

## Problem Set #8 Solutions

---

### 1) The formula is $n(n+1)$ . Proof:

We will show that property  $P(n)$  holds for all integers  $n > 0$  using the weak mathematical induction. Here, property  $P(n)$  means that

$$2 + 4 + \dots + \dots + 2n = n(n+1)$$

The base case is for  $n = 1$ .

BASE CASE:

$$1(1 + 1) = 2 = 2$$

INDUCTIVE CASE:

Assume as our inductive hypothesis that  $P(k)$  holds. Now we will show that this implies that  $P(k+1)$  holds, namely that

$$2 + \dots + 2k + 2(k+1) = (k+1)(k+2)$$

Let's begin with our inductive hypothesis and manipulate it to reach our desired conclusion.

$$\begin{array}{llll} 2 + \dots + 2k & = & k(k+1) & \text{by IH} \\ 2 + \dots + 2k + 2(k+1) & = & k(k+1) + 2(k+1) & \text{add } (k+1) \text{ to both sides} \\ = & & (k+1)(k+2) & \text{factor out } (k+1) \end{array}$$

CONCLUSION:

We have shown that our base case  $P(0)$  holds and that  $P(n+1)$  holds whenever  $P(n)$  holds (i.e.,  $P(n) \rightarrow P(n+1)$ ). By the principle of mathematical induction,  $P(n)$  holds for all integers  $n > 0$ .

## 2) Proof:

We will show that property  $P(n)$  holds for all integers  $n \geq 0$  using the weak mathematical induction. Here, property  $P(n)$  means that  $3 \cdot 5^0 + 3 \cdot 5 + 3 \cdot 5^2 + \dots + 3 \cdot 5^n = 3 \cdot (5^{n+1} - 1)/4$

BASE CASE:

$$3 \cdot (5^{0+1} - 1)/4 = 3 \cdot (4)/4 = 3$$

INDUCTIVE CASE:

Assume as our inductive hypothesis that  $P(k)$  holds. Now we will show that this implies that  $P(k+1)$  holds, namely that

$3 \cdot 5^0 + 3 \cdot 5 + \dots + 3 \cdot 5^k + 3 \cdot 5^{k+1} = 3 \cdot (5^{k+1+1} - 1)/4$  Let's begin with hypothesis and manipulate it to prove the desired conclusion.

$$\begin{aligned} 3 + \dots + 3 \cdot 5^k &= 3 \cdot (5^{k+1} - 1)/4 \\ 3 + \dots + 3 \cdot 5^k + 3 \cdot 5^{k+1} &= 3 \cdot (5^{k+1} - 1)/4 + 3 \cdot 5^{k+1} \\ &= 3 \cdot (5^{k+1} - 1)/4 + 4(3 \cdot 5^{k+1})/4 \\ &= (3 \cdot (5^{k+1} - 1) + 4(3 \cdot 5^{k+1}))/4 \\ &= (15 \cdot 5^{k+1} - 3)/4 \\ &= 3 \cdot (5 \cdot 5^{k+1} - 1)/4 \\ &= 3 \cdot (5^{k+1+1} - 1)/4 \end{aligned}$$

CONCLUSION:

We have shown that our base case  $P(0)$  holds and that  $P(n+1)$  holds whenever  $P(n)$  holds (i.e.,  $P(n) \rightarrow P(n+1)$ ). By the principle of mathematical induction,  $P(n)$  holds for all integers  $n \geq 0$ .

