1. Match the erroneous proofs (a)-(e) with the reasons (1)-(4) they are not valid inductive proofs of the claims. Some reasons may be used more than once and others not at all.

   (a) Proposition: If $a_1 = 3$ and $a_{n+1} = 3a_n + 2$ for all $n \geq 1$, then $a_n = 3^n - 1$ for all n.
   Proof: Induct on n. The base case $n = 1$ is trivial. For the inductive step, suppose $a_n = 3^n - 1$. Then $a_{n+1} = 3a_n + 2 = 3(3^n - 1) + 2 = 3^{n+1} - 1$ as required.

   - The argument for the inductive step is correct. The issue is that the base case is wrong: although $a_1 = 3$, the formula gives instead $a_1 = 3^1 - 1 = 2$, which is reason $\boxed{(1)}$.
   - The issue is that the base case is simply asserted rather than actually proven. (Of course, this would have been very obvious if the calculations for the base case were actually given in the proof!)

   (b) Proposition: For every positive integer n, $1 + 2 + 4 + \cdots + 2^n = 2n + 1$.
   Proof: Induct on n. The base case $n = 1$ follows because $1 + 2 = 2 \cdot 1 + 1$. For the inductive step, we want to show that $1 + 2 + 4 + \cdots + 2^{n+1} = 2^{n+2} - 1$. Multiplying both sides by 0 yields $0 = 0$, which is a true statement. Therefore the result holds by induction.

   - The error is that the argument in the inductive step starts out by assuming $P(n+1)$ and then shows that it implies a true statement (in this case that, $0 = 0$). This is not a valid argument because for an induction proof, the inductive step needs to assume $P(n)$ and show that it implies $P(n+1)$. This is reason $\boxed{(2)}$.

   (c) Proposition: If $a_1 = 2$, and $a_{n+1} = 4a_n - 4a_{n-1}$ for all $n \geq 1$, then $a_n = 2^n$ for all n.
   Proof: Strong induction on n. The base case $n = 1$ follows since $a_1 = 2 = 2^1$. For the inductive step, suppose $a_k = 2^k$ for all $k \leq n$. Then $a_{n+1} = 4a_n - 4a_{n-1} = 4 \cdot 2^n - 4 \cdot 2^{n-1} = 4 \cdot 2^n - 2 \cdot 2^n = 2 \cdot 2^n = 2^{n+1}$ as required.

   - The issue here is that the inductive step uses the two previous cases $k = n$ and $k = n - 1$, but only one base case is actually established, which is reason $\boxed{(3)}$.
   - One way to see that this is a problem is to use the recurrence to find a_2 (i.e., by setting $n = 1$), it yields $a_2 = 4a_1 - 4a_0$, but a_0 has not been defined!

   (d) Proposition: All horses are the same color.
   Proof: Induct on n, the number of horses. The base case $n = 1$ is trivial. For the inductive step, suppose that any $n + 1$ horses are the same color. Ignoring the last horse yields means that we need to show that n horses are the same color, which is true by the induction hypothesis. Therefore the result holds by induction.

   - The error is that the proof of the inductive step assumes $P(n + 1)$ and uses it to establish $P(n)$: that is backwards from the correct logic, which is to show that $P(n)$ implies $P(n + 1)$, and is reason $\boxed{(4)}$.

   (e) Proposition: For every positive integer n, $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n + 1)$.
   Proof: Induct on n. The base case $n = 1$ follows because $1 = \frac{1}{2}(1)(2)$. For the inductive step, suppose that $1+2+3+\cdots+n+(n+1) = \frac{1}{2}(n+1)(n+2)$. Subtracting $n+1$ from both sides yields $1+2+3+\cdots+n = \frac{1}{2}(n + 1)(n + 2) - (n + 1) = \frac{1}{2}n(n + 1)$, as required. Therefore the result holds by induction.

