### Министерство науки и высшего образования Российской Федерации

1. Санкт-Петербургский политехнический университет Петра Великого
2. —
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 3**

1. **«ГРАФЫ ИЗОГЕНИЙ ЭЛЛИПТИЧЕСКИХ КРИВЫХ»**
2. по дисциплине «Методы алгебраической геометрии в криптографии»
3. Выполнил
4. студент гр. 5151001/00201 Устюгов А.А.

<*подпись*>

1. Проверил:
2. старший преподаватель Ярмак А.В.

<*подпись*>

1. Санкт-Петербург
2. 2023

# Цель работы

Исследование графовой структуры, показывающей действие изогений на множестве j-инвариантов эллиптических кривых, заданных над конечным полем.

# Порядок выполнения работы

1. Получить у преподавателя задание с требованием к числу классов и характеристики поля.

2. Разработать программу П-1, выполняющую построение графов j-инвариантов изогенных несуперсингулярных эллиптических кривых для различных простых степеней изогений и вычисление звезды изогений

# Ход работы

Необходимо построить граф изогений несуперсингулярных кривых. На вход подается число классов h, которое должно быть больше 100.

Для подсчета числа классов я в цикле задаюсь фундаментальным дискриминантом эндоморфизма Фробениуса, задавая его как простое число. Перебирая возможные дискриминанты, считаю для них число классов с помощью алгоритма, выполненного в лабораторной работе №1. В итоге был найден дискриминант D = -5711 и число классов h = 109.

По найденному дискриминанту нахожу характеристику поля p. p = 37472371.

С помощью, встроенной в Sage, функции вычисляю полином Гильберта и нахожу его корни, которые являются j-инвариантами кривых.

Убедился в том, что кривые, соответствующие данным j-инвариантам, не являются суперсингулярными. Для этого по j-инварианту нахожу коэффициенты A, B кривой и с помощью встроенного метода sage проверяю на суперсингулярность.

С помощью установленной базы данных с модулярными полиномами, начинаю строить цепочку j-инвариантов изогенных кривых. Считаю степени l, которые являются простыми числами Элкиса, которые задают подстановку на j-инвариантах. Были выбраны l=5,7,11,13,17. Теперь начинаю вычислять цепочки j-инвариантов и строить граф.

Для l=5:

Цепочка: [37259002, 23097470, 34772294, 27634352, 20311, 19576669, 29868269, 14891556, 8446837, 12616088, 12920120, 5583511, 9203343, 1096759, 27191251, 485237, 28706666, 21662071, 17039118, 29892455, 1905797, 13820086, 23975513, 32818950, 19653950, 21183690, 33570870, 23445631, 33537056, 22355057, 88346, 18119168, 11193617, 31569993, 3502147, 34359969, 7384577, 12171956, 3633511, 17407900, 11646903, 2743940, 31669580, 27173305, 2999306, 14105826, 15086277, 36800549, 30337511, 27776410, 36570023, 34673749, 31791751, 10393647, 28044850, 4033379, 13437788, 15437224, 21163678, 2062177, 22852799, 10525812, 6173860, 25238829, 9596211, 17984305, 21424674, 28795167, 21818221, 21005644, 8392406, 20265017, 12027084, 16887005, 17152786, 34965115, 36974590, 15748641, 23400156, 30816613, 30736793, 9459247, 13942511, 6616386, 7594340, 28658478, 27908331, 12074590, 30663058, 29046402, 37176614, 32723406, 10539086, 6608666, 26907999, 7731693, 22752961, 22441986, 13865525, 33435506, 5809320, 22028604, 5061018, 18066475, 29433276, 34835206, 1074961, 28909376, 5723962]

