Билет 6 Теорема о полноте системы полиномов в P_k

Теорема 1 Система полиномов по mod k ($k \geq 2$) полна в $P_k \Leftrightarrow k = p$, где p – простое число .

Доказательство:

$$j_i(x) = \begin{cases} 1, & x = i \\ 0, & x \neq i \end{cases}$$

Пусть $f(x_1, x_2, ..., x_n) \in P_k$.

Для любой функции $f(x_1, x_2, ..., x_n)$ из P_k имеет место представление :

$$f(x_1, x_2, ..., x_n) = \sum_{(\sigma_1, ..., \sigma_n)} j_{\sigma_1}(x_1) \dots j_{\sigma_n}(x_n) * f(\sigma_1, \sigma_2, \dots, \sigma_n) \, (mod\, k)$$

Вопрос о представимости функции f полиномами по $mod\, k$ сводится к вопросу о представимости в виде полиномов функций $j_0(x), ..., j_{k-1}(x)$.

Заметим, что :

$$j_\sigma(x) = j_0(x - \sigma).$$

Тогда :

$$f(x_1, x_2, ..., x_n) = \sum_{(\sigma_1, ..., \sigma_n)} j_0(x_1 - \sigma_1) \dots j_0(x_n - \sigma_n) * f(\sigma_1, \sigma_2, \dots, \sigma_n) \, (mod\, k)$$

Т.е. система полиномов по mod k полна тогда и только тогда , когда представима в виде полинома функции $j_0(x)$. Рассмотрим два возможных случая , когда k – простое число и когда k – составное число .

1.Пусть k=p, где p – простое число, то по малой теореме Ферма :

$$a^{k-1} \equiv 1 \, (mod\, k) \, (1 \leq a \leq k-1)$$

получаем :

$$j_0(x) = 1 - x^{k-1} \, (mod\, k)$$

$$f(x_1, x_2, ..., x_n) = \sum_{(\sigma_1, ..., \sigma_n)} (1 - (x_1 - \sigma_1)^{k-1}) ... (1 - (x_n - \sigma_n)^{k-1}) *$$
$$* f(\sigma_1, \sigma_2, \dots, \sigma_n) \, (mod \, k)$$

Затем перемножаем скобки по свойствам дистрибутивности, коммутативности и ассоциативности; приводим подобные слагаемые. Получим полином по модулю k для функции $f(x_1, x_2, \dots, x_n)$.

Существование полинома по модулю k для каждой k – значной функции при простых k доказано.

2.Пусть $k \neq p$. Тогда $k = k_1 * k_2$, где $k_1 \geq k_2 > 1$.

Докажем от противного , что в этом случае $j_0(x)$ не задается полиномом по модулю k.

Пусть функция $j_0(x)$ задается полиномом по модулю k :

$$j_0(x) = c_s x^s + c_{s-1} x^{s-1} + ... + c_1 x + c_0 \, (mod \, k)$$

При $x = 0$ получим :

$$j_0(0) = c_0 = 1$$

При $x = k_2$ получим :

$$j_0(k_2) = c_s k_2^s + c_{s-1} k_2^{s-1} + ... + c_1 k_2 + c_0 = 0 \, (mod \, k)$$

Откуда :

$$k_2 * (c_s k_2^{s-1} + c_{s-1} k_2^{s-2} + ... + c_1) = k - 1 \, (mod \, k)$$

Таким образом k и $k - 1$ делятся на k_2 .

Это возможно только, если $k_2 = 1$ – противоречие . Следовательно , при составных k никакой полином по модулю k не задает функцию $j_0(x)$. Теорема доказана .

Вспомогательные данные

Рассмотрим Z_p - поле вычетов по mod p .

Теорема 2 (малая теорема Ферма). Если a не делится на простое число p , то $a^{p-1} \equiv 1\,(mod\,p)$

Теорема 3 (теорема Эйлера). Если a и m взаимны просты, то $a^{\phi(m)} \equiv 1\,(mod\,m)$, где $\phi(m)$ - функция Эйлера

Теорема 4 (теорема Лагранжа). Пусть группа G конечна , и H-ее подгруппа. Тогда порядок G равен порядку H , умноженному на количество её левых или правых классов смежности (индекс)

Следствие из теоремы 4. Порядок конечной группы делится на порядок любой ее подгруппы

Малая теорема Ферма является следствием теоремы Эйлера. В свою очередь, теорема Эйлера является следствием теоремы Лагранжа, примененной к приведенной системе вычетов по модулю m.

Доказательство теоремы Эйлера :

Рассмотрим мультипликативную группу Z_n^* обратимых элементов кольца вычетов Z_n. Ее порядок равен $\phi(n)$ согласно определению функции Эйлера.Поскольку число a взаимно просто с n , соответствующий ему элемент $\bar{a}$ в Z_n является обратимым и принадлежит Z_n^* . Элемент $\bar{a} \in Z_n^*$ порождает циклическую подгруппу, порядок которой , согласно теореме Лагранжа, делит $\phi(n)$, отсюда $\bar{a}^{\phi(n)} = \bar{1}$.