Math 541

Solutions to HW #4

1. Use the Euclidean algorithm to compute the greatest common divisor of 320353 and 257642.

$$\begin{aligned}
320353 &= 257642(1) + 62711 \\
257642 &= 62711(4) + 6798 \\
62711 &= 6798(9) + 1529 \\
6798 &= 1529(4) + 682 \\
1529 &= 682(2) + 165 \\
682 &= 165(4) + 22 \\
165 &= 22(7) + 11 \\
22 &= 11(2) + 0
\end{aligned}$$

We conclude that g.c.d.(320353, 257642) = 11.

2. Prove that the equation

$$320353x + 257642y = 1$$

has no solutions with x, y in $\mathbb{Z}$. (Please do this question directly without referring to theorems from class.)

- From (1), we know that g.c.d(320353, 257642) = 11. We can use this to determine that $320353 = 11 \cdot 29123$, and $257642 = 11 \cdot 23422$. Then $320353x + 257642y = (11 \cdot 29123)x + (11 \cdot 23422)y = 11 \cdot (29123x + 23422y)$. That is, 11 divides any integral solution of the equation $320353x + 257642y$. Since 11 does not divide 1, we conclude that the equation has no integer solutions.

3. Compute the following values: $\phi(100)$, $\phi(40)$, $\phi(101)$.

[Recall that we have formulas $\phi(p^n) = p^n - p^{n-1}$ and $\phi(mn) = \phi(m)\phi(n)$ if m and n are relatively prime.]

- $\phi(100) = \phi(2^2 \cdot 5^2) = (2-1)(2^1)(5-1)(5^1) = (1)(2)(4)(5) = 20$
- $\phi(40) = \phi(2^3 \cdot 5^1) = (2-1)(2^2)(5-1)(5^0) = (1)(4)(4)(1) = 16$
- $\phi(101) = (101-1)(101^0) = 100$ (101 is a prime!)

4. Give 5 examples of groups with 8 elements. Do these groups have distinct multiplication tables up to reordering?

- $(\mathbb{Z}_8, +)$, i.e. $\mathbb{Z}_8$ under addition
- $U(15)$, since $\phi(15) = \phi(3 \cdot 5) = (3-1)(5-1) = (2)(4) = 8$.
- $U(16)$, since $\phi(16) = \phi(2^4) = (2-1)(2^3) = (1)(8) = 8$.
- $U(20)$, since $\phi(20) = \phi(2^2 \cdot 5) = (2-1)(2^1)(5-1) = (1)(2)(4) = 8$.
- $U(24)$, since $\phi(24) = \phi(2^3 \cdot 3) = (2-1)(2^2)(3-1) = (1)(4)(2) = 8$.
- The multiplication tables for $\mathbb{Z}_8$, $U(15)$, $U(16)$, $U(20)$, $U(24)$ follow:

– $(\mathbb{Z}_8, +) =$

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

– $U(15) =$

·	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

– $U(16) =$

·	1	3	5	7	9	11	13	15
1	1	3	5	7	9	11	13	15
3	3	9	15	5	11	1	7	13
5	5	15	9	3	13	7	1	11
7	7	5	3	1	15	13	11	9
9	9	11	13	15	1	3	5	7
11	11	1	7	13	3	9	15	5
13	13	7	1	11	5	15	9	3
15	15	13	11	9	7	5	3	1

– $U(20) =$

·	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	15
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

– $U(24) =$

·	1	5	7	11	13	17	19	23
1	1	5	7	11	13	17	19	23
5	5	1	11	7	17	13	23	19
7	7	11	1	5	19	23	13	17
11	11	7	5	1	23	19	17	13
13	13	17	19	23	1	5	7	11
17	17	13	23	19	5	1	11	7
19	19	23	13	17	7	11	1	5
23	23	29	17	13	11	7	5	1

- We see quickly that $U(24)$ is distinct from the others, since it is the only one with the property that for any $a \in U(24)$, $a^2 \equiv 1 \pmod{24}$.
- Z_8 is all different from all the others, since it has 4 distinct elements that appear on the diagonal, whereas $U(15)$, $U(16)$, and $U(20)$ each have 2 distinct elements on the diagonal.

