Re: Factoring problem, my assertion revisited

Source: http://sci.tech−archive.net/Archive/sci.math/2005−02/2764.html

---

From: Tim Peters (*tim.one_at_comcast.net*)
Date: 02/09/05

```
Date: Tue, 8 Feb 2005 19:47:33 −0500
```

[Rick Decker]
> Right. However, there are problems with James' method that work against
*> making the factorization of T *too* easy. In particular, a candidate*
> factorization has to satisfy a condition involving quadratic residues
> mod primes dividing M. That means that with too small a set of candidate
> factors you might very well not get any useful ones at all.
...
> I'm pretty sure I've posted a sample using James' method to factor 15.
> I have another one factoring 391 if anyone's interested.

Rick, you're one of the handful of people here who sincerely tries to make sense of what JSH might be saying. You can tell who those people are by noting who JSH attacks most fiercely <0.1 wink −− & hi, Nora ;−)>.

I'm not as willing as you to fill in so many wide gaps in his logic and presentation. So while I don't know whether your idea of JSH's method has anything in common with what JSH thinks it is (I'll take him at his word −− all othres are as ants to his overwhelming mathematical power), I'm in fact more interested in seeing your development. So, yes, an example for 391 would be appreciated!

You did give an example for 15 before, but _then_ your best attempt at guessing what JSH meant came to the conclusion that every non−zero rational x was a solution to his equations. In that universe, it was hard not to find an x with numerator(x) divisible by 3 <heh>.