МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

А. В. Чашкин

ЛЕКЦИИ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ

Учебное пособие

Содержание

1 Число неприводимых многочленов

Применим метод производящих функций для нахождения числа неприводимых многочленов над полем $\mathbb{Z}_p$. Число неприводимых многочленов степени n, укоторых коэффициент при старшей степени равен единице, обозначим через $P(n)$.

Лемма 1 *Для последовательности $P(n)$ справедливо рекуррентное равенство*

$$p^n = \sum_{m|n} mP(m). \tag{1.1}$$

Доказательство. Пусть $p_{1m}, p_{p2m}, \cdots, p_{P(m)m}$ — все неприводимые многочлены степени m. Нетрудно видеть, что, раскрывая скобки в произведении

$$\prod_{m=1}^{\infty} \prod_{k=1}^{P(m)} \Big(1 + p_{km} + (p_{km})^2 + \cdots + (p_{km})^l + \dots\Big), \tag{1.2}$$

получим сумму $\sum$ всевозможных произведений неприводимых многочленов, причем каждое произведение встретится в этой сумме ровно один раз. Так как каждый многочлен единственным образом раскладывается в произведение неприводимых многочленов, то в $\sum$ будет содержаться ровно p^n произведений степени n. Каждому неприводимому многочлену степени m поставим в соответствие одночлен x^m, а произведению (1.2) — произведение

$$\prod_{m=1}^{\infty} \prod_{k=1}^{P(m)} \Big(1 + x^m + (x^m)^2 + \cdots + (x^k m)^l + \dots\Big) = \prod_{m=1}^{\infty} \left(\frac{1}{1-x^n}\right)^{P(m)}. \tag{1.3}$$

Так как существует ровно p^n многочленов степени n, укоторых коэффициент при x^n равен единице, то легко видеть, что в ряду, получившемся после раскрытия скобок в (1.3), коэффициент при x^n будет равен p^n. Следовательно,

$$\frac{1}{1-px} = \prod_{m=1}^{\infty} \left(\frac{1}{1-x^n}\right)^{P(m)}. \tag{1.4}$$

Логарифмируя правую и левую части (1.4), получим новое равенство

$$\ln \frac{1}{1-px} = \sum_{m=1}^{\infty} P(m) \ln \frac{1}{1-x^n}.$$

Теперь, применяя формулу $\ln \frac{1}{1-x} = \sum_{n=1}^{\infty} \frac{1}{n} x^n$, разложим в ряд правую и левую части последнего равенства:

$$\sum_{n=1}^{\infty} \frac{1}{n} p^n x^n = \sum_{m=1}^{\infty} \sum_{k=1}^{\infty} \frac{1}{k} P(m) x^{km} = \sum_{n=1}^{\infty} \left(\sum_{km=n} \frac{1}{k} P(m) \right) x^n.$$

Приравнивая в получившемся равенстве коэффициенты при n-й степени x, находим

$$\frac{1}{n} p^n = \sum_{km=n} \frac{1}{k} P(m) = \sum_{m \mid n} \frac{m}{n} P(m).$$

Лемма доказана.

Для того, чтобы из равенства (1.1) в явном виде выразить функцию $P(n)$ воспользуемся формулой обращения Мебиуса, которую докажем далее в лемме (3). Сначала определим функцию Мебиуса

$$\mu(m) = \begin{cases} 1, & \text{если } n = 1; \\ (-1)^k, & \text{если } n \text{ — произведение } k \text{ простых чисел;} \\ 0, & \text{если } n \text{ делится на квадрат простого числа,} \end{cases}$$

и покажем, что имеет место следующее утверждение.

Лемма 2 *Справедливо равенство*

$$\sum_{m|n} = \begin{cases} 1, & \text{если } n = 1; \\ 0, & \text{если } n > 0. \end{cases} \tag{1.5}$$

Доказательство. Если $n = 1$, то единица является единственным делителем, и, следовательно, $\mu(1) = 1$. При $n > 1$ представим n в виде произведения простых чисел:$n = p_1^{q_1} \cdots p_r^{q_r}$. Легко видеть, что в сумме (1.5) нужно учитывать только делители без кратных множителей. Поэтому

$$\sum_{m|n} \mu(m) = \sum_{k=0}^{r} \sum_{1 \le i_1 < \cdots < i_k \le r} \mu(p_{i_1} \cdots p_{i_k}) = \sum_{k}^{r} = \sum \binom{r}{k} (-1)^k = 0.$$

Лемма доказана.

Лемма 3 *Функци $f(n)$ и $h(n)$, определенные на множестве целых положительных чисел, удовлетворяют равенству*

$$f(n) = \sum_{m|n} h(m) \qquad \textit{при всех } n \in \mathbb{N} \tag{1.6}$$

тогда и только тогда, когда

$$f(n) = \sum_{m|n} \mu(\frac{n}{m}) f(m) \qquad \textit{при всех } n \in \mathbb{N} \tag{1.7}$$

Доказательство. Покажем, что из (1.6) следует(1.7). Для этого прежде всего заметим, что

$$\sum_{m|n} \mu(\frac{n}{m}) f(m) = \sum_{m|n} \mu(m) f(\frac{n}{m}),$$

так как суммы, стоящие в обеих частях равенства, отличаются только порядком следования слагаемых. Затем в правую часть последнего равенства вместо $f(m)$ подставим правую часть равенства (1.6). Меняя в получившейся двойной сумме порядок суммирования и применяя лемму е(1), получим следующую цепочку равенств:

$$\begin{aligned}\sum_{m|n} \mu(m) f(\frac{n}{m}) &= \sum_{m|n} \mu(m) \sum_{k|\frac{n}{m}} h(k) = \\ &= \sum_{m|n} \sum_{k|\frac{n}{k}} \mu(m) h(k) = \sum_{km|n} \mu(m) h(k) = \\ &= \sum_{k|n} \sum_{m|\frac{n}{k}} \mu(m) h(k) = \sum_{k|n} h(k) \sum_{m|\frac{n}{k}} \mu(m) = h(n).\end{aligned}$$

Таким образом, справедливость равенства (1.7) установлена. Обратное утверждение доказывается аналогично. Лемма доказана.

Теоркма 1 *Для числа $P(n)$ неприводимых многочленов степени n справедливо равенство*

$$P(n) = \frac{1}{n} \sum_{m|n} \mu(\frac{n}{m}) p^m.$$

Доказательство. Из леммы (1) следует, что равенство (1.6) леммы (3) справедливо при $f(n) = p^n$ и $h(n) = nP(n)$ для всех натуральных n. Поэтому утверждение теоремы следует непосредственно из леммы (3). Теорема доказана.