

Листок 3

Тема 3 (1.3). Первообразные корни

Упражнения и задачи

1. Пусть p — простое, докажите, что $p \nmid \binom{p}{k}$ для $1 \leq k < p$.
2. Пусть $p > 2$ — простое, $l \geq 2$. Докажите, что $\forall a \in \mathbb{Z} \ (1 + ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \pmod{p^l}$.
3. Пусть $p > 2$ — простое, g — первообразный корень $\pmod{p^n}$. Докажите, что тогда g — первообразный корень \pmod{p} .
4. Пусть p — простое, $p \equiv 1 \pmod{4}$. Докажите что g — первообразный корень $\pmod{p} \Leftrightarrow -g$ — первообразный корень \pmod{p} .
5. Пусть p — простое, $p \equiv 3 \pmod{4}$. Докажите что g — первообразный корень $\pmod{p} \Leftrightarrow -g$ имеет порядок $(p-1)/2$.
6. Пусть $p > 2$ — простое. Докажите, что g — первообразный корень $\pmod{p} \Leftrightarrow g^{(p-1)/q} \not\equiv 1 \pmod{p}$ для всех простых делителей $q \mid p-1$.
7. Пусть $p > 2$ — простое. Докажите, что $\prod'_{g \pmod{p}} g \equiv (-1)^{\varphi(p-1)} \pmod{p}$, где \prod' — произведение по всем $0 \leq g \leq p-1$, g — первообразный корень \pmod{p} .
8. Пусть g — первообразный корень \pmod{p} , $d \mid (p-1)$. Докажите, что $g^{(p-1)/d}$ имеет порядок d , а также что a является d -ой степенью $\Leftrightarrow a \equiv g^{kd} \pmod{p}$ для некоторого k .
9. Пусть G — конечная циклическая группа порядка n , g — образующая G . Докажите, что все образующие имеют вид g^k , $(k, n) = 1$.
10. 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 \pmod{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 $x^n \equiv a \pmod{n}$ ([IR, глава 4]).
- Основы криптографии с открытым ключом: протокол Диффи–Хеллмана и RSA, [Stein-ent], глава 3.