Homework #3. Due Wednesday, February 6th, in class

Reading:

1. For this homework assignment: Sections 3.5 and parts of Chapter 4.

2. For the next two classes: Sections 4.3, 4.1 and 5.1. Also review the definition of the ring of congruence classes $\mathbb{Z}_n$ (see Chapter 3).

Problems:

1. Let p, q and r be distinct primes and let a, b, c be integers. Consider the system of congruences

$$x \equiv a \mod p^3 q; \quad x \equiv b \mod p^2 q^2 r; \quad x \equiv c \mod pq^3.$$

(a) Prove that the system has a solution if and only if $a \equiv b \mod p^2 q$ and $b \equiv c \mod pq^2$.

(b) Let $p = 5, q = 2, r = 3$. Assuming hypotheses of (a) hold, find a formula for the general solution to the system (in terms of a, b and c).

2. Find all solutions mod 30 to the congruence $x^2 \equiv x \mod 30$ making as few computations as possible. In particular, do not solve more than three systems of linear congruences in the course of your proof.

3.

(a) Find the general solution to the congruence $x^3 \equiv 2 \mod 5^3$ using the method introduced in class.

(b) Prove that the congruence $x^4 + x \equiv 7 \mod 5^2$ has no solutions

(c) Prove that for any integer k s.t. $k \equiv 2 \mod 5$, the congruence $x^4 + x \equiv k \mod 5^2$ has either no solutions or more than one solution modulo 5^2.

4. Let p be a prime.

(a) Use Problem 8 from Homework#2 to prove Fermat's little theorem: $x^p \equiv x \mod p$ for any $x \in \mathbb{Z}$.

(b) Deduce from (a) that $x^{p-1} \equiv 1 \mod p$ whenever $gcd(x, p) = 1$.

Note that a completely different proof of these results is given in Section 4.1.

5. Use Problem 4 to prove that $x^{13} \equiv x \mod 70$ for any $x \in \mathbb{Z}$.

6.

(a) Prove that $x^2 \equiv 1 \mod 24$ for any x such that $gcd(x, 24) = 1$.

(b) Let m and k be positive integers such that $gcd(m, k) = 1$. Let $x \in \mathbb{Z}$ be such that $gcd(x, m) = 1$. Prove that there exists $y \in \mathbb{Z}$ such that $y \equiv x \mod m$ and $gcd(y, k) = 1$. Deduce that any such y also satisfies $gcd(y, m) = 1$ and hence also $gcd(y, mk) = 1$. **Hint:** use CRT.

(c) Let S be the set of all positive integers n such that $x^2 \equiv 1 \mod n$ for any x with $gcd(x, n) = 1$ (for instance, $24 \in S$ by (a)). Use (b) to prove that if $n \in S$ and $n = p_1^{a_1} \dots p_k^{a_k}$ with $p_1, \dots, p_k$ distinct primes, then $p_i^{a_i} \in S$.

(d) Prove that if $m = p^k$ where p is prime, then there are precisely $p^{k-1}(p-1)$ integers between 1 and $m = p^k$ which are coprime to p.

(e) Now use (c), (d) and the result of Example 3.18 from the book to prove that 24 is the largest element of S.