

Re: JSH: Factoring and residues

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-07/msg03202.html>

- *From:* "Tim Peters" <tim.one@xxxxxxxxxxxxx>
 - *Date:* Sun, 16 Jul 2006 03:50:36 -0400
-

[jstevh@xxxxxxx]

...
I was wrong in thinking that picking x_{res} and getting k with a chosen S would guarantee T .

Yup.

However, while I have been reasonable,

On that point, yes, and I'm indecently grateful for that break from "the usual".

you have not, as you keep fighting a political battle to convince other people that there is nothing to these ideas.

Stating, proving, and reporting true things about the method you posted is not political. It's math. People can believe whatever they like as far as I'm concerned, but I'm given some evidence instead of just whining, threatening, and bullshitting. That's your act, and I don't want it.

...
But you haven't shown that the method usually fails.

It's quite true that I haven't proved that. I've presented analysis of the math that's strong enough to strongly /suggest/ (to people who know what they're doing — and sorry if that leaves you out) that it's extremely likely to be true. But no, it hasn't been rigorously proved. Pay my usual consulting rate, and I'd be willing to take on that tedious task in earnest full-time.

As in last year's methods, you require first picking values for a pile of

Re: JSH: Factoring and residues

independent variables, and it's quite difficult to rigorously analyze such a messy approach, especially when you have no idea how to go about picking values that "are likely" to work. So, after doing enough math to convince myself that it was unlikely to work well no matter what strategy was used (short of exploiting a known factorization in advance), I implemented it, and tried lots of strategies. They all sucked, on average requiring more gcds than the random-gcd factoring method was expected to take.

From that, it's an empirical observation that all strategies required more tries before success the larger T's smallest prime factor, much like (but worse than) the random-gcd factoring method.

And I'll tell you something: that's utterly unsurprising to anyone but you. You're the one living on wishful thinking here, and for everyone else my experiments just confirm what they already expected would be true from looking at your math/. You given no mathematical reason here to expect this to work well under any conditions. None. Nada. Zip. You only have hope that it will work well "somehow", unsupported by any mathematical argument for why it even could work well.

You've stated it.

Yes. This is a fact: it almost always failed on the first try at factoring a non-trivial T, independent of the strategy tried for picking x_{res} , S, and a factorization of k^2+S . I tried picking them large, small, near the square root, at 10/20/.../90 percentiles, correlated, anti-correlated, independently. It's very boring when you can see no reason to expect a strategy to work well, many reasons to expect them not to work well, and everything you try sucks. But up to you now -- I'm out of that now.

I've stepped in to show what's mathematically shown, having to revise my own views as there were things I missed or was wrong about, as I learn more, myself, about this approach.

Implement it, and you'll learn a lot more. I daresay you learned more simply from me pestering you to finish factoring 35 on alt.math.undergrad than you learned by thinking about it for days from a vacuum devoid of experience. You have a terrible track record at finding the problems in your own work, and trying examples is the easiest way for you to oppose that weakness.

Now you've backtracked to something that's true: while there's no reason to hope this method can efficiently factor the T you give it, it does efficiently factor other integers, vaguely related to T via

Re: JSH: Factoring and residues

chains of information—losing congruences. That's incredibly weaker than the original claims, but at least it's a true claim.

I haven't back-tracked as I've learned more given more information, and had some mistaken ideas cleared up.

Give it up — you plastered crazy false claims about having "solved the factoring problem" on multiple newsgroups multiple times at the start of this one. You thought it would factor T reliably and quickly then. You no longer think that.

It's basic research. Some expansion of knowledge along the way is understandable.

Can't have it both ways, bubba: either you've "solved the factoring problem", or you haven't. If you haven't (and you haven't ;-)), then yes, you've certainly backtracked from your original claims. And that's a /good/ thing, because your original claims were false.

....

That opens the real question of how often when you find S and k for your x_{res} , will you get some other answer coming in,

More often the larger T's smallest prime factor, and you're already very unlikely to factor incoming T with 6 digits.

