The Distribution of Pseudoprimes

Matt Green

September, 2002

The RSA crypto-system relies on the availability of very large prime numbers. Tests for finding these large primes can be categorized as deterministic and probabilistic. Deterministic tests, such as the Sieve of Erastothenes, offer a 100 percent assurance that the number tested and passed as prime is actually prime. Despite their refusal to err, deterministic tests are generally not used to find large primes because they are very slow (with the exception of a recently discovered polynomial time algorithm). Probabilistic tests offer a much quicker way to find large primes with only a negligibal amount of error.

I have studied a simple, and comparatively to other probabilistic tests, error prone test based on Fermat's little theorem. Fermat's little theorem states that if b is a natural number and n a prime then $b^{n-1} \equiv 1 \pmod{n}$. To test a number n for primality we pick any natural number less than n and greater than 1 and first see if it is relatively prime to n. If it is, then we use this number as a base b and see if Fermat's little theorem holds for n and b. If the theorem doesn't hold, then we know that n is not prime. If the theorem does hold then we can accept n as prime right now, leaving a large chance that we have made an error, or we can test again with a different base. Chances improve that n is prime with every base that passes but for really big numbers it is cumbersome to test all possible bases.

A number that passes the aforementioned test for an arbitrary base b but is composite is called a pseudoprime base b. I have studied pseudoprimes base 2, which I will henceforth just call pseudoprimes. I have also investigated a family of pseudoprimes called Carmichael numbers, which are pseudoprime with all bases relatively prime. Knowing of the prime number theorem (not necesarrily understanding), and the great interest in the distribution of prime numbers, I naturally became curious as to whether there was any theorem describing the distribution of pseudoprimes or Carmichael numbers. It seemed to be a good research opportunity and so I began by writing some programs in the Java programming language to count pseudoprimes. I

also began writing a program to count Carmichael numbers, which is more computationally intensive. My counts would then serve to give me some approximations on the density of pseudoprimes and Carmichael numbers up to an arbitrary upper bound.

The results of my programs were accurate but lacked the range I needed in order to make any reasonable estimate on pseudoprime density. My limitations mostly came in the form of a lack of computer memory. I looked around on the internet and eventually came across a reference to a paper on Carmichael numbers, and I was later able to obtain this paper thanks to Professor McCallum. This paper contained pseudoprime counts and Carmichael number counts up to 10^{16} where as I was only able to achieve counts up to 10^{11}. This motivated me to stop trying to expand my programs and instead focus on theory, which was an appealing prospect.

I eventually came across a paper written by Carl Pomerance entitled "On the Distribution of Pseudoprimes". Here was the argument I had been looking for. In this paper I will define terms and prove theorems needed to understand Pomerance's argument and will then follow his argument closely, giving supplementary explanation along the way.

First, the smallest integer x such that $b^x \equiv 1 \pmod{n}$ is called the order of b modulo n. In Pomerance's paper, he will represent the order of 2 modulo m with $l_2(m)$.

A useful generalization of Fermat's little theorem, called Euler's theorem, states that for relatively prime integers b and n, $b^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n)$ is the Euler phi function. The phi function counts the number of numbers less than n that are relatively prime to n. A proof of this theorem was given in our project proposal but I'd like to revise it so I will do it again here.

The multiplicative group modulo n, Z/n^x has $\phi(n)$ elements all relatively prime to n. It is important to know that if p is prime, then there exists an element b in the multiplicative group Z/p^x with an order of $p-1$. The element b is called a generator of the group Z/p^x or a primitive root of p. In fact for any number of the form p^a where p is prime and a is any positive integer, there is a primitive root for p^a.

