Math 342 Problem set 3 (due 27/9/11)

The natural numbers

1. Using the division Theorem, prove that if a,b are two non-zero integers then every common multiple of a,b is divisible by the least common multiple $[a,b]$.
   Hint: Show that the remainder obtained when dividing one common multiple by another is also a common mulitple.

2. Prove Bezout's Theorem as follows: Given $a,b \in \mathbb{Z}$ not both zero let $I = \{xa+by \mid x,y \in \mathbb{Z}\}$. Show that the smallest positive member of I is the gcd of a,b.
   Hint: You need to show that I has positive members. To show that the number your produced divides a and b use the idea of problem 1.

Using Euclid's Algorithm

DEFINITION. We say that two integers a,b are *relatively prime* (or *coprime*) if $(a,b) = 1$.

3. For every integer n show that n and $n+1$ are relatively prime.

4. Find the gcd of 98 and 21 using subtractions only (list your intermediate steps).

5. (§3A.E7) Improving Euclid's algorithm with the idea of the previous problem, find the gcd of 21063 and 43137, listing your intermediate steps (you may want to use a calculator). How many remainders did you calculate?

Using Bezout's Theorem

6.
   (a) Using Euclid's Algorithm, find integers r,s such that $12r+17s = 1$.
   (b) Find integers m,n such that $12m+17n = 8$.
   (c) You take a 12-quart jug and a 17-quart jug to a stream. How would you bring back exactly 8 quarts of water?

The efficiency of Euclid's Algorithm

Let $a > b > 0$ be two integers, and let $0 = r_0 < r_1 < r_2 < \cdots < r_{T-1}$ be the remainders calculated by the improved algorithm of problem 4 (starting with a,b), *in reverse order*. In other words, $r_0 = 0$ is the remainder of the final, exact, division of r_2 by r_1. r_1 is the remainder when dividing r_3 by r_2 and so on, all the way to r_{T-1} which is the remainder of dividing a by b (which we denote r_T). Note that T is the number of divisions performed during the run.

Let $\{a_n\}_{n=0}^{\infty}$ be the Fibonacci sequence from Problem Set 2.

7. Prove by induction on n that, for $0 \le n \le T$, we have $a_n \le r_n$.
   Hint: For the induction step, express r_{n+1} using r_n, r_{n-1} and the quotient in the division, and use the defining property of the Fibonacci sequence.

8. The case $n = T$ of what you just proved reads: $a_T \leq b$. In the previous problem set you showed that for $T \geq 1$, $a_T \geq \frac{1}{3}R^T$ where $R = \frac{1+\sqrt{5}}{2}$. Conclude that, when running the improved algorithm on (a,b) one needs at most $C \log b + D$ divisions, where C, D are two constants. What are C, D?

Solving congruences

9. For each $a \in \{0,1,2\}$ find all $x \in \mathbb{Z}$ such that x^2 leaves remainder a when divided by 3.
Hint: first show that the remainder of x^2 only depends on that of x, and then divide into cases based on the latter remainder.