Основы комбинаторики и теории чисел

Сергей Григорян

12 декабря 2024 г.

Содержание

1 Лекция 15

Задача 1.1.

$$(a_1, b_1), \ldots, (a_f, b_f) \in \mathbb{Z}^2$$
$$m \in \mathbb{N}$$

Вопрос: при каком наим. f можно гарантировать, что сумма каких-то m пар по обоим коор-там делится на m.

Замечание. *$f \geq 4m - 3$. Пример: $m - 1$ раз повторяем $(1, 1)$, затем $m - 1$ раз $(0, 1)$, потом $(0, 0)$ и $(1, 0)$.*

Что думали люди:

- Гипотеза Кемница: $f = 4m - 3$
- 90-е — Алон и Дубинер: $f \leq 6m - 5, m >$
- 2000 год: Роньяи $f \leq 4m - 2$
- 2005 год: Райер: $f = 4m - 3$

Доказательство. Докажем это для $m = p$ — простое.

$$F(x_1, \ldots, x_n) \text{ — многочлен от } n \text{ переменных}$$
$$F(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$
$$F(x, y) = \sum c(a, b) x^a y^b$$

Причём члены суммы — одночлены/мономы.

Определение 1.1. Степень монома — сумма степеней входящих в него переменных

Определение 1.2. Степень полинома — наиб. степень мономов.

Теорема 1.1 (Шевалле-Варнинга)**.** *Пусть $F_1, \ldots, F_k \in \mathbb{Z}_p[x_1, \ldots, x_n]$ Пусть $\deg F_1 + \ldots + \deg F_k < n$. Рассм. систему сравнений:*

$$\begin{cases} F_1(x_1, \ldots, x_n) \equiv 0 \pmod p \\ \vdots \\ F_k(x_1, \ldots, x_n) \equiv 0 \pmod p \end{cases}$$

Утверждение теоремы: *Если $(0, \ldots, 0)$ — решение системы, то $\exists (x_1, \ldots, x_n)$ — нетривиальный набор, кот. тоже явл-ся решением системы.*

<u>Лемма</u> 1.2. *Пусть* $(a_1, b_1), \ldots, (a_{3p}, b_{3p}) \in \mathbb{Z}^2$ *и* $\sum_{i=1}^{3p} a_i \equiv \sum_{i=1}^{3p} \equiv 0 \pmod p$*. Тогда*

$$\exists I \subset \{1, 2, \ldots, 3p\}, |I| = p, \sum_{i \in I} a_i \equiv \sum_{i \in I} b_i \equiv 0 \pmod p$$

Доказательство. Сделаем 3 многочлена:

$$F_1(x_1, \ldots, x_{3p-1}) = \sum_{i=1}^{3p-1} a_i x_i^{p-1}$$

$$F_2(\ldots) = \sum_{i=1}^{3p-1} b_i x_i^{p-1}$$

$$F_3(\ldots) = \sum_{i=1}^{3p-1} x_i^{p-1}$$

$$\deg F_1 + \deg F_2 + \deg F_3 = 3p - 3 < 3p - 1$$

Заметим, что $(0, \ldots, 0)$ — удовл. трём мн-нам $\Rightarrow$ по т. Шевалле-Варнинга $\exists (x_1, \ldots, x_n)$, удовл. трём мн-нам, в кот. не все равны 0
Обозначим J — мн-во номеров этих x_i, кот. не равны 0.
Мы знаем:

$$\sum_{i=1}^{3p-1} a_i x_i^{p-1} \equiv 0 \pmod p$$

Заметим, что мы можем взять чисто ненулевые x_i, т. е. из J:

$$\sum_{i \in J} a_i x_i^{p-1} \equiv 0 \pmod p \overset{\text{МТФ}}{\equiv} a_i \equiv 0 \pmod p$$

Аналогично:

$$\sum_{i \in J} b_i \equiv 0 \pmod p$$

$$\sum_{i \in J} 1 \equiv 0 \pmod p$$

$$\Rightarrow |J| \in \{p, 2p\}$$

$$|J| = p \Rightarrow I := J$$

$$|J| = 2p \Rightarrow I := \{1, 2, 3, \ldots 3p\} \setminus J$$

Лемма доказана. □

Пусть $n = 4p - 2$. Предположим, что $\forall I \subset \{1, \ldots, n\}, |I| = p$, либо $\sum_{i \in I} a_i \not\equiv 0 \pmod p$, либо $\sum_{i \in I} b_i \not\equiv 0 \pmod p$ (Заметим, что отсюда следует то же самое и для $|I| = 3p$ по доказанной лемме)
Введём многочлен-КРОКОДИЛ:

$$F(x_1, \ldots, x_n) = \left(\left(\sum_{i=1}^{n} a_i x_i\right)^{p-1} - 1\right) \cdot \left(\left(\sum_{i=1}^{n} b_i x_i\right)^{p-1} - 1\right) \cdot$$

$$\cdot \left(\left(\sum_{i=1}^{n} x_i\right)^{p-1} - 1\right) \cdot (\sigma_p(x_1, \ldots, x_n) - 2)$$

Где $\sigma_p(x_1, \ldots, x_n)$ — симметрический мн-н:

$$\sigma_1(x_1, \ldots, x_n) = x_1 + \ldots + x_n$$

$$\sigma_2(x_1, \ldots, x_n) = x_1 x_2 + \ldots + x_{n-1} x_n$$

$$\sigma(3)(x_1, \ldots, x_n) = x_1 x_2 x_3 + \ldots + x_{n-2} x_{n-1} x_n$$

$$\vdots$$

Разберём КРОКОДИЛА по косточкам (битикам):

$$(x_1, \ldots, x_n) \in \{0, 1\}^n$$

1) Пусть число ненулевых коор-т равно p или $3p$, I — мн-во ненулвых коор-т:

$$\sum_{i=1}^{n} a_i x_i = \sum_{i \in I} a_i$$

$$\sum_{i=1}^{n} b_i x_i = \sum_{i \in I} b_i$$

Тогда $F(x_1, \ldots, x_n) \equiv 0 \pmod p$

2) Пусть число ненулевых коор-т равно $2p$, тогда:

$$\sigma_p(x_1, \ldots, x_n) = C_{2p}^{p} \equiv 2 \pmod p$$

$$\Rightarrow F \equiv 0 \pmod p$$

3) Пусть мн-во ненулевых коор-т имеет мощность, <u>не делящуюся на p</u>.

$$\Rightarrow \left(\left(\sum_{i=1}^{n} x_i\right)^{p-1} - 1\right) \equiv 0 \pmod p$$

$$\Rightarrow F \equiv 0 \pmod p$$

4) Остался единственный случай, когда $(x_1, \ldots, x_n) = (0, 0, \ldots, 0)$, тогда:

$$F(0, 0, \ldots, 0) = 2$$

Раскроем скобки, получим что слагаемое имеет соотв. вид, изменим его так:

$$cx_1^{\alpha_1} \ldots x_n^{\alpha_n} \to cx_1^{\beta_1} \ldots x_n^{\beta_n}$$

$$\alpha_i = 0 \Rightarrow \beta_i = 0$$

$$\alpha_i \geq 1 \Rightarrow \beta_i = 1$$

Получаем полином $\widetilde{F}(x_1, \ldots, x_n)$.
УЛЬТРА МЕГА КАТАРСИС:
на $(x_1, \ldots, x_n) \in \{0, 1\}^n \Rightarrow F = \widetilde{F}$. Получаем, что:

$$\widetilde{F} = 2(1 - x_1) \ldots (1 - x_n)$$

$$\deg \widetilde{F} = n = 4p - 2$$

$\square$