Math325 Number Theory: Assignment 4 (November 30th 2010)

Answer all questions and give complete reasons and checks for your answers. Hand in ALL of your rough working together with your final answers. The parts of the questions are weighted as shown on the right of the question. Use of Maple to investigate or check answers is encouraged where appropriate but all working must be given by hand. You are reminded that plagiarism is a serious offense and when caught you will suffer the penalties specified by the University.

1. In any base we can have a point just like the standard decimal point, using long division and that 1 is the same as $1.0000\ldots$, as usual.

   (a) Verify that, in dozenal (the modern name for duodecimal) that $2^{-1} = 0.6$ and $5^{-1} = 0.\overline{2497}$, where the line indicates that the fraction repeats. Find the dozenal representation for δ^{-1} and two other reciprocals of integers in dozenal. [3]

   (b) Prove that in any base b that if $d > 1$ is a divisor of 10 then there will be exactly one digit after the point in d^{-1}. Determine when a reciprocal will not repeat for every base and how many places there will be after the point for the reciprocal of such any number n when written in a particular base b. [5]

2. Suppose $a > 0$ and $c \geq 2$. What is the value of the continued fraction which is $(a; 1, c)$? What are the values of the continued fractions which are $(a; \overline{1, c})$ and $(a; 1, \overline{c})$? Explain why, using the continued fractions, which of these three numbers is the largest. [7]

3. Create a number n (different from all others in the class) which is the product of 3 primes between 30 and 60.

   (a) Determine how many steps Fermat factorisation would take for nk with each multiplier $k = 1, 5$ and 15 and verify this for your smallest answer. [2]

   (b) How many steps should Pollard $p - 1$ need for your n, at worst? Check this. [2]

4. (a) Create a 3 letter word using the standard 29 letter alphabet and determine its value as a trigraph. [1]

   (b) Create a public/private key pair using $n = 25777 = 149 \times 173$ and encrypt your message so that I can read it and know it came from you, knowing only your public key. Assume my public key is $e = 12999$. [5]