Re: Surrogate factoring ideas to ponder

Source: http://sci.tech−archive.net/Archive/sci.math/2005−03/7550.html

---

jstevh_at_msn.com
Date: 03/22/05

```
Date: 21 Mar 2005 17:29:15 −0800
```

C. Bond wrote:
> jstevh@msn.com wrote:
>
> > Part of the reason I find myself still focusing on a sign variation
on
> > my earlier quadratics is that I can easily get to a surprising
> > relation.
>
> You seem surprised at nearly anything −− except that you're usually
wrong!
>
> [snip]
>

It looks like I can focus on just a few key equations:

yz^2 − Az + j^2 = 0

and

(y/A^2)A^2 z^2 − Az + j^2 = 0

which follows trivially from it, along with

b_2 f_1 = (Az + 2M^2 +/− sqrt((Az + 2M^2)^2 + 4M^2T))/2

where I have b_2 a factor of M, the target that is to be factored,
while f_1 is just a factor of T, as I talked about in my original post.

And importantly, I also have

Az = Ax(Ax +/− sqrt((Ax − 2j^2)^2 + 4Tj^2))/(2Ax − 2M^2)

where I can get Az from the factorization of Tj^2.

Where I have Ax from

yx^2 − Ax + M^2 = 0,

where also, trivially, I have

(y/A^2)A^2 x^2 − Ax + M^2 = 0.

So I CAN get a difference of squares for M, as I have this set of solutions with which to get Az and get a rational

sqrt((Az + 2M^2)^2 + 4M^2T))

where I have M setup for a difference of squares.

What's intriguing here is that if you factor T and j, and you calculate Az, and plug it in, then that square root is *guaranteed* to be rational.

So with this method, getting a difference of square with M is trivial.

The question is, what would block it from factoring M?

James Harris