a - a_0 b_0^{-1} b)/x, b)$.

По построению, при каждой итерации шага 3 суммарная степень многочленов a и b уменьшается, если только она не равна нулю (в этом случае алгоритм заканчивает работу на следующей итерации). Отсюда следует, что, если $\deg a, \deg b < n$, то всего выполняется не более $2n-1$ итераций, каждая из которых имеет сложность $O(n)$.

Описанный бинарный алгоритм работает «справа налево» — от младших разрядов к старшим. Симметричным образом может быть построен левосторонний бинарный алгоритм. Из левосторонних алгоритмов НОД более известен алгоритм Евклида, основанный на операции деления с остатком. В 1971 г. Шёнхаге построил асимптотически быстрый алгоритм НОД (для чисел), основываясь на алгоритме Евклида и используя идеи Лехмера и Кнута. Далее будет описана правосторонняя версия этого алгоритма.

2 Правостороннее деление с остатком

Через $\nu(a)$ будем обозначать номер самого младшего ненулевого коэффициента многочлена a с соглашением $\nu(0) = +\infty$ (нумерация с нуля).

Правосторонние частное $q(x)$ и остаток $r(x)$ от деления $a(x)$ на $b(x) \not\equiv 0$ определяются как единственная пара многочленов, удовлетворяющая соотношениям:

$$r(x) = a(x) + q(x)b(x)x^{\nu(a)-\nu(b)}, \quad \nu(r) > \nu(b), \tag{1}$$

$$\begin{cases} q = 0, & \nu(a) > \nu(b), \\ \deg q \le \nu(b) - \nu(a), & \text{иначе} \end{cases}.$$

Будем использовать обозначение $(q, r) = \text{ПД}\,(a, b)$.

Лемма 1. *Операция* $\text{ПД}\,(a, b)$ *определена однозначно.*

Доказательство. В случае $\nu(a) > \nu(b)$ утверждение очевидно. Иначе, из (1) следует

$$\frac{a(x)}{x^{\nu(a)}} + q(x)\frac{b(x)}{x^{\nu(b)}} = 0 \mod x^{\nu(b)-\nu(a)+1}.$$

Тогда если обозначить $a' = a/x^{\nu(a)}$ и $b' = b/x^{\nu(b)}$, то многочлен q определяется однозначно как

$$q = -a'/b' \bmod x^{\nu(b)-\nu(a)+1}. \tag{2}$$

Для выполнения правостороннего деления может быть модифицирован алгоритм Штрассена для обычного деления с остатком:

Правостороннее деление многочленов.

Вход: многочлены a и $b \not\equiv 0$ из $F[x]$.

1. Если $\nu(a) > \nu(b)$, то $\text{ПД}\,(a, b) = (0, a)$.

2. Иначе, вычислить $B = b/x^{\nu(b)}$ и $c = B^{-1} \bmod x^{\nu(b)-\nu(a)+1}$.

3. Вычислить $q = -ac \bmod x^{\nu(b)-\nu(a)+1}$ и $r = a + qB$. Положить $\text{ПД}\,(a,b) = (q,r)$.

Сложность алгоритма есть $O(M(n))$.

Лемма 2. $\text{НОД}\,(a,b) = x^{-t}\text{НОД}\,(b,r)$, *где* $t = \max\{\nu(b)-\nu(a), 0\}$.

Доказательство. Если $\nu(a) > \nu(b)$, то $t = 0$ и $r = a$. В этом случае утверждение леммы очевидно. Иначе, справедлива цепочка равенств:

$$\text{НОД}\,(a,b) = x^{\nu(a)}\text{НОД}\left(\frac{a}{x^{\nu(a)}}, \frac{b}{x^{\nu(b)}}\right) \overset{(*)}{=} x^{\nu(a)}\text{НОД}\left(\frac{r}{x^{\nu(a)}}, \frac{b}{x^{\nu(b)}}\right) =$$
$$= x^{\nu(a)}\text{НОД}\left(\frac{r}{x^{\nu(b)}}, \frac{b}{x^{\nu(b)}}\right) = x^{\nu(a)-\nu(b)}\text{НОД}\,(b,r) = x^{-t}\text{НОД}\,(b,r),$$

где равенство $(*)$ верно в силу

$$\frac{a(x)}{x^{\nu(a)}} + q(x)\frac{b(x)}{x^{\nu(b)}} = \frac{r(x)}{x^{\nu(a)}}.$$

Лемма доказана.

Результат правостороннего деления зависит только от правых частей делимого и делителя — имеет место свойство, аналогичное свойству Лехмера для обычного деления с остатком.

