

## EXAMINATION PAPER

Examination Session: May/June

2020

Year:

Exam Code:

MATH2617-WE01

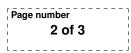
Title:

## Elementary Number Theory II

Time (for guidance only):	2 hours	
Additional Material provided:		
Materials Permitted:		
Calculators Permitted:	Yes	Models Permitted: There is no restriction on the model of calculator which may be used.

Instructions to Candidates:	Credit will be given for your answers to all questions. Questions in Section B carry <b>ONE and a HALF times</b> as many marks as those in Section A.
	Please start each question on a new page. Please write your CIS username at the top of each page.
	Show your working and explain your reasoning.

**Revision:** 



## SECTION A

**Q1** 1.1 Let  $a, b \in \mathbb{N}$  such that gcd(a, b) = 1. Determine the possible values of

$$gcd(a-b, a+b).$$

You must prove that only certain values are possible and give examples of a and b for which these values are obtained.

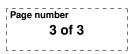
**1.2** Find all  $n \in \mathbb{N}$  (if any) such that  $\varphi(n) = 14$ . Here  $\varphi$  is the Euler  $\varphi$ -function.

**Q2** 2.1 Find a number  $a \in \mathbb{N}$  such that  $103a \equiv 1 \pmod{23}$ .

**2.2** Find an integer 0 < n < 23 such that if  $x \in \mathbb{Z}$  is a solution to the congruence

$$103x^5 \equiv 1 \pmod{23},$$

then we must have  $x \equiv n \pmod{23}$ . In other words, show that if  $103x^5 \equiv 1 \pmod{23}$  has a solution x, then  $x \equiv n \pmod{23}$ .



## SECTION B

- Q3 3.1 Find the last digit of 7<sup>999,999</sup>.
  - 3.2 Find the smallest positive integer solution to the system of congruences

$$x \equiv 10 \pmod{11},$$
$$x \equiv 3 \pmod{15}.$$

- **3.3** Evaluate the Legendre symbol  $\left(\frac{107}{1009}\right)$ . You may assume without proof that 107 and 1009 are primes.
- **Q4** Let p be a prime such that p = 2q + 1, where q is an odd prime. Let  $a \in \mathbb{Z}$  such that 1 < a < p 1.
  - **4.1** Show that ord  $_p(-a^2) \in \{1, 2, q, 2q\}.$
  - **4.2** Show that ord  $_p(-a^2) \neq 1$ .
  - **4.3** Show that  $\operatorname{ord}_p(-a^2) \neq 2$ . (Hint: Assuming the opposite, which two integers does  $\operatorname{ord}_p(a)$  have to divide? Why is that impossible?)
  - **4.4** Show that  $\operatorname{ord}_p(-a^2) \neq q$  and conclude that  $-a^2$  is a primitive root modulo p.
- **Q5** Let p be a prime and let  $x, a \in \mathbb{Z}$  be such that  $x^2 \equiv a \pmod{p}$ .
  - **5.1** Show that if  $y^2 \equiv a \pmod{p^2}$ , for some  $y \in \mathbb{Z}$ , then

$$y = \pm x + pk_{z}$$

for some  $k \in \mathbb{Z}$  such that  $\pm 2xk \equiv \frac{a-x^2}{p} \pmod{p}$ .

- **5.2** Conversely, show that if y = x + pk, for some  $k \in \mathbb{Z}$  such that  $2xk \equiv \frac{a-x^2}{p} \pmod{p}$ , then  $y^2 \equiv a \pmod{p^2}$ .
- **5.3** Assume that  $p \neq 2$  and that p does not divide a. Show that there exists a solution  $y \in \mathbb{Z}$  to the congruence  $y^2 \equiv a \pmod{p^2}$ .
- **5.4** Find a  $y \in \mathbb{N}$  such that  $y^2 \equiv 3 \pmod{121}$  (*Hint: Use the previous part.*)