На рисунке 1 представлен граф изогении степени 5

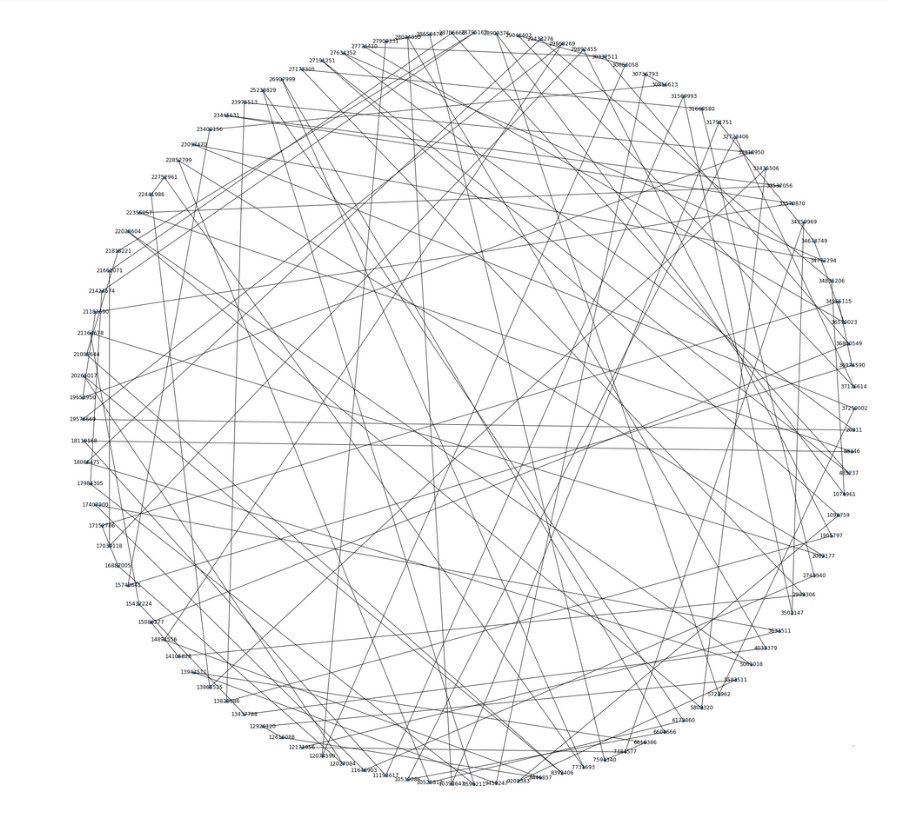


Рисунок 1 – граф изогении степени 5

Для l = 7:

Цепочка: [37259002, 27173305, 27908331, 1905797, 25238829, 1074961, 11646903, 6616386, 21662071, 22852799, 18066475, 12171956, 30736793, 27191251, 15437224, 5809320, 3502147, 15748641, 5583511, 28044850, 22441986, 18119168, 17152786, 8446837, 34673749, 26907999, 33537056, 20265017, 19576669, 30337511, 32723406, 21183690, 21818221, 34772294, 14105826, 30663058, 23975513, 17984305, 5723962, 31669580, 28658478, 29892455, 6173860, 34835206, 17407900, 13942511, 28706666, 2062177, 5061018, 7384577, 30816613, 1096759, 13437788, 33435506, 31569993, 36974590, 12920120, 10393647, 22752961, 88346, 16887005, 14891556, 36570023, 6608666, 23445631, 8392406, 20311, 36800549, 37176614, 19653950, 28795167, 23097470, 2999306, 12074590, 13820086, 9596211, 28909376, 2743940, 7594340, 17039118, 10525812, 29433276, 3633511, 9459247, 485237, 21163678, 22028604, 34359969, 23400156, 9203343, 4033379, 13865525, 11193617, 34965115, 12616088, 31791751, 7731693, 22355057, 12027084, 29868269, 27776410, 10539086, 33570870, 21005644, 27634352, 15086277, 29046402, 32818950, 21424674]

На рисунке 2 представлен граф изогении степени 7.