But you just make statements without proof as if the idea of mathematics has escaped you.

That was reporting a testing result.

Mathematics is not about just making statements, as people who are mathematicians believe that you can actually prove things to be true, or not true, using the tools of mathematics.

Fine: prove there exists a strategy for picking S, x_{res} , and a

Re: JSH: Factoring and residues

factorization of k^2+S such that the method factors composite T efficiently.

No? How about a proof that's /likely/ to be true? No? Anything real?

instead as the math shifts to some T other than the one you want, and the good news is that other T 's will tend to be integers of absolute value bigger than yours,

Because the largest T satisfying the congruences is $|S - 2*x*k|$, and when you pick $S=1$ $x_{res}=1$ (as you've always done so far), $k = (T+1)/2$. Therefore the largest T satisfying the congruences is $|1 - (T+1)*x|$, which has a minimum value of T at $x=1$ ($x=0$ isn't useful).

Well, it seems to me that there must be some pressure against larger T 's, as there are an infinity of possible ones, correct?

I don't know what your assumptions are in asking in that question. Once x and y are computed, the set of T that satisfy all the congruences is exactly the set of integer divisors of x^2-y^2 . That much is so easy to prove that it's really just observation: $x^2-y^2 = 0 \pmod T$ /means/ that T divides x^2-y^2 . Therefore T must be an integer divisor of x^2-y^2 , and every integer divisor of x^2-y^2 obviously "works".

But as you go up you get larger and larger numbers, so the likelihood of getting them drops rapidly.

Sounds like a strategy to me for maximizing your chances of getting the T you want could be lurking in there—or in plain sight.

Sorry, couldn't follow the reasoning there.

which means there are probably strategies for limiting that happening.

See above. Pick larger S , and, more importantly, since

$$x = z-k = (f_1 + f_2)/2 - k$$

Re: JSH: Factoring and residues

pick f_1 and f_2 to minimize the absolute value of that expression.

Which is not a mathematical statement.

Huh? $x = (f_1 + f_2)/2 - k$. k is fixed, and there are a finite number of ways to factor $S+k^2$ as the product f_1*f_2 . You're saying you don't know how to minimize x given all that? LOL. Or you don't know /why/ you want to minimize $|x|$? Or what? This is /purely/ math. I give up.

Now I think you're playing politics in an effort to convince others to ignore this research.

People who look over my posting of a roadmap of my research may wonder how it's possible I could have so much research and it not be recognized.

Doubt it.

Well, people like Tim Peters are part of the problem.

Nope. Look for a mirror.

I LIKE mathematics. And I LIKE talking about mathematics.

And there are people who LOVE to reply to me just to tell people that I'm wrong or that what I found is useless.

Nobody gets a free ride on a technical newsgroup. If you don't want critical evaluation of your ideas, don't post. If you want better evaluations, post better ideas — and work at improving your technical writing — and drop the ranting.

I'm just one voice.

I'm tempted to delete off the rest of Tim Peters reply,

Fine by me.

Re: JSH: Factoring and residues

but it might help to leave it in, especially so that some of you can understand the other weapon of people like him—tedium.

They make long posts which are a pain to reply to where they say nothing of mathematical importance.

This is mostly because it takes 100x more effort than it should to bring you to an understanding of a true thing. If everything isn't explained in extreme, elementary detail, and usually repeated many times, you don't get it. But if anything is explained in even moderate detail, you bitch about "long posts". LOL! Such a delight it is to correspond with you ;-)

Eventually I get tired of bothering with them and abandon threads, which they take as an opportunity to have the last word.

OK, you have the last word on this one, if you want it. I won't reply. Go ahead, tell me I'm going to be killed again, that I'm lying scum, that I'm facing imminent legal action, whatever you like. Or don't — also fine by me if you don't reply.

There are LOTS of them and one of me.

There's only one of everyone, you know.

...