Proof: By the fundamental theorem of arithmetic, $p-1$ can be expressed as a unique product of primes, say $p-1 = q_1^{a_1} q_2^{a_2} q_3^{a_3} \cdots$. If a has order s modulo p and b has order t modulo p, then if $\gcd(s,t) = 1$, the order of ab is st. If we prove that there exist numbers $x_1, x_2, \ldots$ such that the order of x_i is $q_i^{a_i}$ modulo p, then $\prod_{i=1} x_i$ will have order $p-1$ modulo p. We know that $x^{p-1} - 1 \equiv 0 \pmod{p}$ has exactly $p-1$ solutions, all the naturals from 0 to $p-1$. So since if $d|p-1$, then $x^{p-1}-1 = (x^d-1)(x^{p-1-d}+x^{p-2-d}+\cdots+x+1)$, we can write the previous congruence relation as $(x^d-1)(x^{p-1-d}+x^{p-2-d}+\cdots+x+1) \equiv 0 \pmod{p}$. Using induction, it can easily be proven that an n

degree polynomial has at most n solutions modulo a prime p. So $x^d - 1$ has at most d solutions modulo p and $x^{p-1-d} + \cdots + x + 1$ has at most $p - 1 - d$ solutions modulo p, but since $x^{p-1} - 1$ has exactly $p - 1$ solutions modulo p, $x^d - 1$must have exactly d solutions modulo p and $x^{p-1-d} + \cdots + x + 1$ must have exactly $p-1-d$ solutions modulo p. Therefore if $d|p-1$ then $x^d - 1$ has exactly d solutions. Now we want $q_i^{a_i}$ to be the order of x_i modulo p. So we need numbers x with orders that divide $q_i^{a_i}$ but that don't divide $q_i^{a_i-1}$. Since there are exactly $q_i^{a_i}$ solutions to $x^{q_i^{a_i}} - 1 \equiv 0 \pmod{p}$ and exactly q_i^{ai-1} solutions to $x^{q_i^{a_i-1}} - 1 \equiv 0 \pmod{p}$ then there are $q_i^{a_i} - q_i^{a_1-1}$ solutions that have order $q_i^{a_i}$ modulo p, which just so happens to be $\phi(q_i^{a_i})$. Thus the number of primitive roots of a prime p is $\phi(q_1^{a_1})\phi(q_2^{a_2}) \cdots = \phi(p-1) > 1$. This can easliy be extended to prime power by noting that $x^{p^a-1} \equiv 1 \pmod{p^a} \equiv 1 \pmod{p}$ and then using the same argument as given above.

Another useful formula is called the Euler Product. It converts the Riemann zeta function from a sum over all the naturals to a product over all the primes. Here it is:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{n=1}^{\infty} \frac{1}{1 - \frac{1}{p_n^s}}.$$

Proof: Let $S = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$. Then

$$S - \frac{1}{2^s}S = (1 - \frac{1}{2^s})S = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \cdots$$

and

$$(1 - \frac{1}{2^s})S - \frac{1}{3^s}(1 - \frac{1}{2^s})S = (1 - \frac{1}{2^s})(1 - \frac{1}{3^s})S = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \cdots$$

Continuing this process over all the prime numbers, which might take a while, we eventually get

$$S \prod_{n=1}^{\infty} 1 - \frac{1}{p_n^s} = 1$$

This shows that

$$S = \prod_{n=1}^{\infty} \frac{1}{1 - \frac{1}{p_n^s}}$$

as needed.

Here I will give a more rigorus definition of a Carmichael number because they are just so neat. A Carmichael number n satisfies all the following critirea:

1. For a Carmichael number n, if a prime $p|n$, then $p - 1|n - 1$.

This follows directly from Fermat's little theorem. We know that $b^{n-1} \equiv 1 \pmod{n}$ for all bases b that are not multiples of n and since $p|n$, $b^{n-1} \equiv 1$

(mod p). From Fermat's little theorem we have that $b^{p-1} \equiv 1 \pmod{p}$ so the order of any base is at most $p-1$, and we already know that there is at least one base b with an order $p-1$. Therefore $n-1$ must be a multiple of $p-1$ for $b^{n-1} \equiv 1 \pmod{n}$.

