

Re: SF: Areas of confusion, infinity

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/0916.html>

From: Proginoskes (*proginoskes_at_email.msn.com*)

Date: 04/15/05

Date: 14 Apr 2005 19:22:57 -0700

jst...@msn.com wrote:

- > *One of the problems with surrogate factoring in terms*
- > *of understanding it, is that it utilizes infinite sets,*
- > *notably the set of rationals.*

And you, James Harris, are unqualified for talking about infinite sets. You claimed in an earlier thread that you knew "set theory and Cantor" much more than I did, yet in the same post you called a certain integer "countable". This shows you don't even know how to use the terminology.

You throw out a statistic of 50% success of the "SF Theorem". Where did this number come from? Well, you define two sets S and T of rational numbers, one where the SF "Method" succeeds, and one where it fails. However, you fail to notice that these two sets of rational numbers may have different probabilities, and you did even worse, because there are OTHER sets of rational numbers; i.e., there are rational numbers which aren't elements of S or T.

Perhaps a better view of why your "analysis" is wrong is the following: Let A be the set of integers evenly divisible by 100, and B the rest of the integers. In both cases, A and B are infinite sets, but if you choose an integer N at random, uniformly (i.e., the probability of choosing any integer is the same as the probability of any other number), you'll find that the probability that N is in A is 1/100, but the probability that it's in B is 99/100. This is because the remainder of N divided by 100 is as equally likely to be m as n, where m and n are any integers between 0 and 99.

If you are going to object to this, I suggest that you sit down with a book on number theory, especially one covering p-adic arithmetic.

- > *The naive view is that since in the set of rationals every number*
- > *except 0 is a factor of every other number*

The "naive" view here is correct. In the ring of rational numbers, every nonzero rational number IS a factor of every other nonzero rational number. Period. The statement is trivial; i.e., there's nothing that needs to be proved.

In the ring of integers, not every integer is a factor of every other integer. That's what make the factoring problem interesting, i.e., not trivial. So when the world, except for you, talk about factoring numbers, it's always about factoring into integers.

> *that you can't use it in factoring,*

I've devoted a lot of time to this. My final opinion, after doing real research, is that it probably cannot be used.

> *which may be why I discovered the surrogate factoring*
> *theorem, while others did not,*

There are other possible reasons why other people haven't discovered it. First of all, you are making some assumptions that you don't state in the theorem, namely that the quadratic equation

$$y z^2 - A z + j^2 = 0$$

is true. A theorem has to be self-contained, so you have to state any assumptions that you're making, or construct them from basic principles during the proof.

You remember assumptions, right? You claimed to have a physics background, which means that whenever you run an experiment (remember those? Where you test the theory that someone is claims is true? What kind of physics person doesn't do experiments?), you always have to state the assumptions you're making in your calculation. You also have to include the apparatus, the goal of the experiment, how you're using the equipment, and how you're processing the date, and whether the final statistics support your hypothesis.

Every physics person should know this; it's called the Scientific Method, and it has been used by physicists to determine whether Nature behaves the ways that Man's equations behave.

The mathematics world has a similar thing, called simulation. But you seem to be ignoring it, as well as the rigor of proof.

> *as it necessarily has to use rationals*
> *because of equations like*
>
> $yz^2 - Az + j^2 = 0$

And you STILL haven't explained where it came from! Did it fall out of the sky, like manna?

> *and I say the naive view as I've already proven that is*
> *is naive with the surrogate factoring theorem.*
>
> *How?*

- >
- > *Well, the surrogate factoring theorem links rational*
- > *factorizations, but in so doing, it shows no inclination*
- > *for trivial versus non-trivial factorizations.*

And this is why it's useless. If you were able to say exactly WHEN you can find a non-trivial factor of M, then you would have a real theorem. You would then have the key I've been talking about, in that if you have a theorem that actually gives conditions under which b_2 is an integer (or a non-trivial rational), THEN you would have something that would shut up everyone of the liars^H^H^H^H^H disagrees at sci.math.

- > *It simply doesn't indicate a preference either way.*

Neither does my version of the SF Theorem (which takes a factor f_1 of T and assigns b_2 the value of f_1 , thus finding a rational factor of M), which is why both are useless. But at least I didn't waste time trying to show that the algebra is correct. (Your "proof" is nothing more than symbolic manipulation, which is regarded as almost trivial by the mathematics community; this is the main reason why your SF Theorem should (will?) never make it into a journal. All that you show is, in essence, that if $x = 2 \ln(y)$, then $y = e^{(x/2)}$; you are just rewriting the equations in terms of other variables.)

- > *So you can pick rational factors as you see fit, and*
- > *you'll get rational factors in exchange, where there's*
- > *no reason I've yet seen or heard for the math to be*
- > *choosy.*

Which is the very downfall for SF: It doesn't matter; you may just as well choose an integer between 1 and M at random.

