Math 3354, Section 2. Fall 2010. First midterm.

1. (7 pts) Find the SMALLEST POSITIVE integer x such that

$$20x \equiv 56 \mod 99$$

Note: You may use any method you like to find the solution, but you should clearly justify why your x is a solution and why it is the smallest positive solution.

2. Consider the relation $\sim$ on $\mathbb{Z}$ given by $x \sim y \iff 4 \mid (x^3 - y^3)$.

(a) (3 pts) Prove that $\sim$ is an equivalence relation. Do not skip steps.

(b) (4 pts) Find the number of distinct equivalence classes with respect to $\sim$ and explicitly describe elements in each class. You do not have to justify your answer but make sure that your answer is clearly stated.

3. In both parts of this problem k, m and n are positive integers such that

$$k \mid (m+n) \text{ and } k \mid (m-n).$$

(a) (4 pts) Assume that k is odd. Prove that $k \mid m$ and $k \mid n$. Clearly justify all the steps. In particular, it should be clear how you use that k is odd.

(b) (2 pts) Prove by an explicit example that if we do not assume that k is odd, then the assertion $k \mid m$ may be false.

4. (5 pts) Define the sequence $\{a_n\}_{n=1}^{\infty}$ by $a_1 = 2$ and $a_{n+1} = 2a_n^2 + 1$ for $n \geq 1$. Prove that

$$a_n \equiv 2 \mod 7 \quad \text{for all} \quad n \in \mathbb{Z}^+.$$

5. (7 pts) Let a, b and c be positive integers. Let

$$d = gcd(a,b) \text{ and } e = gcd(d,c) = gcd(gcd(a,b),c).$$

Prove that

$$e = 1 \iff \text{there exist } u, v, w \in \mathbb{Z} \text{ s.t. } au + bv + cw = 1.$$

Hint: For the forward direction ("$\Rightarrow$") use the GCD Theorem. For the backward direction ("$\Leftarrow$") it may be convenient to do a proof by contradiction.

6. Let R be a commutative ring. An element $a \in R$ is called **nilpotent** if $a \neq 0$, but $a^k = 0$ for some $k \in \mathbb{Z}^+$ (as usual a^k means $\underbrace{a \cdot \ldots \cdot a}_{k \text{ times}}$). For instance, $[6]$ is a nilpotent element in $\mathbb{Z}_{18}$ since $[6] \neq [0]$, but $[6]^2 = [36] = [0]$.

(a) (1 pt) Let $n = p^a$ where p is a prime and $a \geq 2$. Find (explicitly) a nilpotent element in $\mathbb{Z}_n$. You do not have to justify yuor answer.

(b) (3 pts) (generalization of (a)) Let $n \geq 2$, and suppose that there exists a prime p such that $p^2 \mid n$. Find a nilpotent element $[x] \in \mathbb{Z}_n$ and prove that your element $[x]$ is indeed nilpotent.

(c) (4 pts) Now suppose that $n \in \mathbb{Z}^+$ is not divisible by p^2 for any prime p (by UFT, this is equivalent to saying that $n = p_1 \dots p_k$ where $p_1, \dots, p_k$ are distinct primes). Prove that $\mathbb{Z}_n$ has no nilpotent elements.