

Surrogate factoring, theory versus implementation

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-01/1746.html>

jstevh_at_msn.com

Date: 01/23/05

Date: 23 Jan 2005 08:51:42 -0800

There are actually two discussions that can take place about my surrogate factoring theory:

The theory itself, and implementations of the theory.

Not surprisingly some posters have seized on the efficacy of my prototype program, which primarily is a proof-of-concept, which I have put out there so you can get some sense of how things are going without having to first read through the paper.

If that prototype had worked as well as I'd hoped, I wouldn't be posting about it.

I'm talking this out now on Usenet *because* I'm seeing a failures in that program that puzzle me, and having hit a wall, I'm talking the problem out.

First thing with a young theory with an implementation that doesn't behave as expected is to check the theory!!!

Maybe it's just wrong.

I've checked the theory, and it's not wrong.

Maybe I messed up in checking my own theory, so it seems reasonable that I might suppose that if there were any serious people on these groups with a modicum of interest that they might go check the theory and point out any errors in it.

I don't see that happening.

Mostly it's just a bunch of chattering.

Now I continue to work on understanding the theory, and in extending it, for instance I stepped through an important argument to try and see the probability that this method would factor.

That argument indicated that if you have $f_1 f_2 = j^2 T$, where

$$M^2 = j^2 + T$$

and M is your target to be factored and T is the surrogate factored instead in order to get that target factorization, then for some random f_1 and f_2 , that is taking one of the combinations of factors that multiply to give $j^2 T$, the probability that it will factor M is almost exactly 50%.

And there are LOTS of combinations typically for factors of $j^2 T$ by two's, so the method should work well over 90% of the time, and more like over 99% of the time, which is not what I'm seeing with my implementation, though part of it is that it's heavily recursive, in that it calls itself to factor T.

That is, the surrogate factoring method is itself being called to factor the top level surrogate, in an iterative process which goes down to a T small enough to be factored by a list of primes up to 200.

The size of T in my prototype program drops by about 1/6th with each iteration, which is what I deliberately programmed in.

So, since T is on the order of M^2 , the number of iterations for a number M of around magnitude 10, is about 26 iterations.

You can work out the probabilities for what's the likelihood of failure with 90% factoring with that many iterations.

Still I think the program is doing worse than that, and I'm working on why.

There are two discussions: theory and implementation

The theory should be the simplest area to actually attack as it's not complicated.

See <http://groups.yahoo.com/group/sufactor/>

Now the discussions can go on indefinitely as posters who reply to me usually just say something negative or mocking.

Why do they bother? Who knows. It is Usenet and some people think that responding to someone making claims they don't *believe* are true, with some reply just claiming something is not true, will work.

It's some odd problem in the human brain. I think some of these posters actually believe that by replying saying I must be wrong, they are actually affecting whether or not I'm wrong, without ever having to worry about looking over the mathematical theory or check an algorithm.

It's a weird quirk of the human brain. Some people believe that by saying something is true, they make it true.

In contrast, note I have a paper, which outlines a mathematical theory. I have an implementation in a program that tries to step through that theory, and it does often factor.

It's in its failures that my primary interest lies.

Right now I'm not most interested in the successes here, but in the failures.

If you are a highly intelligent person with a great deal of competence in this area then you will find that I will not react badly to a cogent reply.

You may also find that you will be verbally abused if you just make a cogent reply without joining in the gang behavior of simply trying to *claim* I'm wrong.

In my experience that is a serious fear for most of you. You do not wish to look stupid, in such a public arena, and you do not want to anger the posters who make it a point of going after people who don't follow a certain line.

Ok, that's your choice. But make no mistake, this research could very well impact your life, and sooner, not later.

If down the road your simple social fears meant that you did not make yourself part of the process and maybe help produce a better outcome, then remember that, as your own failure.

But still, often the best beginnings are with failures, if you can learn from them.

James Harris