   - The error is the same mistake as in part (d): the inductive step starts out by assuming $P(n + 1)$ and then reduces it to $P(n)$. This is backwards from the correct logic, which is to show that $P(n)$ implies $P(n + 1)$, and is reason $\boxed{(4)}$. (One could also reasonably argue that this is reason $\boxed{(2)}$ as well.)
   - In this case, the mistake can be fixed by writing the steps in the correct order (start with $1 + 2 + \cdots + n = \frac{1}{2}n(n + 1)$ and add $n + 1$ to both sides to obtain $1 + 2 + \cdots + (n + 1) = \frac{1}{2}(n + 1)(n + 2)$).

2. For each pair of integers (a, b), use the Euclidean algorithm to calculate their greatest common divisor $d = \gcd(a, b)$ and also to find integers x and y such that $d = ax + by$.

   (a) $a = 44$, $b = 12$.

   - Applying the Euclidean algorithm to $a = 44$ and $b = 12$ yields

$$\begin{aligned} 44 &= 3 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 \end{aligned}$$

     and thus the gcd is the last nonzero remainder of $\boxed{4}$.

   - For the linear combination, we solve for the remainders:

$$\begin{array}{rcccl} 8 & = & & = & 1 \cdot 44 - 3 \cdot 12 \\ 4 & = & 12 - 1 \cdot 8 & = & -1 \cdot 44 + 4 \cdot 12 \end{array}$$

     and so we see $\boxed{4 = -1 \cdot 44 + 4 \cdot 12}$ so we can take $x = -1$ and $y = 4$.

   (b) $a = 481$, $b = 24$.

   - Applying the Euclidean algorithm to $a = 481$ and $b = 24$ yields

$$\begin{aligned} 481 &= 20 \cdot 24 + 1 \\ 24 &= 24 \cdot 1 \end{aligned}$$

     and thus the gcd is the last nonzero remainder of $\boxed{1}$.

   - For the linear combination, we trivially solve for the remainder $\boxed{1 = 1 \cdot 481 - 20 \cdot 24}$ so we can take $x = 1$ and $y = -20$.

   (c) $a = 18063$, $b = 2025$.

   - Applying the Euclidean algorithm to $a = 18063$ and $b = 2025$ yields

$$\begin{array}{rcl} 18063 & = & 8 \cdot 2025 + 1863 \\ 2025 & = & 1 \cdot 1863 + 162 \\ 1863 & = & 11 \cdot 162 + 81 \\ 162 & = & 2 \cdot 81 \end{array}$$

     and so the gcd is the last nonzero remainder of $\boxed{81}$.

   - For the linear combination, we solve for the remainders:

$$\begin{array}{rcccl} 1863 & = & & = & 1 \cdot 18063 - 8 \cdot 2025 \\ 162 & = & 2025 - 1 \cdot 1863 & = & -1 \cdot 18063 + 9 \cdot 2025 \\ 81 & = & 1863 - 11 \cdot 162 & = & 12 \cdot 18063 - 107 \cdot 2025 \end{array}$$

     and so we see $\boxed{81 = 12 \cdot 18063 - 107 \cdot 2025}$ so we can take $x = 12$ and $y = -107$.

   (d) $a = 12445$, $b = 5567$.

   - Applying the Euclidean algorithm to $a = 12445$ and $b = 5567$ yields

$$\begin{array}{rcl} 12445 & = & 2 \cdot 5567 + 1311 \\ 5567 & = & 4 \cdot 1311 + 323 \\ 1311 & = & 4 \cdot 323 + 19 \\ 323 & = & 17 \cdot 19 \end{array}$$

     and so the gcd is the last nonzero remainder of $\boxed{19}$.

   - For the linear combination, we solve for the remainders:

$$\begin{array}{rcccl} 1311 & = & & = & 1 \cdot 12445 - 2 \cdot 5567 \\ 323 & = & 5567 - 4 \cdot 1311 & = & -4 \cdot 12445 + 9 \cdot 5567 \\ 19 & = & 1311 - 4 \cdot 323 & = & 17 \cdot 12445 - 38 \cdot 5567 \end{array}$$

     and so we see $\boxed{19 = 17 \cdot 12445 - 38 \cdot 5567}$ so we can take $x = 17$ and $y = -38$.

