CSE 20: Discrete Mathematics

Spring Quarter 1998

Solutions for Homework Assignment #5

Section 4.1

7.

$$
\begin{aligned}
a_0 &= 2 \cdot 0 + 1 = 1 & \qquad b_0 &= (0-1)^3 + 0 + 2 = 1 \\
a_1 &= 2 \cdot 1 + 1 = 3 & \qquad b_0 &= (1-1)^3 + 1 + 2 = 3 \\
a_2 &= 2 \cdot 2 + 1 = 5 & \qquad b_0 &= (2-1)^3 + 2 + 2 = 5 \\
a_3 &= 2 \cdot 3 + 1 = 7 & \qquad b_0 &= (3-1)^3 + 3 + 2 = 13
\end{aligned}
$$

So $a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2$ and $a_0 \neq b_0$.

14.

$$a_n = \frac{n}{(n+1)^2} \qquad \text{for all integers } n \geq 1$$

18. e.

$$\prod_{k=2}^{2} a_k = -2$$

23.

$$\sum_{k=-1}^{1} (k^3 + 2) = ((-1)^3 + 2) + (0^3 + 2) + (1^3 + 2) = 6$$

24. The solution is in the textbook.

36.

$$\frac{1}{2!} + \frac{2}{3!} + \frac{3}{4!} + \cdots + \frac{n}{(n+1)!} = \sum_{k=1}^{n} \frac{k}{(k+1)!}$$

40. When $k = 1$, $i = 1 + 1 = 2$. When $k = n$, $i = n + 1$.
Since $i = k + 1$, then $k = i - 1$.
So,

$$\frac{k^2}{k+1} = \frac{(i-1)^2}{(i-1)+1} = \frac{(i-1)^2}{i}.$$

Therefore,

$$\prod_{k=1}^{n} \frac{k^2}{k+1} = \prod_{i=2}^{n+1} \frac{(i-1)^2}{i}.$$

43. When $i = 1$, $j = 1 - 1 = 0$. When $i = n-1$, $j = n-2$.
Since $j = i - 1$, then $i = j + 1$.
So

$$\frac{i}{(n-i)^2} = \frac{j+1}{(n-(j+1))^2} + \frac{j+1}{(n-j-1))^2}.$$

Therefore,

$$\sum_{i=1}^{n-1} \frac{i}{(n-i)^2} = \sum_{j=0}^{n-2} \frac{j+1}{(n-j-1))^2}.$$

Section 4.2

2. *Proof by induction:*

Let $P(n)$ be the property "A postage of n¢ can be obtained using 3¢ and 5¢ stamps".

The property is true for $n = 8$:
A postage of 8¢ can be obtained using one 3¢ stamp and one 5¢ stamp.

If the property is true for $n = k$ then it is true for $n = k + 1$:
Suppose that for some integer $k \geq 8$, a postage of k cents can be obtained using 3¢ and 5¢ stamps.

We must show that a postage of $k+1$ cents can be obtained using 3¢ and 5¢ stamps.

But if there is a 5¢ stamp among those use to make up the k cents of postage, replace it by two 3¢ stamps;
the result will be $k + 1$ cents of postage.

And if no 5¢ stamp is use to make up the k cents of postage, then at least three 3¢ stamps must be use because $k \geq 8$. Remove three 3¢ stamps and replace them by two 5¢ stamps; the result will be $(k+1)$¢ of postage.

Thus in either case $(k + 1)$ ¢ of postage can be obtained using 3¢ and 5¢ stamps *[as was to be shown]*.

5. The solution is in the textbook.

7. *Proof by induction:*

The formula is true for $n = 1$:
The formula hold for $n = 1$ because for $n = 1$ the left-hand side is 1 and the right-hand side is $1 \cdot (2 \cdot 1 - 1) = 1$ also.

If the formula is true for $n = k$ then it is true for $n = k + 1$:
Suppose $1 + 5 + 9 + \ldots + (4k - 3) = k(2k - 1)$ for some integer $k \geq 1$.

