EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May	2019	MATH2617-WE01

Title:
Elementary Number Theory II

Time Allowed:	2 hours	
Additional Material provided:	None	
Materials Permitted:	None	
Calculators Permitted:	No	Models Permitted: Use of electronic calculators is forbidden.
Visiting Students may use dictionaries: No		

Instructions to Candidates:	Credit will be given for the best **TWO** answers from Section A and the best **TWO** answers from Section B. Questions in Section B carry **ONE and a HALF times** as many marks as those in Section A.

Revision:	

ED01/2019

SECTION A

1. (a) Find all $n \in \mathbb{N}$ such that $\varphi(n) = 2$, where φ is the Euler φ-function. (You must justify that you have found all such n.)

   (b) Find a solution $x \in \mathbb{Z}$, $0 < x < 221$ to the system of congruences

$$\begin{aligned} 2x &\equiv 5 \pmod{13}, \\ 3x &\equiv 7 \pmod{17}. \end{aligned}$$

2. (a) Let $m, n \in \mathbb{N}$. Show that

$$\gcd\left(\frac{m}{\gcd(m,n)}, \frac{n}{\gcd(m,n)}\right) = 1.$$

   (b) Let $a, b, n \in \mathbb{N}$ and let d be a common divisor of a and b. Show that if $a \equiv b \pmod{n}$, then

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{n/\gcd(d,n)}.$$

3. Let p be an odd prime.

   (a) Give a proof of the result from the lectures that there are exactly $(p-1)/2$ quadratic residues modulo p.

   (b) Let $a \in \mathbb{Z}$ be such that p does not divide a. Show the result from the lectures that $0, a, 2a, \ldots, (p-1)a$ is a complete set of residues mod p and use this to evaluate the sum

$$\sum_{i=1}^{p-1} \left(\frac{ai}{p}\right),$$

   where $\left(\frac{ai}{p}\right)$ is the Legendre symbol.

SECTION B

4. (a) Evaluate the Legendre symbol $\left(\frac{59}{131}\right)$.

   (b) Show that 5 is a quadratic residue (QR) modulo every prime of the form $10n+1$ and that it is not a QR modulo every prime of the form $10n-7$, for $n \in \mathbb{N}$.

   (c) Let p be a prime of the form $8n+1$, $n \in \mathbb{N}$. Show that the polynomial $x^8 - 1$ divides the polynomial $x^{p-1} - 1$, that is, show that there exists a polynomial $g(x)$ such that

   $$x^{p-1} - 1 = (x^8 - 1)g(x).$$

   Use this to prove that the congruence $x^4 \equiv -1 \pmod{p}$ has a solution $x \in \mathbb{N}$.

   (d) Let p be an odd prime which is not of the form $8n+1$ for any $n \in \mathbb{N}$. Show that the congruence

   $$x^4 \equiv -1 \pmod{p}$$

   does not have any solution $x \in \mathbb{N}$.

5. (a) Let g be a primitive root mod 17 and let $i \in \mathbb{N}$ be a number such that $g^i \equiv 13 \pmod{17}$. Show that for any $n \in \mathbb{N}$, we have $g^{in} \equiv 13 \pmod{17}$ if and only if $in \equiv i \pmod{16}$.

   (b) Find a primitive root g mod 17 and a number $i \in \mathbb{N}$ such that $g^i \equiv 13 \pmod{17}$. Justify your answer.

   (c) Find four distinct solutions $x \in \mathbb{N}$ with $x < 17$ to the congruence

   $$x^{44} \equiv 13 \pmod{17}.$$

6. (a) Find natural numbers a and b such that

   $$\left|\sqrt{52} - \frac{a}{b}\right| < 10^{-6}.$$

   (b) Assume that $x^4 - y^4 = 2z^2$ has a solution in natural numbers x, y, z. Show that there exists a solution $a^4 - b^4 = 2c^2$ in natural numbers a, b, c such that a and b are odd.

   (c) Assume that a, b, c are as in the previous part. Show that there exists a solution $a_1^4 - b_1^4 = 2c_1^2$ in natural numbers a_1, b_1, c_1 such that $\gcd(a_1, b_1, c_1) = 1$.