Workshop Specification and Testing, Week 5

Further Exercises with Induction

---

1. The *gossip problem* is the following. N people each have a secret. How many phone calls are needed to ensure that everyone knows all secrets? Assume that during any call, the two persons in the call share all secrets they know. Clearly, if there are two people, one call is enough. Similarly, if there are three people a, b, c, the following procedure works: a calls b, so both know the secrets of a and b. Next b calls c, so b knows all secrets and c knows the secrets of b, c. Finally c calls a. As a result a, b also know all secrets. So 3 calls are enough. Prove the following by induction: for $N \geq 4$ it holds that $2(N-2)$ calls are enough to ensure that everyone knows all secrets.

Answer:

First take the case of 4 agents a, b, c, d. Let a call b, then c call d, then a call c and finally b call d. After this, they all know all secrets. So $4 = 2(4-2)$ calls are enough, and the property holds for the base case.

Next assume that the property holds for the case of N people, that is, the gossip problem for N people can be solved in $2(N-2)$ calls. Let x be a new person. Proceed as follows. First x calls one of the N people to exchange their secrets. Next follow the gossip procedure for N people in $2(N-2)$ calls, while making sure that the secret of x gets known to all others. Finally, the person that receives the last call in this procedure calls x and tells her all he knows. This ensures that everyone in the group of $N+1$ persons knows all secrets. The total number of calls is $2 + 2(N-2) = 2((N+1)-2)$. Done.

---

2. Prove by induction that the following definition of the Extended Euclidean algorithn is correct:

```
fctGcd :: Integer -> Integer -> (Integer,Integer)
fctGcd a b =
  if b == 0
  then (1,0)
  else
     let
       (q,r) = quotRem a b
       (s,t) = fctGcd b r
     in (t, s - q*t)
```

Explanation: the extended algorithm is supposed to compute two integers x, y with the property that $xa + yb = \gcd(a, b)$, where a, b are the input to the function.

Answer:

1. Suppose $b = 0$. Then the gcd of a and b is a, and indeed $a = 1a + 0b$.

2. Suppose $b > 0$. Assume that for $0 \leq m < n \leq b$ it holds that fctGcd n m yields (x, y) with $\gcd(n, m) = xn + ym$. Now let q, r be such that $a = qb + r$. We may suppose, by the induction hypothesis, that fctGcd b r yields (s, t) with $\gcd(b, r) = sb + tr$. From $a = qb + r$ we get that $r = a - qb$. Since $\gcd(a, b) = \gcd(b, r)$ we have that $\gcd(a, b) = \gcd(b, r) = sb + t(a - qb) = ta + (s - qt)b$. So t and $(s - qt)$ are the required integers. Done.

---

3. Prove with induction that $(1 - \frac{1}{4})(1 - \frac{1}{9}) \cdots (1 - \frac{1}{n^2}) = \frac{n+1}{2n}$.

Answer:

Basis: $n = 2$ We have $(1 - \frac{1}{2^2}) = (1 - \frac{1}{4}) = \frac{2+1}{2^2} = \frac{3}{4}$.

Induction step: Suppose $(1 - \frac{1}{4})(1 - \frac{1}{9}) \cdots (1 - \frac{1}{n^2}) = \frac{n+1}{2n}$ We have to show that $(1 - \frac{1}{4})(1 - \frac{1}{9}) \cdots (1 - \frac{1}{n^2})(1 - \frac{1}{n+1^2}) = \frac{n+2}{2n+2}$.

We have

$$(1 - \frac{1}{4})(1 - \frac{1}{9}) \cdots (1 - \frac{1}{n^2})(1 - \frac{1}{n+1^2}) =$$

(induction hypothesis)

$$= \frac{n+1}{2n}(1 - \frac{1}{n+1^2}) = \frac{n+1}{2n} - \frac{n+1}{2n(n+1)} = \frac{(n+1)^2}{2n(n+1)} - \frac{1}{2n(n+1)} = \frac{n^2+2n}{n(2n+2)} = \frac{n+2}{2n+2}.$$

Done.

---

4. In an earlier workshop we have seen the match removal game for two players. situation: a number of matches is on a stack. The players take turns. A move consists in removing 1, 2 or 3 matches from the stack. The player who can make the last move (the move that leaves the stack empty) has won the game. Suppose there are $4N$ matches on the stack, and the other player moves. Then if the player takes x matches, you should take $4 - x$ matches. Now consider the following variation: you can take 1, 3

or 4 matches. The player who takes the last match(es) wins. Prove by induction that now the configurations with $7N$ or $7N + 2$ matches and the other player moving are sure wins. Explain what the winning strategy is.

Answer:

Base case: $N = 0$ and the other person moves. Then there are 2 matches still on the table. So the player has to take a single match and you can take the last match. You win.

Suppose a configuration with $7N$ or $7N + 2$ and the other player moving is a win for you. Now assume we are in the case $7(N+1) = 7N+7$ or $7(N+1)+2 = 7N+9$.

Distinguish several cases:

- Case $7N + 7$ and the other takes 1 match. You take 4 matches and you are in case $7N + 2$ with the other player moving. A win for you by the induction hypothesis.
- Case $7N + 7$ and the other takes 3 matches. You take 4 matches and you are in case $7N$ with the other player moving. A win for you by the induction hypothesis.
- Case $7N + 7$ and the other takes 4 matches. You take 3 matches and you are in case $7N$ with the other player moving. A win for you by the induction hypothesis.
- Case $7N + 9$ and the other takes 1 match. You take one match, and you are in case $7N + 7$ with the other player moving. Act as in the three above cases for a sure win.
- Case $7N + 9$ and the other takes 3 matches. You take 4 matches and you are in case $7N + 2$ with the other player moving. A win for you by the induction hypothesis.
- Case $7N + 9$ and the other takes 4 matches. You take 3 matches and you are in case $7N + 2$ with the other player moving. A win for you by the induction hypothesis.

