$$1 = c_1 \cdots c_s \, q_{s+1}(x) \cdots q_t(x)$$

(считаем, что $t \geq s$).

При $t > s$ будем иметь противоречие. Значит, $t = s$ и $q_i(x) = c_i p_i(x)$ $(i = 1, \dots, s)$

Обычно разложение данного многочлена $f(x) \in F[x]$ на неприводимые множители записывают в виде:

$$f(x) = c \cdot p_1(x)^{k_1} \cdots p_s(x)^{k_s}$$

где $p_1(x), \dots, p_s(x)$ попарно непропорциональные нормированные неприводимые над F мн-ны (нормированные – старший коэф. – единица)

Эта запись единственна с точностью до нумерации мн-нов $p_1(x), \dots, p_s(x)$

Указанная запись наз. КАНОНИЧЕСКИМ РАЗЛОЖЕНИЕМ мн-на $f(x) \in F[x]$.

Если известно каноническое разложение мн-нов $f_1(x), \dots, f_m(x) \in F[x]$, то НОД и НОК этих мн-в могут быть найдены при помощи хорошо известного школьного правила

Замечание

На практике предпочтительнее, вообще говоря, использовать для отыскания НОД и НОК алгоритм Евклида.

Опр. Пусть $f(x) \in F[x]$, $f(x) = a_n x^n + \dots + a_1 x + a_0$

Производной этого мн-на наз. многочлен вида

$$f'(x) = n a_n x^{n-1} + \dots + a_1 \in F[x]$$

Здесь $k a_k$ понимается как $\underbrace{a_k + \dots + a_k}_{k \text{ слагаемых}}$

Пример

$F = F_2$ – поле из 2х эл-тов

Пусть $f(x) = x^2 + 1$. Тогда $f'(x) = (1+1)x = 0$

(*) Далее будем считать, что F – поле нулевой характеристики ($\mathrm{char}\, F = 0$), т.е. суммы вида $1 + 1 + \dots + 1$ отличны от нуля. В этом случае, как легко видеть

$$\deg f'(x) = \deg f(x) - 1$$

Операция дифференцирования многочленов подчиняется обычным правилам. Например, имеет место формула Лейбница

$$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$$

($f(x), g(x) \in F[x]$) Используя ее, нетрудно установить следующее утверждение: если многочлен $f(x)$ взаимно прост со своей производной $f'(x)$, то $f(x)$ не имеет кратных неприводимых делителей. (Действительно, пусть $f(x) = p(x)^k f_1(x)$, где $p(x)$ — неприводимый многочлен, $k > 1$. Тогда $f'(x) = k\,p(x)^{k-1} p'(x) f_1(x) + p(x)^k f_1'(x)$, т.е. $f'(x)$ делится по крайней мере на $p(x)^{k-1}$.) Однако обратное утверждение не всегда верно. Например, многочлен $p(x) = x^2 - t \in \mathbb{F}_2(t)[x]$ неприводим, но $p'(x) = 0$. Если поле F имеет нулевую характеристику, то все в порядке, так как в этом случае $\deg f'(x) = \deg f(x) - 1$.

Теорема 10

Пусть $f(x) \in F[x]$, $f(x) = p(x)^k g(x)$, где $g(x)$ не делится на $p(x)$ — неприводимый многочлен над F (т.е. $p(x)$ — неприводимый множитель мн-на $f(x)$ кратности k).

Тогда $p(x)$ — неприводимый множитель мн-на $f'(x)$ кратности $k-1$. (при $k=1$ $p(x)$ не входит в каноническое разложение $f'(x)$)

Доказательство

Справедливы правила известные дифференцирования суммы и произведения (в частности, степени)

Имеем

$$f'(x) = k\,p(x)^{k-1} p'(x) g(x) + p(x)^k g'(x) =$$
$$= p(x)^{k-1} \left(k p'(x) g(x) + p(x) g'(x)\right)$$

Значит, $f(x)$ делится на $p(x)^{k-1}$. Покажем, что

$$h(x) = k p'(x) g(x) + p(x) g'(x) \text{ не делится}$$

не делится на $p(x)$. Для этого достаточно установить, что

$$k p'(x) g(x)$$

не делится на $p(x)$

Поскольку $p'(x) \neq 0$ ($\deg p'(x) = \deg p(x) - 1$), то $kp'(x) \neq 0$ ($\operatorname{char} F = 0$)

Если бы произведение $kp'(x)g(x)$ было кратно $p(x)$, то либо $kp'(x)$ делится на $p(x)$, что невозможно, либо $g(x)$ делится на $p(x)$, что не так по условию

Итак,

$$f'(x) = p(x)^{k-1} h(x)$$

где $h(x)$ не делится на $p(x)$

Таким образом $p(x)$ - неприводимый множитель многочлена $f'(x)$ кратности $k-1$.

Опишем процедуру выделения кратных неприводимых множителей заданного многочлена $f(x)$

Пусть

$$f(x) = cp_1(x)^{k_1} \quad p_s(x)^{k}$$

– каноническое разложение

Рассмотрим

$$d(x) = НОД\left(f(x), f'(x)\right) = \; = p_1(x)^{k_1-1} \quad p_s(x)^{k\ -1}$$

т е неприводимые множители $d(x)$ суть кратные неприводимые множители $f(x)$

Отыскание $d(x)$ и есть выделение в $f(x)$ кратных неприводимых множителей

Отметим, что $d(x)$ может быть найден без использования канонического разложения $f(x)$ при помощи алгоритма Евклида

Далее можно освободиться от кратных множителей, т е перейти от многочлена $f(x)$ к

$$\tilde{f}(x) = \frac{f(x)}{d(x)}$$

Имеем

$$\tilde{f}(x) = cp_1(x) \quad p_s(x),$$

т е $\tilde{f}(x)$ имеет те же неприводимые множители, что и $f(x)$, но они входят в каноническое разложение только в первой степени

Отыскав каноническое разложение $\tilde{f}(x)$, затем можно найти и каноническое разложение $f(x)$