1. (30 points)
   This exercise is regarding a real bug, the *Zune bug*, caused by a piece of code in Microsoft’s Zune player, which takes an integer representing days and finds the corresponding year.

   Find the bug using Dafny (see attached file zune.dfy). And fix the code (if you use any source on the internet, you must cite the source). And prove that the code terminates using Dafny.

   Note: The IsLeapYear() method has not been implemented. Its implementation is not important for termination.

   Submit a hardcopy print-out of your final program and also send your file by email.

   Solution: Posted on website.

2. (20 points)
   Let $(L, \sqsubseteq, \sqcup, \sqcap, 0, 1)$ be a lattice. Let $f : L \to L$ be a monotonic function.

   Let $a \in L$ with $f(a) \sqsubseteq a$. Prove, formally, that:

   - For every $n \in \mathbb{N}$, $f^n(a) \sqsubseteq a$.
   - Assume that $p$ is a fixed point of $f$ and $p \sqsubseteq a$, and also assume that $f^m(a) = f^{m+1}(a) = r$, for a particular $m \in \mathbb{N}$. Then prove that $p \sqsubseteq r$.

   Solution:

   - We will prove by induction on $n \in \mathbb{N}, n > 0$ that $f^n(a) \sqsubseteq a$.
     
     **Base case:** When $n = 1$, $f(a) \sqsubseteq a$, follows from the assumption.
     
     **Induction step:** Let $n > 1$.
     
     Let us assume the induction hypothesis:
     
     For every $i$, $1 \leq i < n$, $f^i(a) \sqsubseteq a$.
     
     By induction hypothesis, we know $f^{n-1}(a) \sqsubseteq a$ (since $1 \leq n-1 < n$).
     
     By monotonicity of $f$, $f(f^{n-1}(a)) \sqsubseteq f(a)$.
     
     Since $f(a) \sqsubseteq a$, it follows that $f^n(a) \sqsubseteq a$. QED.

   - We prove by induction on $n$ that $p \sqsubseteq f^n(a)$ for every $n \in \mathbb{N}, n > 0$.
     
     This will prove that $p \sqsubseteq r$, since $r = f^{m+1}(a)$.
     
     **Base case:** $n = 1$.
     
     Since $p \sqsubseteq a$, by monotonicity of $f$, it follows that $f(p) \sqsubseteq f(a)$. Since $p$ is a fixed point of $f$, $f(p) = p$. Hence $p \sqsubseteq f(a)$.
     
     **Induction step:** Let $n > 1$.
     
     Let us assume the induction hypothesis:
     
     For every $i$, $1 \leq i < n$, $p \sqsubseteq f^i(a)$.
     
     By induction hypothesis, we know $p \sqsubseteq f^{n-1}(a)$ (since $1 \leq n-1 < n$).
By monotonicity of $f$, $f(p) \subseteq f(f^{n-1}(a))$. Since $p$ is a fixed point, $f(p) = p$. Hence $p \subseteq f^n(a)$. QED.

3. (30 points)
We are exploring predicate abstraction in this exercise.
Assume a program has a single variable $x$.
Assume we track three predicates:
$p_1$: true iff $x$ is multiple of 8
$p_2$: true iff $x$ is multiple of 2
$p_3$: true iff $x = 0$

Describe accurate abstract transformers for the following operations:

- $x := c$; (where $c$ is a constant)
- $x := 2 \times x$
- $x := 4 \times x$

For each of the statements above, you need to give a sequence of statements that update the value of $p_1$, $p_2$, $p_3$ that best reflect the effect of the concrete semantics of the above statements.

Finally, analyze the following program by describing the value of the predicates after each of these statements, and argue what we can know from the abstract analysis after the end of the following program:

```
x := 1;
x := 2 \times x;
x := 4 \times x;
x := 2 \times x;
```

Solution:

Below, $\star$ means "true/false".

The abstract transformer for $x := c$ is:

- Update of $p_1$:
  If $c$ is a multiple of 8 then
  
  $p_1' = true$
  else
  
  $p_1' = false$

- Update of $p_2$:
  If $c$ is a multiple of 2, then
  
  $p_2' = true$
  else
  
  $p_2' = false$
• Update of \( p_3 \):
  If \( c = 0 \)
  \[ p_3' = \text{true}; \]
  else
  \[ p_2' = \text{false}; \]

The abstract transformer for \( x := 2 \times x \) is:

• if (\( p_1 \) or \( p_3 \)) then \( p_1' = \text{true} \) else \( p_1' = \ast \);
  \[ p_2' = \text{true}; \]
  \[ p_3' = p_3 \]

The abstract transformer for \( x := 4 \times x \) is:

• if (\( p_1 \) or \( p_2 \) or \( p_3 \)) then \( p_1' = \text{true} \) else \( p_1' = \ast \);
  if (\( p_1 \) or \( p_2 \) or \( p_3 \)) then \( p_2' = \text{true} \) else \( p_2' = \ast \);
  \[ p_3' = p_3 \]

The following shows the states reached executing the abstract transformer for each statement:

\{p1=*, p2=*, p3=*\}
\( x := 1; \)  \{p1=F, p2=F, p3=F\}
\( x := 2 \times x; \)  \{p1=*, p2=T, p3=F\}
\( x := 4 \times x; \)  \{p1=T, p2=T, p3=F\}
\( x := 2 \times x; \)  \{p1=T, p2=T, p3=F\}

So at the end of the above program, we know from the abstract states reached that \( x \) is a multiple of 8, is a multiple of 4, and is non-zero.

4. (20 points)
Perform model-checking manually on the following transition system with propositions \( \{ p, q, r \} \). Check which states satisfy the CTL formula \( A(pU(EFq)) \) on this system by listing the precise set of states that satisfy its subformulas, inductively.
For every subformula (including the formula itself), from simpler to more complex, list the precise set of states that satisfy the subformula.

**Solution:**
Let the three states in the diagram be \( u \) (with \( p, \neg q, r \) true), \( v \) (with \( p, \neg q, \neg r \) true), and \( w \) (with \( p, q, r \) true).

The set of states satisfying the various subformulas are as follows:

- \( p: u, v, w \)
- \( q: w \)
- \( EFq: u, v, w \)
- \( A(pU(EFq)): u, v, w \)