(e) $a = 18200$, $b = 3505$.

- Applying the Euclidean algorithm to $a = 18200$ and $b = 3505$ yields

$$\begin{aligned} 18200 &= 5 \cdot 3505 + 675 \\ 3505 &= 5 \cdot 675 + 130 \\ 675 &= 5 \cdot 130 + 25 \\ 130 &= 5 \cdot 25 + 5 \\ 25 &= 5 \cdot 5 \end{aligned}$$

  and so the gcd is the last nonzero remainder of $\boxed{5}$.
- For the linear combination, we solve for the remainders:

$$\begin{array}{rcccc} 675 & = & & = & 1 \cdot 18200 - 5 \cdot 3505 \\ 130 & = & 3505 - 5 \cdot 675 & = & -5 \cdot 18200 + 26 \cdot 3505 \\ 25 & = & 675 - 5 \cdot 130 & = & 26 \cdot 18200 - 135 \cdot 3505 \\ 5 & = & 130 - 5 \cdot 25 & = & -135 \cdot 18200 + 701 \cdot 3505 \end{array}$$

  and so we see $\boxed{5 = -135 \cdot 18200 + 701 \cdot 3505}$ so we can take $x = -135$ and $y = 701$.

(f) $a = 233$, $b = 144$.

- Applying the Euclidean algorithm to $a = 233$ and $b = 144$ yields

$$\begin{aligned} 233 &= 1 \cdot 144 + 89 \\ 144 &= 1 \cdot 89 + 55 \\ 89 &= 1 \cdot 55 + 34 \\ 55 &= 1 \cdot 34 + 21 \\ 34 &= 1 \cdot 21 + 13 \\ 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

  and so the gcd is the last nonzero remainder of $\boxed{1}$.
- For the linear combination, we solve for the remainders:

$$\begin{array}{rcccc} 89 & = & & = & 233 - 1 \cdot 144 \\ 55 & = & 144 - 1 \cdot 89 & = & -1 \cdot 233 + 2 \cdot 144 \\ 34 & = & 89 - 1 \cdot 55 & = & 2 \cdot 233 - 3 \cdot 144 \\ 21 & = & 55 - 1 \cdot 34 & = & -3 \cdot 233 + 5 \cdot 144 \\ 13 & = & 34 - 1 \cdot 21 & = & 5 \cdot 233 - 8 \cdot 144 \\ 8 & = & 21 - 1 \cdot 13 & = & -8 \cdot 233 + 13 \cdot 144 \\ 5 & = & 13 - 1 \cdot 8 & = & 13 \cdot 233 - 21 \cdot 144 \\ 3 & = & 8 - 1 \cdot 5 & = & -21 \cdot 233 + 34 \cdot 144 \\ 2 & = & 5 - 1 \cdot 3 & = & 34 \cdot 233 - 55 \cdot 144 \\ 1 & = & 3 - 1 \cdot 2 & = & -55 \cdot 233 + 89 \cdot 144 \end{array}$$

  and so we see $\boxed{1 = -55 \cdot 233 + 89 \cdot 144}$ so we can take $x = -55$ and $y = 89$.

3. Prove the following basic properties of divisibility (note that some of these properties are referred to, but not proven, in the course notes; you are expected to give the details of the proof!):

   (a) If a, b are integers, show that $a|b$ if and only if $a|(-b)$.

   - First suppose $a|b$ so that $b = pa$ for some integer p. Then $-b = (-p)a$ so $a|(-b)$.
   - Conversely, suppose $a|(-b)$ so that $-b = qa$ for some integer q. Then $b = (-q)a$ so $a|b$.

   (b) If a, b, m are integers with $m \neq 0$, show that $a|b$ if and only if $(ma)|(mb)$.

