Lab01-Proof

CS363-Computability Theory, Xiaofeng Gao, Spring 2016

$*$ Please upload your assignment to TA's FTP. Contact nongeek.zv@gmail.com for any questions.

$*$ Name:________ StudentId: ________ Email: ________

1. Prove that for any integer $n > 2$, there is a prime p satisfying $n < p < n!$. (Hint: consider a prime factor p of $n! - 1$ and use proof by contradiction)
2. Use minimal counterexample principle to prove that: for every integer $n > 17$, there exist integers $i_n \geq 0$ and $j_n \geq 0$, such that $n = i_n \times 4 + j_n \times 7$.
3. Suppose $a_0 = 1$, $a_1 = 2$, $a_2 = 3$, $a_k = a_{k-1} + a_{k-2} + a_{k-3}$ for $k \geq 3$. Use strong principle of mathematical induction to prove that $a_n \leq 2^n$ for all integers $n \geq 0$.
4. Consider the following loop, written in pseudocode:

```
while B do
  | S;
end
```

A condition P is called an invariant of the loop if whenever P and B are both true, and S is executed once, P is still true.

(a) Prove that if P is an invariant of the loop, and P is true before the first iteration of the loop, then if the loop eventually terminates (i.e., after some number of iterations, B is false), P is still true.

(b) Suppose x and y are integer variables, and initally $x \geq 0$ and $y > 0$. Consider the following program fragment:

```
q = 0;
r = x;
while r ≥ y do
  | q = q + 1;
  | r = r − y;
end
```

By considering the condition $(r \geq 0) \wedge (x = q \times y + r)$, prove that when this loop terminates, the values of q and r will be the integer quotient and remainder, respectively, when x is divided by y; in other words, $x = q \times y + r$ and $0 \leq r < y$.