www.mymathscloud.com

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) Define the Euler totient function φ.
   (b) Prove that for any prime p and any positive integer a, we have
   $$\varphi(p^a) = (p-1)p^{a-1}.$$
   (c) Factorize 2013 into primes and hence calculate $\varphi(2013)$.
   (d) Calculate $5^{12121203}$ modulo 2013 by any method you choose. (Express your answer as an integer between 0 and 2012.)
   (e) Solve the congruence $x^{343} \equiv 2 \bmod 2013$. (Express your answer as an integer between 0 and 2012.)

2. (a) Let p be a prime number. Explain what is meant by a *primitive root modulo* p.
   (b) Describe a method for finding a primitive root modulo p.
   (c) Using your method, find a primitive root modulo 41.
   (d) Calculate the Teichmüller lift $T(2)$ of 2 modulo 5^3.
   (e) Decompose the element $33 \in (\mathbb{Z}/5^3)^\times$ in the form
   $$33 \equiv T(x) \cdot \exp(5y) \bmod 5^3,$$
   where $x \in \mathbb{F}_5^\times$ and $y \in \mathbb{Z}/25$.

3. (a) Define the quadratic residue symbol $\left(\frac{a}{p}\right)$.
   (b) State and prove Euler's criterion.
   (c) Calculate the quadratic residue symbol $\left(\frac{124}{199}\right)$, showing your working.
   (d) Which of the following congruences have solutions ? Justify your answers.
      (i) $x^2 \equiv 124 \bmod (199^{300})$,
      (ii) $x^2 \equiv 124 \bmod (4 \times 199)$,
      (iii) $x^2 \equiv 124 \bmod (16 \times 199)$.

www.mymathscloud.com

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

   (b) Find a solution to the congruence

$$x^3 + 2x^2 + x - 1 \equiv 0 \bmod 81.$$

   Write your answer as an integer between 0 and 80.

5. (a) Define the valuation v_p, where p is a prime number.

   (b) Write down a criterion for a series $\sum_{m=1}^{\infty} a_m$ of numbers $a_m \in \mathbb{Z}_{(p)}$ to converge p-adically.

   (c) Assuming that p is an odd prime, show that the binomial series expansion of $\sqrt[4]{1+px}$ converges modulo p^n for all integers x. (You may assume without proof that $v_p(n!) \leq \frac{n}{p-1}$).

   (d) Using the binomial expansion in (c), find a solution to the congruence

$$x^4 \equiv 6 \bmod 125.$$

   Write x as an integer between 0 and 124.

6. (a) Using Euclid's algorithm in $\mathbb{Z}[i]$, show that $18+3i$ and $5+4i$ are coprime and find Gaussian integers h, k such that

$$(18+3i)h + (5+4i)k = 1.$$

   (b) State and prove the decomposition law for Gaussian integers.

   (c) Factorize 37 and 41 into Gaussian primes.

   (d) Hence write the number 3034 as a sum of two squares.