

## Листок 4

### Тема 4(1.4). Квадратичные вычеты

#### Упражнения и задачи

1. Докажите, что существует бесконечно много простых  $p \equiv 1 \pmod{4}$  и  $p \equiv 3 \pmod{4}$ .
2. Докажите, что  $\left\lceil \frac{p-1}{4} \right\rceil$  четно  $\Leftrightarrow p = 8k \pm 1$ .
3. Докажите свойства символа Якоби:
  - $a \equiv b \pmod{P} \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$ ;
  - $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right) \left(\frac{b}{P}\right)$ ;
  - $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right) \left(\frac{a}{Q}\right)$ .
4. Пусть  $\alpha$  — иррациональное число. Докажите, что последовательность  $(\{n\alpha\})_{n=1}^{\infty}$  равномерно распределена  $\bmod 1$ .
5. Пусть  $p$  — простое,  $(a, p) = 1$ . Докажите, что число решений сравнения  $ax^2 + bx + c \equiv 0 \pmod{p}$  равно  $1 + \left(\frac{b^2 - 4ac}{p}\right)$ .
6. Докажите, что если  $(a, p) = 1$  то  $\sum_{x \bmod p} \left(\frac{ax+b}{p}\right) = 0$ .
7. Используя замену переменных, докажите, что число решений сравнения  $x^2 - y^2 \equiv a \pmod{p}$  равно  $p - 1$ , если  $(a, p) = 1$ , и  $2p - 1$ , если  $p|a$ . Выразите число решений этого сравнения через сумму с символом Лежандра. Используя эти выражения, найдите значение для суммы  $\sum_{y \bmod p} \left(\frac{y^2+a}{p}\right)$ .
8. Докажите, что если  $(a, p) = 1$  то  $\sum_{x \bmod p} \left(\frac{x(x+a)}{p}\right) = -1$ .
9. Пусть  $r_1, \dots, r_{(p-1)/2}$  — квадратичные вычеты в промежутке  $[1; p]$ . Докажите, что их произведение  $\equiv 1 \pmod{p}$ , если  $p \equiv 3 \pmod{4}$ , и  $\equiv -1 \pmod{p}$ , если  $p \equiv 1 \pmod{4}$ .
10. Пусть  $p \equiv 1 \pmod{4}$  — простое,  $(a, p) = 1$ ,  $S(a) = \sum_{x \bmod p} \left(\frac{x(x^2+a)}{p}\right)$ . Докажите, что
  - $S(a) \equiv 0 \pmod{2}$ ;
  - $S(at^2) = \left(\frac{t}{p}\right) S(a)$ ;
  - если  $r, n$  — такие, что  $\left(\frac{r}{p}\right) = 1$ ,  $\left(\frac{n}{p}\right) = -1$ , то  $p = \left(\frac{1}{2}S(r)\right)^2 + \left(\frac{1}{2}S(n)\right)^2$ .
11. Пусть  $f(x) \in \mathbb{Z}[x]$ . Будем говорить, что простое  $p$  делит  $f(x)$ , если  $\exists n \in \mathbb{Z}$  такое, что  $p|f(n)$ . Опишите простые делители многочленов  $x^2 + 1$  и  $x^2 - 2$ . Докажите, что если  $p$  делит  $x^4 - x^2 + 1$ , то  $p \equiv 1 \pmod{12}$ .
12. Пусть  $D > 0$  — нечетное и свободное от квадратов. Докажите, что  $\exists b \in \mathbb{Z}$ ,  $(b, D) = 1$  такое, что  $\left(\frac{b}{D}\right) = -1$ . Докажите также, что  $\sum' \left(\frac{a}{D}\right) = 0$ , где суммирование берется по приведенной системе вычетов  $\bmod D$ .

13. Пусть  $p$  — нечетное простое. Докажите, что

$$\left(\frac{2}{p}\right) = \prod_{j=1}^{(p-1)/2} 2 \cos\left(\frac{2\pi j}{p}\right),$$

а также, что если  $p > 3$  то

$$\left(\frac{3}{p}\right) = \prod_{j=1}^{(p-1)/2} \left(3 - 4 \sin^2\left(\frac{2\pi j}{p}\right)\right).$$

### SageMath

- Исследуйте основные функции SageMath связанные с вычислением квадратичных вычетов и символов Лежандра и Якоби:
  - Квадратичные вычеты: `quadratic_residues()`;
  - Символы: `kronecker()`, `jacobi()`.
- Пусть  $r(p)$  — наименьший квадратичный вычет  $\bmod p$ ,  $n(p)$  — наименьший квадратичный невычет  $\bmod p$ ,  $d(p)$  — максимальное расстояние между соседними квадратичными невычетами  $\bmod p$ . Постройте частотные таблицы для  $r(p)$ ,  $n(p)$ ,  $d(p)$ . Что можно заметить?  
(Согласно гипотезам Виноградова,  $\forall \varepsilon > 0 \frac{d(p)}{p^\varepsilon} \rightarrow 0, \frac{n(p)}{p^\varepsilon} \rightarrow 0, \frac{r(p)}{p^\varepsilon} \rightarrow 0$  при  $p \rightarrow \infty$ .)
- Проведите численные эксперименты относительно равномерного распределения последовательностей, которые упоминались в лекции:
  - $(\{n\alpha\})_{n=1}^\infty$ ,  $\alpha$  — иррациональное;
  - $(\{p\alpha\})_{p=1}^\infty$ ,  $\alpha$  — иррациональное,  $p$  пробегает все простые;
  - $(\{\frac{x_p}{p}\})_{p=1}^\infty$ ,  $x_p$  — решение сравнения  $x^2 \equiv a \pmod{p}$ ,  $p$  пробегает все простые.

### Темы для самостоятельного изучения

- Когда простое  $q$  является квадратичным вычетом по модулю простого  $p$ ? (Приложение квадратичного закона взаимности, [IR, §5.2, теорема 2]).
- Существует бесконечно много простых таких, что  $\left(\frac{a}{p}\right) = -1$ , где  $a$  — целое, отличное от квадрата. ([IR, §5.2, теорема 3]).
- Критерий разрешимости сравнения  $x^2 \equiv a \pmod{m}$  для произвольного  $m$ . ([IR, §5.1, предложение 5.1.1], [Вин, §V.4]).