Многочлены над полем $\mathbb{Z}_p$

Определение. Множество элементов F с введёнными на нём алгебраическими операциями сложения $+$ и умножения $*$ ($\forall a, b \in F \quad (a+b) \in F,\ a*b \in F$) называется *полем* $(F, +, *)$, если выполнены следующие аксиомы:

- Коммутативность сложения: $\forall a, b \in F \quad a + b = b + a$.
- Ассоциативность сложения: $\forall a, b, c \in F \quad (a + b) + c = a + (b + c)$.
- Существование нулевого элемента: $\exists 0 \in F\colon \forall a \in F \quad a + 0 = a$.
- Существование противоположного элемента: $\forall a \in F\ \exists(-a) \in F\colon a + (-a) = 0$.
- Коммутативность умножения: $\forall a, b \in F \quad a * b = b * a$.
- Ассоциативность умножения: $\forall a, b, c \in F \quad (a * b) * c = a * (b * c)$.
- Существование единичного элемента: $\exists 1 \in F\colon \forall a \in F \quad a * 1 = a$.
- Существование обратного элемента для ненулевых элементов:
$(\forall a \in F\colon a \neq 0)\ \exists a^{-1} \in F\colon a * a^{-1} = 1$.
- Дистрибутивность умножения относительно сложения:
$\forall a, b, c \in F \quad (a + b) * c = (a * c) + (b * c)$.

1. Докажите, что множество остатков при делении на простое число p является полем. Оно обозначается $\mathbb{Z}_p$.

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 $\mathbb{F}[x]$.

2. **(a)** Сформулируйте и докажите теорему Безу для многочленов над полем $\mathbb{Z}_p$.
(b) Сформулируйте и докажите теорему Виета для многочленов над полем $\mathbb{Z}_p$.

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

4. **(a)** 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 $x^p - x$.
(b) 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.)

5. 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.

6. 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)

7. **(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 $\mathbb{Z}$. (То есть не представляется в виде произведения двух многочленов ненулевой степени с целыми коэффициентами)

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