Problem Set 9

Deliverable: Submit your responses as a single, readable PDF file on the collab site before **6:29pm** on **Friday, 1 December**.

Version: updated 21 November 2017 (just fixing typos, cosmetic changes, and added $\star$ for problem 9).

Collaboration Policy - Collaboration Policy (identical to PS5)

For this assignment, you may work in groups of one to three students to write-up a solution together. If you work with teammates, exactly one of you should submit one assignment that represents your collective best work with all of your names and UVA ids clearly marked on it. *Everyone on a team should understand everything you turn in for the assignment well enough to be able to produce it completely on your own.* All teammates must review the submissions before it is submitted to make sure you understand everything on it and that your name and UVA id are clearly marked on it.

Preparation

This problem set focuses on number theory — Chapter 9 of the MCS book, and Classes 20, 22, and 23.

Directions

Solve all the 9 problems. Your answers should be clear, consise, and convincing.

Wily Theorem

1. Fermat's last theorem, proved by Andrew Wiles in 1994, states that: for any natural $n > 2$ there are *no* natural numbers a, b, c such that
$$a^n + b^n = c^n.$$
Assuming Fermat's theorem, give a simple proof that $\sqrt[n]{2}$ is *not* a rational number.
(Hint: you can also give a dirct proof that does not use the Fermat's last theorem, but note that you then might loose the joy of proving a corollary to Fermat's theorem :)

Fast Exponentiation

2. In the Diffie Hellman key-exchange protocol described in Class 23, Alice and Bob need to compute $g^x \mod p$ and $g^y \mod p$ for some $1 \leq g, x, y \leq p-1$. Suppose p is a (prime) number that has 1000 bits when represented in binary.

   (a) Explain what is wrong (from a practical efficiency point of view) with using the following algorithm for computing g^x. (The $rem(a,p)$ operation computes the remainder of a modulo p using the well-known efficient division algorithm.)

   ```
   def SlowExp(g,p,x):
       a = 1
       while x > 0:
           a = a * g
           a = rem(a,p)
           x = x - 1
       return a
   ```

   Hint: try to estimate how many multiplications are used.

   (b) Describe a modified version of the "Fast Exponentiation Program" in Section 6.3.1 of the book that is useful computing $g^x \mod p$. How many multiplications does this program do in maximum to obtain g^x for an arbitrary $1 \leq x \leq p-1$ for a 1000 digit p?

Abelian Groups

For each set (R) and operator (P) described below, explain why it is not an Abelian group (defined in Class 22). Your answer should include a convincing supporting argument that shows why the given set and operator do not satisfy at least one of the required properties.

3. $R = \mathbb{Z}, P =$ *gcd* where *gcd* is a binary operator that takes two integers as input and outputs their greatest common divisor.
4. $R = \mathbb{Z}, P = -$.
5. $R = \{T, F\}, P =$ OR. (Hint: what must the identity be, and which element has no inverse?)

Fields

For each set (R) and first and second operations (P_+, $P_\times$), answer if the set and operations are a *field* (as defined in Class 23). A good answer will either show how the given set and operations satisfy the required properties (including explaning what the additive identify and multiplicative identity are), or show how it fails to satisfy one of the required properties.

6. $R = \mathbb{N}_{12}, P_+ = + \pmod{12}, P_\times = \times \pmod{12}$.
7. $R = \{\sharp, \flat\}$ $P_+ = \{(\sharp,\sharp) \to \sharp, (\sharp,\flat) \to \flat, (\flat,\sharp) \to \flat, (\flat,\flat) \to \sharp\}$ and $P_\times = \{(\sharp,\sharp) \to \sharp, (\sharp,\flat) \to \sharp, (\flat,\sharp) \to \sharp, (\flat,\flat) \to \flat\}$.
8. $R = \mathbb{N}_{31}, P_+ = \times \pmod{31}, P_\times = + \pmod{31}$.

Field Properties

9. ($\star$) Suppose R is an arbitrary field with some additive and multiplicative operations $P_+, P_\times$. Suppose we are given any $a, b, c \in R$ where $a \neq 0$; namely, a is not the additive identity element (usually denoted with 0). Then prove that there is a unique solution for variable $x \in R$ that satisfies $(a\ P_\times\ x)\ P_+\ b = c$.

   Hint: use the properties of the fields and describe a step by step process to actually find x.

   (Note the interesting message of this problem: fields shape the abstract notion that allows solving linear equations. Here we show it for a single variable linear equation, but the idea actually extends to multi-variable systems of equations.)

