Поэтому вопрос о представимости функции f полиномами по mod k сводится к вопросу о представимости в виде полиномов функций

$$j_0(x), \ldots, j_{k-1}(x).$$

В силу того, что

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

мы можем утверждать, что система полиномов по mod k полна тогда и только тогда, когда представима в виде полинома функция $j_0(x)$.

1. Пусть $k = p$. В этом случае, опираясь на малую теорему Ферма $a^{p-1} \equiv 1 \pmod p$ $(1 \leqslant a \leqslant p-1)$, получаем

$$j_0(x) = 1 - x^{p-1} \pmod p,$$

т. е. система полиномов полна в P_k*).

Можно указать другой способ решения этой же задачи. Будем искать представление функции $g(x)$, зависящей от одной переменной, в виде полинома, пользуясь методом неопределенных коэффициентов

$$g(x) = a_0 + a_1 x + \ldots + a_{p-1}x^{p-1}.$$

Мы получаем систему уравнений

$$\begin{aligned}
&a_0 + a_1 \cdot 0^1 + a_2 \cdot 0^2 + \ldots + a_{p-1} \cdot 0^{p-1} = g(0),\\
&a_0 + a_1 \cdot 1^1 + a_2 \cdot 1^2 + \ldots + a_{p-1} \cdot 1^{p-1} = g(1),\\
&a_0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + \ldots + a_{p-1} \cdot 2^{p-1} = g(2),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&a_0 + a_1(p-1)^1 + a_2(p-1)^2 + \ldots + a_{p-1}(p-1)^{p-1} =\\
&\qquad\qquad = g(p-1).
\end{aligned}$$

Определитель этой системы

$$\Delta = \begin{vmatrix}
1 & 0 & 0 & \ldots & 0\\
1 & 1 & 1^2 & \ldots & 1^{p-1}\\
1 & 2 & 2^2 & \ldots & 2^{p-1}\\
\ldots & \ldots & \ldots & \ldots & \ldots\\
1 & p-1 & (p-1)^2 & \ldots & (p-1)^{p-1}
\end{vmatrix}$$

есть определитель Вандермонда. Как известно,

$$\Delta = \prod_{0 < i < j < p-1} (j - i).$$

*) Малая теорема Ферма обосновывается так. Пусть $1 \leqslant a \leqslant p-1$, тогда числа $r_1 = a \cdot 1, \ldots, r_{p-1} = a(p-1)$ не сравнимы по mod p. Поэтому $r_1 \ldots r_{p-1} \equiv (p-1)! \pmod p$ и $(p-1)! \equiv a^{p-1}(p-1)! \pmod p$ или $1 \equiv a^{p-1} \pmod p$.

Так как p — простое число, то $\Delta \not\equiv 0 \pmod p$. Пользуясь правилом Крамера и учитывая, что $\Delta \not\equiv 0 \pmod p$, мы сможем решить в целых числах сравнения

$$a_i \Delta \equiv \Delta_i \pmod p \quad (i = 0, \ldots, p-1),$$

где Δ_i — соответствующий минор. Итак, мы приходим к единственному решению исходной системы и, следовательно, к полиному, изображающему $g(x)$.

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

$$j_0(x) = b_0 + b_1 x + \ldots + b_s x^s \pmod k.$$

При $x = 0$ получаем $b_0 = 1$. При $x = k_1$ получаем

$$0 = 1 + b_1 k_1 + \ldots + b_s k_1^s \pmod k$$

или

$$k - 1 = b_1 k_1 + \ldots + b_s k_1^s \pmod k,$$

т. е. $k - 1$ делится на k_1. Таким образом, k и $k-1$ делятся на k_1, что возможно только при $k_1 = 1$. Мы пришли к противоречию. Следовательно, при $k \neq p$ функция $j_0(x)$ не представима полиномом по mod k.

Доказанная теорема может быть легко обобщена на случай, когда на E_k возможно определить две операции: $\oplus$ и $\times$ — сложение и умножение, относительно которых E_k образует поле. Как показывается в алгебре, конечное поле или поле Галуа, существует тогда и только тогда, когда $k = p^m$. В этом случае оно определяется с точностью до изоморфизма однозначным образом. При этом относительно сложения оно образует абелеву группу характеристики p, т. е. для любого элемента α выполняется соотношение

$$\underbrace{\alpha \oplus \ldots \oplus \alpha}_{p} = 0,$$

где 0 — нуль группы. Эту группу можно определить, рассматривая числа α, как числа в p-ичной системе счисления, т. е. в виде наборов $(\alpha_1, \ldots, \alpha_m)$, и операцию $\alpha \oplus \beta = (\alpha_1 + \beta_1, \ldots, \alpha_m + \beta_m)$ ($+$ обозначает сложение по mod p). Все элементы поля Галуа, кроме 0, образуют относительно второй операции циклическую группу.

Пример 5. Пусть $k = 2^2$. Тогда операция $\oplus$ имеет вид как в табл. 4. Для построения таблицы для операции $\times$ заметим, что числа 1, 2, 3 могут быть выражены