Midterm #2 (15%)

CS3330 Scientific Computing, Instructor: Cheng-Hsin Hsu

Department of Computing Science, National Tsing Hua University, Taiwan

1:20 p.m. – , Dec. 4th, 2015

- **Please create a single latex document, write your solution (no need to copy the questions, but please clearly mark the question numbers *in order*) into it. That is, all the answers should go to the same .tex file (NOT 1 tex file per question). Please typeset your .tex file, and submit both (and only) your .tex and .pdf files before you leave the classroom. No partial credits will be given to students who fail to submit his/her .tex and .pdf files. In other words, I will only grade the .pdf file. Remember to put your name and student ID on the first page.**
- **You are allowed (actually encouraged) to search online for tips.**
- **You are not allowed to copy and paste source codes from the Internet. Furthermore, you cannot exchange (online/offline) messages with any of your peers during the exam. These are considered as academic dishonesty, which automatically leads to zero point. Furthermore, we will have no choice but report this incident to the university.**

1) (5%) In one of the lectures, we discuss how to perform integral in SageMath. Suppose, we want to calculate $\int_{-2}^{2} e^{-x^5} \sin x^3$. Answer the following questions.

   a) (1%) Let's quickly check the shape of this formula. Please use the command:

   ```
   plot(exp(-x^5)*sin(x^3), x, -5, 5, ymin=-1, ymax=1)
   ```

   to create a figure. Please include the figure and your observations on its shape in your writeup.

   b) (2%) The command `integral` allows us to perform definite integral. Please try it in SageMath, and explain why we didn't get a numerical answer?

   c) (2%) What if we can live with an approximated value of this integral? What SageMath command we may leverage? Please show your results and explain the meanings of the two elements of the returned pair.

2) (5%) Euler's ϕ function is defined as follows: $\phi(x)$ is the number of integers $1 \leq z \leq x$ where $\gcd(z, x) = 1$. Answer the following questions. Note that you won't get any point if you don't show your work.

   a) (1%) For a prime number p, what is $\phi(p)$?

   b) (1%) In SageMath, we use `euler_phi` to calculate Euler's ϕ function. Try to calculate $\phi(11), \phi(13)$, and $\phi(11 \times 13)$. Explain what you observe. Do you think we can generalize this observation to all distinct prime numbers p and q, rather than the specific numbers used here?

   c) (3%) Prove $\phi(pq) = \phi(p)\phi(q)$ for any distinct prime numbers p and q. Please type up your proof.

3) (5%) The Fermat's Little Theorem is written as: for any prime number p and for any $a \not\equiv 0 \pmod{p}$, we have: $a^{p-1} \equiv 1 \pmod{p}$. Please answer the following questions.

   a) (1%) First check the if the Mersenne number $2^{1279} - 1$ is prime using SageMath. Explain which function did you use to achieve this.

   b) (1%) Pick an arbitrary a value and verify Fermat's Little Theorem. One naive way to do this is to calculate a^{p-1} and then do the $\pmod{p}$. Why this is a bad idea?

   c) (3%) Based on the previous subquestion, develop a better approach to verify Fermat's Little Theorem using 3 different a values. After presenting your solution, please implement it in SageMath and show me how you verify the theorem.