MAS 4203 – QUIZ 5 – Summer 2014

~~Tuesday, August 5~~ **MAKE-UP**

NAME:

Instructions: all work should be written in a proper and coherent manner, and in a way that any student in the class can follow your work. Show all necessary reasoning and working. When giving proofs your reasoning should be clear. Only scientific or basic calculators are allowed.

TOTAL: 15 points = 100%

1. [1 + 2 + 2 + 2½ = 7½ points]

1 (a) Complete the Definition: Let p be an ___ prime and let $a \in \mathbb{Z}$ with ___. The Legendre symbol, denoted ___ is

$$\left(\frac{a}{p}\right) = \begin{cases} \_\_\_, & \text{if } \_\_\_\_\_ \\ \_\_\_, & \text{if } \_\_\_\_\_ \end{cases}$$

2 (b) Complete Euler's Criterion: Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Then

$$\left(\frac{a}{p}\right) \equiv \_\_\_\_\_ \pmod{p}.$$

2 (c) Complete Gauss's Lemma: Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Then

$$\left(\frac{a}{p}\right) = (-1)^n$$

where n is ___ of the integers ___ that are ___

$2\frac{1}{2}$ (d) Use Gauss's Lemma to prove that

$$\left(\frac{2}{p}\right) = (-1)^n$$

where $n = \frac{1}{2}(p-1) - \left[\frac{p}{4}\right]$ and p is any odd prime.

2. [1 + 2 + 2 + $2\frac{1}{2}$ = $7\frac{1}{2}$ points]

1 (a) Complete the Law of Quadratic Reciprocity:

Let p, q be _____ primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\text{------}}$$

$$= \begin{cases} 1, & \text{if } \_\_\_\_\_ \\ -1, & \text{if } \_\_\_\_\_ \end{cases}$$

If p _____ Then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

If p _____ Then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

(3)

2 (b) Find $\left(\frac{2819}{4177}\right)$. Show all reasoning.

2. (c) Complete Eisenstein's Lemma: Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$ and ____.

If

$$N = \sum_{j=1}^{(p-1)/2} \text{----}$$

then

$$\left(\frac{a}{p}\right) = \text{----}.$$

2½ (d) Find congruences that characterise all prime numbers p for which 70 is a quadratic residue mod p.

3. [3 bonus points]

RSA is one of the first practicable _____ cryptosystems and is widely used for _____ data transmission. In such a cryptosystem, the encryption key is _____ and differs from the decryption key which is kept _____. In RSA, this asymmetry is based on the practical difficulty of _____ the product of two large _____ _____. RSA stands for R___ R_____, A___ S_____ and L_____ A_____, who first publicly described the algorithm in _____.