- Each of $U(15)$, $U(16)$, and $U(20)$ have the same multiplication table up to reordering. This can be seen in the following way. Note that 2 has order 4 and 14 has order 2 in $U(15)$. A quick computation shows that the elements $\{2^a 14^b \ : \ 0 \leq a \leq 3, 0 \leq b \leq 1\}$ are all distinct and give all elements of $U(15)$. Similarly, 3 has order 4 and 15 has order 2 in $U(16)$. A similar computation shows that the elements $\{3^a 15^b \ : \ 0 \leq a \leq 3, 0 \leq b \leq 1\}$ are all distinct and give all elements of $U(16)$. In particular, matching $2^a 14^b$ in $U(15)$ with $3^a 15^b$ in $U(16)$ gives an isomorphism between the two groups. Similarly, one can compare these groups with $U(20)$ by taking an element of order 4 and another of order 2 and proceeding in the same manner.

5. Compute the order of $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ in $\mathrm{GL}_2(\mathbb{Z}_3)$ - that is, find the smallest positive integer d such that A^d is the identity matrix.

   - We do this problem with direct computation:
   - $A^1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
     $A^2 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$
     $A^3 = \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}$
     $A^4 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$
     $A^5 = \begin{bmatrix} 0 & 2 \\ 2 & 2 \end{bmatrix}$
     $A^6 = \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix}$
     $A^7 = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$
     $A^8 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
   - We conclude that the order of $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ is 8.

6. The group $U(17)$ has 16 elements. Thus, for any element $a \in U(17)$, we have that the order of a divides 16 (as proven in class). Is the converse true? That is, for each positive divisor d of 16, try to find an element of order d. Try this question also for $U(15)$.

   - The converse is true in $U(17)$.
   - By Fermat's Little Theorem, we know that for each element a of $U(17)$, $a^{16} \equiv 1 \pmod{17}$. Therefore, if any element has order less than 16, this order must divide 16. The positive divisors of 16 are 1, 2, 4, 8, and 16. We start by considering the element 2:
     - Since $2^{16} \equiv 1 \pmod{17}$, by Fermat's Little Theorem, we now check 2^8: $2^8 = 256 \equiv 1 \pmod{17}$. Therefore, $16^2 = (2^4)^2 = 2^8 = 256 \equiv 1 \pmod{17}$, and $4^4 = (2^2)^4 = 2^8 = 256 \equiv 1 \pmod{17}$. Very quickly we see that there are elements of order 8, 4, and 2, and these are 2, 4, and 16, respectively.
     - Since $3^{16} \equiv 1 \pmod{17}$, we now check 3^8: $3^8 = 6561 \equiv 16 \pmod{17}$. Next we check 3^4: $3^4 = 81 \equiv 13 \pmod{17}$. Finally, we check $3^2 = 9 \equiv 9 \pmod{17}$. We conclude that the order of 3 is 16.
   - The converse is not true in $U(15)$.

- Note that $U(15)$ has order 8, thus we must consider whether there are elements of order 2, 4, and 8.
  - Referencing the table given above for $U(15)$, we see very quickly that there are three elements of order 2 (just scan the diagonal for 1's, with the exception being the identity). Though somewhat less immediate, there are also exactly four elements of order 4 (start with 2, whose diagonal entry is 4; then $4 \cdot 2 = 8$ and $8 \cdot 2 = 16 \equiv 1 \pmod{15}$).
  - Considering that this group has only eight elements, and that there are three elements of order 2, four elements of order 4, and there is one element of order 1 (the identity, 1), we conclude that there can be no element of order 8.

7. Let a and b be elements of $U(m)$. Let e be the order of a and let f be the order of b. Prove that the order of ab divides ef. Give an example where the order of ab is smaller than ef.

- Since $a^e \equiv 1 \pmod{m}$ and $b^f \equiv 1 \pmod{m}$, we have

$$(ab)^{ef} \equiv a^{ef}b^{ef} \equiv (a^e)^f(b^f)^e \equiv 1^f 1^e \equiv 1 \pmod{m}.$$

  Now, using division algorithm, write $ef = \text{ord}(ab)q + r$ with $0 \leq r < \text{ord}(a)$. Then

$$1 \equiv (ab)^{ef} \equiv (ab)^{\text{ord}(ab)q+r} \equiv ((ab)^{\text{ord}(ab)})^q(ab)^r \equiv 1^q(ab)^r \equiv (ab)^r \pmod{m}$$

  Since r is less than the order of ab and $(ab)^r \equiv 1 \pmod{m}$, we must have that $r = 0$. Thus $ef = \text{ord}(a)q$ and $\text{ord}(a)$ divides ef.
- Example where ab is smaller than ef:
  - Referencing the table for $U(15)$ given above, we see that 2 has order 4, and 4 has order 2, but that $(2 \cdot 4) = 8$ has order 4, which is less than 8.