№ 53

Р. 1

(ТК) Лагранта о числе корней ур-ия по пр-му модулю

(ТК) (Лагранта)

$f(x) = a_n x^n + a_n x^{n-1} + \dots + a_0 \equiv 0 \pmod p$, где a_i - целые.

Тогда, если $\exists\ n+1$ р-е решение (по mod p), то $\forall i\ a_i \equiv 0 \pmod p$.

Т.е. ур-ие имеет n корней р-х наименьш.

Д-во

$$f(x) = a(x-x_1)(x-x_2)\dots(x-x_n) + \text{I}$$
$$+ b(x-x_1)(x-x_2)\dots(x-x_{n-1}) + \text{II}$$
$$\dots$$
$$+ k(x-x_1)(x-x_2) +$$
$$+ l(x-x_1) +$$
$$+ m$$

Подст. x_1

$0 \equiv f(x_1) = m \Rightarrow m \vdots p$

Подст x_2

$0 \equiv f(x_2) = l(x_2-x_1) + m \equiv l(x_2-x_1) \Rightarrow l(x_1-x_2) \vdots p \Rightarrow l \vdots p$

(т.к. $x_1 \not\equiv x_2 \pmod p$)

Подставим $x_3 \dots x_{n+1} \Rightarrow \begin{cases} a \vdots p \\ \vdots \\ m \vdots p \end{cases}$

т.к. $a_i \equiv \alpha_1 a + \alpha_2 b + \alpha_3 c + \dots + \alpha_{n+1} m \Rightarrow \forall i\ a_i = 0$ ЧТД