We must show that

$$1 + 5 + 9 + \ldots + (4(k + 1) - 3) = (k + 1)[2(k + 1) - 1]$$

or, equivalently,

$$1 + 5 + 9 + \ldots + (4(k + 1) - 3) = (k + 1)(2k + 1).$$

But

$$\begin{aligned}
&1 + 5 + 9 + \ldots + (4(k + 1) - 3) & \\
=&1 + 5 + 9 + \ldots + (4k - 3) + (4(k + 1) - 3) & \text{by algebra} \\
=&k(2k - 1) + (4(k + 1) - 3) & \text{by induction hypothesis} \\
=&2k^2 - k + 4k + 4 - 3 & \\
=&k^2 + 3k + 1 & \\
=&(k + 1)(2k + 1) & \textit{[as was to be shown].}
\end{aligned}$$

9. The solution is in the textbook.

13. *Proof by induction:*

The formula is true for $n = 0$:
The formula holds for $n = 0$ because $\sum_{i=1}^{0+1} i \cdot 2^i = 1 \cdot 2^1 = 2$ and $0 \cdot 2^{0+2} + 2 = 2$ also.

If the formula is true for $n = k$ then it is true for $n = k + 1$:
Suppose $\sum_{i=1}^{k+1} i \cdot 2^i = k \cdot 2^{k+2} + 2$ for some integer $k \geq 0$.

We must show that

$$\sum_{i=1}^{(k+1)+1} i \cdot 2^i = (k + 1) \cdot 2^{(k+1)+2} + 2$$

or, equivalently,

$$\sum_{i=1}^{k+2} i \cdot 2^i = (k + 1) \cdot 2^{k+3} + 2.$$

But

$$\begin{aligned}
\sum_{i=1}^{k+2} i \cdot 2^i &= \sum_{i=1}^{k+1} i \cdot 2^i + (k+2)2^{k+2} && \text{by algebra} \\
&= (k \cdot 2^{k+2} + 2) + (k+2)2^{k+2} && \text{by induction hypothesis} \\
&= (k + (k+2))2^{k+2} + 2 \\
&= (2k+2)2^{k+2} + 2 \\
&= (k+1)2^{k+3} + 2 && \textit{[as was to be shown].}
\end{aligned}$$

20.

$$\begin{aligned}
5 + 10 + 15 + 20 + \ldots + 300 &= 5(1 + 2 + 3 + \ldots + 60) \\
&= 5\left(\frac{60 \cdot 61}{2}\right) \\
&= 9150
\end{aligned}$$

28. a.

$$\begin{aligned}
2 + 4 + 8 + \ldots + 2^{40} &= 2(1 + 2 + 2^2 + \ldots + 2^{39}) \\
&= 2\left(\frac{2^{39+1} - 1}{2 - 1}\right) \\
&= 2^{41} - 2
\end{aligned}$$

b. 40 generations = 1200 years (at 30 years per generation)

c. Since $2^{41} - 2 \cong 2.2 \times 10^{12} > 10^{10}$, not all ancestors are distinct: some ancestors on different branches of the family must be the same.

29. The solution is in the textbook.

Section 4.3

4. *Formula:*

$$\sum_{i=1}^{n} (-1)^{i-1} i^2 = (-1)^{n-1}(1 + 2 + 3 + \ldots + n)$$

or

$$\sum_{i=1}^{n}(-1)^{i-1}i^2 = (-1)^{n-1}\frac{n(n+1)}{2}$$

(by Theorem 4.2.1) for all integers $n \geq 1$.

Proof by induction:

The formula is true for $n = 1$:
The formula holds for $n = 1$ because $\sum_{i=1}^{1}(-1)^{i-1}i^2 = (-1)^0 \cdot 1^2$ and $(-1)^{1-1} \cdot \frac{1(1+1)}{2} = 1$ also.

