Homework 4, MORALLY Due Feb 23

NOTE: DUE MONDAY FEB 23 IN RECITATION. IF YOUR CAT DIES THEN WED FEB 25 IN RECITATION.

1. (0 points but you have to answer) What is your name? Write it clearly. Staple your HW.

2. (30 points) Find a set X such that the following is true (and prove it).

   - $X \subseteq \{0, 1, 2, 3, 4, 5, 6, 7\}$
   - For all $n \in \mathsf{N}$, there exists $a \in X$ such that $n^2 \equiv a \pmod 8$.
   - For all $a \in X$, there exists $n \in \mathsf{N}$ such that $n^2 \equiv a \pmod 8$.

   SOLUTION TO PROBLEM 2

   In this problem all $\equiv$ are $\pmod 8$.

   Lets just compute all of those squares:

   $0^2 \equiv 0$

   $1^2 \equiv 1$

   $2^2 \equiv 4$

   $3^2 \equiv 9 \equiv 1$

   $4^2 \equiv 16 \equiv 0$

   $5^2 \equiv 25 \equiv 1$

   $6^2 \equiv 36 \equiv 4$

   $7^2 \equiv 49 \equiv 1$

   So $X = \{0, 1, 4\}$.

   Why does this work: Note that for ANY n there exists $a \in \{0, 1, 2, 3, 4, 5, 6, 7\}$ such that $n \equiv a \pmod 8$

   So

   $n^2 \equiv a^2 \pmod 8$

   And from the above we know that for $a \in \{0, 1, 2, 3, 4, 5, 6, 7\}$ $a^2 \pmod 8 \in \{0, 1, 4\}$.

   (NOTE- In case you didn't see it, here is a proof that $x \equiv y \pmod n$ implies $x^2 \equiv y^2 \mod n$

$x \equiv y \pmod{n}$ Hence there exists q_1, q_2, r such that

$x = q_1 n + r$ and $y = q_2 n + r$ and $r \in \{0, \ldots, n-1\}$.

Hence

$x^2 \equiv q_1 n^2 + 2rq_1 n + r^2 \equiv r^2 \pmod{n}$

$y^2 \equiv q_2 n^2 + 2rq_2 n + r^2 \equiv r^2 \pmod{n}$

Since both x^2 and y^2 are equiv to r^2, they are equiv to each other.)

END OF SOLUTION TO PROBLEM 2

3. (30 points) Show that if $n \equiv 7 \pmod{8}$ then n CANNOT be written as the sum of three squares. (HINT: use the last problem.)

   SOLUTION TO PROBLEM 3

   In this problem $\equiv$ is $\equiv \pmod{8}$.

   Assume that $n \equiv 7$ and $n = x^2 + y^2 + z^2$. Take this equation mod 8 to get

   $7 \equiv x^2 + y^2 + z^2$.

   By the prior problem x^2, y^2, z^2 are all $\equiv$ something in $\{0, 1, 4\}$. Let $a \equiv x^2$, $b \equiv y^2$, $c \equiv z^2$. Hence

   $7 \equiv a + b + c$ where $a, b, c \in \{0, 1, 4\}$.

   We show that this cannot be by a few cases.

   (a) None of a, b, c is 4. Then $0 + 0 + 0 \le a + b + c \le 1 + 1 + 1 = 3$ Hence $a + b + c \not\equiv 7$.

   (b) Exactly One of a, b, c is 4. We assume $a = 4$ and $b, c \in \{0, 1\}$. Then we have $4 + b + c \equiv 7$, so $b + c \equiv 3$. Since $b, c \in \{0, 1\}$ we have $0 = 0 + 0 \le b + c \le 1 + 1 = 2$. Hence $b + c \not\equiv 3$.

   (c) Exactly two of a, b, c are 4. We assume $a = b = 4$ and $c \in \{0, 1\}$. Then $a + b + c \equiv 4 + 4 + c \equiv 1 + c$. So $c + 1 \equiv 7$ so $c \equiv 6$. But we know that $c \not\equiv 6$.

   (d) All three of a, b, c are 4. Then $a + b + c \equiv 4 + 4 + 4 \equiv 12 \equiv 5 \not\equiv 7$.

   END OF SOLUTION TO PROBLEM 3

4. (20 points) Compute the following the smart way. Show all work and do not use a calculator.

