INTERNAL STUDENTS ONLY

THE UNIVERSITY OF QUEENSLAND

Second Semester Examination, November, 1999.

MP313

NUMBER THEORY III

(UNIT COURSES)

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

Attempt **SIX** questions only.
All questions carry the same number of marks.

1. (a) Define Euler's function $\phi(n)$ and prove that

$$\sum_{d|n} \phi(d) = n.$$

(b) Determine the positive integers n for which $\phi(n) = 2^k$ for some $k \geq 1$.

(c) Explain how the Chinese remainder theorem enables us to deduce that $\phi(mn) = \phi(m)\phi(n)$ if $\gcd(m, n) = 1$.

(d) If $\sigma(n)$ denotes the sum of the positive divisors of n, prove that

$$\sum_{k=1}^{n} \sigma(k) = \sum_{j=1}^{n} j \left\lfloor \frac{n}{j} \right\rfloor,$$

where $\lfloor x \rfloor$ denotes the integer part symbol.

2. (a) Define the Möbius function $\mu(n)$ and prove that

(i) $\sum_{d|n} \mu(d) = 0$ if $n > 1$.

(ii) $\sum_{d|n} |\mu(d)| = 2^{\omega(n)}$ if $n > 1$, where $\omega(n)$ is the number of distinct prime factors of n.

(b) State the Möbius inversion formula.

(c) Let $z, n \in \mathbb{N}$ and $T(z, n)$ be the number of integers x satisfying $1 \leq x \leq z$ and $\gcd(x, n) = 1$.

(i) Prove that $T(z, n) = \sum_{d|n} \mu(d) \left\lfloor \frac{z}{d} \right\rfloor$.

(ii) Deduce that that $T(z, n) = \frac{z}{n}\phi(n) + U(z, n)$, where $|U(z, n)| \leq d(n)$, where $d(n)$ is the divisor function.

Questions 3–6 on next page

 TURN OVER

3. (a) Define the term *primitive root (mod n).*

   (b) Given that 2 is a primitive root $\pmod{29}$, solve the congruence

$$x^{21} \equiv 2^{14} \pmod{29}.$$

   (c) Let $p = 4n + 1$ be a prime. If g is a primitive root $\pmod{p}$, prove that $-g$ is also a primitive root $\pmod{p}$.

   (d) If p is a prime, prove that the number of primitive roots $\pmod{p}$ in the range $1 \leq x \leq p - 1$ is $\phi(p - 1)$.

4. (a) Define $\text{ord}_m n$ if $\gcd(m, n) = 1$.

   (b) If $\gcd(m, n) = 1$ and $\gcd(a, mn) = 1$, prove that

$$\text{ord}_{mn} a = \text{lcm}\,(\text{ord}_m a, \text{ord}_n a).$$

   (c) If p is an odd prime dividing $x^3 + 1$ but not $x + 1$, prove that $p \equiv 1 \pmod{6}$ by considering $\text{ord}_p x$.

   (d) Let p be an odd prime. If $p - 1 = 2^s t$, where t is odd, prove that the number of integers x in $1 \leq x \leq p - 1$, for which $\text{ord}_p x$ is even, is equal to $(p - 1)(1 - 1/2^s)$.

5. (a) Define the term *quadratic residue (mod p), Legendre symbol* $\left(\frac{a}{p}\right)$, where p is an odd prime.

   (b) Let a be an integer not divisible by the odd prime p. Prove that a is a quadratic residue $\pmod{p}$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. (Hint: In one direction, use the existence of a primitive root $\pmod{p}$.)

   (c) Show that the congruence $x^2 + 37x + 48 \equiv 0 \pmod{109}$ is solvable by completing the square. Also find the solutions (mod 109) using `peralta` in CALC.

   (d) Prove that $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{3}$.

   (e) Let $p = 2q + 1$ be a prime, where q is a prime. If $\left(\frac{a}{p}\right) = -1$ and a is not congruent to $-1 \pmod{p}$, prove that a is a primitive root (mod p).

6. (a) Define the term *reduced quadratic irrational* and prove that $\alpha = \lfloor\sqrt{d}\rfloor + \sqrt{d}$ is a reduced quadratic irrational, if d is a non–square positive integer.

   (b) Determine the quadratic irrational defined by $\alpha = [\overline{1, 2, 1}]$ and check your answer using `surd` in CALC.

   (c) Derive the continued fraction expansion of $\sqrt{41}$ and hence determine the solutions in least positive integers x and y of $x^2 - 41y^2 = -1$ (if a solution exists) and also of $x^2 - 41y^2 = 1$.

Questions 7 on next page

 TURN TO PAGE 3

7. (a) Define the terms *p–adic integer, p–adic number, p–adic unit.*

   (b) Which rational numbers are (a) p–adic integers, (b) p–adic units?

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

   (d) Find the rational number r defined by the periodic 5–adic series

$$r = 4 + 2 \cdot 5 + 4 \cdot 5^2 + 2 \cdot 5^3 + \cdots$$

   (e) Find the digits a_1 and a_2 of the canonical expansion $\sqrt{7} = 1 + a_1 3 + a_2 3^2 + \cdots$ in $\hat{\mathbb{Z}}_3$.