2. A Carmichael number n is squarefree, that is, has no repeated prime factors.

Suppose $p^2|n$. Then from Fermat's little theorem we know that for b relatively prime to n, $b^{n-1} \equiv 1 \pmod{n}$ and since $p^2|n$, $b^{n-1} \equiv 1 \pmod{p^2}$. Now, by Euler's theorem $b^{\phi(p^2)} \equiv 1 \pmod{p^2}$. Recall that numbers of the form p^a, where p is prime and a is an aribitrary integer, have primitive roots, which means there is an element b of the multiplicative group modulo p^2 that has an order of $\phi(p^2)$. Numbers less thanp^2 that are relatively prime to p^2 are those that are not factors of p and there are $p^2 - p$ of them, so $\phi(p^2) = p(p-1)$. Since n is a pseudoprime base b, the order of b must divide $n-1$, that is, $p(p-1)|n-1$. But this is impossible since $p|n$ and $n-1 \equiv -1 \pmod{p}$. Thus n is not pseudoprime base b and cannot be a Carmichael number. It follows that n must be squarefree.

3. A Carmichel number n has at least three prime factors.

Suppose $n = pq$ where $p \neq q$. Then $n - p = p(q-1) \equiv 0 \pmod{q-1}$ so $p \equiv n \pmod{q-1}$. Likewise, $n - q = q(p-1) \equiv 0 \pmod{p-1}$ hence $q \equiv n \pmod{p-1}$. Now since $p-1 \mid n-1$ and $q-1 \mid n-1$, we know that $n \equiv 1 \pmod{p-1}$ and $n \equiv 1 \pmod{q-1}$ so $p \equiv 1 \pmod{q-1}$ and $q \equiv 1 \pmod{p-1}$. But this implies that $p = q$, which is a contradiction of the requirement that n be squarefree. Thus n must have at least three prime factors.

As I said before, I have been interested in what can be said about the distribution of pseudoprimes. This has been my main motivation for reading the paper by Pomerance. I also wish to explain and hopefully clarify ideas that show up in the paper so that any interested undergraduate could easily come to an understanding of the material. This is why I have included all of the elementary number theory definitions and proofs.

The goal of Pomerance's paper is to prove a theorem that gives an upper bound on the pseudoprime counting function, $P(x)$, which gives the number of pseudoprimes less than x, for large x values. In doing this he improves upon a previous upper bound given by the famous mathmatician Paul Erdos in 1956.

In fact, he ends up proving that

$$P(x) \leq xe^{-\frac{\log x \log\log\log x}{2\log\log x}},$$

for all sufficiently large x.

To obtain this upper bound, Pomerance begins by proving a theorem about the number of solutions to the equation $l_2(m) = n$ for $m < x$ and natural numbers n.

Theorem 1.

There is an x_0 such that if n is a natural number and $x \geq x_0$, then

$$|\{m \leq x : l_2(m) = n\}| \leq xe^{-\log x} \frac{3 + \log loglogx}{2 \log \log x}.$$

My commentary:

The conditions that $m \leq x$ and $l_2(m) = n$ are very restrictive. Pomerance goes on to say that we can assume that $n < x$ since $l_2(m) \leq \phi(m) < m \leq x$.

If $l_2(m) = n$, this means that $2^n \equiv 1 \pmod{m}$, or in other words $m|2^n - 1$. Numbers of the form $2^n - 1$ are called Mersenne numbers and there are heavy restrictions on what their factors can be.

If $n = kd$ then

$$a^n - 1 = (a^d - 1)(a^{d(k-1)} + a^{d(k-2)} + \cdots + a^d + 1)$$

So if n is composite, then for each divisor d of n, $2^d - 1|2^n - 1$.

If a prime $p|a^n - 1$ then either $p|a^d - 1$ for $d < n, d|n$ or $p \equiv 1 \pmod{2n}$. This is easy to prove using Fermat's little theorem and the fact that ********.

So if $m|2^n - 1$ then the prime divisors of m, p, all either divide $2^d - 1$ for $d < n, d|n$ or are congruent to 1 modulo $2n$, that is, $2n|p - 1$. It is easy to see that the numbers m can be are very limited.

