1. Match the erroneous proofs (a)-(f) with the reasons (1)-(5) they are not valid inductive proofs of the claims. Some reasons may be used more than once and others not at all.

   Reasons:

   (1) The proof does not actually check that the base case is correct.
   (2) The proof of the inductive step shows that the claimed result implies a true statement instead of proving the claimed result.
   (3) The proof of the inductive step assumes more base cases than are actually checked.
   (4) The proof of the inductive step shows that the result for $n+1$ implies the result for n, rather than the other way around.
   (5) The inductive step makes an invalid assumption about n.

   (a) Proposition: For every positive integer n, $1+2+4+\cdots+2^n = 2n+1$.
   Proof: Induction 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 $\boxed{(2)}$.

   (b) 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: Induction 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!)

   (c) Proposition: All horses are the same color.
   Proof: Induction 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 $\boxed{(4)}$.

   (d) Proposition: For every positive integer n, $1+2+3+\cdots+n = \frac{1}{2}n(n+1)$.
   Proof: Induction 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 $1+2+\cdots+(n+1) = \frac{1}{2}(n+1)(n+2)$).

   (e) 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!

(f) Proposition: For all positive integers n, $2^n > n^2$.
Proof: Induction on n. The base case $n = 1$ follows since $2 > 1$. For the inductive step, suppose $2^n > n^2$. Then $2^{n+1} = 2 \cdot 2^n > 2n^2 > n^2 + n^2 \geq n^2 + 3n > n^2 + 2n + 1 = (n+1)^2$ since $n \geq 3$.

- The issue here is that the statement $n^2 \geq 3n$ in the middle uses the assumption $n \geq 3$, but the base case only handles $n = 1$. The inductive step makes an invalid assumption about n: reason $\boxed{(5)}$.
- One way to see that this is a problem is to notice that the claimed statement is false when $n = 2$, $n = 3$, and $n = 4$!

---

2. The goal of this problem is to explore some methods for finding greatest common divisors.

(a) Find all divisors of 20 and of 28, list the common divisors, and use the list to find the greatest common divisor.

- Divisors of 20: $\boxed{-20, -10, -5, -4, -2, -1, 1, 2, 4, 5, 10, 20}$.
- Divisors of 28: $\boxed{-28, -14, -7, -4, -2, -1, 1, 2, 4, 7, 14, 28}$.
- Common divisors: $\boxed{-4, -2, -1, 1, 2, 4}$ and greatest common divisor $\boxed{4}$.

(b) Find all divisors of 33 and of 90, list the common divisors, and use the list to find the greatest common divisor.

- Divisors of 33: $\boxed{-33, -11, -3, -1, 1, 3, 11, 33}$.
- Divisors of 90: $\boxed{-90, -45, -30, -18, -15, -10, -9, -6, -5, -3, -2, -1, 1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90}$.
- Common divisors: $\boxed{-3, -1, 1, 3}$ and greatest common divisor $\boxed{3}$.

(c) Claim: Starting with any pair of positive integers (a, b), repeatedly subtract the smaller number in the pair from the larger, until one of the numbers reaches zero: then the other number is $\gcd(a, b)$.
Test the claim using the pairs $(20, 28)$ and $(33, 90)$: does it give the correct gcd?

- $(20, 28) \to (20, 8) \to (12, 8) \to (4, 8) \to (4, 4) \to (4, 0)$ yielding gcd $\boxed{4}$. That agrees with (a).
- $(33, 90) \to (33, 57) \to (33, 24) \to (33, 9) \to (24, 9) \to (15, 9) \to (6, 9) \to (6, 3) \to (3, 3) \to (3, 0)$ yielding gcd $\boxed{3}$, which also agrees.

(d) Which method, of the ones given in (a)/(b) and in (c), would be faster on two 10-digit numbers?

- Although the method of (c) involves a lot of subtraction, it's much easier than computing the list of divisors of a given integer.

Remark: In fact, the method described in (c), using iterated subtraction, was the original formulation of the Euclidean algorithm. (The version we discuss in lecture is faster, but requires computing remainders.)

