12. Выражение НОД через исходные многочлены.

Алгоритм Евклида поиска НОД
Пусть $f(x), g(x) \in F[x], g(x) \neq 0$ и $f(x) = q_1(x)g(x) + r_1(x), g(x) = q_2(x)r_1(x) + r_2(x)$.

Поделим с остатком $f(x)$ на $g(x)$. Пусть r_1 - остаток. Тогда поделим $g(x)$ на r_1 с остатком r_2. Теперь поделим r_1 на r_2 с остатком r_3, и так далее. Алгоритм продолжается, пока мы не получим нулевой остаток. Последний ненулевой остаток r_k - и есть НОД $f(x)$ и $g(x)$.

То, что алгоритм завершится за конечное число шагов следует из того, что на каждом шаге степени остатков уменьшаются $\implies$ на каком-то шаге получится нулевой остаток.

Под словом "выразить" в этом контексте имеется в виду представление наибольшего общего делителя в виде $d(x) = f(x)u(x) + g(x)v(x)$, где $u(x)$ и $v(x)$ -- какие-то многочлены. Их требуется найти, чтобы выполнялось указанное равенство. Есть теорема, что для НОД оно будет выполнено при удачном выборе множителей.

Одним из способов решить эту задачу является метод неопределённых коэффициентов. Пусть степени f и g равны m и n. Тогда u и v подбираются в виде выражений степени $n-1$ и $m-1$ с буквенными коэффициентами. После раскрытия скобок и приравнивания коэффициентов при одинаковых степенях у многочленов в левой и правой части получится система из $m+n$ линейных уравнений от такого же количества неизвестных. Этот метод очень часто бывает удобен, но здесь лучше поступить по-другому.

Алгоритм Евклида в общем виде устроен так. Сначала делим f_1 на f_2, получая остаток f_3. Затем делим f_2 на f_3, обозначая остаток через f_4. И так далее, пока не окажется, что f_{n-1} нацело разделилось на f_n. Тогда f_n и будет являться НОД.

Теперь, идя по записям снизу вверх, мы сначала выражаем f_n через f_{n-1} и f_{n-2}. Это легко сделать, так как f_n появилось как остаток от деления f_{n-2} на f_{n-1}. Далее мы можем по такому же принципу выразить f_{n-1} через f_{n-2} и f_{n-3}. Подставляя это выражение в предыдущую формулу, мы сможем избавиться от f_{n-1}, после чего f_n окажется выраженным уже через f_{n-2} и f_{n-3}. Далее идём вверх по такому же принципу, и итогом будет выражение f_n через f_1 и f_2, что нам и требуется.

Для примера: пусть $f_1 = f_2q_1 + f_3$, $f_2 = f_3q_2 + f_4$, $f_3 = f_4q_3$. Тогда НОД равен f_4, и мы его выражаем как $f_4 = f_2 - f_3q_3 = f_2 - (f_1 - f_2q_2)q_3$, и далее после упрощений получается выражение вида $f_1u + f_2v$.