Лемма 3. *Пусть* $\nu(a) \le \nu(b)$, $b' \equiv b \bmod x^l$, $l \ge 2\nu(b) - \nu(a) + 1$, $a' \equiv a \bmod x^{l-(\nu(b)-\nu(a))}$. *Обозначим* $(q,r) = \text{ПД}\,(a,b)$ *и* $(q',r') = \text{ПД}\,(a',b')$. *Тогда* $q = q'$ *и* $r \equiv r' \bmod x^{l-(\nu(b)-\nu(a))}$.

Доказательство. Справедливость леммы вытекает из того факта, что согласно (2) частное q зависит только от $2\nu(b) - \nu(a) + 1$ младших коэффициентов $b(x)$ и от $\nu(b) + 1$ младших коэффициентов $a(x)$. Сравнение $r \equiv r'$ затем следует из (1).

Обозначим $r_0 = a$, $r_1 = b$ и далее $(q_{i-1}, r_i) = \text{ПД}\,(r_{i-2}, r_{i-1})$. Также обозначим $\nu_i = \nu(r_i) - \nu(r_{i-1})$.

Лемма 4. *Если* $r_i \ne 0$, *то справедлива формула:*

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = x^{\nu(a)-\nu(r_i)} \begin{pmatrix} 0 & x^{\nu_i} \\ x^{\nu_i} & q_i \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 0 & x^{\nu_1} \\ x^{\nu_1} & q_1 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}.$$

Кроме того, $\text{НОД}\,(r_i, r_{i+1}) = x^{\nu(r_i)-\nu(a)}\text{НОД}\,(a,b)$.

Доказательство. Формула доказывается по индукции. Пусть $(q, r) = $ ПД (a, b). Тогда в силу (1)

$$\begin{pmatrix} b \\ r \end{pmatrix} = x^{\nu(a)-\nu(b)} \begin{pmatrix} 0 & x^{\nu(b)-\nu(a)} \\ x^{\nu(b)-\nu(a)} & q \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Докажем индуктивный переход:

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = x^{-\nu_i} \begin{pmatrix} 0 & x^{\nu_i} \\ x^{\nu_i} & q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} =$$

$$= x^{(\nu(a)-\nu(r_{i-1}))-(\nu(r_i)-\nu(r_{i-1}))} \begin{pmatrix} 0 & x^{\nu_i} \\ x^{\nu_i} & q_i \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 0 & x^{\nu_1} \\ x^{\nu_1} & q_1 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}.$$

Аналогично устанавливается соотношение для НОД. Основанием индукции является лемма 2. Индуктивный переход:

$$\text{НОД}\,(r_i, r_{i+1}) = x^{\nu_i}\text{НОД}\,(r_{i-1}, r_i) = x^{(\nu(r_i)-\nu(r_{i-1})+(\nu(r_{i-1})-\nu(a))}\text{НОД}\,(a, b).$$

Лемма доказана.

Для матрицы перехода введем обозначение

$$M_i = \begin{pmatrix} 0 & x^{\nu_i} \\ x^{\nu_i} & q_i \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 0 & x^{\nu_1} \\ x^{\nu_1} & q_1 \end{pmatrix}.$$

Заметим, что элементами матрицы M_i являются многочлены степени не выше $\nu(r_i) - \nu(a)$.

Из доказанных лемм следует

Лемма 5. *Пусть $\nu(a) \leq \nu(b)$ и $\nu(a') \leq \nu(b')$. Обозначим через $\{r_i\}$, $\{q_i\}$ и $\{r'_i\}$, $\{q'_i\}$ последовательности правосторонних частных и остатков от деления a на b и a' на b' соответственно. Пусть $a \equiv a' \bmod x^l$, $b \equiv b' \bmod x^l$, где $l \geq 2\nu(r_j) + 1$. Тогда для всех $i \leq j$ выполнено $q_i = q'_i$ (как следствие, совпадают и матрицы перехода) и $r_{i+1} \equiv r'_{i+1} \bmod x^{l-\nu(r_i)}$.*

Доказательство. Если $j = 1$, то утверждение следует из леммы 3, поскольку $2\nu(r_1) + 1 \geq 2\nu(r_1) - \nu(r_0) + 1$.

Докажем индуктивный переход от j к $j+1$. В силу $l \geq 2\nu(r_{j+1}) + 1 > 2\nu(r_j)+1$ по предположению имеем $q_i = q'_i$, а также $r_{i+1} \equiv r'_{i+1} \bmod x^{l-\nu(r_i)}$ для всех $i \leq j$. В частности,

$$r_{j+1} \equiv r'_{j+1} \bmod x^{l-\nu(r_j)}, \qquad r_j \equiv r'_j \bmod x^{l-\nu(r_j)}.$$

Поскольку $l - \nu(r_j) \geq 2\nu(r_{j+1}) - \nu(r_j) + 1$, то по лемме 3 заключаем, что $q_{j+1} = q'_{j+1}$ и

$$r_{j+2} \equiv r'_{j+2} \bmod x^{(l-\nu(r_j))-(\nu(r_{j+1})-\nu(r_j))},$$

что и требовалось.