### 3) Proof:

We will show that property  $P(n)$  holds for all integers  $n \geq 0$  using the weak mathematical induction. Here, property  $P(n)$  means that  $1 \cdot 2 + 2 \cdot 3 + \dots + n \cdot (n+1) = n(n+1)(n+2)/3$

#### BASE CASE:

In the case of  $P(1)$ :

$$1(1+1) = 2 = (1 \cdot 2 \cdot 3)/3$$

#### INDUCTIVE CASE:

Assume as our inductive hypothesis that  $P(k)$  holds. Now we will show that this implies that  $P(k+1)$  holds, namely that

$$1 \cdot 2 + 2 \cdot 3 + \dots + k \cdot (k+1) + (k+1)((k+1) + 1) = (k+1)((k+1)+1)((k+1)+2)/3$$

or, simplifying:

$$1 \cdot 2 + 2 \cdot 3 + \dots + k \cdot (k+1) + (k+1)(k+2) = (k+1)(k+2)(k+3)/3$$

Let's begin with hypothesis and manipulate it to prove the desired conclusion.

$$1 \cdot 2 + 2 \cdot 3 + \dots + k \cdot (k+1) = k(k+2)(k+3)/3 \quad \text{Inductive Hyp.}$$

$$1 \cdot 2 + \dots + k \cdot (k+1) + (k+1)(k+2) = k(k+1)(k+2)/3 + (k+1)(k+2) \quad \text{Algebra}$$

$$1 \cdot 2 + \dots + k \cdot (k+1) + (k+1)(k+2) = (k/3 + 1)(k+1)(k+2) \quad \text{Algebra}$$

$$1 \cdot 2 + \dots + k \cdot (k+1) + (k+1)(k+2) = (k/3 + 1)(k+1)(k+2) \quad \text{Algebra}$$

$$1 \cdot 2 + \dots + k \cdot (k+1) + (k+1)(k+2) = ((k+3)/3)(k+1)(k+2) \quad \text{Algebra}$$

$$1 \cdot 2 + \dots + k \cdot (k+1) + (k+1)(k+2) = (k+1)(k+2)(k+3)/3$$

Therefore, we have reached our desired conclusion  $P(k+1)$  through algebraic operations,

#### CONCLUSION:

We have shown that our base case  $P(1)$  holds and that  $P(n+1)$  holds whenever  $P(n)$  holds (i.e.,  $P(n) \rightarrow P(n+1)$ ). By the principle of mathematical induction,  $P(n)$  holds for all integers  $n \geq 1$ .

#### 4) Formula: $d_n = 3^n \cdot n!$

To find this formula, we find a closed-form version of the sequence. We can see that the sequence  $u_1 = 3, u_n = u_{n-1} + 3$  produces the values

3, 6, 9, 12, ... ,  $3n$

So the closed-form is  $u_n = 3n$ . Since you will use this fact in the main proof, you should prove that it is correct. At the very minimum, you should say “clearly”. That indicates that you know that the formula needs justification, but that you think that it’s obvious. That’s stretching it a bit, though—we’d prefer the proof, which follows the main proof.

Now, when we consider the product  $d_n = u_1 \cdot u_2 \cdot \dots \cdot u_n$ , we can rewrite it as

$d_n = 3 \cdot 6 \cdot \dots \cdot (3n)$  Each of the  $n$  terms has a factor of 3, so

$$d_n = 3^n \cdot (1 \cdot 2 \cdot \dots \cdot n)$$

$$d_n = 3^n \cdot n!$$

We will guess this as the closed-form solution. To prove this is correct with regards to the recursive definition of the sequence we use induction:

BASE CASE:

$$P(1): d_1 = u_1 = 3 = 3^1 \cdot 1!$$

INDUCTIVE CASE: Let us assume that  $P(k)$  holds for some  $k \geq 1$ , that is,  $d_k = u_1 \cdot u_2 \cdot \dots \cdot u_k = 3^k \cdot k!$   
We will use this to prove that  $P(k+1)$  holds, that is,  $d_{k+1} = u_1 \cdot u_2 \cdot \dots \cdot u_k \cdot u_{k+1} = 3^{k+1} \cdot (k+1)!$

