Math 105, Fall 2010, HW1

1. Prove the following statements for positive integers x, y:
   (a) If x, y are both even, then $\gcd(x, y) = 2 \cdot \gcd(x/2, y/2)$.
   (b) If x is even and y is odd, then $\gcd(x, y) = \gcd(x/2, y)$.
   (c) If x and y are both odd and $x > y$, then $\gcd(x, y) = \gcd((x - y)/2, y)$.
2. Develop these facts into a general gcd algorithm for positive integers.
3. Prove a complexity estimate for your algorithm that shows that this "binary" gcd rivals Euclid's gcd algorithm.
4. Can you find a way to extend this new gcd algorithm to finding integers a, b with $\gcd(x, y) = ax + by$?
5. Let $\varphi(n)$ denote Euler's function at n, namely the order of the unit group of $(\mathbb{Z}/n\mathbb{Z})^*$. We know that φ is multiplicative and that $\varphi(p^k) = (p-1)p^{k-1}$ for primes p and positive integers k. Prove that $\varphi(n) > \sqrt{n}$ for $n > 6$.
6. Let R be a ring (commutative with 1) and let $f, g \in R[x]$ with f monic. Prove that there are unique $q, r \in R[x]$ with $g = qf + r$ and either $r = 0$ or $\deg r < \deg f$.