   - First suppose $a|b$, so that $b = pa$ for some integer p. Then $mb = mpa = p(ma)$ so $(ma)|(mb)$.
   - Conversely suppose $(ma)|(mb)$, so that $mb = p(ma)$ for some integer p. Since $m \neq 0$ we can cancel m to conclude that $b = pa$, meaning $a|b$ as required.

   (c) If a, b, c are integers such that $a|b$ and $a \nmid c$, show that $a \nmid (b + c)$.

   - Suppose by way of contradiction that $a|(b + c)$. Then $b + c = ka$ for some k, and also since $a|b$ we have $b = la$ for some l.
   - But then $c = (b + c) - b = ka - la = (k - l)a$ would be divisible by a, which is a contradiction.

   (d) If a, b, c, x, y are integers such that $a|b$ and $a|c$, show that $a|(xb + yc)$.

   - By definition, if $a|b$ and $a|c$, then there exist integers p and q with $b = pa$ and $c = qa$.
   - Then $xb + yc = x(pa) + y(qa) = (xp)a + (yq)a = (xp + yq)a$, and so for $k = xy + yq$ we see that $xb + yc = ka$, meaning that $a|(xb + yc)$.

   (e) If a, b are integers, show that a, b and $a, a + b$ have the same set of common divisors.

   - Suppose d is a common divisor of a, b so that $d|a$ and $d|b$. Then $d|a$ and $d|(a + b)$ as well, so d is a common divisor of $a, a + b$.
   - Conversely, if e is a common divisor of $a, a+b$ so that $e|a$ and $e|(a+b)$, then $e|a$ and $e|[(a+b)-a] = b$ as well, so e is a common divisor of a, b.
   - Together these two statements imply that a, b and $a, a + b$ have the same set of common divisors.

---

4. The Fibonacci numbers are defined as follows: $F_1 = F_2 = 1$ and for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. The first few terms of the Fibonacci sequence are 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, ...

   (a) Prove that $F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$ for every positive integer n. [Hint: Use induction.]

   - We prove the result by induction on n.
   - For the base case $n = 1$, we must verify $F_1 = F_3 - 2$, which is true because $F_3 = 3$ and $F_1 = 1$.
   - For the inductive step, we assume that $F_1 + F_2 + F_3 + \cdots + F_k = F_{k+2} - 1$ and must show that $F_1 + F_2 + F_3 + \cdots + F_k + F_{k+1} = F_{k+3} - 1$.
   - Then $F_1 + F_2 + F_3 + \cdots + F_k + F_{k+1} = [F_1 + F_2 + F_3 + \cdots + F_k] + F_{k+1} = F_{k+2} - 1 + F_{k+1} = F_{k+3} - 1$ as required.
   - Hence by induction, $F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$ for every positive integer n.

   (b) Prove that $F_{n+1}^2 - F_n F_{n+2} = (-1)^n$ for every positive integer n.

   - We prove the result by induction on n.
   - For the base case $n = 1$, we must verify $F_2^2 - F_1 F_3 = -1$, which is true since $F_2 = 1$, $F_1 = 1$, and $F_3 = 2$.
   - For the inductive step, we assume that $F_{n+1}^2 - F_n F_{n+2} = (-1)^n$ and must show that $F_{n+2}^2 - F_{n+1} F_{n+3} = (-1)^{n+1}$.
   - By definition, we have $F_{n+3} = F_{n+2} + F_{n+1}$, so $F_{n+2}^2 - F_{n+1} F_{n+3} = F_{n+2}^2 - F_{n+1}[F_{n+1} + F_{n+2}] = F_{n+2}[F_{n+2} - F_{n+1}] - F_{n+1}^2 = F_{n+2} F_n - F_{n+1}^2 = -(-1)^n = (-1)^{n+1}$, as required.
   - Hence by induction, $F_{n+1}^2 - F_n F_{n+2} = (-1)^n$ for every positive integer n.

(c) Prove that $F_{2n+1} = F_{n+1}^2 + F_n^2$ and $F_{2n+2} = F_{n+1}(F_{n+2} + F_n)$ for all $n \geq 1$. [Hint: Show both together by induction.]