$u_1 \cdot u_2 \cdot \dots \cdot u_k = 3^k \cdot k!$	Inductive Hypothesis
$u_1 \cdot u_2 \cdot \dots \cdot u_k \cdot u_{k+1} = 3^k \cdot k! \cdot u_{k+1}$	Algebra
$d_k = 3^k \cdot k! \cdot 3(k+1)$	Replacement of $u_k$ with $3(k+1)$
$d_k = 3^{k+1} \cdot (k+1)!$	Algebra

CONCLUSION:

We have shown that our base case  $P(1)$  holds and that  $P(n+1)$  holds whenever  $P(n)$  holds (i.e.,  $P(n) \rightarrow P(n+1)$ ). By the principle of mathematical induction,  $P(n)$  holds for all integers  $n \geq 1$ , proving that our formula for  $d_n$  is correct

(continued next page)

Subproof:

Given the recursively defined sequence  $u_1 = 3$ ,  $u_n = u_{n-1} + 3$ , show that

$P(n)$ :  $u_n = 3n$  holds for all positive integers  $n$ .

BASE CASE

$P(1)$  states that  $u_1 = 3 \cdot 1 = 3$ , and this is true by the definition of the sequence.

INDUCTIVE STEP

Assume  $P(k)$ :  $u_k = 3k$

Show  $P(k+1)$ :  $u_{k+1} = 3 \cdot (k+1)$

Proof:

$$\begin{aligned}u_{k+1} &= u_k + 3 \\ &= 3k + 3 \\ &= 3(k + 1)\end{aligned}$$

Recursive definition of sequence  
Inductive hypothesis  
Factoring

So,  $P(k+1)$  holds when  $P(k)$  holds, and this, with the base case, means that  $P(n)$  holds for all positive  $n$  by the Principle of Mathematical Induction.

5) This holds true for all  $n \geq 4$ . First, let us show that it does not hold for  $n < 4$ .

n	n!	$2^n$
0	1	1
1	1	2
2	2	4
3	6	8

BASE CASE: For the case of  $n = 4$ ,  $4! = 24$  and  $2^4 = 16$ , so  $n! > 2^n$ .

INDUCTIVE CASE: Let us assume that  $P(k)$  holds for some  $k \geq 4$ , that is,  $k! > 2^k$ . We will use this to prove that  $P(k+1)$  holds, that is,  $(k+1)! > 2^{k+1}$ .

$k! > 2^k$	Inductive Hypothesis
$(k+1)k! > (k+1) \cdot 2^k$	Algebra
$(k+1)! > (k+1) \cdot 2^k$	Definition of factorial
$(k+1)! > 2 \cdot 2^k$	Preserves inequality, because $k+1 > 2$ by IH
$(k+1)! > 2^{k+1}$	

The key step here is that, since we are working with an inequality, we can substitute 2 for  $(k+1)$  and preserve the inequality, because  $(k+1) > 2$ . Therefore, we have proven  $P(k) \rightarrow P(k+1)$ .

CONCLUSION:

We have shown that our base case  $P(4)$  holds and that  $P(n+1)$  holds whenever  $P(n)$  holds (i.e.,  $P(n) \rightarrow P(n+1)$ ). By the principle of mathematical induction,  $P(n)$  holds for all integers  $n \geq 4$ .

6) We can form any integer amount except 1¢, 3¢, and 5¢.

BASE CASES:

As special cases we show we can get 2¢ (one 2¢ stamp), 4¢ (two 2¢ stamps), 6¢ (three 2¢ stamps), and 7¢ (one 7¢ stamp). Now, we will look inductively at the proof for all values  $> 7$ ¢.

INDUCTIVE CASE:

Assume as our inductive hypothesis that  $P(k)$  holds, namely, that the machine can make  $k$ ¢ out of 2¢ and 7¢ stamps for some  $k > 7$ , suppose  $k$ ¢ =  $x \cdot 2$ ¢ +  $y \cdot 7$ ¢ for  $x \geq 0$ ,  $y \geq 0$ .

