

Об определении наименьшего показателя ω , при котором выражение $X^\omega - 1$ делится нацело на многочлен $F(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n$, по простому модулю P .

Пусть

$$F(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n \quad . \quad . \quad . \quad (1)$$

будет неприводимая, по модулю p , функция.

Рассмотрим процесс алгебраического деления по простому модулю p выражения

$$x^{(0)} - 1$$

на многочлен

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n$$

Если частное от деления выразим в виде многочлена

$$E_0 x^{(0)-n} + E_1 x^{(0)-n-1} + E_2 x^{(0)-n-2} + \dots + E_{(0)-n-1} x + E_{(0)-n},$$

а остаток —

$$b_0 x^{n-1} + b_1 x^{n-2} + \dots + b_{n-2} x + b_{n-1},$$

то будем иметь следующее сравнение по модулю p .

$$x^{\omega-1} \equiv (x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n) (E_0 x^{\omega-n} + E_1 x^{\omega-n-1} + \\ + E_2 x^{\omega-n-2} + \dots + E_{\omega-n-1} x + E_{\omega-n}) + b_0 x_{n-1} + b_1 x_{n-2} + b_2 x_{n-3} + \dots + \\ + b_{n-2} x + b_{n-1} \pmod{p} \quad (2)$$

Произведя умножение и сравнивая по модулю p коэффициенты при одинаковых степенях x той и другой части сравнения (2), получим: ряд сравнений

$$\left. \begin{aligned} E_0 &\equiv 1 \\ E_1 + a_1 E_0 &\equiv 0 \\ E_2 + a_1 E_1 + a_2 E_0 &\equiv 0 \\ \dots\dots\dots \\ E_{n-1} + a_1 E_{n-2} + a_2 E_{n-3} + \dots + a_{n-2} E_1 + a_{n-1} E_0 &\equiv 0 \end{aligned} \right\} \dots\dots (3) \pmod{p}$$

для начальных значений $E_0, E_1, E_2, \dots, E_{n-1}$ коэффициентов частного; а также рекуррентную формулу для вычисления всех последующих коэффициентов частного при $i = n, n+1, \dots$.

$$E_i + a_1 E_{i-1} + a_2 E_{i-2} + \dots + a_n E_{i-n} \equiv 0 \pmod{p} \quad (I)$$

и следующий ряд сравнений для n последних значений коэффициентов частного

$$\left. \begin{aligned} &a_1 E_{\omega-n} + a_2 E_{\omega-n-1} + \dots + a_n E_{\omega-2n+1} + b_0' \equiv 0 \\ &a_2 E_{\omega-n} + a_3 E_{\omega-n-1} + \dots + a_n E_{\omega-2n+2} + b_1 \equiv 0 \\ &a_3 E_{\omega-n} + a_4 E_{\omega-n-1} + \dots + a_n E_{\omega-2n+3} + b_2 \equiv 0 \\ &\dots\dots\dots \\ &a_{n-1} E_{\omega-n} + a_n E_{\omega-n-1} + b_{n-2} \equiv 0 \\ &a_n E_{\omega-n-1} - 1 + b_{n-1} \equiv 0 \end{aligned} \right\} \quad \begin{array}{l} \dots\dots(4) \\ (\text{mod } p) \end{array}$$

Из сравнений (4), принимая во внимание (I), имеем:

$$\left. \begin{aligned} b_0 &\equiv -a_1 E_{\omega-n} - a_2 E_{\omega-n-1} - \dots - a_n E_{\omega-2n+1} \equiv E_{\omega-n+1} \\ b_1 &\equiv -a_2 E_{\omega-n} - a_3 E_{\omega-n-1} - \dots - a_n E_{\omega-2n+2} \equiv E_{\omega-n+2} + a_1 E_{\omega-n+1} \\ &\vdots \\ b_{n-2} &\equiv -a_{n-1} E_{\omega-n} - a_n E_{\omega-n-1} \equiv E_{\omega-1} + a_1 E_{\omega-2} + \dots + a_{n-2} E_{\omega-n+1} \\ b_{n-2} &\equiv -a_n E_{\omega-n+1} \equiv E_{\omega} + a_1 E_{\omega-1} + a_2 E_{\omega-2} + \dots + a_{n-1} E_{\omega-n+1} \end{aligned} \right\} \pmod p \quad . \quad (5)$$

