Нормирования и p-адические числа.

Задача 1°. Найдите p-адическое разложение для
a) $\frac{2}{3}$ в $\mathbb{Q}_2$; b) $-\frac{1}{6}$ в $\mathbb{Q}_7$; c) $\frac{1}{10}$ в $\mathbb{Q}_{11}$; d) $\frac{1}{120}$ в $\mathbb{Q}_5$.
e) Докажите, что p-адическое разложение числа $a \in \mathbb{Q}_p$ периодично начиная с некоторого места тогда и только тогда, когда $a \in \mathbb{Q}$.

Задача 2°. a) Пусть $c \in \mathbb{Z}, p \nmid c$. Покажите, что в $\mathbb{Q}_p$ последовательность c^{p^n} сходится и для её предела γ имеет место: $\gamma \equiv c \mod p$ и $\gamma^{p-1} = 1$. Выведите отсюда, что $t^{p-1} - 1$ целиком раскладывается на линейные множители в $\mathbb{Q}_p$.
Эта конструкция даёт канонические представители мультипликативной группы $\mathbb{F}_p^\times$ в $\mathbb{Z}_p$ — представители Тейхмюллера.
b) Докажите, что при нечётном p корни из единицы, содержащиеся в $\mathbb{Q}_p$, — в точности корни степени $p-1$, а корни из единицы, лежащие в $\mathbb{Q}_2$, — это ± 1.
Подсказка: рассмотрите гомоморфизм $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times$.

Задача 3. Покажите, что над $\mathbb{Q}_p$ существуют расширения произвольной степени.

Задача 4 (мультипликативная группа поля $\mathbb{Q}_p$). Положим $U = \mathbb{Z}_p^\times, U_n = 1 + p^n\mathbb{Z}_p$.
a) Покажите, что $U = \varprojlim U/U_n$ и $U_n/U_{n+1} = \mathbb{Z}/p\mathbb{Z}$.
b) Докажите, что имеет место разложение $U = V \times U_1$, где $V = \{x \in U \mid x^{p-1} = 1\}$ — подгруппа корней степени $p-1$ из единицы в $\mathbb{Q}_p$.
c) Пусть $x \in U_n - U_{n+1}$ и $n \geq 1$, если $p \neq 2$, и $n \geq 2$, если $p = 2$. Покажите, что $x^p \in U_{n+1} - U_{n+2}$.
d) Убедитесь, что при $p \neq 2$ группа U_1/U_n циклическая и выведите отсюда, что $U_1 \cong \mathbb{Z}_p$.
e) Докажите, что $U_1 \cong \{\pm 1\} \times U_2 \cong \{\pm 1\} \times \mathbb{Z}_2$ при $p = 2$.
f) Получите, что $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ при $p \neq 2$ и $\mathbb{Q}_2^\times \cong \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.

Задача 5. a) Убедитесь, что поля $\mathbb{Q}_p$ и $\mathbb{Q}_q$, не изоморфны, если $p \neq q$, а также, что $\mathbb{Q}_p$ не изоморфно $\mathbb{R}$.
b) Докажите, что поле $\mathbb{Q}_p$ не имеет автоморфизмов, отличных от тождественного.
Подсказка: покажите, что все автоморфизмы автоматические непрерывны.

Задача 6. Пусть $f(x) = ax^2 + bx + c$, где $a, b, c \in \mathbb{Z}, a \neq 0$. Покажите, что существует бесконечно много простых чисел p, для которых $f(x)$ имеет корень в $\mathbb{Z}_p$.
Подсказка: можно считать, что $a = 1$, $c \neq 0$, $d = b^2 - 4c \neq 0$. Если e — любое целое число, делящееся на все простые числа, входящие в $2cd$, то $f(e^N) \to \infty$ при $N \to \infty$, но $|f(e^N)|_p$ ограничено снизу для $p \mid e$.

