1. Use the extended Euclidean Algorithm to compute the greatest common divisor of 119 and 161, and express the greatest common divisor as an integer combination of 119 and 161. Show your work.

Solution. The successive divisions are $161 = 119 \cdot 1 + 42$, $119 = 42 \cdot 2 + 35$, $42 = 35 \cdot 1 + 7$, and $35 = 7 \cdot 5 + 0$.

So, $\gcd(161, 119) = \gcd(42, 119) = \gcd(42, 35) = \gcd(7, 35) = \gcd(7, 0) = 7$.

Back substitution of non-zero remainders yields $7 = -4 \cdot 119 + 3 \cdot 161$.

2. (i) Show that for every integer x, x^2 and $4x^4 + x + 1$ are coprime.

Solution. Let x be an integer. We use the theorem that says that for all integers a, b, and c, $\gcd(a, b) = \gcd(a, b - ac)$. Thus, $\gcd(x^2, 4x^4 + x + 1) = \gcd(x^2, x + 1) = \gcd(1, x + 1) = 1$, as desired. Note that we subtracted $(x + 1)(x - 1)$ from x^2 for the second to last equality.

(ii) Show that for every prime p and every integer x,

$$p \mid x^2 - 1 \implies (p \mid (x + 1)^2 \text{ or } p \mid x^3 - 1).$$

Solution. Let p be a prime and let x be an integer. Assume that $p \mid x^2 - 1$. Since p is prime, this means that $p \mid x - 1$ or $p \mid x + 1$. If $p \mid x + 1$, then $p \mid (x + 1)^2$ since $(x + 1)^2$ is a multiple of $x + 1$. If $p \mid x - 1$, then $p \mid x^3 - 1$ since $x^3 - 1$ is a multiple of $x - 1$, namely $x^3 - 1 = (x - 1)(x^2 + x + 1)$.
In either case, the conclusion is satisfied, as desired.

3. Show by induction that for all natural numbers n

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

Solution. Let $p(n) :=$ "$1 - 2 + 2^2 - 2^3 + \cdots + (-1)^n 2^n = \frac{1-(-2)^{n+1}}{3}$"

Base case) $p(0) :=$ "$1 - 2 + 2^2 - 2^3 + \cdots + (-1)^0 2^0 = \frac{1-(-2)^{0+1}}{3}$"
is true since $1 = \frac{3}{3} = \frac{1-(-2)}{3}$.

Induction step) Assume that k is a natural number and that $p(k)$ is true.

Then $1 - 2 + 2^2 - 2^3 + \cdots + (-1)^{k+1}2^{k+1}$

is equal to $(1 - 2 + 2^2 - 2^3 + \cdots + (-1)^k 2^k) + (-1)^{k+1}2^{k+1}$

which by the induction hypothesis is equal to

$\frac{1-(-2)^{k+1}}{3} + (-1)^{k+1}2^{k+1}$

which upon using 3 as a common denominator becomes

$\frac{1-(-2)^{k+1}+3(-2)^{k+1}}{3} = \frac{1+2(-2)^{k+1}}{3} = \frac{1-(-2)^{k+2}}{3}$, as desired.

4. Recall the definition of len and app:

$$\begin{array}{ll} \mathsf{len}(\mathsf{nil}) = 0 & \mathsf{app}(a, \mathsf{nil}) = a :: \mathsf{nil} \\ \mathsf{len}(a :: L) = \mathsf{len}(L) + 1 & \mathsf{app}(a, b :: L) = b :: \mathsf{app}(a, L) \end{array}$$

Let insert be defined to be:

$$\begin{array}{l} \mathsf{insert}(L, x, 1) = x :: L \\ \mathsf{insert}(a :: L, x, i) = a :: \mathsf{insert}(L, x, i-1) \quad \text{for } i > 1 \end{array}$$

You may assume that $1 \le i \le \mathsf{len}(L) + 1$.

Show that $\mathsf{insert}(L, x, \mathsf{len}(L) + 1) = L :: x$.

Solution. We proceed by structural induction on L.

Base Case: $L = \mathsf{nil}$.

$$\begin{aligned} \mathsf{insert}(\mathsf{nil}, x, \mathsf{len}(\mathsf{nil}) + 1) &= \mathsf{insert}(\mathsf{nil}, x, 1) && (\mathsf{len}_1) \\ &= x :: \mathsf{nil} && (\mathsf{insert}_1) \\ &= \mathsf{nil} :: x && (\mathsf{app}_1) \end{aligned}$$

Inductive Step: Let $L = a :: L'$ for some list L'. Assume $\mathsf{insert}(L', x, \mathsf{len}(L') + 1) = L' :: x$.

$$\begin{aligned} \mathsf{insert}(L, x, \mathsf{len}(L) + 1) &= \mathsf{insert}(a :: L', x, \mathsf{len}(a :: L') + 1) \\ &= a :: \mathsf{insert}(L', x, \mathsf{len}(a :: L')) && (\mathsf{insert}_1) \\ &= a :: \mathsf{insert}(L', x, \mathsf{len}(L') + 1) && (\mathsf{len}_1) \\ &= a :: (L' :: x) && (\text{IH}) \\ &= (a :: L') :: x && (\mathsf{app}_2) \\ &= L :: x \end{aligned}$$

5. Let $S = \{f \mid f : \mathbb{N} \to \{0,1\}\}$ be the set of all functions that map the natural numbers to $\{0,1\}$. Define a relation $\sim$ on S as follows:
for $f, g \in S$, $f \sim g$ if there is $N \in \mathbb{N}$ such that for all $n \geq N, f(n) = g(n)$.

(i) Prove that $\sim$ is reflexive.

Solution. Let $f \in S$ and pick $N = 0$. Then, since $f(n) = f(n)$ for all $n \geq N = 0$, we have $f \sim f$.

(ii) Prove that $\sim$ is transitive.

Solution. Let $f, g, h \in S$ and suppose that $f \sim g$ and $g \sim h$. Since $f \sim g$, there exists some $N_1 \in \mathbb{N}$ such that $f(n) = g(n)$ for all $n \geq N_1$. Since $g \sim h$, there exists some $N_2 \in \mathbb{N}$ such that for all $n \geq N_2, g(n) = h(n)$. Taking $n \geq \max\{N_1, N_2\}$, we have that $f(n) = g(n)$ and $g(n) = h(n)$, so $f(n) = h(n)$. Therefore, picking $N = \max\{N_1, N_2\}$ shows that $f \sim h$.

Bonus. Prove the following statement without using uniqueness of factorization: For all pairs of coprime integers a and b and integers n,
$(a \mid n$ and $b \mid n)$ implies $ab \mid n$.

Solution. Let a, b, and n be integers, with a and b coprime. Assume that $a \mid n$ and $b \mid n$. Since a and b are coprime, there exist integers x and y, such that $ax + by = 1$. Multiplying by n yields $nax + nby = n$. Since $a \mid n$ and $b \mid n$, there exist integers k and j such that $n = ak$ and $n = bj$. Substituting these into the previous equation yields $n = abjx + abky = ab(jx + ky)$. Since $jx + ky$ is an integer, we have $ab \mid n$, as desired.