На основании формул (5) остаток

$$b_0 x^{n-1} + b_1 x^{n-2} + b_2 x^{n-3} + \dots + b_{n-2} x + b_{n-1}$$

запишется в виде

$$E_{\omega-n+1} x^{n-1} + (E_{\omega-n+2} + a_1 E_{\omega-n+1}) x^{n-2} + \dots + E_{\omega} + (E_{\omega-1} a_1 + a_2 E_{\omega-2} + \dots + a_{n-1} E_{\omega-n+1}) - 1 \quad \dots \quad (6)$$

Вернемся теперь к сравнению (I) и заменим в нем i на $n+i$, тогда будем иметь

$$E_{i+n} + a_1 E_{i+n-1} + a_2 E_{i+n-2} + \dots + a_{n-1} E_{i+1} + a_n E_i \equiv 0 \pmod{p}$$

Из него, подставляя вместо i ряд значений $i = -1, -2, \dots, -n+1$, получим

[illegible]

Из сопоставления сравнений (3) и (7) получим ряд

$$E_{-n+1} \equiv E_{-n+2} \equiv \dots \equiv E_{-2} \equiv E_{-1} \equiv 0; E_0 \equiv 1 \pmod{p} \dots (8)$$

или

$$E_{-n+1}=0; E_{-n+2}=0; \dots E_{-2}=0; E_{-1}=0; E_0=1 \quad (\text{II})$$

Пусть $\alpha_1, \alpha_2, \dots, \alpha_n$, корни функции

$$F(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n$$

Выразим коэффициенты частного

$$E_0, E_1, E_2, \dots, E_n$$

в виде функций корней

$$\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha_n$$

Действительно, по самому смыслу алгебраической операции, имеем:

$$\frac{x^{\omega}-1}{F(x)}=x^{\omega-n}+E_1 x^{\omega-n-1}+E_2 x^{\omega-n-2}+\ldots+E_{\omega-n}+ \\ +\frac{E_{\omega-n+1}}{x}+\frac{E_{\omega-n+2}}{x^2}+\ldots-\frac{1}{F(x)} \ldots \ldots \ldots (9)$$

С другой стороны

$$\begin{aligned} \frac{x\omega - 1}{F(x)} &= x^{\omega-n} \cdot \frac{1}{1 - \frac{\alpha_1}{x}} \cdot \frac{1}{1 - \frac{\alpha_2}{x}} \cdot \dots \cdot \frac{1}{1 - \frac{\alpha_n}{x}} \cdot \frac{1}{F(x)} = \\ &= x^{\omega-n} \left(1 + \frac{\alpha_1}{x} + \frac{\alpha_1^2}{x^2} + \dots \right) \left(1 + \frac{\alpha_2}{x} + \frac{\alpha_2^2}{x^2} + \dots \right) \dots \left(1 + \frac{\alpha_n}{x} + \frac{\alpha_n^2}{x^2} + \dots \right) \end{aligned} \quad (10)$$

Из (9) и (10), находим:

$$\begin{aligned} E_1 &= \alpha_1 + \alpha_2 + \alpha_3 + \dots + \alpha_n = \sum \alpha_i \\ E_2 &= \alpha_1^2 + \alpha_2^2 + \dots + \alpha_n^2 + \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \dots + \dots = \sum \alpha_i^2 + \sum \alpha_i \alpha_j \\ &\dots \dots \dots \end{aligned}$$

Таким образом, каждое E_i есть целая однородная i -ой степени симметрическая функция всех корней уравнения.

$$F(x) \equiv 0$$

Предположим, что ω — наименьший показатель, при котором выражение $x^\omega - 1$ нацело делится по простому модулю p на неприводимую по этому модулю функцию $F(x)$.

