

Re: Finding large primes, quickly

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-08/msg00907.html>

- *From:* jstevh@xxxxxxx
 - *Date:* 13 Aug 2006 12:53:30 -0700
-

Rotwang wrote:

You're missing a lot of it, because this thread didn't really start on sci.math, and doesn't belong here at all. It started on sci.crypt

My mistake, apologies to James.

No prob. I'm not really all that thin-skinned. I can't be.

And just so this is settled, my thinking was that you could use a simple property of quadratic residues to build up to large primes quickly, by iterating with something like

$n^2 - 2$

but Tim Peters noted that what I'd found was already well-known and demonstrated that you could get similar behavior with other stuff, so I lost interest.

Now to me, much simpler would have been some objective reply to my original posts on this subject, without all the other stuff, and things could have been much nicer.

I really don't like all the useless arguing, though I like to argue—about the value of the ideas themselves—not with all this personal and political crap, but when I try to just be objective, other posters have a field day.

Years of experience have thought me to hit back quite quickly, or you find that other people start repeating what posters going after you in personal ways are saying, and in my case, they even put stuff on webpages!!!

So it can be a really big deal for me to just try and let them be and take the high road.

Kind of why politics in other areas disintegrates so rapidly, as the

Re: Finding large primes, quickly

candidate who tries to take the high road and not sling mud——tends to get taken apart by the one who does.

James Harris

.