

## Re: Baillie–Pomerance–Selfridge–Wagstaff papers on pseudoprimes now online

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-03/2161.html>

---

**From:** Francois Griend ([fgriend@micronet.fr](mailto:fgriend@micronet.fr))

**Date:** 03/27/03

From: Francois Griend <[fgriend@micronet.fr](mailto:fgriend@micronet.fr)>

Date: Thu, 27 Mar 2003 10:50:42 +0100

In article <NSmga.466\$Uw4.114561147@twister2.starband.net>,

"Roger Schlafly" <[rogersc@mindspring.com](mailto:rogersc@mindspring.com)> wrote:

> *Is there any document that corrects the errors in the ANSI  
> prime testing?*

As explained by Don Johnson in another branch of this thread, Burt Kaliski has drafted a minor revision of ANSI X9.80.

Main points:

- In the Lucas test, a search for  $D$  in  $5, -7, 9, -11..$  such that  $\text{Jacobi}(D,p)=-1$  will fail if  $p$  is an exact square; now it is asked to test if  $p$  is an exact square, maybe after a number of values of  $D$  have been tried without success. This insures the test terminates.
- If during the above search a  $D$  is found such that  $\text{Jacobi}(D,p)=0$ , it is asked to declare  $p$  composite; this makes the test slightly more selective, and most importantly reconciles it with the list of pseudoprimes given by Baillie and Wagstaff.
- The algorithm for computing  $\text{Jacobi}(D,n)$  is corrected, (previously it did not even work for the worked-out example) and expanded to negative  $D$ .
- It is explained how to compute  $A/2 \bmod p$  when  $A$  and  $p$  are odd, and that numerical examples for the Lucas series are given with reduction modulo  $p$  in the range  $(-p/2, p/2)$ .
- The Lucas–Lehmer test is renamed Lucas; my apologies to Bob Silverman for this one, which I now understand is reversing his work, and debatable. If that helps, I am happy with "Lehman's Lucas test"...

sci.crypt: Re: Baillie–Pomerance–Selfridge–Wagstaff papers on pseudoprimes now online

- There is expanded bibliographical reference to the origin of combining a strong pseudoprime test to base 2 and this Lucas test, and on an unclaimed prize offered for a counterexample.
- The random choice of base for the Miller–Rabin test is now on  $[2, p-2]$  rather than  $[2, p-1]$ , for symmetry.
- The Shawe–Taylor algorithm is fixed to always produce primes in the appropriate range.

Francois Grieu