Math 541

Solutions to HW #3

1. Gallian Chapter 2: 3,5

   - #3 Show that (a) $\{1, 2, 3\}$ under multiplication modulo 4 is not a group, but that (b) $\{1, 2, 3, 4\}$ under multiplication modulo 5 is a group.

     (a) This is not a group, since it is not closed. Consider that $2 \cdot 2 \equiv 0 \pmod 4$, and that 0 is not in the set.

     (b) This is a group. A quick multiplication table shows that the operation is binary. By associativity of multiplication in the integers, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, so the operation is associative. Consider any element $a \in \mathbb{Z}_5 - \{0\}$. Then $1 \cdot a = a \cdot 1 = a$, so there is an identity, namely 1. Consider any element $a \in \mathbb{Z}_5 - \{0\}$. Then a has an inverse. The justification follows: $1 \cdot 1 = 1 \equiv 1 \pmod 5$; $2 \cdot 3 = 6 \equiv 1 \pmod 5$; $3 \cdot 2 = 6 \equiv 1 \pmod 5$; $4 \cdot 4 = 16 \equiv 1 \pmod 5$.

   - #5 Find the inverse of the matrix $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $GL(2, \mathbb{Z}_{11})$.

     We have
     $$\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}^{-1} = \frac{1}{2 \cdot 5 - 3 \cdot 6} \begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 5 & 5 \\ 8 & 2 \end{bmatrix} = 4 \begin{bmatrix} 5 & 5 \\ 8 & 2 \end{bmatrix} = \begin{bmatrix} 9 & 9 \\ 10 & 8 \end{bmatrix}.$$

2. Compute $2^{2047423023} \pmod{11}$.

   - Fermat's Little Theorem tells us that $a^p \equiv a$ (mod p), where p is a prime. Or, if a and p are coprime, then $a^{p-1} \equiv 1$ (mod p).

     Since 2 and 11 are coprime, we make use of the second part of Fermat's Little Theorem, which tells us that $2^{10} \equiv 1 \pmod{11}$. This also means that $2^{20} = 2^{10} \cdot 2^{10} \equiv 1 \cdot 1 = 1 \pmod{11}$, and in general that $2^{10b} \equiv 1 \pmod{11}$, where b is any positive integer. Thus, $2^{2047423023} = 2^{2047423020} \cdot 2^3 \equiv 1 \cdot 2^3 = 8 \pmod{11}$.

3. Find the multiplicative inverse of 7 in $\mathbb{Z}_{11}$. Find the multiplicative inverse of 7 in $\mathbb{Z}_{101}$.

   - In $\mathbb{Z}_{11}$, the multiplicative inverse of 7 is 8, since $7 \cdot 8 = 56 \equiv 1 \pmod{11}$.
   - In $\mathbb{Z}_{101}$, the multiplicative inverse of 7 is 29, since $7 \cdot 29 = 203 \equiv 1 \pmod{101}$.

4. For integers a and b, we say $a \mid b$ (read as a divides b) if there exists an integer k such that $ak = b$. For each of the following statements either prove them or give a counter-example.

   (a) For all a in $\mathbb{Z}$, we have $a \mid a$.

   - This is true. For all a in $\mathbb{Z}$, we have $a \cdot 1 = a$. This fits the above definition with $k = 1$.

   (b) For all a, b, c in $\mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.

   - This is true. We have $ak_1 = b$ and $bk_2 = c$. This gives $(ak_1)k_2 = c$, or $a(k_1k_2) = c$. This fits the above definition with $k_1k_2 = k$.

   (c) For all a, b in $\mathbb{Z}$, if $a \mid b$, then $b \mid a$.

   - This is not true. Consider that $2 \cdot 2 = 4$, but that there is no integer k such that $4k = 2$.

   (d) For all a, b, c in $\mathbb{Z}$, if $a \mid b$ and $a \mid c$, then $a \mid b + c$.

   - This is true. We have $ak_1 = b$ and $ak_2 = c$. Therefore, $b + c = ak_1 + ak_2 = a(k_1 + k_2)$, which fits the above definition with $k_1 + k_2 = k$.

   (e) For all a, b, c in $\mathbb{Z}$, if $a \mid b$ and $c \mid b$, then $a + c \mid b$.

   - This is not true. Consider that $2 \cdot 3 = 6$ and $3 \cdot 2 = 6$ (i.e. 2 and 3 both divide 6), but that there is no integer k such that $(2 + 3)k = 5k = 6$.

(f) For all a, b in $\mathbb{Z}$, if $a \mid b$, then $a \mid bc$.

- This is true. We have $ak_1 = b$. Therefore $bc = (ak_1)c = a(k_1c)$, so $a \mid bc$, where $k_1c = k$ in the above definition.

