CS 4801: Assignment 4

Adam Camilli (aocamilli@wpi.edu)

Wednesday 5th December, 2018

1. Consider the multiplicative group of $\mathbb{Z}_{79}^*$.

   (a) What are the possible element order? How many element exist for each order?

$$\mathbb{Z}_{79}^* = a \in \mathbb{Z}_{79} \mid a \perp 79$$

Therefore we may count the size of $\mathbb{Z}_{79}^*$ with Euler's totient function (for prime numbers, since 79 is prime):

$$\phi(79^1) = 79^{1-1}(79-1) = 78$$

There are 78 elements in $\mathbb{Z}_{79}^*$ from $\mathbb{Z}_{79} = \{0, 1, \ldots 78\}$:

$$\mathbb{Z}_{79}^* = \{1, 2, \ldots, 78\}$$

The order m of the set $\mathbb{Z}_{79}^*$ is just the count of elements 78. Therefore the possible element orders are the elements which divide 78:

$$\begin{aligned} 78 &= 2^1 \cdot 3^1 \cdot 13^1 \\ &\Downarrow \\ 78 &= 6 \cdot 13 \\ &= 2 \cdot 39 \\ &= 3 \cdot 26 \\ &= 1 \cdot 78 \end{aligned}$$

This gives us the possible element orders. To find how many elements exist for each, we use Euler's totient function:

Order	# Elements	Order	# Elements
6	$\phi(6) = 2$	13	$\phi(13) = 12$
2	$\phi(2) = 1$	39	$\phi(39) = 24$
3	$\phi(3) = 2$	26	$\phi(26) = 12$
1	$\phi(1) = 1$	78	$\phi(78) = 24$

(b) Determine the order of all elements of $\mathbb{Z}_{79}^*$.

To determine the order, we need to use arithmetic modulo 79. The technical definition of an element a's order $|a|$ is the smallest m such that

$$a^m = e$$

where e is the identity element 1.

Essentially, to calculate $|a|$, we examine the powers of a to find all values of m where $a^m \bmod 79 = 1$ and m is one of the possible element orders we calculated earlier.

There must be at least one such m for all $a \in \mathbb{Z}_{79}^*$, since finite groups are closed under multiplication. In fact, we already know how many a's will fit each possible m since this is found by $\phi(m)$. We can thus simply pick $\phi(m)$ number of a's from the integer solutions of $a^m \bmod 79 = 1$ for each m using one rule:

i. Exclude results shared with smaller, non-coprime ms (i.e. for 39, exclude results shared with 3,6,13, and 26)

Order (m)	# Elements ($\phi(m)$)	Elements ($a^m \bmod 79 = 1$) of order m
1	1	1
2	1	78
3	2	$23, 55$
6	2	$24, 56$
13	12	$8, 10, 18, 21, 22, 38, 46, 52, 62, 64, 65, 67$
26	12	$12, 14, 15, 17, 27, 33, 41, 57, 58, 61, 69, 71$
39	24	$2, 4, 5, 9, 11, 13, 16, 19, 20, 25, 26, 31, 32, 36, 40, 42, 44, 45, 49, 50, 51, 72, 73, 76$
78	24	$3, 6, 7, 28, 29, 30, 34, 35, 37, 39, 43, 47, 48, 53, 54, 59, 60, 63, 66, 68, 70, 74, 75, 77$

(c) What are the generators of $\mathbb{Z}_{79}^*$?

For every positive integer n, The possible orders are the positive numbers that divide $\texttt{ord}(\mathbb{Z}_{79}^*) = 78$. The generators conversely are those that are coprime to 78:

$$78 = 2^1 \cdot 3^1 \cdot 13^1$$
$$\phi(78) = 78 \prod_{p|78} \left(1 - \frac{1}{p}\right)$$
$$\phi(78) = 78 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{13}\right) = 24$$

These 24 generators are simply the elements of $\mathbb{Z}_{79}^*$ that are smaller than and coprime to its order 78:

$$\left\langle \mathbb{Z}_{79}^* \right\rangle == \{1, 5, 7, 11, 17, 19, 23, 25,$$
$$29, 31, 35, 37, 41, 43, 47, 49,$$
$$53, 55, 59, 61, 67, 71, 73, 77\}$$

(d) Write the elements of $\mathbb{Z}_{79}^*$ as powers of 7.