Задача 7. a°) Пусть $F(x_1, \ldots, x_n) = a_1x_1^m + \cdots + a_nx_n^m \in \mathbb{Z}_p[x_1, \ldots, x_n], r = v_p(m), s = \max(v_p(a_1), \ldots, v_p(a_n)), N = 2(r+s)+1$. Докажите, что уравнение $F(x_1, \ldots, x_n) = 0$ имеет ненулевое решение в $\mathbb{Z}_p$ тогда и только тогда, когда сравнение $F \equiv 0 \mod p^N$ имеет примитивное решение.
b^*) Докажите, что уравнение $3x^3+4y^3+5z^3 = 0$ имеет нетривиальное решение в $\mathbb{Z}_p$ при любом p. (Используя разложение на простые в кубических расширениях $\mathbb{Q}$, мы в дальнейшем убедимся, что это уравнение не имеет нетривиальных рациональных решений).
Подсказка: убедитесь сначала, что сравнение $3x^3 + 4y^3 + 5z^3 \equiv 0 \mod p$ имеет решение при всех p.

Задача 8. Для многочлена $F(x_1, \ldots, x_m) \in \mathbb{Z}_p[x_1, \ldots, x_m]$ обозначим через c_n число решений сравнения $F(x_1, \ldots, x_m) \equiv 0 \mod p^n$ и рассмотрим *ряд Пуанкаре* $\phi(t) = \sum_{n=1}^{\infty} c_n t^n$.
a) Вычислите ряд Пуанкаре для $F(x) = a_1x_1^2 + \cdots + a_mx_m^2$, где $a_k \in \mathbb{Z}_p^\times$. Убедитесь, что $\phi(t)$ — рациональная функция.

b) Найдите ряд Пуанкаре для многочлена $F(x_1, \dots, x_m)$, обладающего свойством: для всякого решения сравнения $F(x_1, \dots, x_m) \equiv 0 \mod p$ при некотором $i = 1, \dots, m$ имеем $\frac{\partial F}{\partial x_i} \not\equiv 0 \mod p$.

c) Посчитайте ряд Пуанкаре для многочлена $F(x, y) = x^2 - y^3$.

Имеется теорема Игусы о том, что ряд Пуанкаре всегда рационален. Известны различные её доказательства, основывающиеся на разрешении особенностей алгебраических многообразий, p-адическом интегрировании, теории моделей.

Задача 9°. Для целого положительного числа n определим $\binom{a}{n} = \frac{a(a-1)\dots(a-n+1)}{n!}$. Покажите, что $\binom{a}{n} \in \mathbb{Z}_p$, если $a \in \mathbb{Z}_p$.

Задача 10° (квадратные корни). a) Пусть $p \neq 2$, и пусть $c \in \mathbb{Q}_p$ удовлетворяет условию $|c|_p < 1$. Покажите, что

$$1 + \binom{\frac{1}{2}}{1} c + \binom{\frac{1}{2}}{2} c^2 + \dots + \binom{\frac{1}{2}}{n} c^n + \dots$$

сходится к квадратному корню из $1 + c$.

b) Найдите такое $d \in \mathbb{Q}$, что $|d^2 - 11|_5 \leq 5^{-10}$.

Задача 11 (ряды в $\mathbb{Q}_p$). a°) Покажите, что степенной ряд $\sum\limits_{k=1}^{\infty} a_k x^k, a_k, x \in \mathbb{Q}_p$ сходится при $|x|_p < r$ и расходится при $|x|_p > r$, где $\frac{1}{r} = \limsup |a_n|_p^{1/n}$. Что может происходить со сходимостью на границе $|x|_p = r$?

b°) Убедитесь, что ряд $\log(1 + x) = \sum\limits_{k=1}^{\infty} \frac{(-1)^{k+1} x^k}{k}$ сходится при $|x|_p < 1$ и расходится при $|x|_p \geq 1$.

c) Найдите радиус сходимости ряда $\exp(x) = \sum\limits_{k=0}^{\infty} \frac{x^k}{k!}$. Сходится ли этот ряд на границе круга сходимости?

d) Проверьте, что в $\mathbb{Q}_p$ имеют место равенства:

$$\log((1 + x)(1 + y)) = \log(1 + x) + \log(1 + y), \ \exp(x + y) = \exp(x) \exp(y),$$
$$\exp(\log(1 + x)) = 1 + x, \ \log(\exp(x)) = x.$$

Выведите отсюда, что exp и log — взаимно обратные изоморфизмы некоторой окрестности 0 в аддитивной группе $\mathbb{Z}_p$ и некоторой окрестности 1 в мультипликативной группе $\mathbb{Z}_p^\times$.

e^*) Исследуйте сходимость ряда $\sum\limits_{k=0}^{\infty} \binom{a}{k} x^k$.

