END-SEMESTER EXAM | NUMBER THEORY | MAY 2022

ISI BANGALORE | 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) There are a total of **110** points in the paper. You will be awarded a maximum of **100**.

(c) $\mathbb{Z}$ = integers

---

1. [15 points] Do **any one** out of (i) and (ii):
   (i) Describe the last $n+2$ digits of 243^{10^n+1}. (Hints: $243 = 3^5$. What is the group structure of $(\mathbb{Z}/10^m\mathbb{Z})^\times$?)
   (ii) Let p, q be distinct odd primes such that $p-1$ divides $q-1$. If $(n, pq) = 1$, then show that $n^{q-1} \equiv 1 \pmod{pq}$.

2. [20 points] Describe all the rational points of the hyperbola $x^2 - y^2 = 6$. You may use the following steps:
   (i) Find a rational point p on the curve. (Hint: Can you find a nonzero integer solution of the homogenised equation $X^2 - Y^2 = 6Z^2$?)
   (ii) From p, project the curve to the X-axis or the Y-axis and look at the inverse map.

3. [15 points] Do **any one** out of (i) and (ii):
   (i) Let $R = \mathbb{Z}/11^5\mathbb{Z}$. Find a square-root of 3 and the multiplicative inverse of 6 in R. (Hint: Obtain your answers in terms of suitable 11-adic expansions.)
   (ii) Show that $x^2 + 11y^2 = 3$ has a solution in $\mathbb{Z}/p\mathbb{Z}$ for every prime p. (Hint: What is the cardinality of the set S of squares in $\mathbb{Z}/p\mathbb{Z}$ or its translates ? What if $p = 2$ or $p = 11$?)

4. [10+10=20 points] Do **any two** out of (i), (ii) and (iii):
   (i) Evaluate the Legendre symbol $\left(\frac{46}{83}\right)$.
   (ii) Describe all the primes p such that 10 is a quadratic residue modulo p.
   (iii) Set $\zeta := e^{2\pi i/7}$. Find an element α in $\mathbb{Z}[\zeta]$ such that $\alpha^2 = -7$. Verify your answer.

5. [5+5+10 = 20 points]
   (i) Define the Dirichlet convolution $f * g$ of two arithmetic functions f, g.
   (ii) For an arithmetic function f, define what it means for f to be multiplicative and for f to be completely multiplicative.
   (iii) Let μ be the Mobius function, $\nu(n)$ = the number of divisors of n, and $N(n) = n$ for all n. Identify $\nu * \mu$. Using this or otherwise, identify $\mu * (N * \nu)$.

6. [20 points] Using Euler's summation formula or otherwise, prove that for $x \geq 2$ we have

$$\sum_{n \leq x} \frac{\log n}{n} = \frac{1}{2}\log^2 x + A + O\left(\frac{\log x}{x}\right)$$

for some constant A. Here n ranges over integers such that $1 \leq n \leq \lfloor x \rfloor$.