(g) For all a, b in $\mathbb{Z}$, if $a \mid bc$, then $a \mid b$ and $a \mid c$.

- This is not true. Consider that $2 \mid 2 \cdot 3 = 6$, but $2 \nmid 3$ since there is no integer k such that $2k = 3$.

5. Find all m such that $U(m)$ has size 6. How do the multiplication tables of the groups you found compare? Do the same but now find $U(m)$ of size 7.

- All m's such that $U(m)$ has size 6 include 7, 9, 14, and 18.
- To see that this is the entire list, we use the Euler phi function, $\phi(n)$, which gives us the number of integers less than n that are coprime with n. Some properties of this function include $\phi(mn) = \phi(m)\phi(n)$, where m and n are coprime, and $\phi(p^k) = (p-1)p^{k-1}$, where p is a prime, and k is a positive integer. Combining these two facts we conclude that $\phi(n) = \phi(p_1^{k_1}p_2^{k_2}...p_m^{k_m}) = (p_1-1)p_1^{k_1-1}(p_2-1)p_2^{k_2-1}...(p_m-1)p_m^{k_m-1}$, where each p_i is prime. The statement $n = p_1^{k_1}p_2^{k_2}...p_m^{k_m}$, with each p_i prime, comes from the Fundamental Theorem of Arithmetic.
- Since $U(m)$ contains only elements coprime with m, we are looking for all m such that $\phi(m) = 6$. From HW 2, we know that $U(9)$ has six elements. In fact, $\phi(9) = \phi(3^2) = (3-1)3^1 = (2)3 = 6$, which confirms this result. Also, $U(7)$ has six elements, because the primality of 7 tells us that $\phi(7) = (7-1)7^0 = (6)1 = 6$. Similarly, $U(14)$ has six elements, since $\phi(14) = \phi(2\cdot 7) = \phi(2)\phi(7) = (2-1)(7-1) = (1)(6) = 6$, and $U(18)$ has six elements, since $\phi(18) = \phi(2 \cdot 3^2) = \phi(2)\phi(3^2) = (1)(6) = 6$.
- It can be shown using multiple cases that no such m besides 7, 9, 14, and 18 exists.
- The multiplication tables for $U(7)$, $U(9)$, $U(14)$, $U(18)$ follow:

– $U(7) =$

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

– $U(9) =$

·	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

– $U(14) =$

·	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

– $U(18) =$

$\cdot$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

- These tables are all equivalent to $U(6)$ under the following identities:
  - $U(6)$ to $U(9)$:

$$\begin{aligned} 1 &\leftrightarrow 1 \\ 2 &\leftrightarrow 4 \\ 3 &\leftrightarrow 2 \\ 4 &\leftrightarrow 7 \\ 5 &\leftrightarrow 5 \\ 6 &\leftrightarrow 1 \end{aligned}$$

  - $U(6)$ to $U(14)$:

$$\begin{aligned} 1 &\leftrightarrow 1 \\ 2 &\leftrightarrow 3 \\ 3 &\leftrightarrow 5 \\ 4 &\leftrightarrow 9 \\ 5 &\leftrightarrow 11 \\ 6 &\leftrightarrow 13 \end{aligned}$$

  - $U(6)$ to $U(18)$:

$$\begin{aligned} 1 &\leftrightarrow 1 \\ 2 &\leftrightarrow 7 \\ 3 &\leftrightarrow 5 \\ 4 &\leftrightarrow 13 \\ 5 &\leftrightarrow 11 \\ 6 &\leftrightarrow 17 \end{aligned}$$

- For the second part of this question, we seek a contradiction. Suppose that there is some n such that $\phi(n) = 7$. Note that each integer n can be written $n = p_1^{k_1} p_2^{k_2} ... p_m^{k_m}$, with each p_i a distinct prime, and each k a positive integer. Thus, $\phi(n) = (p_1 - 1)p_1^{k_1 - 1}(p_2 - 1)p_2^{k_2 - 1} ... (p_m - 1)p_m^{k_m - 1} = 7$. Therefore, $(p_i - 1)$ divides 7 for all $1 \leq i \leq m$. But, for all $p_i > 2$, $p_i - 1$ is even, so $p_i - 1 = 2b$ for some integer b, which implies that $2 \mid 7$, a contradiction. Thus, for any integer n that is a multiple of primes greater than 2, $\phi(n) \neq 7$. This leaves us with the case when $p_i^k = 2^k$ for some positive integer k. Well, $\phi(2^3) = 4 < 7 < \phi(2^4) = 8$. Since $\phi(2^k) > 7$ for all $k > 4$, we conclude that there is no integer n such that $\phi(n) = 7$.

6. Find all distinct multiplication tables for groups of size 5. (Here "distinct" means, as in class, up to relabeling of the elements.)
7. (Challenge question) Do the same but for groups of size 6!