Квадратичные вычеты и невычеты

Задача 1. а) Какие простые числа встречаются в разложении выражений вида n^2+1 на простые множители?

б) Докажите, что простых чисел вида $4k+1$ бесконечно много.

Задача 2. Докажите, что сравнение $ax^2+bx+c \equiv 0 \mod p$ имеет два решения по модулю p, если дискриминант — квадратичный вычет; не имеет решений, если дискриминант — квадратичный невычет; имеет ровно одно решение по модулю p, если дискриминант равен нулю по модулю p.

Задача 3 (теорема Жирара). Пусть x^2+y^2 делится на простое число p вида $4k+3$. Докажите, что x и y делятся на p.

Задача 4. С помощью квадратичного закона взаимости вычислите символы Лежандра:
а) $\left(\frac{57}{239}\right)$; **б)** $\left(\frac{179}{1543}\right)$; **в)** $\left(\frac{1789}{2017}\right)$.

Задача 5. Разрешимо ли по модулю 239 уравнение $x^2+57x+179=0$?

Доказательство квадратичного закона взаимности

Далее через p и q обозначаются различные нечетные простые числа.

Задача 6* (ключевая лемма). а) Покажите, что

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{n=1}^{(p-1)/2} \left\lfloor \frac{2nq}{p} \right\rfloor}$$

Задача 7*. Рассмотрим целые точки в прямоугольнике $1 \le x \le p-1$, $1 \le y \le q-1$.

а) Докажите, что прямая $y = qx/p$ не пересекает его по целым точкам.

б) Докажите, что число точек с *четными* абсциссами, лежащих ниже этой прямой, равно

$$\sum_{n=1}^{(p-1)/2} \left\lfloor \frac{2nq}{p} \right\rfloor,$$

а число точек с *нечетными* ординатами, лежащими выше этой прямой, равно

$$\sum_{m=1}^{(q-1)/2} \left\lfloor \frac{2pm}{q} \right\rfloor.$$

в) Докажите, что последние два числа имеют ту же четность, что и число целых точек в прямоугольнике $1 \le x \le \frac{p-1}{2}$, $1 \le y \le \frac{q-1}{2}$, лежащих соответственно ниже и выше прямой $y = qx/p$.

Задача 8* (квадратичный закон взаимности). Докажите, что

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Евгений Юрьевич Смирнов, esmirnov@hse.ru