

Re: Basically a sieve method, relation to quantum

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-01/6641.html>

From: David C. Ullrich (ullrich_at_math.okstate.edu)

Date: 01/23/05

Date: Sun, 23 Jan 2005 08:03:03 -0600

On Sat, 22 Jan 2005 19:25:31 -0500, "Tim Peters" <tim.one@comcast.net> wrote:

>[\[jstevh@msn.com\]](mailto:jstevh@msn.com)

>...

>> *To factor an RSA challenge number I'd need a full factorization of some number off of it. Now $T = M^2 - j^2$, where M is the target number, and j is a number you get to pick.*

>

>*That's where you often get off track, failing to engage your full abilities.*

>*What you want instead is a method that will factor M given a factorization*

>*of $T = M+j$, where j is a number you get to pick. For example, pick $j=0$, and*

>*then your algorithm will run in linear time.*

Damm. I was going to suggest deriving a factorization of M from a factorization of $2*M$, but your idea is much simpler and more elegant.

Oh well, not the first time something like this has happened – I guess we math guys should leave the actual programming to the pros.

>*Picking $j=0$ in $T=M^2-j^2$ is*

>*good too, but then you're left with tedious work to weed out the repeated*

>*factors. Set your goal higher.*

>

David C. Ullrich