Midterm #5:

Prove $42 \mid n^7 - n$ for all n.

Note: $42 = 2 \cdot 3 \cdot 7$ so it's enough to show that $2, 3, 7 \mid n^7 - n$.

i.e. Show

$n^7 \equiv n \mod 2$ $\quad 0^7 \equiv 0 \quad 1^7 \equiv 1$

$n^7 \equiv n \mod 3$ $\quad (-1)^7 \equiv -1$

$n^7 \equiv n \mod 7$ $\quad -3, -2, -1, 0, 1, 2, 3$

$2^7 \equiv 2 \mod 7$

$3^7 \equiv 3 \mod 7$ easy to check

Goal: How to find k s.t.

$a^k \equiv 1 \mod n$?

For today, will focus on when

$n = p$ is prime.

As an aside: a CRT example:
CRT is algorithmic. Don't memorize formulas!!

$$\begin{cases} x \equiv 5 \bmod 7 \\ x \equiv 7 \bmod 11 \\ x \equiv 3 \bmod 13 \end{cases} \Rightarrow x \equiv 40 \bmod 77$$

Solve System pair wise:

$x = 5 + 7k$

$\Rightarrow 5 + 7k \equiv 7 \bmod 11$

$7k \equiv 2 \bmod 11$

$\Rightarrow k \equiv 2 \cdot 8 \equiv 5 \bmod 11$

$k = 5 + 11\ell$

$$x = 5 + 7(5 + 11l) = 40 + 77l$$

$$40 + 77l \equiv 3 \mod 13$$

$$1 - l \equiv 3 \mod 13$$

$$l \equiv -2 \equiv 11 \mod 13$$

$$l = 11 + 13m$$

$$x = 40 + 77 \cdot (11 + 13m)$$

$$= 887 + 1001m$$

i.e.

$$x \equiv 887 \mod 1001$$

Solves the System of congruences

Orders

Def: For an integer a w/ $\gcd(a,n)=1$ the **order of a mod n** $\operatorname{ord}_n(a)$ is the smallest positive integer k s.t. $a^k \equiv 1 \bmod n$.

Ex: $7^4 \equiv 1 \bmod 100$ and 4 is the smallest integer w/ this property.

So $\operatorname{ord}_{100}(7) = 4$.

Prop: $a^k \equiv 1 \bmod n \iff$

$\operatorname{ord}_n(a) \mid k.$

Proof: $\Leftarrow$ if $\operatorname{ord}_n(a) \mid k$

$k = \operatorname{ord}_n(a) \cdot \ell$ for some ℓ.

$$a^k = a^{\operatorname{ord}_n(a) \cdot \ell} = \left(a^{\operatorname{ord}_n(a)}\right)^{\ell}$$

$$\equiv 1^{\ell} \bmod n$$

$$\equiv 1 \bmod n.$$

$\Rightarrow$ Suppose $a^k \equiv 1 \bmod n$.

By div. algorithm,

$k = \text{ord}_n(a) \cdot q + r \qquad 0 \leq r < \text{ord}_n(a)$

for some q, r.

$$a^k = a^{\text{ord}_n(a) \cdot q + r} = \left(a^{\text{ord}_n(a)}\right)^q \cdot a^r$$

$$1 \equiv a^r \mod n$$

B/C $0 \leq r < \text{ord}_n(a)$ and

$\text{ord}_n(a)$ is the smallest

positive integer w/ this prop

$\Rightarrow \quad r = 0.$

$\Rightarrow \quad k = \text{ord}_n(a) \cdot q$

$\Rightarrow \quad \text{ord}_n(a) \mid k$ ☒

Thm: (Fermat's Little Theorem)

Let p be prime. For any a s.t. $\gcd(a,p) = 1$ we have

$$a^{p-1} \equiv 1 \bmod p$$

Cor: $\operatorname{ord}_p(a) \mid p-1$.

Proof: Lecture tomorrow (?)

Ex: Compute $100^{101^{102}} \bmod 13$

Soln: By Fermat's little thm,

$$100^{12} \equiv 9^{12} \equiv 1 \mod 13.$$

So need to compute $101^{102} \mod 12$.

$$101^{102} \equiv 5^{102} \mod 12$$

Note that $5^4 \equiv 1 \mod 12$

$$5^{102} \equiv 5^2 \equiv 1 \mod 12$$

$$9^{101^{102}} \equiv 9^{12 \cdot l + 1} \equiv 9 \mod 13.$$

Ex: For which values of k is $2^{2^k} \equiv 1 \bmod 23$?

Soln:

$2^{2^k} \equiv 1 \bmod 23 \Rightarrow$

$\operatorname{ord}_{23}(2) \mid 2^k$. How to Compute $\operatorname{ord}_{23}(2)$?

By Fermat's little theorem,

$2^{22} \equiv 1 \bmod 23$.

So $\operatorname{ord}_{23}(2) \mid 22$.

So $\operatorname{ord}_{23}(2) = 1, 2, 11, 22.$

Checking manually, we find

$$2^{11} \equiv 1 \bmod 22,$$ so

$$\operatorname{ord}_{23}(2) = 11.$$

There is no k s.t. $11 \mid 2^k$

So no values of k work.

Ex: Find a s.t.

$$a^{37} \equiv 102^{70} + 1 \bmod 113$$

Soln:

By Fermat's little thm,

$$a^{112} \equiv 1 \mod 113$$

$$a^{111} \cdot a \equiv 1 \mod 113$$

$$a^{111} \equiv a^{-1} \mod 113$$

Note that $37 \cdot 3 \equiv 111$

$\Rightarrow$

$$a^{-1} \equiv a^{111} \equiv (10^{70}+1)^3 \mod 113$$

Let's compute

$$102^{70} + 1 \mod 113$$

$$\equiv (-11)^{70} + 1 \mod 113$$

$$\equiv 11^{70} + 1 \mod 113$$

Since $11^{112} \equiv 1 \mod 113$

$$\text{ord}_{113}(11) \mid 112$$

$$\text{Ord}_{113}(11) = 1, 2, 4, 7, 8, 14, 16, 28, 56, 112.$$

Turns out

$\operatorname{ord}_{113}(11) = 56.$

$11^{70} + 1 \equiv 11^{14} + 1 \mod 113$

$\equiv 99 \mod 113$

$a^{-1} \equiv 99^3 \equiv 81 \mod 113$

to find a, find the

inverse of $81 \mod 113$.

i.e. Solve $81x \equiv 1 \mod 113.$

If you do this, you'll find

$a \equiv 60 \mod 113$.

Last rmk: Fermat's little thm makes midterm problem easy:

$n^{p-1} \equiv 1 \mod p$ for $n \not\equiv 0 \mod p$

So mult. by n says

$n^p \equiv n \mod p$. This also is true for

$n \equiv 0 \bmod p$, so for <u>any</u> n,

$n^p \equiv n \bmod p$ when p is prime.

Immediately get

$n^2 \equiv n \bmod 2 \Rightarrow n^7 \equiv n \bmod 2$

$n^3 \equiv n \bmod 3 \Rightarrow n^7 \equiv n \bmod 3$

$n^7 \equiv n \bmod 7$

$\Rightarrow \quad n^7 \equiv n \bmod 42.$