1. Пусть $F$ — поле. Покажите, что функция $|\cdot|$ на кольце многочленов $F[x]$, заданная как $|f| := 2^{\deg f}$ для $f \neq 0$ и $|0| = 0$, определяет норму на $F[x]$, которая удовлетворяет усиленному неравенству треугольника.

2. Пусть $|\cdot|$ — норма на кольце $A$, которая удовлетворяет $|a+b| \leqslant \max(|a|, |b|)$ для всех $a$ и $b$ в $A$.

   а) Покажите, что $|a| \neq |b| \implies |a + b| = \max(|a|, |b|)$. (Подсказка: $|a| = |a + b - b|$ и $|b| = |b + a - a|$.)

   б) Покажите, что если заданы $a_1, a_2, \ldots, a_n \in A$ и одно из них больше по норме чем другие, то $|a_1 + a_2 + \cdots + a_n| = \max |a_i|$.

3. Пусть $|\cdot|$ — норма на кольце $A$.

   а) Докажите, что сложение и умножение — непрерывные функции относительно нормы: если $|a_n - a| \to 0$ и $|b_n - b| \to 0$ при $n \to \infty$, то $|(a_n + b_n) - (a + b)| \to 0$ и $|a_n b_n - ab| \to 0$ при $n \to \infty$.

   б) Докажите, что всякий многочлен $f(x) = c_d x^d + \cdots + c_1 x + c_0$, где $c_i \in A$, определяет непрерывную функцию из $A$ в $A$: если $|a_n - a| \to 0$ при $n \to \infty$, то $|f(a_n) - f(a)| \to 0$ при $n \to \infty$.

   в) Верны ли предыдущие пункты, если условие $|ab| = |a||b|$ заменяется условием $|ab| \leqslant |a||b|$ для всех $a, b \in A$?

4. Пусть $A$ — кольцо с нормой $|\cdot|$ и $\{x_n\}$ — фундаментальная последовательность в $A$ относительно этой нормы.

   а) Докажите, что $\{|x_n|\}$ — фундаментальная последовательность в $\mathbf{R}$.

   б) Покажите, что если подпоследовательность $\{x_{n_i}\}$ сходится в $A$, то вся последовательность $\{x_n\}$ сходится к одному и тому же пределу.

   в) Если $x_n \not\to 0$, то существует такое $c > 0$, что $|x_n| \geq c$ для всех достаточно больших $n$.

   г) Если $x_n \not\to 0$ и $|x + y| \leq \max(|x|, |y|)$ для всех $x$ и $y$, то нормы $|x_n|$ *одинаковы* для всех достаточно больших $n$.

5. Пусть $f(x) = x^3 - x^2 - 2x - 8$. Используйте лемму Гензеля чтобы доказать, что $f(x)$ имеет 3 корня в $\mathbf{Z}_2$. (Осторожно: два решения сравнимы по модулю 2, поэтому, чтобы найти подходящие приближения к корням в лемме Гензеля, нужно работать по модулю 4.)

6. Сколько корней у многочлена $x^3 - x - 2$ в $\mathbf{Z}_2$?

7. Пусть $k$ — целое. Мы хотим доказать, что сравнение $y^2 \equiv x^3 + k \bmod m$ разрешимо для всякого $m$. (Уравнение $y^2 = x^3 + k$ иногда разрешимо над $\mathbf{Z}$, иногда не разрешимо, например, $y^2 = x^3 - 5$ не имеет никаких целых решений. Из этой задачи вы увидите, что сравнение $y^2 \equiv x^3 - 5 \bmod m$ разрешимо для всякого $m$.)

   а) Докажите, что достаточно проверить результат, когда $m$ — степень простого числа.

   б) Докажите, что $y^2 \equiv x^3 + k \bmod 2$ имеет решение $(x_0, y_0)$, где $x_0 \equiv 1 \bmod 2$. Затем для всякого $r \geq 1$ докажите, что существует такое $x_r$, что $y_0^2 \equiv x_r^3 + k \bmod 2^r$. (Подсказка: покажите с помощью леммы Гензеля, что всякое нечётное число является кубом в $\mathbf{Z}_2$.)

   в) В случаях $p = 3$ и $p = 5$ найдите для каждого $k \bmod p$ такое $x_0 \bmod p$, что $1 \equiv x_0^3 + k \bmod p$. Выведите для всех $r \geq 1$, что существует такое $y_r \equiv 1 \bmod p$, что $y_r^2 \equiv x_0^3 + k \bmod p^r$. (Подсказка: по лемме Гензеля при $p \neq 2$ всякое $a \equiv 1 \bmod p$ является квадратом в $\mathbf{Z}_p$.)

