Re: SF: Generalized SFT's

Source: http://sci.tech−archive.net/Archive/sci.math/2005−04/msg03551.html

- *From*: "Tim Peters" <tim.one@xxxxxxxxxxx>
- *Date*: Sun, 24 Apr 2005 13:21:39 −0400

[cutting the distribution list down to just sci.math, and suggesting
others do too]

[Justin]
>>> Please demonstrate using an example.

[JSH]
>> Why? I suggest you follow the algebraic proof. What does a single
>> example tell you anyway beyond absolute proof?

An example is a start at learning whether the theorem can be used to factor integers as the product of other integers. Several people have tried this now, and "discovered" what really ought to be obvious, and even to you: pick any composite M. Your theorem leads to the trivial conclusion (or would, if you carried it a few easy steps beyond where you declared victory and went into head−in−the−sand mode) that there are an infinite number of rationals r such that 1 < gcd(num(r), M) < M. But it provides no help in finding such an r. Everyone already knew that such r exist. Not only on sci.math today, but a thousand years ago too. The point is _finding_ such r, and no flavor of SFT to date is any help with that.

[Mark Atherton]
> I can't work out how to use your algebraic proof as an algorithm to factor
> (for example) 15. I'm obviously missing something here. Why
> don't you humour me and Justin and help us see your method?

He doesn't have a factoring method here, just a proof that factors can be derived from some−− but not all −−elements of an infinite set. C. Bond fleshed out an almost−complete example of factoring 15 last week, and I added the last little step. Look that up if you really care; there's nothing relevantly different about the "generalized" SFT (which at least Rick Decker has already explained to JSH). The "last little step" is the one James refuses to try, and there's no way to complete it successfully short of:

− knowing the integer factorization in advance (then it's easy)

− systematically choosing rational inputs so that the rational outputs systematically cover the possible prime divisors of M; there are many ways to do this, but they're just absurdly obscured ways of systematically choosing integer trial divisors, or integer trial gcd candidates, directly

− pure luck

So why won't James try it? Because he's made a complete ass of himself insisting that this (non)method is a major result, accusing posters telling him true things of being "lying scum", and so on. And James is deceptive (perhaps deliberately to others, perhaps helplessly to himself) when he says he's not afraid to be proven wrong here.

Over in the "Full Retraction with my Apologies" thread, James wrote this, about an earlier, similar episode:

I'd come on and rant a bit at posters and about mathematicians not accepting my work, and challenge people to check for themselves.

And then I found out I was wrong.

I don't know if I can describe the feeling, but it's a horrible feeling.

To me it was such a huge, horrible thing, and I don't know how long it was before I posted that I was wrong, and pulled down websites, and settled into this new world of going from thinking I was on top of the world−−or about to be−−to realizing that the posters who kept saying I was wrong, were right.

Does that sound like a man who doesn't fear being shown wrong? Every bit of his behavior now is consistent with that being shown wrong here too would indeed be a "huge, horrible thing" to him, a thing he'd do nearly anything to avoid enduring again.

He won't try it because _trying_ it, even once, leaves no doubt about whether he's right. At some level he must know that already. Why? Heh −− because there's no other comprehensible reason for refusing to try. He knows darned well too that his previous rounds of "proven correct" factoring algorithms (back when he still tried to give algorithms) were proved wrong by trying examples, and small examples at that.

Note that this time, SFT is true so far as it goes. James "conveniently" shifts claims, so that if you say "but you're wrong" he reads it as you claiming SFT is false. It's not. What he's wrong about is that SFT is of any use in finding integer factors. It indeed pumps out an infinity of "rational factors", and an integer factor can indeed be derived from an infinite subset of those. But it's of no help finding an element of the winning subset.

.

- ***Follow−Ups***:
  - ***Re: SF: Generalized SFT's***
    - *From:* Mark Atherton

- Prev by Date: ***Re: Prove that a set is a monoid, but not a ring***
- Next by Date: ***Re: second order ODE (numerical)***
- Previous by thread: ***fractal dimension***
- Next by thread: ***Re: SF: Generalized SFT's***
- Index(es):
  - ***Date***
  - ***Thread***