Квадратичная взаимность

Задача 1. С помощью квадратичного закона взаимности выясните, разрешимо ли сравнение $x^2 = a \pmod{2017}$, где a — номер Вашей школы.

ПРИМЕЧАНИЕ. 2017 — простое число.

Задача 2 (еще одно доказательство). Пусть $p = 2k + 1$ простое.

а) Докажите, что лемму Гаусса о числе «положительных» остатков, переходящих в «отрицательные», можно переписать в виде

$$\left(\frac{q}{p}\right) = \prod_{m=1}^k \frac{\sin \frac{2\pi m q}{p}}{\sin \frac{2\pi m}{p}}.$$

б) Пусть $q = 2l + 1$. Докажите, что

$$\frac{\sin q\alpha}{\sin \alpha} = (-4)^l \prod_{n=1}^l \left(\sin^2 \alpha - \sin^2 \frac{2\pi n}{q} \right);$$

УКАЗАНИЕ. Рассмотрите левую часть как многочлен от $\sin^2 \alpha$. Чему равны его корни?

в)

$$\left(\frac{q}{p}\right) = (-4)^{kl} \prod_{m,n} \left(\sin^2 \frac{2\pi m}{p} - \sin^2 \frac{2\pi n}{q} \right).$$

г) Выведите из предыдущей задачи квадратичный закон взаимности.

Задача 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 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 5. Напомним, что гипотеза Эйлера утверждает, что для данного a для всех простых чисел p вида $4an+r$ все символы Лежандра $\left(\frac{a}{p}\right)$ равны между собой¹. Выведите гипотезу Эйлера из квадратичного закона взаимности.

Задача 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 (если вы понимаете, о чем идет речь).

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

Для получения зачета достаточно сдать 7 пунктов задач.

Евгений Юрьевич Смирнов: esmirnov@hse.ru

¹Ср. с утверждением о том, когда квадратичными вычетами/невычетами являются -1 и 2 .