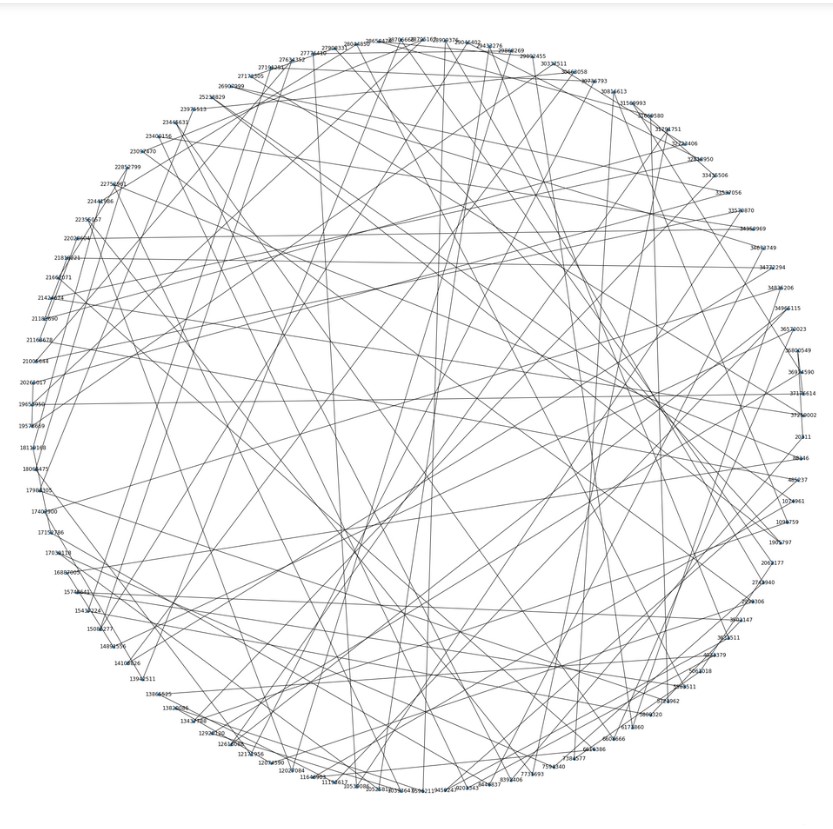


Рисунок 2 – граф изогении степени 7

Для l =11:

Цепочка: [37259002, 36800549, 26907999, 11193617, 30816613, 21662071, 9596211, 34772294, 27776410, 22752961, 3502147, 9459247, 29892455, 21424674, 20311, 34673749, 13865525, 7384577, 6616386, 13820086, 21818221, 29868269, 10393647, 5809320, 3633511, 28658478, 32818950, 8392406, 8446837, 4033379, 5061018, 11646903, 12074590, 21183690, 12027084, 12920120, 15437224, 29433276, 31669580, 29046402, 23445631, 17152786, 9203343, 2062177, 1074961, 2999306, 32723406, 22355057, 36974590, 27191251, 10525812, 5723962, 15086277, 6608666, 18119168, 23400156, 28706666, 25238829, 23097470, 30337511, 7731693, 31569993, 30736793, 17039118, 17984305, 27634352, 36570023, 22441986, 34359969, 13942511, 1905797, 28795167, 19576669, 31791751, 33435506, 12171956, 7594340, 23975513, 21005644, 14891556, 28044850, 22028604, 17407900, 27908331, 19653950, 20265017, 12616088, 13437788, 18066475, 2743940, 30663058, 33570870, 16887005, 5583511, 21163678, 34835206, 27173305, 37176614, 33537056, 34965115, 1096759, 22852799, 28909376, 14105826, 10539086, 88346, 15748641, 485237, 6173860]

На рисунке 3 представлен граф изогении степени 11.

