Mathematics 124 Fall 2003

HOMEWORK ASSIGNMENT # 2
DUE, Friday, October 10

Collaboration: On the homework sets, collaboration is not only allowed but encouraged. However, you must write up and understand your own individual homework solutions, and you may not share written solutions. If you learn how to solve a problem by talking to a classmate, CA, or looking it up in a book, you should cite the source in your homework write-up, just as you would reference your sources in a literature or history class.
Show all your working, and write up your solutions as neatly as possible.

1. (3 points) Let p be prime. Prove that
$$\binom{2p}{p} \equiv 2 \mod p.$$

2. [**Primitive Roots modulo prime powers**] Let p be an odd prime. Let ϵ be an integer that reduces to a primitive root modulo p.
   (a) (3 points) Prove that
   $$(1+p)^p \equiv 1 + p^2 \mod p^3.$$
   (b) (1 point) Prove that
   $$(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \mod p^n,$$
   and that $(1+p)$ has exact order p^{n-1} modulo p^n.
   (c) (1 point) Prove that $\eta := \epsilon^{p^{n-1}}$ satisfies $\eta^{p-1} \equiv 1 \mod p^n$.
   (d) (2 points) Prove that $\eta \equiv \epsilon \mod p$, and deduce that $\eta \mod p^n$ has exact order $p-1$.
   (e) (2 points) It follows from the argument presented in class that $\chi := \eta \times (1+p)$ has order $(p-1)p^{n-1}$ modulo p^n. Using this, show that every integer coprime to p is congruent to $\chi^k \mod p^n$ for some k. We say that χ is a primitive root modulo p^n.
   (f) (1 point) Prove there does not exist a primitive root modulo $8 = 2^3$. What goes wrong above when $p = 2$?

3. Let p be prime, and let k be a positive integer. Let $S = \sum_{a=1}^{p-1} a^k$.
   (a) (2 points) Prove that
   $$S \equiv \sum_{n=0}^{p-2} \epsilon^{nk},$$
   where ϵ is some (any) primitive root modulo p.

(b) (3 points) Prove that $(\epsilon^k - 1)S \equiv 0 \mod p$.

(c) (1 point) If $(p-1)$ does not divide k, deduce that $S \equiv 0 \mod p$.

(d) (1 point) If $(p-1)|k$, prove directly that $S \equiv p - 1 \equiv -1 \mod p$.