---

3. Prove the following:

(a) For every integer $n \geq 2$, it is true that $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1) \cdot n = \frac{1}{3}n(n-1)(n+1)$.

- We prove the result by induction on n.
- For the base case $n = 2$, we verify $1 \cdot 2 = \frac{1}{3}2(2-1)(2+1)$: true, as both quantities equal 2.
- For the inductive step, we assume that $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1) \cdot n = \frac{1}{3}n(n-1)(n+1)$ and must show that $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1) \cdot n + n \cdot (n+1) = \frac{1}{3}(n+1)n(n+2)$.
- Using the inductive hypothesis, we see that $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1) \cdot n + n \cdot (n+1) = \frac{1}{3}n(n-1)(n+1) + n(n+1) = n(n+1)[\frac{n-1}{3} + 1] = \frac{1}{3}n(n+1)(n+2)$, as desired.
- Hence, by induction, $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1) \cdot n = \frac{1}{3}n(n-1)(n+1)$ for all $n \geq 2$.

(b) Let $a_0 = 0$, $a_1 = 1$, and, for $n \geq 0$, let $a_{n+2} = 5a_{n+1} - 6a_n$. Prove that $a_n = 3^n - 2^n$ for all $n \geq 0$.

- We prove the result by induction on n.
- For the base cases $n = 0$ and $n = 1$, we must verify $0 = a_0 = 3^0 - 2^0$ and $1 = a_1 = 3^1 - 2^1$ and these are both true.
- For the inductive step, suppose that $a_{n+1} = 3^{n+1} - 2^{n+1}$ and $a_n = 3^n - 2^n$. Then by definition $a_{n+2} = 5a_{n+1} - 6a_n = 5(3^{n+1} - 2^{n+1}) - 6(3^n - 2^n) = 15 \cdot 3^n - 6 \cdot 3^n - 10 \cdot 2^{n+1} + 6 \cdot 2^{n+2} = 9 \cdot 3^n - 4 \cdot 2^n = 3^{n+2} - 2^{n+2}$, as desired.
- Hence, by induction, $a_n = 3^n - 2^n$ for all $n \geq 0$. (Note here that we need two base cases because the inductive step uses the two previous cases.)

---

4. 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, 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 $a|(xb + yc)$.

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

- 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 $e|[a-(a-b)] = b$ 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. Since the gcd is the greatest of the common divisors, they must also have the same gcd.

---

5. 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.

- 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 $F_{2n+1} = F_{2n} + F_{2n-1} = F_n(F_{n+1} + F_{n-1}) + F_n^2 + F_{n-1}^2 = F_n F_{n+1} + F_{n-1}F_{n+1} + F_n^2 = F_{n+1}^2 + F_n^2$ as required.
- Also, $F_{2n+2} = F_{2n+1} + F_{2n} = F_{n+1}^2 + F_n^2 + F_n F_{n+1} + F_n F_{n-1} = F_{n+1}^2 + F_n F_{n+1} + F_n F_{n+1} = F_{n+1}(F_{n+2} + F_n)$ as required.

---

6. The goal of this problem is to study a few more miscellaneous properties of Fibonacci numbers, as defined in problem 5. (By convention, we also take $F_0 = 0$.)

(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 $F_{n+k+1} = F_{k+1}F_{n+1} + F_k F_n$, for any nonnegative n and k. [Hint: Strong induction on k.]

- We follow the hint and induct on k: for $k = 0$ the statement says $F_{n+1} = F_1 F_{n+1} + F_0 F_n$, and for $k = 2$ the statement says $F_{n+2} = F_2 F_{n+1} + F_1 F_n = F_{n+1} + F_n$ both of which are true.
- Now suppose that $F_{n+k} = F_k F_{n+1} + F_{k-1}F_n$ holds for all $k \leq l$; we want to show that $F_{n+l+1} = F_{l+1}F_{n+1} + F_l F_n$. We have

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

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_n and F_{n+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 $\gcd(F_a, F_b) = F_{\gcd(a,b)}$.