- > *That means that I can use rationals and rely on human*
- > *choice: a person will pick factors.*

Then you don't have a real algorithm then. (This is also a sneaky way to TRY TO get out of writing a program and seeing that your method fails as badly as choosing random integers.)

- > *The mathematics then gives you factors in exchange.*
- >
- > *Now here's where it's not really tricky, but I've seen*
- > *posters working to try and force the issue that the*
- > *mathematics IS picky, and they rely on pseudo-mathematics.*
- >
- > *If you in picking factors choose to pick trivial and*
- > *non-trivial factors, why, in response to your choices,*
- > *should the theorem only provide trivial factors?*
- >
- > *There's no mathematical reason why.*

And the fact that there's no mathematical reason means that SF is useless.

It's like programming a computer to guess the number of jelly beans in a jar, where the computer just spits out random RATIONAL numbers. A person will be able to see that the answer must be an integer, but the machine doesn't, which makes the computer's algorithm useless.

- > *But posters confuse on this issue by pointing out*
- > *that in the set of rationals every rational except*
- > *0 is a factor of every other rational, so they argue*
- > *that in exchange for your trivial and non-trivial*
- > *factors you will get trivial factors*

-- That should read "you CAN get trivial factors" --

- > *because if you randomly pick a rational from the set*
- > *of rationals it will tend to have a numerator coprime*
- > *to any integer you might want to factor.*
- >
- > *Basically, they argue as if there isn't a link.*
- >
- > *However, the surrogate factoring theorem is not playing*
- > *social games. It's a mathematical theorem which allows*
- > *you to choose factors and in exchange you get factors.*

But the SF Theorem IS playing games! There's no guarantee that you'll get a non-trivial factor, so the factors you get in exchange may be worthless. This is like putting money into a vending machine and getting back dirt.

At least with my "SF Theorem", you get money back when you put money in.

And once again, this is the very point which makes the "SF Theorem" NOT a theorem; it does not GUARANTEE a non-trivial factor, which means that it isn't saying anything at all about the factoring problem.

- > *For the theorem to pick trivial factors only in exchange*
- > *would be a choice.*

But maybe not a "conscious" choice; maybe the choice depends on whether the Twin Prime Conjecture is true, for instance. OTOH, it is possible to use SF, where it intentionally gives you bad factors.

- > *In mathematics there has to be a reason for a theorem to*
- > *make a choice.*

Technically, theorems don't make choices, algorithms do. And the choices that algorithms make are based on formulas, not what "feels right."

- > *Posters don't give any reason.*
- >
- > *Some of you rely on others to try and learn mathematics.*
- > *I've seen posts where people reply at how happy they are*
- > *to be learning this or from posters replying to me, when*
- > *the sad reality is that posters here who know mathematics*
- > *are usually replying to me to confuse a particular issue.*

But you're already confused, because you DON'T know what's going on at an elementary level: countability, probability using infinite sets, algorithms, how to write proofs, etc. It's like you can't speak English but you claim you've written the Great American Novel in it.

The responses are from people who show specific examples, explicitly showing what's going on. So your only choice is to refuse to accept basic arithmetic, like $2 + 2 = 4$, or $0 + x = x$, because that's what the responses are based on.

- > *So they're teaching you bogus stuff.*

People can always check what these posters are saying by working out the examples on their own. It is easy to find out what's true and what's false in arithmetic.

- > *Ok, so naturally, you may tell yourself, I'd say that*
- > *posters are teaching your wrong information, when you*
- > *may feel confident that I'm the person who is wrong.*

If a poster reading this for the first time looks at your statement, they may decide that perhaps posters are not telling the truth, but they should also wonder whether YOU'RE telling the truth.

A statement like that is a double-edged sword.

- > *But, notice, the surrogate factoring theorem simply links factors.*

Yes. But not in a way that links certain decidable factors of T to desired (integer) factors of M , and that's its shortcoming.

- > *You have factors of $j^2 T$, where j is some number you choose, and T*
- is*
- > *given by*
- >
- > $T = M^2 - j^2$
- >
- > *where M is presumably the number you're trying to factor.*
- >
- > *If you get factors of $j^2 T$, then using the theorem you*
- > *get factors of*

That's a big if. Sure, $T = (M + j)(M - j)$, but you still have to factor $M + j$ and $M - j$, but in addition, you also need to factor j .

If you choose j so that its bigger than M , then you end up needing to factor two integers which are bigger than M (namely $M + j$ and j), and factor one number which may be bigger than M in absolute value ($M - j$). It looks like the "recursion" is going in the wrong direction!

Sure, you could choose j so that $M + j = 2^n$, where n is a positive integer (with, say, $n = \text{floor}(\log_2(M))$), so you have its factorization, but you still have to factor j and $M - j$.

