Многочлены над $\mathbb{F}_p$

Полем $\mathbb{F}_p$ называется множество остатков по модулю p со стандартными операциями. *Многочленом над* $\mathbb{F}_p$ называется многочлен, коэффициенты которого являются числами из $\mathbb{F}_p$. Множество многочленов с коэффициентами в $\mathbb{F}_p$ мы будем обозначать через $\mathbb{F}_p[x]$.

Многочлены над $\mathbb{F}_p$ мало чем отличаются от обычных многочленов над $\mathbb{R}$. В частности, для них верны следующие утверждения.

Теорема Безу. Дан многочлен $P \in \mathbb{F}_p[x]$ и некоторый вычет a. Тогда существует многочлен Q, для которого $P(x) = (x-a)Q(x) + P(a)$.

Следствие. Количество корней с учётом кратности многочлена над полем $\mathbb{F}_p$ не превосходит его степени.

Теорема Виета. Пусть многочлен $P(x) \in \mathbb{F}_p[x]$ и $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_n \neq 0$ имеет корни $x_1, x_2, \ldots, x_n$. Тогда

$$\frac{a_{n-k}}{a_n} = (-1)^k \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} x_{i_1} x_{i_2} \ldots x_{i_k}, \quad k = 1, \ldots, n.$$

1. Поделите с остатком многочлен $P(x)$ на $Q(x)$ в случае

(а) $P(x), Q(x) \in \mathbb{F}_{11}[x]$: $P(x) = x^3$, $Q(x) = 6x^2 + x + 1$;

(б) $P(x), Q(x) \in \mathbb{F}_7[x]$: $P(x) = x^7 + 2x + 1$, $Q(x) = x - 3$.

2. **(а)** Разложите многочлен $x^{p-1} - 1$ на множители над полем $\mathbb{F}_p$.

(б) Выведите из предыдущих задач теорему Вильсона.

3. Ваня выписал на доску все упорядоченные наборы из трёх различных натуральных чисел $1 \leqslant x < y < z \leqslant p$. Затем он перемножил числа в каждой тройке, а результаты сложил. Какой остаток даёт получившееся число при делении на p?

4. **(а)** Пусть $f(x) \in \mathbb{F}_p[x]$. Докажите, что $f(x)^p = f(x^p)$.

(б) Докажите, что $C_{p^n}^k$ кратно p при любом натуральном $0 < k < p^n$.

5. Докажите, что любую функцию $f : \mathbb{F}_p \to \mathbb{F}_p$ можно задать многочленом степени не выше $p - 1$.

6. $f(x)$ и $g(x)$ — два многочлена над $\mathbb{F}_p$, где p — простое число. Известно, что для любого $x \in \mathbb{F}_p$ выполнено $f(g(x)) = x$. Докажите, для любого $x \in \mathbb{F}_p$ также имеет место равенство $g(f(x)) = x$.

7. 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.

8. Натуральные числа a, b, c, d таковы, что $a^2 + b^2 + ab = c^2 + d^2 + cd$. Докажите, что число $a + b + c + d$ — составное.