МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І.І.МЕЧНИКОВА

(повне найменування вищого навчального закладу)

Факультет математики, фізики та інформаційних технологій

(повне найменування інституту, назва факультету (відділення))

Кафедра комп'ютерної алгебри та дискретної математики

(повна назва кафедри (предметної, циклової комісії))

Дипломна робота

на здобуття освітньо-кваліфікаційного рівня «бакалавр»

(освітньо-кваліфікаційний рівень)

на тему «Псевдопрості Фробениуса»

«Psevdoprime numbers of Frobenies»

Виконала: студентка денної форми навчання
напряму підготовки 6.050102 – Комп'ютерна інженерія

(шифр і назва напряму підготовки, спеціальності)

Біла Юлія Василівна

(прізвище, ім'я, по-батькові)

Керівник доц. Бєлозьоров Г.С.

(науковий ступінь, вчене звання, прізвище та ініціали, підпис)

Рецензент доц. Варбанець С.П.

(науковий ступінь, вчене звання, прізвище та ініціали)

Рекомендовано до захисту:

Протокол засідання кафедри

№___ від «___»_____ 2019 р.

Завідувач кафедри

_____ _П. Д. Варбанець_

(підпис) (прізвище, ініціали)

Захищено на засіданні ЕК № ___

протокол № __ від «___» ____ 2019 р.

Оцінка _____/_____/_____

(за національною шкалою, шкалою ECTS, бали)

Голова ЕК

_____ _О.О. Арсірій_

(підпис) (прізвище, ініціали)

Одеса – 2019

АННОТАЦІЯ

Темою даної дипломної роботи є побудова комп'ютерної моделі ймовірнісного простого тесту Фробениуса.

З більшості класів псевдопростих чисел були обрані три «основних», які і стали предметом порівняння. Це числа Кармайкла, Фібоначчі та Лукаса.

За основу ймовірнісного простого тесту взятий поліном Фібоначчі $x^2 - x - 1$ та розглянутий цей самий поліном з різними коефіцієнтами. Призначення програмного продукту полягає в тестуванні великих масивів чисел на простоту і виділенні серед них саме псевдопростих Фробениуса.

Мовою розробки є Perl, для написання коду і компіляції використане середовище розробки XCode.

АННОТАЦИЯ

Темой данной дипломной работы является построение компьютерной модели вероятностного простого теста Фробениуса.

Из большинства классов псевдопростых чисел были выбраны три «основных», которые и стали предметом сравнения. Это числа Кармайкла, Фибоначчи и Лукаса.

За основу вероятностного простого теста взят многочлен Фибоначчи $x^2 - x - 1$ и рассмотрен этот самый многочлен с различными коэффициентами. Назначение программного продукта заключается в тестировании больших массивов чисел на простоту и выделении среди них именно псевдопростых Фробениуса.

Языком разработки является Perl, для написания кода и компиляции использована среда разработки XCode.

ANNOTATION

The main topic of this diploma project is the producing of the computer model of Probable Prime Test by Frobenies.

There were choosen three "common" numbers, which have become the object of comparation in the most of pseudoprime numbers. They are the numbers by Carmichael, Fibonacci and Lukas.

As basis of Probable Prime Test the polynome by Fibonacci was taken and it was reviewed with different factors. The purpose of the program product is to test the big number arrays for primality and to separate from them the pseudoprimes by Frobenies.

The implementation was carried out using the Perl development language, the XCode development environment was used for writing code and compiling.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ І ТЕРМІНІВ

Скорочення

НСД – найбільший спільний дільник

НСНД – найбільший спільний нормований дільник

СНД – спільний нормований дільник

mod – конгруенція по модулю

deg – ступінь многочлена (також позначається як ∂)

PRP – ймовірне просте число

SPRP – сильне ймовірне просте число

ВСТУП

Із появою у 1976 році ідеології відкритого ключа та з розвитком можливостей обчислювальної техніки в криптографії почали активно використовувати фундаментальні результати теорії чисел і сучасної прикладної алгебри. Так однією з головних обчислювальних задач сучасної криптографії є задача пошуку великих простих чисел.

Більшість сучасних асиметричних криптосистем так чи інакше використовують великі прості числа. Саме вони добре підходять для побудови односторонніх функцій. Нагадаємо, що односторонніми називають такі функції, які легко обчислюються для довільного вхідного значення, але аргумент при заданому значенні функції знайти важко. Такі задачі, як обчислення дискретного логарифму, або розклад на множники, можуть бути використані при побудові односторонніх функцій і традиційно вважаються складними.

Числа повинні бути достатньо великими, щоб забезпечувати криптоаналітичну стійкість використовуваного алгоритму. В той же час, їх потрібно генерувати порівняно швидко. Це обумовлює важливість побудови ефективних алгоритмів для перевірки великого випадкового числа на простоту (випадковість обраного числа теж є важливою для забезпечення стійкості). Всі такі алгоритми можна поділити на дві групи: детерміновані та ймовірнісні. Перші встановлюють простоту числа математично строго, і, як правило, потребують багато часу для перевірки, в той час як другі просто мінімізують ймовірність похибки у визначенні простоти після кожного послідовного свого запуску, що має назву ймовірнісні прості тести.