If the formula is true for $n = k$ then it is true for $n = k+1$:
Suppose

$$\sum_{i=1}^{k}(-1)^{i-1}i^2 = (-1)^{k-1}\frac{k(k+1)}{2} \qquad \text{for some integer } k \geq 1.$$

We must show that

$$\sum_{i=1}^{k+1}(-1)^{i-1}i^2 = (-1)^{(k+1)-1}\frac{(k+1)((k+1)+1)}{2},$$

or, equivalently,

$$\sum_{i=1}^{k+1}(-1)^{i-1}i^2 = (-1)^{k}\frac{(k+1)(k+2)}{2}.$$

But

$$\begin{aligned}
\sum_{i=1}^{k+1}(-1)^{i-1}i^2 &= \sum_{i=1}^{k+1}(-1)^{i-1}i^2 + (-1)^{(k+1)-1}(k+1)^2 && \text{by algebra} \\
&= (-1)^{k-1} \cdot \frac{k(k+1)}{2} + (-1)^k(k+1)^2 && \text{by induction hypothesis} \\
&= (-1)^{k-1}(k+1)\left(\frac{k}{2} + (-1)^k(k+1)\right) \\
&= (-1)^{k-1}(k+1)\left(\frac{k-2k-2}{2}\right) \\
&= (-1)^{k-1}(k+1)\left(\frac{-k-2}{2}\right) \\
&= (-1)^{k-1}(k+1)\left(\frac{-(k+2)}{2}\right) \\
&= (-1)6k \cdot \frac{k+1k+2}{2} && \textit{[as was to be shown].}
\end{aligned}$$

5.

$$\sum_{k=1}^{1} \frac{k}{(k+1)!} = \frac{1}{2!} \qquad = \frac{1}{2} = \frac{2!-1}{2!}$$

$$\sum_{k=1}^{2} \frac{k}{(k+1)!} = \frac{1}{2} + \frac{2}{3!} \qquad = \frac{5}{6} = \frac{3!-1}{3!}$$

$$\sum_{k=1}^{3} \frac{k}{(k+1)!} = \frac{5}{6} + \frac{3}{4!} \qquad = \frac{23}{24} = \frac{4!-1}{4!}$$

$$\sum_{k=1}^{4} \frac{k}{(k+1)!} = \frac{23}{24} + \frac{4}{5!} \qquad = \frac{119}{120} = \frac{5!-1}{5!}$$

$$\sum_{k=1}^{5} \frac{k}{(k+1)!} = \frac{119}{120} + \frac{5}{6!} \qquad = \frac{719}{720} = \frac{6!-1}{6!}$$

So we conjecture that

$$\sum_{k=1}^{n} \frac{k}{(k+1)!} = \frac{(n+1)!-1}{(n+1)!}$$

Proof by induction:

The formula holds for $n = 1$:
The calculation above shows that $\sum_{k=1}^{1} \frac{k}{(k+1)!} = \frac{(1+1)!-1}{(1+1)!}$.

If the formula holds for $n = r$ then it holds for $n = r+1$:
Suppose that for some integer $r \geq 1$,

$$\sum_{k=1}^{r} \frac{k}{(k+1)!} = \frac{(r+1)!-1}{(r+1)!}.$$

We must show that

$$\sum_{k=1}^{r+1} \frac{k}{(k+1)!} = \frac{[(r+1)+1]!-1}{[(r+1)+1]!},$$

or, equivalently,

$$\sum_{k=1}^{r+1} \frac{k}{(k+1)!} = \frac{(r+2)!-1}{(r+2)!}.$$

But

$$\begin{aligned}
\sum_{k=1}^{r+1} \frac{k}{(k+1)!} &= \sum_{k=1}^{r} \frac{k}{(k+1)!} + \frac{r+1}{[(r+1)+1]!} && \text{by algebra} \\
&= \frac{(r+1)!-1}{(r+1)!} + \frac{r+1}{(r+2)!} && \text{by induction hypothesis} \\
&= \frac{(r+1)!-1}{(r+1)!} \cdot \frac{n+2}{n+2} + \frac{r+1}{(r+2)!} \\
&= \frac{(r+2)!-(r+2)}{(r+2)!} + \frac{r+1}{(r+2)!} \\
&= \frac{(r+2)!-1}{(r+2)!} && \textit{[as was to be shown].}
\end{aligned}$$

7. a.

$$P(5) : 5^2 < 2^5$$

$P(5)$ is true because $25 < 32$.

b.

$$P(k) : k^2 < 2^k$$

c.

$$P(k+1) : (k+1)^2 < 2^{k+1}$$

d. *We must show:* If k is any integer with $k \geq 5$ and $k^2 < 2^k$, then $(k+1)^2 < 2^{k+1}$.

