

Квадратичные вычеты

Задача 7.1. Вычислите символы Лежандра:

а) $\left(\frac{-1}{p}\right)$; б) $\left(\frac{2}{p}\right)$; в) $\left(\frac{2027}{2029}\right)$; г) $\left(\frac{57}{179}\right)$; д) $\left(\frac{1147}{1999}\right)$.

Задача 7.2. Разрешимы ли сравнения:

а) $x^2 \equiv 666 \pmod{2017}$;

б) $x^2 \equiv 777 \pmod{2021}$,

в) $x^2 \equiv 999 \pmod{2022}$?

УКАЗАНИЕ. Числа 1999, 2017, 2027, 2029 — простые; число 2021 — составное.

Задача 7.3. а) Найдите количество решений уравнения $x^2 + y^2 = 1$ над $\mathbb{F}_p$.

б) Докажите, что уравнение $x^2 + y^2 = a$ разрешимо при любом $a \in \mathbb{F}_p$.

Задача 7.4. Пусть p нечетное простое число, и $p-1 = rs$. Докажите, что для ненулевого остатка a сравнение $x^r = a \pmod{p}$ разрешимо тогда и только тогда, когда $x^s = 1 \pmod{p}$.

Задача 7.5. Гипотеза Эйлера (доказанная Гауссом) утверждает, что для данного a для всех простых чисел p вида $4ap + r$ все символы Лежандра $\left(\frac{a}{p}\right)$ равны между собой¹. Выведите гипотезу Эйлера из квадратичного закона взаимности.

Задача 7.6. Докажите, что простых чисел вида:

а) $4k + 3$; б) $4k + 1$ бесконечно много.

УКАЗАНИЕ. В п. а) имитируйте доказательство Евклида. В п. б) воспользуйтесь описанием простых элементов в кольце гауссовых чисел.

▷ Теорема Дирихле (сложная) утверждает, что в любой арифметической прогрессии, в которой взаимно просты первый член и разность, бесконечно много простых чисел.

¹Ср. с утверждением о том, когда квадратичными вычетами или невычетами являются -1 и 2 — задача 7.1 аб).