В этом случае для коэффициентов остатка

$$b_0 x^{n-1} + b_1 x^{n-2} + \dots + b_{n-2} x + b_{n-1}$$

получим ряд сравнений

$$b_0 \equiv b_1 \equiv b_2 \equiv b_3 \equiv \dots \equiv b_{n-2} \equiv b_{n-1} \equiv 0 \pmod{p}$$

откуда на основании (5)

[illegible]

ИЛИ

$$E_{\omega-n+1} \equiv E_{\omega-n-2} \equiv \dots \equiv E_{\omega+1} \equiv 0; E_{\omega} \equiv 1 \pmod{p} \text{ (III)}$$

Таким образом, если ω есть наименьший показатель, при котором деление выражения $x^\omega - 1$ по простому модулю p на неприводимую по этому модулю функцию $F(x)$ совершается нацело, то ряд значений величин $E_0, E_1, \dots, E_i$ составляемый по рекуррентной формуле

$$E_i + a_1 E_{i-1} + \dots + a_n E_{i-n} \equiv 0 \pmod{p}$$

является по модулю p рядом периодическим, с числом членов периода ω .

Покажем, что для функции $F(x) = x^k F_1(x)$, где

$$F_i(x) = x^n + Ax^{n-1} + Bx^{n-2} + \dots + L \quad (12)$$



ряд значений E_i составит из k нулей и периодического ряда для функции (12), т. е.

$$\left. \begin{array}{c} 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ E_0 \\ E_1 \\ \cdot \\ \cdot \\ \cdot \end{array} \right\} \begin{array}{l} k \text{ нулей} \\ \\ \omega \\ \text{для функции} \\ x^n + Ax^{n-1} + Bx^{n-2} + \dots L \end{array}$$

В самом деле, функция $F(x)$ будет степени $n+k$ и, следовательно, для нее рекуррентная формула имеет вид

$$E_{n-k+1} \equiv 0; E_{n-k+2} \equiv 0; E_{n-k+3} \equiv 0; \dots E_1 \equiv 0; E_2 \equiv 1 \pmod{p}$$

Все дальнейшие значения $E_1, E_2, E_3, \dots$, будут совпадать со значениями величин $E'_1, E'_2, E'_3, \dots$ коэффициентов частного

$$\frac{x^\omega - 1}{F_1(x)}$$

и потому ряд значений величин E_i для функции $F(x)$ будет отличаться от такового же для $F_1(x)$ только тем, что в него войдут k нулей.

Пусть функция разлагается на ряд неприводимых функций $F_1(x), F_2(x), \dots, F_s(x)$, среди которых нет сравнимых между собой по модулю p .

Обозначим наименьшие показатели для функции $F(x)$ через ω , а для $F_1(x), F_2(x), \dots, F_s(x)$, соответственно, через

$$\omega_1, \omega_2, \dots, \omega_s.$$

Пусть

$$\omega_1 = \delta \omega'_1, \omega_2 = \delta \omega'_2, \dots, \omega_s = \delta \omega'_s$$

