

## Midterm Practice Problems

This practice exam should take 90 minutes.

1. (Number of subsets. Show that a set of  $n$  elements has  $2^n$  subsets.) Use proof by induction over  $|A|$  to show the following claim: For any set  $A$ ,  $|\mathcal{P}(A)| = 2^{|A|}$ .

Proof: We will prove by induction that, for all  $n \in \mathbb{Z}_+$ , the following holds:  $P(n)$  Any set of  $n$  elements has  $2^n$  subsets.

**Base case:**

Since any 1-element set has 2 subsets, namely the empty set and the set itself, and  $2^1 = 2$ , the statement  $P(n)$  is true for  $n = 1$ .

**Induction step:** Let  $k \in \mathbb{Z}_+$  be given and suppose  $P(k)$  is true, i.e., that any  $k$ -element set has  $2^k$  subsets. We seek to show that  $P(k+1)$  is true as well, i.e., that any  $(k+1)$ -element set has  $2^{k+1}$  subsets.

Let  $A$  be a set with  $(k+1)$  elements. Let  $a$  be an element of  $A$ , and let  $A' = A - \{a\}$  (so that  $A'$  is a set with  $k$  elements). We classify the subsets of  $A$  into two types: (I) subsets that do not contain  $a$ , and (II) subsets that do contain  $a$ . The subsets of type (I) are exactly the subsets of the set  $A'$ . Since  $A'$  has  $k$  elements, the induction hypothesis can be applied to this set and we get that there are  $2^k$  subsets of type (I). The subsets of type (II) are exactly the sets of the form  $B = B' \cup \{a\}$ , where  $B'$  is a subset of  $A'$ . By the induction hypothesis there are  $2^k$  such sets  $B'$ , and hence  $2^k$  subsets of type (II). Since there are  $2^k$  subsets of each of the two types, the total number of subsets of  $A$  is  $2^k + 2^k = 2^{k+1}$ . Since  $A$  was an arbitrary  $(k+1)$ -element set, we have proved that any  $(k+1)$ -element set has  $2^{k+1}$  subsets. Thus  $P(k+1)$  is true, completing the induction step. Conclusion: By the principle of induction,  $P(n)$  is true for all  $n \in \mathbb{Z}_+$ .

2. Use proof by contradiction to show that  $n^4 \notin \mathcal{O}(n^2)$ . **You may not use the limit rule. Please use the formal definition of big O.**
3. Assume  $x \in \mathbb{Z}$  and  $y \in \mathbb{N}$ . If all  $y$ 's can not be divided by  $x$ , then  $x$  is 0.

For the sake of contradiction, suppose that if all  $y$ s can not be divided by  $x$ , then  $x$  is not 0. Case 1: If  $x > 0$ , then  $x \in \mathbb{N}$ , so  $x|x$  which is a contradiction. Case 2: If  $x < 0$ , then  $-x \in \mathbb{N}$ , so  $x|(-x)$ , a contradiction.

4. A Pythagorean triple consists of three positive integers  $a$ ,  $b$ , and  $c$  such that  $a^2 + b^2 = c^2$ , commonly written as  $(a, b, c)$ . When a Pythagorean triple  $a$ ,  $b$  and  $c$  have a greatest common divisor of 1, the triple is called primitive. Given  $x, y, z$  is a primitive Pythagorean triple, show that the greatest common divisor between  $x$  and  $y$  is 1 and the greatest common divisor between  $x$  and  $z$  is 1 and the greatest common divisor between  $y$  and  $z$  is 1. (Note that the greatest common divisor of  $a$  and  $b$  is the largest positive integer that divides both  $a$  and  $b$  and must be greater than or equal to 1.)

*Note: the greatest common divisor of two numbers  $x$  and  $y$  being larger than 1 can be written as  $(x, y) > 1$*

Proof. Suppose  $x, y, z$  is a primitive Pythagorean triple and  $(x, y) > 1$ . Then, there is a prime  $p$  such that  $p \mid (x, y)$ , so that  $p \mid x$  and  $p \mid y$ . Since  $p \mid x$  and  $p \mid y$ , we know that  $p \mid (x^2 + y^2) = z^2$ . Because  $p \mid z^2$ , we can conclude that  $p \mid z$ . This is a contradiction since  $(x, y, z) = 1$ . Therefore,  $(x, y) = 1$ . In a similar manner we can easily show that  $(x, z) = (y, z) = 1$ .

5. In a town, the mayor announced that there are imposters among the citizens. Everyone knows each other's identity, but not their own. The town forbids people to share knowledge of each others' identity to ensure the imposters are not warned. During the day, the police will set up a hideout near one of the imposters' homes and will arrest all imposters at night when all hideouts are in place. Once the arrest

is made, people will hear about the act the next morning. Show that given there are  $n$  imposters, an imposter will learn about their own identity on the  $n$ th morning.

(B.C.) When  $n = 1$  and the mayor made the announcement, the imposter will know there are not imposters in town, so that he is the imposter on the first day.

(I.H.) Given  $k$  imposters, where  $k \geq n$ , the police will take  $k$  nights to set up the hideouts and arrest all imposters on the  $k$ th night. The imposters expect to hear about the arrest on the  $k$ th morning and will know that they are an imposter when they do not hear about the arrest on the  $k$ th morning.

(I.S.) Assume  $k + 1$  imposters are in town, the imposters will there are  $k$  imposters in town, and the case in the I.H. applies. When they do not hear about the arrest on the  $k + 1$ th morning, they will learn that they are the imposters.

6. We know the addition formula for the tangent is as follows,

$$\tan(\alpha + \beta) = \frac{\tan \alpha + \tan \beta}{1 - \tan \alpha \tan \beta}.$$

Prove or disprove  $\tan 1^\circ$  is rational. You can use  $\tan 30^\circ = \frac{1}{\sqrt{3}}$ ,  $\tan 45^\circ = 1$  and  $\tan 60^\circ = \sqrt{3}$  if you need.

$\tan 1^\circ$  is an irrational number. For the sake of contradiction, assume  $\tan 1^\circ$  a rational number. We show  $\tan n^\circ$  is a rational number for all  $n$  by induction.

**B.C.** For  $n = 1$ ,  $\tan 1^\circ$  a rational number by assumption.

**I.H.** For  $n = k (k \geq 1)$ , assume  $\tan k^\circ$  is a rational number.

**I.S.** By recurrence formula, since  $\tan 1^\circ$  and  $\tan k^\circ$  are rational numbers,

$$\tan(k + 1)^\circ = \frac{\tan k^\circ + \tan 1^\circ}{1 - \tan k^\circ \tan 1^\circ}$$

is a rational number. Thus we can conclude  $\tan n^\circ$  is a rational number for all  $n$ . But this contradicts the fact that  $\tan 30^\circ = \frac{1}{\sqrt{3}}$ , which is irrational. Thus,  $\tan 1^\circ$  is an irrational number.