Многочлены над $\mathbb{Z}_p$

Обозначение. $\mathbb{Z}_p$ — множество остатков при делении на простое p.

Определение. Многочлен $f(x) = a_0 + a_1x + ... + a_kx^k$ лежит над $\mathbb{Z}_p$, если $a_0, a_1, ..., a_k \in \mathbb{Z}_p$

Множество всех многочленов над $\mathbb{Z}_p$ обозначается через $\mathbb{Z}_p[x]$

Пусть даны два многочлена $f = a_0+a_1x+...+a_kx^k \in \mathbb{Z}_p[x]$ и $g = b_0+b_1x+...+b_mx^m \in \mathbb{Z}_p[x]$

- Суммой этих многочленов назовем многочлен $h = c_0+c_1x+...+c_qx^q \in \mathbb{Z}_p[x]$ такой, что $c_i \equiv a_i + b_i \mod p$
- Произведением этих многочленов назовем многочлен $h = c_0 + c_1x + ...c_qx^q \in \mathbb{Z}_p[x]$ такой, что $c_i \equiv \sum_{s+t=i} a_sb_t \mod p$

Определение. Значением многочлена $f = a_0 + a_1x + ... + a_kx^k \in \mathbb{Z}_p[x]$ в элементе $x_0 \in \mathbb{Z}_p$ называется элемент $f(x_0) \in \mathbb{Z}_p$ такой, что $f(x_0) \equiv a_0 + a_1x_0 + ... + a_kx_0^k \mod p$

Определение. Неприводимый многочлен — это многочлен, который нельзя представить в виде произведения двух многочленов ненулевой степени.

1. **(а)** Разложить на неприводимые множители многочлен $f(x) = x^2 + x + 1$ с коэффициентами в $\mathbb{Z}_3$.

   (б) Разложить на неприводимые множители многочлен $f(x) = x^3 + x + 1$ с коэффициентами в $\mathbb{Z}_3$.

   (в) Разложить на неприводимые множители многочлен $f(x) = x^4 + x^2 + 1$ с коэффициентами в $\mathbb{Z}_2$.

2. Для каждого простого p найдите количество неприводимых над $\mathbb{Z}_p$ многочленов степени 3.

3. **(а)** Пусть $f, g \in \mathbb{Z}_p[x]$. 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 $h : \mathbb{Z}_p \to \mathbb{Z}_p$ — произвольная функция. Докажите, что найдется многочлен
   $f \in \mathbb{Z}_p[x]$, для которого при любом $c \in \mathbb{Z}_p$ выполнено $f(c) = h(c)$.

   (в) Докажите, что в прошлом пункте найдется такой многочлен степени не выше $p - 1$.

4. Назовём многочлен с коэффициентами в $\mathbb{Z}_p$ перестановочным по модулю p, если его значения дают все возможные остатки при делении на p. Существует ли перестановочный по модулю 101 многочлен степени **(а)** 17 **(б)** 100 **(в)** 10?

5. Пусть для натурального числа n и простого числа p нашлись натуральные числа $a_1, ..., a_{n+1}$ 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.

7. Пусть p — нечётное простое. Про целые числа $a_1, a_2, ..., a_p$ известно, что $a_1^k + a_2^k + ... + a_p^k$ делится на p при любом натуральном k. Докажите, что все a_i числа попарно сравнимы по модулю p.