Листок 1
Тема 1 (1.1). Простые числа

Упражнения и задачи

1. Докажите свойства делимости:
   - $a|a$, $a \neq 0$;
   - $a|b, b|a \implies a = \pm b$;
   - $a|b, b|c \implies a|c$;
   - $a|b, a|c \implies a|b \pm c$.

2. Алгоритм Евклида: Пусть $a, b \in \mathbb{Z} \setminus \{0\}, a > b$, определим последовательность $b > r_1 > r_2 > \dots > r_n$ следующим образом: $a = bq_0 + r_1$, $b = r_1 q_1 + r_2$, $r_1 = r_2 q_2 + r_3$, $\dots r_n = r_{n-1} q_{n-1} + r_n$. Докажите, что $\exists n : r_{n-1} = r_n q_n$ и $r_n = (a, b)$. (Сначала докажите , что $(a, b) = (b, r_1)$).

3. Докажите, что $\sqrt{2}$ — иррациональное число, т.е. что не $\exists$ рационального $r = a/b$ $(a, b \in \mathbb{Z})$ такого, что $r^2 = 2$.

4. Пусть $\alpha \in \mathbb{R}$, $b \in \mathbb{Z}_+$, докажите, что $\left[\dfrac{[\alpha]}{b}\right] = \dfrac{\alpha}{b}$.

5. Пусть $(a, b) = 1$, докажите, что $(a + b, a - b) = 1$ или 2.

6. Пусть $a, b, c \in \mathbb{Z}$, докажите что уравнение $ax + by = c$ разрешимо в целых числах $\iff d = (a, b)|c$. Докажите также, что если x_0, y_0 — решение этого уравнения, то все решения имеют вид $x = x_0 + t\dfrac{b}{d}$, $y = y_0 - t\dfrac{b}{d}$, где $t \in \mathbb{Z}$.

7. Докажите следующие свойства:
   - $\nu_p([a, b]) = \max(\nu_p(a), \nu_p(b))$;
   - $\nu_p(a + b) \geqslant \min(\nu_p(a), \nu_p(b))$, причем $\nu_p(a + b) = \min(\nu_p(a), \nu_p(b))$, если $\nu_p(a) \neq \nu_p(b)$;
   - $(a, b)[a, b] = ab$;
   - $(a + b, [a, b]) = (a, b)$.

8. Докажите, что $\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$

9. Докажите, что существует бесконечно много простых вида $4k - 1$, $k \in \mathbb{Z}$.

10. Пусть $a, b, c, d \in \mathbb{Z}$, $(a, b) = 1$, $(c, d) = 1$. Докажите, что если $\dfrac{a}{b} + \dfrac{c}{d} \in \mathbb{Z}$, то $b = \pm d$.

11. Пусть $n \in \mathbb{Z}$, $n > 2$ Докажите, что числа
$$\frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n};\ \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{2n+1}$$
не являются целыми.

12. Пусть $f(n)$ — мультипликативная функция. Докажите, что функции
$$g(n) = \sum_{d|n} f(d),\ h(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$$
также мультипликативны.

13. Докажите, что $\forall n \in \mathbb{Z}$

$$\sum_{d|n} \mu(\frac{n}{d})\nu(d) = 1, \ \sum_{d|n} \mu(\frac{n}{d})\sigma(d) = n.$$

14. Докажите, что $\forall m, n \in \mathbb{Z}$
    - $\varphi(n)\varphi(m) = \varphi((n,m))\varphi([n,m])$;
    - $\varphi(mn)\varphi((m,n)) = (m,n)\varphi(m)\varphi(n)$.

15. Пусть $P, Q \in \mathbb{Z}_+$ — нечетные, $(P,Q) = 1$. Докажите, что

$$\sum_{0<x<\frac{Q}{2}} \left[\frac{P}{Q}x\right] + \sum_{0<y<\frac{P}{2}} \left[\frac{Q}{P}y\right] = \frac{P-1}{2}\frac{Q-1}{2}.$$

(Используйте подсчет целых точек в некоторой ограниченной области на плоскости).

SageMath

- Исследуйте основные теоретико-числовые функции в SageMath:
  - НОД, НОК: `gcd()`, `xgcd()`, `lcm()`;
  - разложение на множители: `factor()`, `valuation()`;
  - простые числа: `is_prime()`, `next_prime()`, `previous_prime()`;
  - делители: `divisors()`, `prime_divisors()` ;
  - функции Эйлера и Мёбиуса, число и сумма делителей: `euler_phi()`, `moebius()`, `sigma()`;
  - число простых чисел: `prime_pi()` (постройте график этой функции).