MATHEMATICS/THEORETICAL PROJECTS

NAME: Binyameen Mohamedy
PROVISIONAL PROJECT TOPIC: Recursive Prime Generating Functions
PROVISIONAL EXPO CATEGORY: Mathematics

Introduction

The author aims to prove a mathematical conjecture stating that a certain infinite family of functions always output prime numbers or 1, as well as properties of the primes produced. Rowland (2008) provided work in the field together with other authors, but they failed to solve Conjecture 1, leaving a need for a resolution to this and other problems.

Purpose/Application:

Encryption systems:

RSA encryption (named after its creators R. Rivest, A. Shamir and L. Adleman) is currently the strongest encryption system in the world. It secures banking details, internet communication, VPNs, and more. Even with a supercomputer, it is extremely difficult to decrypt RSA encrypted information.

However, with the development of quantum computers, expected to appear on the market in the following few decades, this security of RSA encryption is being threatened. Due to the extraordinary computing power of a quantum computer, it can decode the encrypted information. This has led many mathematicians and computer scientists to try and seek an alternate encryption system that wouldn't be compromised by a quantum computer.

One application of the authors work is to modify RSA to make it stronger through an alternate method to generate much larger primes faster. This would increase the strength of encrypted data. This will help anyone who uses online banking to secure their data.

Development of a new theory:

It will help mathematicians in pursuing ideas that were laid out by Rowland. The work solves Conjecture 1-4 , proving a 16-year-old problem and further developing the field.

Nation building:

This helps South Africa as it has a severe lack of contribution to mathematics and physics with no South African Nobel prize winners or Fields medallist (Nobel prize equivalent in mathematics). It can inspire young kids to pursue Mathematics and have South Africa compete internationally in Mathematics.

It would also help fight stereotypes others may have of South Africa not being developed in the STEM field and encourage foreign students to apply at South African universities.
Einstein and his contemporaries made Germany a centre of science, giving Germans some to be proud of and unite under. Nation building can be done through science and help South Africa in the same fashion as sports.

New ideas of the author:

The new ideas provided by the author is from key Conjectures on critical components of the problem formulated through numerical data and for Conjecture 4 it is a new link connecting the field of Sieve theory to Recursive prime generating functions.

Sieve theory is a field in which types of specified primes are found from a set of integers by removing unwanted integers in various ways. The tools developed in Sieve theory was the key component in the work that won James Maynard the Fields Medal (Nobel Prize of Mathematics) in 2022, Atle Selberg in 1950 and Terence Tao 2006. Many other figures in Sieve theory won other prestigious awards.

Definitions and Concepts:

- gcd(a, b) is the greatest common divisor of a and b.
- Initial Condition: a(h)=k, for some h and k positive integers (See Table 1 for examples)
- Let a(n)[1] = a(n-1) + gcd(a(n-1), n), for every n>h
- b(n) = gcd(a(n-1), n)
- $B(n) = \sum_{k=h+1}^{n} b(k)$
- max(f(x)) is the largest value of f(x) for x>t, for some constant t.
- ln(n) is the natural logarithm of n
- prime number: a number not divisible by any numbers other than 1 and itself

N	*a(n)*	*b(n)*	*B(n)*	*B(n)*
1	7	-	-	-
2	8	1	1	1
3	9	1	1+1	2
4	10	1	1+1+1	3
5	15	5	1+1+1+5	8
6	18	3	1+1+1+5+3	11
7	19	1	1+1+1+5+3+1	12
8	20	1	1+1+1+5+3+1+1	13
9	21	1	1+1+1+5+3+1+1+1	14
10	22	1	1+1+1+5+3+1+1+1+1	15

Table 1: h=1, a(h)=7 --> a(1)=7

Literature review:

Rowland's function:

Rowland (2008) proved that b(n) is prime or 1 for every n>m, under the assumption a(m)=rm (r=2 or r=3) for at least 1 integer m. thus b(n) produced 1 or prime for all n, for a(1)=7 as a(5)=15=3·5. He was not able to prove that the assumption holds for every initial condition.

[1] The function a(n) is named Rowland's function

Ruiz-Cabello/Chamizo/Raboso (2011) proved Conjecture 1 and 2 for the special case of h=1, it is still unsolved for all h>1. Their methods are inspired by Cloitre (2011) and differ from the authors.

Related functions:

Ruiz-Cabello (2017) and Shepke (2014) are based on the function b(n) replaced with the lowest common divisor instead, with its own 'lcm' version of Conjecture 1 and 2, which was only proved conditionally.

Cloitre (2011) created a new formulation of the general idea connecting a more general recursive prime function to famous Conjectures such as the Twin prime Conjecture, Goldbach's Conjecture, Legendre's Conjecture and more.

Shevelev V. (2010) found new recursive functions that generated primes in relation to the famous Twin prime Conjecture. His proofs are flawed and null however his Conjectures have good numerical support.

Conjecture 1- 4 remain unsolved in general.

Problem Statement:

Are Conjectures 1-4 true?

Research question(s):

Are Conjectures 1- 4 true? From those answers can the function b(n) be used to generate primes for RSA encryption?

Aim:

To explore the topic of Rowland's work by solving or providing significant partial progress on Conjectures 1- 4.

