I. Вычеты и невычеты

Везде далее p — простое число (обычно не равное 2).

Задача 1. а) Уравнение $x^2 = a$ имеет по модулю p не более двух решений.
б) Квадратное уравнение по модулю p имеет не более двух решений.

▷ Ненулевой остаток a по модулю p называется *квадратичным вычетом*, если уравнение $x^2 = a \pmod p$ имеет решение, *квадратичным невычетом* в противном случае.

Задача 2. Сколько всего квадратичных вычетов по модулю p?

Задача 3. а) Произведение квадратичных вычетов — квадратичный вычет.
б) Произведение вычета и невычета — невычет.
в) Произведение невычетов — вычет. (Указание. Предыдущая задача поможет.)

▷ *Символ Лежандра* $\left(\frac{a}{p}\right)$ определяется как

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

Утверждения трех предыдущих задач учат, что

i) $\#\{x \mid x^2 = a \pmod p\} = 1 + \left(\frac{a}{p}\right)$; ii) $\sum \left(\frac{a}{p}\right) = 0$; iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Задача 4. а) Количество квадратичных вычетов по модулю p четно тогда и только тогда, когда $p = 4k + 1$.
б) Если a — квадратичный вычет, то и a^{-1} — квадратичный вычет.
в) Количество квадратичных вычетов по модулю p четно тогда и только тогда, когда -1 — квадратичный вычет по модулю p.

▷ Таким образом, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Задача 5. Если $p = 4k + 1$, то $(2k)!$ — корень из -1 по модулю p.
(Указание. Ср. с теоремой Вильсона, $(p-1)! \equiv -1 \pmod p$.)

* * *

Задача 6*. Рассмотрим преобразование $\sigma\colon x \mapsto \dfrac{1}{1-x}$ множества $(\mathbb{Z}/p) \cup \{\infty\}$.
а) $\sigma^3 = \mathrm{Id}$;
б) число неподвижных точек отображения σ сравнимо с $p + 1$ по модулю 3;
в) $(-3/p) = 1 \iff p = 3k + 1$.

Задача 7*. а) Уравнение $x^2 + y^2 = a \pmod p$ всегда имеет решения.
б) Вычислите сумму выражений $\left(\frac{t}{p}\right)\left(\frac{1-t}{p}\right)$ по всем остаткам t по модулю p.
в) Найдите число решений уравнения $x^2 + y^2 = 1 \pmod p$.
г) Выразите $(2/p)$ через остаток от деления p на 8. (Указание. Почти все решения предыдущего уравнения разбиваются на восьмерки $\{(\pm x, \pm y), (\pm y, \pm x)\}$.)

▷ Гипотеза Эйлера (доказанная Гауссом) состоит в том, что символ Лежандра $\left(\frac{a}{p}\right)$ зависит только от остатка p по модулю $4a$.

II. Квадратичные формы

Задача 8. а) Если x^2+y^2 делится на $p=4k+3$, то и x, и y делятся на p;
б) Для (любого) $p=4k+1$ это не верно.

Задача 9. Для любого ненулевого остатка i по модулю p существуют такие целые числа x и y, что $0<|x|,|y|<\sqrt{p}$ и $x\equiv yi \pmod p$ ("лемма Туэ").
(Указание. Рассмотрите остатки по модулю p всех чисел вида $x-yi$ для $0\leqslant x,y<\sqrt{p}$.)

Задача 10. а) Любое простое число вида $4k+1$ представимо в виде суммы двух квадратов ("рождественская теорема Ферма").
б) Если числа m и n представимы в виде суммы двух квадратов, то и их произведение представимо в виде суммы двух квадратов.
в) Целое число представимо в виде суммы двух квадратов тогда и только тогда, когда каждый простой делитель вида $4k+3$ входит в его разложение на простые множители в четной степени.