The only thing mathematically that is true is that two congruences hold:

$$x^2 - y^2 = 0 \pmod{T}$$

and

$$S - 2x_{\text{res}}k = 0 \pmod{T}$$

where my idea has you selecting S and k , and solving an equation that follows using

$$x^2 - y^2 = S - 2x_{\text{res}}k$$

where you factor $S+k^2$ to get y , which means mathematically at that point, the algebra JUST has S and k^2 , so it can give you solutions that work with x_{res} and T different from your choices, which fit with the congruences.

That's what the mathematics says.

Re: JSH: Factoring and residues

Cough. Weren't you the one complaining about "tedium" just above? What do you think endless repetition of the same stuff is?

Well, maybe, maybe not, but why one way or the other?

See above. You have no way here to find useful solutions to:

$$x^2 = y^2 \pmod{T}$$

for a /fixed/ T . Instead you're effectively picking x and y , then solving for T . But that's trivial to solve — none of the machinery in your method is needed for that, and it's of no use for factoring a /fixed/ T regardless.

I've repeated what the mathematics actually says, while you've mainly just STATED things without proof.

Which statement in the paragraph of mine above are you disputing? For example, are you claiming now you /do/ have a way to find useful solutions to that congruence for a fixed T ? If so, I haven't seen it. Are you claiming that your method /doesn't/ find specific values for x and y ? That the T 's it /does/ work for /don't/ have to divide $x^2 - y^2$? That it's /not/ trivial to solve for T given x and y ? That it /is/ useful to solve for T given x and y ? Etc. I made purely mathematical assertions there, and you gave 0 math in response.

Your statements follow the trend of downplaying the method, which I say is a political position.

Not really. The plain truth is that I've found nothing of genuine mathematical interest in this method, and increasing reason to expect it won't lead anywhere. That may or may not be a failing on my part, but it's true all the same. My considered opinions sound negative because they /are/ negative, not because I have a political agenda. I truly believe there's nothing of real value here.

For goodness sake, man, you can't even factor 35 with this method (although I did that for you). How can you sanely expect anyone to think it's "promising"? The key bit of math you /thought/ was true at the start has been shown false, and the only real mathematical reason to look at this died with it. It's certainly true that nobody else shares your desperate /hope/ that something can nevertheless be salvaged here — and a salvage operation

Re: JSH: Factoring and residues

it did become after the primary claim failed.

Readers who think such politics is a minor thing need only look over the roadmap of my current mathematical discoveries, to get some comprehension of how powerful it is when people play politics with mathematics.

Just take one thing—I have a short proof of Fermat's Last Theorem.

To shoot down consideration of it, people need only make fun of the CLAIM.

I see you're continuing your effort to teach me how to do math here.

....

The nature of mathematical discovery is that until you're right, you're wrong.

I've had years of working to find mathematical answers and in every case, guess what?

In every case, I was wrong, until I was right.

Past failures have no impact on whether or not the current ideas work or not.

Each idea stands alone, and necessarily, guess what?

Ideas that are wrong, failed.

It just does not matter how many times I failed before, when current ideas are right here and the question is about their validity.

See "tedium" above. I'm sure you never tire of this rant, but most people still reading your posts have seen it 100s of times by now.

The answer is objectivity: consider these ideas on their merits.

Ah, there's the rub: to everyone but you, it's obvious that I've looked at these ideas far more objectively than you're /capable/ of doing. Sucks for you, but it's the truth.

Re: JSH: Factoring and residues

Now I have experience with my other mathematical results where people kept claiming I was wrong when I was right, and there's a dead math journal to tell you how powerful human denial can be.

That dead journal published a paper outlining the key controversial mathematics that holds together my proof of Fermat's Last Theorem.

But it died quietly, with little fanfare or notice...social forces are more powerful than most of you are willing to admit, which is why they have been winning for so long.

People may be able to shoot down your research just by SAYING it's wrong.

James Harris

See "tedium" above. Zero math, same old rants.