this last step because $\binom{n}{0} = \binom{n}{n} = 1$.

15. The "induction" step is false when $n = 2$.

16. Let $X \subset \mathbb{N}$ be non-empty with no least element and let $Y = \mathbb{N} \backslash X$. Since X has no least element, $1 \in Y$. Now, suppose $k \in Y$ for all $k < n$. Thus $k \notin X$ for all $k < n$. If $n \in X$, then n would be the least element in X, thus $n \notin X$ and so $n \in Y$. Therefore Y satisfies criteria (1) and (2) of the Principle of Mathematical Induction and so $Y = \mathbb{N}$. That is, $X = \emptyset$, a contradiction.

17. *Hint:* It's probably easier to prove that the Strong Principle is equivalent to the Well-ordering Principle. This works because of Theorem 1.1 and Exercise 16.

Chapter 2 — The Integers

1. (a) $(13)(21) + (-8)(34) = 1$
   (b) $(157)(772) + (-50)(2424) = 4$
   (c) $(-53)(2007) + (524)(203) = 1$
   (d) $(4)(3604) + (-3)(4770) = 106$

2. (a) Note that $\gcd(a, b)$ divides both a and b.
   (b) $\gcd(a, b)$ must divide 3, so is either 1 or 3. But 3 divides both these integers.
   (c) $\gcd(a, b)$ is either 1, 2, or 4. But the integers are odd, and so the gcd is 1.
   (d) Note this does not essentially speed up the process in the last 3 cases. In part (a) $\gcd(a, b)$ is either 1 or 13.

3. There are two things to prove here: each linear combination of a and b is a multiple of $\gcd(a, b)$ and each multiple of $\gcd(a, b)$ can be written as a linear combination of a and b. The latter part follows from the GCD identity. For the former, note that a common divisor of a and b also divides $ax + by$.

4. This follows immediately from Exercise 3.

5. The base case $n = 1$ is trivial. For induction, assume $p | a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_{n-1}) a_n$, for $n > 1$, and then apply the prime property, and induction.

6. Note that $\gcd(a, b)$ divides $a + b$.

7. (a) Consider $(n + 1)! + 2, (n + 1)! + 3, \cdots, (n + 1)! + (n + 1)$.
   (b) $6! + 2$. Of course, there might be a run of 5 earlier.

8. Use induction on n. Note that if d divides b and $a + b$, d divides a.

9. Use the GCD identity: Let $g = \gcd(b, c)$. Then $g = bx + cy$ and this is the least positive linear combination of b and c. Now suppose $h = \gcd(ab, ac) = abx' + acy' = a(bx' + cy')$. Now if $bx' + cy'$ were not the least such positive linear combination then a smaller such would lead to a smaller linear combination of ab and ac to get h.

10. First, the given term clearly divides both a and b. Now suppose d is a common divisor of a and b. Now if p is a prime dividing d then it must be one of the primes listed in both a and b and its power is no larger than s_i. Thus d divides the $\gcd(a, b)$ given.

11. $2^2 \cdot 3 \cdot 5 \cdot 19$, $2 \cdot 5 \cdot 3^2 \cdot 7$. In place of the s_i use the larger of n_i and m_i.

12. This follows easily using the formulations from Exercises 10 and 11.

13. By way of contradiction, assume $\text{lcm}(a, b) = x$ does not divide m. By the Division Theorem, $x = dm + r$, where $0 \leq r < x$. Argue that r is a common multiple of a and b. This forces $r = 0$.

14. Use contradiction assuming that $\sqrt{2} = a/b$ where a and b are relatively prime. Square both sides and clear the denominator, and then consider whether each side is even or odd. Your contradiction will be that both a and b are even.

15. (a) That triangle DEP is isosceles follows from the observation that triangle ADP is isosceles. Now note that $s = r + \sqrt{2}r$.

    (b) *Hint:* Consider the square with three vertices E, P, and C, and use part (a). Why does this mean that the algorithm never halts? (Consider what happens if d and s are integer multiples of a common value.)

16. If n is the smallest number divisible by primes $p_1 \ldots p_k$ and p is a different prime, then p does not divide n. Prove this by contradiction.

17. (a) Note the first recursive call is $\gcd(772, 108)$.

    (b) The first recursive call (from $\gcd(285, 255, g, x, y)$) will be $\gcd(255, 30, g, x, y)$. The next will be $\gcd(30, 15, g, x, y)$. The next last one is $\gcd(15, 0, g, x, y)$. These calls then return with values for g, x, and y.

18. (a) Note $r_{i+2} = r_{i+1} \cdot q + r_i$ and $r_i < r_{i+1} < r_{i+2}$. So, if $r_{i+1} \leq 1/2\ r_{i+2}$ we're done. Suppose $r_{i+1} > 1/2\ r_{i+2}$. Then $r_{i+2} = r_{i+1} \cdot q + (r_{i+2} - r_{i+1})$ and $r_{i+2} - r_{i+1} < 1/2\ r_{i+2}$.

    (b) So, in the worst case, the remainder is halved every 2 steps. Thus if it takes $2n$ steps for the remainder to reach 1, $\max(a, b)/2^n = 1$ So, $n \approx \log_2(\max(a, b))$. Thus, it will take about $2 \log_2(\max(a, b))$ steps.

19. We know from Exercise 1.14 that $\binom{p}{k}$ is an integer. But

$$\binom{p}{k} = \frac{p!}{(p-k)!k!}.$$

    The denominator of this quotient is not divisible by the prime p, because it is a product of integers strictly less than p. However, the numerator is obviously divisible by p. Thus the quotient must also be divisible by p.

Chapter 3 — Modular Arithmetic

1. $[0]_8 = \{\ldots, -16, -8, 0, 8, \ldots\}$, $[1]_8 = \{\ldots, -16, -7, 1, 9, \ldots\}$, $[2]_8 = \{\ldots, -14, -6, 2, 10, \ldots\}$, $[3]_8 = \{\ldots, -13, -5, 3, 11, \ldots\}$, $[4]_8 = \{\ldots, -12, -4, 4, 12, \ldots\}$, $[5]_8 = \{\ldots, -11, -3, 5, 11, \ldots\}$, $[6]_8 = \{\ldots, -10, -2, 6, 14, \ldots\}$, $[7]_8 = \{\ldots, -9, -1, 7, 15, \ldots\}$.

   $[1]_8^{-1} = [1]_8$, $[3]_8^{-1} = [3]_8$, $[5]_8^{-1} = [5]_8$, $[7]_8^{-1} = [7]_8$.

2. $[1], [2], [4], [7], [8], [11], [13], [14]$; $[3]X = [2]$.