Задача 11. а) $p\neq 2$ представимо в виде $x^2+2y^2 \iff \left(\frac{-2}{p}\right)=1$;
б) $p\neq 3$ представимо в виде $x^2+3y^2 \iff \left(\frac{-3}{p}\right)=1$.

Задача 12. а) Из предыдущей задачи следует, что
$\left(\frac{-2}{p}\right)=1 \implies p=8k\pm 1$; $\left(\frac{-3}{p}\right)=1 \implies p=3k+1$.
б) ...И вообще, если q такое простое число, что $p=x^2+qy^2 \iff (-q/p)=1$, то $(-q/p)=1 \implies (p/q)=1$.

▷ Правильное обобщение последнего утверждения на произвольные простые p и q составляет содержание *квадратичного закона взаимности* Гаусса.

в) Приведите пример такого $p>5$, что $(-5/p)=1$, но p не представимо в виде x^2+5y^2.

* * *

▷ *Теорема Лежандра* состоит в том, что уравнение

$$ax^2+by^2+cz^2=0$$

(a, b, c взаимно просты и свободны от квадратов) имеет нетривиальные решения $\iff$ оно имеет нетривиальные решения в действительных числах и по всем простым модулям.

Задача 13*. Выведите из теоремы Лежандра, что для простых $p=4k+3$ и $q=4l+1$ $(-q/p)=1 \implies (p/q)=-1$, $(p/q)=1 \implies (-q/p)=-1$.

Лежандр (1752–1833) пытался вывести из своей теоремы квадратичный закон взаимности с 1785 года, но преуспел лишь частично: в 1858 году Парижская Академия объявила конкурс на устранение пробела в одной из лемм Лежандра, а в 1930 году эта лемма была опровергнута.

Задача 14*. а) В условиях теоремы Л. существуют такие линейные функции L и M, что

$$ax^2+by^2+cz^2=L(x,y,z)M(x,y,z) \pmod{abc}.$$

б) Существуют такие числа x, y и z (не все равные нулю), что $ax^2+by^2+cz^2$ есть либо 0, либо $|abc|$. (Указание. Действуйте в духе леммы Туэ.)
в) Завершите доказательство теоремы Лежандра. (Указание. Пусть $ax^2+by^2-cz^2=abc$. Воспользуйтесь тем, что $abc\cdot z^2=ab\cdot cz^2$.)

III. Корни из единицы

В следующей задаче и далее все уравнения рассматриваются в остатках по модулю p. Напомним, что уравнение степени n имеет в поле (в частности, в остатках по модулю p) не более n корней.

Задача 15. а) Если числа k и $p-1$ взаимно просты, то уравнение $x^k = a$ имеет ровно одно решение для каждого a.

б) Если $p-1$ делится на k и уравнение $x^k = a$ имеет решение, то оно имеет ровно k решений (в частности, существуют нетривиальные корни степени k из единицы).

в) Если $p-1$ делится на k, то уравнение $x^k = a$ имеет решение тогда и только тогда, когда $x^{(p-1)/k} \equiv 1 \pmod p$.

(Указание. Стоит вспомнить малую теорему Ферма.)

▷ В частности, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ («критерий Эйлера»).

Задача 16. Уравнение $x^2+x+1=0$ имеет решение тогда и только тогда, когда а) $\left(\frac{-3}{p}\right) = 1$; б) существует нетривиальный кубический корень из единицы (т. е. $p = 3k+1$).

В сущности речь идет о равенстве $\sqrt[3]{1} = -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$. Для комплексных чисел оно хорошо видно из тригонометрической формы.

Задача 17. а) Какие простые числа встречаются в разложении на простые множители чисел вида n^2+1?

б) Простых чисел вида $4k+1$ бесконечно много.

в) Простых чисел вида $3k+1$ бесконечно много.

Теорема Дирихле утверждает, что вообще в любой арифметической прогрессии, в которой разность взаимно проста с начальным членом, содержится бесконечно много простых чисел. Правильно обобщая рассуждения выше не очень сложно доказать теорему Дирихле для прогрессий вида $dk+1$ — но общий случай принципиально сложнее.

