

Re: JSH: Surrogate factoring, periodic behavior

Source: <http://sci.tech--archive.net/Archive/sci.math/2007-09/msg00052.html>

- *From:* JSH <jstevh@xxxxxxxxxx>
 - *Date:* Sat, 01 Sep 2007 05:21:41 -0000
-

On Aug 31, 9:07 pm, Enrico <ungerne...@xxxxxxx> wrote:

On Aug 31, 10:09?am, JSH <jst...@xxxxxxxxxx> wrote:

Having completed better analysis on surrogate factoring I found the equations > <big snip>
James Harris

Direct calculation of n in JSH's Surrogate,

$$S=2*k^2 + n*T$$

given p, T, and k where
T is an odd composite integer
p is an integer divisor of T
k is an integer

Let A, B, C, D be elements of matrix M:

B D
A C

If
 $A = (p+k) - T \bmod (p+k)$
 $C = T \bmod (p+k)$
and $\text{Det } M = -[2*k^2 \bmod (p+k)] = B*C - A*D$

then $n = B + D$

Example:

T = 20303
p = 79

Re: JSH: Surrogate factoring, periodic behavior

$k = 23$

Factored trying 5 surrogates on the fifth surrogate using $k=1$ where the start was with $n=7$.

Part of the problem I've run into with comments about surrogate factoring have been repeated claims it works only as good as trial division, but hey, I programmed the damn thing.

I know you people are lying.

The current algorithms I'm trying now are actually crappier than what I had before which would factor out small numbers with only a couple of surrogates.

So, the problem here is that I have a Java program where I can stick in your numbers and watch the damn thing do better than you claim it can do.

So I KNOW you are lying while it's not clear why.

But people who don't program this thing for themselves need to understand that these people are not telling you the real truth here, and God only knows exactly why.

If surrogate factoring had worked really crappy all along I'd have given up on it myself, but instead I found it crapped out with slightly bigger numbers, and definitely not with primes less than 100.

James Harris

.