End commentary

Proof. We may assume $x > n$ for otherwise there are no $m \leq x$ with $l_2(m) = n$. If $c > 0$ then

$$\sum_{m \leq x, l_2(m)=n} 1 \leq x^c \sum_{l_2(m)=n} m^{-c} \leq x^c \sum_{p|mthenl_2(p)|n} m^{-c} = x^c \prod_{l_2(p)|n} (1-p^{-c})^{-1} = x^c A,$$

say.

My commentary:

The indexes for the second and third sums are essentially the same. If $l_2(m) = n$ then $2^n \equiv 1 \pmod{m}$. For $p|m$, $2^n \equiv 1 \pmod{p}$ so $l_2(p) = p - 1|n$. Pomerance says that the number of elements in the set $m \leq x : l_2(m) = n$ is less than or equal to some multiple of x^c. Next he defines what c is but you musn't despair at its strangeness. His choice for c makes much more sense at end of the proof.

End commentary

We shall choose $c = 1 - (4 + \log \log \log x)/(2 \log \log x)$, where x is large enough so that $c \geq 7/8$.

The theorem will follow if we show

$$\log A = o(\log x / \log\log x).$$

Note that, since $c \geq 7/8$,

$$\log A = \sum_{l_2(p)|n} p^{-c} + O(1) = \sum_{d|n} \sum_{l_2(p)=d} p^{-c} + O(1).$$

My commentary:
It is hard (it was for me) to see that

$$\log A = \sum_{l_2(p)|n} p^{-c} + O(1).$$

So I will give an explanatory embellishment. First consider that the geometric series

$$1 + x^2 + x^3 + \cdots = \frac{1}{1-x}, for |x| < 1.$$

Integrating term by term we can obtain

$$x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots = -\log(1-x) = log(1-x)^{-1}.$$

Notice that by the properties of logarithms,

$$\log A = \log \prod_{l_2(p)|n} (1-p^{-c})^{-1} = \sum_{l_2(p)|n} \log(1-p^{-c})^{-1}.$$

Now let $p^{-c} = x$ so that

$$\sum_{l_2(p)|n} \log(1-p^{-c})^{-1} = \sum_{l_2(p)|n} \log(1-x)^{-1} = \sum_{l_2(p)|n} (x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots) = \sum_{l_2(p)|n} \sum_{k=1}^{\infty} \frac{x^k}{k}.$$

If we take out the sum of all the $k = 1$ terms we get

$$\sum_{l_2(p)|n} x + \sum_{l_2(p)|n} \sum_{k=2}^{\infty} \frac{x^k}{k}.$$

Now we must show that $\sum_{l_2(p)|n} \sum_{k=2} x^k/k$ converges. Since

$$\sum_{k=2}^{\infty} \frac{x^k}{k} = \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \cdots = x^2(\frac{1}{2} + \frac{x}{3} + \frac{x^2}{4} + \cdots) < x^2(1 + x + x^2 + \cdots) = \frac{x^2}{1-x},$$

we now can write

$$\sum_{l_2(p)|n} \sum_{k=2}^{\infty} \frac{x^k}{k} < \sum_{l_2(p)|n} \frac{x^2}{1-x} < \sum_{l_2(p)|n} x^2 = \sum_{l_2(p)|n} p^{-2c}.$$

The last term is a harmonic series that converges if the power of p is less than -1. Since $c \geq 7/8$, the last term converges and we get

$$\log A = \sum_{l_2(p)|n} p^{-c} + O(1).$$

End commentary

The primes p with $l_2(p) = d$ all divide $2^d - 1$, so there are less than d such primes. Say they are $q_1, q_2, \ldots, q_t$ where $0 \leq t < d$. Each $q_i \equiv 1 \pmod{d}$, so that

$$\sum_{l_2(p)=d} p^{-c} = \sum_{i=1}^{t} (di+1)^{-c} < d^{-c} \sum_{i=1}^{d-1} i^{-c} < (1-c)^{-1} d^{1-2c}.$$

