Дополнительные главы теории чисел

А. Зыкин

Годовой спецкурс

1. **Эллиптические кривые.** Напоминания из теории кривых. Геометрические свойства эллиптических кривых. Изогении, модуль Тейта, спаривание Вейля. Эллиптические кривые над $\mathbb{C}$ и решетки. Эллиптические кривые над конечными полями, суперсингулярные эллиптические кривые. Формальные группы и эллиптические кривые. Когомологии Галуа, высоты и теорема Морделла-Вейля. L-функции эллиптических кривых, гипотеза Таниямы-Вейля.
2. **Модулярные формы – базовые свойства.** Эллиптические функции, j-инвариант. Алгебра модулярных форм относительно $SL_2(\mathbb{Z})$. Дельта функция, число разбиений, сумма четырех квадратов. L-функции модулярных форм, функциональное уравнение. Операторы Гекке и эйлерово произведение. Модулярные формы относительно конгруэнц-подгрупп – набросок теории.
3.**Аналитические методы в алгебраической теории чисел.** Распределение простых чисел и дзета-функция Римана. Теорема Дирихле о простых числах в арифметических прогрессиях. Функциональное уравнение для дзета-функции Дедекинда и формула для вычета.
4. **Локальные и глобальные поля.** Нормирования полей алгебраических чисел. Анализ в p-адических полях. Разложение на простые идеалы и пополненные локальные кольца. Дифферента и ветвление. Круговые поля. Идели и адели. Модулярные формы и адели.
5. **Основы теории полей классов.** Формулировки основных результатов. Приложения: гильбертово поле классов и разложение простых, квадратичные формы и принцип Хассе, центральные простые алгебры. Эллиптические кривые с комплексным умножением – формулировки результатов.
6.**Кривые над конечными полями.** Аналогия числовые поля – функциональные поля. Геометрия кривых над конечными полями. Гипотеза Римана для кривых над конечными полями. Проблема нахождения максимального числа точек на кривых над конечным полем.

Требования к слушателям: От слушателей требуется свободное владение основами алгебры, анализа (вещественного и комплексного), знакомство с теорией Галуа, теорией алгебраических чисел (конечные расширения $\mathbb{Q}$ и разложение на простые в них), основами алгебраической геометрии.

Литература.

1. Боревич З. И., Шафаревич И. Р. «Теория чисел». - М.: Наука, 1985.
2. Вейль А. «Основы теории чисел». - М.: Едиториал УРСС, 2004.
3. Влэдуц С. Г., Ногин Д. Ю., Цфасман М. А.. «Алгеброгеометрические коды. Основные понятия». – М.: МЦНМО, 2003г.
4. Кнапп Э. «Эллиптические кривые». - М.: Факториал Пресс, 2004.
5. Коблиц Н. « p-адические числа, p-адический анализ и дзета-функции». - М.: Мир, 1982.
6. Ленг С. «Алгебраические числа». - М.: Мир, 1972.
7. Ленг С. «Введение в теорию модулярных форм». - М.: Мир, 1979.
8. Карацуба А.Л. «Основы аналитической теории чисел». - М.: Наука, 1983. - 240с.
9. Касселс Дж., Фрёлих А. (ред.) «Алгебраическая теория чисел». - М.: Мир, 1969.
10. Манин Ю. И., Панчишкин А. А. «Введение в современную теорию чисел». - М.: МЦНМО, 2009.
11. Серр Ж.-П. «Курс арифметики». - М.: Мир, 1972.
12. Cox D., Primes of the form x2 + ny2, Pure and Appl. Math., Wiley, 1989.
13. Newman D.J. «Analytic Number Theory», Springer-Verlag, GTM 177, 1998.
14. Silverman J. «The Arithmetic of Elliptic Curves», Springer-Verlag, GTM 106, 1986.
15. Silverman J. «Advanced Topics in the Arithmetic of Elliptic Curves», Springer-Verlag, GTM 151, 1995.