

JSH: Difference of squares

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-03/7560.html>

jstevh_at_msn.com

Date: 03/22/05

Date: 21 Mar 2005 17:44:14 -0800

I think that maybe many of you don't know the significance of my surrogate factoring methods so easily giving you a difference of squares with some target M to be factored, so I'll explain again how factoring is typically done.

Consider

$$x(x+a) = M$$

where M is your target, as then you can use the quadratic formula to solve for x, and get

$$x = (-a \pm \sqrt{a^2 - 4M})/2$$

and most of the work in factoring has to do with figuring out some a, such that the square root is an integer, and you factor M.

Now with surrogate factoring though, you get

$$\sqrt{(Az + 2M^2)^2 + 4M^2T}$$

where you have M lined up for a difference of squares, and you just have Az as the variable, where you get a LOT of solutions for Az just by factoring T and some other number I call j, which is what has been done before.

Here, though, importantly, you have rationals, which makes it harder upfront, but still doesn't explain preferential factoring of M, such that you only get trivial factors.

The weird thing you see, is that the previous methods I tried worked so badly.

Clearly **something** was blocking the factorization of M into non-trivial factors.

If you know anything about factoring, seeing how easily I can get a difference of squares should scare you more than just a little bit, as

it means that even if I'm wrong now, that finding a way to get this to work might just be some little thing, as you have the difference of square—easily.

You see, the other factoring methods, like even the Number Field Sieve, basically work to get you to a difference of squares.

Surrogate factoring hands it to you from the start.

SOMETHING must have been blocking that difference of squares from factoring M with my earlier work, and if that is handled, then that's it.

My own perspective is that you people are NUTS, as if someone figures this out, then who knows what will happen?

But your confidence in the face of such basic mathematics—in believing it must be wrong I guess because I talk about it—is foolhardy at best.

James Harris