Comments on test homework due July 3

2.7.4. One must realize that in the usual polynomial long division algorithm, if $f(x)$ is any polynomial with integer coefficients, and if $h(x)$ is any monic polynomial with integer coefficients, then the quotient and remainder will also have integer coefficients. Most of you used induction, so let me use that approach here. Certainly the result is true if f has $k = 0$ solutions. Suppose we have shown the result whenever a polynomial f has k solutions. Now suppose f has $k+1$ solutions, say, $a_1, a_2, ..., a_k, b$. By induction we have $h(x)$ such that

$$f(x) \equiv (x - a_1)(x - a_2)...(x - a_k)g(x) \bmod p$$

for some polynomial $g(x)$. Since $f(b) \equiv 0 \bmod p$ we have $g(b) \equiv 0 \bmod p$. Now use the usual long division algorithm to find integer polynomials $q(x)$ and $r(x)$ with

$$g(x) = (x - b)q(x) + r(x)$$

But degree of r less than degree of $x - b$ means $r(x)$ is a constant. Plugging in $x = b$, we see that $r(b) \equiv 0 \bmod p$ hence $r(x)$ is the zero polynomial modulo p. Thus,

$$f(x) \equiv (x - a_1)...(x - a_k)(x - b)q(x) \bmod p$$

completing our proof by induction.

2.8.6 First, note the modulus m might be composite, so it is not necessarily prime so we do not have any cyclic group structure.

We will prove the contrapositive. Suppose two of these are congruent, say, $a^i \equiv a^j \bmod m$ for $1 \leq i < j \leq h$. Since $a^h \equiv 1 \bmod m$ it is easy to find inverses, in fact, $a^{-i} \equiv a^{h-i} \bmod m$. Thus, $1 \equiv a^{j-i} \bmod m$ so the order of a modulo m is smaller than h. QED.

2.8.13 Most of you realized that Theorem 2.37 is a natural way to approach this problem, so let me use that approach also.

This is an *if and only if*; first we will prove the *if* via contrapositive.

Suppose that $(k, p-1) = r > 1$. By Theorem 2.37, $x^k \equiv 1 \bmod p$ has either $r > 1$ or zero solutions. But $x = 1$ is a solution hence it must have r solutions with at least one $a > 1$ satisfying $a^k \equiv 1 \bmod p$. but then the set 1^k, 2^k, ..., $(p-i)^k$ has less than $p-1$ elements modulo p so cannot be a complete reduced residue system.

Now we prove the *only if* half via contrapositive.

Suppose the set 1^k, 2^k, ..., $(p-1)^k$ is not a complete residue system. Every term is relatively prime to p so there must exist $i^k \equiv j^k \bmod p$ for some $i \neq j$. Setting $a \equiv i^k \bmod p$, we see that the equation $x^k \equiv a \bmod p$ has at least two solutions. By Theorem 2.37, $(k, p-1) > 1$. QED.