# Листок 12
# Тема 12(3.3). Лемма Гензеля, сравнения и кольцо целых p-адических чисел

**Упражнения и задачи**

1. Пусть $k$ — произвольное поле, $F(X) \in k[x]$. Докажите формулу Тейлора для формальной производной $F'$.

2. Докажите, что порядок фактор группы $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ равен 8. Укажите соответствующее множество представителей.

3. Пусть $p \neq 2$, $\alpha, \beta \in \mathbb{Z}_p$, $p \nmid \alpha, p \nmid \beta$. Докажите, что разрешимость сравнения $\alpha x^p \equiv \beta \pmod{p^2}$ достаточна для разрешимости уравнения $\alpha x^p = \beta$ в $\mathbb{Q}_p$.

4. Пусть $p \neq 2$, $U = U(\mathbb{Z}_p)$ — группа $p$-адических единиц, $U_n = 1 + p^n\mathbb{Z}_p$. ($U_n = \{\alpha \in \mathbb{Z}_p : \nu_p(\alpha - 1) \geqslant n\}$, т.е. $U_n$ — $p$-адические окрестности единичного элемента). Докажите следующие свойства:

   - $U_n/U_{n+1} = \mathbb{Z}/p\mathbb{Z}$, $U = \varprojlim U_n$;
   - $U = U_1V$, где $V$ — циклическая подгруппа корней степени $p-1$ из единицы;
   - Если $\alpha \in U_n \setminus U_{n+1}$, то $\alpha^p \in U_{n+1} \setminus U_{n+2}$;
   - $U_1/U_n$ — циклическая группа, $U_1 \cong \mathbb{Z}_p$.

   Сделайте вывод о структуре мультипликативной группы $\mathbb{Q}_p$: $\mathbb{Q}_p^* \cong \mathbb{Z}\times\mathbb{Z}_p\times\mathbb{Z}/(p-1)\mathbb{Z}$.

5. *Пусть $F(x_1, \dots, x_n) \in \mathbb{Z}_p[x_1, \dots, x_n]$, $N_m$ — число решений сравнения $F \equiv 0 \pmod{p^m}$, $L_F(u) = \sum_{m=0}^{\infty} N_m u^m$ — так называемый ряд Пуанкаре (вспомните дзета функцию Артина).

   - Найдите ряд Пуанкаре для $F = \alpha_1 x_1 + \dots + \alpha_n x_n$, где $\alpha_i \in \mathbb{Z}_p^*$. Убедитесь, что в этом случае $L_F(u)$ — рациональная функция.
   - Найдите ряд Пуанкаре для многочлена $F(x_1, \dots, x_n)$, обладающего свойством: для всякого решения сравнения $F(x_1, \dots, x_n) \equiv 0 \pmod{p}$ при некотором $i$ имеем $F'_{x_i}(x_1, \dots, x_n) \not\equiv 0 \pmod{p}$;
   - Найдите ряд Пуанкаре для $F(x, y) = x^2 - y^3$;
   - Докажите рациональность ряда Пуанкаре для многочленов одной переменной.

   (Существует теорема (Игусы) о том, что $L_F$ всегда является рациональной функцией).

6. Докажите $p$-адический критерий Эйзенштейна: пусть $f \in \mathbb{Z}_p[x]$, $f(x) = a_0x^n + \dots a_n$, $f$ – неприводим, если $p \nmid a_0$, $p \mid a_i$ $1 \leqslant i \leqslant n$, $p^2 \nmid a_n$.

7. Верно ли следующее: $f \in \mathbb{Z}[x]$ неприводим в $f \in \mathbb{Q}[x] \Leftrightarrow f$ неприводим в $\mathbb{Q}_p[x]$ $\forall p \leqslant \infty$?

8. Докажите, что уравнение $(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$ разрешимо в $\mathbb{Q}_p$ $\forall p \leqslant \infty$ но не разрешимо в $\mathbb{Q}$.

**SageMath**

- Исследуйте функции SageMath для работы с многочленами с $p$-адическими коэффициентами:
  - Разложение многочлена: `factor()`.
  - В контексте Леммы Гензеля: `hensel_lift()`.

**Темы для самостоятельного изучения**

- Разрешимость уравнений с квадратичными формами над полем $p$-адических чисел ([БШ §I.6 п.2).

- Приложение теоремы Минковского-Хассе для квадратичной формы от трёх переменных ([Gouv §4.8]).