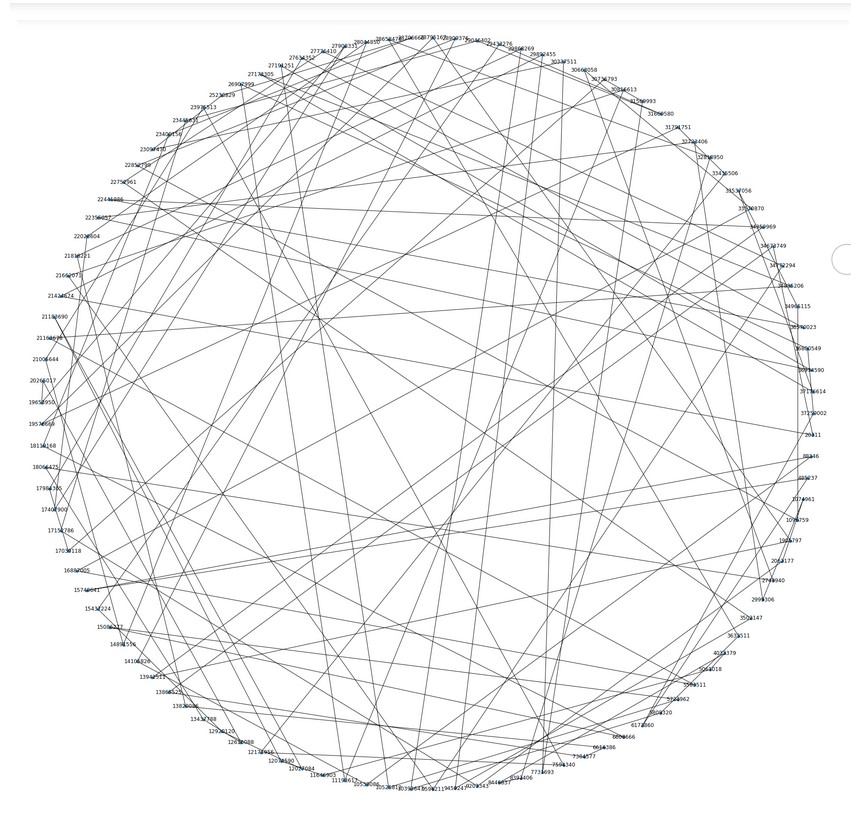


Рисунок 3 – граф изогении степени 11

Для l=13:

Цепочка: [37259002, 17407900, 23400156, 8446837, 36800549, 27908331, 28706666, 4033379, 26907999, 19653950, 25238829, 5061018, 11193617, 20265017, 23097470, 11646903, 30816613, 12616088, 30337511, 12074590, 21662071, 13437788, 7731693, 21183690, 9596211, 18066475, 31569993, 12027084, 34772294, 2743940, 30736793, 12920120, 27776410, 30663058, 17039118, 15437224, 22752961, 33570870, 17984305, 29433276, 3502147, 16887005, 27634352, 31669580, 9459247, 5583511, 36570023, 29046402, 29892455, 21163678, 22441986, 23445631, 21424674, 34835206, 34359969, 17152786, 20311, 27173305, 13942511, 9203343, 34673749, 37176614, 1905797, 2062177, 13865525, 33537056, 28795167, 1074961, 7384577, 34965115, 19576669, 2999306, 6616386, 1096759, 31791751, 32723406, 13820086, 22852799, 33435506, 22355057, 21818221, 28909376, 12171956, 36974590, 29868269, 14105826, 7594340, 27191251, 10393647, 10539086, 23975513, 10525812, 5809320, 88346, 21005644, 5723962, 3633511, 15748641, 14891556, 15086277, 28658478, 485237, 28044850, 6608666, 32818950, 6173860, 22028604, 18119168, 8392406]

На рисунке 4 представлен граф изогении степени 13.

