

**Вопросы к коллоквиуму по теории чисел**  
**1 курс, 2 поток. 2018г., лектор - Н.Г. Мощевитин**

1. Теоремы о делении с остатком. Обычное деление с остатком, деление с остатком с отрицательным остатком, и с остатком минимальным по модулю. Наибольший общий делитель и наименьшее общее кратное нескольких чисел. Теорема о том, что наименьшее общее кратное делит любое общее кратное. Теорема о том, что наибольший общий делитель делится на произвольный общий делитель.

2. Алгоритм Евклида нахождения наибольшего общего делителя двух чисел. Представление рациональных чисел в виде конечных обыкновенных цепных дробей и цепных дробей с минусами.

3. Оценка количества шагов в алгоритме Евклида и оценка длины разложения рационального числа в обыкновенную цепную дробь.

4. Формальные цепные дроби. Подходящие дроби. Рекуррентные соотношения для числителей и знаменателей подходящих дробей. Равенство  $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$ .

5. Значение обыкновенной цепной дроби (теорема о том, что для каждой формальной цепной дроби существует предел у последовательности подходящих дробей.) Иррациональность значения бесконечной цепной дроби.

6. Теорема о том, что всякое иррациональное вещественное число представляется в виде значения некоторой обыкновенной бесконечной цепной дроби.

7. Квадратичные иррациональности и обыкновенные цепные дроби. Теорема Лагранжа.

8. Теорема о линейном представлении наибольшего общего делителя, как следствие применения алгоритма Евклида. Важная лемма, как следствие теоремы о линейном представлении НОД.

9. Простые числа. Бесконечность множества простых чисел. Решето Эратосфена. Основная теорема арифметики о единственности разложения натуральных чисел на простые множители.

10. Теорема о стремлении к бесконечности суммы  $\sum_{p \leq x} \frac{1}{p}$ .

11. Мультипликативные функции и их простейшие свойства. Суммы по делителям. Функция Мебиуса. Формула  $\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0 & n > 1 \end{cases}$ ,

12. Функция Эйлера. Формулы  $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ .

13. Формула обращения Мебиуса и примеры ее применения. Формула  $\sum_{d|n} \varphi(d) = n$ .
14. Сравнения и их основные свойства. Условие разрешимости линейного сравнения от одной переменной. Классы вычетов. Полная и приведенная системы вычетов.
15. Доказательство мультипликативности функции Эйлера с помощью построения приведенной системы вычетов по модулю  $mn$  в виде  $mx + ny$ ;  $1 \leq x \leq n, (x, n) = 1; 1 \leq y \leq m, (y, m) = 1$  (для взаимно простых  $m$  и  $n$ ).
16. Китайская теорема об остатках.
17. Теорема Эйлера, малая теорема Ферма.
18. Теорема о том, что у ненулевого многочлена по простому модулю количество корней не превосходит его степени. Равенство многочленов по модулю  $p$  как функций и как многочленов. Разложение на множители многочлена  $x^{p-1} - 1$  по модулю  $p$ . Теорема Вильсона.
19. Квадратичные вычеты и невычеты. Простейшие свойства. Символ Лежандра. Теорема Эйлера.
20. Лемма Гаусса о символе Лежандра.
21. Квадратичный закон взаимности Гаусса и вычисление символа Лежандра  $\left(\frac{2}{p}\right)$ .
22. Показатель элемента по модулю  $m$  и его простейшие свойства. Теорема о том, что каждое  $n$ , такое что  $a^n \equiv 1 \pmod{m}$  делится на показатель  $a$  по модулю  $m$ . Показатель произведения двух элементов с взаимно простыми показателями.
23. Первообразные корни по модулю  $m$ . Существование первообразного корня по простому модулю. Критерий первообразного корня.
24. Отсутствие первообразных корней по модулям  $2^\alpha p^\beta, \alpha \geq 2, \beta \geq 1$  и по модулю  $m$ , когда у  $m$  есть два различны нечетных простых делителя. Структура группы обратимых элементов по модулю  $2^\alpha, \alpha \geq 3$  и отсутствие первообразных корней по этим модулям.
- 25\*. Существование первообразного корня по модулям  $p^\alpha$  и  $2p^\alpha$ .
- 26\*. Лемма Гензеля. Решение полиномиальных сравнений по составному модулю. Количество решений сравнения  $x^2 \equiv a \pmod{2^\alpha p_1^{\alpha_1} \cdots p_t^{\alpha_t}}$ .
- 27\*. Символ Якоби и его свойства.

**Примечание.** Из вопросов, помеченных звездочкой \* в конце списка, на коллоквиум выносятся только те, которые будут полностью рассказаны на лекциях до 26 ноября включительно.