Comparison of SS, MR, AKS and Trial Division for Primality

Kevin van As
4076311
MSc Applied Physics

Laurent Verweijen
SID
MSc ???

ABSTRACT

MyAwesomeAbstract!

Keywords

randomized algorithms, primality, SS, MR, AKS

1. INTRODUCTION

People spend a lot of time finding the prime numbers. I don't know why...

2. THEORY

There exist several algorithms to check whether a given integer, n, is a prime number. The easiest among them all is the "trial division" (TD) algorithm, described in Sec. 2.1. It is a deterministic algorithm with a $O(\sqrt{n})$ complexity. Several different algorithms have been devised, both deterministic and random, to beat this complexity. All randomized algorithms below are based on "Femat's Theorem" for primality [1], which says that "$\forall$ prime n,

$$a^{n-1} \equiv 1 (\mathrm{mod}\, n), \tag{1}$$

$\forall a \in Z_n^*$". Sadly, there does as well exist an infinite set of composite numbers which satisfy this criterion. They are the so-called "Carmichael numbers". Each of the randomized algorithms below deals with these numbers in their own way.

2.1 Trial Division

In the trial division (TD), we start with the very definition of a prime number: it is only dividable by 1 and itself. To test this statement, we divide by every integer up to $\sqrt{n}$. If any of those divisions result in an integer, the number is not a prime. Otherwise, it must neccesarily be a prime, from the very definition. TD is a deterministic algorithm with $O(\sqrt{n})$ complexity.

2.2 Wheel-Sieve

Table 1: Execution time as a function of n. Each datapoint consists of 10,000 samples.

Range\Method	AKS	MR	SS	TD	WS
2-500	6.55E9	1.86E-2	2.20E-2	3.61E-3	1.06E-2
501-5000	-	1.94E-2	2.52E-2	4.65E-3	1.26E-2
5001-50000	-	2.11E-2	2.82E-2	6.36E-3	1.44E-2
50001-500000	-	2.19E-2	3.15E-2	1.03E-2	1.74E-2

Table 2: Error (fraction) as a function of n. Each datapoint consists of 10,000 samples. All methods have a one-sided error: they may say "prime", while it is a composite.

Range\Method	AKS	MR	SS	TD	WS
2-500	0	1.27E-2	9.52E-3	0	0
501-5000	-	2.64E-3	2.99E-3	0	0
5001-50000	-	1.11E-3	5.53E-4	0	0
50001-500000	-	1.09E-4	0	0	0

2.3 Solovay-Strassen

2.4 Miller-Rabin

Miller-Rabin (MR) is a randomized algorithm with a one-sided error; It is an RP algorithm for compositeness. If n is a prime number, it will return prime. If n is a composite, it may incorrectly say prime.

2.5 Angrawal-Kayal-Saxena

3. RESULTS

4. CONCLUSIONS

I have succesfully simulated Argon in solid, liquid and gaseous form. I have computed the pressure, and shown that the computed pressure is in agreement with Verlet's original paper, but as well that the pressure matches nature at 0 °C. Pair-correlation functions have been created, which show clear differences between the three phases. I have attempted to compute the diffusion coefficient, and I have found the right order of magnitude. At the same time, the graphs show there is still a bug present, so further attention is needed to find more accurate predictions for the diffusion coefficient. I have qualitatively looked into the phase transition from solid to liquid and theorised that the phase transition occurs when particles oscillate sufficiently much

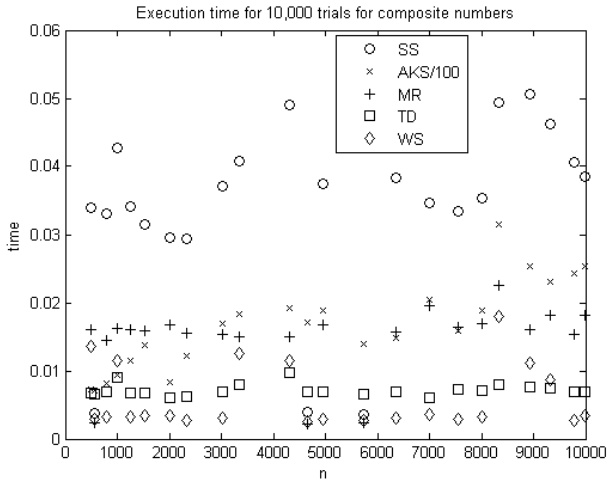

Figure 1: Execution time for small composite numbers, n. Each measurement consists of 10,000 samples.

