Number Theory for Beginners Ma3 2007 **Homework 1**

Instructions: Credit on homework assignments will only be given for proofs. For example, in question 1, it is required to state a year, prove that it is a prime, and prove that there is no sooner year that is prime.

Due: Thursday April 19, 5pm.

1. When is the next prime year?

2. Decompose 5084 as a product of primes. Show that for any number (= positive integer) n at most $\sqrt{n}$ computations are needed to test if n is prime.

3. Write out a computation of the highest common factor of 114 amd 20 using the Euclidean Algorithm. Use it to write $2 = 114x - 20y$ for some positive integers x and y.

4. Show that $(a, b)\{a, b\} = ab$, i.e. the product of the highest common factor and least common multiple of two numbers is equal to their product.

5. Show that for any number n there are n consecutive composite numbers. Is this true with 'composite' replaced by 'prime'?

6. Suppose P is a set of size p and $1 \leq q \leq p$. How many subsets of size q does P have? If p is prime show that this number is divisible by p. Is this true with 'prime' replaced by 'composite'? If p is prime, show by induction on n that $n^p - n$ is divisible by p.

7. Suppose we apply the Euclidean Algorithm to the pair (a, b) and it takes t steps. For $0 \leq i \leq t$ let (a_i, b_i) be the pair obtained after i steps. Show that $a_{i+1}b_{i+1} < a_i b_i/2$ for $0 \leq i \leq t-1$. Deduce that the algorithm needs at most $\log_2 a + \log_2 b$ steps. Give an infinite sequence of pairs (a, b) for which the algorithm takes at least $\frac{1}{10}(\log_2 a + \log_2 b)$ steps.