

## Re: Surrogate factoring, corrected algorithm

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2005-02/6412.html>

---

**From:** Décio Luiz Gazzoni Filho (*decio\_at\_decpp.removethis.net*)

**Date:** 02/17/05

Date: Thu, 17 Feb 2005 02:52:08 -0200

Tim Peters wrote:

> [JSH]

> [...]

>> Then the corrected algorithm is as follows.

>

> As far as I can see, the only difference from the weekend's algorithm is

> that this one iterates over splittings of  $T^3 j^2$  instead of over  $T j^2$ .

> I'll note up front that cubing  $T$  can enormously increase the number of

> distinct  $f_1 f_2$  splittings, and so also the number of gcds tried.

If you're choosing random  $j$ 's, I agree. However, see my sibling post where I propose a new sieving procedure which leads to values of  $T$  of the form  $2^3 p_1 p_2$ , where  $p_1$  and  $p_2$  are two huge primes. That cuts back drastically the number of divisors. In fact, there are only 160 ways to split  $T$ .

Unfortunately I can't control the number of factors of  $j$  (and thus  $j^2$ ), but the fact that  $j = O(\log^2 M)$  and thus is small already takes care of that.

Décio