ЛЕКЦИЯ №2

Тема: Наибольший общий делитель двух многочленов. Алгоритм Евклида. Неприводимые многочлены.

Определение 8. *Пусть f(x)и g(x) –многочлены из* $P[x]$. *Назовем многочлен d(x) из* $P[x]$ *назовем общим делителем многочленов f(x)и g(x), если он – делитель как f(x), так и g(x).*

Определение 9. *Общий делитель D(x) двух многочленов f(x)и g(x) из* $P[x]$ *называется наибольшим, если он делит любой общий делитель этих многочленов.*

Теорема 9 (О существовании и единственности НОД двух произвольных многочленов). *Для любых двух многочленов f(x)и g(x) из* $P[x]$ *существует такой многочлен* $D(x)$в $P[x]$, *который является их НОД, причем он определяется однозначно с точностью до множителя нулевой степени.*

□. Для нахождения D(x) используем алгоритм Евклида. Он заключается в следующем. Если f(x)= g(x)=0, то НОД (f(x), g(x))=0. Если g(x)≠ 0, то разделим с остатком f(x)на g(x), - получим неполное частное q(x) и остаток r(x). Затем g(x) разделим на остаток r(x)(когда r(x)≠ 0), - получим неполное частное $q_1(x)$и остаток $r_1(x)$ и т. д. Степени получающихся остатков убывают. Однако, понятно, что этот процесс конечен, т. е. в какой-то момент остаток $r_{k+1}(x)$ станет равным нулю. Это значит, что остаток $r_k(x)$ разделится нацело на предыдущий остаток $r_{k-1}(x)$. Покажем, что $r_k(x)$ – это искомый наибольший общий делитель.

Действительно,

$$\begin{cases} f(x) = g(x)\cdot q(x) + r(x) \\ g(x) = r(x)\cdot q_1(x) + r_1(x) \\ r(x) = r_1(x)\cdot q_2(x) + r_2(x) \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ r_{k-2}(x) = r_{k-1}(x)\cdot q_k(x) + r_k(x) \\ r_{k-1}(x) = r_k(x)\cdot q_{k+1}(x) \end{cases} \qquad (4)$$

Рассмотрим предпоследнее равенство

$$r_{k-2}(x) = r_{k-1}(x)\cdot q_k(x) + r_k(x).$$

Правая часть этого равенства делится на $r_k(x)$, так как каждое слагаемое делится на $r_k(x)$. Значит, и левая часть делится на $r_k(x)$.

Рассмотрим третье снизу равенство:

$$r_{k-3}(x) = r_{k-2}(x) \cdot q_{k-1}(x) + r_{k-1}(x).$$

Правая часть этого равенства делится на $r_k(x)$. Отсюда $r_{k-3}(x)$ делится на $r_k(x)$. Так, двигаясь снизу вверх, получим, что g(x) и *r(x)*делятся на $r_k(x)$. Следовательно, *f*(*x*) делится на $r_k(x)$. Таким образом, r_k(x) −общий делитель *f*(*x*)и *g*(*x*).

Рассмотрим теперь первое равенство

$$f(x) = g(x) \cdot q(x) + r(x).$$

Допустим, что d(x) – некоторый общий делитель *f*(*x*)и *g*(*x*). Тогда

$$r(x) = f(x) - g(x) \cdot q(x).$$

Отсюда *r(x)* делится на *d(x).*Рассмотрим второе сверху равенство

$$g(x) = r(x) \cdot q_1(x) + r_1(x).$$

Получим, что $r_1(x)$ делится на *d(x).* Спускаясь постепенно вниз, получим, что $r_k(x)$ делится на *d(x).*Таким образом, $r_k(x)$ делится на любой общий делитель многочленов *f*(*x*)и *g*(*x*). Значит, НОД (*f*(*x*), *g*(*x*))= $r_k(x)$. От противного легко доказать, что два НОД отличаются только на общий скалярный множитель. ■

Примечание. *Так как алгоритм Евклида сводится к последовательному применению алгоритма деления с остатком (см теорему 8), значит НОД, найденный пи помощи алгоритма Евклида, не зависит от того, будем ли мы рассматривать f*(*x*)и *g*(*x*) над полем P или его расширением.