* * *

Так как $\cos\frac{2\pi}{8} = \frac{\sqrt{2}}{2}$, естественно ожидать, что из существования корня 8 степени из единицы следует, что 2 — квадратичный вычет.

Задача 18. а) Если $z^8 = 1$, $z^4 \neq 1$, то $(z+z^{-1})^2 = 2$.

б) Если $p = 8k+1$, то $(2/p) = 1$.

Задача 19*. а) Докажите *аналогичным образом*, что если $p = 8k+1$, то $(-2/p) = 1$.

б) Если $(2/p) = (-2/p) = 1$, то $p = 8k+1$.

Задача 20. а) Пусть $x^4+x^3+x^2+x+1=0$. Какому квадратному уравнению удовлетворяет $t = x + x^{-1}$?

б*) Вычислите $\cos(2\pi/5)$ и докажите, что правильный пятиугольник можно построить циркулем и линейкой.

в) Если $p = 5k+1$, то $(5/p) = 1$.

г) Приведите пример $p \neq 5k+1$ ($p \neq 2$), такого что $(5/p) = 1$.

IV. Квадратичные расширения

▷ Возникает надежда, что $\sqrt{\pm q}$ выражется через корень степени q из единицы — и, соответственно, $\pm q$ является квадратичным вычетом по крайней мере для $p = qk + 1$ (мы видели это для $q = 3, 5$ и нечто похожее в особом случае $q = 2$). Остаются две проблемы:

i) как получить такое выражения для корня в общем случае;

ii) что делать, если корня из единицы нужной степени среди остатков по модулю p нет.

Решив эти проблемы можно получить одно из доказательств Гаусса квадратичного закона взаимности. Мы немного поговорим только о второй.

▷ Пусть K — поле, d — его элемент. По аналогии с комплексными числами будем рассматривать $K(\sqrt{d})$ — совокупность формальных записей вида $a + b\sqrt{d}$ (где a и b элементы поля, а $\sqrt{d}$ — формальный символ) с естественными операциями сложения и умножения.

Задача 21. Если целые числа m и n представимы в виде $x^2 + dy^2$, то и число mn представимо в таком виде.

Задача 22. $K(\sqrt{d})$ поле тогда и только тогда, когда d не является квадратом в K.

Задача 23. а) Для любого (нечетного) p существует поле из p^2 элементов.

б*) Любые два поля из p^2 элементов изоморфны.

Задача 24. Пусть d — невычет по модулю p, $\sigma\colon x \mapsto x^p, \mathbb{F}_p(\sqrt{d}) \to \mathbb{F}_p(\sqrt{d})$ ("автоморфизм Фробениуса").

а) $\sigma(xy) = \sigma(x)\sigma(y)$, $\sigma(x + y) = \sigma(x) + \sigma(y)$; б) $\sigma(x) = x \iff x \in \mathbb{F}_p$;

в) если x — корень многочлена из $\mathbb{F}_p[x]$, то и $\sigma(x)$ его корень; г) $\sigma^2 = \mathrm{Id}$;

(Ср. с комплексным сопряжением.)

Задача 25. Пусть $(5/p) = 1$, но $p \neq 5k + 1$.

а) Дискриминант d уравнения $x + x^{-1} = \sqrt{5}$ — невычет.

б) В поле $\mathbb{F}_p(\sqrt{d})$ элемент x — корень 5 степени из единицы.

в) Автоморфизм Фробениуса поля $\mathbb{F}_p(\sqrt{d})$ меняет местами x и x^{-1}.

г) $p = 5k - 1$.

Задача 26. а) $(5/p) = 1 \iff p = 5k \pm 1 \iff (p/5) = 1$; б) $(2/p) = 1 \iff p = 8k \pm 1$.