Quiz 2
DM, Monsoon 2021

Duration : 60 mins
Max marks : 10

1. (2 marks) Use the theory of congruences to show that 19 divides $10 \cdot 8^{n-1} + 3^{3n-1}$ for every positive integer n.

2. (2 marks) By working modulo two different integers, find the missing digits x, y in the calculation below:

$$23456789 \times 98765432 = 231x71989891y848.$$

3. (2 marks) Let a, b be positive integers such that $\gcd(a, b) = 1$. Show that

$$\gcd(8a + 5b, 5a + 3b) = 1.$$

4. (2 marks) Let $f : \mathbb{N} \to \mathbb{R}$ be a real-valued function defined on the nonnegative integers. A *limit point* of f is a real number $r \in \mathbb{R}$ such that $f(n)$ is close to r for infinitely many $n \in \mathbb{N}$, where "close to" means within distance ϵ for whatever positive real number ϵ you may choose. The fact that r is a limit point of f can be expressed by a logical formula of the form:

$$\mathbf{Q_1}\mathbf{Q_2}\mathbf{Q_3}(|f(n) - r| \leq \epsilon),$$

where $\mathbf{Q_1}, \mathbf{Q_2}, \mathbf{Q_3}$ are quantifiers from among the following:

$\forall n$	$\exists n$	$\forall n \geq m$	$\exists n \geq m$
$\forall m$	$\exists m$	$\forall m \geq n$	$\exists m \geq n$
$\forall \epsilon \geq 0$	$\exists \epsilon \geq 0$	$\forall \epsilon > 0$	$\exists \epsilon > 0$.

Here m, n range over nonnegative integers, and ϵ ranges over real numbers. Identify the quantifiers $\mathbf{Q_1}, \mathbf{Q_2}, \mathbf{Q_3}$.

5. (2 marks) In a public-key system using RSA, you intercept the ciphertext $c = 13$ sent to a user whose public key is $e = 43, n = 143$. You succeeded in factoring n and determining that the inverse of e modulo $\varphi(n)$ is $d = 67$. Provide detailed calculations to show how the plaintext m can be recovered. [Hint: Chinese Remainder theorem.]