Note all powers are evaluated considered mod79 :

$1 = 1^7$	$2 = 13^7$	$3 = 30^7$	$4 = 11^7$	$5 = 32^7$	$6 = 74^7$
$7 = 70^7$	$8 = 64^7$	$9 = 31^7$	$10 = 21^7$	$11 = 19^7$	$12 = 14^7$
$13 = 16^7$	$14 = 41^7$	$15 = 12^7$	$16 = 42^7$	$17 = 27^7$	$18 = 8^7$
$19 = 26^7$	$20 = 36^7$	$21 = 46^7$	$22 = 10^7$	$23 = 23^7$	$24 = 24^7$
$25 = 76^7$	$26 = 50^7$	$27 = 61^7$	$28 = 59^7$	$29 = 39^7$	$30 = 77^7$
$31 = 4^7$	$32 = 72^7$	$33 = 17^7$	$34 = 35^7$	$35 = 28^7$	$36 = 25^7$
$37 = 34^7$	$38 = 22^7$	$39 = 6^7$	$40 = 73^7$	$41 = 57^7$	$42 = 45^7$
$43 = 54^7$	$44 = 51^7$	$45 = 44^7$	$46 = 62^7$	$47 = 7^7$	$48 = 75^7$
$49 = 2^7$	$50 = 40^7$	$51 = 20^7$	$52 = 18^7$	$53 = 29^7$	$54 = 3^7$
$55 = 55^7$	$56 = 56^7$	$57 = 69^7$	$58 = 33^7$	$59 = 43^7$	$60 = 53^7$
$61 = 71^7$	$62 = 52^7$	$63 = 37^7$	$64 = 67^7$	$65 = 38^7$	$66 = 63^7$
$67 = 65^7$	$68 = 60^7$	$69 = 58^7$	$70 = 48^7$	$71 = 15^7$	$72 = 9^7$
$73 = 5^7$	$74 = 47^7$	$75 = 68^7$	$76 = 49^7$	$77 = 66^7$	$78 = 78^7$

2. Use Baby-step Giant-step Algorithm to compute following discrete logarithm problems:

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

1. Set up:

$$\mathbb{Z}_{59}^*, t = \left\lfloor \sqrt{58} \right\rfloor = 7, q = 58$$

2. Giant steps:

$$k = 0 \ldots \left\lfloor \frac{q}{t} \right\rfloor = 8$$

$$\begin{aligned}
&k = 0 \quad g_0 = 2^{0 \cdot 7} = 1 \bmod 59 \\
&k = 1 \quad g_1 = 2^{1 \cdot 7} = 20 \bmod 59 \\
&\ldots \\
&k = 8 \quad g_1 = 2^{8 \cdot 7} = 15 \bmod 59 \text{ (found by brute-force accidentally)} \\
&k = 9 \quad g_1 = 2^{9 \cdot 7} = 32 \bmod 59 \text{ (found by brute-force accidentally)}
\end{aligned}$$

$$g = \{1, 20, 56, 29, 54, 9, 15, \mathbf{32}\}$$

3. Baby steps:

$$i = 0 \ldots 7, \alpha = 2 :$$

$$\begin{aligned}
&i = 0 \qquad h_0 = 15 * 2^0 = 1 \bmod 59 \\
&i = 1 \qquad h_1 = 15 * 2^1 = 30 \bmod 59 \\
&\ldots
\end{aligned}$$

$$h = \{1, 30, 1, 2, 4, 8, 16, \mathbf{32}\}$$

4. Solve:

$$\begin{aligned}
h \cdot 2^7 = h_7 &= g_9 = 2^{63} \\
2^7 \cdot h &= 2^{63} \\
h &= 2^{56} \\
x &= \log_2 h = \mathbf{56}
\end{aligned}$$

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

1. Set up:
$$\mathbb{Z}_{79}^*, t = \lfloor\sqrt{78}\rfloor = 8, q = 78$$

2. Giant steps:
$$k = 0 \ldots \lfloor\frac{q}{t}\rfloor = 9$$

$$\begin{aligned} &k = 0 && g_0 = 11^{0\cdot 8} = 1 \bmod 79 \\ &k = 1 && g_1 = 11^{1\cdot 8} = 44 \bmod 79 \\ &\ldots \end{aligned}$$

$$g = \{1, 44, 40, 22, 20, 11, 10, \mathbf{45}, 5, 62\}$$

3. Baby steps:
$$i = 0 \ldots 8, \alpha = 11$$

$$\begin{aligned} &i = 0 && h_0 = 23 * 11^0 = 1 \bmod 79 \\ &i = 1 && h_1 = 23 * 11^1 = 16 \bmod 79 \\ &\ldots \end{aligned}$$

$$h = \{1, 16, 18, 40, \mathbf{45}\}$$

4. Solve:

$$\begin{aligned} h \cdot 11^4 &= h_4 = g_7 = 11^{56} \\ 11^4 \cdot h &= 11^{56} \\ h &= 11^{52} \\ x &= \log_{11} h = \mathbf{52} \end{aligned}$$