- We show both statements simultaneously by induction on n.
- For the base case $n = 1$, we have $F_3 = F_2^2 + F_1^2 = 2$ and $F_4 = F_2(F_3 + F_1) = 1(2+1) = 3$, as required.
- For the inductive step, suppose that $F_{2n-1} = F_n^2 + F_{n-1}^2$ and $F_{2n} = F_n(F_{n+1} + F_{n-1})$
- Then $F_{2n+1} = F_{2n} + F_{2n-1} = F_n(F_{n+1} + F_{n-1}) + F_n^2 + F_{n-1}^2 = F_nF_{n+1} + F_{n-1}F_{n+1} + F_n^2 = F_{n+1}^2 + F_n^2$ as required.
- Also, $F_{2n+2} = F_{2n+1} + F_{2n} = F_{n+1}^2 + F_n^2 + F_nF_{n+1} + F_nF_{n-1} = F_{n+1}^2 + F_nF_{n+1} + F_nF_{n+1} = F_{n+1}(F_{n+2} + F_n)$ as required.

---

5. The goal of this problem is to study a few more miscellaneous properties of Fibonacci numbers, as defined in problem 4.

(a) Find $\gcd(F_5, F_{10})$, $\gcd(F_6, F_9)$, $\gcd(F_6, F_{12})$, and $\gcd(F_{12}, F_{13})$.

- We have $\gcd(F_5, F_{10}) = \gcd(5, 55) = \boxed{5}$, $\gcd(F_6, F_9) = \gcd(8, 34) = \boxed{2}$, $\gcd(F_6, F_{12}) = \gcd(8, 144) = \boxed{8}$, and $\gcd(F_{12}, F_{13}) = \gcd(144, 233) = \boxed{1}$.

(b) Show that $F_{n+k} = F_kF_{n+1} + F_{k-1}F_n$, for any nonnegative n and k. [Hint: Induct on k.]

- We follow the hint and induct on k: for $k = 1$ the statement says $F_{n+1} = F_1F_{n+1} + F_0F_n$, and for $k = 2$ the statement says $F_{n+2} = F_2F_{n+1} + F_1F_n = F_{n+1} + F_n$ both of which are true.
- Now suppose that $F_{n+k} = F_kF_{n+1} + F_{k-1}F_n$ holds for all $k \leq l$; we want to show that $F_{n+l+1} = F_{l+1}F_{n+1} + F_lF_n$. We have

$$\begin{aligned} F_{n+l+1} &= F_{n+l} + F_{n+l-1} \\ &= [F_lF_{n+1} + F_{l-1}F_n] + [F_{l-1}F_{n+1} + F_{l-2}F_n] \\ &= [F_l + F_{l-1}]\, F_{n+1} + [F_{l-1} + F_{l-2}]F_n \\ &= F_{l+1}F_{n+1} + F_lF_n, \end{aligned}$$

where we used the inductive hypothesis for $k = l$ and $k = l - 1$.

(c) Show that $F_a | F_{na}$ for all positive integers n. [Hint: Use (b).]

- We use induction on n. For the base case $n = 1$ we clearly have $F_a | F_a$.
- For the inductive step, suppose F_a divides F_{na}. Then using (a) we see that $F_{(n+1)a} = F_{na}F_{n+a} + F_{na-1}F_a$ is the sum of two terms each divisible by F_a, so it is also divisible by F_a.

(d) Show that F_a and F_{a+1} are relatively prime for all n.

- This is another induction: we have $\gcd(F_1, F_2) = \gcd(1, 1) = 1$, and for the inductive step if F_{n-1} and F_n are relatively prime, then so are $F_{n-1} + F_n = F_{n+1}$ and F_n.

Remark: It can in fact be shown using the results in (b), (c), and (d) that the gcd of any two Fibonacci numbers is another Fibonacci number, and more specifically that $\gcd(F_a, F_b) = F_{\gcd(a,b)}$.
