Abstract Algebra (MATH6302), Fall 2024
Homework Assignment 2

Joel Sleeba

September 11, 2024

1. **Solution:** Consider $\mathcal{A} = \{\{1,2,3\},\{2,5\}\} \cup \{\{x\},\ x \in \mathbb{Z}\}$. We define a relation on $\mathbb{Z}$ where we claim $x \sim y$ if there exists $A \in \mathcal{A}$ such that $x, y \in A$. We claim this is reflexive and symmetric but not transitive.

   - (Reflexivity) Let $a \in \mathbb{Z}$. Then since $\{a\} \in \mathcal{A}$, we get $a \sim a$ and we are done.
   - (Symmetry) Let $x \sim y$. Then there exists some $A \in \mathcal{A}$ with $x, y \in A$. This implies $y, x \in A$ and we get $y \sim x$.
   - (Not Transitive) $1 \sim 2$ since $\{1,2,3\} \in \mathcal{A}$ and $2 \sim 5$ since $\{2,5\} \in \mathcal{A}$. But $1 \not\sim 5$ since there are no elements in $\mathcal{A}$ containing 1 and 5.

2. **Solution:** We will show that the relation defined is reflexive, symmetric and transitive.

   - (Reflexivity) $(a,b) \sim (a,b)$ since $ab - ba = 0$ for all $a, b \in \mathbb{Z}$.
   - (Symmetry) Let $(a,b) \sim (c,d)$. Then $ad - bc = 0$, by the definition of the relation $\sim$. This implies $cb - da = 0$ by the commutativity of addition of multiplication in $\mathbb{Z}$, which is equivalent to $(c,d) \sim (a,b)$.
   - (Transitivity) Let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$ where $b, d, f \neq 0$. Then $ad - bc = 0$ and $cf - de = 0$. Since $d \neq 0$ by assumption, $adf = bcf = bed$ implies $af = be$ which gives $(a,b) \sim (e,f)$.

3. **Solution:**

   (a) Cyclic. $C_2 \times C_5 \cong C_{10}$. $(1,1)$ generates the whole group.

   (b) Not cyclic. Assume it is with generator (a,b). Now since we know that $a, b \in C_4$, we get $a^4 = b^4 = 0$ (identity element of C_4). This gives that $(a,b)^4 = (0,0)$, the identity element of $C_4 \times C_4$. Because our choice of (a,b) was arbitrary, this gives that the order of every element is at most 4. Since $C_4 \times C_4$ has 16 elements, this contradicts our assumption that it is cyclic.

   (c) Cyclic. $\forall n \in \mathbb{N}, n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$. So, 1 generates the group

   (d) Not cyclic. Assume $a \in \mathbb{Q}$ be a positive rational number and consider $\langle a \rangle$, the subgroup generated by a which is precisely $\{na : n \in \mathbb{Z}\}$. Now $a/2$ is again a rational but $a/2 \notin \langle a \rangle$. Hence $\mathbb{Q}$ is not cyclic.

   (e) Not cyclic. Assume it is and suppose that $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ is the generator. Then $(k_1 a, k_2 b) \notin \langle (a,b) \rangle$ if $(k_1, k_2) = 1$

   (f) Cyclic. Since $18 = 2 \times 3^2$, by the primitive root theorem we get that Z^*_{18} is cyclic.

   (g) Not cyclic. Since $36 = 4 \times 3^2$, by the primitive root theorem we get that it is not cyclic.

   (h) Not cyclic. Since $A \Delta A = \emptyset$ for all set A, unless $\mathcal{P}(S)$ contains only two elements, it won't be cyclic. But $|P(S)| = 2$ if and only if $|S| = 1$.

4. **Solution:** $\mathcal{P}(\{1,2\}) = \{\Phi, \{1\}, \{2\}, \{1,2\}\}$. Moreover from last assignment, we see that $(\mathcal{P}(\{1,2\}), \Delta)$ is a group. Since it has 4 elements, are there are only two distinct groups of order 4 upto isomorphism (namely the cyclic group of order 4, and the Klein 4 group), $(\mathcal{P}(\{1,2\}), \Delta)$ must be isomorphic to either one of them.

   It is clear that the identity element of this group must be Φ, since $A \Delta \Phi = A$ for all subgroup A of $\{1,2\}$. Moreover we see that $A \Delta A = (A \cup A) \setminus (A \cup A) = A \setminus A = \Phi$. Hence every element in the group $(\mathcal{P}(\{1,2\}), \Delta)$ is its own inverse. Since we know this is a property of the Klein 4 group, we get that $(\mathcal{P}(\{1,2\}), \Delta)$ is isomorphic to V_4, the Klein group of order 4.

