

# Re: JSH: SF Algorithm

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-09/msg02127.html>

---

- *From:* "T.H. Ray" <[thray123@xxxxxxx](mailto:thray123@xxxxxxx)>
  - *Date:* Tue, 11 Sep 2007 08:17:37 EDT
- 

Oh well, enough bravado on my part as I'm not certain this will work and waiting for Wednesday just seems silly. The Bulletin of the AMS did reject. Why would they change their minds between now and then?

The expert opinion is noted. Here is what my research says, which presumably then will not work, but I do not know why it would not.

As I (among others, I expect) have repeatedly told you, if you would learn how to write a proof, you WOULD know why it does not work. The first use of a proof is to self-inform.

Tom

Given a target composite  $T$ , from theory using  $x^2 = y^2 \pmod T$  and  $k = 2x \pmod T$ , it can be proven that

$$(x+k)^2 = y^2 + 2k^2 \pmod T$$

must be true for any solution of a difference of squares.

Explicitly to solve you need solutions for

$$(x+k)^2 = y^2 + 2k^2 + nT.$$

The algorithm picks  $x$  directly, choosing  $x = \text{floor}(\text{sqrt}(T))$ , so  $k = 2x$ , and then ranges for the  $n$ 's from

$$n_{\text{max}} = \text{floor}(((x+k)^2 - 2k^2)/T)$$

and

$$n_{\min} = \text{floor}((4(x+k-1) - 2k^2)/T)$$

which with my program has meant roughly 32 surrogates to factor.

By the theory, if you can fully factor all 32 surrogates for any target T, then you will non-trivially factor T.

If you cannot factor all 32 with the given x, you can increment it by 1 and try again, indefinitely.

Note that you can also use  $x = \text{floor}(\text{sqrt}(2T))$  to have about 64 surrogates and much greater odds but I'm not clear how that works exactly and besides if you can factor 32 with the first one then you have the target in hand.

It is so weirdly simple and I think the theory is correct, but I guess I could be wrong.

I have tried to implement with my own programs but as I pointed out in a previous post, I use recursion and with big numbers fewer and fewer of the surrogates get factored, so it craps out.

I am not confident that I can work that problem out so what I said earlier was bravado on my part.

James Harris