3 Быстрый алгоритм для функции ПНОД

Правосторонний вариант быстрого алгоритма НОД Кнута—Шёнхаге основан на лемме 5. Введем функцию $\text{ПНОД}_n(a,b) = (r_j, r_{j+1}, M_j)$, где $j = \min\{i \geq 0 \mid \nu(r_{i+1}) \geq n/2\}$, а M_j — соответствующая матрица перехода:

$$\begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix} = x^{\nu(a)-\nu(r_j)} M_j \begin{pmatrix} a \\ b \end{pmatrix}.$$

Быстрый алгоритм для функции ПНОД основан на принципе «деления пополам».

Быстрый алгоритм для функции ПНОД.

Вход: многочлены $a \not\equiv 0$ и b из $F[x]$ степени не выше $n-1$, $\nu(a) \leq \nu(b)$.

1. Если $\nu(b) \geq n/2$, то $\text{ПНОД}_n(a,b) = (a,b,E)$, где E — единичная матрица.

   Иначе:

2. Пусть $k = \lceil n/2 \rceil$, $a_0 = a \bmod x^k$ и $b_0 = b \bmod x^k$. Вычислить $(c_0, d_0, M') = \text{ПНОД}_k(a_0, b_0)$.

   Заметим, что вычисление функции ПНОД правомерно, т.к. $a_0 \not\equiv 0$ в силу $\nu(a) \leq \nu(b) < n/2$.

3. Вычислить

$$\begin{pmatrix} r_{j'} \\ r_{j'+1} \end{pmatrix} = x^{\nu(a_0)-\nu(c_0)} M' \begin{pmatrix} a - a_0 \\ b - b_0 \end{pmatrix} + \begin{pmatrix} c_0 \\ d_0 \end{pmatrix} = x^{\nu(a)-\nu(r_{j'})} M' \begin{pmatrix} a \\ b \end{pmatrix}.$$

   Проверим корректность формулы. Рассмотрим два случая.

   а) Если $\nu(b_0) \geq k/2$, то $M' = E$, $a_0 = c_0$, $b_0 = d_0$, следовательно, $r_{j'} = a$ и $r_{j'+1} = b$.

   б) Иначе $\nu(r_{j'}) = \nu(c_0) < k/2$. Поэтому $k \geq 2\nu(r_{j'})+1$. Следовательно, согласно лемме 5, правосторонние частные $q_1, \ldots, q_{j'}$ одинаковы для (a,b) и (a_0,b_0) и, значит, совпадают соответствующие матрицы перехода. Кроме того остатки r_i при $i \leq j'+1$ совпадают по модулю $x^{k-\nu(r_{j'})}$ с остатками из соответствующей последовательности для (a_0,b_0). В частности, $c_0 \equiv r_{j'} \bmod x^{\nu(r_{j'})+1}$, поэтому $\nu(c_0) = \nu(r_{j'})$.

Окончательно имеем:

$$\begin{pmatrix} r_{j'} \\ r_{j'+1} \end{pmatrix} = x^{\nu(a)-\nu(r_{j'})} M' \begin{pmatrix} a \\ b \end{pmatrix} = x^{\nu(a_0)-\nu(c_0)} M' \begin{pmatrix} a \\ b \end{pmatrix} =$$
$$= x^{\nu(a_0)-\nu(c_0)} \left(M' \begin{pmatrix} a - a_0 \\ b - b_0 \end{pmatrix} + M' \begin{pmatrix} a_0 \\ b_0 \end{pmatrix} \right).$$

Далее заметим, что $\nu(r_{j'+1}) \geq l = \lceil k/2 \rceil$.

4. Если $\nu(r_{j'+1}) \geq n/2$, то $\text{ПНОД}_n(a, b) = (r_{j'}, r_{j'+1}, M')$.

   Иначе:

5. Если $\nu(r_{j'}) \geq l$, то положить $(a', b') = (r_{j'}, r_{j'+1})$ и $Q = E$. В противном случае вычислить $(q_{j'+1}, r_{j'+2}) = \text{ПД}(r_{j'}, r_{j'+1})$ и положить $(a', b') = (r_{j'+1}, r_{j'+2})$, а $Q = \begin{pmatrix} 0 & x^{\nu_{j'+1}} \\ x^{\nu_{j'+1}} & q_{j'+1} \end{pmatrix}$.

