Билет № 1.

Эллиптические кривые и криптография - 2. Весна 2011.

Криптосистемы на эллиптических кривых. Задание текста точками эллиптической кривой: вероятностный метод.

Задачи.

1. Пусть многочлен $x^3 + ax + b$ разлагается над F_q на линейные множители. Доказать, что группа точек на кривой $y^2 = x^3 + ax + b$ не является циклической.

2. Найти тип кривой $y^2 = x^3 - 1$ над F_{25}.

Билет № 2.

Эллиптические кривые и криптография - 2. Весна 2011.

Вычисление кратности данной точки: метод последовательного удвоения. Сложность вычисления кратности точки. Методы выбора эллиптической кривой и точки на ней.

Задачи.

1. Доказать, что число точек на эллиптической кривой $y^2 + y = x^3$ над полем F_q, $q \equiv 2 \pmod 3$ равно $q + 1$.

2. Найти количество точек на кривой $y^2 + y = x^3 - x + 1$ над F_{2^r}.

Билет № 3.

Эллиптические кривые и криптография - 2. Весна 2011.

Аналоги ключевого обмена Диффи-Хелмана, системы Мэсси-Омуры и системы Эль-Гамаля. Задача дискретного логарифмирования на эллиптической кривой.

Задачи.

1. Доказать, что число точек на кривой $y^2 = x^3 - x$ над полем F_q, $q \equiv 3 \pmod 4$ равно $q + 1$.

2. Вычислить число точек на эллиптической кривой $y^2 = x^3 - x$ над F_{1331}.

Билет № 4.

Эллиптические кривые и криптография - 2. Весна 2011.

Число точек на эллиптической кривой над конечным полем. Теорема Хассе и первая теорема Дойринга-Ватерхауза. Сложность вычисления порядка группы эллиптической кривой над простым полем по методу Шуфа.

Задачи.

1. Пусть многочлен $x^3 + ax + b$ разлагается над F_q на линейные множители. Доказать, что группа точек на кривой $y^2 = x^3 + ax + b$ не является циклической.

2. Найти количество точек на кривой $y^2 + y = x^3 - x + 1$ над F_{3^r}.

Билет № 5.

Эллиптические кривые и криптография - 2. Весна 2011.

Рост числа точек на эллиптической кривой при расширении основного поля. Дзета-функция и теорема Вейля.

Задачи.

1. Доказать, что число точек на эллиптической кривой $y^2 = x^3 - 1$ над полем F_q, $q \equiv 2 \pmod 3$, q нечётно, равно $q + 1$.

2. Вычислить дзета-функцию для кривой $y^2 = x^3 - x$ над F_{11}.

Билет № 6.

Эллиптические кривые и криптография - 2. Весна 2011.

Групповая структура на эллиптической кривой над конечным полем: тип кривой, вторая теорема Дойринга-Ватерхауза.

Задачи.

1. Найти количество точек на кривой $y^2 = x^3 - x$ над кольцом Z_{441}.

2. Вычислить дзета-функцию для кривой $y^2 = x^3 - x$ над F_{13}.

Билет № 7.

Эллиптические кривые и криптография - 2. Весна 2011.

Проверка числа на простоту: метод Поклингктона и его обобщение метод Гольдвассера-Килиана, вычисление вероятностей успеха в обоих случаях.

Задачи.

1. Докажите, что если у многочлена $x^3 + ax + b$ есть корень в поле F_q, то число точек на кривой $y^2 = x^3 + ax + b$ над F_q чётно.

2. Найти число точек на кривой $y^2 + y = x^3$ над кольцом Z_{55}.

Билет № 8.

Эллиптические кривые и криптография - 2. Весна 2011.

Числа Ферма и Мерсенна. Алгоритмы проверки на простоту.

Задачи.

1. Какая точка кривой соответствует числу 4 при кодировании чисел 0,1,2,..., 7 точками на кривой $y^2 = x^3 - 1$ над полем F_{71} так, чтобы вероятность неудачи была $\frac{1}{2^{10}}$?

2. Вычислить дзета-функцию для кривой $y^2 = x^3 - x$ над F_{13}.

Билет № 9.

Эллиптические кривые и криптография - 2. Весна 2011.

Разложение числа на множители: $(p-1)$-метод Полларда и Метод Ленстры. Оценки на выбор границ.

Задачи.

1. Пусть E – эллиптическая кривая над полем F_p. Пусть N_r – число точек на этой кривой над полем F_{p^r}. Докажите, что при $r > 1$, $p > 3$ число N_r является составным.

2. Найти тип кривой $y^2 = x^3 - x$ над F_{27}.

Билет № 9.

Эллиптические кривые и криптография - 2. Весна 2011.

Разложение числа на множители: $(p-1)$-метод Полларда и Метод Ленстры. Оценки на выбор границ.

Задачи.

1. Пусть E – эллиптическая кривая над полем F_p. Пусть N_r – число точек на этой кривой над полем F_{p^r}. Докажите, что при $r > 1$, $p > 3$ число N_r является составным.

2. Найти тип кривой $y^2 = x^3 - x$ над F_{27}.

Билет № 9.

Эллиптические кривые и криптография - 2. Весна 2011.

Разложение числа на множители: $(p-1)$-метод Полларда и Метод Ленстры. Оценки на выбор границ.

Задачи.

1. Пусть E – эллиптическая кривая над полем F_p. Пусть N_r – число точек на этой кривой над полем F_{p^r}. Докажите, что при $r > 1$, $p > 3$ число N_r является составным.

2. Найти тип кривой $y^2 = x^3 - x$ над F_{27}.

Билет № 9.

Эллиптические кривые и криптография - 2. Весна 2011.

Разложение числа на множители: $(p-1)$-метод Полларда и Метод Ленстры. Оценки на выбор границ.

Задачи.

1. Пусть E – эллиптическая кривая над полем F_p. Пусть N_r – число точек на этой кривой над полем F_{p^r}. Докажите, что при $r > 1$, $p > 3$ число N_r является составным.

2. Найти тип кривой $y^2 = x^3 - x$ над F_{27}.