

Re: JSH: Surrogate factoring, periodic behavior

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-09/msg00040.html>

- *From:* Enrico <ungernerik@xxxxxxx>
 - *Date:* Fri, 31 Aug 2007 21:07:04 -0700
-

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
k = 23

$p+k = 79+23 = 102$
 $T \bmod (p+k) = 20303 \bmod 102 = 5$
 $A = 102 - 5 = 97$

Re: JSH: Surrogate factoring, periodic behavior

$$C = 5$$

$$\text{Det } M = -[2 \cdot 23^2 \bmod (79+23)]$$

$$\text{Det } M = -[1058 \bmod (102)] = -38$$

Smallest positive solutions for B, D are

$$B = 70, D = 4$$

$$B \cdot C - A \cdot D = 70 \cdot 5 - 97 \cdot 4 = 350 - 388 = -38$$

checks ok so far.

$$n = B + D = 70 + 4 = 74$$

so, $(p+k)$ divides S at $n' = J \cdot (p+k) + n$
with J in integer.

$$\text{If } J = 0, n' = 74$$

$$S = 2 \cdot 23^2 + 74 \cdot 20303 = 1503480$$

$$\text{and } S/(p+k) = 1503480/102 = 14740$$

$$\text{If } J = 1, n' = 1 \cdot 102 + 74 = 176$$

$$S = 2 \cdot 23^2 + 176 \cdot 20303 = 3574386$$

$$S/(p+k) = 3574386/102 = 35043$$

$$\text{If } J = -1, n' = -1 \cdot 102 + 74 = -28$$

$$S = 2 \cdot 23^2 - 28 \cdot 20303 = -567426$$

$$S/(p+k) = -567426/102 = -5563$$

So, the desired factor 102 can be found in S
where $n' = J \cdot (p+k) + n$ to produce the factor
 $79 = 102 - 23 = (p+k) - k$, which divides T

Getting n' using only some properties of T
and not knowing a factor of T beforehand is
the object of JSH's method, which currently
is still much worse than trial division.

Sieving is possible on all the S , but if k is 1 or coprime
to T , it looks like you get candidate values of $(p+k)$
covering all integers not containing any factor of T .

Enrico

.