Name: Solutions

Directions: Show all work. No credit for answers without work.

1. **[2 points]** Give the definition of the order of an element a in $\mathbb{F}_p$.

The order of a in $\mathbb{F}_p$ is the least positive integer k such that $a^k = 1$.

2. **[2 points]** Find the order of 5 in $\mathbb{F}_{11}$.

We compute powers of 5:

k	1	2	3	4	5
5^k	5	3	4	9	(1)

Therefore the order of 5 in $\mathbb{F}_{11}$ is $\boxed{5}$.

3. **[2 points]** List out all the possibilities for the order of an element in $\mathbb{F}_{13}$.

The order divides $p-1$, or 12. Therefore the possible orders are $\boxed{1, 2, 3, 4, 6, \text{ and } 12.}$

4. **[2 parts, 1 point each]** Suppose you wish to check whether 2 is a primitive root in $\mathbb{F}_{151}$.

(a) Which modular exponentiation computations would you need to perform? Use as few computations as possible. (Do not actually perform the computations.)

- $p-1 = 150 = 2 \cdot 3 \cdot 5^2$
- Need to compute $2^{150/2}$, $2^{150/3}$, and $2^{150/5}$ or

$$\boxed{2^{30},\ 2^{50},\ \text{and } 2^{75}}$$

(b) Describe how you would interpret the results of your computations in part (a) to determine whether 2 is a primitive root in $\mathbb{F}_{151}$.

If any of these powers of 2 equals 1, then 2 is <u>not</u> a primitive root.

If all of these powers of 2 are not equal to 1, then 2 is a primitive root.

5. **[2 points]** Given that 7 is a primitive root of $\mathbb{F}_{71}$, find three more primitive roots of $\mathbb{F}_{71}$.

- 7^k is a primitive root $\iff \gcd(k, p-1) = 1$
  $\iff \gcd(k, 70) = 1$.
- $70 = 2 \cdot 5 \cdot 7$
- Smallest k with $\gcd(k, 70) = 1$: 3, 9, 11.
- $7^3 = 59$; $7^9 = (7^3)^3 = (59)^3 = 47$; $7^{11} = 7^9 \cdot 7^2 = (47) \cdot (49) = 31$.
- So, other primitive roots are: $\boxed{59, 47, \text{ and } 31.}$ Other answers possible.