**MA 3H1**

**THE UNIVERSITY OF WARWICK**

**THIRD YEAR EXAMINATION: April 2010**

**TOPICS IN NUMBER THEORY**

---

Time Allowed: **3 hours**

Read carefully the instructions on the answer book and make sure that the particulars required are entered on each answer book.

Calculators are not needed and are not permitted in this examination.

ANSWER 4 QUESTIONS.
If you have answered more than the required 4 questions in this examination, you will only be given credit for your 4 best answers.

The numbers in the margin indicate approximately how many marks are available for each part of a question.

---

**1.** Let $p$ be a prime.

a) What does it mean for an integer $g$ to have order $d$ modulo $p$? **[2]**

b) Show that if $g$ has order $d$ modulo $p$ and if $g^m \equiv 1 \pmod{p}$ then $d \mid m$. **[6]**

c) Suppose $g_1$ and $g_2$ respectively have orders $d_1$, $d_2$ modulo $p$. Suppose moreover that $\gcd(d_1, d_2) = 1$. Show that $g_1 g_2$ has order $d_1 d_2$ modulo $p$. **[6]**

d) What does it mean for $g$ to be a primitive root modulo $p$? **[2]**

e) Show that $p$ must have a primitive root. You may assume that if $q^e$ is a prime power dividing $p-1$ then $x^{q^e} \equiv 1 \pmod{p}$ has precisely $q^e$ incongruent solutions modulo $p$. **[6]**

f) Find a primitive root for 149. You may use the following observations: **[3]**

$$149 = 2^2 \times 37 + 1, \qquad 5^{37} \equiv 44^4 \equiv 1 \pmod{149}, \qquad 44^2 \not\equiv 1 \pmod{149}.$$

---

**2.** a) Let $a$ be an integer and $p$ an odd prime. Show that

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

You may assume standard facts about primitive roots. **[7]**

b) State without proof the two supplements to the law of quadratic reciprocity. **[4]**

c) Let $x$ be an even integer. Show that every prime divisor $p$ of $x^4 + 1$ satisfies

$$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1,$$

and hence $p \equiv 1 \pmod 8$. **Hint:** You might find it helpful to observe that $x^4 + 1 = (x^2 + 1)^2 - 2x^2$. **[7]**

d) Deduce that there are infinitely many primes $p \equiv 1 \pmod 8$. **[7]**

---

**3.** a) State Blichfeldt's Theorem and Minkowski's Theorem. **[6]**

b) Give a proof of Minkowski's Theorem assuming Blichfeldt's Theorem. **[6]**

c) Let $a$, $b > 0$. Show that the area of the ellipse

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} < 1$$

is $\pi ab$. You may assume the formula for the area of a circle. **[6]**

d) Suppose $\lambda$ and $N$ are coprime positive integers satisfying

$$\lambda^2 \equiv 2 \pmod{N}.$$

Show that there are integers $x$, $y$ such that **[7]**

$$x^2 - 2y^2 = \pm N.$$

**Hint:** In Minkowski's Theorem, take the convex symmetric set to be

$$C = \{(x, y) \in \mathbb{R}^2 : x^2 + 2y^2 < 2N\}.$$

---

**4.** a) Let $f(X) \in \mathbb{Z}[X]$, $a \in \mathbb{Z}$ and $n$ a positive integer. Show that $f^{(n)}(a)/n!$ is an integer. **[4]**

b) Let $f(X) \in \mathbb{Z}[X]$. Let $p$ be a prime and $m \geq 1$. Suppose $a \in \mathbb{Z}$ satisfies

$$f(a) \equiv 0 \pmod{p^m}, \qquad f'(a) \not\equiv 0 \pmod{p}.$$

Show that there exists some $b \in \mathbb{Z}$ such that **[8]**

$$b \equiv a \pmod{p^m}, \qquad f(b) \equiv 0 \pmod{p^{m+1}}.$$

c) Solve the following simultaneous system of congruences **[4]**

$$x^2 \equiv 3 \pmod{5^3}, \qquad x^2 \equiv 6 \pmod{7}.$$

d) Solve the following simultaneous system of congruences **[9]**

$$y^3 \equiv 3 \pmod{5^3}, \qquad y \equiv 1 \pmod{4}.$$

---

**5.** Let $p$ be a prime.

a) Let $\alpha$ be a rational number. Define $\mathrm{ord}_p(\alpha)$ and $|\alpha|_p$. **[2]**

b) Let $\alpha$, $\beta$ be rational numbers. Prove that

$$\mathrm{ord}_p(\alpha + \beta) \geq \min\{\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)\},$$

and **[8]**

$$|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}.$$

c) Prove that the series of rational numbers $\sum_{n=1}^{\infty} a_n$ converges in $\mathbb{Q}_p$ if and only if $\lim_{n\to\infty} |a_n|_p = 0$. You may assume that a sequence converges in $\mathbb{Q}_p$ if and only if it is $p$-adically Cauchy. **[7]**

d) State—with proof—for which primes $p$ do the following series converge in $\mathbb{Q}_p$?

(i) $1 + (21/2)^2 + (21/2)^4 + (21/2)^8 + \cdots$. **[4]**

(ii) $1^1 + 2^2 + 3^3 + 4^4 + \cdots$. **[4]**

---



**END**