COL 202 Oct 7

Minor 2

6

Name: Kamalnath.P **Entry Number** 2015CS10244

1. You are NOT allowed to stand up or leave the seat at the end of exam till all answer scripts are collected and counted.
2. You are NOT allowed to leave the exam hall during the exam period unless on medical emergency.
3. Calculators and phones are NOT allowed.
4. You are NOT allowed to ask any questions during the exam. If in doubt, make (and state) your assumptions.

Q1. (6 marks) Let n be a positive integer. Show that given any set of $n + 2$ distinct integers, either there are two integers in the set whose sum is divisible by $2n$, or there are two integers in the set whose difference is divisible by $2n$.

A) when a number is divisible by $2n$ the possible remainders are $\in \{0, 1, 2 \ldots\ldots, 2n-1\} = S$

Case i) If any two of the given set of $n+2$ distinct integers give same remainder with '$2n$' then we can take difference of those two which is divisible by $2n$.

ex:- $a, b \in S$

$a = r \pmod{2n}$
$b = r \pmod{2n}$
$\Rightarrow a - b = 0 \pmod{2n}$

Case ii) all $n+2$ numbers $\in S$ give distinct remainders with $2n$. Let us organise the set of possible remainders left by $2n$ as follows.

$\{(0), (1, 2n-1), (2, 2n-2) \ldots\ldots (n-1, n+1), n\}$

$n+1$ entities

when $n+2$ numbers $\in S$ are divided by $2n$ the distinct remainders ($n+2$ in number) left by them are pigeons and the above $n+1$ entities are holes. As all remainders are distinct the $(n+2)$th number's remainder must be

$2n \mid a+b$

Q2. (8 marks) Recall that a positive integer m is a Carmichael number if $b^{m-1} = 1 (\mathrm{mod}\ m)$ for all integers b, such that $1 < b < m$ and $\gcd(b, m) = 1$. Let n be a positive integer which is NOT a Carmichael number. Let S denote the set of integers b such that $\gcd(b, n) = 1$ and $1 < b < n$. Let S' be the set of integers x in S for which $x^{n-1} = 1 (\mathrm{mod}\ n)$. Prove that $|S'| \leq |S|/2$.

A) ~~case (i) If n is a prime number~~

n can't be a prime number because if it is by fermats little theorem we get $\forall\ b \quad \gcd(b,n) = 1$

$b^{n-1} = 1 \pmod n$

$\Rightarrow |S'| = |S|$ in this case.

$\therefore$ n has to be composite number,

let the prime factorization of n be

$n = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t}$

S' be the set of integers x in S for which

$x^{n-1} = 1 \pmod n$.

$\therefore x^{n-1} = 1 \pmod{p_1^{a_1}}$

$x^{n-1} = 1 \pmod{p_t^{a_t}}$

number of p_1 multiples occurs $\forall\ a < n$

$= \left[\frac{n}{p_1}\right] - 1$

similarly for all other primes.

by chinese Remainder theorem, this

$\therefore |S| = n - \left(\left[\frac{n}{p_1}\right] - 1 \ldots \left[\frac{n}{p_t}\right] - 1\right)$

$= n + t - \left(\left[\frac{n}{p_1}\right] + \left[\frac{n}{p_2}\right] \ldots \left[\frac{n}{p_t}\right]\right)$

Q3. **(6 marks)** Let S be a set of positive real numbers which have the following property: for every finite subset A of S, the sum of the numbers in A is at most 1. Prove that S is countable (you can use the fact that the union of a countable number of countable sets is countable).

A) 1) If S is ~~infi~~ finite set then it is trivial

2) Let S be infinite set with every finite subset A of S, the sum of numbers in A is atmost 1,

take two finite subsets of A_p, A_q of S.

$\{a_1, \ldots, a_p\} = A_p$

$\{b_1, \ldots, b_q\} = A_q$

$\sum a_i \leq 1 \qquad \sum b_i \leq 1$

map all a_i to $\frac{1}{2^{k_i}}$ such that $a_i \leq \frac{1}{2^{k_i}}$ (closest)

map all b_j to $\frac{1}{2^{l_j}}$ $b_i \leq \frac{1}{2^{l_j}}$

$k_i = l_j$ if and only if $a_i = b_j$

Let $A_R = A_p \cup A_q$

Σ of all elements in $A_p \cup A_q$

$\leq \sum_{i}^{|A_p \cup A_q|} \frac{1}{2^i} < 1$

If we take union of all finite subsets

still $\leq \sum_{i} \frac{1}{2^i} < \sum_{i=1}^{\infty} \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} \ldots \frac{1}{2^\infty} = 1$

≤ 1

this shows $S \equiv |A_1 \cup A_2 \ldots|$ can have an injection with $\mathbb{Z}^+$ is lesser