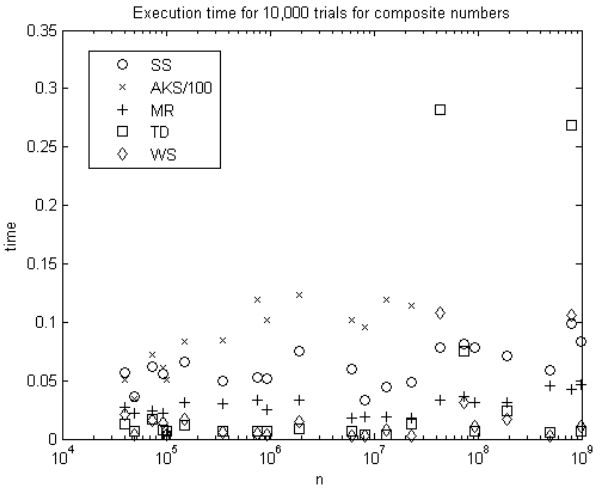

Figure 3: Execution time for a large range of composite numbers, n. Each measurement consists of 10,000 samples.

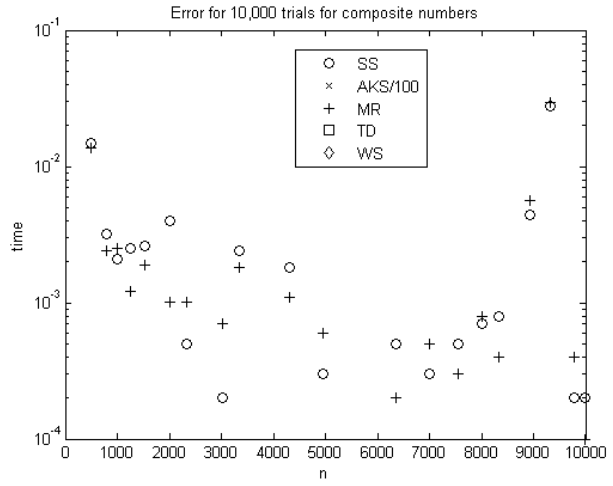

Figure 2: Error (false prime prediction) for small composite numbers, n. Each measurement consists of 10,000 samples.

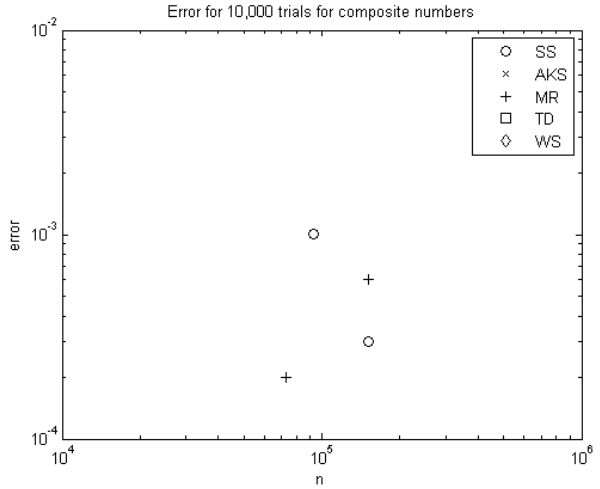

Figure 4: Error (false prime prediction) for a large range of composite numbers, n. Each measurement consists of 10,000 samples.

such that they can 'touch' each other and thus cause a snowball effect, destroying the crystal lattice. Further research is required to study this phase transition and the other 3 phase transitions in more detail.

5. REFERENCES

[1] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge University Press, 2007.