

# JSH: Let's recap

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-09/msg03067.html>

---

- *From:* "Amebias" <[spamless@xxxxxxxxxxxxx](mailto:spamless@xxxxxxxxxxxxx)>
  - *Date:* Fri, 14 Sep 2007 21:22:44 -0500
- 

I will sacrifice your actual lives against the needs of the future, against the children yet to be born.

As far as I'm concerned if you make the wrong choice, you simply killed yourselves.

I'm the "crackpot" with yet another idea claiming it's important.

And I have no choice but to sacrifice the few against the needs of the many.

They sure don't trust me.

Now it is clear that what I call surrogate factoring IS a new way to factor and is as fundamental in mathematics as methods related to congruence of squares, and there is no way to show it is just trivial, meaning that like methods before it, there is the possibility of a growing body of research that continually improves it.

Surrogate factoring preferentially yanks out small prime factors. And it doesn't seem to care much how big the number is when it does that yanking.

The mathematics is very fundamental as I've only added  $k = 2x \pmod T$ , to  $x^2 = y^2 \pmod T$ , so you have a basis in very rudimentary equations, and now after a year I am certain that it cannot be shown to be trivial.

So it's about time, effort and the natural maturation of an idea.

Previous factoring methods took hundreds of years to reach maturity, but that was without modern computing technology, modern mathematical technique, modern problem solving technique, and trillions of dollars flowing behind an encryption standard that could be made obsolete motivating highly intelligent people to work very hard.

Past history with my prior research indicates that modern mathematicians have taken an absolute position of holding against my research in denial—no matter what.

Even the destruction of a modern electronic mathematical journal had little if any impact, as you can see by searching on "SWJPAM".

Like with my first attempts at factoring algorithms back about 5 years ago, I was just working on extensions of ideas used by Fermat.

Later I had the concept of surrogate factoring as an idea from a question: could you factor one number using another?

And method after method after method failed as I'd figure out or others would figure out that it was something trivial where the underlying relations were often about random or some kind of sieving that would not be earth-shattering in terms of impact on the problem.

So the first year of the life of the latest surrogate factoring research where after over 3 years of searching I realized I only needed to add one variable  $k$ , where  $k = 2x \pmod{T}$ , where  $T$  is the target to factor, was really about finding some way to trivialize the research.

And it survived that year plus.

But factoring research has the potential of breaking them like people before who have often been broken by taking absolute positions against more powerful forces. Consider Chinese in the Boxer Rebellion who thought that painting themselves "magically" could stop bullets.

And in this case, breaking the absolutism of the mathematical community is unlikely to happen without changing the economic landscape of the entire world.

Whether you realize it or not the preamble with any factoring research that I do is looking for some way to show it's trivial.

There is no way that I can see that mathematicians ignoring this research and waiting until it matures is helpful for my own country, currently the dominant world power.

But it is the decision of the modern mathematical and cryptography community that holds sway here as the world trust you.

They trust you, so that is how you have the power to decide the fate of the world.

If you all say it's not, and you're wrong, then the maturation process of surrogate factoring can happen mostly in the dark, and the world instead of facing a relatively new idea that has a distance to go in order to be as powerful as it can be, can instead face a fully matured factoring method—known because it is unleashed.

## JSH: Let's recap

The issue here is ignorance in the now, and full realization later.

Or an end to the absolute position taken by the world's mathematical community against my research now, versus later.

Fight me on this and you can wake up in a few years to a totally changed world order where you helped create it, dashing the now dominant countries to the ground on their fateful and naive trust in your honesty about your discipline.

History shows that in these situations, your choice is usually against your own best interest, which is why history is so interesting, as empires fall not just on the decisions of the world leaders, but on the seemingly minor ones of people at the fulcrum point.

And this time, in this history to be, the lever is surrogate factoring, and I assure you that with years of research under my belt I now even more firmly believe that it can move the world.

The challenge to me is to balance the needs of the many against the wants of the few.

As I consider the livelihoods of mathematicians around the world, and the savings of people around the world, including in my own country, against the survival of the human race depending on ever forward progress in our knowledge, science and technology.

Except I somewhat accidentally discovered how rapidly it can be improved while typing in some numbers when I watched it factor a 100+ bit number, so already it is far beyond methods based on congruence of squares at this point in its life, and has behavior more like Dixon's.

James Harris

.