9. *Proof by induction:*

The property holds for $n = 1$:
The property holds for $n = 1$ because $2^{3 \cdot 1} - 1 = 7$ and 7 is divisible by 7.

If the property holds for $n = k$ then it holds for $n = k + 1$:
Suppose $2^{3k} - 1$ is divisible by 7 for some integer $k \geq 1$.

We must show that $2^{3(k+1)} - 1$ is divisible by 7.

By definition of divisibility $2^{3k} - 1 = 7r$ for some integer r.

Then

$$\begin{aligned}
2^{3(k+1)} - 1 &= 2^{3k+3} - 1 && \text{by algebra} \\
&= 2^3 2^{3k} - 1 \\
&= (7+1)2^{3k} - 1 \\
&= 7 \cdot 2^{3k} + (2^{3k} - 1) \\
&= 7 \cdot 2^{3k} + 7r && \text{by induction hypothesis} \\
&= 7(2^{3k} + r)
\end{aligned}$$

which is divisible by 7 because $2^{3k} + r$ is an integer.

Therefore, $2^{3(k+1)} - 1$ is divisible by 7 *[as was to be shown]*.

18. *Proof by induction:*

The inequality holds for $n = 2$:
To show the inequality holds for $n = 2$ we must show that $\sqrt{2} < \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}}$.
But this inequality is true if, and only if, $2 < \sqrt{2} + 1$ (by multiplying both sides by $\sqrt{2}$).
And this is true if, and only if, $1 < \sqrt{2}$ (by subtracting 2 from both sides).
But $1 < \sqrt{2}$, and so the inequality holds for $n = 2$.

If the inequality holds for $n = k$ then it holds for $n = k + 1$:
Suppose

$$\sqrt{k} < \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{k}}$$

for some integer $k \geq 2$.

We must show that

$$\sqrt{k+1} < \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{k+1}}.$$

But for each integer $k \geq 2$,

$$\sqrt{k} < \sqrt{k+1}$$

and so (multiplying both sides by $\sqrt{k}$)

$$k < \sqrt{k} \cdot \sqrt{k+1}.$$

Adding 1 to both sides gives

$$k + 1 < \sqrt{k} \cdot \sqrt{k+1} + 1$$

and dividing both sides by $\sqrt{k+1}$ gives

$$\sqrt{k+1} < \sqrt{k} + \frac{1}{\sqrt{k+1}}.$$

By substitution from the inductive hypothesis, then,

$$\sqrt{k+1} < \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{k+1}}.$$

[as was to be shown].

21. The solution is in the textbook.

23. *Proof by induction:*

The formula holds for $n = 0$: We must show that $c_0 = 3^{2^0}$. But $3^{2^0} = 3^1 = 3$ and $c_0 = 3$ by definition. So the formula holds for $n = 0$.

If the formula holds for $n = k$ then it holds for $n = k + 1$: Suppose that for some integer $k \geq 0$, $c_k = 3^{2^k}$. We must show that $c_{k+1} = 3^{2^{k+1}}$. But by definition of c_0, c_1, c_2 ..., substitution from the inductive hypothesis, and the laws of algebra,

$$c_{k+1} = (c_k)^2 = (3^{2^k})^2 = 3^{2 \cdot 2^k} = 3^{2^{k+1}}$$

[as was to be shown].

29. *Proof by induction:*

The formula holds for $n = 1$: For $n = 1$ the left-hand side of the equation is

$$\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}^1 = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$$

and the right-hand side is

$$\begin{bmatrix} 2^1 & 1 \cdot 2^{1-1} \\ 0 & 2^1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$$

also. So the formula holds for $n = 1$.

