Вопросы коллоквиума по алгебре

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

Осень 2014

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