Homework 3 MORALLY Due Feb 21 at 9:00AM
WARNING: THIS HW IS SIX PAGES LONG!!!!!!!!!!!!!!!!!

1. (25 points) Give a sentence in the first order language of $<$ that is TRUE in $\mathsf{Q} + \mathsf{Z}$ but FALSE in $\mathsf{Z} + \mathsf{Q}$.

GO TO NEXT PAGE

2. (25 points) Let p be a prime and $g \in \{1, \ldots, p-1\}$. g is a *generator for mod p* if

$$\{g^1, \ldots, g^{p-1}\} = \{1, \ldots, p-1\}.$$

(Note that we are NOT saying $g_1 = 1$, $g^2 = 2$, $\ldots$ $g^{p-1} = p-1$.)

A *safe prime* is a prime number p of the form:

$$p = 2q + 1$$

where q is also a prime number.

(a) (0 points but you will need this for part 3.) Write a program that will, given p, a safe prime, and $g \in \{1, \ldots, p-1\}$, determines if g is a generator for mod p.

(b) (0 points but you will need this for part 3.) Write a program that will, given safe prime p, determine how many generators for mod p there are.

(c) (25 points) Run the program on all primes ≤ 1000 and submit your program by emailing it to Emily (ekaplitz@umd.edu).

(d) (0 points but I REALLY WANT YOU TO DO THIS. This is the WHOLE POINT OF THE PROBLEM, but since it is speculative its hard to grade. Do it for ENLIGHTENMENT!) Graph $f(p) =$ the number of generators mod p. See if you can determine what function its close to (e.g., is it close to $\sqrt{p}$?)

GOTO NEXT PAGE

3. (25 points)

   (a) (25 points) Show that $7^{1/3}$ is irrational. (First proof a lemma about mods.)

   (b) (0 points, BUT DO IT!!!!) Try to use your proof to show that $8^{1/3}$ is irrational. What goes wrong?

GOTO NEXT PAGE

4. (25 points) Show that 23 CANNOT be written as the sum of ≤ 8 cubes.

GOTO NEXT PAGE

5. (Extra Credit) Show that $2^{1/3}$ does not satisfy any quadratic equation of the form $ax^2 + bx + c = 0$ with $a, b, c \in \mathsf{Z}$ and $a \neq 0$.

GOTO NEXT PAGE

6. (Extra Credit)

   Known for all k, DUP wins the k-round DUP-SPOILER game with Z and $\mathsf{Z} + \mathsf{Z}$.

   Hence there is no **First Order** sentence that is TRUE for $\mathsf{Z} + \mathsf{Z}$ but FALSE for Z.

   Give a **Second Order** sentence that is TRUE in $\mathsf{Z} + \mathsf{Z}$ but false in Z.