Вопросы коллоквиума по алгебре

Группы 151, 153 (лектор А. Ю. Лузгарев)

Осень 2012

1. Множества, подмножества, основные операции над множествами.
2. Отображения: образ, прообраз, инъекция, сюръекция, биекция.
3. Композиция отображений, ее ассоциативность.
4. Бинарные отношения и отношения эквивалентности.
5. Теорема о разбиении на классы эквивалентности. Фактор-множество.
6. Метод математической индукции. Бинарные операции.
7. Делимость: определения и простейшие свойства. Ассоциированность.
8. Теорема о делении с остатком.
9. Наибольший общий делитель; его существование и единственность. Линейное представление НОД.
10. Алгорифм Эвклида.
11. Свойства НОД. Взаимная простота, свойства взаимно простых чисел.
12. Линейные диофантовы уравнения. Полное описание множества решений уравнения с двумя неизвестными.
13. НОД нескольких чисел и критерий разрешимости линейного диофантова уравнения с несколькими неизвестными.
14. Простые числа, их свойства.
15. Основная теорема арифметики.
16. Каноническое разложение. Приложения: НОД, число делителей.
17. Сравнения по модулю. Свойства.
18. Китайская теорема об остатках.
19. Классы вычетов, действия над ними. Кольцо классов вычетов.
20. Критерий обратимости кольца классов вычетов. Поле классов вычетов по простому модулю.
21. Теорема Вильсона.
22. Функция Эйлера. Переформулировка китайской теоремы об остатках в терминах колец классов вычетов.
23. Мультипликативность функции Эйлера. Формула для функции Эйлера.
24. Теорема Эйлера и малая теорема Ферма.
25. Алгоритм шифрования RSA.