Hypothesis/Conjecture:

Conjectures:

1) b(n) is prime or 1 for every value of n greater than some fixed value.
2) b(n) generates infinitely many distinct prime numbers.
3) Every prime, excluding a small finite amount, appears in the sequence of b(n) infinitely often
4) The number of distinct primes generated up to a given integer N, denoted by $p(N)$, is bounded between multiples of ln(N). C_1 ln(N) < $p(N)$ < C_2 ln(N), for some positive constants C_1, C_2
   In big O notation, $p(N) \asymp ln(N)$

Criteria for r:

a) r=1 if a(h) ≤h or a(h)=h+2
b) r=2 if h+1≤a(h)≤2h+1, a(h)≠h+2
   a. if a(h)=h+2 than $\frac{a(n)}{n} \sim n \; as \; n \to \infty$
c) r=3 if a(h)>2h+1

Rowland's assumption:

- There exists an integer n such that a(n)=rn for r=2 or r=3
    - Assuming the above Rowland provided a conditional proof of Conjecture 1 through induction

Method

Materials and Equipment

Desmos was initially used to compute and graph data. It was however to weak and replaced with python and the matpotlib library. Python will also be used to compute numerical data. A journal will be used to do mathematics. No other materials or equipment are needed.

Procedure:

The following is an outline for the proof of Conjectures 1-4

Conjecture 1:

Proving the following lemmas will prove Conjecture 1 as they prove Rowland's assumption:

Lemma 1: $\frac{a(n)}{n} \leq C$, for some constant C and every n.

Let g = max($\frac{a(n)}{n}$) [2]

Proposition 1: min($\frac{a(n-1)}{n-1}$)= $\frac{g+1}{2}$

lemma 2: n divides a(n) when a(n) hits its maximum.

lemma 3: $2 \leq g \leq 3$ if a(h)≥ h+3

proving g ϵ {2,3} would prove Rowland's assumption as g would fit the description of the value r.

a method of proof would be by splitting the problem into cases:

case 1: all trivial cases for g≠2 and g≠3.

case 2: g=2, the author will use proof by contradiction.

case 3: will follow consequently from case 2.

Conjecture 2:

Rowland proved that if m_{n-1} is such a number that a(m_{n-1}) = rm_{n-1} then a(m_n) = rm_n and b(m_n) is the smallest prime factor of $(r-1)m_{n-1}-1$.

Generalising the problem, Define the sequence $k_n = vj_n - 1$ for some constant integer v and sequence of increasing integers with j_1 being some positive integer greater than 4.

[2] For the rest of the paper, for $max(\frac{a(n)}{n})$ and $min(\frac{a(n)}{n})$ n>3a(h)

Proving Conjecture 2 amounts to proving that for all values of j_1 and v, there will be an infinite subsequence of k_n in which no 2 elements share a divisor greater than 1. Which is to say the elements in the subsequence will all have different prime factors from each other.

Main idea of the proof is to consider a finite sequence of k's up to the n-th term. What is the longest subsequence in which all elements have differing prime factors? Putting a lower bound on that number such that the expression tends to infinity as n tends to infinity will prove the Conjecture.

Conjecture 3:

Conjecture 3 is a stronger statement of Conjecture 2. Proving Conjecture 3 is basically proving that for every prime p, there exists infinitely many k_n whose smallest prime factor is p.

The proof is still being developed. The author will aim to prove Conjecture 3 however in the instance of time failure the weaker statement of Conjecture 2 will be proved achieving a partial result.

Conjecture 4

Conjecture 4 can be derived through sieve methods. See research report for more details.

Data analysis:
Have the proof be peer reviewed by 3 mathematicians and be submitted to a mathematics journal.

Ethics

All work obtained from other source, i.e. graphs, tables, figures, papers etc has properly been cited and acknowledged.

Safety

Nothing in this work includes any safety violations of any kind. It is a purely theoretical project.

Time Frames

Literature review end: March 2024
Start of proof: April 2024
Partial results: June 2024
Project report write up and poster for regional: July 2024
Proof finished: August 2024
Peer review: August 2024-September 2024

References

Rowland, E.S. (2008) '*A natural prime-generating recurrence*', *Journal of Integer Sequences [electronic only]*. Available at: https://eudml.org/doc/45342 (Accessed: 25 July 2024).

Cloitre, B. (2011), '*10 conjectures in Additive Number Theory*' *arXiv.org*. Available at: https://arxiv.org/abs/1101.4274 (Accessed: 25 July 2024).

Chamizo, F., Raboso, D. and Ruiz-Cabello, S. (2011) '*On Rowland's sequence*', *The Electronic Journal of Combinatorics*. Available at: https://www.combinatorics.org/ojs/index.php/eljc/article/view/v18i2p10 (Accessed: 25 July 2024).

Serafín Ruiz-Cabello (2017) 'On the use of the least common multiple to build a prime-generating recurrence', *International Journal of Number Theory*, 13(04), pp. 819–833. Available at: https://doi.org/10.1142/s1793042117500439.

Schepke M. (2014), 'On prime generating sequences', Available at: http://www.riemannhypothesis.info/wp-content/uploads/2014/10/schepke_prime_generating_sequences.pdf

Shevelev, V. (2010), '*Three theorems on twin primes*', *arXiv.org*. Available at: https://doi.org/10.48550/arXiv.0911.5478.

Teacher's/Mentor's comments and suggestions:
Teacher's/Mentor's name, signature and date: