Math 445 Number Theory

August 30, 2004

Our previous approaches to checking for primes are too labor intensive! Fermat's Little Theorem provides a better way.

$(a, b) = \gcd(a.b) =$ greatest common divisor ; $a \underset{p}{\equiv} b$ means $p|b - a$;

FLT: If p is prime and $(a, p) = 1$, then $p|a^{p-1} - 1$ (i.e., $a^{p-1} \underset{p}{\equiv} 1$)

(Alternatively, if p is prime then $a^p \underset{p}{\equiv} a$ for all a .)

Main ingredients:

(1) If p is prime, $(a, p) = 1$, and $ab \underset{p}{\equiv} ac$, then $b \underset{p}{\equiv} c$

(2) If $(a, n) = 1$ and $(b, n) = 1$, then $(ab, n) = 1$

Then to prove FLT, look at

$$N = (p-1)!a^{p-1} = (1 \cdot a)(2 \cdot a) \cdots ((p-1) \cdot a) \ .$$

If we show that $N \underset{p}{\equiv} (p-1)!$, then since $((p-1)!, p) = 1$ (by (2) and induction), we have $a^{p-1} \underset{p}{\equiv} 1$ by (1). But, again by (1), if $xa \underset{p}{\equiv} ya$ then $x \underset{p}{\equiv} y$, so each of $1 \cdot a, 2 \cdot a, \ldots , (p-1) \cdot a$ are distinct, mod p. I.e., this list is the same, mod p, as $1, 2, \ldots , p-1$, except for possibly being written in a different order. But then the products of the two lists are the same, as desired.

FLT describes a property shared by all prime numbers. What is remarkable is that most composite numbers *don't* have this property. A composite number n for which $a^n \underset{n}{\equiv} a$ is called a *pseudoprime to the base a*. If n is a pseudoprime to all bases, it is called a *Carmichael number*.

Unfortunately (for primality testing), Carmichael numbers do exist. The smallest is $561 = 3 \cdot 11 \cdot 17$.

It is a fact that Carmichael numbers can be characterized precisely as those n for which their prime factorization $n = p_1 \cdots p_k$ has $p_1 < p_2 < \ldots < p_k$ (factors are *distinct*) and $p_i - 1|n - 1$ for every i. We showed that numbers of this form *are* Carmichael numbers.

Next step: find a *better* property of primes to test for!