Многочлены над конечными полями

Определение. Многочленом $f(x)$ над конечным полем $\mathbb{F}$ называется формальная сумма вида

$$f(x) = f_0 + f_1 x + \ldots + f_m x^m, f_i \in \mathbb{F}, f_m \neq 0.$$

Множество многочленов над полем $\mathbb{F}$ обозначается $\mathbb{F}[x]$.

0. **(а)** Сформулируйте и докажите теорему Безу для многочленов над полем $\mathbb{F}$.
(б) Сформулируйте и докажите теорему Виета для многочленов над полем $\mathbb{F}$.

1. **(а)** Разложите на множители над $\mathbb{Z}_p$ многочлен $x^{p-1} - 1$.
(б) Пользуясь предыдущим пунктом, докажите теорему Вильсона:
$(p-1)! \equiv -1 \ (mod \ p)$ при простом p.
(в) Найдите сумму $\sum\limits_{0<x<y<z<p} xyz \ (mod \ p)$.

2. **(а)** Пусть $f(x), g(x) \in \mathbb{Z}_p[x]$. При этом для любого $c \in \mathbb{Z}_p$ выполнено $f(c) = g(c)$. Докажите, что $f(x) - g(x)$ делится на $x^p - x$.
(б) Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$ — произвольная функция. Тогда найдется многочлен $f(x) \in \mathbb{Z}_p[x]$, для которого при любом c выполнено $f(c) = g(c)$. (Другими словами, при работе с полем $\mathbb{Z}_p$ не имеет смысла рассматривать какие-либо функции кроме многочленов)

3. Пусть для натурального числа n и простого числа p нашлись натуральные числа $a_1, \ldots, a_{n+1}$ такие, что их n-е степени дают одинаковые остатки при деление на p. Докажите, что какие-то a_i и a_j дают одинаковые остатки при деление на p.

4. Докажите, что над полем $\mathbb{Z}_p$ существует бесконечно много неприводимых многочленов. (Неприводимый многочлен — это многочлен, который нельзя представить в виде произведения двух многочленов ненулевой степени)

5. $f(x) \in \mathbb{Z}[x], f(0) = 0, f(1) = 1$. Простое число p такого, что для любого целого n остаток от деления $f(n)$ на p равен 0 или 1. Докажите, что $\deg(f) \geqslant p - 1$.

6. **Критерий Эйзенштейна.** Пусть $f(x)$ — многочлен с целыми, у которого старший коэффициент не делится на простое число p, все остальные коэффициенты делятся на p, а свободный член не делится на p^2. Тогда $f(x)$ неприводим над $\mathbb{Z}$.

7. Докажите, что многочлен $x^{n-1} + x^{n-2} + \cdots + 1$ неприводим тогда и только тогда, когда n — простое число.

8. Существует ли пара многочленов с целыми коэффициентами $P(x)$ и $Q(x)$ степени выше первой, удовлетворяющих тождеству

$$P(Q(x)) = x^{3375} + 3375x^{3374} + 2x + 1?$$