5. **Solution:** Recall that if $G_1, G_2, \ldots, G_n$ are groups, then their direct product $\mathcal{G} = G_1 \times G_2 \times \cdots \times G_n$ is a group under the operation $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n)$ with identity element $(e_1, e_2, \ldots, e_n)$ where each e_j is the identity element in G_j.

   ($\implies$) Assume that $\mathcal{G}$ is an Abelian group. Let $1 \leq i \leq n$, we will show that G_i is Abelian. Let $g, h \in G_i$. Consider the corresponding elements $\tilde{g} = (e_1, e_2, \ldots, e_{i-1}, g, e_{i+1}, \ldots, e_n)$ and $\tilde{h} = (e_1, e_2, \ldots, e_{i-1}, h, e_{i+1}, \ldots, e_n)$ in $\mathcal{G}$. Since we know that $\mathcal{G}$ is Abelian, we get $\tilde{g}\tilde{h} = \tilde{h}\tilde{g}$. This by the definition of multiplication implies

$$(e_1, e_2, \ldots, e_{i-1}, gh, e_{i+1}, \ldots, e_n) = (e_1, e_2, \ldots, e_{i-1}, hg, e_{i+1}, \ldots, e_n)$$

   which implies $gh = hg$. Now since $g, h \in G_i$ was arbitrary and $1 \leq i \leq n$ was arbitrary, we get that G_i is Abelian for all $1 \leq i \leq n$.

   ($\impliedby$) Conversely, if each G_i is Abelian, then for $\tilde{g} = (g_1, g_2, \ldots, g_n), \tilde{h} = (h_1, h_2, \ldots, h_n) \in \mathcal{G}$,

$$\begin{aligned} \tilde{g}\tilde{h} &= (g_1h_1, g_2h_2, \ldots, g_nh_n) \\ &= (h_1g_1, h_2g_2, \ldots h_ng_n) \\ &= \tilde{h}\tilde{g} \end{aligned}$$

   which shows $\mathcal{G}$ is Abelian.

6. **Solution:** We will show that the relation is reflexive, symmetric, and transitive.

   - (Reflexivity) Let $g \in C_n$, then $g^{-1}g = e \in H$ since $e \in H$.
   - (Symmetry) Let $g \sim h$. Then $g^{-1}h \in H$. Since H is a subgroup, $(g^{-1}h)^{-1} = h^{-1}g \in H$ which implies $h \sim g$.
   - (Transitivity) Let $f \sim g$ and $g \sim h$. Then $f^{-1}g, g^{-1}h \in H$ and $f^{-1}h = f^{-1}(gg^{-1})h = (f^{-1}g)(g^{-1}h) \in H$. Hence $f \sim h$.

7. **Solution:**

   (a) We know that an $x \in \mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ is in $\mathbb{Z}_n^*$ if and only if there exists an $y \in \mathbb{Z}_n$ with $xy \equiv 1 \mod n$, which is equivalent to $\gcd(x, n) = 1$. Hence

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \ : \ \gcd(x, n) = 1\}$$

Then by the definition of Euler-totient function, we get that the cardinality of $\mathbb{Z}_n^*$ is $\phi(n)$. Specifically for this question, it would be $\phi(900)$. Since $900 = 2^2 3^2 5^2$, we get that $\phi(900) = 2(2-1)3(3-1)5(5-1) = 240$. Hence $|G| = 240$

(b) Since $\gcd(11, 900) = 1$, we see that $11 \in \mathbb{Z}_{900}^*$. So $11^{-1} \in \mathbb{Z}_{900}^*$. To find 11^{-1}, we use the reverse Euclidean algorithm. We see that

$$\begin{aligned}
900 &= 11 \times 81 + 9 \\
11 &= 9 \times 1 + 2 \\
9 &= 2 \times 4 + 1
\end{aligned}$$

so reversing it we get

$$\begin{aligned}
1 &= 9 - 2 \times 4 \\
&= 9 - (11 - 9) \times 4 \\
&= 9 \times 5 - 11 \times 4 \\
&= (900 - 11 \times 81) \times 5 - 11 \times 4 \\
&= 900 \times 5 + 11 \times (-409)
\end{aligned}$$

So $11^{-1} \equiv -409 \mod 900 = 419 \mod 900$. Hence $11^{-1} = 419$ in Z_{900}^*.

