1. (a) Define what it means for a function f defined on the positive integers to be *multiplicative*. [2]

   (b) Prove that the divisor function τ (defined as $\tau(n)$ being the number of divisors of n) is multiplicative. [7]

   (c) Prove that if f is a multiplicative function with $f(n) \neq 0$ for all $n \in \mathbb{N}$, then so is $1/f$. [2]

   (d) Prove that the Euler product for the Dirichlet series for $1/\tau$ is

   $$\prod_p \left(-p^s \log(1-p^{-s})\right).$$

   [7]

   (e) (not connected with (a)-(d) above). Let g be the function $g : \mathbb{R} \to \mathbb{Z}$ given by

   $$g(x) = \left\lfloor \frac{x}{2} \right\rfloor + \left\lfloor \frac{x}{3} \right\rfloor + \left\lfloor \frac{x}{6} \right\rfloor.$$

   Describe explicitly, with justification, the following three sets:

   i. $\{x \in \mathbb{R} : g(x) = 3\}$;
   ii. $\{x \in \mathbb{R} : g(x) = 4\}$;
   iii. $\{x \in \mathbb{R} : g(x) = x\}$.

   [7]

2. (a) Define the Legendre symbol $\left(\frac{a}{p}\right)$ for p an odd prime.

   Evaluate $\left(\frac{a}{7}\right)$ for all $a \in \{1, 2, 3, 4, 5, 6\}$. [3]

   (b) State and prove Gauss's Lemma (which gives a formula for $\left(\frac{a}{p}\right)$, for p an odd prime). [7]

   (c) Apply Gauss's Lemma to prove that $\left(\frac{2}{p}\right) = -1$ when p is a prime $\equiv 3 \pmod 8$. [6]

   (d) State without proof the Law of Quadratic Reciprocity. [3]

   (e) Apply quadratic reciprocity to find a 6-element set B such that $\left(\frac{7}{p}\right) = 1$ iff p is a prime with $p \equiv b \pmod{28}$ for some $b \in B$. [6]

[Continued overleaf...]

3. (a) Let p and q be distinct primes. Prove that if $\gcd(a, pq) = 1$ then $a^{\mathrm{lcm}(p-1,q-1)} \equiv 1 \pmod{pq}$. [5]

   (b) Now let g be a primitive root $\pmod{p}$ and h be a primitive root $\pmod{q}$. Using g and h, apply the Chinese Remainder Theorem to specify an integer a whose order $\pmod{pq}$ is (exactly) $\mathrm{lcm}(p-1, q-1)$. [5]

   (c) Now suppose that p is the larger of the primes p and q.
   Calculate $pq - 1 \pmod{p-1} \in \{0, 1, \ldots, p-2\}$.
   Deduce that $p - 1 \nmid pq - 1$. [5]

   (d) Use the above to show that there is an a with $\gcd(a, pq) = 1$ and $a^{pq-1} \not\equiv 1 \pmod{pq}$. [5]

   (e) Define a Carmichael number. Deduce from the above that a Carmichael number must have at least 3 prime factors. [5]
   [You may assume without proof that all Carmichael numbers are squarefree.]

4. (a) Suppose that $x^2 \equiv a \pmod{p^n}$ for some integers a and x with $\gcd(a, p) = 1$, odd prime p and integer $n \geq 1$. Show, with proof, how to produce an integer x_1 such that $x_1 \equiv x \pmod{p^n}$ and $x_1^2 \equiv a \pmod{p^{2n}}$. [8]

   (b) Starting with an integer a and an odd prime p satisfying $\left(\frac{a}{p}\right) = 1$, explain how part (a) can be used to solve $x^2 = a$ in the p-adic field $\mathbb{Q}_p$. [6]

   (c) For an odd prime p, write $(p^2 - 1)/4$ as a p-adic integer in the form $b_0 + b_1 p$, where $b_0, b_1 \in \{0, 1, \ldots, p-1\}$. [4]
   [You might find the identity $p^2 - 1 = p - 1 + (p-1)p = 3p - 1 + (p-3)p$ useful.]

   (d) Use the identity $-\frac{1}{4} = \frac{(p^2-1)/4}{1-p^2}$ to write $1/4$ as a p-adic integer in the form $a_0 + a_1 p + a_2 p^2 + \ldots$, where $a_0, a_1, a_2, \cdots \in \{0, 1, \ldots, p-1\}$. [7]

[End of Paper]