My commentary:

Here Pomerance is trying to get an upper bound on the sum $\sum_{l_2(p)} p^{-c}$ so that he can bound $\log A$. There are less than d primes, which he labels q_i, that satisfy $l_2(q_i) = d$ because, like the author says, they must all divide $2^d - 1$. But $2^d - 1 < 2^d < \prod_{i=1}^{d} p_i$, where the product is over the first d distinct prime numbers. Therefore $2^d - 1$ must have less than d different prime factors. From Fermat's little theorem we know that for each q_i, $2^{q_i - 1} \equiv 1 \pmod{q_i}$ so $d = l_2(q_i) | q_i - 1$, that is, $q_i \equiv 1 \pmod{d}$. Now each q_i can be written as $di + 1$ for some integer i. The sum $\sum_{i=1}^{t} (di+1)^{-c}$ is obviously very rough, since it is highly unlikely that all or even most of the primes q_i would be in the arithmetic progression $di + 1$ for $1 \leq i < t$, but it does work to give an upper bound on $\sum_{l_2(p)=d} p^{-c}$ since in general, $(di + 1) < q_i$.

Moving on,

$$\sum_{i=1}^{t} (di+1)^{-c} = \frac{1}{(d+1)^c} + \frac{1}{(2d+1)^c} + \cdots + \frac{1}{(dt+1)^c}$$

and

$$d^{-c} \sum_{i=1}^{d-1} i^{-c} = \frac{1}{d^c} + \frac{1}{(2d)^c} + \cdots + \frac{1}{((d-1)d)^c}.$$

This makes it a bit clearer that the first sum is smaller than the second not only because there are possibly more terms in the second, but the denominators are smaller in the second. The term $(1-c)^{-1} d^{1-2c}$ is a little tricky to

arrive at, and it foreshadows some extremely tricky events later in the proof. Consider that

$$\sum_{i=1}^{d-1} i^{-c} \approx \int_1^{d-1} x^{-c} dx = \frac{(d-1)^{1-c} - 1}{1-c} < \frac{d^{1-c}}{1-c}.$$

So now we can say that

$$d^{-c} \sum_{i=1}^{d-1} i^{-c} < d^{-c}(\frac{d^{1-c}}{1-c}) = (1-c)^{-1} d^{1-2c}.$$

End commentary

Thus,

$$\log A \leq (1-c)^{-1} \sum_{d|n} d^{1-2c} + O(1) \leq (1-c)^{-1} \prod_{p|n} (1-p^{1-2c})^{-1} + O(1).$$

My commentary:

This should be pretty clear. He substitutes in the previous result to get an upper bound on $\log A$ and then again uses the Euler product formula to go from the sum to the product.

End commentary

Now, since $1 - 2c \leq -3/4$,

$$\log \prod_{p|n} (1-p^{1-2c})^{-1} = \sum_{p|n} p^{1-2c} + O(1) \leq \sum_{2 \log x} p^{1-2c} + O(1),$$

where x is sufficiently large, so that $\prod_{p \leq 2 \log x} p \geq x$. Using partial summation and the prime number theorem, it is seen that

$$\log \prod_{p|n} (1-p^{1-2c})^{-1} \ll \frac{(\log x)^{2-2c}}{(2-2c) \log \log x} \ll \frac{\log \log x}{\log \log \log x}.$$

Thus, if x is sufficiently large, we have

$$\prod_{p|n} (1-p^{1-2c})^{-1} \leq (\log x)^{1/2},$$

so that we have

$$\log A \leq \frac{2 \log \log x}{4 + \log \log \log x} (\log x)^{1/2} + O(1),$$

which proves the theorem.

My commentary:

This is when Pomerance resorts to mathemagic. I will attempt to clarify.

To begin, he uses the same trick he did when saying that $\log A = \sum_{l_2(p)|n} p^{-c}$ when saying that $\log \prod_{p|n}(1-p^{1-2c})^{-1} = \sum_{p|n} p^{1-2c} + O(1)$. Now I'll give the partial summation formula and prove that it is true.