8. **Solution:** The equation is $5457x \equiv 3317 \mod 5885$. We find the gcd of 5885 and 5457 using the Euclidean algorithm.

$$\begin{aligned}
5885 &= 5457 \times 1 + 428 \\
5457 &= 428 \times 12 + 321 \\
428 &= 321 \times 1 + 107 \\
321 &= 107 \times 3
\end{aligned}$$

Hence we see that $\gcd(5885, 5457) = 107$ and $107 | 3317$ as $3317 = 107 \times 31$. Hence dividing the whole equation by the common denominator, we see that solving $5457x \equiv 3317 \mod 5885$ is equivalent to solving

$$51x \equiv 31 \mod 55$$

Hence we use the euclidean algorithm again,

$$\begin{aligned}55 &= 51 \times 1 + 4\\ 51 &= 4 \times 12 + 3\\ 4 &= 3 \times 1 + 1\\ 3 &= 1 \times 3\end{aligned}$$

Reversing this gives us

$$\begin{aligned}1 &= 4 - 3\\ &= 4 - (51 - 4 \times 12)\\ &= 4 \times 13 - 51\\ &= (55 - 51) \times 13 - 51\\ &= 55 \times 13 - 51 \times 14\\ &= 55 \times 13 + 51 \times (-14)\end{aligned}$$

So we see that $51^{-1} \equiv -14 \mod 55$ and $-14 \equiv 41 \mod 55$. Hence the primitive modulo class of 41 is the solution for the equation $51x \equiv 1 \mod 51$. So multiplying the equation $51x \equiv 31 \mod 55$ with $55^{-1} = 41$, we see that $x \equiv 31 \times 41 \mod 55 = 1271 \mod 55 = 6 \mod 55$. Hence the solution set for the original equation is $\{55n + 6 \ : \ n \in \mathbb{Z}\}$

9. **Solution:** Since $101, 103, 107$ are coprimes to each other, chineese remainder theorem gives that there is a unique solution for x in the $Z_{101\times103\times107} = \mathbb{Z}_{1113121}$.

   Now $x \equiv 43 \mod 101$ implies $x = 101k_1 + 43$. Substituting this to the next equation, we get $101k_1 + 43 \equiv 10 \mod 103$ which is equivalent to $k_1 \equiv (101^{-1})70 \mod 103$. Now using the reverse Euclidean algorithm, we find the inverse of 101 in Z_{103}. Since $1 = 101 \times 51 + 103 \times (-50)$, we see that $101^{-1} = 51 \in \mathbb{Z}_{103}$. Therefore $k_1 \equiv 51 \times 70 \equiv 68 \mod 103$. Hence $k_1 = 104k_2 + 68$ and $x = 101(103k_2 + 68) + 43 = 10403k_2 + 6911$.

   Now we substitute this to the next equation to get $10403k_2 + 6911 \equiv 96 \mod 107$ which is eqiuvalent to $k_2 \equiv (10403^{-1})33 \mod 107$. Now similarly using the reverse euclidean algorithm, we find that $1 = 4764 \times 107 + 10403(-49)$. Hence we see that $10403^{-1} = -49 \equiv 58 \mod 107$. Hence $k_2 \equiv 58 \times 33 \equiv 1914 \equiv 95 \mod 107$. Therefore $k_2 = 107n + 95$ and $x = 10403(107n + 95) + 6911 = 113121n + 995196$.

   Hence the solution set of the system of equations is $\{113121n + 995196, n \in \mathbb{N}\}$.

10. **Solution:** Given that 10 is a primitive root modulo 313. This gives that $\langle 10 \rangle = Z^*_{313}$. Moreover since we know that 313 is a prime, $\phi(313) = 312$ and therefore $|10| = 312$. Therefore if $x = 10^a \in \langle 10 \rangle$ with $x^3 = 1 \mod 313$, then either $x = 1$ or $|10^a| = 3$. But we know that for any cyclic group with generator g, $|g^a| = \frac{|g|}{(a,|g|)}$. Therefore if

$$|10^a| = \frac{|10|}{(a, |10|)} = \frac{312}{(a, 312)} = 3$$

one must have $(a, 312) = \frac{312}{3} = 104$. The only possible candidates for a are $104, 208$. Hence the residue classes which satisfy the given equation are $[1], [10^{104}], [10^{208}]$. Now using the usual theatrics, we see that this is exactly $[1], [214]$ and $[98]$ respectively.

