UW Math Circle Problems for October 31 & November 7 '07

Periodicity and Remainders

The last digits of the Fibonacci numbers are 1, 1, 2, 3, 5, 8, 3, 1, 4, 5, 9, 4, 3, 7, 0, 7, 7, 4, 1, 5, 6, 1, 7, 8, 5, 3, 8, 1, 9, 0, 9, 9, 8, 7, 5, 2, 7, 9, 6, 5, 1, 6, 7, 3, 0, 3, 3, 6, 9, 5, 4, 9, 3, 2, 5, 7, 2, 9, 1, 0, 1, 1, 2, 3, . . .

- Show that this sequence is periodic.

The ideas mentioned here relate this to a problem that we saw earlier: "show that F_k divides F_n whenever k divides n."

When x, y, m are integers and $m > 0$, we say that "x is equivalent to y modulo m", or "$x \equiv y \pmod{m}$", if the integer $x - y$ is divisible by m.

- If $a \equiv b \pmod{m}$ show that $b \equiv a \pmod{m}$; if n is a factor of m show that $a \equiv b \pmod{n}$.
- If $a \equiv b \pmod{m}$ and $a \equiv c \pmod{m}$, show that $b \equiv c \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, show that $a + c \equiv b + d \pmod{m}$ and $ac = bd \pmod{m}$.

Do you see why modular arithmetic relates to looking at the last digit? the last k digits? More generally than what we had before, we can show the following:

- The Fibonacci numbers and Lucas numbers are each periodic modulo m, for any positive integer m. Can you show that one of the first 10^8 Fibonacci numbers ends in four zeroes?
- What happens to the last digits of the sequence $1, 2, 4, 8, 16, \ldots$?

A similar but much harder problem is to investigate Pascal's triangle (of binomial coefficients) modulo m. Try writing out the $m = 2$ case by hand.

Here are some other typical (and not-so-typical) problems that can be solved using modular arithmetic and/or periodicity.

- Prove that $2x + 3y$ is divisible by 17 if and only if $9x + 5y$ is divisible by 17.
- (i) Prove that if a, b, c are odd integers then $ax^2 + bx + c$ does not have rational roots. (ii) If m and n are positive integers, show that $4mn - m - n$ cannot be a perfect square. (iii) If $a^2 + b^2 = c^2$, show $3|ab$. (iv) Show that the sum of m consecutive squares cannot be a square for the cases $m = 3, 4, 5, 6$. (iv) Find 11 consecutive squares whose sum is a square.
- Prove that if a, b, c, d, m are integers such that 5 does not divide d and 5 does divide am^3+bm^2+cm+d, then there exists an integer n so that 5 divides $dn^3 + cn^2 + bn + a$.
- Prove that $2^n + 1$ is never divisible by 7, that $2^{2n} + 24n - 10$ is always divisible by 18, and that $23^{2n+2} + 13^{6n+2}$ is always divisible by 120.
- Show that if x, y, z are integers and $x^3 + 3y^3 + 9z^3 = 9xyz$ then $x = y = z = 0$. What if they are rational numbers?

Two numbers x and y are *relatively prime* (in symbols, $a \perp b$) if they have no common factors other than 1 (and -1).

- If $ar \equiv br \pmod{m}$ and $r \perp m$, show $a \equiv b \pmod{m}$. Is there a counterexample if $r \not\perp m$?
- *Fermat's Little Theorem:* If p is a prime number and p does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$.
- *Euler's Theorem:* If $q \geq 2$ and $q \perp a$, show $a^{\phi(q)} \equiv 1 \pmod{q}$; here $\phi(q)$ counts how many integers between 1 and q are relatively prime to q.
- Show that Fermat's little theorem is a special case of Euler's theorem. Prove one or both of them.
- Show that if x and y are relatively prime integers, that $\phi(xy) = \phi(x)\phi(y)$.
- Using Fermat's little theorem, if p is a prime that divides $4x^2 + 1$ for some integer x, show $p \equiv 1 \pmod{4}$.
- Using the previous question, show there are infinitely many primes that are equivalent to 1 modulo 4.

Challenge problem from last weeks' topics: determine all rational numbers a, b, c for which the roots of $x^3 + ax^2 + bx + c = 0$ are a, b, c.