

Re: Factoring with cubic equations?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/0546.html>

From: lapin des pyrenees (*moc_at_com*)

Date: 10/06/03

Date: Sun, 5 Oct 2003 19:30:52 -0400

"Simon Johnson" <Ckwop@hotmail.com> wrote in message
news:f5668ae7.0310050718.6f75490b@posting.google.com...
> *"lapin des pyrenees" <moc@com> wrote in message
news:<vT2dnd0IK4_jWOOiU-KYjA@golden.net>...*
> > *the reason we use $f(x)=x^2$ is not because it's the "quickest non-linear
> > polynomial", the real reason is because we are too dumb to derive a
quicker
> > polynomial!*
> >
> > *btw, I derived a way to generate all the squares used in the QS method.*
> >
> > *Note: I did not say that: given a number N I can tell you the squares
x^2
> > and y^2. All I am saying is that there exist a way to generate all those
> > squares independently of the corresponding number N to which they
relate.*
> >
> > *If this result is important, by that I mean (as a question) will it
make
> > the search for the squares related to a given number faster if we knew
where
> > to look?
> > if it is faster, I will release the way it's done.*
> >
> > *le lapin des vosges*
> >
> >
> > *I conjecture (someone correct me if i'm wrong) that the problem of
> > finding a polynomial that colides quicker than $f(x) = x^2 \bmod n$ is
> > roughly equal to the amount of effort to brute-force that collision
> > with $f(x) = x^2 \bmod n$.*
> >

the nice thing about " I conjecture" is that it's easy and you don't have to prove a thing!

> *Finding your polynomials is probaby harder than using GNFS on big*

sci.crypt: Re: Factoring with cubic equations?

> *numbers.*

>

how can you say it's harder if you don't even know how " my method " works.
what is the basis or your judgment? this is about science not politics. how
about some hard work on your part that demonstrate something useful instead
of conjecturing...

I conjecture that you don't understand how the method works! prove me wrong!

le lapin des alpes maritimes
vive la france

> *Simon.*