Perhaps if you choose j so that $M + j = p^n$, where p is a (positive) prime less than 100, $n = \text{floor}(\log_p(M))$, you may make $M - j$ small (choose the p which makes $M - j$ the smallest), but you still have j to deal with.

There are three things which could make your life harder (factoring bigger numbers), and it only looks like two of them can be controlled at any given moment!

- > $M^2 T$
- >
- > *and if you are doing the factoring of $j^2 T$, you can use*
- > *trivial and non-trivial factors, right?*

Yes, but which ones are the RIGHT ones? That's what a real (i.e., non-trivial and usable) SF Theorem would say.

- > *For those confused on trivial versus non-trivial, consider*
- > *15.*
- >
- > *15 is a factor of 15, since $15(1) = 15$, but it's a trivial,*
- > *as in easy,*

"Easy" isn't the right word here; "easy" means it doesn't require too much work. "Trivial" is the best word here, since 1 is, BY DEFINITION, a factor of any integer N .

DEFINITION: An integer m is a factor of n if n/m is an integer.

PROPOSITION: 1 is a factor of every integer N .

Proof: $N/1 = N$, which is an integer; the definition says then that m is a factor of n .

- > *factor, as it doesn't take any work for people*
- > *to figure that out.*
- >
- > *However 3 is a non-trivial factor, as $3(5) = 15$, and you*
- > *need to know a little more to realize that it's a factor.*

- >
- > *Human beings distinguish between hard and easy factors.*

Wait, where did the word "hard" come in? The right thing for you to say here is:

] Human beings distinguish between non-trivial and trivial
] factors.

- > *Now, if the surrogate factoring theorem, like human beings,*
- > *distinguishes between hard and trivial factors then it*
- > *must have a reason, as mathematics is that way.*

Yes. If the SF Theorem is to be valuable, there has to be a VERY GOOD REASON why it is. That reason is in the proof.

- > *There is a reason for everything in mathematics.*
- >
- > *If you choose trivial and non-trivial factors to use*
- > *with the theorem, why should it link your factor to*
- > *only or mostly trivial factors?*

Because you can generate the trivial factors of your target T easily. Then the theorem would tell you what (non-trivial) factors of M match up with those.

In short, (1) finding trivial factors of T is easy; (2) if you have a way to match up the trivial factors of T with the non-trivial factors of M, then (3) you have an easy way to find the non-trivial factors of M. (i.e., Use the theorem.) And then you have SOLVED the factorization problem!

What you're suggesting is (1) finding trivial factors of T is easy; (2) a SF Theorem "should" match trivial factors of T with trivial factors of M, so (3) you have an easy way to find the non-trivial factors of M. (i.e., Use the theorem.) And then you have DONE NOTHING!

You're actually arguing against doing ANYTHING useful.

- > *If it does there has to be a mathematical reason.*
- > *Understand?*

Yes. And THAT REASON is the reason why finding non-trivial integer factors is hard (i.e., cannot be done in poly-time). Understand?

- > *However, if it does not, then guess what?*
- >
- > *If it does not then it means that people could develop*
- > *ideas from that theorem and build algorithms that could*
- > *factor very efficiently, and very quickly.*

As opposed to not being able to build an algorithm at all.

- > *If they do so, then while we're arguing out these points*
- > *on Usenet, there may be some people who are factoring*
- > *rather large numbers.*
- >
- > *All it takes is for them to be less gullible than those*
- > *of you who listen to people who lie to you about basic*
- > *mathematics.*

Or people who read your posts and believe them.

- > *Remember the link aspect of the surrogate factoring*
- > *theorem,*

Of course I remember it; it's the only reason for having a SF Theorem.

- > *and ask yourself, why should the theorem give only*
- > *trivial factors in exchange*
- > *for trivial and non-trivial factors?*

Because then it's possible to use those ideas. The SF Theorem has no usable ideas.

The only "algorithm" you can get from it is the following:

Given M:

- (1) Look at all possible values of j , k_1 , and f_1 (since you haven't ever said which values are the "right" ones), calculate b_1 , and see whether it's a non-trivial factor of M.

This "algorithm" takes an infinite amount of time, and thus, strictly speaking, is not an algorithm. (There are, as you know, an infinite number of rational numbers.) An undergraduate can write the following algorithm:

Given M:

- (1) Look at all integers j between 2 and $M - 1$, and see whether they're a factor of M. [We don't have to worry about non-trivial factors here; 1 and M are excluded.]

This IS an algorithm; for any value of M, it will stop, after $M - 2$ values of j .

Which one is more efficient?

On the other hand, if you had a real SF Theorem, you could do the following:

Given M:

- (1) Calculate the optimal j , k_1 , f_1 , using M and the theorem.

(2) Calculate the value of b_1 from these values. THE THEOREM WOULD THEN GUARANTEE THAT THIS IS A NON-TRIVIAL FACTOR OF M .