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

1. Set up:

$$\mathbb{Z}_{79}^*, t = \lfloor\sqrt{78}\rfloor = 8, q = 78$$

2. Giant steps:

$$k = 0 \ldots \lfloor\frac{q}{t}\rfloor = 9$$

$$\begin{aligned} k &= 0 & g_0 &= 11^{0 \cdot 8} = 1 \bmod 79 \\ k &= 1 & g_1 &= 11^{1 \cdot 8} = 44 \bmod 79 \\ &\ldots \end{aligned}$$

$$g = \{1, 44, 40, 22, 20, 11, 10, 45, 5, 62\}$$

3. Baby steps:

$$i = 0 \ldots 8, \alpha = 11$$

$$\begin{aligned} i &= 0 & h_0 &= 7 * 11^0 = 1 \bmod 79 \\ i &= 1 & h_1 &= 7 * 11^1 = 77 \bmod 79 \\ &\ldots \end{aligned}$$

$$h = \{1, 77, 57, 74, 24, 27, 60, 28, 31\}$$

4. Cannot be solved: No such value x exists

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

1. Set up:

$$\mathbb{Z}_{103}^*, t = \lfloor \sqrt{102} \rfloor = 10, q = 102$$

2. Giant steps:

$$k = 0 \ldots \lfloor \frac{q}{t} \rfloor = 10$$

$$\begin{aligned} &k = 0 && g_0 = 7^{0 \cdot 10} = 1 \bmod 103 \\ &k = 1 && g_1 = 7^{1 \cdot 10} = 15 \bmod 103 \\ &\ldots \end{aligned}$$

$$g = \{1, 15, 19, 79, 52, 59, 61, 91, 26, 81, 82\}$$

3. Baby steps:

$$i = 0 \ldots 10, \alpha = 7$$

$$\begin{aligned} &i = 0 && h_0 = 100 * 7^0 = 100 \bmod 103 \\ &i = 1 && h_1 = 100 * 7^1 = 82 \bmod 103 \\ &\ldots \end{aligned}$$

$$h = \{1, 82, \mathbf{59}\}$$

4. Solve:

$$\begin{aligned} h \cdot 7^2 = h_2 = g_5 &= 7^{50} \\ 7^2 \cdot h &= 7^{50} \\ h &= 7^{48} \\ x &= \log_7 h = \mathbf{48} \end{aligned}$$

(e) $100 = 7^x \bmod 101$ (or equivalently $\log_7 100 \bmod 101$)

1. Set up:

$$\mathbb{Z}_{101}^*, t = \lfloor \sqrt{100} \rfloor = 10, q = 100$$

2. Giant steps:

$$k = 0 \ldots \lfloor \frac{q}{t} \rfloor = 10$$

$$\begin{aligned} &k = 0 \qquad && g_0 = 7^{0 \cdot 10} = 1 \bmod 101 \\ &k = 1 \qquad && g_1 = 7^{1 \cdot 10} = 65 \bmod 103 \\ &\ldots \end{aligned}$$

$$g = \{1, 65, 84, 6, 87, 100, 36, 17, 95, 14, 1\}$$

3. Baby steps:

$$i = 0 \ldots 10, \alpha = 7$$

$$\begin{aligned} &i = 0 \qquad && h_0 = 100 * 7^0 = 100 \bmod 101 \\ &i = 1 \qquad && h_1 = 100 * 7^1 = 94 \bmod 101 \\ &\ldots \end{aligned}$$

$$h = \{1, 94, 52, 61, 23, 60, 16, 11, 77, 34, \mathbf{36}\}$$

4. Solve:

$$\begin{aligned} h \cdot 7^{10} &= h_{10} = g_6 = 7^{60} \\ 7^{10} \cdot h &= 7^{60} \\ h &= 7^{50} \\ x &= \log_7 h = \mathbf{50} \end{aligned}$$

3. D-H Key Exchange: Alice and Bob want to generate a common key. They agreed to use prime number $p = 809$ and generator $\alpha = 3$. Alice's private key $= 17$, Bob's private key $= 41$. Find the followings and show every intermediate step:

   (a) Alice's public key

   > Alice and Bob's private keys 17 and 41 can be shown (Alice, Bob) to both be primitive elements of $\mathbb{Z}^*_{809}$. Therefore Alice's public key is simply
   > $$x = \alpha^{17} \bmod 809 = 302$$

   (b) Bob's public key

   > And Bob's public key is simply
   > $$y = \alpha^{41} \bmod 809 = 153$$

   (c) Common key generated by Alice and Bob

   > Since the keys are primitive roots, the following
   > $$x^{17} \bmod 809 = y^{41} \bmod 809 = 410$$