Math 580/780I Notes 5

Modular Arithmetic:

- Definition. Two integers a and b are congruent modulo an integer n if $n|(a-b)$.
- Notation. $a \equiv b \pmod{n}$.
- **Examples.** What will be the time 1000 hours from now? On what day of the week will September 8 be in 2011?
- **Theorem 9.** *Let a, b, c, and n be integers. Then each of the following holds.*

(i) If $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$.
(ii) If $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$.
(iii) If $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $ac \equiv bd \pmod{n}$.
(iv) If $a \equiv b \pmod{n}$ *and* $d|n$, *then* $a \equiv b \pmod{d}$.

- **Proof:** Give the usual proofs. In particular, in (iii), observe that $a - b = kn$ and $c - d = \ell n$ for some integers k and ℓ so that

$$ac - bd = (a-b)c + (c-d)b = (kc + \ell b)n,$$

and the result follows.

- **Comment:** Note that (iii) implies that if $a \equiv b \pmod{n}$ and k is a positive integer, then $a^k \equiv b^k \pmod{n}$.
- **Theorem 10.** *Let m be a positive integer, and let a be an integer relatively prime to m. Then there is an integer x for which $ax \equiv 1 \pmod{m}$.*
- **Proof:** Use that there are integers x and y such that $ax + my = 1$.
- **Comments:** The x in Theorem 10 is called the inverse of a modulo m. It is unique modulo m since $(a, m) = 1$ and $ax \equiv ay \mod m$ implies $x \equiv y \pmod{m}$. Also, note that if $(a, m) \neq 1$, then a does not have an inverse modulo m (since $ax - 1 = mk$ would be impossible).
- **Examples.**

(1) Explain the usual tests for divisibility by each of 2, 3, 4, 5, 6, 9, and 11.
(2) What is the last digit of 7^{1000}?
(3) Determine the last digits of the numbers in the sequence $23, 23^{23}, 23^{(23^{23})}, \ldots$.
(4) Is $375274387734528757482790487012848712773 1$ a sum of two squares?
(5) Let $F_n = 2^{(2^n)} + 1$ (the nth Fermat number). Explain why $641|F_5$. Use that $641 = 2^4 + 5^4$ and $641 = 5 \times 2^7 + 1$.

- **Comments:** A regular n-gon is constructible with straight-edge and compass if and only if $n = 2^k p_1 \cdots p_r \geq 3$ where k and r are non-negative integers and $p_1, \ldots, p_r$ are distinct Fermat primes. The only known Fermat primes are F_n for $0 \leq n \leq 4$ (i.e., 3, 5, 17, 257, and 65537), and it is believed that these are the only Fermat primes.

Homework:

(1) Calculate the inverse of 7 modulo 2010. (It may help to look at the proof of Theorem 10.)

(2) Calculate the inverse of 9109 modulo 2732791. (Even if you didn't like the hint on Problem 1, it may help to look at the proof of Theorem 10 here.)

(3) Prove that if $n \equiv 7 \pmod 8$, then n is not a sum of 3 squares.

(4) Prove that for every non-constant polynomial $f(x)$ with integer coefficients, there is an integer m such that $f(m)$ is composite.

(5) A large furniture store sells 6 kinds of dining room suites, whose prices are \$231, \$273, \$429, \$600.60, \$1001, and \$1501.50, respectively. Once a South American buyer came, purchased some suites, paid the total amount due, \$13519.90, and sailed for South America. The manager lost the duplicate bill of sale and had no other memorandum of each kind of suite purchased. Help him by determining the exact number of suites of each kind the South American buyer bought. (Don't forget to show that your solution is unique.)

(6) Prove that if 7 divides the sum of two squares, then 7 divides each of the two squares. In other words, if a and b are integers such that 7 divides $a^2 + b^2$, then show that 7 divides both a and b.

Challenge Problem:

Find (with proof) the smallest integer > 1 dividing at least one number in the sequence $31, 331, 3331, 33331, \ldots$.