Homework 3 MORALLY Due Feb 14 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 $\mathsf{Z}+\mathsf{Q}$.

   SOLUTION

$$(\exists w)(\forall x)(\forall y)[x < y < w \rightarrow (\exists z)[x < z < y].$$

   END OF SOLUTION

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?

SOLUTION

1) All mods are mod 7.

Claim If $n^3 \equiv 0$ then $n \equiv 0$.

Proof We take the contrapositive: If $n \not\equiv 0$ then $n \not\equiv 0$. Cases:

$n \equiv 1 \Rightarrow n^3 \equiv 1^3 \equiv 1 \not\equiv 0$.

$n \equiv 2 \Rightarrow n^3 \equiv 2^3 \equiv 1 \not\equiv 0$.

$n \equiv 3 \Rightarrow n^3 \equiv 3^3 \equiv 6 \not\equiv 0$.

$n \equiv 4 \Rightarrow n^3 \equiv 4^3 \equiv 1 \not\equiv 0$.

$n \equiv 5 \Rightarrow n^3 \equiv 5^3 \equiv 6 \not\equiv 0$.

$n \equiv 6 \Rightarrow n^3 \equiv 5^3 \equiv 6 \not\equiv 0$.

End of Proof

We now do the proof. Assume, BWOC, that $7^{1/3} = \frac{a}{b}$ where a, b are in lowest terms.

$7^{1/3}b = a$

$7b^3 = a^3$, so $a^3 \equiv 0$, so by Claim $a \equiv 0$. Let $a = 7c$.

$7b^3 = (7c)^3$, so $b^3 = 7^2c^3$, so $b^3 \equiv 0$, so by Claim $b \equiv 0$.

a, b are both divisible by 7 and hence not rel prime.

2) The step $n \not\equiv 0 \pmod 8 \Rightarrow n^3 \not\equiv 0 \pmod 8$ does not work when $n \equiv 2 \pmod 8$.

END OF SOLUTION

GOTO NEXT PAGE

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

SOLUTION

Assume $23 = x_1^3 + \cdots + x_8^3$ where $x_1 \le \cdots \le x_8$.

Case 1 $x_8 \ge 3$. This cannot happen since $3^3 = 27 > 23$.

Case 2 $x_8 = 2$.

Case 2.1 $x_8 = x_7 = x_6 = 2$. Then $2^3+2^3+2^3 = 24 > 23$, so this cannot happen.

Case 2.2 $x_8 = 2$, $x_7 = 2$, $x_6 = x_5 = x_4 = x_3 = x_2 = x_1$. But then

$$2^3 + 2^3 + 6 \times 1^3 = 8 + 8 + 6 = 22.$$

So that does not work.

Case 2.3 $x_8 = 1$. Then all x_i are 1, so the sum is 8 which is < 23.

END OF SOLUTION

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 $a, b, c \in \mathsf{Z}$.

SOLUTION

Assume BWOC that $2^{1/3}$ satisfies a quadratic over Z. By the quadratic formula there exists $d, e, f \in \mathsf{Q}$ such that

$$2^{1/3} = d + ef^{1/2}$$

Cube both sides

$$2 = d^3 + 3d^2ef^{1/2} + 3de^2f + ef^{3/2}$$

There are rationals r, s, t such that

$$r = sf^{1/2} + tf^{3/2}$$

$$r = f^{1/2}(s + tf)$$

$$f^{1/2} = \frac{r}{s + tf}$$

So $f^{1/2}$ is rational.

Hence

$$2^{1/3} = d + ef^{1/2} \text{ is rational.}$$

END OF SOLUTION

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.

   SOLUTION

   We want to say there is a infinite set A which we think of as the first Z and a element z which we think of as (say) 0 in the second Z, so that everything in A is less than z.

   $(\exists A \subseteq L)(\exists z \in L)[$

   - $(\forall x \in L)[(x \in A \Rightarrow (\exists y)[x < y \wedge y \in A]]$
   - $(\forall x \in L)[(x \in A \Rightarrow x < z]$

   $]$

   END OF SOLUTION