We want to show  $P(k+1)$ , that the machine can make  $(k+1)$ ¢.

Consider two cases: First, that the solution for  $k$ ¢ involves at least one 7¢ stamp, that is,  $y \geq 1$ . The machine can then make  $(k + 1)$ ¢ by using one fewer 7¢ stamp, and four additional 2¢ stamps, ie, use  $(x + 4)$  2¢ stamps and  $(y - 1)$  7¢ stamps. The total value dispensed is then

$(x + 4) \cdot 2$ ¢ + $(y - 1) \cdot 7$ ¢	Algebra
$x \cdot 2$ ¢ + $y \cdot 7$ ¢ + 8¢ - 7¢	Algebra
$k$ ¢ + 1¢	Application of inductive hypothesis

Now, suppose that the solution for  $k$ ¢ involved no 7¢ stamps, that is,  $y = 0$ . If this is the case, since  $k > 7$ , we must have  $x \geq 4$ . So, the machine can make  $(k+1)$ ¢ by removing three 2¢ stamps, and adding one 7¢ stamp, ie use  $(x - 3)$  2¢ stamps and one 7¢ stamps. The total value dispensed is then

$(x - 3) \cdot 2$ ¢ + 7¢	Algebra
$x \cdot 2$ ¢ - 6¢ + 7¢	Algebra
$k$ ¢ + 1¢	Application of inductive hypothesis

Therefore, in either case the machine can dispense  $(k+1)$ ¢ worth of stamps, and we have shown that  $P(k) \rightarrow P(k+1)$  for  $k \geq 7$ .

CONCLUSION:

We have shown that our base case  $P(7)$  holds and that  $P(n+1)$  holds whenever  $P(n)$  holds (i.e.,  $P(n) \rightarrow P(n+1)$ ). By the principle of mathematical induction,  $P(n)$  holds for all integers  $n \geq 7$ . We have also shown the special cases of  $n = 2$ ,  $n = 4$ , and  $n = 6$ . Therefore,  $P(n)$  is true for all positive  $n$  except  $n = 1$ ,  $n = 3$ , and  $n = 5$ .

## 7) Proof:

We will show that property  $P(n)$  holds for odd integers  $n > 0$  using the weak mathematical induction. Here, property  $P(n)$  will mean means that

$$8 \mid (a_n)^2 - 1$$

Where  $a_n$  represents the  $n^{\text{th}}$  odd integer, ie  $a_n = (2n - 1)$ . We have introduced the  $a_n$  notation to provide a mapping from positive integers to positive odd integers, ie  $(1 \rightarrow 1, 2 \rightarrow 3, 3 \rightarrow 5, \text{ etc})$ . Thus, if we can prove that  $P(n)$  holds for all integers  $n > 0$ , then we show that  $8 \mid m^2 - 1$  for all odd integers  $m$ .

The base case is for  $n = 1$  (for the first odd integer  $2(1) - 1 = 1$ ).

BASE CASE:

$$P(1) = (a_1)^2 - 1 = (2(1) - 1)^2 - 1 = 1 - 1 = 0 = 8c \text{ for } c = 0$$

INDUCTIVE CASE:

Assume as our inductive hypothesis that  $P(k)$ , so  $8 \mid (a_k)^2 - 1$ , or equivalently  $8 \mid (2k - 1)^2 - 1$ . Now we will show that this implies that  $P(k+1)$  holds, namely that

$$\begin{aligned} 8 \mid (a_{k+1})^2 - 1 \\ 8 \mid (2(k+1) - 1)^2 - 1 \\ 8 \mid (2k + 1)^2 - 1 \end{aligned}$$