   Заметим, что $\nu(a'), \nu(b') \geq l$, но $\nu(a') < n/2$ в силу 4.

6. Пусть $a_1 = x^{-l} a' \bmod x^{2(k-l)}$ и $b_1 = x^{-l} b' \bmod x^{2(k-l)}$. Вычислить $(c_1, d_1, M'') = \text{ПНОД}_{2(k-l)}(a_1, b_1)$.

   Вычисление ПНОД корректно, т.к. $a_1 \not\equiv 0$ в силу $\nu(a_1) < n/2 - l < 2(k - l)$.

7. Вычислить

$$\begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix} = x^{\nu(a_1)-\nu(c_1)} M'' \begin{pmatrix} a' - a_1 x^l \\ b' - b_1 x^l \end{pmatrix} + x^l \begin{pmatrix} c_1 \\ d_1 \end{pmatrix}.$$

   Проверим корректность формулы. Рассмотрим два случая.

   а) Если $\nu(b_1) \geq k - l$ (это значит, что $\nu(b') \geq n/2$), то $M'' = E$, $c_1 = a_1$, $d_1 = b_1$, следовательно, $r_j = a'$ и $r_{j+1} = b'$.

   б) Иначе $\nu(b_1) < k - l$. Следовательно $\nu(c_1) < k - l$, поэтому $2(k - l) \geq 2\nu(c_1) + 1$. Следовательно, согласно лемме 5, последовательность правосторонних остатков вплоть до d_1 совпадает для $(x^{-l}a', x^{-l}b')$ и (a_1, b_1) по модулю $x^{2(k-l)-\nu(c_1)}$, что влечет совпадение и по модулю x^{k-l+1}. Совпадают и правосторонние частные, значит, и матрицы перехода. Поэтому имеем $\nu(c_1) = \nu(r_j) + l$ и далее

$$\begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix} = x^{\nu(a')-\nu(r_j)} M'' \begin{pmatrix} a' \\ b' \end{pmatrix} = x^{\nu(a_1)-\nu(c_1)} M'' \begin{pmatrix} a' \\ b' \end{pmatrix} =$$
$$= x^{\nu(a_1)-\nu(c_1)} \left(M'' \begin{pmatrix} a' - x^l a_1 \\ b' - x^l b_1 \end{pmatrix} + x^l M'' \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \right).$$

8. $\text{ПНОД}_n(a,b) = (r_j, r_{j+1}, M_j)$, где $M_j = M''QM'$.

   Действительно, $\nu(r_{j+1}) \geq \min\{\nu(d_1), k-l+1\} + l \geq k-l+l \geq n/2$, а $\nu(r_j) = \nu(c_1) + l < k-l+l = k$, поэтому $\nu(r_j) < n/2$.

Таким образом, вычисление ПНОД_n сведено к двум операциям $\text{ПНОД}_{n/2}$, операции правостороннего деления, а также нескольким умножениям, сравнениям, вычислениям функции ν, приведениям по модулю одночлена, откуда вытекает рекуррентное соотношение:

$$L(\text{ПНОД}_n) \leq 2L(\text{ПНОД}_{\lceil n/2 \rceil}) + O(M(n) + I(n) + n),$$

из которого следует оценка сложности

$$L(\text{ПНОД}_n) = O(M(n) \log n).$$

4 Быстрый алгоритм для НОД

Используя схему для ПНОД, несложно построить схему для НОД. Рассмотрим следующий алгоритм.

Быстрый алгоритм для НОД *многочленов.*

Вход: многочлены $a \not\equiv 0$ и b из $F[x]$ степени не выше $n-1$.

1. Если $\nu(a) > \nu(b)$, то $\text{НОД}\,(a,b) = \text{НОД}\,(b,a)$.
2. Вычислить $(a', b', M') = \text{ПНОД}_n(a,b)$.
3. Если $b' = 0$, то $\text{НОД}\,(a,b) = x^{\nu(a)-\nu(a')}a'$.
4. Вычислить $(q,r) = \text{ПД}\,(a',b')$. Пусть $a'' = x^{-\lceil n/2 \rceil}b'$, $b'' = x^{-\lceil n/2 \rceil}r$.
5. $\text{НОД}\,(a,b) = x^{\nu(a)-\nu(a'')}\text{НОД}\,(a'',b'')$.

Если обозначить через $G(n)$ сложность вычисления НОД многочленов степени $< n$, то получаем соотношение:

$$G(n) \leq G(n/2) + L(\text{ПНОД}_n) + O(M(n)),$$

из которого следует $G(n) = O(M(n) \log n)$.