If the formula holds for $n = k$ then it holds for $n = k + 1$: Suppose that for some integer $k \geq 1$,

$$\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}^k = \begin{bmatrix} 2^k & k \cdot 2^{k-1} \\ 0 & 2^k \end{bmatrix}$$

We must show that

$$\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}^{k+1} = \begin{bmatrix} 2^{k+1} & (k+1) \cdot 2^{(k+1)-1} \\ 0 & 2^{k+1} \end{bmatrix}.$$

or, equivalently,

$$\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}^{k+1} = \begin{bmatrix} 2^{k+1} & (k+1) \cdot 2^k \\ 0 & 2^{k+1} \end{bmatrix}.$$

But by definition of matrix multiplication, substitution from the inductive hypothesis, and the laws of algebra

$$\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}^{k+1} = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}^{k} = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 2^k & k \cdot 2^{k-1} \\ 0 & 2^k \end{bmatrix}$$
$$= \begin{bmatrix} 2 \cdot 2^k + 1 \cdot 0 & 2 \cdot k \cdot 2^{k-1} + 1 \cdot 2^k \\ 0 \cdot 2^k + 2 \cdot 0 & 0 \cdot k \cdot 2^{k-1} + 2 \cdot 2^k \end{bmatrix} = \begin{bmatrix} 2^{k+1} & (k+1) \cdot 2^k \\ 0 & 2^{k+1} \end{bmatrix}.$$

[as was to be shown].

Section 4.4

2. *Proof:* Let $P(n)$ be the property "b_n is divisible by 3." We prove by strong mathematical induction that this property is true for all integers $n \geq 1$.

   The property is true for $n = 1$ and $n = 2$: $b_1 = 3$ and $b_2 = 6$ and both 3 and 6 are divisible by 3.

   If the property is true for all integers i with $1 \leq i < k$ then it is true for k:

   Let $k > 2$ be an integer and suppose b_i is divisible by 3 for all integers i with $1 \leq i < k$. *[This is the inductive hypothesis.]* We must show that b_k is divisible by 3.

   By definition of b_k, $b_k = b_{k-2} + b_{k-1}$. Since $k > 2$, $1 \leq k - 2 < k$ and $1 \leq k - 1 < k$, and so by inductive hypothesis, both b_{k-1} and b_{k-2} are divisible by 3.

   Thus *[by exercise 14 of Section 3.3]* the sum of b_{k-1} and b_{k-2}, which is b_k, is also divisible by 3 *[as was to be shown].*

5. *Proof:* Let $P(n)$ be the inequality "$e_n \leq 3^n$." We prove by strong mathematical induction that this inequality is true for all integers $n \geq 0$.

   The inequality is true for $n = 0$, 1 and 2: $e_0 = 1$, $e_1 = 2$ and $e_2 = 3$ and $1 \leq 3^0$, $2 \leq 3^1$ and $3 \leq 3^3$.

   If the property is true for all integers i with $1 \leq i < k$ then it is true for k:

   Let $k > 2$ be an integer and suppose $e_i \leq 3^i$ for all integers i with $1 \leq i < k$. *[This is the inductive hypothesis.]* We must show that $e_k \leq 3^k$.

   By definition of e_k, $e_k = e_{k-1} + e_{k-2} + e_{k-3}$. Since $k > 2$, $1 \leq k-3 < k$ and so by inductive hypothesis, $e_{k-1} \leq 3^{k-1}$, $e_{k-2} \leq 3^{k-2}$, and $e_{k-3} \leq 3^{k-3}$.

   Adding the inequalities and using the basic laws of algebra gives

$$\begin{aligned} e_{k-1} + e_{k-2} + e_{k-3} &\leq 3^{k-1} + 3^{k-2} + 3^{k-3} \\ &\leq 3^{k-1} + 3^{k-1} + 3^{k-1} \\ &= 3 \cdot 3^{k-1} \\ &= 3^k \end{aligned}$$

But $e_{k-1}+e_{k-2}+e_{k-3}=e_k$ and so $e_k \leq 3^k$ *[as was to be shown]*.

10. The inductive step fails when $k=1$. The reason is that to go from $k=1$ to $k=2$, one evaluates

$$\frac{r^{k-1}\cdot r^{k-1}}{r^{k-2}}$$

for $k=1$. But the inductive hypothesis only says that $r^i=1$ for all i with $0 \leq i < k$ and when $k=1$ then $k-2=-1<0$. Therefore it cannot be deduced from the inductive hypothesis that $r^{k-2}=1$.

11. This problem is solved in the book.

13. The answer is "no".

Counterexample 1:

Let $P(n)$ be "$n+24$ is composite." Then $P(0)$, $P(1)$, and $P(2)$ are all true (because 24, 25, and 26 are all composite), and for all integers $k \geq 0$, if $P(k)$ is true, then $P(3k)$ is true (because $3k+24 = 3\cdot(k+8)$ is composite for every integer k).

