

Вспомогат. пр.-ме 2-5-3 для $d=1, n=p$.

12) p -простое. Среди $2p-1$ целых чисел найдется p чисел, таких что их сумма делится на p

Д-во

Д-н от противоположного.

Пусть $m(p) = 2p-1$. Т.е. $\exists a_1, a_2, \dots, a_{2p-1}$ чисел, таких что $\forall J \subset \{1, \dots, (2p-1)\} : |J| = p : \sum_{i \in J} a_i \not\equiv 0 \pmod{p}$.

$$\text{Пусть } S = \sum_{\substack{J \subset \{1, \dots, (2p-1)\} \\ |J| = p}} \left(\sum_{i \in J} a_i \right)^{p-1}$$

Лемма 1: $C_{2p-1}^p \equiv 1 \pmod{p}$

Лемма 2: $\forall q \in \{1, \dots, p-1\} C_{2p-1-q}^{p-q} \equiv 0 \pmod{p}$

По малой ТЛ Ферма $\left(\sum a_i \right)^{p-1} \equiv 1 \pmod{p} \Rightarrow S \equiv C_{2p-1}^p \equiv 1 \pmod{p}$

С другой стороны $\left(\sum_{i \in J} a_i \right)^{p-1}$ — это вып-е вида

$a_{i_1}^{2i_1} \dots a_{i_q}^{2i_q}$. Каждое такое вып-е возникает в S

столько раз, сколько таких $J \subset \{1, \dots, (2p-1)\}, |J| = p :$

$\{i_1, \dots, i_q\} \subset J$. А их ровно C_{2p-1-q}^{p-q} , где $1 \leq q \leq p-1$.

Тогда каждый коэф. в S имеет вид $C_{2p-1-q}^{p-q} \equiv 0 \pmod{p}$,

$\Rightarrow S \equiv 0 \pmod{p} ?!$ 