In other words, that the  $k+1$ th odd integer is divisible by 8. We start with our inductive hypothesis and manipulate it to demonstrate our desired conclusion:

$$\begin{aligned} (2k - 1)^2 - 1 &= 8c && \text{(Inductive Hypothesis)} \\ (4k^2 - 4k + 1) - 1 &= 8c && \text{(Algebraic expansion)} \\ (4k^2 - 4k + 1) - 1 + 8k &= 8c + 8k && \text{(8k added to each side of equation)} \\ (4k^2 + 4k + 1) - 1 &= 8(c + k) && \text{(Re-arranged terms)} \\ (2k + 1)^2 - 1 &= 8(c + k) && \text{(Factoring)} \end{aligned}$$

Therefore,  $8 \mid (2k + 1)^2 - 1$ , since  $(c + k)$  is an integer, and we have proven  $P(k + 1)$ .

CONCLUSION:

We have shown that our base case  $P(0)$  holds and that  $P(n+1)$  holds whenever  $P(n)$  holds (i.e.,  $P(n) \rightarrow P(n+1)$ ). By the principle of mathematical induction,  $P(n)$  holds for all integers  $n > 0$ . In other words, all odd integers are divisible by 8.

### 7) Alternate, non-inductive proof:

Let us directly consider the value  $(2k - 1)^2 - 1$ , which represents  $n^2 - 1$  for some odd integer  $n$ :

$$\begin{aligned}(2k - 1)^2 - 1 &= (4k^2 - 4k + 1) - 1 \\ &= 4k^2 - 4k \\ &= 4(k^2 - k) \\ &= 4(k)(k - 1)\end{aligned}$$

Now, since  $k$  itself is an integer, it must be odd or even, and we can consider each case:

Case 1:  $k$  is odd, say  $k = 2m + 1$

$$\begin{aligned}(2k - 1)^2 - 1 &= 4(k)(k - 1) \\ &= 4(2m + 1)(2m + 1 - 1) \\ &= 4(2m + 1)(2m) \\ &= 8(m)(2m + 1)\end{aligned}$$

So,  $8 \mid (2k - 1)^2 - 1$  in this case.

Case 2:  $k$  is even, say  $k = 2m$

$$\begin{aligned}(2k - 1)^2 - 1 &= 4(k)(k - 1) \\ &= 4(2m)(2m - 1) \\ &= 8(m)(2m - 1)\end{aligned}$$

Again we see that  $8 \mid (2k - 1)^2 - 1$ .

Therefore, in either case we have  $8 \mid (2k - 1)^2 - 1$ , and thus  $8 \mid n^2 - 1$  for any odd integer  $n$ .

**8) The problem is the assumption is the application of the inductive hypothesis wherein it is assumed that  $a^{n-1} = 1$ .** The inductive hypothesis assumes that  $a^i = 1$  for all  $i = 0, 1, \dots, n$ . However, 0 is within the domain of values for  $n$  ( $n \geq 0$ ), and so if in our inductive step we allow  $n = 0$ , then  $a^{n-1} = a^{-1}$ , which our inductive hypothesis does not cover (and in truth,  $a^{-1} = 1$  only when  $a = 1$ ).

In this case, one can reason that the induction step must fail to show  $P(0) \rightarrow P(1)$ , since  $P(0)$  is in fact true ( $a^0 = 1$ ) but  $P(1)$  is not. In general, if an erroneous inductive proof appears to show something which is not true, there has to be a problem either with the base case, or with applying the inductive hypothesis to show  $P(n) \rightarrow P(n + 1)$  for the first value of  $n+1$  which doesn't satisfy  $P(n + 1)$ .

