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

Methods

2.1 Base Analysis

Each primality test was analyzed in a standard way over three trials; the raw data is available in Appendix A. Each trial tested a different k value, and consisted of:

- Generating a random set (S) of 10^4 integers such that $10^6 < x < 2 * 10^6$
- Using SageMath's `is_prime` to check for primality for each integer in S
- Running the primality test with k attempts run on each integer in S with respect to some base a
- Counting all pseudoprimes which passed the primality test 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

a was a choice of either all random bases, 2, 3, 5, and a pair of 2, 3, or 5. Each trial was timed with the Linux `time` command, recording the real, or total wall time, elapsed.

3 Results

Simplified tables and synthesized figures

The results over three trials of Fermat's Primality Test are shown in Table 1. The results over three trials of Euler's Primality Test are shown in Table 2.

4 Discussion

Discussion of results

5 Conclusion

Conclusion

References

Appendix A Raw Data for Primality Tests

A.1 Fermat's Primality Test

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

	All Random Bases		
	Trial 1	Trial 2	Trial 3
Running Time	2m45.313s	2m46.200s	2m42.205s
Lowest k required	12	74	93
Pseudoprimes passed at lowest k	0	0.33	0
Range of lowest k required	81		
Range of number of pseudoprimes passed	0.33		
	Base 2		
	Trial 1	Trial 2	Trial 3
Running Time	2m28.057s	2m29.196s	2m31.840s
Lowest k required	45	24	8
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	37		
Range of number of pseudoprimes passed	0		
	Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	2m30.574s	2m46.716s	2m27.309s
Lowest k required	13	60	16
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	44		
Range of number of pseudoprimes passed	0		
	Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	2m27.032s	2m26.897s	2m23.043s
Lowest k required	4	27	7
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	20		
Range of number of pseudoprimes passed	0		
	Base 2 and Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	4m40.323s	5m13.970s	4m51.122s
Lowest k required	19	25	13
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	12		
Range of number of pseudoprimes passed	0		
	Base 3 and Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	5m6.811s	5m1.727s	4m41.699s
Lowest k required	2	7	6
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	5		
Range of number of pseudoprimes passed	0		
	Base 2 and Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	4m47.168s	5m38.154s	5m26.986s
Lowest k required	6	11	10
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	5		
Range of number of pseudoprimes passed	0		

A.2 Euler's Primality Test

Table 2: Raw data for Euler's Primality Test Trials

	All Random Bases		
	Trial 1	Trial 2	Trial 3
Running Time	1m50.609s	2m4.602s	1m53.909s
Lowest k required	3	5	2
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	3		
Range of number of pseudoprimes passed	0		
	Base 2		
	Trial 1	Trial 2	Trial 3
Running Time	1m45.231s	1m41.760s	1m37.776s
Lowest k required	2	1	3
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	2		
Range of number of pseudoprimes passed	0		
	Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	1m52.067s	1m39.540s	1m37.529s
Lowest k required	2	2	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	1		
Range of number of pseudoprimes passed	0		
	Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	1m51.691s	1m42.775s	1m52.078s
Lowest k required	2	2	2
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	3m32.639s	3m8.813s	3m3.992s
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	3m17.024s	2m59.818s	3m5.117s
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	3m4.498s	3m14.970s	2m57.338s
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		