   г) Для каждого $k \bmod 7$ найдите такое $(x_0, y_0) \bmod p$, что $y_0^2 \equiv x_0^3 + k \bmod 7$, и $x_0 \not\equiv 0 \bmod 7$ или $y_0 \not\equiv 0 \bmod 7$. Выведите для всех $r \geq 1$, что существует такое $(x_r, y_r)$, что $y_r^2 \equiv x_r^3 + k \bmod 7^r$.

   д) Из теории эллиптических кривых или сумм Якоби следует, что для всякого простого $p \geq 11$ сравнение $y^2 \equiv x^3 + k \bmod p$ имеет решение $(x, y)$, где $y \not\equiv 0 \bmod p$. Выведите отсюда с помощью леммы Гензеля, что сравнение $y^2 \equiv x^3 + k \bmod p^r$ разрешимо для всякого $r \geq 1$.

8. Рассмотрим метод Ньютона в $\mathbf{Z}_{10}$!

   а) Пусть $f(x) = x^2 - x$. Начиная с первого приближения $a_1 = 5$, положим $a_{k+1} = a_k - f(a_k)/f'(a_k) = a_k^2/(2a_k - 1)$. Вычислите $|a_k - \alpha|_{10}$ для $k \leq 4$, где

$\alpha = 5260982128\ldots$ такой корень $f(x)$, что $\alpha \equiv 5 \bmod 10$. Повторите процесс, выбрав $a_1 = 6$ как первое приближение к корню $\beta = 6739017871\ldots$.

b) Пусть $f(x) = x^3 - x$. Этот многочлен имеет (единственный) такой корень $\gamma = 4260982128\ldots$, что $\gamma \equiv 4 \bmod 10$. Вычислите $|\gamma - a_k|_{10}$ для $k \leq 4$, где $a_1 = 4$ и числа $a_k$ строятся методом Ньютона. (Всего есть 9 корней многочлена $f(x)$ в $\mathbf{Z}_{10}$.)

9. а) В $\mathbf{R}$ если $0 < |x| < 1$, то последовательность $|x^n/n|$ монотонно убывающая. Верно ли аналогичное утверждения в $\mathbf{Q}_p$: правда ли, что если $0 < |x|_p < 1$, то последовательность $|x^n/n|_p$ монотонно убывает?

   в) Пусть $x \in \mathbf{Q}_p$. Докажите, что если $p$ нечётное простое число и $|x|_p \leqslant 1/p$, то $|x^n/n|_p < |x|_p$ для $n \geqslant 2$. Если $|x|_2 \leqslant 1/4$, то $|x^n/n|_2 < |x|_2$ для $n \geqslant 2$. Если $|x|_2 = 1/2$, то $|x^n/n|_2 < |x|_2$ для $n \geqslant 3$.

10. Для простого $p$, последовательность $p^n/(p^n + 1)$ стремится при $n \to \infty$ к 1 в $\mathbf{R}$ и к 0 в $\mathbf{Q}_p$.

    а) Найдите такую последовательность рациональных чисел $\{r_n\}$, что $r_n \to 0$ в $\mathbf{R}$ и $r_n \to 1$ в $\mathbf{Q}_p$ при $n \to \infty$.

    б) Для $\alpha$ и $\beta$ из $\mathbf{Q}$, найдите явно такую последовательность $\{r_n\}$ в $\mathbf{Q}$, что $r_n \to \alpha$ в $\mathbf{R}$ и $r_n \to \beta$ в $\mathbf{Q}_p$ при $n \to \infty$.

    в) Для $\alpha \in \mathbf{R}$ и $\beta \in \mathbf{Q}_p$ докажите, что существует такая последовательность $\{r_n\}$ в $\mathbf{Q}$, что $r_n \to \alpha$ в $\mathbf{R}$ и $r_n \to \beta$ в $\mathbf{Q}_p$ при $n \to \infty$.

    г) Для простых $p_1, p_2, \ldots, p_k$, пусть $\alpha \in \mathbf{R}$ и $\alpha_i \in \mathbf{Q}_{p_i}$ для $1 \leq i \leq k$. Докажите, что существует такая последовательность $\{r_n\}$ в $\mathbf{Q}$, что $r_n \to \alpha$ в $\mathbf{R}$ и $r_n \to \alpha_i$ в $\mathbf{Q}_{p_i}$ при $n \to \infty$. (Это значит, что обыкновенный модуль и $p$-адические нормы для различных простых $p$ «независимы»: сходимость последовательности рациональных чисел по одной такой норме не говорят нам ничего о сходимости этой последовательности по другим таким нормам.)