

## Re: Basically a sieve method, relation to quantum

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2005-01/6488.html>

---

**From:** Jesse F. Hughes ([jesse\\_at\\_phiwumbda.org](mailto:jesse_at_phiwumbda.org))

**Date:** 01/22/05

Date: Sat, 22 Jan 2005 18:37:49 +0100

jstevh@msn.com writes:

> *Jesse F. Hughes wrote:*

>> *jstevh@msn.com writes:*

>>

>> > *The original algorithm in my program, will, my current analysis*

> *shows,*

>> > *factor about 50% of the time, which is astounding.*

>> >

>> > *I get a sense that some of you don't get it, so let's say you take*

> *some*

>> > *RSA challenge number, and calculate  $j$  and  $T$ , and factor them, and*

> *then*

>> > *run them through the algorithm.*

>> >

>> > *My research indicates you have a 50% chance of factoring the*

> *number.*

>>

>> *Funny. A few minutes later, you said, "So, if it fails to find*

>> *factors 50% of the time, when it recurses with large numbers, it will*

>> *rapidly do worse."*

>>

>> *But here you seem to say that the 50% rate holds for RSA-size*

> *numbers.*

>>

>> *Does the success rate decrease as the size of the factors increases?*

>> *Does it decrease dramatically?*

>>

>

> *You're not paying attention or you're not very bright.*

>

> *The algorithm depends on factoring  $T$ , the surrogate.*

>

> *I need a factorization of a number that can be fairly large in and of*

> *itself.*

>

> *In fact,  $T$  is about the size of  $M^2$ .*

>

sci.math: Re: Basically a sieve method, relation to quantum

- > *My program gets T by calling itself.*
- >
- > *It is HEAVILY recursive.*
- >
- > *It calls itself to factor T, so if it factors approximately 50% of the*
- > *time, you do the math.*
- >
- > *Actually, I think now the algorithm factors at a much higher rate,*
- > *which is how the program is as successful as it is!*
- >
- > *I know, for some of you the idea of recursion is too subtle, and you*
- > *can't quite understand how a factoring program that needs a*
- > *factorization to work, can actually work by calling itself!!!*

Yeah, recursion has always been a mystery to me, I tell you what.

- > *In any event, you can do it a different way, by using some other means*
- > *to factor T, and my research indicates that it will factor at least 50%*
- > *of the time if you do that, while my heavily recursive program will*
- > *fall off in effective factoring at very dinky numbers.*
- > *Understand now?*

Not particularly.

I'd understand a bit better if you had answered the following two questions.

Does the success rate decrease as the size of the factors increases?  
Does it decrease dramatically?

Instead your answer seems to be: suppose that we know how to factor T quickly. Then we plug that magic algorithm into my algorithm and we approach 50% success. Rather strange response.

Could you just answer the questions asked? Thanks much.

Your faithful archivist,

--

Jesse F. Hughes

"Besides, discoverers are too proud to kiss butt. Indiana Jones would never kiss some academic's ass to get published, and neither will I."

--James Harris