CS201A: Math for CS I/Discrete Mathematics
Assignment 1 Solution

Ayush Bansal

August 13, 2017

1. Problem 1 Solution

1.1 Part (a)

Following result is assumed for p (prime number) in the problem:

$$p \mid m^2 \tag{1.1}$$

We will be proving the following result:

$$p \mid m \quad , m \in \mathbb{Z} \tag{1.2}$$

Proof. Lets assume:

$$p \nmid m \tag{1.3}$$

We are going to use the following:

Theorem 1 (GCD is a Linear Combination)**.** *For any non-zero integers a and b, there exist integers s and t such that $gcd(a,b) = as + bt$. Moreover, $gcd(a,b)$ is the smallest positive integer of the form $as + bt$.*

Corollary 1.1. *If a and b are relatively prime, then there exist integers s and t such that $as + bt = 1$*

Since p is a prime number and does not divide m (1.3), we get the following:

$$ps + mt = 1$$

Multiplying the above equation by m

$$pms + m^2t = m$$

The **LHS** is divisble by p by using (1.1), thus **RHS** must also be divisible by p which yields:

$$p \mid m$$

The above equation is a **Contradiction** to (1.3) and thus proves our result (1.2). ☐

1.2 Part (b)

In the above part p was a prime number but now we consider p as a composite number.

Proof. Lets assume (1.3) again, only this time p is composite. This time, $gcd(p,m) = 1$ will not always be true. Lets assume:

$$gcd(p,m) = b \quad , b \in \mathbb{N}$$

Using **Theorem 1** and multiplying by m:

$$ps + mt = b$$
$$pms + m^2t = mb$$

Since **LHS** is divisible by p, **RHS** is divisible by p which yields:

$$p \mid mb$$

But the above equation simplifies to $p \mid m$ only when $b = 1$ which is not always true. Thus in case of p being a composite number, above equation doesn't necessarily hold. ☐

1.3 Part (c)

For a prime number p, we will be proving:

$$\boxed{\sqrt{p} \quad is \quad irrational}$$

Proof. Lets assume that p is a rational number which gives:

$$\sqrt{p} = \frac{a}{b} \quad where \quad gcd(a,b) = 1, \quad a,b \in \mathbb{Z}, b \neq 0 \tag{1.4}$$

Squaring both sides and multiplying by b:

$$b^2 p = a^2 \tag{1.5}$$

The **LHS** is divisible by p, thus:

$$p \mid a^2 \tag{1.6}$$

$$p \mid a \quad , by \quad (a) \tag{1.7}$$

The above can be rewritten as following:

$$a = kp \quad , k \in \mathbb{Z}$$
$$b^2 p = k^2 p^2$$
$$b^2 = k^2 p$$

By the similar arguments made for a we get:

$$p \mid b \tag{1.8}$$

Using (1.7) and (1.8), we can see that $gcd(a,b) = p$ which is **Contradiction** to (1.4) and proves our result. □

2. Problem 2 Solution

2.1 Part (a)

We are given a polynomial with real number x as the solution:

$$x^n + c_1 x^{n-1} + \cdots + c_{n-1} x + c_n = 0 \quad , c_i, i = 1..n \in \mathbb{Z} \tag{2.1}$$

The result we have to prove is:

$$\boxed{x \in \mathbb{Z} \quad \vee \quad x \notin \mathbb{Q}} \tag{2.2}$$

Proof. Lets assume x to be rational number, thus from (1.4)

$$x = \frac{a}{b}$$

Putting value in (2.1) and multiplying equation by b^n:

$$a^n + c_1 a^{n-1} b + \cdots + c_{n-1} a b^{n-1} + c_n b^n = 0 \tag{2.3}$$

In (2.3), **RHS** is divisible by b, thus **LHS** must be divisible by b, and we get this final result after taking modular of LHS:

$$b \mid a^n \tag{2.4}$$

Theorem 2 (Fundamental Theorem of Arithmetic). *Every integer greater than* 1 *is a prime or a product of primes. This product is unique, except for the order in which the factors appear. That is, if* $n = p_1p_2..p_r$ *and* $n = q_1q_2..q_s$*, where* $p's$ *and* $q's$ *are primes, then* $r = s$ *and, after renumbering the* $q's$*, we have* $p_i = q_i$ *for all* i.