11. **Solution:** We see that $7^4 = 2401$ has its ones digit equal to 1. Therefore $7^{4n} = (7^4)^n = (2401)^n$ must have its ones digit equal to 1 for all $n \in \mathbb{N}$. By the same logic we see that the ones digit of $7^{4n+1}, 7^{4n+2}, 7^{4n+3}$ must be $7, 9$, and 3 respectively. Hence to find the ones digit of $7^{7^{7^7}}$, we just need to find out the residue class of $7^{7^7} = 7^{49}$. $49 = 32 + 16 + 1$

    - $7^1 \mod 4 = 3$
    - $7^2 \mod 4 = (7 \mod 4)(7 \mod 4) = 3^2 \mod 4 = 1$
    - $7^4 \mod 4 = (7^2 \mod 4)(7^2 \mod 4) = 1^2 \mod 4 = 1$

    Now since we are going to keep multiplying by 1 while finding the residue classes of 7 rasied to higher powers of 2, we conclude that $7^{16}, 7^{32}$ both lie in the residue class of $1 \mod 4$. Hence $7^{49} \mod 4 = 1 \times 1 \times 3 \mod 7 = 3$. Therefore $7^{7^7} = 4n+3$ for some $n \in \mathbb{N}$, and therefore by our previous reasoning, we see that the ones digit of $7^{7^{7^7}}$ is 3.

12. **Solution:** We see that 1074 = 1024 + 32+ 16 + 2.

    - $8^2 \mod 211 = 64 \mod 211$
    - $8^4 \mod 211 = 4096 \mod 211 = 87$
    - $8^8 \mod 211 = (8^4 \mod 211)(8^4 \mod 211) = 87^2 \mod 211 = 184$

- $8^{16} \mod 211 = (8^8 \mod 211)(8^8 \mod 211) = 184^2 \mod 211 = 96$
- $8^{32} \mod 211 = (8^{16} \mod 211)(8^{16} \mod 211) = 96^2 \mod 211 = 143$
- $8^{64} \mod 211 = (8^{32} \mod 211)(8^{32} \mod 211) = 143^2 \mod 211 = 193$
- $8^{128} \mod 211 = (8^{64} \mod 211)(8^{64} \mod 211) = 193^2 \mod 211 = 113$
- $8^{256} \mod 211 = (8^{128} \mod 211)(8^{128} \mod 211) = 113^2 \mod 211 = 109$
- $8^{512} \mod 211 = (8^{256} \mod 211)(8^{256} \mod 211) = 109^2 \mod 211 = 65$
- $8^{1024} \mod 211 = (8^{512} \mod 211)(8^{512} \mod 211) = 65^2 \mod 211 = 5$

Therefore $8^{1074} \mod 211 = 5 \times 143 \times 96 \times 64 \mod 211 = 4392960 \mod 211 = 151$

13. **Solution:** Using Bezout's lemma we see that $\gcd(a, n) = \gcd(a + kn, n)$ for all $k \in \mathbb{Z}$. Hence the statement we have to prove is equivalent to showing $a \in \mathbb{Z}_n$ is a generator for $\mathbb{Z}_n$ if and only if $(a, n) = 1$. (a here is assumed to be the smallest positive integer in the corresponding residue class $[a]$, and we will continue this convention)

    ($\implies$) Let $a \in \mathbb{Z}_n$ with $(a, n) = d \neq 1$. Then for $k = \frac{n}{d} > 1$ (still an integer), we get $ak = \frac{an}{d}$, Since $d|a$, we get that $n|ak$ which gives that $ak \mod n = 0$. Therefore the strict subset $\{a, 2a, \ldots, (k-1)a, 0 = ka\}$ is closed under modular addition, which makes it a proper subgroup. Thus we see that a cannot generate $\mathbb{Z}_n$

    ($\impliedby$) Conversely, if $(a, n) = 1$ then by Bezout's lemma there exists k_1, k_2 with $(k_1, k_2) = 1$ such that $ak_1 + nk_2 = 1$. which implies $ak_1 \equiv 1 \mod n$. This implies ak_1 is the equivalent class of 1. Now since we know $[1]$ is a generator for $\mathbb{Z}_n$, we see that a generate $\mathbb{Z}_n$.

14. **Solution:** Since 103 is a prime we see that Z_{103}^* has 102 elements and that it is a cyclic group. Let g be a generator of the group. If g^a is any other generator for $1 \leq a \leq 102$, we must have $|g^a| = \frac{|g|}{(a,|g|)} = \frac{102}{(a,102)} = 102$ which gives $(a, 102) = 1$. There is exactly $\phi(102) = 32$ such a by the definition of the Euler-totient function.

