1a. Factors of 78: 1, 2, 3, 6, 13, 26, 39, 78
Only the orders that are factors of 78 (listed above) have elements. The other order numbers have no elements. For example, 4 and 5 have zero elements!
I counted up the reoccurring orders in part b to find the following:

Order	Elements
1	1
2	1
3	2
6	2
13	12
26	12
39	24
78	24

1b.
I generated an excel sheet named CS4801_HW4Prob1 to see the full list of numbers to find the following:

Elements	Order
1	1
2	39
3	78
4	39
5	39
6	78
7	78
8	13
9	39
10	13
11	39
12	26
13	39
14	26
15	26
16	39
17	26
18	13
19	39
20	39
21	13
22	13
23	3
24	6

25	39
26	39
27	26
28	78
29	78
30	78
31	39
32	39
33	26
34	78
35	78
36	39
37	78
38	13
39	78
40	39
41	26
42	39
43	78
44	39
45	39
46	13
47	78
48	78
49	39
50	39
51	39
52	13
53	78
54	78
55	3
56	6
57	26
58	26
59	78
60	78
61	26
62	13
63	78
64	13
65	13
66	78

67	13
68	78
69	26
70	78
71	26
72	39
73	39
74	78
75	78
76	39
77	78
78	2

1c. Should be 24 generators: 3, 6, 7, 28, 29, 30, 34, 35, 37, 39, 43, 47, 48, 53, 54, 59, 60, 63, 66, 68, 70, 74, 75, 77
See excel sheet named CS4801_HW4Prob1 that I generated to see the full list of numbers and how I calculated them.

1d.

Element	Power of 7
1	7
2	49
3	27
4	31
5	59
6	18
7	47
8	13
9	12
10	5
11	35
12	8
13	56
14	76
15	58
16	11
17	77
18	65
19	60
20	25
21	17

22	40
23	43
24	64
25	53
26	55
27	69
28	9
29	63
30	46
31	6
32	42
33	57
34	4
35	28
36	38
37	29
38	45
39	78
40	72
41	30
42	52
43	48
44	20
45	61
46	32
47	66
48	67
49	74
50	44
51	71
52	23
53	3
54	21
55	68
56	2
57	14
58	19
59	54
60	62

61	39
62	36
63	15
64	26
65	24
66	10
67	70
68	16
69	33
70	73
71	37
72	22
73	75
74	51
75	41
76	50
77	34
78	1

#2 and #3 ARE ON THE NEXT PAGE...

2.

2 a) $15 = 2^x \bmod 59$ ($\log_2 15 \bmod 59$)

$q = 59-1 = 58$ $p = 59$ $\alpha = 2$

1. $t = \sqrt{58} = 7$

2. for $k=0$ to $\lceil \frac{q}{t} \rceil = \lceil \frac{58}{7} \rceil = 8$

$k=0$ $f_0 = 2^{0\cdot7} = \boxed{1} \bmod 59$

$k=1$ $f_1 = 2^{1\cdot7} = 10 \bmod 59$

$k=2$ $f_2 = 2^{2\cdot7} = 41 \bmod 59$

$k=3$ $f_3 = 2^{3\cdot7} = 56 \bmod 59$

$k=4$ $f_4 = 2^{4\cdot7} = 29 \bmod 59$

$k=5$ $f_5 = 2^{5\cdot7} = 54 \bmod 59$

$k=6$ $f_6 = 2^{6\cdot7} = 9 \bmod 59$

$k=7$ $f_7 = 2^{7\cdot7} = 31 \bmod 59$

$k=8$ f_8 $2^{8\cdot7} = \boxed{15} \bmod 59$

3. $i=0$ to 7

$i=0$ $15\cdot2^0 \bmod 59$ x

$i=1$ $15\cdot2^1 \bmod 59$ x

$i=2$ $15\cdot2^2 \bmod 59 = 1 \bmod 59$ ✓

$h\cdot2^2 = 2^0$ $h = 2^{56}$ $x = \log_2 2^{56}$ $\boxed{x = 56}$

b) $23 = 11^x \bmod 79$ ($\log_{11} 23 \bmod 79$)

$q = 79-1 = 78$ $p = 79$ $\alpha = 11$

1. $t = \sqrt{78} = 8$

2. for $k=0$ to $\lceil \frac{78}{8} \rceil = 9$

$k=0$ $f_0 = 11^{0\cdot8} = 1 \bmod 79$

$k=1$ $f_1 = 11^{1\cdot8} = 44 \bmod 79$

$k=2$ $f_2 = 11^{2\cdot8} = 40 \bmod 79$

$k=3$ $f_3 = 11^{3\cdot8} = 22 \bmod 79$

$k=4$ $f_4 = 11^{4\cdot8} = 20 \bmod 79$

$k=5$ $f_5 = 11^{5\cdot8} = 11 \bmod 79$

$k=6$ $f_6 = 11^{6\cdot8} = 10 \bmod 79$

$k=7$ $f_7 = 11^{7\cdot8} = 45 \bmod 79$

$k=8$ $f_8 = 11^{8\cdot8} = 5 \bmod 79$

$k=9$ $f_9 = 11^{9\cdot8} = 62 \bmod 79$

3. $i = 0$ to 8

$i=0$ $23 \cdot 11^0 \bmod 79$ ×

$i=1$ $23 \cdot 11^1 \bmod 79 = 16 \bmod 79$ ×

$i=2$ $23 \cdot 11^2 \bmod 79 = 18 \bmod 79$ ×

$i=3$ $23 \cdot 11^3 \bmod 79 = 40 \bmod 79$ ✓

$h \cdot 11^3 = 11^{16}$ $h = 11^{13}$ $x = \log_{11} 11^{13}$ $\boxed{x = 13}$

c) $7 = 11^x \bmod 79$ ($\log_{11} 7 \bmod 79$)

