Math 3207 Assignment 5, December 2018

Please show all working and reasoning to get full marks for any question. Hand in your rough working as well so I can see how you investigated and reached your final results. You can use Maple at any point and can email me any worksheets you created.

You are reminded that plagiarism is a serious offense and when it is detected you will be punished. Feel free to discuss the questions in general with myself and your colleagues but the work attempted must be yours alone. A maximum of $20 - \frac{p_y}{2}$ marks can be received for this assignment if you hand your work in y days after the deadline, where p_y is the y^{th} prime number; $p_1 := 2$, $p_2 := 3$, $p_3 := 5$, $p_4 := 7$, $p_5 := 11$, etc.

1. You have randomly picked one of the slips of paper with n and f on.

   (a) Use surd arithmetic to find the first six terms in the continued fraction of $\sqrt{n}$, and use the table method to calculate the convergents $\frac{\alpha_j}{\beta_j}$. [3]

   (b) Calculate and factorise the values of $\alpha_j^2 - n\beta_j^2$ and hence identify a combination of them which is a square number. Use this and the Euclidean algorithm with n to find one of the two prime factors of n. [3]

   (c) Determine which real number has repeating continued fraction f and hence find a rational number which approximates f to 5 decimal places. [3]

2. (a) Use your knowledge of the factorisation of your m to determine how many steps standard Fermat factorisation will take. Why will it find it more quickly if use $3m$ instead? Similarly, factorise $p-1$ for all the factors p of n and determine which of them is the smoothest, and so indicate if Pollard $p-1$ factorisation would succeed after 10 iterations or not. [3]

   (b) Use Pollard Rho on n with $a := 59$ and $b := 222$ and verify that it finds a factor within six iterations. [2]

3. Recall that a Carmichael number c must satisfy $a^{c-1} \equiv 1 \pmod{c}$ for all a which have $\gcd(a, c) = 1$.

   (a) Given any even c find an a for which the condition cannot be true, so showing that there are no even Carmichael numbers. [1]

   (b) Now suppose that $c = p^k m$ where $\gcd(p, m) = 1$. Let a be the number which is congruent to 1 (mod m) and $1 + p$ (mod p^k). Assuming that c is Carmichael, explain why $a^c \equiv a \pmod{p^2}$ and find a contradiction after establishing that $a \equiv 1 + p \pmod{p^2}$. [3]

   (c) Factorise your number m into 3 primes p, q and r and verify that $p-1$, $q-1$ and $r-1$ all divide into $m-1$. Use this property to explain why no number t which is the product of just two primes can have the property that one less than its prime factors divides into $t-1$. [2]

A5a: $n := 12877$ $\quad f := (1, 2; \overline{2, 7})$ $\quad m := 2465$

A5b: $n := 12707$ $\quad f := (1, 1; \overline{3, 7})$ $\quad m := 2821$