ARE THERE COUNTER-EXAMPLES TO THE BAILLIE – PSW PRIMALITY TEST?

Carl Pomerance

1984

to Arjen K. Lenstra on the defense of his doctoral thesis

In [2] the following procedure is suggested for deciding whether a positive integer n is prime or composite:

(1) Perform a base 2 strong pseudoprime test on n. If this test fails, declare n composite and halt. If this test succeeds, n is probably prime. Go on to step (2).

(2) In the sequence $5, -7, 9, -11, 13, \dots$ find the first number D for which $(D/n) = -1$. Then perform a Lucas pseudoprime test with discriminant D on n (a specific one of these tests as described in [2]). If this test fails, declare n composite. If this test succeeds, n is "very probably" prime.

Although it first appeared in [2], the idea of trying such a combined test originated with Baillie.

In an exhaustive search up to $25 \cdot 10^9$ in [2], no composite number was found that passed both (1) and (2). In fact, if (1) is weakened to just an ordinary base 2 pseudoprime test, every composite $n \le 25 \cdot 10^9$ fails either (1) or (2).

The authors of [2] have offered a prize of \$30 (U.S.) for a composite number n (with its prime factorization) that passes (1) and (2) or a proof that no such n exists. Since the publication of [2], the second author has increased his \$10 share of the prize money ten-fold, so now the award stands at \$120. (The cheap first and third authors have not increased their shares as yet, although the third author has contemplated offering a "bit" more.)

In the interests of helping Arjen start his post-doctoral career on a sound financial footing, I will give here some hint on how a counter-example to this Baillie-PSW "primality test" may be constructed. In fact, I will give a heuristic argument that will show that the number of counter-examples up to x is $\gg x^{1-\epsilon}$ for any $\epsilon > 0$. This argument is based on one by Erdos [1] that suggested there are many Carmichael numbers.

Let $k > 4$ be arbitrary but fixed and let T be large. Let $P_k(T)$ denote the set of primes p in the interval $[T, T^k]$ such that

(a) $p \equiv 3 \bmod 8$, $(5/p) = -1$,

(b) $(p-1)/2$ is square free and composed solely of primes $q < T$ with $q \equiv 1 \bmod 4$,

(c) $(p+1)/4$ is square free and composed solely of primes $q < T$ with $q \equiv 3 \bmod 4$.

Of course, 1/8 of all primes (asymptotically) in $[T, T^k]$ satisfy condition (a), and it can be shown that the conditions that $(p-1)/2$ and $(p+1)/4$ also be square free

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

still leaves a positive fraction of all primes in $[T, T^k]$. Heuristically, the conditions that $p-1$ and $p+1$ are composed solely of primes below T, allow us to keep still a positive proportion of all primes in $[T, T^k]$ (using k fixed). Finally, the event that every prime in $(p-1)/2$ is 1 mod 4 should occur with probability $c(\log T)^{-1/2}$ and similarly for the event that every prime in $(p+1)/4$ is 3 mod 4. Thus the cardinality of $P_k(T)$ should be asymptotically as $T \to \infty$

$$\frac{cT^k}{\log^2 T}$$

where c is positive constant that depends on the choice of k. We now form square free numbers n composed of ℓ primes of $P_k(T)$, where ℓ is odd and just below $T^2/\log(T^k)$. The number of choices for n is thus about

$$\binom{[cT^k/\log^2 T]}{\ell} > e^{T^2(1-3/k)}$$

for large T (and k fixed). Also, each such n is less than e^{T^2}.

Let Q_1 denote the product of the primes $q < T$ with $q \equiv 1 \bmod 4$ and let Q_3 denote the product of the primes $q < T$ with $q \equiv 3 \bmod 4$. Then $(Q_1, Q_3) = 1$ and $Q_1 Q_3 \approx e^T$. Thus the number of choices for n formed that in addition satisfy

$$n \equiv 1 \bmod Q_1, n \equiv -1 \bmod Q_3$$

should, heuristically, be at least

$$e^{T^2(1-3/k)}/e^{2T} > e^{T^2(1-4/k)}$$

for large T.

But any such n is a counter-example to the Baillie-PSW primality test. Indeed, n will be a Carmichael number so it will automatically be a base 2 pseudoprime. Since $n \equiv 3 \bmod 8$ and each $p|n$ is also $\equiv 3 \bmod 8$, it is easy to see that n will also be a strong base 2 pseudoprime. Since $(5/n) = -1$, since every prime $p|n$ satisfies $(5/p) = -1$, and since $p+1|n+1$ for every prime $p|n$, it follows that n is a Lucas pseudoprime for any Lucas test with discriminant 5.

We thus see that for any fixed k and all large T, there should be at least $e^{T^2(1-4/k)}$ counter-examples to Baillie-PSW below e^{T^2}. That is, if we let $x = e^{T^2}$, then there are at least $x^{1-4/k}$ counter-examples below x, so long as x is large. Since k is arbitrary, our argument implies that the number of counter-examples below x is $\gg x^{1-\epsilon}$ for any $\epsilon > 0$.

Remark. Both in the APR primality test and in the Cohen-Lenstra variation there is a part where many kinds of pseudo-primality tests are performed followed by a step where a limited amount of trial division is performed. No one has ever encountered an example of a number where the trial division was really needed – that is, every number that has made it through the pseudo-primality tests actually was prime. Perhaps an argument similar to the one here can show that in fact there are composite numbers that pass all the pseudo-primality tests and for which the trial division step is really needed to distinguish them from the primes.

References

1. P. Erdos, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen **4** (1956), 201–206.
2. C. Pomerance, J.L. Selfridge, and S.S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003–1026.

Department of Mathematics, University of Georgia, Athens, GA 30602 U.S.A.