Name: Solutions

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

1. [**10 points**] Find a primitive root modulo 7. Show work that verifies your selection is a primitive root.

$a \backslash n$	0	1	2	3	4	5	6	order
2	1	2	4	1				3 ×
3	1	3	2	6	4	5	1	6 ✓

Since 3 has order 6,

$\boxed{3}$ is a primitive root.

(The other primitive root is 5.)

2. [**5 points**] Let m and n be large integers. Suppose that $2^{m-1} \equiv 1 \pmod{m}$ and $2^{n-1} \equiv 4 \pmod{n}$. What, if anything, can you conclude about whether m and/or n is prime, and why?

By Fermat's Little Theorem, if p is prime and $p > 2$, then $2^{p-1} \equiv 1 \pmod{p}$.

Since $2^{n-1} \equiv 4 \pmod{n}$ and $4 \not\equiv 1 \pmod{n}$ when n is large, we conclude that $\boxed{n \text{ is not prime.}}$

Although $2^{m-1} \equiv 1 \pmod{m}$ is consistent with m being prime, we reach $\boxed{\text{no conclusion about whether } m \text{ is prime or not.}}$

3. [**3 parts, 4 points each**] Short Answer (no need to show work on this problem). Let p be an odd prime and let g be a primitive root in $\mathbb{F}_p$.

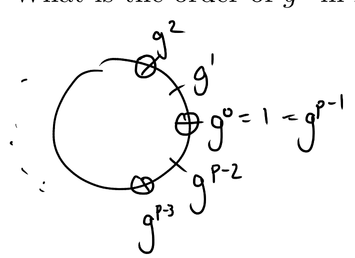
(a) How many primitive roots are there in $\mathbb{F}_p$?

$\boxed{\phi(p-1)}$

(b) What is the order of g in $\mathbb{F}_p$?

Since g is a primitive root, g has order $\boxed{p-1}$.

(c) What is the order of g^2 in $\mathbb{F}_p$?



The order of g^2 is $\boxed{\frac{p-1}{2}}$

4. Alice and Bob use the multiplication symmetric cipher with prime $p = 421$ and $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathbb{F}_p^*$. Recall that the encryption function is given by $e_k(m) = km$. They choose the key $k = 182$.

   (a) [**5 points**] Alice wishes to send the message $m = 282$ to Bob. What is the corresponding cipher text?

   $$e_k(282) = k \cdot 282 = (182)(282) = 51{,}324 \equiv \boxed{383} \pmod p$$

   (b) [**10 points**] Alice receives the ciphertext $c = 296$ in response. What is the corresponding plaintext message?

   We have $d_k(c) = k^{-1}c$. So $d_k(296) = k^{-1} \cdot (296) = (182)^{-1} \cdot (296)$.

   <u>Use EEA to find $(182)^{-1}$:</u>

   $421 = (2)(182) + 57$

   $182 = (3)(57) + 11$

   $57 = (5)(11) + 2$

   $11 = (5)(2) + 1$

   $$\begin{aligned} 1 &= 11 - (5)(2) \\ &= 11 - (5)[57 - (5)(11)] \\ &= (26)(11) - (5)(57) \\ &= (26)[182 - (3)(57)] - (5)(57) \\ &= (26)(182) - (83)(57) \\ &= (26)(182) - (83)[421 - (2)(182)] \\ &= (192)(182) - (83)(421) \end{aligned}$$

   $k^{-1} = (182)^{-1} = 192$

   So

   $$d_k(296) = (192) \cdot (296) = 56832 = \boxed{418}$$

   (c) [**5 points**] How many plaintext/ciphertext pairs does Eve need to compute the shared key? Explain.

   $\boxed{\text{Just 1.}}$ Given (m_1, c_1) with $c_1 = k m_1$, Eve finds k by computing both sides by m_1^{-1} to get $k = c_1 m_1^{-1}$.

