МАТЕМАТИКА

Арифметика вычетов по модулю

Шарич Владимир Златкович

Высшая школа экономики

Национальный исследовательский университет

Факультет математики

2018/2019

Теоремы про $\mathbb{F}_p$

Теоремы про $\mathbb{F}_p$

Теорема Вильсона

Теоремы про $\mathbb{F}_p$

Теорема Вильсона

Если $p \in \mathbb{P}$, то $(p-1)! \equiv_p -1$.

Теоремы про $\mathbb{F}_p$

Теорема Вильсона

Если $p \in \mathbb{P}$, то $(p-1)! \equiv_p -1$.

$\square$ Какие $\in \mathbb{F}_p$ являются корнями $x^{p-1} - 1$?

Теоремы про $\mathbb{F}_p$

Теорема Вильсона

Если $p \in \mathbb{P}$, то $(p-1)! \equiv_p -1$.

□ Какие $\in \mathbb{F}_p$ являются корнями $x^{p-1} - 1$?

$$x^{p-1} - 1 = (x-1)(x-2)...(x-(p-1))$$

Теоремы про $\mathbb{F}_p$

Теорема Вильсона

Если $p \in \mathbb{P}$, то $(p-1)! \equiv_p -1$.

□ Какие $\in \mathbb{F}_p$ являются корнями $x^{p-1} - 1$?

$$x^{p-1} - 1 = (x-1)(x-2)...(x-(p-1))$$

Свободные члены равны. ■

Простое число $p = 4k + 1$ является делителем числа вида $n^2 + 1$.

Простое число $p = 4k + 1$ является делителем числа вида $n^2 + 1$. $\square$ $n = (2k)!$ $\blacksquare$

Простое число $p = 4k + 1$ является делителем числа вида $n^2 + 1$. $\square$ $n = (2k)!$ $\blacksquare$

Теорема Ферма-Эйлера

Простое число $p = 4k + 1$ является делителем числа вида $n^2 + 1$. $\square$ $n = (2k)!$ $\blacksquare$

Теорема Ферма-Эйлера

Простое число $p = 4k + 1$ является суммой двух квадратов.

Простое число $p = 4k + 1$ является делителем числа вида $n^2 + 1$. $\square$ $n = (2k)!$ $\blacksquare$

Теорема Ферма-Эйлера

Простое число $p = 4k + 1$ является суммой двух квадратов.

$\square$ $p \mid n^2 + 1$

Простое число $p = 4k + 1$ является делителем числа вида $n^2 + 1$. $\square$ $n = (2k)!$ $\blacksquare$

Теорема Ферма-Эйлера

Простое число $p = 4k + 1$ является суммой двух квадратов.

$\square$ $p \mid n^2 + 1 = (n - \mathrm{i})(n + \mathrm{i})$.

Простое число $p = 4k + 1$ является делителем числа вида $n^2 + 1$. $\square$ $n = (2k)!$ $\blacksquare$

Теорема Ферма-Эйлера

Простое число $p = 4k + 1$ является суммой двух квадратов.

$\square$ $p \mid n^2 + 1 = (n - \mathrm{i})(n + \mathrm{i})$.

$n - \mathrm{i} = r_1 r_2 \ldots r_t$

Простое число $p = 4k + 1$ является делителем числа вида $n^2 + 1$. $\square$ $n = (2k)!$ $\blacksquare$

Теорема Ферма-Эйлера

Простое число $p = 4k + 1$ является суммой двух квадратов.

$\square$ $p \mid n^2 + 1 = (n - \mathrm{i})(n + \mathrm{i})$.

$n - \mathrm{i} = r_1 r_2 ... r_t \Rightarrow n + \mathrm{i} = \overline{r_1 r_2} ... \overline{r_t}$

Простое число $p = 4k + 1$ является делителем числа вида $n^2 + 1$. $\square$ $n = (2k)!$ $\blacksquare$

Теорема Ферма-Эйлера

Простое число $p = 4k + 1$ является суммой двух квадратов.

$\square$ $p \mid n^2 + 1 = (n - \mathrm{i})(n + \mathrm{i})$.