Теорема 10. *Если D(x) – наибольший общий делитель многочленов f(x)и g(x), g(x)≠* 0 *из* $P[x]$*, то в том же кольце можно найти такую пару многочленов* $\varphi(x)$ *и* $\psi(x)$ *, что*

$$f(x) \cdot \varphi(x) + g(x) \cdot \psi(x) = D(x)$$

□. Возьмем предпоследнее равенство из (4)

$r_{k-2}(x) = r_{k-1}(x) \cdot q_k(x) + r_k(x) \Leftrightarrow r_k(x) = r_{k-2}(x) - r_{k-1}(x) \cdot q_k(x).$

D(x)= $r_k(x)$. *D(x)*= $r_{k-2}(x) - r_{k-1}(x) \cdot q_k(x)$

$$r_{k-3}(x) = r_{k-2}(x) \cdot q_{k-1}(x) + r_{k-1}(x) \Leftrightarrow$$

$$r_{k-1}(x) = r_{k-3}(x) - r_{k-2}(x) \cdot q_{k-1}(x)$$

$D(x) = r_{k-2}(x) \cdot \varphi_1(x) + r_{k-3}(x) \cdot \psi_1(x)$, *где* $\varphi_1(x) = 1 + q_k(x)q_{k-1}(x)$;

$$\psi_1(x) = -q_k$$

Идя снизу вверх,

$$D(x) = r_{k-3}(x) \cdot \varphi_2(x) + r_{k-4}(x) \cdot \psi_2(x),$$

и т. д. , наконец,

$$D(x) = f(x) \cdot \varphi_{k-1}(x) + g(x) \cdot \psi_{k-1}(x). \blacksquare$$

Определение 10. *Два многочлена называются взаимно –простыми, если их наибольший общий делитель равен константе.*

Теорема 11. *Для взаимно простых многочленов f(x) и g(x) найдутся два таких многочлена* $\varphi(x)$ *и* $\psi(x)$*, что*

$$f(x) \cdot \varphi(x) + g(x) \cdot \psi(x) = 1$$

Теорема 12. *Если для многочленов f(x) и g(x) найдутся два таких многочлена* $\varphi(x)$ *и* $\psi(x)$*, что выполняется равенство*

$$f(x) \cdot \varphi(x) + g(x) \cdot \psi(x) = 1,$$

то $f(x)$ *и* $g(x)$ *взаимно простые.*

Определение 11. *Многочлен f(x) из* $P[x]$ *со степенью, большей 1, называется приводимым над полем P, если он может быть представлен (т. е. разложен) в виде произведения двух и более многочленов меньших степеней из того же кольца* $P[x]$.

Примеры.

1) $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ - приведение многочлена над полем рациональных чисел; дальнейшее разложение над полем рациональных чисел невозможно (корни квадратных трехчленов иррациональные).

2) $x^2 - 2 = \left(x - \sqrt{2}\right)(x + \sqrt{2})$ – разложение многочлена над полем действительных чисел; дальнейшего разложения не существует, так как степень множителей уже равна 1, и меньше невозможно.

3) $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3) = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)\left(x - \sqrt{3}\right)(x + +\sqrt{3})$ – разложение многочлена до произведения неприводимых многочленов над полем действительных чисел.

4) $x^2 - x + 1$ - многочлен неприводим над полем действительных чисел, так как дискриминант отрицательный; следовательно, корни многочлена комплексные.

5) $x^2 - x + 1 = \left(x - \frac{1-i\sqrt{3}}{2}\right)(x - \frac{1+i\sqrt{3}}{2})$- приведение того же многочлена над полем комплексных чисел через комплексные корни.

