Re: SF: Back to theory

Source: http://sci.tech−archive.net/Archive/sci.math/2005−02/9246.html

---

jstevh_at_msn.com
Date: 02/25/05

Date: 25 Feb 2005 04:26:08 −0800

jstevh@msn.com wrote:
> *I see a lot of negative postings about my ideas, and surrogate*
> *factoring is getting a lot of bashing, but hey, it's just an idea.*
>
> *It may not be practical−−ever. But it's still just an idea, and I*
can
> *discuss it as just an idea, having long ago backed away from calling*
it
> *a solution to the factoring problem.*
>
> *Now some posters seem to be obsessed with political posting meant to*
> *drive others away from my idea. I say, look at what they're doing as*
> *just that−−political postings.*
>
> *Now to the theory.*
>
> *Basically with the latest surrogate factoring I've been analyzing the*
> *quadratics:*
>
> *yx^2 + Ax − M^2 = 0*
>
> *and*
>
> *yz^2 + Az − j^2 = 0*
>
> *where T = M^2 − j^2*
>
> *and my algorithms focus on y, for several reasons, not the least of*
> *which it *seems* to only need the factorization of T, while other*
> *algorithms, which I'll get to later, require that both j and T be*
> *factored, while doing far worse than algorithms that just use*
> *factoring T.*

<deleted>

> *One thing worth mentioning is that explicit equations relating x and*
y
> *to factors of T and j are easily derived:*

> *>*
> *> y = A^2(f_1 − b_1)(f_2 − b_2)/(b_1 f_2 + b_2 f_1 − 2b_1 b_2)^2*
> *>*
> *> where b_1 b_2 = −j^2 and f_1 f_2 = T,*
> *>*
> *> and*
> *>*
> *> x = (b_1 f_2 + b_2 f_1 − 2b_1 b_2)/A.*
> *>*

I get those equations by using

(a_1 x + b_1)(a_2 x + b_2) = yx^2 + Ax − j^2,

so

(a_1 x + b_1)(a_2 x + b_2) = T

and then I use f_1 f_2 = T, so

a_1 x + b_1 = f_1

and

a_2 x + b_2 = f_2

and it's easy enough to solve for explicit solutions to y and x in terms of the factorizations of j and T.

But I just realized that I can do the same with

yz^2 + Az − j^2 = 0,

to explicitly solve y and z in terms of the factorizations of M and T, but, I have the same y, so maybe you can just use the explicit equations for y, for each of the factorizations and map them together to pull out the factors of M.

If so, the correct algorithm is nothing like what I've been doing.

That would be a twist.

James Harris