Дискретное логарифмирование

1. Задача дискретного логарифмирования. Пример её решения в $\mathbb{F}_p^*$.
2. Методы Полига-Хеллмана и Полларда решения задачи дискретного логарифмирования.
3. Эллиптическая кривая. Форма Вейерштрасса. Дискриминант и j-инвариант. Сложение точек.
4. $K[E]$ и $K(E)$. Гомогенизация и дегомогенизация.
5. Униформизатор. Порядок функции в точке. Порядок в каждой точке кривой функции $x - x_1$.
6. Нули и полюса многочленов из $K[E]$. Совпадение количества нулей и полюсов (с учётом порядков).
7. Дивизоры. Группы Пикара. Изоморфизм $Pic^0(E) \simeq E$.
8. Рациональные отображения. Кольцо эндоморфизмов $End(E)$.
9. Эндоморфизмы умножения на целое число. Многочлены деления. Кривые с комплексным умножением.
10. p-адическая фильтрация. Лемма Гензеля и теорема об изоморфизме $E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \simeq E(\mathbb{F}_p)$.
11. p-адический логарифм и теорема об изоморфизме $E_s(\mathbb{Q}_p)/E_{s+1}(\mathbb{Q}_p) \simeq \mathbb{F}_p^+$ при $s > 0$. Дискретное логарифмирование на кривых с $|E(\mathbb{F}_p)| = p$.
12. Квадратичные расширения поля $\mathbb{Q}$. Кольца целых чисел в этих расширениях. Эндоморфизм Фробениуса. Теорема Хассе. Структура группы точек эллиптической кривой над конечными полями.
13. Структура группы точек эллиптической кривой вида $y^2 = x^3 + ax$ над $\mathbb{F}_p$ при $p \equiv 1 \pmod 4$. Структура группы точек эллиптической кривой вида $y^2 = x^3 + b$ над $\mathbb{F}_p$ при $p \equiv 1 \pmod 3$. Дискретное логарифмирование на этих кривых.

Спаривания на эллиптической кривой

1. Дивизоры на эллиптической кривой. Изогении. Теоремы о верхней и нижней звёздочке. Степень и индекс ветвления изогении.
2. Закон взаимности Вейля.
3. Спаривание Вейля. Различные определения (без доказательства эквивалентности). Свойства (с доказательством).
4. Доказательство эквивалентности различных определений спаривания Вейля.
5. Сведение задачи дискретного логарифмирования в группе точек $E(\mathbb{F}_p)$ к аналогичной задаче в $\mathbb{F}_{p^k}^*$, где k такое, что $\mu_n \subset \mathbb{F}_{p^k}^*$.
6. Спаривание Тэйта. Различные определения и их эквивалентность (в том числе определение, нужное для доказательства невырожденности).
7. Свойства спаривания Тэйта.
8. Алгоритм Миллера вычисления спариваний.
9. Спаривания эйта и Хесса. Их связь.
10. Доказательство теоремы Хассе.