Homework 4, MORALLY Due Feb 26

1. (30 points-15 points each)

   (a) Show that if $x \equiv 0 \pmod{21}$ and $y \equiv 0 \pmod{24}$ then $x + y \equiv 0 \pmod{3}$.

   (b) Make a conjecture and prove it of the form
   If $x \equiv 0 \pmod{m}$ and $y \equiv 0 \pmod{n}$ then $x+y \equiv 0 \pmod{BLANK}$

2. (30 points-10 points for the a,b,c and then 0 for d)

   (a) Compute the following MOD 23 and spot a pattern.

   $$7^0, 7^1, 7^2, \ldots$$

   The pattern should be of the form $7^n \equiv 7^{n+a} \equiv 7^{n+2a} \equiv \cdots \pmod{23}$. You need to find the a.

   Give us that pattern.

   (b) Use that pattern to compute $7^{1000} \pmod{23}$.

   (c) (In this problem we guide you through doing $7^{1000} \pmod{23}$ the way we did it in class.)

   IN THIS PROBLEM ALL CALCULATIONS ARE MOD 23.

      i. Write 1000 as a sum of powers of 2.

      ii. Fill in the following table:

      $7^{2^0} \equiv X$

      $7^{2^1} \equiv (7^{2^0})^2 \equiv X$

      $7^{2^2} \equiv (7^{2^1})^2 \equiv X$

      $\vdots$

      Until you get the last power of 2 that you need.

      iii. Use the last two parts to get $7^{1000} \pmod{23}$.

   (d) Did you prefer going this by looking for a pattern OR by the class method? Why?

3. Before we get to the problem I will tell two theorems with proofs and where we are going with this.

   Theorem 1 For all $a \in \mathsf{Z}$, $a^5 \equiv a \pmod 5$

   Proof: We do this with 5 cases depending on $a \pmod 5$.

   (a) $a \equiv 0 \pmod 5$. Need $0^5 \equiv 0 \pmod 5$ which is $0 \equiv 0 \pmod 5$, TRUE.

   (b) $a \equiv 1 \pmod 5$. Need $1^5 \equiv 1 \pmod 5$ which is $1 \equiv 1 \pmod 5$, TRUE.

   (c) $a \equiv 2 \pmod 5$. Need $2^5 \equiv 2 \pmod 5$ which is $32 \equiv 2 \pmod 5$, TRUE.

   (d) $a \equiv 3 \pmod 5$. Need $3^5 \equiv 3 \pmod 5$. I DO THIS by HAND WITH SHORTCUTS:

   $3 \times 3 \equiv 9 \equiv -1$. SO $(3 \times 3) \times (3 \times 3) \times 3 \equiv -1 \times -1 \times 3 \equiv 3$.

   so TRUE.

   (e) $a \equiv 4 \pmod 5$. Need $4^5 \equiv 4 \pmod 5$. I DO THIS BY HAND WITH SHORTCUTS

   $4 \equiv -1$. SO $(4{\times}4){\times}(4{\times}4){\times}4 \equiv 4 \equiv (-1{\times}-1){\times}(-1{\times}-1){\times}4 \equiv 4$.

   so TRUE.

   END OF PROOF

Next Page for Theorem 2

Theorem 2 There exists $a \in \mathsf{Z}$, $a^4 \not\equiv a \pmod 4$

Proof: We do this with by TRYING to prove the opposite and seeing where we fail.

(a) $a \equiv 0 \pmod 4$. Need $0^4 \equiv 0 \pmod 4$ which is $0 \equiv 0 \pmod 4$, TRUE.

(b) $a \equiv 1 \pmod 4$. Need $1^4 \equiv 1 \pmod 4$ which is $1 \equiv 1 \pmod 4$, TRUE.

(c) $a \equiv 2 \pmod 4$. Need $2^4 \equiv 2 \pmod 5$ which is $0 \equiv 2 \pmod 4$. STOP. THIS IS NOT TRUE.

So take $a = 2$ (or any number that is $\equiv 2 \pmod 4$) for the a in the Theorem.

End of Proof

Next Page for the Assignment

Here is our question:

For which m is it the case that $(\forall a \in \mathsf{Z})[a^m \equiv a \pmod{m}]$*?*

(a) (0 points but you will need it for the next part) Write a program that will, on input a, m, compute $a^m \pmod{m}$. (If Python has a library for exponentiation mod m, you should use it.)

(b) (0 points but you will need it for the next part) Write a program that will do the following: given $m \in \mathsf{N}$, $m \geq 2$, determine if

$$(\forall a \in \mathsf{Z})[a^m \equiv a \pmod{m}].$$

The basic idea of the program is to determine for $0 \leq a \leq m-1$ if you ALWAYS get

$$a^m \equiv a \pmod{m}.$$

If you do, then GREAT the statement is true. If NOT then there is a counterexample. The program should report TRUE or FALSE, and if FALSE then supply the counterexample.

Email all code to Emily (Ekaplitz@umd.edu). Just send the .py file with both programs in it. This will allow me to give partial credit if your code spits something out weird.

(c) (40 points) Produce a table of the following form; however, the table below only goes up to 4 and yours should go up to 200.

m	T or F	Counterexample if exists
2	T	
3	T	
4	F	$2^4 \not\equiv 2 \pmod{4}$
5	T	

(d) (0 points but you have to do it) Based on your data make a conjecture of the following form:

$$(\forall a \in \mathsf{Z})[a^m \equiv a \pmod{m}].$$

iff

BLANK(m)

You need to fill in the BLANK.