1.

Везде далее p — нечетное простое число.

Задача 1. а) Если $x^2 = y^2 \pmod p$, то $x = \pm y \pmod p$.
б) Квадратное уравнение по модулю p имеет не более двух решений.

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

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

Утверждение предыдущей задачи состоит в том, что символ Лежандра мультипликативен,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

−1.

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, $(p-1)! \equiv -1 \mod p$.)

Задача 6. а) Какие простые числа встречаются в разложении на простые множители чисел вида $n^2 + 1$?
б) Простых чисел вида $4k + 1$ бесконечно много.

Задача 7. Если $a^2 + b^2$ делится на $p = 4k + 3$, то и a, и b делятся на p;
а) для $p = 4k + 1$ это неверно.

Задача 8. а) Пусть $i^2 \equiv -1 \pmod p$. Существуют такие целые числа a и b, что $0 < |a|, |b| < \sqrt{p}$ и $a + bi \equiv 0 \pmod p$ ("лемма Туэ").
(Указание. Рассмотрите остатки по модулю p всех чисел вида $x + iy$ для $0 \leqslant x, y < \sqrt{p}$.)
б) Любое простое число вида $4k + 1$ представимо в виде суммы двух квадратов ("рождественская теорема Ферма").
в) Целое число представимо в виде суммы квадратов тогда и только тогда, когда каждый простой делитель вида $4k + 3$ входит в его разложение на простые множители в четной степени.

-3.

Задача 9*. Рассмотрим преобразование $\sigma\colon x \mapsto \frac{1}{1-x}$ 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) $\left(\frac{-3}{p}\right) = 1 \iff p = 3k+1$.

(Быть может кто-то из читателей сможет обобщить это вычисление на другие a?)

В следующей задаче и далее все уравнения рассматриваются в остатках по модулю p.

Задача 10. 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 $a^{\frac{p-1}{k}} \equiv 1 \pmod p$.
(Указание. Стоит вспомнить малую теорему Ферма.)

▷ *Теорема о первообразном корне* утверждает, что существует остаток θ такой, что $\theta^0, \theta^1, \ldots, \theta^{p-2}$ — различные остатки (ей можно пользоваться без доказательства).

Задача 11. Пусть $p-1$ делится на k.
а) Если уравнение $x^k = a$ имеет решение, то оно имеет ровно k решений (в частности, существуют нетривиальные корни степени k из единицы).
б) Уравнение $x^k = a$ имеет решение тогда и только тогда, когда $a^{\frac{p-1}{k}} \equiv 1 \pmod p$ („критерий Эйлера").

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

Задача 12. 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 13. Простых чисел вида $3k+1$ бесконечно много.

2 и 5.

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 14. Если $z^8 = 1$, $z^4 \neq 1$, то а) $z^2 + z^{-2} = 0$; б) $(z + z^{-1})^2 = 2$.

Задача 15. а) Если $p = 8k + 1$, то $\left(\frac{2}{p}\right) = 1$; б) если $p = 8k + 1$, то $\left(\frac{-2}{p}\right) = 1$.
в*) Если $\left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = 1$, то $p = 8k + 1$.

Задача 16*. Простое число p представимо в виде $a^2 + 2b^2$ тогда и только тогда, когда $\left(\frac{-2}{p}\right) = 1$.

Задача 17. а) Если $x^4 + x^3 + x^2 + x + 1 = 0$, то $t = x + x^{-1}$ удовлетворет уравнению $t^2 + t - 1 = 0$.
б) Если $p = 5k + 1$, то $\left(\frac{5}{p}\right) = 1$.
в) Вычислите $\cos(2\pi/5)$ и докажите, что правильный пятиугольник можно построить циркулем и линейкой.

2 и 5 (продолжение).

▷ 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 18. Если целые числа m и n представимы в виде $a^2 + b^2D$, то и число mn представимо в таком виде.

Задача 19. $K(\sqrt{D})$ поле тогда и только тогда, когда D не является квадратом в K.

Задача 20. а) Для любого (нечетного) p существует поле из p^2 элементов.
б*) Любые два поля из p^2 элементов изоморфны.

Задача 21. 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 22. Пусть $\left(\frac{5}{p}\right) = 1$, 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 23*. Простых чисел вида а) $5k + 1$; б) $5k - 1$ бесконечно много.

Задача 24. $\left(\frac{5}{p}\right) = 1 \iff p = 5k \pm 1$.

Задача 25. а) Если $\left(\frac{2}{p}\right) = 1$, то $p = 8k \pm 1$; б) $\left(\frac{2}{p}\right) = 1 \iff p = 8k \pm 1$.

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