By (2.4) we can see that, $gcd(a^n, b) = b$ and now 2 cases are possible,
Case 1 ($b = 1$) In this case x will be an integer.
Case 2 ($b \neq 1$) In this case there will be 2 more sub-cases:

Sub-Case 1 ($a^n = k^n, k \in \mathbb{Z}$) In this case (where a is n^{th} power of some integer), using **Theorem 2** we can say that the integer k and b is a multiple of one or more prime numbers such that $gcd(k^n, b) = b$ and we can state that there must a prime factor common between k and b which shows that $gcd(a, b) \neq 1$ and this proves x to be irrational by Part (b) for Problem 1.

Sub-Case 2 ($a^n \neq k^n, k \in \mathbb{Z}$) In this case, there is no integer $k = \sqrt[n]{a^n}$ and thus by using **Theorem 2** we can state that it is not possible to express $\sqrt[n]{a^n}$ as a product of primes since it is not an integer which means $a \notin \mathbb{Z}$, thus it is again a **Contradiction** to (1.4) which states a must be an integer. Thus x must be irrational.

□

2.2 Part (b)

We are given a positive integer m such that:

$$m \neq k^n \quad , k \in \mathbb{N}$$

Proof. Lets assume that $\sqrt[n]{m}$ is rational, then by (1.4):

$$\sqrt[n]{m} = \frac{a}{b}$$

Raise the power of both sides to n and multiplying by b^n:

$$mb^n = a^n$$

Since **LHS** is divisible by b, **RHS** is divisible by b which gives:

$$b \mid a^n$$

The above result is same as (2.4), now following the steps of Part (a), we can prove that $a \notin \mathbb{Z}$ whether or not $b = 1$ or $b \neq 1$, and this is a **Contradiction** to (1.4) and m must be irrational.

□

2.3 Part (c)

We are given 2 integers a and b such that:

$$\sqrt{ab} \notin \mathbb{Q} \tag{2.5}$$

We have to prove that:

$$(\sqrt{a} + \sqrt{b}) \notin \mathbb{Q} \tag{2.6}$$

Proof. Lets assume that $\sqrt{a}+\sqrt{b}$ is a rational number and squaring the equation.

$$\sqrt{a}+\sqrt{b}=x \tag{2.7}$$
$$\sqrt{(ab)}=\frac{1}{2}(x^2-a-b) \tag{2.8}$$

In (2.7) **RHS** is rational, thus **LHS** must also be rational but that is a **Contradiction** by (2.5). □

3. Problem 3 Solution

3.1 Part (a)

We are given the following relation:

$$S_n = 5S_{n-1}-6S_{n-2}, \quad n>1 \tag{3.1}$$
$$S_0=0, S_1=1 \tag{3.2}$$

We need to prove the following the result:

$$\boxed{S_n = 3^n - 2^n} \tag{3.3}$$

Proof. We are going to prove the result using induction.
Base Case for $n=0,1,2$.

$$S_0 = 3^0-2^0=0$$
$$S_1 = 3^1-2^1=1$$
$$S_2 = 5S_1-6S_0=5=3^2-2^2$$

Inductive Hypothesis: We assume following satisfies the claim to prove S_{n+1}

$$S_2 \wedge S_3 \wedge \cdots \wedge S_n$$

Inductive Step: Using the relation (3.1) for $n+1$ and substituting (3.3) for n and $n-1$:

$$S_{n+1}=5S_n-6S_{n-1}$$
$$S_{n+1}=5(3^n-2^n)-6(3^{n-1}-2^{n-1})$$
$$S_{n+1}=(5-2)3^n-(5-3)2^n$$
$$S_{n+1}=3^{n+1}-2^{n+1}$$

By above equations, the result is proved by induction.

