HOMEWORK 2 SOLUTIONS TO SELECTED PROBLEMS

Chapter 0, Problem 18. To simplify $8^{402} \bmod 5$, we first look for a power of 8 which is equal to either 1 or $-1 \bmod 5$.

$$8^2 \bmod 5 = 64 \bmod 5 = -1 \bmod 5$$

Thus, we have

$$8^{402} \bmod 5 = \left(8^2\right)^{201} \bmod 5 = (-1)^{201} \bmod 5 = -1 \bmod 5 = 4 \bmod 5$$

We could also replace 8 by 3, since $8 \bmod 5 = 3 \bmod 5$, and $3^2 \bmod 5 = 9 \bmod 5 = -1 \bmod 5$.

Additional example: What if we had $8^{403} \bmod 5$? There is no integer n such that $\left(8^2\right)^n = 8^{403}$. However, we can use another property of exponents:

$$8^{403} = 8^{402+1} = 8^{402} \cdot 8^1$$

Now we can use the previous method on the 8^{402} factor:

$$8^{403} \bmod 5 = 8^{402} \cdot 8 \bmod 5 = (-1)^{201} \cdot 8 \bmod 5 = 2 \bmod 5$$

Chapter 0, Problem 26. Suppose p is a prime that divides $a_1 \dots a_n$. We wish to show that it divides at least one of the factors a_i for some i. We can use Euclid's lemma along with associativity to break this product of n numbers:

$$(a_1)(a_2 \dots a_n)$$

Remember: in the statement of Euclid's lemma, a and b do not have to be prime. Let us use that lemma with $a = a_1$ and $b = a_2 \dots a_n$. Then p divides a_1 or p divides $a_2 \dots a_n$. If p divides a_1, we are done. Otherwise, p divides $a_2 \dots a_n$. We break that up as

$$(a_2)(a_3 \dots a_n)$$

and use Euclid's lemma again (but with $a = a_2$ and $b = a_3 \dots a_n$): either p divides a_2 or p divides $a_3 \dots a_n$. If p divides a_2, we are done. Otherwise, we continue in the same pattern. No matter what, this process will end (the worst case scenario is that p divides $a_{n-1}a_n$, but then it must divide a_{n-1} or a_n), and p must divide one of the factors a_i for some i.

Warning on using induction: In general, you want to stay away from induction if the variable you use for the induction step is an indexing variable (these tend to show up as subscripts). For example, if you wanted to use induction on this problem, the inductive step is NOT "Suppose if p divides $a_1 \dots a_n$, then p divides a_i for some i. Now suppose p divides $a_1 \dots a_{n+1} \dots$" because the a's used for the statement with n may not the same a's that appear for $n+1$. For another example, consider problem 20 from chapter 0. An inductive step would say "Suppose none of $p_1, \dots, p_n$ divides $p_1 \dots p_n + 1$." This tells us nothing about p_{n+1} and $p_1 \dots p_{n+1} + 1$ (and again these p's may not be the same ones from the beginning of the inductive step), so the inductive proof would get stuck.

Chapter 0, Problem 54. If a and b are integers, define a relation aRb if $a+b$ is even. Let us show that this is not just any relation, but an equivalence relation.

(1) Reflexive property: We need to show that aRa. Unlike the symmetric and transitive properties, we DO NOT ASSUME anything when proving the reflexive property and use only the definition of the relation.
Here, we need to verify that $a+a$ is even for any integer a. But $a+a=2a$ which is a multiple of 2, so aRa.

(2) Symmetric property: We assume that aRb and prove bRa. In this case, we suppose $a+b$ is even. Since $a+b=b+a$, if follows that $b+a$ is even as well. Hence bRa.

(3) Transitive property: We assume two things, aRb and bRc, and prove aRc. That is, $a+b$ and $b+c$ are even, and we need to prove $a+c$ is even. Suppose $a+b=2r$ and $b+c=2s$ for integers r and s. If we add these equations, we get
$$a+b+b+c=2r+2s$$
Subtract $2b$ from both sides:
$$a+c=2r+2s-2b=2(r+s-b)$$
so $a+c$ is even, and hence aRc.

By definition, an equivalence class of an integer a is
$$[a]=\{b\in\mathbb{Z}\,|\,aRb\}=\{b\in\mathbb{Z}\,|\,a+b \text{ is even}\}$$
Let us start with zero:
$$[0]=\{b\in\mathbb{Z}\,|\,0+b \text{ is even}\}$$
If $0+b$ is even, then b itself must be even, so
$$[0]=\{b\in\mathbb{Z}\,|\,b \text{ is even}\}$$
That is, one equivalence class is the set of even numbers. To find other equivalence classes, we pick a number that is not in [0], like 1:
$$[1]=\{b\in\mathbb{Z}\,|\,1+b \text{ is even}\}$$
If $1+b$ is even, then b itself must be odd, so
$$[1]=\{b\in\mathbb{Z}\,|\,b \text{ is odd}\}$$
Thus, another equivalence class is the set of odd numbers. Since every integer is even or odd, this means that there are no other equivalence classes to search for.

