Mat 202 - Tutorial #8

1. [7.47] Let p be an odd prime. Prove that $2(p-3)! \equiv -1 \mod p$.

Recall: [Wilson's Theorem, Theorem 7.4.4] $(p-1)! \equiv -1 \mod p$ for p prime.
[In class you proved $(p-2)! \equiv 1 \mod p$].

$(p-1)! = (p-1)(p-2)(p-3)! = (p^2-3p+2)(p-3)!$

and $p^2-3p+2 \equiv 2 \mod p$.

So, $(p-1)! \equiv -1 \mod p \Leftrightarrow (p^2-3p+2)(p-3)! \equiv -1 \mod p$

$\Leftrightarrow 2(p-3)! \equiv -1 \mod p$.

2. [7.48] Prove the converse of Wilson's Theorem. i.e., Suppose that $p > 1$ and $(p-1)! \equiv -1 \mod p$. Prove that p is prime.

In order to derive a contradiction, suppose p is not prime. Then there must exist some integer $1 < a < p$ s.t. a divideds p (i.e., $ab = p$ for some $1 < b < p$).

Since $(p-1)!$ is the product of all integers b/w 1 and $p-1$, we must have that a is in this product $\Rightarrow$ a divides $(p-1)!$.

$(p-1)!+1 \equiv 0 \mod p \Rightarrow p$ divides $(p-1)!+1$
$\Rightarrow a$ divides $(p-1)!+1$.

But a divides $(p-1)!$ and $[(p-1)!+1] \Rightarrow a = 1$. ↯
∴ p must be prime. ■

3. [7.44] $\boxed{a}$ Prove that 341 is <u>not</u> prime.
$\boxed{b}$ Prove that 341 divides $a^{341} - a$.

$\boxed{a}$ If you had a calculator, you might find that $341 = 11 \cdot 31$. Otherwise, we could use Fermat's Little Theorem:

<u>Recall</u>: <u>Fermat's Little Theorem</u>: p prime and a <u>not</u> a multiple of $p \Rightarrow a^{p-1} \equiv 1 \bmod p$.

<u>Cor. [7.39]</u>: If p prime and $a \in \mathbb{Z} \Rightarrow a^p \equiv a \bmod p$.

<u>Contrapositive</u>: If $a^p \not\equiv a \bmod p \Rightarrow p$ <u>not</u> prime.

So, to show that 341 is <u>not</u> prime, it suffices to find an integer a s.t.

$$a^{341} \not\equiv a \bmod 341.$$

Obviously $a = 2$ won't work (judging by $\boxed{b}$).

Let's try $a = 3$:

$3^6 = 729.$

$$\begin{array}{r} 2(341) = \quad 682 \\ \hline 47 \end{array}$$

$$\begin{array}{r} 56 \\ 6\overline{)336} \\ \underline{30} \\ 36 \end{array}$$

$$3^{341} = (3^6)^{56} 3^5 = (729)^{56} (243) \equiv (47)^{56} (243)$$

⋮

things getting pretty ugly.

Can we find an a whose powers get closer to 341?

$3^2 = 9$

$3^3 = 27$

$$\begin{array}{r} 27 \\ 3 \\ \hline 81 \end{array} \qquad \begin{array}{r} 81 \\ 3 \\ \hline 243 \end{array} \qquad \begin{array}{r} 243 \\ 3 \\ \hline 3^6 = 729 \end{array}$$

$$\begin{array}{r} 341 \\ 2 \\ \hline 682 \end{array} \qquad \begin{array}{r} 729 \\ 682 \\ \hline 47 \end{array}$$

$$\begin{array}{r} 392 \\ 341 \\ \hline 51 \end{array}$$

<u>Try $a=7$:</u> (b/c $7^3 = 343 \equiv 2 \bmod 341$ is nice)

$$3\overline{)339}^{\,113}$$

$$7^{341} = (7^3)^{113} 7^2 \equiv (2)^{113} \cdot 49 \equiv (2^{10})^{11} \cdot 2^3 \cdot 49 \equiv 8 \cdot 49$$

$$\equiv 392 \equiv 51 \bmod 341 \not\equiv 7 \bmod 341$$

341
682
1023

$\Rightarrow$ 341 <u>not</u> prime.

$\boxed{b}$ WTS $2^{341} \equiv 2 \bmod 341$.

$2^{10} = 1024$
$\equiv 1023+1$
$\equiv 1 \bmod 341$.

$$2^{341} = (2^{10})^{34} 2 \equiv (1)^{34} \cdot 2 \equiv 2 \bmod 341.$$

$$\begin{array}{r} 49 \\ 8 \\ \hline 392 \end{array}$$

* Interesting b/c Fermat conjectured that $2^p \equiv 2 \bmod p$ $\Leftrightarrow$ p prime. [obviously $\Leftarrow$ true by Fermat's Little theorem]. But Euler found this counter example for $p=341$ <u>not</u> prime, proving Fermat wrong. *

4. ⓐ Prove that every palindromic integer with an even [7.23] number of digits is divisible by 11. <u>Note</u>: An integer is called <u>palindromic</u> if the digits read the same when written forward or backward. <u>e.g.</u>, 1221, 3443.

Let's denote our integer by:

$$a_0 a_1 \cdots a_n a_n \cdots a_1 a_0 = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n + a_n 10^{n+1} + \cdots + a_1 10^{2n} + a_0 10^{2n+1}$$

$10 \equiv -1 \bmod 11$ $$\equiv a_0 \cancel{(-1)}a_1 + a_2 \cancel{(-1)^2} + \cdots + a_n \cancel{(-1)^n} + a_n \cancel{(-1)^{n+1}} + \cdots + a_1 \cancel{(-1)^{2n}} + a_0 \cancel{(-1)^{2n+1}}$$

$\equiv 0 \bmod 11$. $\therefore$ 11 divides even-digit palindromic integers.

$\boxed{b}$ Prove that every integer whose base K representation is palindromic and has even length is divisible by K+1.

[In $\boxed{a}$ we had $K=10$].

Basically the same argument:

Let's denote our integer by:

$K \equiv -1 \mod (K+1)$ $\quad a_0 + a_1 K + a_2 K^2 + \dots + a_n K^n + a_n K^{n+1} + \dots + a_1 K^{2n} + a_0 K^{2n+1}$

$\equiv a_0 + a_1(-1) + a_2(-1)^2 + \dots + a_n(-1)^n + a_n(-1)^{n+1} + \dots + a_1(-1)^{2n} + a_0(-1)^{2n+1}$

$\equiv 0 \mod (K+1)$.

e.g.) 190 written in base 4 is palindromic:

$\underline{2} + \underline{3} \cdot 4 + \underline{3} \cdot 4^2 + \underline{2} \cdot 4^3 = 2 + 12 + 3 \cdot 16 + 2 \cdot 64 = 190$, so

base 4 it is written as 2332, and

$190 \mod 5 \equiv 0$.

Comment About A5:

$\boxed{1}$ $K^n \not\equiv K \mod n$ in general! e.g.) Above we showed $7^{341} \not\equiv 7 \mod 341$.

$\boxed{2}$ Be careful when you write arguments! Write a coherent argument! e.g.) If I WTS 4 consecutive natural #'s can't end in 116, then saying:

$\left.\begin{array}{l}\text{" 4 consecutive \#'s have 2 evens"} \\ \text{" 116 \underline{not} divisible by 8."}\end{array}\right\}$ is ~~not~~ an argument!