□

3.2 Part (b)

We have to prove the following relation:

$$\boxed{1*2+2*3+\cdots+(n-1)*n=\frac{(n-1)n(n+1)}{3}, \quad n\in\mathbb{N}} \tag{3.4}$$

Proof. We are going to prove the result using induction.
Base Case for $n = 1$:

$$P_1 = 0 * 1 = \frac{(1-1)1(1+1)}{3} = 0$$
$$P_2 = 1 * 2 = \frac{(2-1)2(2+1)}{3} = 2$$

Inductive Hypothesis: Assuming P_n satisfies the claim.
Inductive Step:

$$P_{n+1} = 1 * 2 + 2 * 3 + \cdots + (n-1) * n + n * (n+1)$$
$$P_{n+1} = P_n + n * (n+1)$$
$$P_{n+1} = \frac{(n-1)n(n+1)}{3} + n(n+1)$$
$$P_{n+1} = \frac{n(n+1)(n+2)}{3}$$

By above equations, (3.5) is proved. □

3.3 Part (c)

We have a set of n distinct elements and P_n is the number of subsets formed from this set, and we have to prove the following result:

$$\boxed{P_n = 2^n \quad \forall n \geqslant 0} \tag{3.5}$$

Proof. We are proving the result by hypothesis by induction.
Base Case for $n = 0$, only 1 set is possible (empty set), for $n = 1$, 2 sets are possible (empty set and set of 1 element), for $n = 2$, 4 sets are possible (empty set, 2 sets of 1 element each and 1 set of 2 elements):

$$P_0 = 1 = 2^0$$
$$P_1 = 2 = 2^1$$
$$P_2 = 4 = 2^2$$

Inductive Hypothesis Assume $P_n = 2^n$.
Inductive Step Consider a set of $n+1$ elements.
Let the set be $\{a_1, a_2, \ldots, a_{n+1}\}$, now we kick out 1 element from the set, let it be a_1, then the number of subsets formed by the set of remaining n elements is P_n, and now we can have 2 cases - either add the element a_1 or not add the element to a subset formed by P_n.
Thus by above analogy:

$$P_{n+1} = 2 * P_n$$
$$P_{n+1} = 2 * 2^n$$
$$P_{n+1} = 2^{n+1}$$

By above equations and base case, (3.6) is proved. □

3.4 Part (d)

Proof. We have a string of n distinct letters and P_n is the number of permutations we get from this string, and we have to prove the following result:

$$\boxed{P_n = n!, \quad \forall n \in \mathbb{N}} \tag{3.6}$$

Base Case for $n = 1$, only 1 permutation is possible, for $n = 2$, 2 permutations are possible (ab and ba), for $n = 3$, 6 permutations are possible (abc, cab, bca, cba, acb and bac):

$$P_1 = 1 = 1!$$
$$P_2 = 2 = 2!$$
$$P_3 = 6 = 3!$$

Inductive Hypothesis Assume $P_n = n!$.
Inductive Step Consider a string of $n+1$ letters.
Let the string be $\{s_1, s_2 \ldots, s_{n+1}\}$, now we kick out 1 letter from the string, let it be s_{n+1}, then the number of permutations we get from the string of remaining n letters is P_n, and now we can have $n+1$ cases as there are $n+1$ places we can put the letter s_{n+1} (between the the gaps of n letters - $n-1$ places and 2 ends):

$$P_{n+1} = (n+1) * P_n$$
$$P_{n+1} = (n+1) * n!$$
$$P_{n+1} = (n+1)!$$

By above equation and base cases, (3.7) is proved. □

4. Problem 4 Solution

We are given a $n \times n$ board of white squares and we can choose $m < n^2$ squares randomly and colour them red. In each round we colour some more white squares according to some rules.
Rules:

1. Already red squares remain red.
2. A white square that has atleast 2 red neighbours is coloured red, neighbour is defined as those squares that are immediately to the left/right/up/down.

Conjecture 1. *The smallest necessary value of m for which the whole n × n board can be coloured red after a finitely many number of legal rounds is n.*

Lemma 1.1. *Choosing initial red squares along the diagonal of the board (without leaving a white square in between 2 red squares on the diagonal) results in the maximum number of red squares and this number is m^2, after a finitely many number of rounds, for some $m \leqslant n$.*

Proof. Consider $n \times n$ board to be a matrix with a square in i_{th} row and j_{th} column be denoted by a_{ij}.
Lets first assume that m squares are chosen along the diagonal of the $n \times n$ board, $\{a_{11}, a_{22} \ldots, a_{mm}\}$ (continuous diagonal) are chosen to be coloured red initially. Going by the rules:

After Round 1, the red coloured squares are $\{a_{11}, a_{22} \ldots, a_{mm}\}$ and $\{a_{12}, a_{23} \ldots, a_{(m-1)m}\}$ and $\{a_{21}, a_{32} \ldots, a_{m(m-1)}\}$.
Following the pattern for subsequent rounds till $m-1$ rounds.
After Round (m-1), the red coloured squares will form a $m \times m$ board (matrix) from a_{11} to a_{mm}.