But it is false that $n+24$ for is composite for all integers $n \geq 0$, e.g. 5+24=29 is prime (note that $5 \neq 3k$ for any integer k).

Counterexample 2:

Let $P(n)$ be "$n=0$, $n=1$, $n=2$, or $n=3r$ for some integer r." Then $P(0)$, $P(1)$, and $P(2)$ are all true (because an *or* statement is true if any component is true), and for all integers $k \geq 3$, if $P(k)$ is true, then $P(3k)$ is true (also by definition of the truth value of an *or* statement and by definition of $P(n)$).

But $P(n)$ is not true for all integers $n \geq 0$ (because, for instance, $P(4)$ is not true.

(There may be other counterexamples besides these two.)

Section 4.5

4. *Proof:* Suppose the condition $2^n < (n+2)!$ is true before entry to the loop. Then $2^{n_{old}} < (n_{old}+2)!$. After execution of the loop, $n_{new} = n_{old}+1$. So

$$\begin{aligned} 2^{n_{new}} &= 2^{n_{old}+1} \\ &= 2\cdot 2^{n_{old}} \\ &< 2\cdot(n_{old}+2)! \\ &< (n_{old}+3)\cdot(n_{old}+2)! \quad \textit{[because } n_{old} \geq 0\textit{]} \\ &= (n_{old}+3)! \\ &= (n_{new}+2)! \end{aligned}$$

Hence $2^{n_{new}} < (n_{new}+2)!$.

6. This problem is solved in the book.

9. I **Basis Property:** $I(0)$ is the statement "both A and a are even integers or both are odd integers and $a \geq -1$." According to the pre-condition, this statement is true.

II **Inductive Property:** Suppose k is a nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. Hence as execution reaches the top of the loop, $a_{old} > 0$ and $I(k)$ holds (i.e. a_{old} and A are both even or both odd integers, and $a_{old} \geq -1$).

Execution of statement 1 sets a_{new} equal to $a_{old} - 2$. Hence a_{new} has the same parity as a_{old} which is the same as A.

Also, since $a_{old} > 0$, $a_{new} = a_{old} - 2 > 0 - 2 = -2$. But a_{new} is an integer. So since $a_{new} > -2$, $a_{new} \geq -1$.

Hence after the loop iteration, $I(k+1)$ is true.

III **Eventual falsity of guard:** The guard G is the condition $a > 0$. After each iteration of the loop, $a_{new} = a_{old} - 2 < a_{old}$, and so successive iterations of the loop give a strictly decreasing sequence of integer values of a which eventually becomes less than or equal to zero, at which point G becomes false.

IV **Correctness of the post-condition:** Suppose that N is the least number of iterations after which G is false and $I(N)$ is true.

Then (since G is false) $a \leq 0$ and (since $I(N)$ is true) both a and A are even integers or both are odd integers, and $a \geq -1$.

Putting the inequalities together gives $-1 \leq a \leq 0$, and since a is an integer, $a = -1$ or $a = 0$. Since A and a have the same parity, $a = 0$ if A is even and $a = -1$ if A is odd. This is the post-condition.

10. I **Basis Property:** $I(0)$ is the statement

(1) a and b are nonnegative integers with $\gcd(a, b) = \gcd(A, B)$,

(2) at most one of a and b equals zero,

(3) $0 \leq a + b \leq A + B - 0$

According to the pre-condition, A and B are positive integers, and $a = A$ and $b = B$, so $I(0)$ is true.

