Листок 2
Тема 2 (1.2). Сравнения

Упражнения и задачи

1. Докажите, что $\equiv \pmod m$ задаёт отношение эквивалентности в кольце $\mathbb{Z}$, то есть, 1) $a \equiv a\ (m)$; 2) $a \equiv b\ (m) \Rightarrow b \equiv a\ (m)$; 3) $a \equiv b\ (m),\ b \equiv c\ (m) \Rightarrow a \equiv c\ (m)$.

2. Докажите утверждения про классы вычетов:
   - $\bar{a} = \bar{b} \Leftrightarrow a \equiv b\ (m)$;
   - $\bar{a} \neq \bar{b} \Leftrightarrow \bar{a} \cap \bar{b} = \varnothing$;
   - $|\{\bar{a} : a \in \mathbb{Z}\}| = m$.

3. Докажите, что операции $\bar{a} + \bar{b}$, $\bar{a} \cdot \bar{b}$ на множестве классов вычетов корректно определены, то есть не зависят от выбора представителей классов $\bar{a}$ и $\bar{b}$.

4. Докажите, что множество $F[x]$ многочленов с коэффициентами из поля F является кольцом.

5. Докажите, что $\forall f \in F[x]$, $\deg f \geqslant 1$, f раскладывается в произведение неприводимых многочленов.

6. Докажите, что в кольце $F[x]$ возможно деление с остатком, т.е. $\forall f, g \in F[x]$, $g \neq 0$, $\exists h, r \in F[x] : f = hg + r$, где либо $\deg r < \deg g$, либо $r = 0$.

7. Докажите следующие утверждения про делимость в кольце многочленов:
   - $f, g \in F[x]$ — взаимно простые (т.е. $(f, g) = (1)$), $f | gh \Rightarrow f | h$;
   - $p \in F[x]$ — неприводимый, $p | fg \Rightarrow p | f$ или $p | g$.

8. Докажите, что в кольце многочленов $F[x]$ имеет место однозначнось разложения на неприводимые множители.

9. Используя сравнимость $\bmod n$ докажите, что уравнения $3x^2 + 2 = y^2$ и $7x^3 + 2 = y^3$ не разрешимы в целых числах.

10. Пусть p, q — различные нечетные простые такие что $p - 1 | q - 1$, докажите, что если $(n, pq) = 1$ то $n^{q-1} \equiv 1 (pq)$.

11. Пусть a, b, c — решение диофантова уравнения $a^2 + b^2 = c^2$, $a, b, c \in \mathbb{Z}$, $(a, b) = (b, c) = (c, a) = 1$. Докажите, что существуют целые числа u, v такие, что $c - b = 2u^2$, $c + b = 2v^2$, $(u, v) = 1$, и, как следствие, $a = 2uv$, $b = v^2 - u^2$, $c = v^2 + u^2$.

12. Пусть m, a, b — целые, $m > 1$, $(a, m) = 1$. Докажите, что
    - $\displaystyle\sum_{x \pmod m} \left\{\frac{ax + b}{m}\right\} = \frac{1}{2}(m - 1)$;
    - $\displaystyle\sum_{\substack{x \pmod m \\ (x,m)=1}} \left\{\frac{ax}{m}\right\} = \frac{1}{2}\varphi(m)$.

SageMath

- Исследуйте основные классы и функции SageMath релевантные материалу лекции:

  - Кольцо вычетов и модулярная арифметика: `Integers()`;
  - Китайская теорема об остатках `crt()`;
  - Кольцо многочленов: `PolynomialRing()`;
  - Неприводимость многочлена: `is_irreducible()`;
  - Разложение многочлена на множители: `factor()`;
  - Корни многочлена: `roots()`;
  - Рассмотрите примеры поведения разложения многочлена на множители над $\mathbb{Z}, \mathbb{Q}$ и различными кольцами вычетов $\mathbb{Z}/N\mathbb{Z}$.

Темы для самостоятельного изучения

- Быстрое возведение в степень в $\mathbb{Z}/n\mathbb{Z}$, [Stein-ent], §2.3.
- Проверка на простоту, [Stein-ent], §2.4.