Partial summation formula (Abel summation):

$$\sum_{n=1}^{N} a_n b_n = A_N b_{N+1} + \sum_{n=1}^{N} A_n (b_n - b_{n+1}),$$

where a_n and b_n are sequences and $A_n = \sum_{i=1}^{n} a_i$, $B_n = \sum_{i=1}^{n} b_i$. Proof.

$$\sum_{n=1}^{N} A_n(b_n - b_{n+1}) = A_1 b_1 - A_1 b_2 + A_2 b_2 - A_2 b_3 + \cdots + A_N b_N - A_N b_{N+1}$$

$$= A_1 b_1 + (A_2 - A_1) b_2 + (A_3 - A_2) b_3 + \cdots + (A_N - A_{N-1}) b_N - A_N b_{N+1}$$

$$= a_1 b1 + a_2 b_2 + a_3 b_3 + \cdots + a_N b_N - A_N b_{N+1} = \sum_{n=1}^{N} a_n b_n - A_N b_{N+1}.$$

So

$$\sum_{n=1}^{N} a_n b_n = A_N b_{N+1} + \sum_{n=1}^{N} A_n (b_n - b_{n+1}).$$

Now that we have swallowed all of that, define $a_n = n^{1-2c}$, $b_n = 1$ if n is prime and $b_n = 0$ if n is composite. Then

$$\sum_{p \le 2\log x} p^{1-2c} = \sum_{n=2}^{2\log x} a_n b_n = A_{2\log x} b_{2\log x+1} + \sum_{n=2}^{2\log x} A_n (b_n - b_{n+1}).$$

The average value of b_n can be obtained from the prime number theorem, which says that $\pi(x) \sim x/\log x$. So the number of primes up to $2\log x$ is about $2\log x/\log 2\log x$. I will from now on omit the 2, since in approximating an upper bound, Pomerance omits the 2. This gives an average value for b_n of

$$b_n = B_{n+1} - B_n \approx \frac{n+1}{\log(n+1)} - \frac{n}{\log n} = \frac{n\log n + \log n - n\log(n+1)}{\log n \log(n+1)}.$$

If n is really really huge we can fudge a bit and say that $\log n \approx \log(n+1)$ so that

$$\frac{n\log n + \log n - n\log(n+1)}{\log n \log(n+1)} \approx \frac{1}{\log n}.$$

The sum A_n can be approximated with a definite integral,

$$A_n \approx \int_1^n x^{1-2c} dx = \frac{n^{2-2c} - 1}{2-2c} < \frac{n^{2-2c}}{2-2c},$$

which gives an upper bound on A_n Then we have that

$$A_{\log x} b_{\log x+1} \leq \frac{(\log x)^{2-2c}}{(2-2c)\log\log x}.$$

Now to fully validate Pomerance's results we have to show that

$$\sum_{n=1}^{\log x} A_n(b_n - b_{n+1})$$

gets ignorably small. From our previous results, we can write

$$\sum_{n=1}^{\log x} A_n(b_n - b_{n+1}) = \sum_{n=1}^{\log x} \frac{n^{2-2c}}{2-2c}(\frac{1}{\log n} - \frac{1}{\log(n+1)}).$$

But as n gets really huge the difference $1/\log n - 1/\log(n+1)$ gets very close to zero, so the whole sum goes away.

