

Re: JSH: Factoring and residues

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-07/msg03480.html>

- *From:* "Chuck Grempu" <spamless@xxxxxxxxxx>
 - *Date:* Mon, 17 Jul 2006 12:56:24 -0500
-

<jstevh@xxxxxxx> wrote in message
<news:1153022857.985835.215450@xx>

Tim Peters wrote:

[Tim Peters]

...

And these things are generally false,
although James wishes they were
true:

$$\begin{aligned}x &= x_{\text{res}} \text{ modulo } T \\x^2 &= y^2 \text{ modulo } T \\1 &< \gcd(x+y, T) < T \\1 &< \gcd(x-y, T) < T\end{aligned}$$

[jstevh@xxxxxxx]

The correct mathematical view is that given S and k, you
have an
infinite range of possible x_{res} 's and T's that will satisfy

$$S = 2x_{\text{res}} * k \text{ mod } T$$

and

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

so you can find an S and k that will work with a particular
 x_{res} you
choose, your desired residue for x, but there are an infinity of
other
 x_{res} 's and T's possible for which S and k will also work.

It's as simple as that and there is no reason for anyone to act

Re: JSH: Factoring and residues

like
there's a big mathematical mystery here.

I agree that there isn't, but stop pretending that was your _original_
view
of this method. At its start, this was all delusional nonsense like:

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

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

[JSH]
Kind of one of those odd things, but this idea just did come to me
Saturday in that I just wrote down some equations and hey! I solved
the factoring problem.

Etc, etc.

You didn't solve it, and the primary purpose of my post was to show that,
and explain _why_ the method usually fails to factor the T you give it.
A
secondary purpose was to help others understand what your method _is_,
since
almost nobody else replying to you appeared to have any real idea what
you
were trying to say (your own writeups were unclear on several key
points).

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

You've stated it.

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.

No, you do not learn. You are a Crackpot

Now you've backtracked to something that's true: while there's no reason
to

Re: JSH: Factoring and residues

hope this method can efficiently factor the T you give it, it does efficiently factor /other/ integers, vaguely related to T via 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.

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

You don't care about that.

For example, for those who didn't follow the full story on other newsgroups, given $T=91$ $x_{\text{res}} = S = 1$ as inputs, it can end up deducing that 459 is divisible by 17 and 27. The doesn't look useful to me, but if you can make something useful of it, more power to you.

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.

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.

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

Re: JSH: Factoring and residues

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?

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.

which means there are probably strategies for limiting that happening.

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

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

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

Which is not a mathematical statement.

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.

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

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.

I'm just one voice.

Re: JSH: Factoring and residues

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

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

There are LOTS of them and one of me.

Now the mathematics here is simple and I think neat, but the politics are high, so rather than admit that future development is possible, or even bother giving mathematical reasons for how certain things can happen Tim Peters is just pushing the position that it can't work well.

I explained earlier that, given any inputs and any specific way of factoring $S+k^2$, your method ends up computing specific integers x and y . The set of T for which the congruences hold is then the set of integer divisors of x^2-y^2 , no more, no less. Just like in the example above, given $T=91$ $x_{res} = S = 1$, your method computes $x=5$ and $y=22$ (given one way of factoring $S+k^2$), so that T then satisfies the congruences if and only if T divides $22^2-5^2 = 459$.

There's no mystery about that either.

<SNIP CRAP>.

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

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

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

Re: JSH: Factoring and residues

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.

<SNIP CRAP>

That's why I hate how political this damn field has become as you run into operatives like Peters who are fighting a war--what I call the math wars--and the mathematics is just a pawn in a game about convincing people one way or another.

I have no stake in whether you "solve the factoring problem" or not. It's your ego that's hugely involved in that, not mine. When you post claims that aren't true, sometimes I take time to refute them; when you're going down a road that I clearly see is a dead end, sometimes I try to tell you why. You haven't noticed that I haven't been wrong about one of those yet?
I have ;-)

<SNIP CRAP>