

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/msg00741.html>

- *From:* "Mas Plak" <spamless@xxxxxxxxxxxxx>
 - *Date:* Tue, 4 Sep 2007 18:13:54 -0500
-

"marcus_b" <marcus_bruckner@xxxxxxxxx> wrote in message
news:1188926026.332142.159830@xx

On Sep 4, 11:12 am, riderofgiraffes <mathforum.org...@xxxxxxxxxxxxxxxxx>
wrote:

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 $k=2x \pmod T$
THAT'S the central, unavoidable problem.

I think we may be saying the same thing or closely
related things. He cannot let $k = 2X \pmod T$ until he
specifies X . What he does in fact is the following.
He FIRST chooses k and n , and lets $S = 2k^2 + nT$.
Then he factors S as $S = F1 * F2$, and AFTER THAT,
he chooses X and Y . In the process, he forgets that
he originally wanted $X^2 = Y^2 \pmod T$, and in general
the algorithm he specifies does not give him this
crucial equality. So as a rule he does not end up
with a difference of squares which equals a multiple

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

of T. This largely explains why his method, unlike that of Dixon or the quadratic sieve method, fails most of the time.

Marcus.

a product of a weak mind. JSH may talk big, but is weak intellectually, and a troll.