

Re: JSH: Contradictory behavior, issue of math fraud

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-09/msg00485.html>

- *From:* marcus_b <marcus_bruckner@xxxxxxxxxx>
 - *Date:* Mon, 03 Sep 2007 12:18:38 -0700
-

On Sep 2, 12:19 pm, JSH <jst...@xxxxxxxxxx> wrote:

On Sep 1, 11:27 pm, junoexpress <MTBrenne...@xxxxxxxxxx> wrote:

I believe the burden of proof is on you.

Not necessarily if you believe that a concept can be of interest in and of itself to people who are supposedly experts in a field.

Stupid.

Nobody will be even the slightest bit interested in it until you give some indication (I'm not even saying proof, which I know you can't do) that it's performance is in **some way** optimal.

Why should they waste their time on your half-baked ideas when they're trained in the field and know they have ideas that are at least worth working on.

But if the idea turns out to be a brilliant one which means factoring is not a hard problem after all, then how can mathematicians who not only couldn't figure it out, but who ignored it when presented with it be considered to be true experts in the field?

A hypothetical. Hypotheticals are cheap.

What if **THEY** are the ones deluding themselves and doing research that is valueless because they actually lack real mathematical ability?

Re: JSH: Contradictory behavior, issue of math fraud

So they are incapable of seeing important research as well?

More hypotheticals. You are counting chickens before they are hatched, in fact before there is any reason to think they will ever hatch.

You might as well say: "What if pigs are actually able to fly, and zoologists have overlooked this possibility for centuries?" Should zoologists really spend a lot of time worrying about this?

Challenging Santos to commit every dime is part of that action, as to con artists, what really is more important than money?

I don't know, you tell us. You've been perpetuating a con job on sci.math as long as I can remember, always promising something and never having delivered on one promise. If that's not a con-job, I don't know what is. What's even worse is that a lot of it you've done dishonestly, using others to work out things you can't do, all the while boasting how much smarter you are than the rest of humanity.

Except I HAVE delivered. Instead of just arguing with people over my proof of Fermat's Last Theorem I wrote a paper over a key results that followed from it and got it published.

The publication was a careless error on the part of an incompetent editor. You knew before the paper was submitted that there were fatal objections. You delivered, all right. You delivered crap. And you got what you deserved, and more, in return.

Posters on sci.math then declared that the journal system was flawed and that math journals routinely publish false papers!!!

Oh, no. No one has said math journals routinely publish false papers. There is no evidence for this in general. That particular journal had a poor track record, having previously published at least one very questionable paper.

Re: JSH: Contradictory behavior, issue of math fraud

Re: JSH: Contradictory behavior, issue of math fraud

The papers in it were often poorly edited, and a surprising fraction of them were by the editor himself.

Others mounted an email campaign against the paper and convinced the journal editors it was false, so they yanked it, and later the journal shut down.

The paper was wrong to its very core and wrong in details. It is NORMAL BEHAVIOR to write to the editor when an incorrect paper is published. The editor lied to you regarding peer review. The editor acted AGAINST explicit advice from letter-writers here and yanked your paper with no explanation. It is plausible that the editor was pressured to discontinue the journal because of his incompetence and dishonesty. His handling of your worthless paper was contributing evidence.

With my prime counting research I first found my prime counting function, and then proved how it was different from anything else previously known as to this day no one can give any other partial difference equation used to count prime numbers, and no other known that finds primes on its own.

Your algorithm is a minor variant of Legendre's method. Your algorithm (not 'your function') is not competitive with current methods in speed for counting primes. Neither you nor anyone else have indicated why your 'partial difference equation' is useful or important.

Posters on sci.math when challenged with those points shift the definition of "difference equation" to a non-standard one, and ignore the second point about finding primes or just lie about it.

Repeatedly, by all normal standards, I achieve and posters deny in unreasonable ways all achievements while making dubious achievements of their own--like killing a math journal.

REASONABLE people who listen to me talk about the factoring problem can note that I'm making sense,

No, liar. REASONABLE people here have repeatedly tried to

Re: JSH: Contradictory behavior, issue of math fraud

implement your many variants of surrogate factoring. None are remotely close to competitive with existing methods for factoring integers. Further, you have not provided any rationale for why factors of a surrogate might be connected algebraically or probabilistically to nontrivial factors of the original target. It looks like your rationale is the following: "I have this vague hunch that factoring an integer S which is a function of the target T might have a high probability of producing nontrivial factors of T . The reason this might work is, I am a genius and ideas generated by geniuses often turn out to be right. No one can prove that my vague hunch is wrong, so I am being unfairly ignored by the evil hacks who call themselves mathematicians."

