Indian Statistical Institute
Semestral Examination 2008-2009
M.Math II year
Number Theory

Date: 05-12-2008 Max Marks 100 Duration 3 hours

1. (a) For an odd prime p, let $\mathbb{F}_p = Z/pZ$ in the field of order p. Show that, for $u \in \mathbb{F}_p$, we have

$$\sum_{x \in \mathbb{F}_p} \left(\frac{x(u-x)}{p} \right) = \begin{cases} (-1)^{\frac{p-1}{2}}(p-1) \text{ if } u = 0 \\ (-1)^{\frac{p+1}{2}} \text{ otherwise.} \end{cases}$$

(b) If p, q are two distinct odd primes, let ω be a primitive pth root of unity in the algebraic closure of $\mathbb{F}_q$, and define the Gauss sum S by $S = \sum\limits_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \omega^x$. Use part (a) to show that $S^2 = (-1)^{\frac{p-1}{2}}\, p$.

(c) The map $y \mapsto y^q$ is an automorphism of the algebraic closure of $\mathbb{F}_q$. Use this fact to show that $S^q = \left(\frac{q}{p}\right) S$.

(d) Use the results from (b) and (c) to conclude that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$. [30]

2. (a) Let $p \equiv 1 (\mod 4)$ be a prime. Define $X = \{(a,b,c) \in \mathbb{N}^3 : a^2 + 4bc = p\}$. Show that X is a non-empty finite set. Zagier defined an involution $f : X \to X$ which has a unique fixed point x_0. Using this fact, show that p is a sum of two squares.

(b) Define $g : X \to X$ by $g(a,b,c) = (a,c,b)$. Let $h = f \circ g$. Show that the h-orbit containing x_0 contains a unique fixed point y_0 of g. [20]

3. Define the ring of Gaussian integers and find all the units of this ring. Show that every non-zero element of this ring has a unique factorization into prime elements modulo units. [15]

4. Let $\|\cdot\|_1$ and $\|\cdot\|_2$ be two norms on a field $\mathbb{F}$. Show that the following statements are equivalent: (a) $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent norms
(b) $\|\cdot\|_1$ and $\|\cdot\|_2$ define the same open unit ball
(c) there is constant $\alpha > 0$ such that $\|x\|_2 = \|x\|_1^\alpha$ for all $x \in \mathbb{F}$. [20]

5. (a) Show that every p-adic integer x has a unique expansion $x = \sum\limits_{n=0}^{\infty} x_n\, p^n$ where $0 \le x_n < p$ for each n. Find this expansion for $x = -1$.

(b) Show that this expansion of x is eventually periodic if and only if x is a rational number. [15]

(Hint for part (b). Observe that if N is a natural number, then there are $m, n \ge 0$ such that N divides $p^m(p^n - 1)$.)