

## Многочлены над полем $\mathbb{Z}_p$

группа 10-2

17.10.16

**Определение.** Многочленом  $f(x)$  над конечным полем  $\mathbb{F}$  называется формальная сумма вида

$$f(x) = f_0 + f_1x + \dots + f_mx^m, f_i \in \mathbb{F}, f_m \neq 0.$$

Множество многочленов над полем  $\mathbb{F}$  обозначается  $\mathbb{F}[x]$ .

- (а) Сформулируйте и докажите теорему Безу для многочленов над полем  $\mathbb{F}$ .

(б) Сформулируйте и докажите теорему Виета для многочленов над полем  $\mathbb{F}$ .
- (а) Разложите на множители над  $\mathbb{Z}_p$  многочлен  $x^{p-1} - 1$ .

(б) Пользуясь предыдущим пунктом, докажите теорему Вильсона:  $(p-1)! \equiv -1 \pmod{p}$  при простом  $p$ .

(с) Найдите сумму  $\sum_{0 < x < y < z < p} xyz \pmod{p}$ .
- (а) 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  $x^p - x$ .

(б) Пусть  $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  — 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)
- Пусть для натурального числа  $n$  и простого числа  $p$  найдлись натуральные числа  $a_1, \dots, a_{n+1}$  такие, что их  $n$ -е степени дают одинаковые остатки при делении на  $p$ . Докажите, что какие-то  $a_i$  и  $a_j$  дают одинаковые остатки при делении на  $p$ .
- 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)
- (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)
- Докажите, что многочлен  $x^{n-1} + x^{n-2} + \dots + 1$  неприводим тогда и только тогда, когда  $n$  — простое число.

## Многочлены над полем $\mathbb{Z}_p$

группа 10-2

17.10.16

**Определение.** Многочленом  $f(x)$  над конечным полем  $\mathbb{F}$  называется формальная сумма вида

$$f(x) = f_0 + f_1x + \dots + f_mx^m, f_i \in \mathbb{F}, f_m \neq 0.$$

Множество многочленов над полем  $\mathbb{F}$  обозначается  $\mathbb{F}[x]$ .

- (а) Сформулируйте и докажите теорему Безу для многочленов над полем  $\mathbb{F}$ .

(б) Сформулируйте и докажите теорему Виета для многочленов над полем  $\mathbb{F}$ .
- (а) Разложите на множители над  $\mathbb{Z}_p$  многочлен  $x^{p-1} - 1$ .

(б) Пользуясь предыдущим пунктом, докажите теорему Вильсона:  $(p-1)! \equiv -1 \pmod{p}$  при простом  $p$ .

(с) Найдите сумму  $\sum_{0 < x < y < z < p} xyz \pmod{p}$ .
- (а) 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  $x^p - x$ .

(б) Пусть  $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  — 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)
- Пусть для натурального числа  $n$  и простого числа  $p$  найдлись натуральные числа  $a_1, \dots, a_{n+1}$  такие, что их  $n$ -е степени дают одинаковые остатки при делении на  $p$ . Докажите, что какие-то  $a_i$  и  $a_j$  дают одинаковые остатки при делении на  $p$ .
- 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)
- (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)
- Докажите, что многочлен  $x^{n-1} + x^{n-2} + \dots + 1$  неприводим тогда и только тогда, когда  $n$  — простое число.