Homework Assignment 5

Due **Friday 27-02-04**

We say that a number n is equivalent to r *mod* m (written $n \equiv r \bmod m$) if and only if $n - r = mq$ for some q. In particular if r is the remainder of the division of n by m, (i.e., $n = mq + r$ with $0 \leq r < m$) then $n \equiv r \bmod m$.

1. (i) Show that if m and n are both equivalent to 1 mod 4, then so is $m \cdot n$. (In other words, if $m = 4k + 1$ and $n = 4k' + 1$ for some k, k', then $m \cdot n = 4k'' + 1$ for some k''.)

(*1 point*)

(ii) Show that there are infinitely many primes of the form $4n - 1$.

Hint for (ii): Modify the proof of Euclid's theorem. Write q_n for the n-th prime of the form $4k - 1$. What is q_1? For the inductive step, suppose $q_1, \ldots, q_n$ were all the prime numbers of the form $4k - 1$. Let $c = 4(q_1 \cdot \ldots \cdot q_n) - 1$ and derive a contradiction by showing that c must be divided by one of the primes $q_1, \ldots, q_n$. Notice that to reach this conclusion you need to consider all possible divisors of c : first show that c is not divisible by 2; next, since odd numbers are either of the form $4k + 1$ or of the form $4k - 1$, show that the prime divisors of c cannot be only of the form $4k + 1$.

(*3 points*)

(iii) Suppose in the inductive step you let $c = 4(q_n!) - 1$. Does the argument still hold?

(*1 point*)

2. Define a finite state automaton M on the alphabet $A = \{0, 1\}$ which accepts a word w if and only if w is the binary representation of a number divisible by 5, (e.g., 1010).

(*5 points*)

Hint: The machine M reads from left to right the digits of the binary representation and remembers the value of what it has read so far, but only as a number k mod 5. If a string w is the binary representation of a number equivalent to k mod 5, what are the values mod 5 of the strings $w0$ and $w1$?

3. Consider the language $\mathcal{L}$ on the alphabet $A = \{0\}$ defined by

$$\{0^n \mid n \text{ is a perfect square. }\}$$

(We say that n is a perfect square if $n = m^2$, for some $m \in \mathbf{N}$.) Show that there is no automaton that accepts exactly the language $\mathcal{L}$ (i.e., $\mathcal{L}$ is not a *regular* language).

(*5 points*)

Hint: Let M be a deterministic automaton which accepts all the words in $\mathcal{L}$, let n be the number of states in M and consider the word $w = 0^{n^2}$, i.e., the word consisting of n^2 symbols 0. Show that M must also accept a word $w' = 0^m$ such that $n^2 < m < (n+1)^2$, i.e., a word which not in $\mathcal{L}$.