1. Пусть p — нечётное простое число. Возьмём такое целое g, что $g \bmod p$ — образующий группы $(\mathbf{Z}/p\mathbf{Z})^\times$.

   а) Покажите, что если $g^{p-1} \equiv 1 \bmod p^2$, то $(g+p)^{p-1} \not\equiv 1 \bmod p^2$.

   б) Так как $g+p \equiv g \bmod p$, предположим, что $g^{p-1} \not\equiv 1 \bmod p^2$, не теряя общности (пункт а). Покажите, что $g \bmod p^n$ — образующий группы $(\mathbf{Z}/p^n\mathbf{Z})^\times$ для всех $n \geqslant 2$. (Подсказка: покажите, что $g^{p-1} \bmod p^n$ имеет порядок p^{n-1}.)

2. Пусть $g = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)$. Во время лекции мы узнали, что у g есть собственные значения $\lambda = (5+\sqrt{33})/2 \approx 5{,}372$ и $\mu = (5-\sqrt{33})/2 \approx -0{,}372$ в $\mathbf{R}$, и для произвольного $r \in \mathbf{Q}$ вычислили вещественные пределы $\lim_{n\to\infty} g^n(r) = 2/(\lambda-1)$ и $\lim_{n\to-\infty} g^n(r) = 2/(\mu-1)$, которые *не зависят* от r.

   а) Покажите с помощью леммы Гензеля, что 33 — квадрат в $\mathbf{Q}_2$; тогда у g есть собственные значения в $\mathbf{Q}_2$. Вычислите до 6-ой цифры 2-адические разложения собственных значений g в $\mathbf{Q}_2$.

   б) Даны значения $g^n(1)$ и начальные части их 2-адических разложений:

$$\begin{aligned}
g(1) &= 3/7 = 1 + 2^2 + 2^5 + 2^8 + \cdots, \\
g^2(1) &= 17/37 = 1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^9 + \cdots, \\
g^3(1) &= 91/199 = 1 + 2^2 + 2^3 + 2^6 + 2^7 + 2^8 + 2^9 + \cdots, \\
g^4(1) &= 489/1069 = 1 + 2^2 + 2^3 + 2^5 + 2^9 + \cdots, \\
g^5(1) &= 2627/5743 = 1 + 2^2 + 2^3 + 2^5 + 2^6 + 2^8 + 2^9 + \cdots,
\end{aligned}$$

$$\begin{aligned}
g^{-1}(1) &= -1 = 1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + \cdots, \\
g^{-2}(1) &= -3/2 = \frac{1}{2} + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + \cdots, \\
g^{-3}(1) &= -16/11 = 2^4 + 2^6 + 2^7 + 2^8 + 2^{10} + \cdots, \\
g^{-4}(1) &= -86/59 = 2 + 2^2 + 2^3 + 2^4 + 2^6 + \cdots, \\
g^{-5}(1) &= -462/317 = 2 + 2^3 + 2^4 + 2^9 + \cdots,
\end{aligned}$$

Для каждого рационального r вычислите до 6-ой цифры пределы $\lim_{n\to\infty} g^n(r)$ и $\lim_{n\to-\infty} g^n(r)$ в $\mathbf{Q}_2$. Ответы не должны зависеть от r.

3. Пусть $g = \left(\begin{smallmatrix} 1 & 2 \\ -1 & 1 \end{smallmatrix}\right)$.

   а) Покажите, что у g есть собственные значения в $\mathbf{Q}_3$.

   б) Для каждого рационального r вычислите $\lim_{n\to\infty} g^n(r)$ и $\lim_{n\to-\infty} g^n(r)$ в $\mathbf{Q}_3$ (не зависят от r) до шестой 3-адической цифры.

4. Пусть $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, где $a, b, c, d \in \mathbf{Q}$ и $ad - bc \neq 0$.

   а) Пусть λ — собственное значение g. Покажите, что если $b \neq 0$, то $\binom{b}{\lambda - a}$ является собственным вектором, который соответствует собственному значению λ, и если $c \neq 0$, то соответствующим собственным вектором является $\binom{\lambda - d}{c}$ (такие векторы совпадают, если $b \neq 0$ и $c \neq 0$).

   б) Предположим, что $c = 0$, тогда характеристический многочлен g равен $(x - a)(x - d)$. Если $a/d \neq \pm 1$, покажите, что есть такое простое p, что $|a/d|_p \neq 1$. Предполагая, что $|a/d|_p > 1$, покажите, что для каждого $r \in \mathbf{Q}$, $g^n(r) \to \infty$ при $n \to \infty$ и $g^n(r) \to b/(d-a)$ при $n \to -\infty$. Если же $|a/d|_p < 1$, то покажите, что $g^n(r) \to b/(d - a)$ при $n \to \infty$ и $g^n(r) \to \infty$ при $n \to -\infty$. Из этого выведите, что есть бесконечно много g-орбит на $\mathbf{Q} \cup \{\infty\}$. Что происходит, если $a/d = \pm 1$?

   в) Проведите рассуждение из пункта б при условии, что $b = 0$ вместо $c = 0$ (возможный предел $b/(d - a)$ представляется числом $(a - d)/c$).

   г) Предположим, что $b \neq 0$ и $c \neq 0$. Если существует пополнение поля $\mathbf{Q}$ (т.е., $\mathbf{R}$ или $\mathbf{Q}_p$ для некоторого p), в котором лежат два различных собственных значений λ и μ матрицы g, покажите, что для каждого $r \in \mathbf{Q} \cup \{\infty\}$, $g^n(r)$ сходится к $b/(\lambda - a)$ или к $b/(\mu - a)$ при $n \to \pm\infty$. (Какая именно возможность реализуется зависит от направления предела и пополнения, в котором норма a/d не равна 1.) Из этого выведите, что есть бесконечно много g-орбит на $\mathbf{Q} \cup \{\infty\}$.