Somewhat logical, except for the main premise – the part about being a genius. That part has been contradicted hundreds of times by your performances here. Put bluntly, given the many howlers you have produced, you are orders of magnitude too dumb to be a genius. You are even too dumb to understand why no one here thinks you are a genius.

Gauss, Newton, Euler, Riemann, and Galois were geniuses. Arguably also Dirichlet, Dedekind, Kummer, Kronecker, Hilbert, and Wiles. Imagine these guys sitting around a table in a restaurant discussing their work. I.e., if they were your kind of genius –

Gauss: I am the greatest genius of all time. I proved the Fundamental Theorem of Algebra. The financial crash of 1803 was caused directly by my proof.

Riemann: Fuck off, Gauss. You are a hack. I have an idea for a proof of the Riemann Hypothesis. It is called Surrogate Theorem Proving. First I prove another theorem. Then I maybe can show that when you subtract one from all the arguments in that theorem, you have a better than 50% chance of having a proof of the Riemann Hypothesis, which I wrote and named after me. I want credit for what I didn't do yet. I am decidedly a major, major genius.

Gauss: Um, when cell phones are invented their secret encryption codes will be cracked by the use of my theory of quadratic residues.

Hilbert: Bah, humbug. I have a trivial proof of Fermat's Last Theorem that took me 10 years to write down. It was yanked out of Crelle's Journal, and then the journal crashed and burned. Crelle himself sent me a copy of the referee's report. It said:

Re: JSH: Contradictory behavior, issue of math fraud

"Add one tsp. of finely minced garlic to the melted butter. Stir gently over a low flame until brown. Stir in the grated carrots, chives and celery. Simmer for 12 minutes while stirring, then pour over the asparagus. Serves 5."

This proves my work was peer-reviewed, therefore perfect. A proof cannot be incorrect. Plus I am a super genius. All I have to do is say I have a proof, and presto, it is correct.

Gauss: You fools. Your disciples are trying to obtain my precious bodily fluids. I deny them my essence. I am a super-duper genius.

Dirichlet: LOL. I have this new idea for factoring. Every integer can be factored as the product of two rationals, right? That means infinitely many possible factors, rather than a paltry finite number as are used by existing methods. Think how much better it is to have infinitely many choices rather than just a few trillion. This is HUGE. This is BEYOND HUGE. It's JUMBO-GIGANTIC. It's BIGGETY-BIG!!! Why am I not being given credit? I am one hell of a genius.

Hilbert: You are my lapdogs, all of you. Cantor in particular is a mongrel. I am notifying the Attorney General of Prussia that he is trying to suppress my work, causing the stock market crash of 1929, 30 years from now. I am an EXTREME genius.

Riemann: ROTFLMAO. Um, I took a coach down to Paris last summer to visit Cauchy at my old alma mater where I earned my B.S. in B.S. I showed him my ideas regarding my astrological research on factoring polynomials. He didn't say I was wrong. Later I wrote him a nasty note, calling him a lapdog ('un chien du lap'). Um, he has not replied. Typical.

Galois: I tell you. He never writes. He never calls.

Kronecker: Since when is your alma mater in Paris?

Kummer: Anybody got change for a five? I need some Starbucks'.

Dedekind: Well, I am an IDEAL genius.

Wiles: This Harris guy is wiggling me out. I am putting in a call to NSA. He needs a one-way ticket to Guantanamo.

Cantor: Yup. He's dangerous. He factored a 7-digit number recently. I forget which one. That Hammer of his has me seriously worried.

Re: JSH: Contradictory behavior, issue of math fraud

Fermat: He proved my last theorem, using his famous lemma that if $f(0)$ equals 0, then $f(x)$ is divisible by 7 for all x .

while posters arguing with me, can't even be bothered to present a mathematical argument against my research or in support of their claims.

No, liar. First, the burden of proof is on you to provide reasons your method might be expected to work. You have given no such reasons. Second, people here have tried all your latest-greatest methods as you announce them and found them uniformly worse than existing methods. Third, on many occasions, posters here have pointed out explicit errors in your theory. Perhaps you remember the many times you stated that your method had a probability of 50% or greater of producing nontrivial factors. This was based on your brainless idea that if $T = p * q$ (p, q both prime), and you find factors f and g of T , there is a 50% chance that f and g are equal to p and q or vice versa, since the only ways to factor T are $1 * T$, $T * 1$, $p * q$, and $q * p$. Did you ever manage to understand what was wrong with that?

I challenge you as well to pledge every penny you own to anyone worldwide who loses money if surrogate factoring turns out to be what your community is saying it is not.

SURE, PUT ME DOWN FOR EVERY PENNY, YOU MORON.

