

## Re: JSH: Factoring and residues

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2006-07/msg02545.html>

---

- *From:* "Tim Peters" <[tim.one@xxxxxxxxxxxxx](mailto:tim.one@xxxxxxxxxxxxx)>
  - *Date:* Thu, 13 Jul 2006 03:41:22 -0400
- 

[added "JSH:" to subject; cut sci.crypt & alt.math]

[jstevh@xxxxxxx]

...  
That is the starting equation with a minor re-arranging, but I also add later that

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

[Proginoskes]

without saying what T is.

T is the integer you want to factor. It's another independent variable here.

My best guess, based on your posts, is

$$T = S - 2 \times k,$$

T isn't defined in terms of any of the other 4 (S, k, x, y) variables here. It's introduced for the first time as a constraint:

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

on the possible values for x and y; it has nothing to with S or k, except to the extent that they're indirectly constrained via this constraint on x & y.

although the modular equation above is also true for  $T = 1$ .

His wild hope is that:

Re: JSH: Factoring and residues

$\gcd(x \pm y, T)$

in the end must reveal non-trivial factors of  $T$ .

...  
One interesting point is that  $y$  is never directly related to anything as instead  $y^2$  is.

So how good is your method if it says that, say,  $y^2 = 183$ ?

He hasn't gotten that far yet, because he hasn't tried it, and can't think any straighter than he ever can when overwhelmed by the nervous thrill of impending victory. Leaving aside that "the instructions" for finding  $y$ :

>>  $x+k = \sqrt{y^2 + S + k^2}$   
>>  
>> and finding  $y$  is just a matter of factoring  $(S+k^2)/4$ .

don't make a lick of sense, he hasn't even gotten as far as noticing that there's no reason to imagine  $S+k^2$  is divisible by 4.

Now that's funny :-). In a different set of newsgroups, he started to factor  $T=35$ , and picked  $S=x_{\text{res}}=1$  (giving  $k=18$ ), but dropped it immediately after saying:

[JSH]  
Then  $y$  is found by factoring  $(1+18^2)/4$  and then you have  $x$  as well.

He didn't notice that 325 isn't divisible by 4? Or he did notice it, and that's why he dropped his attempt to factor 35 at that point? Or this is another method where he's happy to settle for arbitrary real factors? Or ....?

The funny thing is that there's no flattering answer :-)

...  
After all, it is mathematics. Why should it care?

Mathematics doesn't care whether there is an efficient factoring algorithm. Computer Science does.

LOL! How true. Another funny thing is that whenever James has made a "math doesn't care" argument in the past, somehow or other math always managed to

Re: JSH: Factoring and residues

care after all, and favored the outcome he didn't want. By now, he should suspect that math has a deep grudge against him personally ;-)

.