(a) $3^{100000000000000} \pmod{7}$

(b) $7^{100000000000000} \pmod{13}$

SOLUTION TO PROBLEM FOUR.a

Recall that in general $a^n \equiv a^{n \pmod{p-1}} \pmod{p}$. Hence in particular $3^{100000000000000} \equiv 3^{100000000000000 \pmod{6}} \pmod{7}$.

We could divide 100000000000000 by 6 and see what the remainder is. Instead we make our calculations easier by seeing what the remainder is mod 2 and mod 3.

$100000000000000 \equiv 0 \pmod{2}$ and $100000000000000 \equiv 1 \pmod{3}$ (a number is congruent to the sum of its digits mod 3).

Why does this help us? Note that every number is either of the form

$6k$: So $\equiv 0 \mod 2$ and $\equiv 0 \pmod{3}$.

$6k + 1$: so $\equiv 1 \pmod{2}$ and $\equiv 1 \pmod{3}$.

$6k + 2$: so $\equiv 0 \pmod{2}$ and $\equiv 2 \pmod{3}$.

$6k + 3$: so $\equiv 1 \pmod{2}$ and $\equiv 0 \pmod{3}$.

$6k + 4$: so $\equiv 0 \pmod{2}$ and $\equiv 1 \pmod{3}$.

$6k + 5$: so $\equiv 1 \pmod{2}$ and $\equiv 2 \pmod{3}$.

The only one that works for us is $6k + 4$ which is $\equiv 4 \pmod{6}$.

So what number in $\{0, 1, 2, 3, 4, 5\}$ is $\equiv 0 \pmod{2}$ and $\equiv 1 \pmod{3}$. There is only one such number, 4. so $3^{100000000000000} \equiv 3^{100000000000000 \pmod{6}} \equiv 3^4 \pmod{7}$.

So we need to computer 3^4.

$3^0 \equiv 1 \pmod{7}$

$3^1 \equiv 3 \pmod{7}$

$3^2 \equiv 9 \equiv 2 \pmod{7}$.

$3^4 \equiv (3^2)^2 \equiv 2^2 \equiv 4 \pmod{7}$.

So the answer is 4. (NOTE- the fact that $3^4 \equiv 4 \pmod{7}$ is an accident, this is not some general theorem.)

WE LEAVE FOUR.b to the reader, but it is similar.

END OF SOLUTION TO PROBLEM FOUR

5. (20 points) You learned that for p *prime* $a^p \equiv a \pmod{p}$. In this problem we will try to find what happens for non-primes.

   (a) Find a number L such that for all $a \in \{0, 1, 2, 3\}$, $a^L \equiv a \pmod{4}$.

   SOLUTION TO PROBLEM 5.

   For all L, $0^L \equiv 0$ and $1^L \equiv 1$ so we just need to look at 2 and 3.

   $2^0 \equiv 1$

   $2^1 \equiv 2$ OH, that works.

   Same with 3^1.

   so $2^1 \equiv 2$ and $3^1 \equiv 3$.

   So take $L = 1$.

   ONLY $L = 1$ works since $2^L \equiv 0$ for $L \geq 2$.

   (b) Find a number L such that for all $a \in \{0, 1, 2, 3, 4, 5\}$, $a^L \equiv a \pmod{6}$.

   We know that $L = 1$ will work. Will any other L work. We know that for all L $0^L \equiv 0$ and $1^L \equiv 1$ so we start at 2 and ignore the $L = 1$ case.

   $2^2 \equiv 4 \not\equiv 2$

   $2^3 \equiv 8 \equiv 2$. So $L = 3$ works for 2.

   Lets see if $L = 3$ works for everything else.

   $3^3 \equiv 27 \equiv 3$ YES!

   $4^3 \equiv 16 \times 4 \equiv 4 \times 4 \equiv 16 \equiv 4$ YES!

   $5^3 \equiv 25 \times 5 \equiv 1 \times 5 \equiv 5$ YES!

   So $L = 3$ works.

   (c) (Optional) Make a conjecture about, for n NOT prime, what is the L such that $a^L \equiv a \pmod{n}$.

   One answer is $L = 1$, but is there another one?

   Note that we have

   For $a = 4$ we get $L = 1$

   For $a = 5$ we get $L = 5$ (note that 5 is prime so we are using $a^p \equiv a$)

   For $a = 6$ we get $L = 3$

   For $n = 7$ we get $L = 7$.

   NOT a smooth pattern.

If curious look up Euler's theorem which is what I originally intended but, as you will see, doesn't quite work out given what I've told you.