Листок 3
Тема 3 (1.3). Первообразные корни

Упражнения и задачи

1. Путь p — простое, докажите, что $p|\binom{n}{k}$ для $1 \leqslant k < p$.
2. Путь $p > 2$ — простое, $l \geqslant 2$. Докажите, что $\forall a \in \mathbb{Z}$ $(1+ap)^{p^{l-2}} \equiv 1 + ap^{l-1}$ (p^l).
3. Пусть $p > 2$ — простое, g — первообразный корень $\bmod p^n$. Докажите, что тогда g — первообразный корень $\bmod p$.
4. Пусть p — простое, $p \equiv 1 (\bmod 4)$. Докажите что g — первообразный корень $(\bmod p)$ $\Leftrightarrow$ $-g$ — первообразный корень $(\bmod p)$.
5. Пусть р — простое, $p \equiv 3 (\bmod 4)$. Докажите что g — первообразный корень $(\bmod p)$ $\Leftrightarrow$ $-g$ имеет порядок $(p-1)/2$.
6. Докажите, что 3 — первообразный корень простого числа вида $p = 2^n + 1$.
7. Пусть $p > 2$ — простое. Докажите, что g — первообразный корень $\bmod p \Leftrightarrow$ $a^{(p-1)/q} \not\equiv 1(p)$ для всех простых делителей $q \mid p-1$.
8. Докажите, что $\prod\limits_g{}' g \equiv (-1)^{\varphi(p-1)}$ (p), где $\prod'$ — произведение по всем $0 \leqslant g \leqslant p-1$, g — первообразный корень $\bmod p$.
9. Пусть g — первообразный корень $\bmod p$, $d|(p-1)$. Докажите, что $g^{(p-1)/d}$ имеет порядок d, а также что a является d-ой степенью $\Leftrightarrow a \equiv g^{kd}(p)$ для некоторого k.
10. Пусть G — конечная циклическая группа порядка n, g — образующая G. Докажите, что все образующие имеют вид g^k, $(k, n) = 1$.
11. Пусть G — конечная абелева группа, a, b – элементы порядков m, n соответственно. Докажите, что если $(m, n) = 1$ то порядок элемента ab равен mn.

SageMath

- Исследуйте основные классы и функции SageMath релевантные материалу лекции:
  - Первообразные корни: `primitive_root(), is_primitive_root()`;
  - Образующие группы единиц: `unit_gens()`;
  - Порядок элемента в кольце вычетов: `multiplicative_order()`;
  - Индекс и дискретный логарифм в кольце вычетов: `log()`;
  - Абелевы группы `AbelianGroup()`, образующие и порядки `gens(), gens_orders()`.
- Пусть a — наименьшее положительное число являющееся первообразным корнем $\bmod p$. Постройте частотную таблицу для a, что можно заметить?
- Пусть $a \neq -1$ и не является полным квадратом. Постройте примеры последовательностей простых, для которых a является первообразным корнем (согласно гипотезе Артина таких простых бесконечно много, также можно оценить плотность их распределения).

Темы для самостоятельного изучения

- Структура группы единиц $U(\mathbb{Z}/2^l\mathbb{Z})$ ([IR, глава 4], [Вин, глава 6]).
- Критерии разрешимости сравнения $x^n \equiv a (\bmod n)$ ([IR, глава 4]).
- Основы криптографии с открытым ключем: протокол Диффи–Хеллмана и RSA, [Steinent], глава 3.