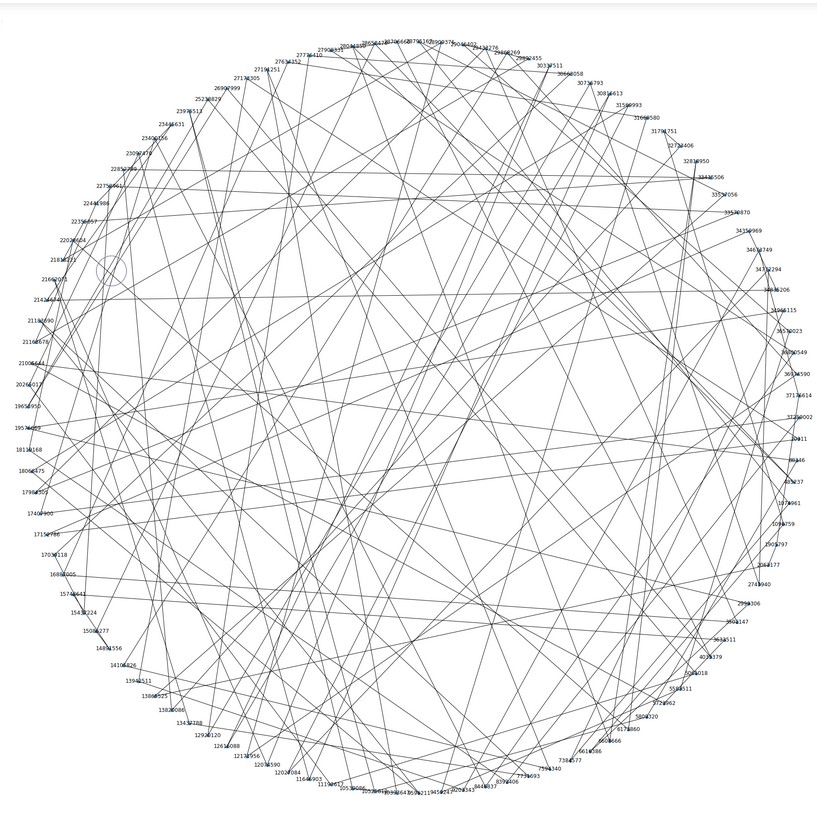


Рисунок 4 – граф изогении степени 13

Для l=17:

Цепочка: [37259002, 22441986, 28658478, 16887005, 10525812, 27776410, 12171956, 21183690, 1096759, 23097470, 13865525, 27908331, 17152786, 6173860, 36570023, 3633511, 33570870, 27191251, 34772294, 33435506, 12074590, 34965115, 25238829, 34673749, 17407900, 23445631, 485237, 27634352, 5809320, 30663058, 36974590, 9596211, 31791751, 11646903, 33537056, 28706666, 20311, 22028604, 29046402, 15748641, 17984305, 10393647, 2743940, 22355057, 21662071, 19576669, 5061018, 37176614, 23400156, 21424674, 28044850, 31669580, 88346, 17039118, 29868269, 18066475, 32723406, 30816613, 28795167, 4033379, 27173305, 18119168, 29892455, 14891556, 29433276, 10539086, 30736793, 21818221, 13437788, 2999306, 11193617, 1905797, 8446837, 34835206, 6608666, 9459247, 21005644, 15437224, 14105826, 31569993, 13820086, 12616088, 1074961, 26907999, 13942511, 8392406, 21163678, 15086277, 3502147, 23975513, 12920120, 28909376, 7731693, 6616386, 20265017, 2062177, 36800549, 34359969, 32818950, 5583511, 5723962, 22752961, 7594340, 12027084, 22852799, 30337511, 7384577, 19653950, 9203343]

На рисунке 5 представлен граф изогении степени 17.

