Math 445 Number Theory

September 19 and 22, 2008

On a lighter note, the analysis we have developed can shed light on *repeating decimal expansions of fractions.*

A number like $\dfrac{1}{13} = 0.076923076923\ldots = 0.\overline{076923}$ has a repeating pattern, every 6 digits (in this case). What this means is that

$$\frac{1}{13} = \frac{76923}{10^6} + \frac{76923}{10^{12}} + \frac{76923}{10^{18}} + \cdots = (76923)\left(\frac{1}{10^6} + \left(\frac{1}{10^6}\right)^2 + \left(\frac{1}{10^6}\right)^3 + \cdots\right)$$
$$= \frac{76923}{10^6 - 1}$$

The *period* of the decinal expansion is 6, because $10^6 - 1 = (13)(76923)$, i.e., $10^6 \equiv 1 \pmod{13}$, and 6 is the smallest positive number for which this is true. Borrowing some terminology from group theory, we say that the *order* of 10, mod 13, is 6, and write $\mathrm{ord}_{13}(10) = 6$; it is the smallest positive power of 10 which is $\equiv 1$ mod n. The definition of $\mathrm{ord}_n(a)$ is similar.

In general, $\mathrm{ord}_n(a)$ makes sense only if $(a,n) = 1$; then, by Euler's Theorem,

$$a^{\Phi(n)} \equiv 1 \pmod{n}$$

where $\Phi(n) =$ the number of integers b between 1 and n with $(b,n) = 1$. So there is a smallest such power of a . Conversely, if $a^k \equiv 1 \pmod{n}$, then $a \cdot a^{k-1} + n \cdot x = 1$ for some x, so $(a,n) = 1$.

Since $a^k, a^m \equiv 1 \pmod{n}$ implies $a^{(k,m)} \equiv 1 \pmod{n}$, if $(a,n) = 1$ then $\mathrm{ord}_n(a) | \Phi(n)$. So we can test for the $\mathrm{ord}_n(a)$ by factoring $\Phi(n) = p_1^{k_1} \cdots p_r^{k_r}$. We know $a^{\Phi(n)} \equiv 1$; if we test each of $a^{\Phi(n)/p_i}$ and none are $\equiv 1$, then $\mathrm{ord}_n(a) = \Phi(n)$. If one of them is $\equiv 1$, then $\mathrm{ord}_n(a) | \Phi(n)/p_i$; continuing in this way, we can quickly determine $\mathrm{ord}_n(a)$.

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 $\mathrm{ord}_d(10) | \Phi(d)$. So $1/n$

eventually repeats (after the terminating decimal has, well, terminated), with period = the period of $1/d$.

We can show that there are n with $\mathrm{ord}_n(10) = \Phi(n)$; in fact, $n = 7^k$ will work. To see this, we can show (directly) that $\mathrm{ord}_7(10) = \Phi(7) = 6$, so $6{=}\mathrm{ord}_7(10)|\mathrm{ord}_{7^k}(10)$ for every k. But $\Phi(7^k) = 7^{k-1} \cdot 6$, so $\mathrm{ord}_{7^k}(10) = 7^{i_k} \cdot 6$ for some i_k. We can show that $i_k = k - 1$ by induction, by showing (by induction!) that for every k, $10^{7^{k-1} \cdot 6} = 1 + 7^k \cdot m$ for some $m \equiv 1 \pmod 7$. Consequently $10^{7^{k-1} \cdot 6}$ <u>cannot</u> be congruent to 1 mod 7^{k+1}, because if $10^{7^{k-1} \cdot 6} = 1 + 7^{k+1} r = 1 + 7^k \cdot 7r$, then $1 + 7^k \cdot m = 1 + 7^k \cdot 7r$, so $m = 7r$, so $m \equiv 0 \pmod 7$, a contradiction. So $\mathrm{ord}_{7^k}(10) = 7^{k-1} \cdot 6 = \Phi(7^k)$ for every $k \geq 1$.

Gauss conjectured that there are infinitely many <u>primes</u> p with $\mathrm{ord}_p(10) = p - 1 = \Phi(p)$, but this remains unsolved...