Кружок в "Хамовниках". 2022-2023 учебный год. 9 класс.

Многочлены над полем $\mathbb{F}_p$

Пусть p — простое число. Обозначим через $\mathbb{F}_p$ множество (поле) остатков от деления на p. Через $0 \in F_p$ будем обозначать нулевой остаток. Множество $\mathbb{F}_p$ состоит из p элементов, которые можно умножать, складывать и вычитать. Более того, любой элемент $a \in F_p$ можно поделить на любой $0 \neq b \in \mathbb{F}_p$. Сложение и умножение являются ассоциативными и коммутативными операциями, дистрибутивность тоже выполняется.

Многочленом $P(x)$ с коэффициентами в $\mathbb{F}_p$ назовём формальное выражение

$$P(x) = a_0 + a_1 x + \ldots + a_k x^k + \ldots,$$

где x — формальная переменная, $a_0, \ldots, a_k, \ldots \in \mathbb{F}_p$ и только конечное число a_i ненулевые. Многочлены можно складывать и умножать, как обычно:

$$(a_0 + \ldots + a_k x^k + \ldots) + (b_0 + \ldots + b_k x^k + \ldots) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_k + b_k)x^k + \ldots$$
$$(a_0 + \ldots + a_k x^k + \ldots) - (b_0 + \ldots + b_k x^k + \ldots) = (a_0 - b_0) + (a_1 - b_1)x + \ldots + (a_k - b_k)x^k + \ldots$$
$$(a_0 + \ldots + a_k x^k + \ldots) \cdot (b_0 \ldots + b_k x^k + \ldots) = (a_0 \cdot b_0) + (a_1 b_0 + a_0 b_1)x \ldots + (a_k b_0 + a_{k-1} b_1 + \ldots + a_0 b_k)x^k + \ldots$$

Часто для краткости мы будем пропускать нулевые слагаемые и записывать многочлены в виде

$$P(x) = a_0 + a_1 x + \ldots + a_n x^n.$$

Множество многочленов с коэффициентами в $\mathbb{F}_p[x]$ мы будем обозначать через $\mathbb{F}_p[x]$.

Степенью многочлена $P(x) = a_0 + a_1 x + \ldots + a_k x^k + \ldots$ называется наибольшее целое d такое, что $a_d \neq 0$. Будем обозначать её через $\deg P(x)$. У нулевого многочлена степень не определена.

Многочлены $P(x) \in \mathbb{F}_p[x]$ можно вычислять на остатках. Иными словами, если $P(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{F}_p[x]$ и $c \in \mathbb{F}_p$ — остаток, то $P(c) = a_0 + a_1 c + \ldots + a_n c^n \in \mathbb{F}_p[x]$ — тоже остаток.

1. Для многочленов $P(x), Q(x) \in \mathbb{F}_p[x]$ докажите, что **(a)** $\deg(P(x) + Q(x)) \leqslant \max(\deg P(x), \deg Q(x))$;
(b) $\deg(P(x)Q(x)) = \deg P(x) + \deg Q(x)$.

2. Пусть $P(x), Q(x) \in \mathbb{F}_p[x]$. Докажите по индукции по $\deg P(x)$, что многочлен $P(x)$ можно поделить на $Q(x)$ с остатком. А именно, что существуют многочлены $S(x), R(x) \in \mathbb{F}_p[x]$ такие, что $\deg R(x) < \deg Q(x)$ и $P(x) = Q(x)S(x) + R(x)$.

3. Поделите с остатком многочлен $P(x)$ на $Q(x)$ в случае
(a) $P(x), Q(x) \in \mathbb{F}_{13}[x]$: $P(x) = x^7$, $Q(x) = x^2 - 1$
(b) $P(x), Q(x) \in \mathbb{F}_{11}[x]$: $P(x) = x^3$, $Q(x) = 6x^2 + x + 1$
(c) $P(x), Q(x) \in \mathbb{F}_7[x]$: $P(x) = x^7 + 2x + 1$, $Q(x) = x - 3$

4. **(a)** Пусть $a_1, \ldots, a_k$ — различные остатки. Докажите, что многочлен $P(x) \in \mathbb{F}_p[x]$ делится на произведение $(x - a_1) \cdot \ldots \cdot (x - a_k)$ тогда и только тогда, когда все a_i являются корнями $P(x)$.

(b) Докажите, что у многочлена степени $n \geqslant 0$ над $\mathbb{F}_p$ не более n различных корней.

Кратностью корня a многочлена $P(x) \in \mathbb{F}_p[x]$ называется наибольшее целое k такое, что $P(x)$ делится на $(x - a)^k$. Будем обозначать её через $\mathrm{mult}_P(a)$.

5. **(a)** Докажите, что $\mathrm{mult}_{P \cdot Q}(a) = \mathrm{mult}_P(a) + \mathrm{mult}_Q(a)$.

(b) Докажите, что у многочлена степени $n \geqslant 0$ не более n корней с учётом кратности.

6. Разложите на множители многочлен **(a)** $x^p - x \in F_p[x]$; **(b)** $x^p - 2 \in F_p[x]$; **(c)** $1 + x + \ldots + x^{p-1} \in F_p[x]$.

7. **Теорема Виета.** . Пусть различные остатки $a_1, \ldots, a_n \in F_p[x]$ — корни многочлена $b_n x^n + \ldots + b_1 x + b_0$. Докажите, что

$$a_1 + \ldots + a_n = -\frac{b_{n-1}}{b_n}$$
$$a_1 a_2 + a_1 a_3 \ldots + a_{n-1} a_n = \frac{b_{n-2}}{b_n}$$
$$\ldots$$
$$a_1 a_2 \ldots a_n = (-1)^n \frac{b_0}{b_n}$$

8. Петя выписал в тетрадку все наборы из трёх 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?

9. **(a)** Докажите, что существует многочлен $P(x) \in \mathbb{F}_p[x]$ такой, что $P(0) = 1$ и $P(a) = 0$ для любого $a \in \mathbb{F}_p \backslash \{0\}$.

(b) Докажите, что любую функцию $\mathbb{F}_p \to \mathbb{F}_p$ можно задать многочленом.

В задачах ниже полезно следующее соображение. Пусть $f(x), g(x), h(x)$ — многочлены с целыми коэффициентами такие, что $f(x) = g(x)h(x)$. Обозначим через $[f(x)]_p \in \mathbb{F}_p[x]$ *редукцию* многочлена $f(x)$, а именно многочлен с коэффициентами в $\mathbb{F}_p$, получающийся из $f(x)$ заменой каждого коэффициента на его остаток от деления на p. Например, $[7x^2+6x-2]_3 = x^2+1$. Аналогично, обозначим через $[g(x)]_p$ и $[h(x)]_p$ редукции многочленов $g(x)$ и $h(x)$, соответственно. Тогда $[f(x)]_p = [g(x)]_p \cdot [h(x)]_p$.

10. Докажите, что многочлен с целыми коэффициентами $3x^{100}+6x^{50}+5$ нельзя представить в виде произведения многочленов с целыми коэффициентами.

11. Пусть p — простое число. Докажите, что многочлен с целыми коэффициентами $f(x) = x^{2p} + px^{p+1} - 1$ нельзя представить в виде произведения многочленов с целыми коэффициентами.

12. Многочлен $(x+1)^n - 1$ с целыми коэффициентами делится на многочлен $x^k + a_{k-1}x^{k-1} + \ldots + a_1x + a_0$ чётной степени k, у которого все коэффициенты нечётны. Докажите, что n делится на $k+1$.