Chapter 1, Problem 6. Given a regular n-sided polygon, we can label one of the corners as "1" and count the rest. To do so, we need to decide whether we count up counter-clockwise or clockwise. The choice we make is an orientation of the polygon.

With this definition, we can describe all rotations of the polygon as "orientation-preserving," because they do not change the orientation. For example, if our labels on the polygon started off clockwise, and we did any rotation, "1" may be in a different place, but our labels would still go up in the clockwise direction. On the other hand, all reflections of the polygon are "orientation-reversing." For example, if the labels went up clockwise and we do any reflection, the labels would now be going counter-clockwise. With a starting orientation, we can identify any sequence of motions (rotations and reflections) as a single rotation or reflection based on whether we end up the same orientation or not. Remember: doing any sequence of

motions is the same as doing a single motion. That is the whole point behind the closure property of groups.

So if we do two or more motions, to determine of the overall result is a rotation or a reflection, we just need to choose an initial orientation and keep track of when it changes. If we start off clockwise and do two reflections, the first one gives us a counter-clockwise orientation, but the second reflection puts us back in a clockwise orientation, so the end result is a rotation. In general, if a have a sequence of motions, you can count how many individual reflections appear in the sequence. A sequence with an even number of reflections is the same as a single rotation, while a sequence with an odd number of reflections must be a single reflection.

Example: if R represents any rotation and F represents any reflection,

(1) RR is a rotation
(2) RF and FR are reflections (they might not be equal)
(3) FRRRRFRRFFFR is a reflection

Chapter 2, Problem 8. Here is the Cayley table for the proposed group:

$\times$	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

We can use the table to check for these properties of a group: closure, identity, inverses. The last property, associativity, cannot be checked with the table.

(1) Closure: To check this, we need to make sure that no new number (besides the labels for the rows and columns) appears in the interior (the 4×4 in the lower right corner) of the table. Here, we see that is the case.
(2) Identity: We can identify the identity element of the group by looking for a row in the interior of the table which matches the column labels at the top. In the problem, the row for multiplying by 25 matches the column labels at the top, so 25 must be the identity. If you want to be careful, we can look for a column in the interior which matches the row labels. We see that it is the column for 25 as well.
(3) Inverses: To guarantee that every element has an inverse without having to manually find the pairs, we can check if every row and every column in the interior of the table has the identity element. Here, we see that 25 appears in every row and column. For example, it appears in row 5, column 5, so this tell us that 5 is its own inverse:
$$5 \times 5 \bmod 40 = 25 \bmod 40$$
(4) Associativity: The table will not help us, but in this problem, we do not need to check, because we know that multiplication mod 40 is associative already.

For comparison, here is the Cayley table for $U(8) = \{1, 3, 5, 7\}$:

$\times$	5	7	1	3
5	1	3	5	7
7	3	1	7	5
1	5	7	1	3
3	7	5	3	1

If we match up the elements between the set $\{5, 15, 25, 35\}$ and $U(8)$ as follows:

$$5 \leftrightarrow 5$$
$$15 \leftrightarrow 7$$
$$25 \leftrightarrow 1$$
$$35 \leftrightarrow 3$$

we see that the Cayley tables line up. So aside from different numbers, our group $\{5, 15, 25, 35\}$ and $U(8)$ have the "same" multiplication. This matching is an example of an "isomorphism" (derived from Greek for "same form"). It means that the groups may look different, but they behave the same.

Bonus: Chapter 2, Problem 5. Let us find the inverse of $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $\mathrm{GL}(2, \mathbb{Z}_{11})$. This is a matrix A in $\mathrm{GL}(2, \mathbb{Z}_{11})$ such that

$$\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix} A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 11$$

Let us try the normal matrix inverse:

$$A = \frac{1}{(2)(5) - (6)(3)} \begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix} = \frac{1}{-8} \begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix}$$

What does it mean to divide by $-8 \bmod 11$? Remember that $\mathbb{Z}_{11}$ is a group under multiplication, so dividing by $-8 \bmod 11$ is the same as multiplying by the inverse of -8 in $\mathbb{Z}_{11}$. Since $-8 \bmod 11 = 3 \bmod 11$, we need to find the inverse of 3 mod 11. Since $3 \times 4 \bmod 11 = 12 \bmod 11 = 1 \bmod 5$, we have that the multiplicative inverse of 3 and -8 in $\mathbb{Z}_{11}$ must be 4. Thus,

$$A = 4 \begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} 20 & -24 \\ -12 & 8 \end{bmatrix}$$

Let us reduce mod 11:

$$A = \begin{bmatrix} 9 & 9 \\ 10 & 8 \end{bmatrix}$$

Check:

$$\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 9 & 9 \\ 10 & 8 \end{bmatrix} = \begin{bmatrix} 34 & 66 \\ 77 & 67 \end{bmatrix} \bmod 11 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 11$$