Сюжет про многочлены и перестановки

(автор - доцент СПбГУ, к.ф.-м.н. М. А. Антипов)

Сюжет состоит из двух частей, первая из которых носит скорее ознакомительный характер. Задачи сюжета можно решать в любом порядке, при необходимости при решении пункта можно ссылаться на утверждения из предыдущих пунктов (даже если Вы их не доказали). Мы рекомендуем участникам, не знакомым с арифметикой вычетов по модулю, тщательно изучить все задачи первой части.

В дальнейшем можно считать известной **малую теорему Ферма**:

если p — простое число, a — целое число, не кратное p, то число a^{p-1} даёт остаток 1 от деления на p.

Часть 1, вводящая в курс дела

Пусть $F[t]$ — многочлен с целыми коэффициентами, n — натуральное число, $Z_n = \{0, 1, \ldots, n-1\}$. Для каждого $a \in Z_n$ положим $F_n(a)$ равным остатку от деления $F(a)$ на n. Таким образом задаётся функция $F_n : Z_n \to Z_n$.

1. Докажите, что если числа a и b дают одинаковые остатки при делении на n, то числа $F(a)$ и $F(b)$ также дают одинаковые остатки при делении на n.

2. Пусть F, G — многочлены с целыми коэффициентами, $F \circ G$ — их композиция (т.е, многочлен, задаваемый формулой $(F \circ G)(x) = F(G(x))$). Докажите, что $(F \circ G)_n(x) = F_n(G_n(x))$ при любом x из Z_n.

3. Пусть n — нечётное число, F — многочлен с целыми коэффициентами такой, что $F_n(2) = F_n(n-2) = 0$. Докажите, что F можно записать в виде $(x^2-4)G(x) + ax + b$, где $G(x)$ — некоторый многочлен с целыми коэффициентами, а a и b — целые числа, кратные n. Приведите для $n = 10$ пример многочлена, для которого это утверждение неверно.

4. Докажите следующее утверждение.

Пусть F, G — многочлены с целыми коэффициентами, p — простое число. Функции F_p и G_p совпадают тогда и только тогда, когда многочлен $F - G$ можно представить в виде суммы двух многочленов, один из которых делится без остатка на многочлен $x^p - x$, а у второго все коэффициенты кратны p.

Подумайте, как описать такие многочлены F и G в случае, когда $n = p^2$ для некоторого простого числа p.

5. Пусть p — простое число. Докажите, что для любой функции $f : Z_p \to Z_p$ найдётся такой многочлен F с целыми коэффициентами, что f совпадает с соответствующей функцией F_p.

Часть 2, исследовательская

Назовём многочлен F *перестановочным по модулю* p, если соответствующая функция F_p — перестановка (т.е., взаимно-однозначное соответствие) чисел 0, 1, 2, $p-1$.

1. Упорядочим простые числа по возрастанию: пусть p_n — n-ое простое число. Рассмотрим все многочлены с неотрицательными целыми коэффициентами, меньшими p_n, степень которых меньше p_n. Какова доля перестановочных (по модулю p_n) многочленов среди них? Найдите предел этой доли при $n \to \infty$.

2. Пусть $p > 2$ — простое число. Докажите, что среди многочленов второй степени со старшим коэффициентом, не делящимся на p, нет перестановочных по модулю p. Приведите пример многочлена четвёртой степени со старшим коэффициентом 1, перестановочного по модулю p при каком-нибудь $p > 3$.

3. Пусть $p > 3$ — простое число. Опишите все перестановочные по модулю p многочлены третьей степени со старшим коэффициентом, не кратным p.

4. Даны два многочлена:

$$x + 1, \qquad x^{p-2} + x^{p-3} + \ldots + x^3 + x^2 + kx + 1.$$

Разрешается несколько раз подставлять один многочлен в другой, а также заменять многочлен на его остаток от деления на $x^p - x$. Сколько различных многочленов степени меньше p (с точностью до слагаемых, все коэффициенты которых кратны p), можно получить такими операциями при $k = 2$? А при $k = 1$?