So you cannot fail to win, which was to be proved.

---

5. Prove that every integer $N \geq 12$ can be written as $4X + 5Y$, with X, Y integers ≥ 0. (Application: if you have supplies of 4-packs and 5-packs of some item, then you can sell any number of items ≥ 12 without ever having to open a pack.)

Answer:

Base case: $N = 12$. This can be written as $4 \cdot 3 + 5 \cdot 0$, so the property holds for the base case.

Induction step. Assume $N = 4X + 5Y$ for some integers X, Y both ≥ 0. Consider the case $N + 1$.

Case 1. $N = 4X + 5Y$ with $X > 0$. In this case $N + 1$ can be written as $4(X - 1) + 5(Y + 1)$. Just replace one 4-pack by a 5-pack. So the property holds for this case.

Case 2. $N = 5Y$. Then we know by the fact that $N \geq 15$ that $Y \geq 3$. In this case $N + 1$ can be written as $4 \cdot 4 + 5(Y - 3)$. So the property holds for this case too.

Done.

---

6. Prove that every integer $N \geq 60$ can be written as $6X + 11Y$, with X, Y integers ≥ 0.

Answer:

The reasoning is very similar to our solution to the previous problem.

Base case: $N = 60$. This can be written as $6 \cdot 10 + 11 \cdot 0$, so the property holds for the base case.

Induction step. Assume $N = 6X + 11Y$ for some integers X, Y both ≥ 0. Consider the case $N + 1$.

Case 1. $N = 6X + 11Y$ with $Y > 0$. In this case $N + 1$ can be written as $6(X + 2) + 11(Y - 1)$. So the property holds for this case.

Case 2. $N = 6X$. Then we know by the fact that $N \geq 60$ that $X \geq 10$. In this case $N + 1$ can be written as $6(X - 9) + 11 \cdot 5$, because $11 \cdot 5 = 6 \cdot 9 + 1$. So the property holds for this case too.

Done.

---

7. The Fibonacci numbers are given by the following recursion:

$$F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n \text{ for } n \geq 0.$$

Prove with induction that for all $n > 1$: $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

Answer:

Recall: $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2$, and so on.

Base case: $n = 2$. In this case we have $F_3F_1 - F_2^2 = 2 - 1 = 1 = (-1)^2$. So the property holds for the base case.

Induction step: Assume (induction hypothesis) that $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$. We have to show $F_{n+2}F_n - F_{n+1}^2 = (-1)^{n+1}$.

The method is to replace F_{n+2} by its definition $F_{n+1} + F_n$, as follows.

$F_{n+2}F_n - F_{n+1}^2 = (F_{n+1} + F_n)F_n - F_{n+1}^2 = F_n^2 + F_{n+1}(F_n - F_{n+1}) =$

(now replace one occurrence of F_{n+1} by $F_n + F_{n-1}$)

$= F_n^2 + F_{n+1}(F_n - (F_n + F_{n-1})) = F_n^2 - F_{n+1}F_{n-1} = -1(F_{n+1}F_{n-1} - F_n^2) =$

(now we can apply the induction hypothesis)

$= -1(-1)^n = (-1)^{n+1}$.

Done.

---

8. The Tower of Hanoi is a tower of 8 disks of different sizes, stacked in order of decreasing size on a peg. Next to the tower, there are two more pegs. The task is to transfer the whole stack of disks to one of the other pegs (using the third peg as an auxiliary) while keeping to the following rules:

(i) move only one disk at a time,

(ii) never place a larger disk on top of a smaller one.

Answer the following questions.

- How many moves does it take to completely transfer a tower consisting of n disks?
- Prove by mathematical induction that your answer to the previous question is correct.
- How many moves does it take to completely transfer the tower of Hanoi?

Answer:

- $2^n - 1$ moves.
- Assume that A is the source peg, B the auxiliary peg, and C the destination peg. We show by induction on n that $2^n - 1$ moves suffice for transferring a Hanoi tower of n disks, and that transfer in less than $2^n - 1$ moves is impossible.
- – Basis: Transferring a tower with no disks takes no moves at all.
- – Induction step: Assume that it takes $2^n - 1$ moves to transfer a Hanoi tower of n disks. We have to show that it takes $2^{n+1} - 1$ moves to transfer a tower of $n + 1$ disks. As induction hypothesis we assume

that n disks can be moved in $2^n - 1$ moves, but not in less than that. Then to move the largest disk from A to C, all other disks must be stacked on B. By the induction hypothesis this can be done in $2^n - 1$, and not in less than $2^n - 1$ moves. Next, it takes one move to get the largest disk from A to C. Notice that this disk cannot go anywhere else, for peg B is occupied by the stack $[1..n]$. Finally, n disks have to be moved from B to C; again this can be done in $2^n - 1$, and not in less than $2^n - 1$ moves. This proves that, all in all, the optimal transfer procedure takes exactly $(2^n - 1) + 1 + (2^n - 1) = 2^{n+1} - 1$ moves.

- $2^8 - 1 = 255$ moves.