Рассмотрим некоторые общие свойства для всех неприводимых многочленов (***многочлены нулевой степени не относятся ни к приводимым, ни к неприводимым многочленам, так же как 1 не относится ни к простым числам, ни к составным числам***):

$\mathbf{1^0}$. *Многочлен первой степени неприводим над любым полем.*

$\mathbf{2^0}$. *Многочлен f(x) из кольца* $P[x]$ *тогда и только тогда не делится на многочлен p(x), неприводимый над полем P, когда f(x) и p(x) взаимно просты.*

$\mathbf{3^0}$. *Если произведение f(x)g(x) двух многочленов f(x) и g(x) из* $P[x]$ *делится на многочлен p(x), неприводимый над P, то на p(x) делится по меньшей мере один из сомножителей f(x) и g(x).*

$\mathbf{4^0}$. *Если произведение* $f_1(x)f_2(x) \dots f_k(x)$ *нескольких многочленов из* $P[x]$ *делится на многочлен p(x), неприводимый над P, то на p(x) делится по меньшей мере один из сомножителей* $f_i(x)$.

Пользуясь этими свойствами, докажем основную теорему.

Теорема 13 (Основная теорема теории делимости многочленов). *Всякий многочлен из кольца* $P[x]$*выше нулевой степени разлагается в произведение неприводимых многочленов:*

$$f(x)=p_1(x)p_2(x) \dots p_k(x),$$

где $p_i(x)$ *– неприводимые над полем P многочлены. Это разложение является единственным с точностью перестановки множителей и множителя нулевой степени.*

□. Покажем сначала, что всякий многочлен *f*(*x*) из $P[x]$ выше нулевой степени разложим в произведение неприводимых множителей.

Допустим, что *f*(*x*) неприводим. Тогда *f*(*x*) = *f*(*x*).

Пусть теперь он приводим. Тогда его модно представить в виде произведения хотя бы двух многочленов меньших степеней:

$$f(x) = f_1(x) \cdot f_2(x) \qquad (5)$$

$f(x), f_1(x), f_2(x) \epsilon P[x]$.

Если $f_1(x)$ и $f_2(x)$ оба неприводимо, то разложение на неприводимые сомножители уже есть.

Если же $f_1(x)$или $f_2(x)$ или оба приводимы, то продолжаем разложение дальше набольшее число множителей. Однако этот процесс все же конечен, так как степень множителей уменьшается, но не может быть меньше 1. Следовательно, на каком-то шаге алгоритма мы получим

$$f(x) = f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_k(x),$$

все $f_i(x)$, $i = 1, \ldots , k$ будут неразложимы.

Докажем теперь единственность разложения. От противного. Допустим, существует два разложения на неприводимые множители из $P[x]$:

$$f(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_k(x),$$

$$f(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_l(x).$$

Будем считать, без ограничения общности, что $k \ll l$.

Тогда

$$p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_k(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_l(x). \qquad (6)$$

Левая часть (6) делится, например, на $p_1(x)$. Тогда и правая часть (6) делится на $p_1(x)$. Согласно 3^0, один из сомножителей правой части делится на $p_1(x)$. Но так как многочлены $q_i(x)$ и $p_1(x)$ неприводимы, они отличаются только на константный множитель. Без ограничения общности, допустим,

$$q_1(x) = c_1 p_1(x).$$

$$p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_k(x) = c_1 p_1(x) \cdot q_2(x) \cdot \ldots \cdot q_l(x).$$

Разделив на $p_1(x)$:

$$p_2(x) \cdot \ldots \cdot p_k(x) = c_1 \cdot q_2(x) \cdot \ldots \cdot q_l(x).$$

Повторяя рассуждения, получим, например,

$$p_3(x) \cdot \ldots \cdot p_k(x) = c_1 \cdot c_2 \cdot q_3(x) \ldots \cdot q_l(x).$$