This is also an algorithm; it will stop after ONE value of j .

Instead of one "optimal" j , k_1 , f_1 , the theorem provides a list of, say $\ln(M)$ "optimal" values for these variables; the running time is $\ln(M)$, which is polynomial time for this problem.

This list of "optimal values" is the key I've been talking about, which I don't think exists.

- > *I've been looking at that question as I want to know*
- > *the actual answer, but posters are working to convince*
- > *others for whatever reasons motivate these people, so*
- > *they basically just say it will only give trivial factors*
- > *for really big numbers, with only two very large prime*
- > *factors.*

If you're so upset about what other people think, why do you even post?

If you're "only brainstorming" at this point, why do you claim you've solved the problem, and the masses are ready to storm the universities?

If you were raised as a "problem solver", why haven't you figured out the answers to these questions already?

- > *Why?*

To point out that you are wrong. Period.

And now for the "Hammer" and "masses storming the university" part of the post:

- > *Well really big numbers are important for encryption*
- > *schemes used to protect the Internet and lots of other*
- > *stuff.*

You've got it backwards here.

It's not the big numbers, it's the (pre-determined) fact that factoring is hard. If factoring were easy, RSA and PGP wouldn't be used for security purposes; it would be like not putting locks on doors.

Mathematics cannot be censored. (You are pretty much forced to believe this; otherwise, there's no use in amateurs working on problems.) IF factoring were easy, then decryption would be easily discovered, and SOMEONE (any yahoo with a computer) can read everyone's stuff, no matter how it's encrypted. This obviously is not happening, so we (which means you, too) are forced to reject the "factoring is actually easy" hypothesis.

- > *So they just pick an area where this work would be*
- > *dramatic, and say that it's not.*
- >
- > *They are acting on social realities, and not mathematical*
- > *ones.*
- >
- > *Notice, what happened when I presented the surrogate*
- > *factoring theorem.*

Did NSA hire you? Did the masses start storming universities? Did computer admins scramble like crazy, looking for a new way to encrypt information?

No. Nothing did.

- > *Some posters promptly tried to challenge whether or*
- > *not it was a theorem.*

It's a theorem that says nothing, like "if $x = \ln(y^2)$, then $y = e^{(x/2)}$." It solves one set of equations for a certain subset of variables.

The theorem is at

http://groups-beta.google.com/group/Surrogate-Factoring/browse_frm/thread/d2716c9b44654f4c/956ac3e0ae651f4f#

. There's no arguing that it says nothing about non-trivial and trivial factors, because those terms don't appear anywhere in the theorem or its proof.

Oh, you added another post in the Surrogate Factoring group:

- > *This group is an open one and I welcome posters*

Why did that group start off with 3 members, which has gone down to 2? Why do people need to be "approved" before they can post there? And guess who's doing the approving — you. This is about as open as Stalin's regime.

And why are you the ONLY person who's posted there? Can't you find any patsies?

- > *Then most settled on calling it trivial and challenging me to*
- > *factor some number with it.*

This is the basic rule in math: Put up or shut up.

- > *However, the theorem is enough to explain the link.*

Then insult the intelligence of every poster to sci.math! This is how you can silence Usenet once and for all, by actually showing that your SF Theorem works!

The fact that you haven't is a very strong argument against it actually saying anything.

> *The link between factors is enough to show importance.*

Bull muffins. The link is everything.

> *Making it work practically is a whole other arena.*

Then how do you know it will work?

> *But I fear it can be done, and I'm not going to do it.*

"I'm not going to do it." Probably because you can't and no one can. That's certainly the easiest explanation.

> *So we're all waiting for those people who will, and*
> *we're waiting to see what they do.*

And you're going to let them?

You say that your old blog got taken over. Well, if someone cracks your codes, they can do the same thing to your current account, and the Surrogate Factoring group. You go down with everyone else. If you're not concerned about it, why should anyone else be?

> *We can talk here as much as we want,*

Talk, no action.

> *but the real power has passed to the people who are*
> *checking, and making it work, assuming they're out*
> *there.*

What do you mean, "assuming"? You said yourself they're out there, learning how to factor and read everyone's e-mails.

> *And I think they would be out there, as not everyone*
> *is gullible and willing to listen to sci.math'ers with*
> *an agenda,*

Everyone has an agenda. What's yours? Trying to convince people that somehow you, an amateur without any proper mathematical training, has solved a problem the rest of the world can't? One which has been a problem for centuries?

> *who just always say that whatever I have is wrong*
> *or unimportant.*

Aha. So the "agenda" is simply telling the truth.

sci.crypt: Re: SF: Areas of confusion, infinity

> *Some people are bound to check.*

And they will find the math -- and the truth -- are not on your side.

--- Christopher Heckman