где δ есть общий наибольший делитель чисел

$$\omega_1, \omega_2, \dots, \omega_s,$$

тогда разности

$$x^\omega - 1, x^{\omega_1} - 1, \dots, x^{\omega_s} - 1$$

делятся соответственно нацело на

$$F(x), F_1(x), F_2(x), \dots, F_s(x)$$

В силу этого имеют место сравнения

$$\omega \equiv 0 \pmod{\delta\omega'_1}$$

$$\omega \equiv 0 \pmod{\delta\omega'_2}$$

$$\dots\dots\dots$$

$$\dots\dots\dots$$

$$\omega \equiv 0 \pmod{\delta\omega'_s}$$

и, следовательно, сравнение

$$\omega \equiv 0 \pmod{\omega_1, \omega_2, \dots, \omega_s}.$$

Значит, если функция $F(x)$ может быть представлена в виде произведения нескольких неприводимых и несоразмерных по модулю p функций

$$F_1(x), F_2(x), \dots, F_s(x),$$

то наименьший показатель ω для $F(x)$ равен общему наименьшему кратному соответственных наименьших показателей $\omega_1, \omega_2, \dots, \omega_s$ для функций $F_1(x), F_2(x), \dots, F_s(x)$

Пусть функция $F(x)$ разлагается на произведение множителей

$$F_1(x)^{m_1}, F_2(x)^{m_2}, \dots, F_s(x)^{m_s}$$

среди которых имеются сравнимые по модулю.

Обозначим через ω наименьший показатель, при котором деление $x^\omega - 1$ на функцию $F(x)$ совершается нацело, а через

$$\alpha_1, \alpha_2, \dots, \alpha_n$$

корни функции $F(x)$.

Если

$$\alpha_1 \equiv \alpha_2 \pmod{p}$$

то, так как каждое E есть целая однородная симметрическая функция корней уравнения $F(x) = 0$, имеем

$$\left. \begin{aligned} E_{\omega-n+1} &\equiv (\omega-n+2) \alpha_1^{\omega-n+1} + (\omega-n+1) \alpha_1^{\omega-n} E'_1 + \dots + E'_{\omega-n+1} \equiv 0 \\ E_{\omega-n+2} &\equiv (\omega-n+3) \alpha_1^{\omega-n+2} + (\omega-n+2) \alpha_1^{\omega-n+1} E'_1 + \dots + E'_{\omega-n+2} \equiv 0 \\ &\dots\dots\dots \\ E_{\omega-1} &\equiv \omega \alpha_1^{\omega-1} + (\omega-1) \alpha_1^{\omega-2} E'_1 + \dots + E'_{\omega-1} \equiv 0 \\ E_\omega &\equiv (\omega+1) \alpha_1^\omega + \omega \alpha_1^{\omega-1} E'_1 + \dots + E'_\omega \equiv 0, \end{aligned} \right\} \pmod{p}$$

где

$$E'_0, E'_1, E'_2, \dots, E'_\omega$$

коэффициенты частного

$$\frac{(x^\omega - 1)(x - \alpha_1)^2}{F(x)},$$

Запишем частное от деления функции $F(x)$ на $(x - \alpha_1)^2$ в виде такого многочлена

$$\frac{F(x)}{(x - \alpha_1)^2} = x^{n-2} + b_1 x^{n-3} + b_2 x^{n-4} + \dots + b_{n-2},$$

подставляя значения

$$E_\omega, E_{\omega-1}, \dots, E_{\omega-n+2}$$

в выражение

$$E_\omega + b_1 E_{\omega-1} + b_2 E_{\omega-2} + \dots + b_{n-2} E_{\omega-n+2},$$

получим

$$(\omega + 1) \alpha_1^\omega \equiv 1 \pmod{p}$$

Также, подставляя те же значения E в выражение

$$E_{\omega-1} + b_1 E_{\omega-2} + b_1 E_{\omega-3} + \dots + b_{n-2} E_{\omega-n+1},$$

найдем

$$\omega \alpha_1^{\omega-1} \equiv 0 \pmod{p}$$

Откуда следует, что

$$\omega \equiv 0 \pmod{p},$$

т. е. если функция $F(x)$ разлагается на произведение функций

$$F_1(x)^{m_1}, F_2(x)^{m_2}, \dots, F_s(x)^{m_s}$$

среди которых есть сравнимые по простому модулю p , то наименьший показатель ω делится на модуль p .