1 Pseudoprimes

> Have you ever noticed that there's no attempt being made to find really large numbers that *aren't* prime? I mean, wouldn't you like to see a news report that says "Today the Department of Computer Sciences at the University of Washington announced that $2^{58,111,625,031} + 8$ is even. This is the largest non-prime yet reported."
>
> — bathroom graffiti, University of Washington

> Un phénomène dont la probabilité est 10^{-50} ne se produira donc jamais, ou du moins ne sera jamais observé.
>
> — Émile Borel, *Les Probabilités et la vie*

Let n be a large odd integer, and suppose that you want to determine whether or not n is prime. The simplest primality test is "trial division." This means that you take an odd integer m and see whether or not it divides n. If $m \neq 1$, n and $m|n$, then n is composite; otherwise, n passes the primality test "trial division by m." As m runs through the odd numbers starting with 3, if n passes all of the trial division tests, then it becomes more and more likely that n is prime. We know for sure that n is prime when m reaches $\sqrt{n}$. Of course, this is an extremely time-consuming way to test whether or not n is prime. The other tests described in this section are much quicker.

Most of the efficient primality tests that are known are similar in general form to the following one.

According to Fermat's Little Theorem, we know that, if n is prime, then for any b such that $g.c.d.(b, n) = 1$ one has

$$b^{n-1} \equiv 1 \ mod \ n. \tag{1}$$

If n is *not* prime, it is still possible (but probably not very likely) that (1) holds.

Definition. If n is an odd composite number and b is an integer such that $g.c.d.(n, b) = 1$ and (1) holds, then n is called a *pseudoprime to the base b*.

In other words, a "pseudoprime" is a number n that "pretends" to be prime by passing the test (1).

Example 1. The number $n = 91$ is a pseudoprime to the base $b = 3$, because $3^{90} \equiv 1 \ mod \ 91$. However, 91 is *not* a pseudoprime to the base 2, because $2^{90} \equiv 64 \ mod \ 91$. If we hadn't already known that 91 is composite, the fact that $2^{90} \not\equiv 1 \ mod \ 91$ would tell us that it is.

Proposition V.1.1. *Let n be an odd composite integer.*

(a) *n is a pseudoprime to the base b, where $g.c.d.(b, n) = 1$, if and only if the order of b in $(\mathbf{Z}/n\mathbf{Z})^*$ (i.e, the least positive power of b which is $\equiv 1 \ mod \ n$) divides $n - 1$.*