Math 445 Number Theory

September 8, 2008

For future reference: Euler's generalization of Fermat's Little Theorem:

Setting $\phi(n)$ = the number of a, $0 \leq a \leq n-1$, with $(a,n)=1$ (the Euler ϕ-, or "totient" function), then whenever $(a,n)=1$ we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

The proof is nearly identical to FLT's: compute $(aa_1)\cdots(aa_{\phi(n)})$, where $a_1,\ldots,a_{\phi(n)}$ are the numbers coprime to n, and note that (for the same reasons!) this is $\equiv a_1\cdots a_{\phi(n)}$; but since this number is coprime to n, we conclude that $a^{\phi(n)} \equiv 1$.

Miller-Rabin Test: Given a number N, and a base a, compute $N-1 = 2^k \cdot d$, with d odd. Then compute

$a_0 = a^d \pmod{N}$, $a_1 = a^{2d} = (a^d)^2 \pmod{N}$, $a_2 = (a_1)^2 \pmod{N}$, ... , $a_k = a^{2^k d} = a_{k-1}^2 \pmod{N}$

If $a_0 = 1$ or $a_i \equiv -1 \pmod{N}$ for some $i \leq k-1$, then N passes the test; it is either prime or a *strong pseudoprime* to the base a. If not, then N is definitely not prime.

Monier and Rabin in 1980 showed that a composite number N is a strong pseudoprime for at most 1/4 of possible bases a. So if N passes this test for m randomly chosen bases $a_1,\ldots,a_m$, then N has only a 1 in 4^m chance of *not* being prime. That is, multiple Miller-Rabin tests are very good at ferreting out non-primes.

Fermat's Little Theorem <u>can</u> tell us that some numbers are prime, though:

Proth's Theorem: If $N = 2^k m + 1$ with $m < 2^k$ and if there is an a with $a^{2^{k-1}m} \equiv -1 \pmod{N}$, then N is prime.

This result is the reason behind why most of the largest known prime numbers are known to be prime! The instructor's personal favorite is $19433 \cdot 2^{1096861} + 1$ (with 330,193 digits), found by the instructor in May of 2008. It is, as of this writing, the 200th largest known prime. The largest at this time is $2^{32582657} - 1$, with 9,808,358 digits, although there are rumors that this may soon change?