

## Problem Set #8

---

**Due: 11/10**

**88 points total; 8 points for each problem**

*Prove all the following using either weak or strong induction. Proper form for your proofs is important!*

1) Find a formula for the sum of the first  $n$  even positive integers and then prove that your formula is correct.

Note that since we are dealing only with even integers, there is sometimes a tendency to think that in the inductive step, you will assume  $P(k)$  for some even integer  $k$  and then show  $P(k+2)$ . But that is not how our principle of induction works—it is used to prove that some proposition  $P(n)$  holds for all integers. So for this problem we have:

$P(n)$  : the sum of the first  $n$  even integers is  $\text{YourFormula}(n)$ .

In the inductive step, you assume  $P(k)$  and prove  $P(k+1)$ . One way to think about this is to consider the sequence  $a_1, a_2, a_3, \dots$  where  $a_i$  is the  $i^{\text{th}}$  even number. Then  $P(n)$  makes an assertion about the sum of the first  $n$  terms of this sequence.

2) Prove:  $3 + 3 \cdot 5 + 3 \cdot 5^2 + \dots + 3 \cdot 5^n = 3 \cdot (5^{n+1} - 1) / 4$

3) Let  $S_n = 1 \cdot 2 + 2 \cdot 3 + \dots + n(n+1)$  for  $n \geq 1$ .  
So  $S_1 = 1(1+1) = 2$

Prove that  $S_n = n(n+1)(n+2)/3$  for all positive integers  $n$

4) Consider the sequence  $u$  defined as follows:

$$u_1 = 3$$

$$u_n = u_{n-1} + 3 \text{ for } n \geq 2.$$

Find a formula for the sequence  $d$  defined by

$$d_n = \prod_{i=1}^n u_i \text{ for } n \geq 1.$$

Prove that your formula is correct.

5) For which non-negative values of  $n$  ( $n$  is an integer) is  $n! > 2^n$ ? Prove your answer.

6) A stamp machine has only 2-cent stamps and 7-cent stamps. Which amounts of postage can the machine dispense assuming a limitless supply of these two kinds of stamps? Prove your answer.

7) Prove that  $n^2 - 1$  is divisible by 8 whenever  $n$  is an odd positive integer. (This is similar to a problem on the last assignment, but here you are using proof by induction.)

(more on the other side)

8) What is wrong with the following "induction"?

NonTheorem  $P(n)$ :  $a^n = 1$  for all  $a \neq 0$  and all  $n \geq 0$ .

Base Case:  $a^0 = 1$

Inductive Hypothesis: Assume that  $a^i = 1$  for  $i = 0, 1, \dots, n$  and prove that  $a^{n+1} = 1$

NonProof:

$$\begin{aligned}
 a^{n+1} &= a^{n+1} \cdot (a^{-1} / a^{-1}) && \text{multiplication by 1} \\
 &= (a^{n+1} \cdot a^{-1}) / a^{-1} && \text{associative law} \\
 &= ((a^n \cdot a) \cdot a^{-1}) / a^{-1} && \text{law of exponents} \\
 &= (a^n \cdot (a \cdot a^{-1})) / a^{-1} && \text{associative law} \\
 &= (a^n \cdot a^0) / a^{-1} && \text{multiplication} \\
 &= (1 \cdot 1) / 1 && \text{inductive hypothesis} \\
 &= 1
 \end{aligned}$$

By the principle of mathematical induction,  $P(n)$  is true for all  $n$ .

9) Show that 7 divides  $11^n - 4^n$  whenever  $n$  is a positive integer.

**The following problems are based on the lectures on cryptography.**

10) **One-time pad basics** Alice and Bob are encrypting binary-string messages using the one-time pad system. To recap, this means the encryption of a message string is  $E_K(M) = M \oplus K$ , where  $K$  is a random, previously agreed upon pad. The symbol  $\oplus$  denotes the XOR (exclusive or) operation. For two binary digits  $X$  and  $Y$ ,  $X \oplus Y$  is 1 if  $X$  and  $Y$  have different values, and it is 0 if they are the same.

Suppose  $M = 1011010001$  and  $K = 1000110111$ .

- What is  $E_K(M)$ ?
- What is  $E_K(E_K(M))$ ? What is the significance of this?

11) **One-time pad reuse** It is critical for security of the one-time pad that a pad is never re-used. To see why, suppose Alice wants to send  $M_1$  and  $M_2$  to Bob, but only has one random pad  $K$  remaining. Alice sends the messages  $C_1 = E_K(M_1)$  and  $C_2 = E_K(M_2)$  to Bob, using  $K$  twice. Suppose Eve intercepts  $C_1$  and  $C_2$ .

You may find the following properties of the  $\oplus$  (exclusive-or) function useful:

- Associativity:  $(A \oplus B) \oplus C = A \oplus (B \oplus C)$
- Commutativity:  $A \oplus B = B \oplus A$
- Zero Identity:  $A \oplus 0 = A$
- Self-Inversion:  $A \oplus A = 0$

- Without knowing  $K$  or either message, what information can Eve learn by computing  $C_1 \oplus C_2$ ?
- Now suppose Eve knows the value of  $M_1$ , and describe how she can compute  $M_2$ .