Задача 12 (Теорема Штрассмана). Пусть $c_0, c_1, c_2, \dots, c_n, \dots$ — элементы из $\mathbb{Z}_p$, не все равные нулю, и пусть $c_n \to 0$. Положим $f(x) = c_0 + c_1 x + \dots + c_n x^n + \dots$ для $x \in \mathbb{Z}_p$. Покажите, что существует лишь конечное число элементов $a \in \mathbb{Z}_p$, для которых $f(a) = 0$. Более точно, если определить $N \geq 0$ условиями $|c_N|_p = \max\limits_n |c_n|_p$ и $|c_n|_p < |c_N|_p$ для всех $n > N$, то уравнение $f(a) = 0$ имеет не более N решений.

Подсказка: если $f(a) = 0$, то $f(x) = \sum c_n(x^n - a^n) = (x - a)g(x)$, где $g(x)$ обладает свойствами, аналогичными $f(x)$.

Задача 13. a°) Покажите, что кольцо $\mathbb{Z}_2$ гомеоморфно Канторову множеству (которое получается выкидыванием из отрезка $[0, 1]$ всех точек, в троичном разложении которых встречается цифра 1).

b) Докажите, что все кольца $\mathbb{Z}_p$ гомеоморфны.

Задача 14°. Покажите, что для всех $x \in \mathbb{Q}, x \neq 0$ имеет место равенство $|x| \cdot \prod\limits_p |x|_p = 1$, где произведение берется по всем простым числам p (эта формула имеет обобщение на случай произвольных конечных расширений $\mathbb{Q}$).

Задача 15. a) Докажите, что нормирование $\| \ \|$ поля F неархимедово тогда и только тогда, когда $\|n\| \leq 1$ для любого натурального числа n.

b) Покажите, что всякое нормирование поля характеристики p неархимедово.

Задача 16. Докажите, что два нормирования $\| \ \|_1$ и $\| \ \|_2$ поля F задают одну и ту же топологию (сходимость) на F в том и только в том случае, когда существует положительное вещественное α, для которого $\| \ \|_1 = \| \ \|_2^\alpha$.

Задача 17°. a) Пусть k — поле, $E = k(t)$. Для $u = t^m \frac{f(t)}{g(t)} \in E, f(0) \neq 0, g(0) \neq 0$ определим $\|u\| = \rho^m$, где $\rho \in \mathbb{R}, 0 < \rho < 1$ — некоторое фиксированное вещественное число. Покажите, что $\| \ \|$ — норма на E и пополнение E по этой норме изоморфно полю рядов Лорана $k((t))$, т. е. состоит из элементов вида $\sum\limits_{k=m}^{\infty} a_k t^k, a_k \in k, m \in \mathbb{Z}$.

b) Опишите все нормирования поля $\mathbb{F}_q(t)$.

Подсказка: кроме нормирования, введённого в пункте a), имеется нормирование, соответствующее „точке на бесконечности“ в $\mathbb{P}^1$: для $u = \frac{f(t)}{g(t)} \in \mathbb{F}_q(t)$ это $\rho^{\deg g - \deg f}$.

Задача 18*. Пусть K — поле с неархимедовым нормированием $\| \ \|$. Положим $\mathcal{O}_K = \{x \in K \mid \|x\| \leq 1\}, \mathfrak{m}_K = \{x \in K \mid \|x\| < 1\}, k = \mathcal{O}_K/\mathfrak{m}_K$. Докажите, что K локально компактно (т. е. существует компактная окрестность 0) тогда и только тогда, когда K — полно, нормирование $\| \ \|$ дискретно (т.е. образ K в $\mathbb{R}$ при этом нормировании — дискретная подгруппа $\mathbb{Z}$), а поле вычетов k конечно.

