10 класс | Квадратичный закон взаимности | 24 ноября 2014

Напоминание 1. Пусть $m > 1$ – натуральное число и a – целое число, взаимно простое с m. Число a называется *квадратичным вычетом* по модулю m, если существует $x \in \mathbb{N}$ такое, что $a \equiv x^2 \pmod{m}$. В противном случае число a называется *квадратичным невычетом* по модулю m.

Напоминание 2. Пусть p – простое число. *Символом Лежандра* называется выражение, обозначаемое $\left(\frac{a}{p}\right)$, равное 1, если a – квадратичный вычет по модулю p; –1, если a – квадратичный невычет по модулю p; и 0, если $a \vdots p$.

Напоминание 3. Символ Лежандра мультипликативен: $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$, где p – простое число.

Напоминание 4. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$, где p – простое нечётное число.

1. Пусть p – простое нечётное число, $t = \frac{p-1}{2}$, $0 < x \leq t$ и $(a, p) = 1$. Докажите, что

а) $ax \equiv (-1)^{[\frac{2ax}{p}]} \cdot r_x \pmod{p}$, где $0 < r_x \leq t$; **б)** $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{t}[\frac{2ax}{p}]}$.

2. Пусть p – простое нечётное число, $t = \frac{p-1}{2}$, $0 < x \leq t$ и a – нечётное число, взаимно простое с p. Докажите, что

а) $\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{t}[\frac{ax}{p}]+\frac{p^2-1}{8}}$; **б)** $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$; **в)** $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{t}[\frac{ax}{p}]}$.

3. а) Пусть p и q — различные простые нечётные числа. Рассмотрим прямоугольник на целочисленной решётке с вершинами в точках $(1, 1)$, $(1, \frac{q-1}{2})$, $(\frac{p-1}{2}, 1)$, $(\frac{p-1}{2}, \frac{q-1}{2})$. Посчитав точки внутри и на границе этого прямоугольника, докажите, что

$$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2} .$$

б) Квадратичный закон взаимности Гаусса. Докажите, что для любых различных нечётных простых чисел p и q верно

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} .$$

4. а) Пусть $(m, n) = 1$. Докажите, что число a является квадратичным вычетом по модулю mn тогда и только тогда, когда оно является квадратичным вычетом по модулям m и n.

б) Пусть p — нечётное простое число, $n \in \mathbb{N}$. Докажите, что a является квадратичным вычетом по модулю p^n тогда и только тогда, когда a является квадратичным вычетом по модулю p.

в) Докажите, что a является квадратичным вычетом по модулю 2^n (где $n > 3$) тогда и только тогда, когда a является квадратичным вычетом по модулю 8.

5. Докажите, что если число $2^n + 1$ — простое ($n > 1$), то 3 является его первообразным корнем.

6. Последовательность $\{x_n\}$ определена рекурсивно: $x_1 = a$ при некотором натуральном a, а также $x_{n+1} = 2x_n + 1$. Пусть $y_n = 2^{x_n} - 1$. Какое максимальное количество подряд идущих простых чисел может быть в последовательности $\{y_n\}$?

7. Докажите, что простых чисел вида $10k - 1$ бесконечно много.

Напоминание 1. Пусть $m > 1$ – натуральное число и a – целое число, взаимно простое с m. Число a называется *квадратичным вычетом* по модулю m, если существует $x \in \mathbb{N}$ такое, что $a \equiv x^2 \pmod{m}$. В противном случае число a называется *квадратичным невычетом* по модулю m.

Напоминание 2. Пусть p – простое число. *Символом Лежандра* называется выражение, обозначаемое $\left(\frac{a}{p}\right)$, равное 1, если a – квадратичный вычет по модулю p; –1, если a – квадратичный невычет по модулю p; и 0, если $a \vdots p$.

Напоминание 3. Символ Лежандра мультипликативен: $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$, где p – простое число.

Напоминание 4. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$, где p – простое нечётное число.

1. Пусть p – простое нечётное число, $t = \frac{p-1}{2}$, $0 < x \leq t$ и $(a, p) = 1$. Докажите, что

а) $ax \equiv (-1)^{[\frac{2ax}{p}]} \cdot r_x \pmod{p}$, где $0 < r_x \leq t$; **б)** $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{t}[\frac{2ax}{p}]}$.

2. Пусть p – простое нечётное число, $t = \frac{p-1}{2}$, $0 < x \leq t$ и a – нечётное число, взаимно простое с p. Докажите, что

а) $\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{t}[\frac{ax}{p}]+\frac{p^2-1}{8}}$; **б)** $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$; **в)** $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{t}[\frac{ax}{p}]}$.

3. а) Пусть p и q — различные простые нечётные числа. Рассмотрим прямоугольник на целочисленной решётке с вершинами в точках $(1, 1)$, $(1, \frac{q-1}{2})$, $(\frac{p-1}{2}, 1)$, $(\frac{p-1}{2}, \frac{q-1}{2})$. Посчитав точки внутри и на границе этого прямоугольника, докажите, что

$$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2} .$$

б) Квадратичный закон взаимности Гаусса. Докажите, что для любых различных нечётных простых чисел p и q верно

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} .$$

4. а) Пусть $(m, n) = 1$. Докажите, что число a является квадратичным вычетом по модулю mn тогда и только тогда, когда оно является квадратичным вычетом по модулям m и n.

б) Пусть p — нечётное простое число, $n \in \mathbb{N}$. Докажите, что a является квадратичным вычетом по модулю p^n тогда и только тогда, когда a является квадратичным вычетом по модулю p.

в) Докажите, что a является квадратичным вычетом по модулю 2^n (где $n > 3$) тогда и только тогда, когда a является квадратичным вычетом по модулю 8.

5. Докажите, что если число $2^n + 1$ — простое ($n > 1$), то 3 является его первообразным корнем.

6. Последовательность $\{x_n\}$ определена рекурсивно: $x_1 = a$ при некотором натуральном a, а также $x_{n+1} = 2x_n + 1$. Пусть $y_n = 2^{x_n} - 1$. Какое максимальное количество подряд идущих простых чисел может быть в последовательности $\{y_n\}$?

7. Докажите, что простых чисел вида $10k - 1$ бесконечно много.