Thus, in this assumption m^2 squares are finally coloured.
Now we choose m squares at some places other than continuous diagonal squares, then there might be two cases:

Case 1 - All the squares which are selected have the property such that *Any two squares have atleast one vertex in common, excluding the above diagonal case* (e.g. a_{12} and a_{21} have one vertex in common). In this case after k rounds, a rectangle of red squares will be formed whose area will be less than $m \times m$ square. Thus it will have $x < m^2$ squares.

Case 2 - All the squares which are selected have the property such that *Atleast one square has no common vertex with any other square*. In this case there are one or more isolated red squares and thus the number of red squares finally will be $y < m^2$.

By above 2 cases we can see that **Lemma 1.1** holds. □

Lemma 1.2. *$m = n$ is the minimum value of m such that after finitely many rounds we get a full $n \times n$ white board coloured red.*

Proof. By the proof of **Lemma 1.1** we can prove our proposition in 2 cases:

Case 1 ($m < n$) - this case will yield a maximum number of $m^2 < n^2$ red coloured squares and thus it is not possible to colour full $n \times n$ board.

Case 2 ($m = n$) - this case will yield a $m^2 = n^2$ red coloured squares which constitutes the full $n \times n$ board.

By above 2 cases, **Lemma 1.2** holds. □

By above 2 lemmas, we can see that for $m \geqslant n$, we can find atleast 1 permutation of the initially red and white coloured $n \times n$ board which will yield a fully red coloured board after a finitely many number of rounds, thus proving our **Conjecture**.

5. Problem 5 Solution

5.1 Part (a)

Claim: $n(n+1)$ is an odd number for every n.
The proof provided for the claim is by induction:
Induction Hypothesis: $(n-1)n$ is odd.
Inductive Step:

$$n(n+1) = (n-1)n + 2n$$

Since $2n$ is even and $(n-1)n$ is odd and thus $n(n+1)$ is odd number.
Flaw: The flaw in the proof is the missing **Base Case**, there exists no $n \in \mathbb{Z}$ such that $(n-1)n$ is odd and thus our **Inductive Hypothesis** is false for every $n \in \mathbb{Z}$.

5.2 Part (b)

Claim: If we have n lines in the plane, no two of which parallel, then they will go through one point.
Base Case:

n=1, true as it is only 1 line.
n=2, true since lines are non parallel.

Inductive Hypothesis: Claim is true for $n-1$ lines.
Inductive Step: Consider a set of n lines - $\{a, b \dots\}$, take out one line c, by **I.H.** other $n-1$ lines meet at a point P, now insert back c and remove line d, the remaining lines pass through point Q, since lines a and b are in both subsets, the points Q and P are same.
Flaw: The flaw in the proof is in **Inductive Step**, the inductive step requires atleast 4 lines - $\{a, b, c, d\}$ to be carried out, but looking at the **Base Case**, we can see that our claim fails even for 3 lines, we can have 3 non-parallel lines not intersecting at a single point.
Suppose $n = 3$, set $S = \{a, b, c\}$, we remove line c, the lines a and b intersect at point P and when we remove line b, the lines a and c intersect at point Q but we cannot prove that point P and Q are same.

5.3 Part (c)

Claim: For $a \in \mathbb{R}, n \in \mathbb{N}, a^n = 1$
Inductive Hypothesis: It holds for n and $n-1$.
Inductive Step: For $n+1$

$$a^{n+1} = \frac{a^n a^n}{a^{n-1}} = \frac{1 \times 1}{1} = 1$$

Flaw: The **Base Case** is not enough to assume the **Inductive Hypothesis**.
Let $n = 1$ and $n - 1 = 0$, $a^1 = a$ and $a^0 = 1$ and by following the steps provided:

$$a^{(1+1)} = \frac{a^1 a^1}{a^{(1-1)}}$$
$$a^2 = \frac{a^2}{1}$$

Thus the above claim is false.