Задача 19 (Теорема Гельфанда—Торнхейма). a) Пусть F — нормированное поле, содержащее $\mathbb{C}$, при этом нормирование $| \ |$ на F продолжает обычное нормирование на $\mathbb{C}$. Пусть $x_0 \in F \setminus \mathbb{C}$. Положим $f(z) = (x_0 - z)^{-1} \colon \mathbb{C} \to F$. Убедитесь, что функция $z \mapsto |f(z)|$ непрерывна, ограничена и достигает наибольшего значения M на некотором замкнутом множестве $D \subset \mathbb{C}$.

b) В обозначениях предыдущего пункта предположим, что $0 \in D$. Пусть ω — примитивный корень степени n из $1, r \in \mathbb{R}, |r/x_0| < 1$. Положим $S(n) = \frac{1}{n} \sum\limits_{k=1}^{n} \frac{1}{x_0 - \omega^k r}$. Убедитесь, что $\lim\limits_{n\to\infty} |S(n)| = |1/x_0| = M$.

c) Докажите, что для любого комплексного числа λ такого, что $|\lambda| = 1$, имеет место $\left|\frac{1}{x_0 - \lambda r}\right| = M$. Выведите отсюда, что $F = \mathbb{C}$.

Подсказка: рассмотрите маленький интервал, содержащий λ, и корни из 1, лежащие в нём.

d) Покажите, что любое поле F с *архимедовым* нормированием изоморфно подполю $\mathbb{C}$ так, что при изоморфизме нормирование на F переходит в стандартное нормирование на $\mathbb{C}$.

Задача 20 (непрерывные функции на $\mathbb{Z}_p$). Наша цель — дать следующую характеризацию непрерывных функций $f \colon \mathbb{Z}_p \to \mathbb{Q}_p$ (теорема Малера): $f(x)$ — непрерывна тогда и только тогда, когда существует такая последовательность $b_i \in \mathbb{Q}_p, b_i \to 0$, что $f(x) = \sum\limits_{i=0}^{\infty} b_i \binom{x}{i}$ для всех $x \in \mathbb{Z}_p$ (здесь $\binom{x}{n} = \frac{x(x-1)\ldots(x-n+1)}{n!}$).

a) Пусть $b_i \in \mathbb{Q}_p$ — последовательность p-адических чисел, $\lim\limits_{i\to\infty} b_i = 0$. Убедитесь, что функция $f(x) = \sum\limits_{i=0}^{\infty} b_i \binom{x}{i}$ является непрерывной функцией на $\mathbb{Z}_p$.

b) Докажите, что для любой последовательности $a_i \in \mathbb{Q}_p$ найдется единственная последовательность b_n такая, что $a_n = \sum\limits_{i=0}^{\infty} \binom{n}{i} b_i$ (на самом деле слагаемые с $i > n$ равны 0).

c) Положим $a(t) = \sum_{n=0}^{\infty} a_n t^n$, $b(t) = \sum_{i=0}^{\infty} b_i t^i$. Покажите, что $b(t) = \frac{1}{1+t} a\left(\frac{t}{t+1}\right)$.

d) Предположим, что функция $n \mapsto a_n$ продолжается до непрерывной функции на $\mathbb{Z}_p$. Пусть $v_p(a_n - a_{n'}) \geq k$, если $v_p(n - n') \geq r$, и $s \in \mathbb{N}$ такое, что $p^s a_n \in \mathbb{Z}_p$ при всех n. Покажите, что $v_p(b_i) \geq k$ при $i > N(k) = (s + k + 1)p^r$. Получите отсюда теорему Малера.

Подсказка: представьте $a(t)$ в виде $P(t)(1 - t^{p^r})^{-1} + p^k \alpha(t), P(t) = \sum_{n=0}^{p^r-1} a_n t^n, \alpha(t) \in \mathbb{Z}_p[[t]]$, воспользуйтесь дальше тем, что $(1 + t)^{p^r} - t^{p^r} \equiv 1 \mod p$.