Поширення ймовірнісних простих тестів в останні роки призвело до появи безлічі визначень зі словом «псевдопросте число» у них. У цій роботі детально розглянуті докази існування псевдопростих чисел Фробениуса зі статті Гретхема та реалізовано і протестовано роботу алгоритму. У 1980, Моньє і Рабін довели, що у сильному ймовірнісному простому тесті

вірогідність помилки не більше $\frac{1}{4}$. Хоча тест, введений у ймовірний простий тест з високою точністю, має асимптотичний час виконання в три рази більше, ніж в тесті на сильне ймовірне просте число. Доведена оцінка помилки набагато менше, ніж $\frac{1}{64}$, досягнута за допомогою трьох сильних ймовірнісних простих тестів. Можливо, основна перевага цього підходу полягає в тому, що замість того, щоб довести десять різних теорем про десять різних типів псевдопростих чисел, можна довести одну теорему про псевдопрості числа Фробениуса та застосувати її до кожного типу псевдопростих чисел.

Таким чином, мета даної дипломної роботи – детально розглянути та побудувати модель ймовірнісного простого тесту Фробениуса та протестувати його на достатньо великому масиві чисел. Для досягнення поставленої мети потрібно вирішити наступні завдання:

1) виконати аналіз джерел дослідження і підготувати матеріали про обрані прості та псевдопрості числа;

2) провести огляд інформації щодо існуючих алгоритмів, що перевіряють число на простоту, а саме алгоритми Кармайкла, Фібоначчі та Лукаса;

3) розглянути тест Фробениуса та псевдопрості Фробениуса;

4) провести комп’ютерне моделювання і тестування роботи ймовірнісного простого тесту Фробениуса;

5) побудувати таблиці ймовірно простих;

6) виділити суто псевдопрості Фробениуса;

7) виконати аналіз кореляції псевдопростих чисел Фробениуса до інших псевдопростих чисел.

ВИСНОВОК

В процесі аналізу питань псевдопростих чисел у криптографії були вирішені наступні питання:

1) виконаний аналіз джерел дослідження і підготовлені матеріали про прості, псевдопрості, сильні псевдопрості числа;

2) проведений огляд інформації щодо існуючих алгоритмів, що перевіряють число на простоту, а саме алгоритми Кармайкла, Фібоначчі та Лукаса;

3) розглянутий тест Фробениуса та псевдопрості Фробениуса;

4) проведено комп'ютерне моделювання і тестування роботи ймовірнісного простого тесту Фробениуса, спроектованого в середовищі розробки XCode, використовуючи мову програмування Perl;

5) побудовані таблиці ймовірних простих;

6) виділені суто псевдопрості Фробениуса;

7) виконаний аналіз кореляції псевдопростих чисел Фробениуса до інших псевдопростих чисел.

З більшості псевдопростих чисел були обрані три «основних», які і стали предметом порівняння. Це числа Кармайкла, Фібоначчі та Лукаса. Виходячи з аналізу цих псевдопростих чисел та їх порівнянням робимо висновок, що вони всі дуже різні, хоча послідовності Лукаса та Фібоначчі схожі за одним винятком, коли у другого P та Q задано константою 1 та -1; псевдопрості Фробениуса мають велику частку псевдопростих Фібоначчі, бо за основу ймовірнісного простого тесту взятий поліном Фібоначчі $x^2 - x - 1$ та розглядуючи цей самвц поліном з різними коефіцієнтами бачимо, що деякі з них збігаються, тобто є ймовірними простими числами Фробениуса.

В результаті моделювання та тестування роботи ймовірнісного простого тесту Фробениуса, спроектованого в середовищі симулятора XCode, використовуючи мову програмування Perl ми переконались, що складене, яке пройшло цей тест буде псевдопростим Фробениуса, але не навпаки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Перевірка на простоту в загальному вигляді [Електронний ресурс] – Режим доступу: http://mathworld.wolfram.com/AKSPrimalityTest.html

2. Рекорди простих чисел по роках [Електронний ресурс] – Режим доступу: https://primes.utm.edu/notes/by_year.html

3. Перші сильні псевдопрості по основі 2 [Електронний ресурс] – Режим доступу: https://oeis.org/A001262

4. Перші сильні псевдопрості по основі 3 [Електронний ресурс] – Режим доступу: https://oeis.org/A020229

5. Перші сильні псевдопрості по основі 5 [Електронний ресурс] – Режим доступу: https://oeis.org/A020231

6. Число Кармайкла - W. R. Alford, Andrew Granville, and Carl Pomerance. There are infinitely many Carmichael numbers. Annals of Mathematics, 140: 703–722, 1994.

7. Псевдопрості Фібоначчі [Електронний ресурс] – Режим доступу: https://oeis.org/A212424

8. Псевдопрості Фробениуса - Jon Grantham (March 2000). "Frobenius Pseudoprimes". Mathematics of Computation. 70 (234): 873–891.

9. Послідовність перших псевдопростих Фробениуса відносно полінома Фібоначчі [Електронний ресурс] – Режим доступу: https://oeis.org/A212424

10. Псевдопрості Лукаса - Robert Baillie; Samuel S. Wagstaff, Jr. (October 1980). "Lucas Pseudoprimes" (PDF). Mathematics of Computation. 35 (152): 1391–1417.

11. Псевдопрості Фібоначчі - Müller, Winfried B.; Oswald,Alan (1993). "Generalized Fibonacci Pseudoprimes and Probable Primes". In G.E. Bergum; et al. (eds.). Applications of Fibonacci Numbers. 5. Kluwer. pp. 459–464.

12. Ричард Крендалл, Померанс Карл. Прості числа: Криптографічні та обчислювальні аспекти. Пер. З англ. / Під ред. та з передм. В. Н. Чубарікова. – М.:УРСС: Книжковий дім «ЛІБРОКОМ», 2011. – 352 – 376.

13. Алгоритмічні проблеми теорії чисел – В. В. Ященко (Жовтень 1998). Введення у криптографію (PDF). – С. 86–99.

14. Простота та факторизація – Н. Коблиц (2001). Курс теорії чисел та криптографії. Москва: Наукове вид-во ТВП. – С. 139 – 180.