Math 3207 Assignment 4, November 2012

Clearly write your answers to the questions showing all reasons, working and checks and indicate what each mathematical calculation is doing. Do not erase anything. Include all rough work and do not commit plagiarism. Feel free to write explanations of what you are thinking at each stage, nothing you can write can lose you marks!

1. (a) Use a dozenal sieve to find all the small primes necessary and then use modular arithmetic and perform at least 3 long divisions in dozenal (giving all digits after the dozenal point) to prove that 147ε is prime [4]

   (b) Use the dozenal rules of divisibility to factorise your number n completely and hence evaluate the Legendre symbol $\left(\frac{n}{147\varepsilon}\right)$ without using any other base than dozenal. [4]

   (c) Convert n into binary without using decimal and then explain how the numbers of digits of any particular integer in two different bases are related in general, by first considering a base which is a divisor of another, and then generalising. [3]

2. (a) Prove that, for any odd prime p and a and b integers such that $(a, p) = 1$, we have either +1, -1 or 0 for this sum of Legendre symbols, and explain what the value will depend on: [3]

$$\sum_{j=1}^{p-1} \left(\frac{aj+b}{p}\right)$$

   (b) Use this result to explain what $\prod_{j=1}^{p-1} \left(\frac{aj+b}{p}\right)$ will therefore equal. [2]

3. This question is in decimal. Use Euler's criterion to verify there is a solution to your quadratic equation. List the first 14 squares mod 97 and hence find the solution by means of the method of removing squares. [4]

4. (a) Modify the proof from the notes to find, given odd primes p and q, all conditions on q so that it is a divisor of $\frac{a^p+1}{a+1}$. Why is this fraction guaranteed to be an integer? [3]

   (b) Find an integer $a > 2$ and prime $p > 2$ such that $\frac{a^p+1}{a+1}$ is prime and unique within the class, explaining why you can be sure. [2]

$$n = 1056 \qquad x^2 \equiv -9 \pmod{97}$$

$$n = 1033 \qquad x^2 \equiv 22 \pmod{97}$$

$$n = 1113 \qquad x^2 \equiv -4 \pmod{97}$$

$$n = 1156 \qquad x^2 \equiv -18 \pmod{97}$$

$$n = 11\delta 9 \qquad x^2 \equiv -3 \pmod{97}$$

$$n = \varepsilon 59 \qquad x^2 \equiv -2 \pmod{97}$$

$$n = 1136 \qquad x^2 \equiv 88 \pmod{97}$$