UNIVERSITY COLLEGE LONDON

EXAMINATION FOR INTERNAL STUDENTS

MODULE CODE : **MATH7701**

ASSESSMENT PATTERN : **MATH7701A**

MODULE NAME : **Number Theory**

DATE : **27-May-14**

TIME : **10:00**

TIME ALLOWED : **2 Hours 0 Minutes**

TURN OVER

All questions may be attempted but only marks obtained on the best **four** *solutions will count.*
The use of an electronic calculator **is** *permitted in this examination.*

1. (a) Solve the following congruence by any method you choose.

$$x^{749} \equiv 3 \bmod 2014.$$

Express your answer as an integer between 0 and 2013.

(b) Explain what is meant by a *primitive root* modulo a prime number p.

(c) Find a primitive root modulo 23, making your method clear.

(d) Show that if a is a primitive root modulo 17, then so is $2a$. Hence or otherwise find all primitive roots modulo 17. (You may use without proof the standard criterion for a number to be a primitive root.)

2. (a) Let p be an odd prime number. Prove that

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

You may use without proof any properties of the ring $\mathbb{Z}[\zeta]$, where $\zeta = e^{2\pi i/8}$.

(b) Calculate the quadratic residue symbol $\left(\frac{134}{211}\right)$, showing your working.

(c) For which prime numbers p does the following congruence have solutions?

$$x^2 \equiv -3 \bmod p.$$

3. (a) State and prove Hensel's Lemma.

(b) Find a solution to the congruence

$$x^3 + x + 4 \equiv 0 \bmod 81.$$

Express your answer as an integer between 0 and 80.

4. (a) Let p be an odd prime and let $x \in \mathbb{Z}_{(p)}$. Show that the series $\exp(px)$ converges p-adically. (You may assume without proof any relevant facts about $v_p(n!)$).

   (b) Calculate the 3-adic logarithm $\log(7)$ mod 81.

   (c) Hence write 7^x mod 81 as a polynomial in x for $x \in \mathbb{Z}_{(p)}$.

   (d) Using your expansion of 7^x, find a solution to the congruence

   $$y^4 \equiv 7 \bmod 81.$$

   How many solutions does this congruence have? (Justify your answer.)

5. (a) Let d be a square-free integer such that $d \not\equiv 1 \bmod 4$, and assume that the corresponding quadratic ring $\mathbb{Z}[\sqrt{d}]$ has unique factorization. Let p be a prime not dividing $2d$. Prove that p splits in $\mathbb{Z}[\sqrt{d}]$ if and only if d is a quadratic residue modulo p.

   (b) Decompose the primes 3, 5 and 23 in the quadratic ring $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$. (You may assume that $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$ has unique factorization.)

   (c) Hence find integers x, y such that

   $$x^2 + xy + 3y^2 = 345.$$

6. (a) Find the continued fraction expansion of $\frac{93}{35}$.

   (b) Find the continued fraction expansion of $\sqrt{7}$.

   (c) Using the continued fraction expansion, find the fundamental solution to Pell's equation $x^2 - 7y^2 = 1$.

   (d) Find two distinct solutions (x_1, y_1) and (x_2, y_2) in positive integers to the equation

   $$x^2 - 7y^2 = 29.$$