Math 445 Number Theory

September 15, 2004

Decimal expansion of $1/n$: we saw that if $(10,n)=1$ then $\text{ord}_n(10)|\Phi(n)$ gives us the period of $1/n$.

If $(10,n)>1$, then we write $n=2^i\cdot 5^j\cdot d$, with $(d,10)=1$. Then

$$\frac{1}{n}=\frac{1}{2^i\cdot 5^j\cdot d}=\frac{A}{2^i\cdot 5^j}+\frac{B}{d}=\frac{A\cdot d+B\cdot 2^i\cdot 5^j}{2^i\cdot 5^j\cdot d}$$

which we can solve for A and B because $1=A\cdot d+B\cdot 2^i\cdot 5^j$ has a solution, since $(d,2^i\cdot 5^j)=1$. Then the first half has a terminating decimal expansion, while the second repeats with some period $\text{ord}_d(10)|\Phi(d)$. So $1/n$ eventually repeats (after the terminating decimal has, well, terminated), with period = the period of $1/d$.

There are methods which (unlike the Miller-Rabin test) can <u>tell</u> us that a number n is prime. One such is

Lucas' Theorem : If n is an integer, and, for every prime p with $p|(n-1)$, there is an a (depending on p) satisfying

$$a^{n-1}\equiv 1 \pmod{n} \text{ and } a^{\frac{n-1}{p}}\not\equiv 1 \pmod{n}$$

then n is prime.

The basic idea: if n isn't prime, then $\Phi(n)<n-1$. So for some prime p, $n-1$ is divisible by a higher power of p than $\Phi(n)$ is. Suppose p^s is the highest power dividing $\Phi(n)$, and p^r is the highest power dividing $n-1$, so $s<r$. Then for the corresponding a,

$$\text{ord}_n(a)|\Phi(n) \text{ and } \text{ord}_n(a)|(n-1) \text{ but } \text{ord}_n(a)\not|\frac{n-1}{p}$$

The last two imply that $\text{ord}_n(a)$ has p^r as a factor, but the first says that it has at most p^s as a factor, a contradiction. So n is prime.

This resuilt is not going to be useful to decide that a random n is prime, because it requires you to know all of the prime factors of $n-1$ (hence its prime factorization). But is works well for numbers where we know this factorization, because we *build* them this way. In particular, it is very effective for testing numbers like $n=p\cdot 2^k+1$ where p is a prime (or a number with few prime factors). Nearly all of the largest known primes of their day were shown to be prime via Lucas' Theorem (and its variants), until the late 1960's.

In particular, one class of numbers that it applies to are the *Fermat numbers* $N=2^n+1$. It is a straightforward calculation to show that if d is an odd factor of $n=dm$, then $N=2^{dm}+1$ has 2^m+1 for a factor. So the only Fermat numbers worth testing for primality are $F_n=2^{2^n}+1$. These <u>are</u> prime for $n=1,2,3,4$, and are known to be composite for n from 5 to 32. Fermat originally thought they were all prime; now we conjecture that all of the rest of them are composite! Note that F_{32} has more than a *billion* digits!