Однако этот процесс не может быть продолжен бесконечно, на каком-то шаге алгоритма получим

$$1 = c_1 \cdot c_2 \cdot \ldots \cdot c_k \cdot q_{k+1}(x) \cdot \ldots \cdot q_l(x).$$

Это значит, что многочлены $q_{k+1}(x), \ldots, q_l(x)$ имеют нулевые степени. Таким образом, $k = l$, и $q_1(x) = c_1 p_1(x)$, …, $q_k(x) = c_k p_k(x)$. ■

Примечание. *Из доказательства основной теоремы, собирая в степень множители, отличающиеся на константный коэффициент, получим формулу:*

$$f(x) = c \cdot p_1^{\alpha_1}(x) \cdot p_2^{\alpha_2}(x) \cdot \ldots \cdot p_s^{\alpha_s}(x), \quad (7)$$

где α_i - целые положительные числа, $c \neq 0$, c - это числа из P.

В этой формуле все множители $p_i^{\alpha_1}(x)$ существенно различны.

α_i - называется кратностью неприводимого множителя $p_i(x)$.

Определение 12. *Многочлен g(x) входит в данный многочлен f(x) с кратностью $\propto$, где $\propto$ -целое положительное число, если f(x) делится на $g^{\propto}(x)$, но не делится на $g^{\propto+1}(x)$. Если $\propto = 1$, то g(x) называется простым множителем или простым делителем. Если же $\propto > 1$, то назовем g(x) кратным множителем или делителем.*

Образец применения алгоритма Евклида

Задача. Найти наибольший общий делитель многочленов над полем рациональных чисел:

$$f(x) = 2x^5 - 3x^4 - 5x^3 + x^2 + 6x + 3$$

$$g(x) = 3x^4 + 2x^3 - 3x^2 - 5x - 2$$

Решение.

$$\begin{array}{l|l} 2x^5 - 3x^4 - 5x^3 + x^2 + 6x + 3 & 3x^4 + 2x^3 - 3x^2 - 5x - 2 \\ \underline{2x^5 + \frac{4}{3}x^4 - 2x^3 - \frac{10}{3}x^2 - \frac{4}{3}\quad x} & \\ -\frac{13}{3}x^4 - 3x^3 + \frac{13}{3}x^2 + \frac{22}{3}x + 3 & \frac{2}{3}x - \frac{13}{9} \\ \underline{-\frac{13}{3}x^4 - \frac{26}{9}x^3 + \frac{13}{3}x^2 + \frac{65}{9}x + \frac{26}{9}} & \\ \boxed{-\frac{1}{9}x^3 + \frac{1}{9}x + \frac{1}{9}} & \end{array}$$

$$\begin{array}{l|l} 3x^4+2x^3-3x^2-5x-2 & -\frac{1}{9}x^3+\frac{1}{9}x+\frac{1}{9} \\ \underline{3x^4-3x^2-3x\qquad\qquad\quad} & \underline{\qquad\qquad\qquad\qquad} \\ 2x^3-2x-2 & -27x-18 \\ \underline{2x^3-2x-2} & \\ 0 & \end{array}$$

Согласно алгоритма Евклида, $-\frac{1}{9}x^3+\frac{1}{9}x+\frac{1}{9}$ является наибольшим общим делителем многочленов.

Действительно, $f(x)=g(x)\cdot\left(\frac{2}{3}x-\frac{13}{9}\right)+\left(-\frac{1}{9}x^3+\frac{1}{9}x+\frac{1}{9}\right)=\left(-\frac{1}{9}x^3+\frac{1}{9}x+\frac{1}{9}\right)\cdot(-27x-18)+\left(-\frac{1}{9}x^3+\frac{1}{9}x+\frac{1}{9}\right)=(x^3-x-1)\cdot(3x+3)=$

$=3(x^3-x-1)\cdot(x+1)$.

Таким образом, с точностью до константного множителя , x^3-x-1 является наибольшим общим делителем многочленов *f(x) и g(x).*

Ответ: x^3-x-1.