$n - \mathrm{i} = r_1 r_2 ... r_t \Rightarrow n + \mathrm{i} = \overline{r_1 r_2} ... \overline{r_t}$

Некоторые пары r_ℓ, $\overline{r_\ell}$ составляют разложение p. $\blacksquare$

Теоремы про $\mathbb{F}_p$

Теорема Шевалле.

Если P — однородный многочлен, степень которого меньше числа переменных, то сравнение $P \equiv_p 0$ имеет нетривиальное решение.

Теоремы про $\mathbb{F}_p$

Теорема Шевалле.
Если P — однородный многочлен, степень которого меньше числа переменных, то сравнение $P \equiv_p 0$ имеет нетривиальное решение.

□ Лемма. Если $P_1(x_1, ..., x_m) = P_2(x_1, ..., x_m)$ для всех $x_1, ..., x_m \in \mathbb{F}_p$, причём степени всех переменных в P_1 и в P_2 не превосходят $p - 1$, то P_1 и P_2 совпадают как многочлены.

Теоремы про $\mathbb{F}_p$

Теорема Шевалле.
Если P — однородный многочлен, степень которого меньше числа переменных, то сравнение $P \equiv_p 0$ имеет нетривиальное решение.

□ Лемма. Если $P_1(x_1, ..., x_m) = P_2(x_1, ..., x_m)$ для всех $x_1, ..., x_m \in \mathbb{F}_p$, причём степени всех переменных в P_1 и в P_2 не превосходят $p-1$, то P_1 и P_2 совпадают как многочлены.

Рассмотрим в $\mathbb{F}_p$ равенство
$1 - (P(x_1, ..., x_m))^{p-1} = (1 - x_1^{p-1})...(1 - x_m^{p-1})$. ■

Теоремы про $\mathbb{F}_p$

Теорема Шевалле-Варнинга.

Если P — однородный многочлен, степень которого меньше числа переменных, то количество решений сравнения $P \equiv_p 0$ в $(\mathbb{F}_p)^m$ положительно и кратно p.

Теоремы про $\mathbb{F}_p$

Теорема Шевалле-Варнинга.

Если P — однородный многочлен, степень которого меньше числа переменных, то количество решений сравнения $P \equiv_p 0$ в $(\mathbb{F}_p)^m$ положительно и кратно p.

□ Рассмотрим $X = \sum_{x_1,\ldots,x_m \in \mathbb{F}_p} (1 - P(x_1, \ldots, x_m)^{p-1})$

Теоремы про $\mathbb{F}_p$

Теорема Шевалле-Варнинга.

Если P — однородный многочлен, степень которого меньше числа переменных, то количество решений сравнения $P \equiv_p 0$ в $(\mathbb{F}_p)^m$ положительно и кратно p.

□ Рассмотрим $X = \sum_{x_1,\ldots,x_m \in \mathbb{F}_p} (1 - P(x_1, \ldots, x_m)^{p-1})$

Очевидное: $X \equiv_p |\{P = 0\}|$

Теоремы про $\mathbb{F}_p$

Теорема Шевалле-Варнинга.

Если P — однородный многочлен, степень которого меньше числа переменных, то количество решений сравнения $P \equiv_p 0$ в $(\mathbb{F}_p)^m$ положительно и кратно p.

□ Рассмотрим $X = \sum_{x_1,\ldots,x_m \in \mathbb{F}_p} (1 - P(x_1, \ldots, x_m)^{p-1})$

Очевидное: $X \equiv_p |\{P = 0\}|$

Неочевидное: $X \vdots p$

Теоремы про $\mathbb{F}_p$

Теорема Шевалле-Варнинга.

Если P — однородный многочлен, степень которого меньше числа переменных, то количество решений сравнения $P \equiv_p 0$ в $(\mathbb{F}_p)^m$ положительно и кратно p.

□ Рассмотрим $X = \sum_{x_1,\ldots,x_m \in \mathbb{F}_p} (1 - P(x_1, \ldots, x_m)^{p-1})$

Очевидное: $X \equiv_p |\{P = 0\}|$

Неочевидное: $X \vdots p$

$$\sum_{x_1,\ldots,x_m \in \mathbb{F}_p} x_1^{k_1} \cdot \ldots \cdot x_m^{k_m} = \left(\sum_{x_1 \in \mathbb{F}_p} x_1^{k_1}\right) \cdot \ldots \cdot \left(\sum_{x_1 \in \mathbb{F}_p} x_m^{k_m}\right)$$

■

Теоремы про $\mathbb{F}_p$

Кто все эти люди?

