Теоретические задачи по курсу «Алгебра и теория чисел»

Примечание: во всех задачах p — простое число.

Разные задачи

1. Найти число решений уравнения $ax^2 + bx + c \equiv 0 \pmod{p}$ (при $a \not\equiv 0 \pmod{p}$).
2. Найти произведение всех квадратичных вычетов по модулю p.
3. Найти сумму всех квадратичных вычетов по модулю p.
4. Найти произведение всех первообразных корней по модулю p.
5. Пусть $n = 2^{2^k} + 1$ (число Ферма).
   a) Доказать, что если $3^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, то число n простое.
   b) Доказать, что если n простое, то $3^{\frac{n-1}{2}} \equiv -1 \pmod{n}$.
6. Пусть K — поле, $G < K^*$ — конечная подгруппа мультипликативной группы поля K. Докажите, что G — циклическая группа. Подсказка: доказательство аналогично доказательству существования первообразного корня по простому модулю.
7. Известно, что $x^4 - x^2 + 1$ делится на p при некотором целом x.
   a) Доказать, что $p \equiv 1 \pmod{3}$.
   b) Доказать, что $p \equiv 1 \pmod{4}$.
   c) Правда ли, что обязательно $p \equiv 1 \pmod{5}$?
   d) Правда ли, что если условия a и b выполнены, то такой x обязательно существует?
8. Доказать бесконечность простых чисел вида $p = 6k + 1$.
9. Пусть число a имеет порядок 3 по модулю p. Найти порядок числа $(1 + a)$ по модулю p.
10. Доказать, что уравнение $x^2 + y^2 \equiv a \pmod{p}$ имеет решение при любом a.
11. Вычислить $\left(\frac{113}{997}\right)$, $\left(\frac{215}{761}\right)$, $\left(\frac{514}{1093}\right)$, $\left(\frac{401}{757}\right)$.

Квадратичные сравнения по модулю 2^n

Рассмотрим уравнение $x^2 \equiv a \pmod{2^n}$ при нечётном a (x — неизвестная, a — параметр).

1. Решить это уравнение при $n \leq 3$ (для всех a).
2. Доказать, что если при $n > 3$ это уравнение имеет решение, то оно имеет ровно четыре решения.
3. Доказать, что при $n > 3$ это уравнение имеет решение тогда и только тогда, когда $a \equiv 1 \pmod{8}$.

Задача о сумме первообразных корней

1. Найти сумму всех первообразных корней по следующим модулям: $p = 11$, $p = 13$, $p = 31$.
2. Пусть $p = 4k + 1$. Доказать, что g — первообразный корень по модулю p тогда и только тогда, когда $(-g)$ — первообраный корень по модулю p.
3. Пусть $p - 1$ делится на q^2 при некотором простом q. Доказать, что сумма всех первообразных корней по модулю p равна нулю.
4. Доказать, что сумма всех первообразных корней по модулю p равна $\mu(p - 1)$.

Число решений уравнения $x^2 + y^2 \equiv 1 \pmod{p}$

1. Найти все решения этого уравнения при $p = 11$.
2. Доказать, что число решений этого уравнения равно $p + \sum\limits_{a=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{1-a}{p}\right)$.
3. Доказать, что $\sum\limits_{a=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{1-a}{p}\right) = (-1)^{\frac{p+1}{2}}$.

Соседние квадратичные вычеты

Определим следующие четыре величины:

- c_{rr} — это количество пар $(n, n+1)$ в множестве $1, 2, \ldots, p-1$ таких, что n и $n+1$ оба являются квадратичными вычетами;
- c_{nr} — это количество пар $(n, n+1)$ в множестве $1, 2, \ldots, p-1$ таких, что n — квадратичный невычет и $n+1$ — квадратичный вычет;
- c_{rn} — это количество пар $(n, n+1)$ в множестве $1, 2, \ldots, p-1$ таких, что n — квадратичный вычет и $n+1$ — квадратичный невычет;
- c_{nn} — это количество пар $(n, n+1)$ в множестве $1, 2, \ldots, p-1$ таких, что n оба являются квадратичными невычетами;

1. Найти суммы $c_{rr} + c_{rn}$, $c_{nr} + c_{nn}$, $c_{rr} + c_{nr}$, $c_{rn} + c_{nn}$.
2. Доказать, что $c_{rr} + c_{nn} - c_{rn} - c_{nr} = \sum\limits_{n=1}^{p-1} \left(\frac{n(n+1)}{p}\right)$ и доказать, что эта сумма равна -1.
3. Вычислить c_{rr}.

Разные задачи

1. Привести пример конечного поля из четырех элементов (выписать таблицы умножения и сложения).
2. Доказать, что если F — конечное поле, то число элементов в F равно p^e, где p — простое.
3. Пусть a_1 и a_2 — различные корни полинома $f(x)$ над полем $\mathbb{Z}/p\mathbb{Z}$. Рассмотрим случайное a и $g(x) = gcd((x+a)^{\frac{p-1}{2}} - 1, f(x))$. Доказать, что вероятность того, что ровно один из корней a_1 и a_2 является корнем $g(x)$ не меньше $\frac{1}{2} - \frac{1}{2p}$.