Math 445 Number Theory

September 1, 2004

Fermat's Little Theorem: If $(a, n) = 1$ and $a^{n-1} \not\equiv 1 \pmod{n}$, then n is not prime.

This is a very effective test, mostly because we can, in fact, effectively compute $a^{n-1} \pmod{n}$, by successive squaring. The idea: write $n-1$ as a sum of powers of 2, by repeatedly subtracting the highest power of 2 less than what remains after doing prior subtractions. E.g.,

$78 = 64 + 14$, $14 = 8 + 6$, $6 = 4 + 2$, so $78 = 2^6 + 2^3 + 2^2 + 2^1$

Then we can compute $a^{78} = a^{2^6} \cdot a^{2^3} \cdot a^{2^2} \cdot a^{2^1}$, mod 79, by first computing each factor (mod 79), using $a^{2^k} = a^{2^{k-1} \cdot 2} = (a^{2^{k-1}})^2$ to proceed in stages. In this way we can compute a^{n-1} , mod n , with under $2 \log_2(n)$ multiplications.

But pseudoprimes exist; Carmichael numbers exist. (There are, in fact, infinitely many of them.) We need a better test! Which we get from:

Fact (Euler): If p is prime and $a^2 \equiv 1 \pmod{p}$,
then $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

Proof: $p | a^2 - 1 = (a-1)(a+1)$ ......

This means that if we suspect that if n is prime, we can test more thoroughly; set $n - 1 = 2^k \cdot d$ with d odd (by repeatedly dividing $n-1$ by 2 until what is left is odd). Then look, mod n at

$$a^d \ , \ a^{2d} \ , \ a^{2^2 d} \ , \ \ldots \ , \ a^{2^k d} = a^{n-1}$$

If n is prime, the last number is 1, and, by Euler, the number *just before* we first start seeing 1's must be -1. If if *don't* see this pattern, then n cannot be prime.

This is the basis for our next test, the Miller-Rabin test.