That leaves us with just $A_{\log x} b_{\log x+1}$, giving

$$\sum_{p|n} p^{1-2c} = \log \prod_{p|n}(1-p^{1-2c})^{-1} \leq \sum_{p\leq 2\log x} p^{1-2c} \ll \frac{(\log x)^{2-2c}}{(2-2c)\log logx}.$$

Substituting in the value of c we get

$$\frac{(\log x)^{\frac{4+\log\log\log x}{\log logx}}}{4+\log\log\log x} < \frac{e^{\log\log\log x}}{\log\log\log x} = \frac{\log\log\{x}{\log\log\log x},$$

and if x is really really huge, then

$$\prod_{p|n}(1-p^{1-2c})^{-1} \leq e^{\frac{\log\log x}{\log\log\log x}} = (\log x)^{\frac{\log x}{\log\log\log x}} \approx (\log x)^{1/2}.$$

So then we resubstitute this bound to get

$$\log A \leq (1-c)^{-1}\prod_{p|n}(1-p^{1-2c})^{-1} + O(1) = \frac{2\log\log x}{4+\log\log\log x}(\log x)^{1/2} + O(1).$$

End commentary

Theorem 2. For all sufficiently large x, we have

$$P(x) \leq xe^{\frac{-\log x\log\log\log x}{2\log\log x}}.$$

Proof. Recalling the definition of $L(x)$ as $exp(\log x \log\log\log x/\log\log x)$, we divide the pseudoprimes $n \leq x$ into four possibly overlapping classes:

(i)$n \leq x(L(x))^{-1}$,
(ii)there is a prime $p|n$ with $l_2(p) \leq L(x)$, $p > (L(x))^3$,
(iii)there is a prime $p|n$ with $l_2(p) > L(x)$,
(iv)$n > x(L(x))^{-1}$ and every prime $p|n$ is at most $(L(x))^3$.
My commentary:

Pomerance defined $L(x)$ in his introduction, which I have not included in this paper. Therefore, there is no need for memory lapse despair. By breaking down the pseudoprimes into four different catagories, Pomerance has made a way to conveniently bound the number in each catagory and then will combine all four upper bounds to get a final upper bound on the number of pseudoprimes less than or equal to x.

End commentary

The number of n in class (i) is obviously at most

$$x(L(x))^{-1}.$$

The number of primes p with $l_2(p) \leq L(x)$ is exactly

$$\sum_{m \leq L(x)} \sum_{l_2(p)=m} 1 < \sum_{m \leq L(x)} m < (L(x))^2.$$

Thus the number of n in clas (ii) is at most

$$\sum_{p>(L(x))^3, L_2(p) \leq L(x)} x/p < x(L(x))^{-3} \sum_{l_2(p) \leq L(x)} 1 < x(L(x))^{-1}.$$

My commentary:

The first sum in that last line is a very rough approximation of the number of pseudoprimes in catagory (ii), since for every p satisfying the conditions in (ii) he sums the number of multples of p less than or equal to x, of which n is only one. This sum does give an upper bound on the number of n in (ii) however.

End Commentary

If n is a pseudoprime and $d|n$, then

$$n \equiv 0 \pmod{d},$$

$$n \equiv 1 \pmod{l_2(d)},$$

$$\gcd(d, l_2(d)) = 1.$$

My commentary:

From the definition of a pseudoprime, the definition of $l_2(d)$ and the fact that $2^{n-1} \equiv 1 \pmod{d}$, we know that $l_2(d)|n-1$. Since $\gcd(n-1, n) = 1$, we also know that $\gcd(d, l_2(d)) = 1$.

End commentary

Thus the number of pseudoprimes $n \leq x$ with $d|n$ is at most $1+x/(dl_2(d))$. If $d = p$, a prime, then we throw out the solution $n = p$, so that in this case there are at most $x/(pl_2(p))$ pseudoprimes $n \leq x$ with $p|n$. Thus the number of n in class (iii) is at most

$$\sum_{2<p\leq x, l_2(p)>L(x)} \frac{x}{pl_2(p)} < \frac{x}{L(x)} \sum_{p\leq x} \frac{1}{p} \sim \frac{x \log\log x}{L(x)}.$$

My commentary

The reason why there are at most $1 + x/(dl_2(d))$ pseudoprimes with $d|n$, $n \leq x$ is because each n under these conditions, as stated by Pomerance, must satisfy both $n \equiv 0 \pmod{d}$ and $n \equiv 1 \pmod{l_2(d)}$. From a very old and very elegant theorem usually called the Chinese remainder theorem, we know that there exist simultaneous solutions n to both conguence relations and that any two solutions n are congruent modulo $dl_2(d)$. Therefore each solution n_i can be written as $n_i = q_i(dl_2(d)) + r$ with $0 \leq r < dl_2(d)$. Pomerance then gives a rough upper bound on how many pseudoprimes n of this form are between 2 and x by counting all the multiples of $dl_2(d)$, $x/(dl_2(d))$, which gives the number of n up to x with the possibility of being one short (in the case that x is not a multiple of $dl_2(d)$, so he adds one to get an upper bound.

