CS 203B: Mathematics for Computer Science-III
Assignment 3

Deadline: 18 : 00 hours, August 26, 2015

General Instructions:

- Write your solutions by furnishing all relevant details (you may assume the results already covered in the class).
- You are strongly encouraged to solve the problems by yourself.
- You may discuss but write the solutions on your own. Any copying will get zero in the whole assignment.
- If you need any clarification, please contact any one of the TAs.
- Please submit the assignment at KD-213/RM-504 before the deadline. Delay in submission will cause deduction in marks.

Question 1: [10]

Use the Orbit-counting (Burnside's) Lemma to find a formula for the number of ways of coloring the faces of a cube with k colors. Assume that two colored cubes which differ by a rotation are identical. Repeat for colorings of the edges, and of the vertices.

Question 2: [10]

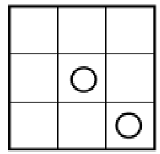
Let the cyclic group of prime order p generated by g act on the set of all p-tuples of elements from $\{1, \cdots, n\}$ by the rule

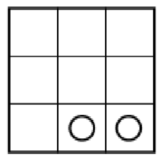
$$(x_1, \cdots, x_p)g = (x_p, x_1, \cdots, x_{p-1}).$$

Now by Orbit-counting (Burnside's) Lemma, prove that $n^p = n(\mod p)$.

Question 3: [10]

Suppose you manufacture an identity card by punching two holes in an 3×3 grid. How many distinct cards can you produce? Use Orbit-counting (Burnside's) Lemma. Look at the figure given below.





Different identity cards with circles showing the holes.

Question 4: [5+5]

(a) Suppose R be a ring. If every element $x \in R$ satisfies $x^2 = x$, prove that R must be commutative (i.e., multiplicative operator associated with R commutes as well).

(b) Prove that only such ring that is also an integral domain is $\mathbb{Z}/2\mathbb{Z}$. (A commutative ring R is an *integral domain* if for every $a, b \in R$ such that $a \neq 0$ and $b \neq 0$, then $a.b \neq 0$ as well.)

Question 5: [5+5]

Define the set $R[x]$ of *formal power series* in the indeterminate x with coefficients from a ring R to be all formal infinite sums $\sum_{n=0}^{\infty} a_n x^n$. Define addition and multiplication of power series in the same way as for the power series with real or complex coefficients, i.e., extend polynomial addition and multiplication to power series as though they were "polynomials of infinite degree":

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n,$$

$$\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (\sum_{k=0}^{n} a_k b_{n-k}) x^n.$$

(a) Prove that $R[x]$ is a commutative ring.

(b) Prove that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[x]$ if and only if a_0 is a unit in R.

Question 6: [3+3+4]

The *center* of a ring R is $\{z \in R | zr = rz \text{ for all } r \in R\}$ (i.e., the set of all elements which commute with every element of R).

(a) Prove that the center of a ring is a subring.

(b) For a fixed element $a \in R$, define $C(a) = \{r \in R | ra = ar\}$. Prove that $C(a)$ is a subring of R containing a.

(c) Prove that the center of R is the intersection of the subrings $C(a)$ over all $a \in R$.

Question 7: [2+4+4]
For rings $Z[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in Z\}$, $d \in Z$, the norm is defined as: $\mid a + b\sqrt{d} \mid^2 = a^2 - b^2 d$.

(a) Show that the norm is multiplicative, i.e., $\mid \alpha\beta \mid = \mid \alpha \mid * \mid \beta \mid$ for $\alpha, \beta \in Z[\sqrt{d}]$.

(b) Prove that $Z[\sqrt{d}]$, $d < 0$, has at most four units. Can you list them?

(c) Show that the ring $Z[\sqrt{d}]$, $d > 0$, has infinitely many units. Can you list units of $Z[\sqrt{2}]$?

Question 8: [5+5]

(a) Show that each of the following is a prime number in the ring $Z[i]$: (i) $1 + i$, (ii) $a + bi$ with $a^2 + b^2 = p$, p a prime number such that $p = 1(\mod 4)$, and (iii) $p \in Z$ with p a prime number such that $p = 3(\mod 4)$.

(b) Show that the ring $Z[\sqrt{-5}]$ does not have unique factorization, by proving that 3, $2 + \sqrt{-5}$, and $2 - \sqrt{-5}$ are primes in the ring and $3 * 3 = (2 + \sqrt{-5}) * (2 - \sqrt{-5})$.