

# ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

## Вопросы к коллоквиуму

1-й поток, 2018г.

*Программа содержит все прочитанные на лекциях темы,  
за исключением цепных дробей.*

1. Наименьшее общее кратное. Любое общее кратное нескольких чисел делится на их наименьшее общее кратное.
2. Наибольший общий делитель. Наибольший общий делитель нескольких чисел делится на любой их общий делитель.
3. Равенство  $[a, b] \cdot (a, b) = ab$ . Докажите, что из условий  $a|bc$ ,  $(a, b) = 1$  следует  $a|c$ .
4. Алгоритм Евклида для вычисления наибольшего общего делителя двух чисел.
5. Решение в целых числах линейных уравнений от двух переменных.
6. Простые числа. Решето Эратосфена. Бесконечность множества простых чисел.
7. Основная теорема арифметики. Каноническое разложение.
8. Показатели  $\nu_p(n)$  и их свойства. Формулы для вычисления кратности вхождения простого числа  $p$  в  $n!$ , в наименьшее общее кратное и в наибольший общий делитель нескольких чисел.
9. Докажите неравенство  $[1, 2, 3, \dots, 2n + 1] > 4^n$ ,  $n \geq 1$ .
10. Теорема Чебышева, оценка снизу.
11. Докажите неравенство  $\prod_{p \leq x} p < 4^x$ ,  $x \geq 2$ .
12. Теорема Чебышева, оценка сверху.
13. Мультипликативные функции и их свойства.
14. Функция Мёбиуса и формула обращения.
15. Функция Эйлера и её свойства (формула для вычисления по делителям, мультипликативность).
16. Сравнения и их основные свойства. Классы вычетов. Полная и приведенная системы вычетов.
17. Теорема Вильсона.
18. Теоремы Эйлера и Ферма.
19. Сравнения с одним неизвестным. Количество решений. Сравнения первой степени (условие разрешимости и количество решений).
20. Китайская теорема об остатках.
21. Полиномиальные сравнения по простому модулю. Теорема Лагранжа о количестве решений полиномиального сравнения по простому модулю.
22. Решение полиномиальных сравнений по модулю равному степени простого числа.
23. Решение полиномиальных сравнений по составному модулю.
24. Символ Лежандра и его свойства.
25. Лемма Гаусса о символе Лежандра.
26. Квадратичный закон взаимности.
27. Теорема о простых числах, по модулю которых разрешимо данное квадратичное сравнение.
28. Порядок числа по заданному модулю и его свойства.
29. Существование первообразных корней по простому модулю.
30. Индексы и их свойства.