

## Коллоквиум

На коллоквиуме:

один вопрос из «Делимость и остатки» (максимум 5 баллов),  
один вопрос из «Ценные дроби, геометрия чисел,  $\mathbb{Z}[x]$ » (максимум 5 баллов),  
по просьбе студента: случайные вопросы по программе (максимум 2 балла).

На коллоквиуме вопросы будут сформулированы без расшифровки.

Расшифровкой могут пользоваться только преподаватели :)

Пункты и вопросы, помеченные *оранжевыми* комментариями, необязательны в текущем учебном году.

Некоторая литература для подготовки: <http://mathschool.ru/knigi/vtch>

### Делимость и остатки

1. Определение евклидова кольца. Евклидовость  $\mathbb{Z}$  и  $\mathbb{Z}[\beta]$ .
  - а) Определение нормы и евклидова кольца.
  - б) Доказательство евклидовости  $\mathbb{Z}$ .
  - в) Доказательство евклидовости  $\mathbb{Z}[\beta]$ .
2. Алгоритм Евклида нахождения НОДа. Линейное представление НОДа.
  - а) Определение НОДа в произвольном евклидовом кольце.
  - б) Алгоритм Евклида в произвольном евклидовом кольце (описание алгоритма, доказательство конечности, место НОД в алгоритме).
  - в) Формулировка и доказательство теоремы о линейном представлении НОД в  $\mathbb{Z}$ .
3. Определение факториального кольца. Факториальность евклидовых колец.
  - а) Определение неприводимого элемента в евклидовом кольце.
  - б) Доказательство того, что любой элемент можно разложить на произведение неприводимых.
  - в) Доказательство того, что разложение на произведение неприводимых единственно, если кольцо евклидово.
4.  $p$ -показатели и их свойства. Постулат Бертрана (б/д). Теорема Чебышёва (б/д).
  - а) Определение  $p$ -показателя.
  - б) Формулировка и доказательство утверждений о  $\nu_p(x+y)$  и  $\nu_p(xy)$ .
  - в) Формулировка и доказательство формулы для  $\nu_p(n!)$ .
  - г) Формулировка постулата Бертрана.

- д) Формулировка теоремы Чебышёва о распределении простых чисел.
5. Теорема Вильсона. Теорема Ферма-Эйлера.
- а) Формулировка и доказательство теоремы Вильсона.
- б) Формулировка и доказательство теоремы Ферма-Эйлера.
6. Теорема Шевалле-Варнинга.
- а) Формулировка и доказательство теоремы Шевалле-Варнинга.
7. Функция Эйлера и её свойства. Теорема Эйлера.
- а) Определение и формула функции Эйлера.
- б) Формулировка и доказательство мультипликативности функции Эйлера.
- в) Формулировка и доказательство теоремы Эйлера.
8. Китайская теорема об остатках.
- а) Формулировка и доказательство китайской теоремы об остатках.
9. Примитивный вычет (первообразный корень).
- а) Определение примитивного вычета по произвольному модулю.
- б) Доказательство существования примитивного вычета по простому модулю.
- в) Описание модулей, по которым существует примитивный вычет (б/д).
10. Квадратичные вычеты и невычеты.
- а) Количество квадратичных вычетов по модулю  $p$ .
- б) Определение символа Лежандра, свойство  $\left(\frac{ab}{p}\right) = \dots$  с доказательством.
- в) Формулировка и доказательство критерия Эйлера.
- г)  $\left(\frac{2}{p}\right) = \dots$  (б/д).
- д) Квадратичный закон взаимности (б/д).

## Цепные дроби, геометрия чисел, $\mathbb{Z}[x]$

11. Континуанты и их свойства.
- а) Определение континуантов.
- б) Разложение матрицы  $\begin{pmatrix} K_n(x_1, \dots, x_n) & K_{n-1}(x_1, \dots, x_{n-1}) \\ K_{n-1}(x_2, \dots, x_n) & K_{n-2}(x_2, \dots, x_{n-1}) \end{pmatrix}$  на произведение.
- в) Разложение  $\frac{K_{n+1}(a_0, a_1, \dots, a_n)}{K_n(a_1, \dots, a_n)}$  в цепную дробь.
12. Значение бесконечной цепной дроби.

- а) Доказательство существования предела подходящих дробей бесконечной цепной дроби.
  - б) (Не входил в изначальную версию) Доказательство того, что цепная дробь предела подходящих дробей совпадает с исходной цепной дробью.
13. (Отменён) Алгоритм вытягивания носов.
- а) Описание алгоритма вытягивания носов.
  - б) Связь алгоритма вытягивания носов с подходящими дробями цепной дроби.
14. Теорема Лагранжа о цепных дробях.
- а) Формулировка и доказательство теоремы Лагранжа о цепных дробях.
15. Формула Пика.
- а) Примитивные треугольники и их площадь.
  - б) Формула Пика для склейки многоугольников.
16. Теорема Бlichфельда. Лемма Минковского.
- а) Формулировка и доказательство теоремы Бlichфельда.
  - б) Формулировка и доказательство леммы Минковского.
17. Теорема Кронекера (теорема Дирихле).
- а) Формулировка и доказательство теоремы Дирихле.
  - б) Формулировка и доказательство теоремы Кронекера.
18. Теорема Вейля о распределении  $\{n\alpha\}$ .
- а) Формулировка и доказательство теоремы Вейля о распределении  $\{n\alpha\}$ .
19. Связь неприводимости многочленов над  $\mathbb{Z}$  и над  $\mathbb{Q}$ .
- а) Формулировка и доказательство леммы Гаусса.
  - б) Доказательство утверждения « $P$  неприводим над  $\mathbb{Z} \Rightarrow P$  неприводим над  $\mathbb{Q}$ ».
20. Признак Эйзенштейна неприводимости многочлена над  $\mathbb{Z}$ . Признак Дюма (б/д).
- а) Формулировка и доказательство признака Эйзенштейна.
  - б) Формулировка теоремы Дюма (б/д).