He then considers only prime divisors $d = p$ in which case the same argumet holds to give an upper bound of n by $1 + x/(pl_2(p))$ but he throws out at least one solition $n = p$ so that the bound becomes just $x/(pl_2(p))$. The rest of the argument for the bound on class (iii) is pretty straight forward except for the last sum of the inverses of the primes.

End commentary If n is in class (iv), then n must have a divisor d with

$$x(L(x))^{-4} < d \leq x(L(x))^{-1}.$$

Thus the number of n in class (iv) is at most

$$\sum\nolimits' (1 + \frac{x}{dl_2(d)}) \leq x(L(x))^{-1} + x \sum\nolimits' \frac{1}{dl_2(d)}$$

$$= x(L(x))^{-1} + x \sum_{m\leq x} \frac{1}{m} \sum\nolimits' \frac{1}{d},$$

where $\sum'$ denotes the sum over odd d satisfying $x(L(x))^{-4} < d \leq x(L(x))^{-1}$. Using Theorem 1 and partial summation, the inner sum is, for large x, at most

$$e^{-logx \frac{2+\log\log\log x}{2\log\log x}}.$$

My commentary:

End commentary Thus, for large x, the number of n in class(iv) is at most

$$xe^{-\log x \frac{1+\log\log\log x}{2\log\log x}}.$$

Hence, using the estimates for the number of pseudoprimes $n \leq x$ in each of the four classes, we have our theorem. My commentary:

End commentary

Now I will prove that

$$\lim_{x\to\infty} \frac{\pi_2(x)}{\pi(x)} = 0.$$

From Pomerance we know that

$$\pi_2(x) \leq xe^{\frac{-\log x \log\log\log x}{2\log\log x}}$$

and from the prime number theorem we know that $\pi(x) \sim \frac{x}{\log x}$. So the fraction $\pi_2(x)/\pi(x)$ is asymptotic to

$$\log xe^{\frac{-\log x\log\log\log x}{2\log\log x}} = e^{\log\log x - \frac{\log x\log\log\log x}{2\log\log x}}$$

. To show that $\frac{\pi_2(x)}{\pi(x)} \to 0$ as $x \to 0$ we need to prove that $\log\log x - \frac{\log x\log\log\log x}{2\log\log x} \to -\infty$ as $x \to \infty$.

$$\log\log x - \frac{\log x\log\log\log x}{2\log\log x}$$

$$= \frac{(\log\log x)^2 - \frac{1}{2}(\log x\log\log\log x)}{\log logx}$$

$$< \frac{(\log\log x)^2 - A\log x}{\log\log x},$$

where A is constant. Applying L'Hopital's rule repeatedly it can be seen that

$$\lim_{x\to\infty} \frac{(\log x)^n}{\log x} = \lim_{x\to\infty} \frac{n!}{x} = 0.$$

So it is also true that

$$\lim_{x\to\infty} \frac{(\log logx)^n}{\log x} = 0.$$

Now applying L'Hopital's rule,

$$\lim_{x\to\infty} \frac{(\log\log x)^2 - A\log x}{\log\log x}$$

$$= \lim_{x\to\infty} 2\log logx - A\log x = \lim_{x\to\infty}(\frac{2\log\log x}{\log x} - A)\log x$$
$$= -A\lim_{x\to\infty}\log x = -\infty,$$

which is what's needed for $\frac{\pi_2(x)}{\pi(x)} \to 0$ as $x \to \infty$.