

Re: JSH: What is surrogate factoring? Once more.

## Re: JSH: What is surrogate factoring? Once more.

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-09/msg00649.html>

---

- *From:* riderofgiraffes <[mathforum.org\\_am@xxxxxxxxxxxxxxxx](mailto:mathforum.org_am@xxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 04 Sep 2007 12:12:53 EDT
- 

I think you are overlooking what is maybe the central unavoidable problem with the Harris idea. As with Fermat's algorithm (and Dixon's, and the quadratic sieve), he wants

$$X^2 = Y^2 \pmod{T}, \text{ i.e.,}$$

$$(X + Y)(X - Y) = 0 \pmod{T}.$$

So say  $T = 77$ . Let  $k = 1$  and  $n = 2$ .

You can't do this. He assumes that  $k=2x(T)$   
\*THAT'S\* the central, unavoidable problem.