Секция «Математика и механика»

Представление некоторых логарифмических функций в виде многочленов с малым числом ненулевых коэффициентов

Раинчик Варвара
Студент
Московский государственный университет имени М.В. Ломоносова,
Механико-математический факультет, Москва, Россия
E-mail: rainvar@rambler.ru

Обозначения: p - нечетное простое; $\zeta = e^{\frac{2\pi i}{p}}$ - примитивный корень из 1 степени p; $\lambda = 1 - \zeta,\ \eta_i = 1 - \lambda^i,\ i \geq 1$.

Теорема 1 (1) *Любой $x \in \mathbb{Z}[\zeta]$, взаимно простой с λ, единственным образом представим в виде:*

$$x \equiv g_0^{p\gamma_0}\eta_1^{\gamma_1} \cdot \ldots \cdot \eta_{p-1}^{\gamma_{p-1}} \pmod{\lambda^p},$$

где $g_0 \in \mathbb{Z}-$ произвольный фиксированный первообразный корень по модулю $p^2, 0 \leq \gamma_0 \leq p-2,\ 0 \leq \gamma_i \leq p-1$ для $i = 1, \ldots, p-1$.

Введём функции $e_m(x)$ для $m = 1, \ldots, p-1$:

$$e_m(x) = \gamma_m \pmod{p}$$

Теорема 2 *Для чисел $x, y \in \mathbb{Z}[\zeta]$ специального вида: $x = 1 - z\lambda,\ z \in \mathbb{Z},\ (z,p) = 1,\ y = 1 + z_1\lambda + \ldots + z_{p-1}\lambda^{p-1},\ z_i \in \mathbb{Z},\ (z_i,p) = 1,\ i = 1, \ldots, p-1$ верны фрмулы:*

$$e_m(x) \equiv \frac{1}{m}\sum_{d|m}\mu(d)z^{\frac{m}{d}} \pmod{p},$$

$$e_m(y) \equiv \frac{1}{m}\sum_{d|m}\mu(d)s_{\frac{m}{d}} \pmod{p},$$

где $\mu()-$ функция Мёбиуса; величины s_k даются выражением:

$$s_k = \frac{k}{(-1)^k}\sum \frac{(-1)^{l_1+\ldots+l_{p-1}}(l_1 + \ldots + l_{p-1} - 1)!}{l_1! \ldots l_{p-1}!} z_1^{l_1} \ldots z_{p-1}^{l_{p-1}}\lambda^k,$$

$k = l_1 + 2l_2 + \ldots + (p-1)l_{p-1}$.

В доказательства этих формул используются свойства символа норменного вычета, основные теоремы для его вычисления, доказанные в [2], и некоторые следствия из них, полученнные в [1].

Литература

1. Назаров В.В., Об использовании свойства коммутирования символа степенного вычета в схемах открытого распределения ключа. Диссертация, Москва, 2006.

2. Artin E., Tate J., Class field theory. Harvard, 1961.