Многочлены 2. Делимость многочленов

Определение 1. Алгоритмом Евклида для многочленов A и B называется последовательность делений с остатком:

$$\begin{aligned}
&A = BQ_1 + R_1\\
&B = R_1Q_2 + R_2\\
&\ldots\\
&R_{n-2} = R_{n-1}Q_n + R_n\\
&R_{n-1} = R_nQ_{n+1}
\end{aligned}$$

Последний ненулевой остаток R_n называется *результатом работы алгоритма Евклида.*

Задача 1. Проведите алгоритм Евклида для многочленов $3x^3-2x^2+x+2$ и x^2-x+1

Замечание. а) Для определения наибольшего общего делителя необходимо, чтобы один из многочленов был ненулевым.
б) Наибольший общий делитель определен с точностью до умножения на константу. Иногда эту константу подбирают так, чтобы многочлен был *приведенным*, т.е. его старший член равнялся 1.

Задача 2. Докажите, следующие три определения наибольшего общего делителя эквивалентны
а) *Наибольшим общим делителем* многочленов A и B, называется их делитель наибольшей степени.
б) *Наибольшим общим делителем* многочленов A и B, называется такой их общий делитель, который делится на любой другой их общий делитель.
в) *Наибольшим общим делителем* многочленов A и B, называется результат работы алгоритма Евклида.

Задача 3. Найдите НОД многочленов а) x^4+2x^3-x-2 и x^2+5x+6; б) x^n-1 и x^m-1; в*) x^n+1 и x^m+1.

Задача 4 (Линейное представление НОД). а) Докажите, что для любых многочленов A и B существуют многочлены U и V такие, что $\text{НОД}(A,B) = AU+BV$;
б) Найдите такие U и V для случая $A = 3x^3-2x^2+x+2$, $B = x^2-x+1$.

Определение 2. Многочлен P называется неприводимым, если он не представляется в виде произведения двух многочленов меньшей степени.

Задача 5 (Ключевая лемма). Докажите, что если P неприводимый многочлен и $AB \vdots P$, то или $A \vdots P$ или $B \vdots P$.

Задача 6 (Основная теорема арифметики). Докажите, что каждый многочлен (степени > 0) раскладывается на неприводимые множители, причем такое разложение единственно. Единственность понимается с точностью до умножения на константы и перестановок сомножителей.

Задача 7. Пусть $A = P_1^{a_1} P_2^{a_2} \cdot \ldots \cdot P_n^{a_n}$, $B = P_1^{b_1} P_2^{b_2} \cdot \ldots \cdot P_n^{b_n}$ разложения на неприводимые множители. Найдите формулу для НОД(A, B).

Задача 8. Докажите, что если многочлен A делится на многочлен B, то все корни многочлена B являются корнями многочлена A. Верно ли обратное утверждение?

Определение 3. Говорят, что число x_0 является *корнем многочлена P кратности k*, если $P(x)$ делится на $(x - x_0)^k$, но не делится на $(x - x_0)^{k+1}$.

Задача 9. Докажите, что многочлен степени n имеет не более n корней с учетом кратности.