$q = 79 - 1 = 78$ $p = 79$ $\alpha = 11$

1. $t = \sqrt{78} = 8$

2. for $k = 0$ to $\lceil \frac{78}{8} \rceil = 9$

Can use the same f_k values as part (b) since the base(11), modulus(79), t, and k iteration values are the same

3. $i = 0$ to 8

$i=0$ $7 \cdot 11^0 \bmod 79$ ×

$i=1$ $7 \cdot 11^1 \bmod 79$ ×

$i=2$ $7 \cdot 11^2 \bmod 79 = 57 \bmod 79$ ×

$i=3$ $7 \cdot 11^3 \bmod 79 = 74 \bmod 79$ ×

$i=4$ $7 \cdot 11^4 \bmod 79 = 24 \bmod 79$ ×

$i=5$ $7 \cdot 11^5 \bmod 79 = 27 \bmod 79$ ×

$i=6$ $7 \cdot 11^6 \bmod 79 = 60 \bmod 79$ ×

$i=7$ $7 \cdot 11^7 \bmod 79 = 28 \bmod 79$ ×

$i=8$ $7 \cdot 11^8 \bmod 79 = 71 \bmod 79$ ×

→ 7 does not have a log base 11 in mod 79

d) $100 = 7^x \bmod 103$ ($\log_7 100 \bmod 103$)

$q = 103 - 1 = 102$ $p = 103$ $\alpha = 7$

1. $t = \sqrt{102} = 10$

2. for $k = 0$ to $\lceil \frac{102}{10} \rceil = 10$

$k=0$ $f_0 = 7^{0 \cdot 10} = 1 \bmod 103$

$k=1$ $f_1 = 7^{1 \cdot 10} = 15 \bmod 103$

$k=2$ $f_2 = 7^{2 \cdot 10} = 19 \bmod 103$

$k=3$ $\delta_3 = 7^{3\cdot 10} = 79 \mod 103$
$k=4$ $\delta_4 = 7^{4\cdot 10} = 52 \mod 103$
$k=5$ $\delta_5 = 7^{5\cdot 10} = 59 \mod 103$
$k=6$ $\delta_6 = 7^{6\cdot 10} = 61 \mod 103$
$k=7$ $\delta_7 = 7^{7\cdot 10} = 91 \mod 103$
$k=8$ $\delta_8 = 7^{8\cdot 10} = 26 \mod 103$
$k=9$ $\delta_9 = 7^{9\cdot 10} = 81 \mod 103$
$k=10$ $\delta_{10} = 7^{10\cdot 10} = 82 \mod 103$

3. $i=0$ to 10
$i=0$ $100\cdot 7^0 \mod 103$ x
$i=1$ $100\cdot 7^1 \mod 103 = 82 \mod 103$ ✓
$h\cdot 7^1 = 7^{100}$ $h = 7^{99}$ $x = \log_7 7^{99}$ $\boxed{x=99}$

e) $100 = 7^x \mod 101$ $(\log_7 100 \mod 101)$
$q = 101-1 = 100$ $p = 101$ $\alpha = 7$
1. $t = \sqrt{100} = 10$

2. for $k=0$ to $\lceil \frac{100}{10} \rceil = 10$
$k=0$ $\delta_0 = 7^{0\cdot 10} = 1 \mod 101$
$k=1$ $\delta_1 = 7^{1\cdot 10} = 65 \mod 101$
$k=2$ $\delta_2 = 7^{2\cdot 10} = 84 \mod 101$
$k=3$ $\delta_3 = 7^{3\cdot 10} = 6 \mod 101$
$k=4$ $\delta_4 = 7^{4\cdot 10} = 87 \mod 101$
$k=5$ $\delta_5 = 7^{5\cdot 10} = 100 \mod 101$
$k=6$ $\delta_6 = 7^{6\cdot 10} = 36 \mod 101$
$k=7$ $\delta_7 = 7^{7\cdot 10} = 17 \mod 101$
$k=8$ $\delta_8 = 7^{8\cdot 10} = 95 \mod 101$
$k=9$ $\delta_9 = 7^{9\cdot 10} = 14 \mod 101$
$k=10$ $\delta_{10} = 7^{10\cdot 10} = 1 \mod 101$

3. $i=0$ to 10
$i=0$ $100\cdot 7^0 \mod 101$
$= 100 \mod 101$ ✓
$h\cdot 7^0 = 7^{5\cdot 10}$
$h = 7^{50}$
$x = \log_7 7^{50}$
$\boxed{x=50}$ ✓

3.

3. a) $K_{pubA} = b_A = \alpha^{a_A} \bmod p$) $k_{prA} = a_A$

$= 3^{17} \bmod 809$

b) $k_{pubB} = b_B = \alpha^{a_B} \bmod p$ $k_{prB} = a_B$

$= 3^{41} \bmod 809$

c) $k_{AB} = \alpha^{a_A \cdot a_B} \bmod p$

$= 3^{17 \cdot 41} \bmod 809 = 3^{697} \bmod 809$

a) 129140163 mod 809

= 302 mod 809

$$\begin{array}{r} 159629 \\ 809 \overline{)129140163} \\ -129139861 \\ \hline 302 \end{array}$$

b) $3.6472996 \times 10^{19} \bmod 809$

Plugged in calculator to get 153 mod 809

c) to get 410 mod 809

plugged in calculator