CS201: MATHEMATICS FOR COMPUTER SCIENCE - I

NITIN SAXENA

ASSIGNMENT 3

POINTS: 35

DATE GIVEN: 03-SEP-2016 DUE: 10-SEP-2016(6PM)

Rules:

- You are strongly encouraged to work *independently*.
- Write the solutions on your own and honorably *acknowledge* the sources if any.
  `http://cse.iitk.ac.in/pages/AntiCheatingPolicy.html`
- Submit your solutions, before time, to your TAs as per the roll numbers: Amit Sinhababu (12000–150130), Pranav Bisht (150131–150365), Ashish Dwivedi (150366–150600), Pulkit Kariryaa (150601–150840).

Question 1: *[8 points]* Given 9 vertices, join all pairs of vertices by either red or blue edge. Show that there is always either a red *triangle* or a blue *quadrilateral*.

Question 2: *[4 points]* Another definition of $g =: \gcd(a, b)$ is: g is the number which divides both a, b and any number which divides both a, b also divides g. Show that the two definitions are equivalent.

Question 3: *[3+4 points]* Write a pseudocode for the extended Euclidean algorithm to compute "$\alpha a + \beta b = 1$", given a, b.

Give a tight estimate for the number of steps as a function of a, b. (Hint: Use the connection with Fibonacci numbers.)

Question 4: *[4+3 points]* Consider a quadratic equation $X^2+aX+b = 0 \mod p$, where p is a prime. Formulate a condition on a, b, p that tells us whether the equation has zero, one or two solutions.

Can there be three, or more, solutions?

Question 5: *[3+6 points]* Let $n \in \mathbb{N}$. Prove that, for every composite $n > 4$, $(n-1)! = 0 \mod n$.

More interestingly, show that for any $n > 1$,

$$n \text{ is prime iff } (n-1)! = -1 \mod n\,.$$

(This is known as *Wilson's primality criterion*.)

□□□