CS203 ASSIGNMENT 3 SEMESTER I, 2017-18

Due Date: 1st September, 2017 **Maximum Marks: 50**

Instructions

- Submit the assignment at the end of class on or before the due date.
- Yours answers should be precise and clearly written.
- Cheating/plagiarizing in any form will be heavily penalized.
- Late submissions will receive a mark of zero.
- Any doubts regarding the assignment can be raised in the discussion forum on moodle.

---

1. (15 points) For each equation given below, find whether there exists integral solutions or not.
    1. $x^3 = y^2 + 3$
    2. $x^3 = y^2 + 1$
2. (25 points) For this question you can assume that if π is a prime in $\mathbb{Z}[i]$ and π divides ab, then either π divides a or b.
    1. Prove Wilson's theorem
    $$(p-1)! = -1 \mod p, \text{ where } p \text{ is a prime number}$$
    2. Prove that if p is a prime number of the form $4n+1$, then we can solve
    $$x^2 \equiv -1 \mod p$$
    3. Prove that if p is a prime number of the form $4n+1$, then there exists integers x, y and c such that $x^2 + y^2 = cp$ and $\gcd(c, p) = 1$.
    4. Prove that for a prime number p if there exists integers x, y and c such that $x^2 + y^2 = cp$ where c is coprime to p then p can't be a prime in $\mathbb{Z}[i]$.
    5. Suppose that p is a prime in $\mathbb{Z}$, but not prime in $\mathbb{Z}[i]$. Then show that $p = a^2 + b^2$ for some integers a and b.
    6. Prove that if p is a prime number of the form $4n+1$, then $p = a^2 + b^2$ for some integers a, b.
3. (10 points)
    1. 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).
    2. Prove that only such ring that is also an integral domain is $Z/2Z$. (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.)