High School Student Institute of Mathematics and Informatics

Summer Research School
Symposium
2021

Primality Testing

Author:

Emilie Ma
University of British Columbia
kewbish@gmail.com

Scientific Advisor:

Pressiana Marinova
Occado Technology Sofia
pressiana.marinova@gmail.com

Abstract

Abstract

1 Introduction

Introduction

2 Methods

2.1 Euler's Primality Test

The results over three trials of Euler's Primality Test are shown in Table 3. Each trial tested a different k value, and consisted of:

- Generating a random set (S) of 10^3 integers such that $10^6 < x < 2 * 10^6$
- Using SageMath's `is_prime` to check for primality for each integer in S
- Running Euler's primality test with k bases tried on each integer in S
- Counting all pseudoprimes which passed Euler's but not Sage's primality test
- Repeat for three sub-trials, average results and return lowest number of bases tried (lowest k) that returned the lowest number of pseudoprimes passed

Each trial was timed with the Linux `time` command, recording the real, or total elapsed wall time, spent.

3 Results

Table 1: Raw data for Euler's Primality Test Trials

	All Random Bases		
	Trial 1	Trial 2	Trial 3
Running Time	13.086s	12.602s	13.797s
Lowest k required	2	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	1		
Range of number of pseudoprimes passed	0		
	Base 2		
	Trial 1	Trial 2	Trial 3
Running Time	14.591s	11.157s	11.129s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	0		
Range of number of pseudoprimes passed	0		
	Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	12.373s	11.691s	10.930s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	0		
Range of number of pseudoprimes passed	0		
	Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	12.429s	11.693s	12.065s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	0		
Range of number of pseudoprimes passed	0		
	Base 2 and Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	19.873s	18.805s	22.055s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	0		
Range of number of pseudoprimes passed	0		
	Base 3 and Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	19.517s	21.474s	21.526s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	0		
Range of number of pseudoprimes passed	0		
	Base 2 and Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	21.338s	19.868s	19.840s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	0		
Range of number of pseudoprimes passed	0		

4 Discussion

Discussion of results

5 Conclusion

Conclusion

References