5. [**5 points**] Alice and Bob switch to the Exclusive-OR cipher with key $k = 01100101$. Alice receives the ciphertext $c = 00101110$. What is the corresponding plaintext?

$$\begin{array}{rl} 01100101 & k \\ \oplus\ 00101110 & c \\ \hline \boxed{01001011} & m \end{array}$$

$e_k(m) = m \oplus k$

$d_k(c) = c \oplus k$

6. **[2 parts, 12 points each]** Alice and Bob use the ElGamal cipher, with $p = 59$ and $g = 11$.

   (a) Alice picks $a = 17$ as her private key and in $\mathbb{F}_p$ computes $A = g^a = (11)^{17} = 14$ as her public key. Bob wishes to send to Alice the message $m = 40$ and picks the random element 8. What does Bob send to Alice?

c_1: $c_1 = g^8 = (11)^8$.

$(11)^2 = 121 = 3$

$(11)^4 = 3^2 = 9$

$(11)^8 = 9^2 = 22$.

So $c_1 = (11)^8 = 22$.

c_2: $c_2 = m \cdot A^8 = 40 \cdot 49 = 1960 = 13$

Need A^8:

$A^2 = (14)^2 = 19$

$A^4 = (19)^2 = 7$

$A^8 = 7^2 = 49$.

Bob sends $(c_1, c_2) = \boxed{(22, 13)}$ to Alice.

   (b) Bob sends a second encrypted message to Alice with ciphertext $(c_1, c_2) = (39, 5)$. Help Alice decrypt Bob's message.

We have $c_1 = g^b$ and $c_2 = m \cdot g^{ab}$.

Alice needs $g^{ab} = (g^b)^a = c_1^a = (39)^{17}$.

$39^2 = 46$

$(39)^4 = (46)^2 = 51$

$(39)^8 = (51)^2 = 5$

$(39)^{16} = 5^2 = 25$

$(39)^{17} = (39)^{16} \cdot (39) = 25 \cdot 39$

$= 31$.

So $g^{ab} = 31$. We need $(31)^{-1}$:

$59 = (1)(31) + 28$

$31 = (1)(28) + 3$

$28 = (9)(3) + 1$

$1 = 28 - (9)(3)$

$= 28 - (9)(31 - (1)(28))$

$= (10)(28) - (9)(31)$

$= (10)[59 - (1)(31)] - (9)(31)$

$= (10)(59) - (19)(31)$

So $(31)^{-1} = -19$.

$5 = m \cdot 31$

$(-19) \cdot 5 = m \cdot (31)(-19)$

$m = (-19) \cdot 5 = -95 = -95 + 2(59)$

$= -95 + 118 = \boxed{23}$

7. Let $p = 179$ and let $g = 3$. We use Shanks's baby-step/giant-step algorithm to compute $\log_g(4)$ in $\mathbb{F}_p$. Note that g has order 89 in $\mathbb{F}_p$, and we may take $n = 1 + \lfloor\sqrt{89}\rfloor = 10$.

(a) [~~8~~ 8 **points**] Compute List 1 (the baby-steps).

i	0	1	2	3	4	5	6	7	8	9
g^i	1	3	9	27	81	64	13	39	117	172

(b) [**12 points**] Compute List 2 (the giant-steps).

j	0	1	2	3	4	5	6	7	8	9
hg^{-jn}	4	68	82	141	70	116	3	51	151	61

$4\cdot 17$ $\quad$ $68\cdot 17$

Need $g^{-1} = (3)^{-1}$.

$179 = (59)(3) + 2$

$3 = (1)(2) + 1$

$1 = 3 - (1)(2)$

$= 3 - (1)[179 - (59)(3)]$

$= (60)(3) - (1)(179)$

So $g^{-1} = 60$.

Need $(g^{-1})^n = (60)^{10}$

$(60)^2 = 20$

$(60)^4 = (20)^2 = 42$

$(60)^8 = (42)^2 = 153$

$g^{-n} = (60)^{10} = (60)^8 \cdot (60)^2$

$= 153 \cdot 20$

$= 17$

giant "stride"

(c) [**4 points**] If it exists, find $\log_g(4)$.

we have $g^1 = 3 = h \cdot g^{-6\cdot n}$

so $g^{6n+1} = h = 4$

so $\log_g(4) = 6n + 1 = 6\cdot 10 + 1 = \boxed{61}$