INTERNAL STUDENTS ONLY

THE UNIVERSITY OF QUEENSLAND

Second Semester Examination, November, 1995.

MP313

NUMBER THEORY III

(UNIT COURSES)

Time: **THREE HOURS** for working
Ten minutes for perusal before examination begins.

Attempt **FIVE** questions.

All questions carry the same number of marks.

Pocket calculators and the CALC calculator allowed.

1. Let
$$g_a = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) e^{\frac{2\pi i t a}{p}}, \quad g = g_1,$$
where p is an odd prime and $\left(\frac{t}{p}\right)$ is the Legendre symbol.

   (a) Prove that $g_a = \left(\frac{a}{p}\right) g$, if p does not divide a.

   (b) Prove that $g^2 = (-1)^{\frac{p-1}{2}} p$.

   (c) (i) **Either** prove the quadratic reciprocity law **or**

   (ii) let $\zeta = e^{\frac{2\pi i}{8}}$, $\tau = \zeta + \zeta^{-1}$ and prove that
$$\tau^p \equiv \left(\frac{2}{p}\right) \tau \,(\mathrm{mod}\, p) \quad \text{and } \tau^p \equiv \zeta^p + \zeta^{-p} \,(\mathrm{mod}\, p)$$
and deduce that $\tau^p \equiv \begin{cases} \tau & \text{if } p \equiv \pm 1 \,(\mathrm{mod}\, 8), \\ -\tau & \text{if } p \equiv \pm 3 \,(\mathrm{mod}\, 8). \end{cases}$

2. (a) Find the continued fraction expansion of $\sqrt{34}$ and hence find the fundamental unit of $\mathbb{Q}(\sqrt{34})$.

   (b) Prove that if $p = 4n + 3$ is a prime, the equation $x^2 - py^2 = 2\left(\frac{2}{p}\right)$ is soluble. (Hint: Start with a solution of $t^2 - 1 = pu^2$ and consider the possibilities t odd and t even.)

3. (a) Prove that $\sum_{p \le n} \frac{\log p}{p} = \log n + O(1)$, by starting with the canonical factorization of $n!$.

   (b) Given a direct product decomposition of an abelian group G:
$$G = \langle g_1 \rangle \times \cdots \langle g_t \rangle$$
where g_i has order m_i, list all characters on G.
If $\hat{G}$ denotes the group of characters on G, prove that
$$\sum_{\chi \in \hat{G}} \chi(a) = \begin{cases} |G| & \text{if } a = e, \\ 0 & \text{if } a \neq e. \end{cases}$$

Question 4–7 on next page

 TURN OVER

4. (a) Describe the irreducible elements of $\mathbb{Z}[i]$. Also list the units.

   (b) Factorize $7 + 4i$ into irreducibles in $\mathbb{Z}[i]$.

   (c) Prove that $\gcd(x + i, x - i) = 1 + i$ if $x \in \mathbb{Z}$ is odd and hence solve the diophantine equation $x^2 + 1 = 2y^3$.

   (d) Prove that $\mathbb{Q}(\sqrt{d})$ is not euclidean if $d < -11$.

5. Prove the Pólya–Vinogradov inequality

$$\left| \sum_{n=A}^{B} \left(\frac{n}{p} \right) \right| < \sqrt{p} \log p.$$

6. (a) Find the 5–adic canonical expansion of $\frac{17}{12}$.

   (b) Let $\alpha \in \mathbb{Z}_p$. Prove that $\alpha^{p^M} \equiv \alpha^{p^{M-1}} \pmod{p^M}$ for $M \geq 1$ and deduce that the sequence $\{\alpha^{p^M}\}$ approaches a limit $\hat{\alpha}$ in $\mathbb{Z}_p$. Show that $\hat{\alpha}^p = \hat{\alpha}$ and $\hat{\alpha} \equiv \alpha \pmod{p}$. Find the first 3 digits of $\hat{\alpha}$ when $\alpha = 2$ and $p = 3$.

   (c) Let $p \equiv 2 \pmod{3}$. If a is an integer not divisible by p, show there is an $x \in \mathbb{Z}_p$ with $x^3 = a$.

7. If $x^2 + y^2 = z^2$, where $x, y, z \in \mathbb{N}$, $\gcd(x, y, z) = 1$ and y is even, prove that

$$x = m^2 - n^2, \;\; y = 2mn, \;\; z = m^2 + n^2,$$

where $\gcd(m, n) = 1$ and precisely one of m and n is even.