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

Recall: [Wilson's Theorem, Theorem 7.4.4] $(p-1)! \equiv -1 \mod p$ for $p$ prime.
[In class you proved $(p-3)! \equiv 1 \mod p$].

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

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

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

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

2. [7.48] Prove the converse of Wilson's Theorem. i.e. Suppose that $p \nmid 1$ 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 $1 \leq a < p$ s.t. $a$ divides $p$ (i.e., $a \cdot b = p$ 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 $\equiv a$ divides $(p-1)!$.

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

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

But $a$ divides $(p-1)!$ and $(p-1)! + 1 \equiv a = 1$.

$\therefore p$ must be prime.
3. [7.44] a) Prove that 341 is not prime.
   b) Prove that 341 divides $a^{341} - 1$.

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

   Recall: Fermat's Little Theorem: $p$ prime and $a \neq 0$ a multiple of $p \Rightarrow a^{p-1} \equiv 1 \mod p$.

   Cor. [7.39]: If $p$ prime and $a \in \mathbb{Z}$ then $a^{p-1} \equiv 1 \mod p$.

   Contrapositive: If $a^p \not\equiv 1 \mod p \Rightarrow p$ not prime.

   So, to show that 341 is not prime, it suffices to find an integer $a$ s.t.

   $341 \mid a^3 - a \mod 341$.

   Obviously $a=2$ won't work (judging by b).

   Let's try $a=3$:

   $3^1 = 9$
   $3^3 = 27$
   $3^5 = 67,291$
   $3^7 = 613,367$
   $3^{341} = 68,841$
   $3^{341} \equiv 56 \mod 341$

   $3_4 = 3$.

   Things getting pretty ugly.

   Can we find an $a$ whose powers get closer to 341?
Try \( a = 7 \): \( \frac{7^3}{341} = 343 \equiv 2 \mod 341 \). Nice.

\[
7 = (7^3)^{1/3} = (a^{113})^{1/3} = (2^{113})^{1/3} = 49 \equiv 8 \cdot 49 = 8 \mod 341
\]

\[
\equiv 342 \cdot 51 \mod 341 \equiv 7 \mod 341
\]

682 \equiv 341 \not\equiv \text{prime}.

1023

**WTS** \( 2 \equiv 2 \mod 341 \).

\[2 = 1024 \equiv 1 \cdot 341 \equiv (2^{10})^{341} \]

\[2 = (2^{10})^{341} \equiv (1)^{341} \cdot 2 \equiv 2 \mod 341.
\]

**Interesting** because Fermat conjectured that \( a^p \equiv a \mod p \) for \( p \) prime. [Obviously false by Fermat's Little Theorem. But Euler found this counter example for \( p = 341 \) not prime, proving Fermat wrong.]

* 4. Prove that every palindromic integer with an even number of digits is divisible by 11. Note: An integer is called palindromic if the digits read the same when written forward or backward, e.g., 12321, 3443.

Let's denote our integer by:

\[
a_0 a_1 \cdots a_n a_{n-1} \cdots a_1 a_0 = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0
\]

\[
10 \equiv -1 \mod 11 = a_0 (10^1) + a_2 (10^2) + \cdots + a_{n-1} (10^{n-1}) + a_n (10^n)
\]

\[
\equiv 0 \mod 11. \therefore 11 \divides \text{even-digit palindromic integers.}
\]
b) Prove that every integer whose base $K$ representation is palindromic and has even length is divisible by $K+1$.

[In 9 we had $K=10$].

Basically the same argument:

Let's denote an integer by:

$$K=-1 \mod (K+1) \quad a_0 + a_1 K + a_2 K^2 + \ldots + a_n K^n + a_{n+1} K^{n+1}$$

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

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

E.g. 190 written in base 4 is palindromic:

$$2 + 3 \cdot 4 + 3 \cdot 4^2 + 2 \cdot 4^3 = 2 + 12 + 3 \cdot 16 + 2 \cdot 64 = 190,$$

so base 4, it is written as 2332, and

$$190 \mod 5 = 0.$$

Comment about A5:

1. $K^n \equiv K \mod n$ in general? e.g. 7 Above we showed $7^{341} \equiv 7 \mod 341$.

2. Be careful when you write arguments! Write a coherent argument! E.g. 7 If I WTS 4 consecutive natural #s can't end in 116, then saying:

"4 consecutive #s have 2 evens" $\exists$ is not an argument!"116 not divisible by 8."