

Re: Surrogate factoring, out of the box

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-01/8579.html>

From: oðin (oðin_at_ragnarok.com)

Date: 01/29/05

Date: Sat, 29 Jan 2005 12:25:51 -0800

> *Well I'll admit that I've been feeling a bit depressed the last couple
> of days, as I had calculations showing at least 50% success with a
> rational x , and then I checked thoroughly and found that my method gave
> a LOT of rational x 's, and wasn't factoring with most of them.*

Oh... so when you claimed that you had the problem solved, you must have been wrong? And those that doubted you were not liars?

> *And then I realized that for most cases it gives you an x that has your
> target itself as the factor.*

Oooops. Not very clever... not really beyond brilliant after all?

> *I puzzled over that result, and realized that the math was too
> efficient in searching through rational solutions...*

Oh I see, you realized that your math was just too efficient... that was the problem all along... that is why it worked so badly...

> *So I squared the target, and it factored.*

You squared the target, and that helped! Hmmmmm.... try throwing in a few trig functions too... It can't really hurt...

> *Why? You need to understand quadratic residues to understand why.*

Do you know what a quadratic residue is? You never explained how it relates to your "work".

> *Basically the probability was too high that it could get quadratic
> residues for both of my factors, so by squaring them, I forced the math
> to look for solution for those factors squared, making it more likely
> that it would fail for at least one, and it did.*

Making it more likely that it would fail? I thought Surrogate Factoring already failed sufficiently well.

sci.math: Re: Surrogate factoring, out of the box

> *I have verified that the value of A is mostly irrelevant,...*

I thought Surrogate Factoring was already mostly irrelevant...

> *I'm still puzzling over the quadratic residues a bit...*

I am not at all surprised.

, as it's not to

> *That's the profoundly fascinating feature of this method, as infinity
> itself is checked for results!*

Remarkable. Has Surrogate Factoring ever found infinity to be a factor of any composite yet?

> *And that is rigorously proven.*

Yes, in classic James Harris style! You just make a claim and poof, you have another proof.

> *Well, infinity is kind of big...*

That is the kind of deep insight we have all come to expect from you.

> *So yeah, if you try to factor something not prime, and get no factors,
> square it.*

And that somehow helps with your claim that the algorithm is efficient?

> *and I'm going to work on settling down the probabilities, as I find it
> curious.*

Keep us posted.

> *Fun. Math is great.*

Yes, it is fun. I wish you could experience it too.