15. **Solution:** Let Graham's number $g = 3^{b_1}$. We should find out $x \in Z_{121}$ such that $x \equiv g \mod 121$. Since $(3, 121) = 1$ and $\phi(121) = 110$, we see that if we can write $b_1 = 110 \times q + b_1$, then using Fermat's little theorem we'll get $g = 3^{110q+r} \mod 121 \equiv (3^{110} \mod 121)^q(3^r \mod 121) = 3^r \mod 121$.

    As a general rule of thumb, we get that if $(3, n) = 1$, then $3^a \mod n \equiv 3^r \mod n$, where $a = \phi(n)q + r$. Now we are at a place to proceed with our calculations.

    - Let $g = 3^{b_1}$ be the Graham's number. Since $(121, 3) = 1$ and $\phi(121) = 110$, $3^{b_1} \equiv 3^{r_1} \mod 121$ where $r_1 = b_1 \mod 110$
    - Now let $b_1 = 3^{b_2}$. Since $(110, 3) = 1$ and $\phi(110) = 40$, $3^{b_2} \equiv 3^{r_2} \mod 110$ where $r_2 = b_2 \mod 40$
    - Now let $b_2 = 3^{b_3}$. Since $(40, 3) = 1$ and $\phi(40) = 16$, $3^{b_3} \equiv 3^{r_3} \mod 40$ where $r_3 = b_3 \mod 16$
    - Now let $b_3 = 3^{b_4}$. Since $(16, 3) = 1$ and $\phi(16) = 8$, $3^{b_4} \equiv 3^{r_4} \mod 16$ where $r_4 = b_4 \mod 8$
    - Now let $b_4 = 3^{b_5}$. Since $(8, 3) = 1$ and $\phi(8) = 4$, $3^{b_5} \equiv 3^{r_5} \mod 8$ where $r_5 = b_5 \mod 4$

    Now since $3 \mod 4 = -1$ and b_5 is an odd number being the odd power 3, we see that $3^{b_5} = -1 \mod 4 = 3 \mod 4$. Hence $r_5 = 3$, Tracing the argument back, we get

    - $r_4 = 3^{r_5} \mod 8 = 3^3 = 27 \mod 8 = 3$
    - $r_3 = 3^{r_4} \mod 16 = 3^3 = 27 \mod 16 = 11$
    - $r_2 = 3^{r_3} \mod 40 = 3^{11} \mod 40 = 27$
    - $r_1 = 3^{r_2} \mod 110 = 3^{27} \mod 110 = 97$
    - $g = 3^{r_1} \mod 121 = 3^{97} \mod 121 = 9$

    Hence $x = 9$ is the required answer.

16. **Solution:** If $y = 1 \mod 9797$ that implies $(y, 9797) = 1$. Since $9797 = 101 \times 97$, this is equivalent to $(y, 97) = 1$ and $(y, 101) = 1$. Hence we look for x^3 which simultaneously satisfy $x^3 = 1 \mod 97$ and $x^3 = 1 \mod 101$. Since

we know that 97 and 101 are primes, we get that Z_{97}^*, Z_{101}^* are cyclic groups with cardinality 96 and 100 respectively.

Since we know that the order of an element in a group must divide the order of the group, and $3 \not| 100$, we get that there are no elements of order 3 in Z_{101}^*. Hence we get that the only element in Z_{101}^* with $x^3 = 1 \mod 101$ is $x = 1$.

Similarly, if $g \in Z_{97}^*$ generate the group, and $|g^k| = 3$, then we must have $\frac{|g|}{(k,|g|)} = \frac{96}{(k,96)} = 3$ which gives $(k, 96) = 32$. Hence the possible values for a are 32 and 64. Since we know that 5 is a generator for Z_{97}^*, we get that the elements in $x \in Z_{97}^*$, with $x^3 = 1 \mod 97$ are specifically $35 = 5^{32} \mod 97$ and $61 = 5^{64} \mod 97$.

Now to find the x which satisfy $x^3 = 1 \mod 9797$, we will use the Chineese remainder theorem to solve the 3 different system of linear equations.

$$\begin{array}{lll} x = 1 \mod 97 & x = 35 \mod 97 & x = 61 \mod 97 \\ x = 1 \mod 101 & x = 1 \mod 101 & x = 1 \mod 101 \end{array}$$

Now using the chinese remainder theorem, we get that the solutions are $1, 5758, 1516 \in Z_{9797}^*$