M

You are not really anonymous and your statement is noted.

At least you have the courage of your convictions.

If the math community is wrong here, I say that its members should be held accountable as experts in the field, whether they demonstrate they actually are or not, as they've created an impossible situation,

Re: JSH: Contradictory behavior, issue of math fraud

where at this point it's hard to see how there is a way to present this information without a potential shock.

So, liar, you are saying you have a way to present such information? You can demonstrate that your method works? And all that's holding you back is your fear that people might be shocked???

A collapse of confidence in the modern math community seems ever more likely. It puzzles me but I have an explanation as old as humanity—greed.

No, liar. There is a simpler explanation. Your idea has no *intelligence* behind it. It's just a Harrisian hunch. There is no reason to pay attention to it. The burden of proof is on you, not on your critics.

Compare surrogate factoring to Dixon's idea. Like you, Dixon wants to find X and Y such that

$$X^2 = Y^2 \pmod T.$$

So here is his core idea. He starts with a 'factor base' of small primes. He finds a collection of Z's such that for each Z,

$$Z^2 \pmod T$$

is a product of primes in the factor base. The exponents of the primes in the product in general are not all even. But if the collection of Z's is large enough, some product X of a subset of the Z's will be such that $X^2 \pmod T$ has all even exponents, i.e., $X^2 \pmod T$ is a square, say, Y^2 . Then

$$X^2 = Y^2 \pmod T, \text{ i.e.,}$$

$$(X + Y)(X - Y) = m \cdot T$$

for some m. There is a good chance that

$$\gcd(X + Y, T) \text{ or } \gcd(X - Y, T)$$

is a nontrivial factor of T.

See, there is an actual rational explanation for why Dixon's

Re: JSH: Contradictory behavior, issue of math fraud

method may work. It is related to Fermat's method, but it is more efficient than just guessing as Fermat's method requires.

Now, here is how your idea is supposed to work.

Let T = the target to be factored.

Let $S = 2k^2 + nT$,

where n and k are to be chosen.

S is the surrogate to be factored. Say $S = F1 * F2$.

Then let $X = (F1 + F2 - 2k)/2$ and $Y = (F1 - F2)/2$.

Then $X + Y = F1 - 1$ and $X - Y = F2 - 1$.

Your hope is that $\gcd(F1 - 1, T)$ or $\gcd(F2 - 1, T)$ are nontrivial factors of T .

So what is a key difference between this and Dixon's method?

It's this. When Dixon obtains X and Y as described above, it is certain that $X^2 = Y^2 \pmod T$. But the same is not true for your values of X and Y . Unlike Dixon, you do NOT automatically obtain

$X^2 = Y^2 \pmod T$.

Your X and Y don't have a special relationship to T . That is really the missing ingredient. If you could fix that, you might have something. As it is, you have barked up the wrong tree for most of the last year, or longer.

By faking math that is "pure" in that it is useless and hard to check, some people could get money for nothing, but lacking real math ability they could fight against actual mathematical proof and lead the world down a path to financial ruin.

No, liar. People like Pollard and Pomerance and Dixon and others, pure mathematicians, have made significant nontrivial headway with the factoring problem. Their subtle theoretical arguments and algorithms show REAL math ability. Ideas, not hunches, are what counts. The evidence is there in the form of factoring of very large RSA numbers. Mathematicians are now working on the theory of quantum computing – perhaps secretly funded by the NSA – if it works, RSA encryption may

Re: JSH: Contradictory behavior, issue of math fraud

be obsolete. All these efforts involve theory and rationale.

You by contrast, are the one who is 'lacking real math ability.' Your SF is an unmotivated hunch, a wisp of wishful thinking. You don't have proof and you don't have numerical evidence and worst of all, you don't have a rationale. You seem to think that being a genius means you don't have to have a rationale. So you just keep whining that no one is giving you credit.

For what?

The main question regarding your concept of surrogate factoring is, Where's the beef? You keep claiming you have the beef, but you don't have it. Now here you are whining that no one is giving you credit for having the beef. You want credit for saying you MIGHT have the beef. Guess what. That's not how the math world, or any world for that matter, operates.

The balance is the future of human knowledge against the wealth of those who trusted people who don't know what they were doing.

You keep dwelling on these grandiose delusions, fantasizing puffed-up galactic importance to something you have not yet accomplished. It does you no good. You just don't have the beef. The coin of the realm is rigorous proof and ideas and numerical evidence, not hyperinflated self-promoting fantasies. Why is this hard for you to understand?

I vote for knowledge and the continued Progress of the human species.

How noble. How trite and fatuous and patronizing. How unearned.

Marcus.

James Harris

.