

Серия 21, квадратичные вычеты

17 июля

В этом листочке p — простое число, не равное 2.

Упражнение. а) Для каждого ненулевого остатка a по простому модулю p существует единственный обратный остаток, т. е. такой остаток b , что $ab \equiv 1 \pmod{p}$. Обозначение: $b = a^{-1}$.

б) Остатки по простому модулю можно делить, т. е. сравнение $ax \equiv b \pmod{p}$ имеет единственное решение.

Определение. Ненулевой вычет a называется *квадратичным вычетом* по простому модулю p , если существует такое b , что $b^2 \equiv a \pmod{p}$. В противном случае a называется *квадратичным невычетом*. Таким образом, вычеты по модулю p разбиваются на 3 группы: нулевой вычет, квадратичные вычеты и квадратичные невычеты.

Задачи

1. Найдите все квадратичные вычеты по модулю 5, 7, 11, 13.
2. а) Докажите, что для ненулевого остатка c квадратное сравнение $x^2 \equiv c \pmod{p}$ имеет ровно два решения по модулю p или не имеет их вовсе.
б) Сколько существует квадратичных вычетов по модулю p ?
3. Докажите, что если x квадратичный вычет, то x^{-1} квадратичный вычет.
4. Докажите, что
 - а) произведение двух квадратичных вычетов — квадратичный вычет;
 - б) произведение квадратичного вычета и квадратичного невычета — квадратичный невычет;
 - в) произведение двух квадратичных невычетов — квадратичный вычет.
5. а) При каких p количество квадратичных вычетов чётно?
б) Докажите, что -1 квадратичный вычет тогда и только тогда, когда $p = 4k + 1$.
в) Используя теорему Вильсона о том, что $(p - 1)! \equiv -1 \pmod{p}$, предложите формулу для корня из -1 при $p = 4k + 1$.
6. 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.
7. Найдите сумму квадратичных вычетов по модулю p .
8. Докажите, что сравнение $ax^2 + bx + c \equiv 0 \pmod{p}$
 - а) имеет два решения по модулю p , если дискриминант — квадратичный вычет;
 - б) не имеет решений, если дискриминант — квадратичный невычет;

в) имеет ровно одно решение по модулю p , если дискриминант равен нулю по модулю p .

Определение. Символом Лежандра называется число

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \text{ делится на } p; \\ 1, & \text{если } a \text{ — квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ — квадратичный невычет по модулю } p. \end{cases}$$

Замечание. Утверждение задачи 4 можно переписать как $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.

Утверждение задачи 5 можно переписать как $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Критерий Эйлера. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

9. а) Проверьте критерий Эйлера для $p = 7$.

б) Докажите, что если a — квадратичный вычет по модулю p , то $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

в) Докажите критерий Эйлера для p вида $4k + 3$.

Указание: используйте, что -1 является квадратичным невычетом.

г) Докажите критерий Эйлера для p вида $4k + 1$.

10. Теорема Жирара. Пусть $x^2 + y^2$ делится на простое число p вида $4k + 3$. Докажите, что x и y делятся на p .

11. Решите в целых числах уравнение $x^3 + 7 = y^2$.