Problem Set 4

Due: Tuesday, February 28 at 9 PM in Room 32-044

Problem 1. Prove all of the following statements except for the two that are false; for those, provide counterexamples. Assume $n > 1$. When proving each statement, you may assume all its predecessors.

(a) $a \equiv a \pmod{n}$

(b) $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$

(c) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$

(d) $a \equiv b \pmod{n}$ implies $a + c \equiv b + c \pmod{n}$

(e) $a \equiv b \pmod{n}$ implies $ac \equiv bc \pmod{n}$

(f) $ac \equiv bc \pmod{n}$ implies $a \equiv b \pmod{n}$ provided $c \not\equiv 0 \pmod{n}$.

(g) $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $a + c \equiv b + d \pmod{n}$

(h) $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $ac \equiv bd \pmod{n}$

(i) $a \equiv b \pmod{n}$ implies $a^k \equiv b^k \pmod{n}$ for all $k \geq 0$.

(j) $a \equiv b \pmod{n}$ implies $k^a \equiv k^b \pmod{n}$ for all $k \geq 0$.

(k) $(a \text{ rem } n) \equiv a \pmod{n}$

Problem 2. Prove that there exists an integer k^{-1} such that

$$k \cdot k^{-1} \equiv 1 \pmod{n}$$

provided $\gcd(k, n) = 1$. Assume $n > 1$.

Problem 3. Reviewing the analysis of RSA may help you solve the following problems. You may assume results proved in recitation.

(a) Let n be a nonnegative integer. Prove that n and n^5 have the same last digit. For example:

$$\underline{2}^5 = 3\underline{2} \qquad\qquad 79\underline{5}^5 = 3077056399\underline{5}$$

(b) Suppose that $p_1, \ldots, p_k$ are distinct primes. Prove that

$$m^{1+(p_1-1)(p_2-1)\cdot(p_k-1)} \equiv m \pmod{p_1 p_2 \ldots p_k}$$

for all m and all $k \geq 1$.

Problem 4. Suppose that p is a prime.

(a) An integer k is *self-inverse* if $k \cdot k \equiv 1 \pmod{p}$. Find all integers that are self-inverse mod p.

(b) *Wilson's Theorem* says that $(p-1)! \equiv -1 \pmod{p}$. The English mathematician Edward Waring said that this statement would probably be extremely difficult to prove because no one had even devised an adequate notation for dealing with primes. (Gauss proved it while standing.) Your turn! Stand up, if you like, and try cancelling terms of $(p-1)!$ in pairs.