II **Inductive Property:** Suppose k is a nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. Then as execution reaches the top of the loop, $a_{old} \neq 0$ and $b_{old} \neq 0$ and

(1) a_{old} and b_{old} are nonnegative integers with $\gcd(a_{old}, b_{old}) = \gcd(A, B)$,

(2) at most one of a_{old} and b_{old} equals zero,

(3) $0 \leq a_{old} + b_{old} \leq A + B - k$

After execution of the statement

"**if** $a \geq b$ **then** $a := a - b$ **else** $b := b - a$"

we have the following:

(1) *Case 1* $(a_{old} \geq b_{old})$*:* In this case $a_{new} = a_{old} - b_{old} \geq 0$ and $b_{new} = b_{old} \geq 0$, and so both a_{new} and b_{new} are nonnegative. Also

$$\begin{aligned} \gcd(a_{new}, b_{new}) &= \gcd(a_{old} - b_{old}, b_{old}) \\ &= \gcd(a_{old}, b_{old}) \end{aligned}$$

by Lemma 3.8.3. But $\gcd(a_{old}, b_{old}) = \gcd(A, B)$ by (1) above. Hence $\gcd(a_{new}, b_{new}) = \gcd(A, B)$.

Case 2 $(a_{old} < b_{old})$*:* In this case $b_{new} = b_{old} - a_{old} \geq 0$ and $a_{new} = a_{old} \geq 0$, and so both a_{new} and b_{new} are nonnegative. Also

$$\begin{aligned} \gcd(a_{new}, b_{new}) &= \gcd(a_{old}, b_{old} - a_{old}) \\ &= \gcd(a_{old}, b_{old}) \end{aligned}$$

by Lemma 3.8.3. But $\gcd(a_{old}, b_{old}) = \gcd(A, B)$ by (1) above. Hence $\gcd(a_{new}, b_{new}) = \gcd(A, B)$.

(2) Because G is true $a_{old} \neq 0$ and $b_{old} \neq 0$, and by (1) above both a_{old} and b_{old} are nonnegative. Hence $a_{old} \geq 0$ and $b_{old} \geq 0$. Since either $a_{new} = a_{old}$ or $b_{new} = b_{old}$, at most one of a_{new} and b_{new} equals zero.

(3) Observe that

$$\begin{aligned} a_{new} + b_{new} &= \begin{cases} a_{old} - b_{old} + b_{old} & \text{if} \quad a_{old} \geq b_{old} \\ a_{old} + b_{old} - a_{old} & \text{if} \quad b_{old} > a_{old} \end{cases} \\ &= \begin{cases} a_{old} & \text{if} \quad a_{old} \geq b_{old} \\ b_{old} & \text{if} \quad b_{old} > a_{old}. \end{cases} \end{aligned}$$

But since $a_{old} \neq 0$ and $b_{old} \neq 0$ and a_{old} and b_{old} are nonnegative integers, $a_{old} \geq 1$ and $b_{old} \geq 1$.
Hence $a_{old} - 1 \geq 0$ and $b_{old} - 1 \geq 0$, and so $a_{old} \leq a_{old} + b_{old} - 1$.
But by (3) above $a_{old} + b_{old} \leq A + B - k$. It follows that

$$a_{new} + b_{new} \leq a_{old} + b_{old} - 1 \leq A + B - (k + 1).$$

III **Eventual Falsity of Guard:** The Guard G is the condition $a \neq 0$ and $b \neq 0$.

Suppose G is never false.. *[We will derive a contradiction.]* Then the loop would iterate indefinitely. But by II. above, for all integers n, after n iterations of the loop, $a \geq 0$, $b \geq 0$, at most one of a and b equals zero, and $0 \leq a + b \leq A + B - n$.

Hence after $A + B$ iterations,

$$0 \leq a + b \leq A + B - (A + B) = 0.$$

Since $a \geq 0$ and $b \geq 0$, it is $a = b = 0$. But this contradicts the fact that at most one of a and b equals zero. Hence the supposition is false, and so after some iteration G is false.

IV **Correctness of the Post-Condition:** Suppose that N is the least number of iterations after which G is false and $I(n)$ is true.

Then (since G is false) $a = 0$ or $b = 0$, and (since $I(n)$ is true) a and b are nonnegative integers with $\gcd(a, b) = \gcd(A, B)$ and at most one of a and b equals zero. Thus

$$\gcd(a, b) = \begin{cases} \gcd(0, b) & \text{if} \quad a = 0 \\ \gcd(a, 0) & \text{if} \quad b = 0 \end{cases}$$

By Lemma 3.8.1. $\gcd(0, b) = b$ and $\gcd(a, 0) = a$. Hence one of a or b is zero and the other is nonzero, and $\gcd(A, B)$ equals whichever of a or b is nonzero.