Теоремы про $\mathbb{F}_p$

Кто все эти люди?

Вильсон

Теоремы про $\mathbb{F}_p$

Кто все эти люди?

Вильсон Джон (Англия, 18 век)

Теоремы про $\mathbb{F}_p$

Кто все эти люди?

Вильсон Джон (Англия, 18 век)

Ферма

Теоремы про $\mathbb{F}_p$

Кто все эти люди?

Вильсон Джон (Англия, 18 век)

Ферма Пьер (Франция, 17 век)

Теоремы про $\mathbb{F}_p$

Кто все эти люди?

Вильсон Джон (Англия, 18 век)

Ферма Пьер (Франция, 17 век) Эйлер

Леонард (Швейцария, Германия, Россия, 18 век)

Теоремы про $\mathbb{F}_p$

Кто все эти люди?

Вильсон Джон (Англия, 18 век)

Ферма Пьер (Франция, 17 век) Эйлер

Леонард (Швейцария, Германия, Россия, 18 век)

Шевалле

Клод (Франция, 20 век)

Теоремы про $\mathbb{F}_p$

Кто все эти люди?

Вильсон Джон (Англия, 18 век)

Ферма Пьер (Франция, 17 век) Эйлер

Леонард (Швейцария, Германия, Россия, 18 век)

Шевалле

Клод (Франция, 20 век)

Варнинг

Эвальд (?, 20 век)

Функция и теорема Эйлера

Функция и теорема Эйлера

Обратимые вычеты.

Функция и теорема Эйлера

Обратимые вычеты.

Если $(a, n) = 1$, то $\exists b : \ ab \equiv_n 1$.

Функция и теорема Эйлера

Обратимые вычеты.

Если $(a, n) = 1$, то $\exists b: \ ab \equiv_n 1$.

Все такие a составляют группу $(\mathbb{Z}/n\mathbb{Z})^\times$.

Функция и теорема Эйлера

Обратимые вычеты.

Если $(a, n) = 1$, то $\exists b: \ ab \equiv_n 1$.

Все такие a составляют группу $(\mathbb{Z}/n\mathbb{Z})^\times$.

Функция Эйлера $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

Функция и теорема Эйлера

Обратимые вычеты.

Если $(a, n) = 1$, то $\exists b: \ ab \equiv_n 1$.

Все такие a составляют группу $(\mathbb{Z}/n\mathbb{Z})^\times$.

Функция Эйлера $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

Прикольное свойство $\sum_{n \vdots d} \varphi(d) = n.$

Функция и теорема Эйлера

Обратимые вычеты.

Если $(a, n) = 1$, то $\exists b: \ ab \equiv_n 1$.

Все такие a составляют группу $(\mathbb{Z}/n\mathbb{Z})^\times$.

Функция Эйлера $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

Прикольное свойство $\sum_{n \vdots d} \varphi(d) = n.$

Мультипликативность

Если $n_1 \perp n_2$, то $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$

Функция и теорема Эйлера

Обратимые вычеты.

Если $(a, n) = 1$, то $\exists b: \ ab \equiv_n 1$.

Все такие a составляют группу $(\mathbb{Z}/n\mathbb{Z})^\times$.

Функция Эйлера $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

Прикольное свойство $\sum_{n \vdots d} \varphi(d) = n.$

Мультипликативность

Если $n_1 \perp n_2$, то $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$

Как бы формула (для $n = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k}$)

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)$$

Теорема Эйлера

Функция и теорема Эйлера

Теорема Эйлера

Если $(m, a) = 1$, то $a^{\varphi(m)} \equiv_m 1$.

Функция и теорема Эйлера

Теорема Эйлера

Если $(m, a) = 1$, то $a^{\varphi(m)} \equiv_m 1$.

□ Теорема Лагранжа для группы $(\mathbb{Z}/m\mathbb{Z})^\times$. ■

Удачных занятий математикой!

Шарич В.З.
mathschool.ru/sharich

Фоксфорд

Высшая школа экономики
Национальный исследовательский университет

Математическая школа

Центр Педагогического Мастерства