### 9) Proof:

We will show that property  $P(n)$  holds for all integers  $n > 0$  using the weak mathematical induction. Here, property  $P(n)$  means that

$$7 \mid 11^n - 4^n$$

OR

$$11^n - 4^n = 7c \text{ for some } c$$

The base case is for  $n = 1$ .

$$\text{BASE CASE: } 11^1 - 4^1 = 11 - 4 = 7 = 7c \text{ for } c = 1$$

INDUCTIVE CASE:

Assume as our inductive hypothesis that  $P(k)$  holds. Now we will show that this implies that  $P(k+1)$  holds, namely that

$$7 \mid 11^{k+1} - 4^{k+1}$$

OR

$$11^{k+1} - 4^{k+1} = 7c \text{ for some } c$$

Let's begin with our inductive hypothesis and manipulate it to get our desired conclusion:

$$\begin{aligned} 11^{k+1} - 4^{k+1} &= 11 \cdot 11^k - 4 \cdot 4^k && \text{Algebra} \\ &= 11 \cdot 11^k - (11 - 7) \cdot 4^k && \text{Algebra } (11 - 7 = 4) \\ &= 11 \cdot 11^k - 11 \cdot 4^k + 7 \cdot 4^k && \text{Algebra} \\ &= 11 \cdot (11^k - 4^k) + 7 \cdot 4^k && \text{Algebra} \\ &= 11 \cdot (7c) + 7 \cdot 4^k && \text{Inductive Hypothesis } (11^k - 4^k = 7c) \\ &= 7 \cdot (11c + 4^k) && \text{Factoring} \end{aligned}$$

Now we can see that  $11^{k+1} - 4^{k+1} = 7 \cdot (11c + 4^k)$ , so  $7 \mid 11^{k+1} - 4^{k+1}$  and we have proven  $P(k + 1)$

CONCLUSION:

We have shown that our base case  $P(0)$  holds and that  $P(n+1)$  holds whenever  $P(n)$  holds (i.e.,  $P(n) \rightarrow P(n+1)$ ). By the principle of mathematical induction,  $P(n)$  holds for all integers  $n > 0$ .

10)

a)  $E_k(M) = M \oplus K$

	1	0	1	1	0	1	0	0	0	1
$\oplus$	1	0	0	0	1	1	0	1	1	1
<hr/>										
	0	0	1	1	1	0	0	1	1	0

b)  $E_k(E_k(M)) = E_k(M) \oplus K$

	0	0	1	1	1	0	0	1	1	0
$\oplus$	1	0	0	0	1	1	0	1	1	1
<hr/>										
	1	0	1	1	0	1	0	0	0	1

This value is just the original message M. The significance of this is that the encryption operation is invertible, that is, it can be undone by anybody with knowledge of the key. This is a necessary condition for any encryption scheme to be useful.

This can also be seen algebraically:

$$\begin{aligned} E_k(E_k(M)) &= E_k(M) \oplus K \\ &= (M \oplus K) \oplus K \\ &= M \oplus (K \oplus K) \\ &= M \oplus 0 \\ &= M \end{aligned}$$

Furthermore, one-time pad decryption is identical to encryption, which is advantageous in that one implementation in hardware or software can both encrypt and decrypt messages. Finally, since both operations are simply an exclusive-or they are very efficient to implement. This is a major practical advantage of one-time pad and similar schemes, such as stream ciphers.

11)

a)	$C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K)$	Known values
	$= M_1 \oplus K \oplus M_2 \oplus K$	Associative property
	$= M_1 \oplus M_2 \oplus K \oplus K$	Commutative property
	$= M_1 \oplus M_2 \oplus 0$	Self-inversion
	$= M_1 \oplus M_2$	Zero identity

While Eve does not learn the exact contents of either message, she does learn the value of the two messages exclusive-or'ed with one another. For many types of messages this is a major violation of secrecy.

b)	$C_1 \oplus C_2 = M_1 \oplus M_2$	Equation from part (a)
	$M_1 \oplus C_1 \oplus C_2 = M_1 \oplus M_1 \oplus M_2$	X-or both sides with $M_1$
	$M_1 \oplus C_1 \oplus C_2 = 0 \oplus M_2$	Self-inversion
	$M_1 \oplus C_1 \oplus C_2 = M_2$	Zero identity

Since  $M_1$ ,  $C_1$ , and  $C_2$  are all known to eve, she can therefore compute  $M_2$