Квадратичные вычеты

Пусть дано натуральное число n. Число a, взаимно простое с n, называется *квадратичным вычетом по модулю* n, если $a \equiv x^2 \pmod p$ для некоторого целого числа x.

1. Докажите, что для каждого квадратичного вычета a по простому модулю p существует ровно два решения сравнения $x^2 \equiv a \pmod p$.
2. Докажите, что существует ровно $(p-1)/2$ квадратичных вычетов по простому модулю p.

Квадратичный закон взаимности

Символом Лежандра называется число $\left(\frac{a}{p}\right)$, в котором числитель a — целое число, не кратное знаменателю — простому числу p. Число $\left(\frac{a}{p}\right)$ равно 1, если a является квадратичным вычетом по модулю p, и равно -1, если a — квадратичный невычет.

3. *Критерий Эйлера.* Докажите, что $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.
4. Числа $a_1, \ldots, a_n$ не кратны p. Докажите, что $\left(\frac{a_1 \cdot \ldots \cdot a_n}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right)$.

Положим $d = (p-1)/2$ и для каждого натурального числа i от 1 до d найдём сравнение $a \cdot i \equiv \varepsilon_i r_i \pmod p$, где $\varepsilon_i = \pm 1$ и $1 < |r_i| \leqslant d$.

5. Докажите двойное равенство $\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \ldots \cdot \varepsilon_d = (-1)^{\sum_{i=1}^{d} \left[\frac{2a \cdot i}{p}\right]}$.
6. Для нечётных a и p докажите равенство $\left(\frac{2}{p}\right) \cdot \left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{d} \left[\frac{a \cdot i}{p}\right] + \frac{p^2-1}{8}}$.
7. Докажите равенство $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
8. Пусть $p \neq q$ — нечётные простые числа, докажите, что $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Равенство из предыдущей задачи называется *квадратичным законом взаимности.*

Символ Якоби

Пусть целое число a и натуральное число $n > 1$ взаимно просты и $n = p_1 \cdot \ldots \cdot p_k$ — разложение числа n на (не обязательно различные) простые множители. Произведение $\left(\frac{a}{p_1}\right) \cdot \ldots \cdot \left(\frac{a}{p_k}\right)$ символов Лежандра называется *символом Якоби* и обозначается так же: $\left(\frac{a}{n}\right)$.

9. Приведите пример квадратичного невычета a по модулю n, для которого $\left(\frac{a}{n}\right) = 1$.
10. Докажите равенство $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.
11. Числа $a_1, \ldots, a_m$ взаимно просты с n. Докажите, что $\left(\frac{a_1 \cdot \ldots \cdot a_m}{n}\right) = \left(\frac{a_1}{n}\right) \cdot \ldots \cdot \left(\frac{a_m}{n}\right)$.
12. Для нечётного n докажите равенство $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.
13. Докажите равенство $\left(\frac{n}{m}\right) \cdot \left(\frac{m}{n}\right) = (-1)^{\frac{(n-1)(m-1)}{4}}$ для любых различных нечётных взаимно простых натуральных чисел m и n.

Рассмотрим сравнение $x^2 \equiv a \pmod n$, как уравнение переменной x. Из КТО следует, что это уравнение достаточно рассматривать, когда n является степенью простого числа.

14. Пусть p — нечётное простое и $(a, p) = 1$. Докажите, что сравнение $x^2 \equiv a \pmod{p^k}$ имеет два решения, если $\left(\frac{a}{p}\right) = 1$, и не имеет решений, если $\left(\frac{a}{p}\right) = -1$.
15. Пусть a — нечётное число и $k \geqslant 3$. Докажите, что сравнение $x^2 \equiv a \pmod{2^k}$ имеет решения только при $a \equiv 1 \pmod 8$, причём таких решений ровно четыре.

Упражнения

Во всех упражнениях число p подразумевается простым.

16. Докажите, что произведение всех квадратичных вычетов по простому модулю p сравнимо с $(-1)^{\frac{p+1}{2}}$ по модулю p.
17. Числа a, b, c не кратны p. Докажите, $ax^2 + by^2 \equiv c \pmod p$ для некоторых $x, y \in \mathbb{Z}$.
18. Докажите, что число $2^{251} - 1$ является составным.
19. Пусть $f(x_1, \ldots, x_n)$ — многочлен второй степени с целыми коэффициентами такой, что $f(0, \ldots, 0) = 0$. Докажите, что при $n \geqslant 3$ сравнение $f(x_1, x_2, \ldots, x_n) \equiv 0$ имеет ненулевое решение по любому простому модулю.
20. Докажите, что у числа $2^n + 1$ нет простых делителей вида $8k + 7$.
21. Пусть $n, m \geqslant 3$ – натуральные числа. Докажите, что $2^m - 1$ не делит $3^n - 1$.
22. Докажите, что уравнение $y^2 = x^3 + 7$ не имеет решений в целых числах.
23. Докажите, что уравнение $y^2 = x^3 - 5$ не имеет решений в целых числах.
24. Существуют ли натуральные числа a, b, и c такие, что число $a^2 + b^2 + c^2$ делится на $2013(ab + bc + ac)$?
25. Натуральные числа a и b таковы, что оба числа $15a + 16b$ и $16a - 15b$ являются полными квадратами. Какое наименьшее значение может принимать меньший из этих квадратов?
26. Найдите натуральное число n между 100 и 1997 такое, что $n \mid 2^n + 2$.
27. Последовательность $(x_n)_{n\in\mathbb{N}}$ натуральных чисел удовлетворяет рекуррентному соотношению $x_{n+1} = 2x_n + 1$ при всех $n \geqslant 1$. Найдите наибольшее число k, для которого найдётся натуральное x_1 такое, что все числа $2^{x_1} - 1, 2^{x_2} - 1, \ldots, 2^{x_k} - 1$ являются простыми.
28. Докажите, что существует бесконечно много натуральных чисел n таких, что у числа $n^2 + 1$ есть простой делитель, больший чем $2n + \sqrt{2n}$. Докажите, что для любого натурального числа a, не являющегося полным квадратом, существует бесконечно много простых чисел p таких, что $\left(\frac{a}{p}\right) = -1$.