Краткая программа зачета **(v14, 09.03.2011)**

0. Индукция

0.1. Доказательство утверждений по индукции (в т. ч. индукция по комбинаторным объектам), различные схемы индукции (использование, вывод из обычной индукции).

1. Множества и отображения

1.1. Понятие множества (элементы и подмножества, равенство множеств). Операции над множествами (определение, доказательство тождеств, выразимость одних операций через другие).

1.2. Образ и прообраз при отображении (определения, согласованность с операциями над множествами).

1.3. Композиция отображений (определение, ассоциативность). Обратное отображение (определение, необходимое и достаточное условие существования), биективность композиции биекций.

1.4. Отношение эквивалентности (определение, (не)зависимость аксиом, фактор по отношению эквивалентности).

1.5*. Равномощность как отношение эквивалентности. Счетность: определение, сохранение при операциях на множествах, счетность как наименьшая бесконечная мощность.

2. Комбинаторика

2.1. Сложение, умножение, деление (раскраски куба, жезлы и подобные задачи) в комбинаторике.

2.2. Комбинаторика множеств и отображений (число подмножеств, число отображений, число биекций, число вложений, число k-элементных подмножеств).

2.3. Четыре взгляда на числа сочетаний: подмножества, пути, треугольник Паскаля, бином Ньютона (доказательство эквивалентности, умение переходить с одного языка на другой). Основные тождества для чисел сочетаний.

2.4*. Формула включений–исключений и ее применения (число сюръекций, НОД и НОК произведения n чисел).

2.5*. Числа Каталана: три определения (триангуляции, бинарные деревья, пути над диагональю), рекуррентное соотношения, формула.

3. Арифметика

3.1. Делимость (определение, свойства). Деление с остатком (определение, существование и единственность).

3.2. Бесконечность множества простых чисел. Основная теорема арифметики: формулировка, доказательство существования, вывод единственности из основной леммы.

3.3. Алгоритм Евклида и линейное представление НОД. Линейное диофантово уравнение ($ax + by = c$ в целых числах), доказательство основной леммы к основной теореме арифметики (если $p \mid ab$, то $p \mid a$ или $p \mid b$).

3.4. Сравнимость по модулю (определение, согласованность с операциями). Линейное сравнение ($ax \equiv b \pmod{n}$). Китайская теорема об остатках и система линейных сравнений.

3.5. Обратимость умножения по простому модулю. Существование порядка вычета. Малая теорема Ферма.

3.6. Решение уравнений в целых числах: использование взаимной простоты (пример: описание пифагоровых троек), приведения по модулю (пример: бесконечность множества натуральных чисел, не представимых в виде суммы двух квадратов).

Звездочкой отмечены необязательные темы. Кроме знания теории для успешной сдачи зачета необходима также способность решать (новые) задачи.