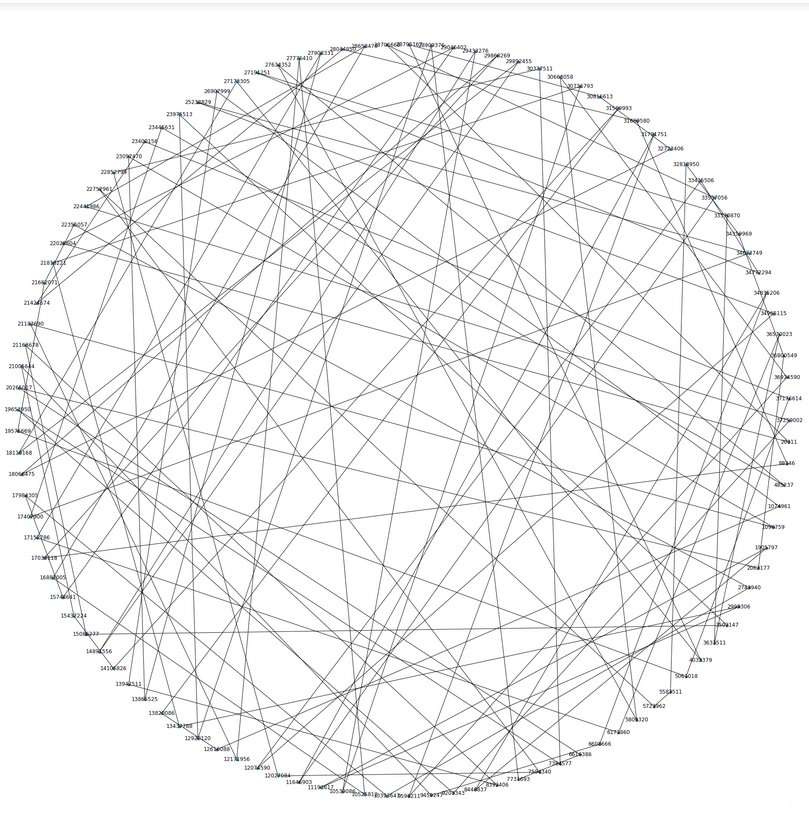


Рисунок 5 – граф изогении степени 17

На рисунке 6 представлена звезда изогении, являющаяся наложением всех графов.

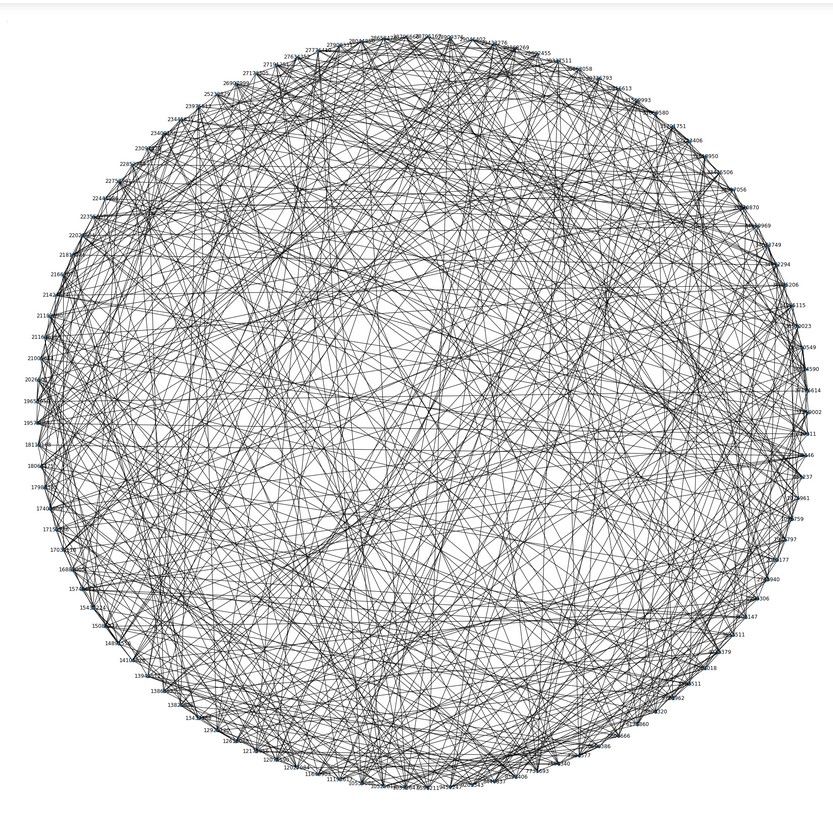


Рисунок 6 – звезда изогении

# Ответы на контрольные вопросы

1. Как определяется число уровней в графе изогений несуперсингулярных кривых в форме вулкана

«Кратер» вулкана– это 𝑗-инварианты кривых с равными кольцами эндоморфизмов (изоморфных максимальному квадратичному порядку). Можно спускаться по вертикальным изогениям, пока они есть. Или из характеристики поля: . Тогда будет с+1 уровней

2. Установить соответствие между группой классов идеалов и группой классов изогений эллиптических кривых

Для всех степеней изогений, лежащих в одном классе, перестановка изогенных эллиптических кривых будет совпадать. Для изогений таких степеней существует изоморфизм между данной группой и группой классов идеалов 𝑂𝐷𝜋 мнимого квадратичного порядка (отсюда следует равенство числа классов идеалов и числа классов изогений).

# Выводы

В данной лабораторной был изучен процесс построения графов изогении разных степеней, а также процесс построения звезды изогении.