Неприводимость многочленов

Определение 1. Пусть K — коммутативное кольцо, многочлен $f \in K\{x_1, \dots, x_n\}$ называется неприводимым, если из представления $f = hg$ следует, что один из многочленов g ил h константа.

Теорема 1. *Пусть K — поле, тогда любой многочлен из $f \in K\{x_1, \dots, x_n\}$ единственным образом раскладывается в произведение неприводимых многочленов $f = f_1 f_2 \dots f_k$ с точностью до перестановки и домножения на константы.*

1. Найдите все неприводимые многочлены не выше, чем четвёртой степени над полем $\mathbb{Z}_2$. (Маленькая подсказка: а сколько всего многочленов не выше четвёртой степени существует по модулю 2?).

Определение 2. Пусть $f \in \mathbb{Z}[x]$, тогда обозначим за $c(f)$ — наибольший общий делитель всех коэффициентов f.

2. а) Пусть $c(f) = 1$ и $c(g) = 1$. Докажите, что $c(fg) = 1$.(*Если $c(fg) \neq 1$, то у него есть простой делитель*)
б) Докажите, что $c(fg) = c(f)c(g)$.
в) **Лемма Гауса** Докажите, что многочлен $f \in \mathbb{Z}[x]$ неприводим над $\mathbb{Z}$ тогда и только тогда, когда он неприводим над $\mathbb{Q}$

3 (Критерий Эйзенштейна). Пусть $f \in \mathbb{Z}[x]$ и $f = a_n x^n + \dots + a_0$. Известно, что $a_n \not\vdots p$, $a_{n-1}, \dots a_0, \vdots p$ и $a_0 \not\vdots p^2$ для некоторого простого p. Докажите, что многочлен f неприводим над $\mathbb{Z}$

4. Пусть p — простое число. Докажите, что многочлен $x^{p-1} + x^{p-2} + \dots + x + 1$ неприводим над $\mathbb{Z}$

5. Докажите, что если p/q — несократимая дробь, являющаяся корнем полинома $f(x) = a_n x^n + \dots + a_1 x + a_0$ с целыми коэффициентами, то $qm - p$ делит $f(m)$ для любого целого m.

6. Доказать, что многочлен $(x - a_1)(x - a_2) \dots (x - a_n) - 1$ неприводим, если $a_1, a_2, \dots, a_n$ — различные целые числа.

7. Докажите, что любой многочлен из $\mathbb{Q}[x]$ представляется в виде суммы двух неприводимых многочленов.

8. а) Пусть $g \in K[x]$ — неприводимый многочлен над полем K. Докажите, что на остатках по модулю многочлена g можно ввести операции сложения и умножения так, чтобы они образовывали поле. Для многочленов б) $x^2 + 1 \in \mathbb{R}[x]$;в) $x^2 - 2 \in \mathbb{Q}[x]$ постройте биективные отображения f из поля остатков этих многочленов в $\mathbb{C}$ и в $\mathbb{Q}[\sqrt{2}]$ соответственно так, чтобы для любых двух остатков a, b выполнялось:

1. $f(a + b) = f(a) + f(b)$;

2. $f(ab) = f(a)f(b)$

Алгоритм Кронекера.

Алгоритм говорит про заданный многочлен $f \in \mathbb{Z}$, является ли он неприводимым. Если не является, то строит многочлен $g \in \mathbb{Z}, \deg g > 0$, который является делителем f. Докажите корректность алгоритма.

1) Пусть $\deg f = n$ и $r = [\frac{n}{2}]$.

2) Рассмотрим числа $c_j = f(j), j = 0, \ldots, r$. Если хотябы одно из чисел $c_j = 0$, алгоритм прекращает свою работу, $g = x - j$.

3) Если все c_j отличны от 0. Для каждого $0 \leqslant j \leqslant r$ Строим множество C_j, состоящее из всех делителей числа c_j.

4) Рассматриваем всевозможные различные наборы чисел $d = d_0, \ldots, d_r$ таких, что $d_i \in C_i$.

5) Для каждого такого набора строим интерполяционный многочлен g_d по точкам $0, 1, \ldots, r$ в которых многочлен принимает значения $d_0, \ldots, d_r$.

6) Проверяем, делится ли f на g_d. Если разделился на какой-то, то алгоритм заканчивает свою работу и возвращает $g = g_d$.

7) Если ни для какого набора $d = d_0, \ldots, d_r$ многочлен f не разделился на g_d, то f неприводим. Алгоритм завершает свою работу.