Задача 21 (конечные подгруппы группы матриц).

a) Пусть $p > 2$ — простое число, пусть A — обратимая $n \times n$-матрица с элементами из $\mathbb{Z}_p$, и пусть $A \equiv I \mod p$, но $A \neq I$. Покажите, что A имеет бесконечный порядок в $\mathrm{GL}_n(\mathbb{Q}_p)$.
Подсказка: покажите сначала, что $A^q \neq I$ для простого показателя $q = p$ и $q \neq p$.

b) Пусть G — конечная группа $n \times n$-матриц с элементами из $\mathbb{Z}_p$. Докажите, что порядок G делит $(p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1})$.
Подсказка: рассмотрите матрицы из G по модулю p.

c) Рассмотрим теперь $n \times n$-матрицу A с элементами из $\mathbb{Z}_2$. Покажите, что, если $A \equiv I \mod 4$, но $A \neq I$, то A имеет бесконечный порядок. Кроме того, если $A \equiv I \mod 2$, то либо $A^2 = I$, либо A имеет бесконечный порядок.

d) Пусть H — конечная группа матриц $A \equiv I \mod 2$. Докажите, что H имеет порядок 2^m при некотором $m \leq n$.
Подсказка: H есть группа $n \times n$-матриц показателя 2, а потому абелева. Выберите базис, состоящий из общих собственных векторов элементов H.

e) Пусть G — конечная группа $n \times n$-матриц с элементами из $\mathbb{Z}_2$. Покажите, что порядок G делит $2^n(2^n - 1)(2^n - 2) \dots (2^n - 2^{n-1})$.

f) Пусть G — конечная подгруппа $\mathrm{GL}_n(\mathbb{Q})$. Докажите, что порядок g группы G делит $g^*(n) = \prod_{q \text{ простое}} q^{\beta(q)}$, где $\beta(2) = n + 2[\frac{n}{2}] + [\frac{n}{2^2}] + [\frac{n}{2^3}] + \dots$ и $\beta(q) = [n/(q-1)] + [n/q(q-1)] + [n/q^2(q-1)] + \dots$ при $q \neq 2$.
Подсказка: G имеет элементы из $\mathbb{Z}_p$ для всех $p > p_0$. Для нечётного q найдите p с помощью теоремы Дирихле о простых в арифметической прогрессии так, чтобы p было примитивным корнем по модулю q^2, и после этого примените пункт b; для $q = 2$ возьмите $p \equiv 3 \mod 8$.

g) Докажите, что, если все элементы группы G имеют определитель 1, то g делит $\frac{1}{2}g^*(n)$.
Аналогичные границы можно доказать для конечных подгрупп в произвольных алгебраических группах над полями алгебраических чисел.

Задача 22 (Теорема фон Штаудта).

a) Определим числа Бернулли равенством $\frac{x}{e^x - 1} = B_0 + \frac{B_1}{1!}x + \dots + \frac{B_k}{k!}x^k + \dots$. Убедитесь, что $B_0 = 1, B_1 = -\frac{1}{2}$ и что $B_k = 0$ для всех нечётных $k > 1$.

b) Докажите, что $S_k(n) = 1^k + 2^k + \dots + (n-1)^k = \sum_{r=0}^{k} \binom{k}{r} \frac{B_r}{k+1-r} n^{k+1-r}$.
Подсказка: посмотрите на тождество $1 + e^x + \dots + e^{(n-1)x} = \frac{e^{nx} - 1}{x} \cdot \frac{x}{e^x - 1}$.

c) Пусть p — простое, выведите, что $B_k = \lim_{n \to 0} n^{-1} S_k(n)$, где предел понимается в p-адическом смысле.

d) Пусть $p = 2$ и k чётно. Покажите, что $|p^{-m-1} S_k(p^{m+1}) - p^{-m} S_k(p^m)|_p \leq 1$.
Подсказка: представьте область суммирования в определении $S_k(p^{m+1})$ в виде $up^m + v$, где $0 \leq u < p$ и $0 \leq v < p^m$.

e) Выведите из предыдущего, что $|B_k - p^{-1} S_k(p)|_p \leq 1$ и, следовательно, что $B_k + p^{-1} \in \mathbb{Z}_p$, если $(p-1) \mid k$, и $B_k \in \mathbb{Z}_p$ в противном случае. Заключите, что $B_k + \sum_{p-\text{простое}, (p-1)|k} p^{-1} \in \mathbb{Z}$.