Lab00-Proof

CS214-Algorithm and Complexity, Xiaofeng Gao, Spring 2019.

* If there is any problem, please contact TA Jiahao Fan.
* Name: Weiqi Feng Student ID: 517021910752 Email: fengweiqi@sjtu.edu.cn

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 prove by contradiction)

Proof.

(i) **Claim 1.1:** For any integer $n > 2$, $n! - 1 > n$.
Since $n > 2$, n and 2 are two distinct factors in $n!$. This gives us an inequality that

$$n! \geq 2n = n + n > n + 1$$

which in turn is equivalent to

$$n! - 1 > n$$

Claim 1.2: $\forall n \in \mathbb{N}$ with $n \geq 2$, it has prime factorizations.
This claim has already been proved in slides*, so we omit the proof of it.

(ii) Since $n! - 1 > n > 2$, the number $n! - 1$ must have a factor p that is a prime. Since p is a divisor of $n! - 1$, this gives us one of the inequalities we need

$$p \leq n! - 1 < n!$$

(iii) To show the other one, suppose for the sake of contradiction that $p \leq n$. Since p in a positive integer less than or equal to n, p is also a factor of $n!$. However, if p is both a factor of $n!$ and $n! - 1$, p has to be a factor of 1, which contradicts the fact that n is a prime.
Therefore, the assumption of $p \leq n$ leads to a contradiction, and we can conclude that $n < p < n!$.

□

2. Use the minimal counterexample principle to prove that for any integer $n > 17$, there exist integers $i_n \geq 0$ and $j_n \geq 0$, such that $n = i_n \times 4 + j_n \times 7$.

Proof.

(i) **Defination 2.1:** $P(n)$: there exist integers $i_n \geq 0$ and $j_n \geq 0$, such that $n = i_n \times 4 + j_n \times 7$.
Firstly, we show the base case when $17 < n < 22$, $P(n)$ is true. For nonnegative integers i and j, such that

$$18 = 1 \times 4 + 2 \times 7$$
$$19 = 3 \times 4 + 1 \times 7$$
$$20 = 5 \times 4 + 0 \times 7$$
$$21 = 0 \times 4 + 3 \times 7$$

Now if it is not true that $P(n)$ is true for every $n > 17$, then there are values of n greater than 17 for which $P(n)$ is false, and therefor there must be a smallest such value, say $n = k$. Since we have verified $P(n)$ from 18 to 21, k must be at least 22.

*Xiaofeng Gao. (2019). Prologue and Notation [Powerpoint slides].

(ii) Therefore, $k-4$ is at least 18, and since k is the smallest value for which P fails, $P(k-4)$ is true. This means that

$$k-4 = i_{k-4} \times 4 + j_{k-4} \times 7$$

Then, however,

$$k = k-4+4 = (i_{k-4}+1) \times 4 + j_{k-4} \times 7$$

According to the definition of $P(n)$, $P(k)$ is true. We have derived a contradiction, which allows us to conclude that our original assumption is false. Therefore, $P(n)$ is true for every $n > 17$.

□

3. Suppose $a_0 = 1$, $a_1 = 2$, $a_2 = 3$, and $a_k = a_{k-1} + a_{k-2} + a_{k-3}$ for $k \geq 3$. Use the strong principle of mathematical induction to prove that $a_n \leq 2^n$ for any integer $n \geq 0$.

Proof.

- **Basic Step.** Firstly, we show that $a_n \leq 2^n$ for $0 \leq n \leq 2$ is true.

$$a_0 = 1 \leq 2^0$$

$$a_1 = 2 \leq 2^1$$

$$a_2 = 3 \leq 2^3$$

- **Induction hypothesis.** $k \geq 2$ and for every n with $2 \leq n \leq k$, $a_n \leq 2^n$.
- **Statement to be shown in induction step.** $a_{k+1} \leq 2^{k+1}$ for $k \geq 2$.
- **Proof of induction step.** According to the condition $k \geq 2$, which is equivalent to $k+1 \geq 3$, this gives us the inequality we need

$$a_{k+1} = a_k + a_{k-1} + a_{k-2} \leq 2^k + 2^{k-1} + 2^{k-2} < 2^k + 2 \cdot 2^{k-1} = 2^{k+1}$$

Therefore, we can conclude that $a_n \leq 2^n$ for any integer $n \geq 0$.

□

4. Prove, by mathematical induction, that

$$(n+1)^2 + (n+2)^2 + (n+3)^2 + \cdots + (2n)^2 = \frac{n(2n+1)(7n+1)}{6}$$

is true for any integer $n \geq 1$.

Proof.

- **Basic step.** Firstly, we show that when $n = 1$, the equation above is true

$$(1+1)^2 = 4 = \frac{24}{6} = \frac{1 \times (2 \times 1 + 1) \times (7 \times 1 + 1)}{6}$$

- **Induction hypothesis.**

$$k \geq 1 \text{ and } (k+1)^2 + (k+2)^2 + (k+3)^2 + \cdots + (2k)^2 = \frac{k(2k+1)(7k+1)}{6}$$

- **Statement to be shown in induction step.**

$$((k+1)+1)^2+((k+1)+2)^2+((k+1)+3)^2+\cdots+(2(k+1))^2 = \frac{(k+1)(2(k+1)+1)(7(k+1)+1)}{6}$$

- **Proof of induction step.**

$$\begin{aligned}
((k+1)+1)^2+\cdots+(2(k+1))^2 &= (k+2)^2+\cdots+(2k+2)^2 \\
&= (k+1)^2+\cdots+(2k)^2+(2k+1)^2+(2k+2)^2-(k+1)^2 \\
&= \frac{k(2k+1)(7k+1)}{6}+7k^2+10k+4 \\
&= \frac{14k^3+51k^2+61k+24}{6} \\
&= \frac{k(14k^2+37k+24)+(14k^2+37k+24)}{6} \\
&= \frac{(k+1)(14k^2+37k+24)}{6} \\
&= \frac{(k+1)(2k+3)(7k+8)}{6} \\
&= \frac{(k+1)(2(k+1)+1)(7(k+1)+1)}{6}
\end{aligned}$$

$\square$

Remark: You need to include your .pdf and .tex files in your uploaded .rar or .zip file.