MID-SEMESTER EXAM	ISI BANGALORE	MARCH 2022
NUMBER THEORY		100 POINTS

Notes.

(a) You may freely use any result proved in class or in the textbook unless you have been asked to prove the same. Use your judgement. All other steps must be justified.

(b) We use $\mathbb{N}$ = natural numbers, $\mathbb{Z}$ = integers, $\mathbb{Q}$ = rational numbers, $\mathbb{R}$ = real numbers, $\mathbb{C}$ = complex numbers.

---

1. [5+10+5 = 20 points]
   (i) Find integers m, n such that $38m + 83n = 1$.
   (ii) Find the smallest positive d such that $d \equiv 21 \pmod{38}$ and $d \equiv 12 \pmod{83}$.
   (iii) Write $\frac{83}{38}$ as a finite continued fraction, i.e., find a finite sequence of positive integers $a_0, a_1, a_2, \ldots$ such that
$$\frac{83}{38} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$$

2. [8+4+8 = 20 points] Prove that $R := \mathbb{Z}[\sqrt{-2}]$ is an Euclidean domain. Identify the units in R. Prove that a prime number $p \in \mathbb{Z}$ splits into two irreducibles in R iff -2 is a square in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

3. [10 points] Prove that the set of positive integers that cannot be written as a sum of at most 3 squares is infinite.

4. [16 points] Let p be a prime. Suppose the residue of $a \in \mathbb{N}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ is a generator. Prove that the residue of at least one among $\{a, a+p\}$ in $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is a generator.

5. [4+8+4 = 16 points]
   (i) Find an element (in decimal form) having order 121 in $(\mathbb{Z}/11^3\mathbb{Z})^\times$.
   (ii) Prove that 2 is a generator of $(\mathbb{Z}/11^m\mathbb{Z})^\times$ for all m.
   (iii) Find the smallest integer $n > 0$ such that the order of 2^n in $(\mathbb{Z}/11^3\mathbb{Z})^\times$ is 10.

6. [6+6+6 = 18 points]
   (i) Using $\sqrt{22} \approx 4.66$ (equality being upto 2 decimal places), choose a rational approximation $p/q \approx \sqrt{22}$ such that the following hold:

   a. $\left|\frac{p}{q} - \sqrt{22}\right| < \frac{1}{q^2}$ b. $\left|N(p + \sqrt{22}q)\right| \leq 2$.

   (ii) Using (i) or otherwise, find a unit $u > 1$ in $\mathbb{Z}[\sqrt{22}]$.
   (iii) Prove that neither the equation $x^2 - 22y^2 = -1$ nor $x^2 - 22y^2 = 2$ has any integer solutions in x, y.