Lab00-Proof

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

∗ Name:史天尧 Student ID:517021910623 Email: sthowling@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.

Lemma 1. *Two adjacent natural numbers are co-prime.*

Proof. Consider that the two adjacent natural numbers are n and $n+1$. If they are not co-prime, then they must have a common divisor other than 1, say a postive integer a. Therefore we have

$$n = ap, \quad n + 1 = aq,$$

where p and q are intergers, and since $n + 1 > n$, $a > 0$, we have that $q > p$, which is equivalent as $q - p \geq 1$. Consequently,

$$\begin{aligned} n + 1 - n &= aq - ap, \\ 1 &= a(q - p), \end{aligned}$$

where $q - p \geq 1$. Therefore we derive that a equals 1, which is in contradiction with the assumption. We can conclude that the original assumption is false. □

With Lemma (1), we know that $n!$ and $n! - 1$ are co-prime. Except for 1, they do not have any common divisor.

Assume that for any integer $n > 2$, there is not a prime p satisfying $n < p < n!$, i.e. no integer between n and $n!$ is a prime. Thus $n! - 1$ has at least one prime factor, which is not itself in this case. Moreover, all natural numbers that are not larger than n are divisors of $n!$, and none of them is divisor of $n! - 1$, since $n!$ and $n! - 1$ are co-prime. Therefore a prime factor of $n! - 1$ must be larger than n, which means there is a prime p satisfying $n < p < n!$. We have derived a contradiction, which allows us to conclude that our original assumption is false. □

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. Define $P(n)$ be the statement that "there exist integers $i_n \geq 0$ and $j_n \geq 0$, such that $n = i_n \times 4 + j_n \times 7$". If $P(n)$ is not true for every $n > 17$, then there are values for which $P(n)$ is false, and there must be a smallest value, say $n = k$.

Since $18 = 1 \times 4 + 2 \times 7$, i.e. $P(18)$ is true, we have $k \geq 19$ and $k - 1 \geq 18$.

Since k is the smallest value for which $P(k)$ is false, $P(k-1)$ is true, i.e. $k-1 = i_k \times 4 + j_k \times 7$, where $i_k, j_k \in \mathbb{N}$. We can derive that

$$\begin{aligned} k = k - 1 + 1 &= i_k \times 4 + j_k \times 7 + 1 \\ &= i_k \times 4 + j_k \times 7 + (2 \times 4 - 1 \times 7) \\ &= (i_k + 2) \times 4 + (j_k - 1) \times 7. \end{aligned}$$

When $j_k \geq 1$, $j_k - 1 \geq 0$, we have that $P(k)$ is true.

When $j_k = 0$, since $k-1 \geq 18$, we have $i_k \geq 5$, as $k-1$ now is divisible by 4, and the smallest possible value of $k-1$ is 20.

Therefore in this case,

$$\begin{aligned} k = k-1+1 &= i_k \times 4 + (3 \times 7 - 5 \times 4) \\ &= (i_k - 5) \times 4 + 3 \times 7. \end{aligned}$$

Since $i_k \geq 5$, $i_k - 5 \geq 0$. This means that $P(k)$ is true.

In conclusion, we have derived a contradiction, which allows us to conclude that our original assumption is false. □

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. Define $P(n)$ be the statement that $a_n \leq 2^n$.

Basis step: When $n = 0$, $a_0 = 1 \leq 2^0$. $P(0)$ is true.

When $n = 1$, $a_1 = 2 \leq 2^1$. $P(1)$ is true.

When $n = 2$, $a_2 = 3 \leq 2^2$. $P(2)$ is true.

Induction hypothesis: Assume that for some $k \geq 2$ and for any n satisfying $2 \leq n \leq k$, $P(n)$ is true.

Proof of induction step: Now let us prove $P(k+1)$.

When $n = k+1$, $a_{k+1} = a_k + a_{k-1} + a_{k-2}$. From the hypothesis, we know that $a_k \leq 2^k$, $a_{k-1} \leq 2^{k-1}$, and $a_{k-2} \leq 2^{k-2}$. Therefore we have

$$\begin{aligned} a_{k+1} &= a_k + a_{k-1} + a_{k-2} \\ &\leq 2^k + 2^{k-1} + 2^{k-2} \\ &\leq 2^k + 2^{k-1} + 2^{k-1} = 2^k + 2^k = 2^{k+1}. \end{aligned}$$

□

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. Define $P(n)$ be the statement that

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

We will try to prove that $P(n)$ is true for every $n \geq 1$.

Basis step: When n equals 1, $1+1 = 2 \times 1 = 2$. We have

$$2^2 = 4 = 1 \times (2 \times 1 + 1) \times (7 \times 1 + 1) \div 6,$$

so $P(1)$ is true.

Induction hypothesis: Assume that $P(k)$ is true for some $k \geq 1$. Then we have $(k+1)^2 + (k+2)^2 + (k+3)^2 + \cdots + (2k)^2 = k(2k+1)(7k+1)/6$.

Proof of induction step: Now let us prove that $P(k+1)$ is true.

$$
\begin{aligned}
&(k+1+1)^2 + (k+1+2)^2 + (k+1+3)^2 + \cdots + (2k)^2 + (2k+1)^2 + (2(k+1))^2 \\
=&(k+1)^2 + (k+2)^2 + (k+3)^2 + \cdots + (2k)^2 + (2k+1)^2 + (2k+2)^2 - (k+1)^2 \\
=&\frac{k(2k+1)(7k+1)}{6} + (2k+1)^2 + 3(k+1)^2 \\
=&\frac{k(2k+1)(7k+1) + 6(2k+1)^2 + 18(k+1)^2}{6} \\
=&\frac{(2k+1)(7k^2+k+12k+6) + 18(k+1)^2}{6} \\
=&\frac{(2k+1)(7k+6)(k+1) + 18(k+1)^2}{6} \\
=&\frac{(k+1)(14k^2+21k+6+18k+18)}{6} \\
=&\frac{(k+1)(2k+3)(7k+8)}{6} \\
=&\frac{(k+1)(2(k+1)+1)(7(k+1)+1)}{6}
\end{aligned}
$$

$\square$