Abstract Algebra
Day 4 Class Work Solutions

1. Compute each of the following in $\mathbb{Z}_7$. Simplify your result as much as possible.

   (a) $6+4$ (b) $4\cdot 2$ (c) $2-5$ (d) 3^4 (e) 3258 (f) -3258

   Solution.

   (a) $6+4=3$
   (b) $4\cdot 2=1$
   (c) $2-5=4$
   (d) $3^4=4$
   (e) $3258=3$
   (f) $-3258=4$

   Ans to (f): $-3258=4$.

2. (a) Describe all integers n such that $n=0$ in $\mathbb{Z}_7$.

   Solution. They are the multiples of 7, i.e., the elements of the set

   $$7\mathbb{Z}=\{n\in\mathbb{Z}\mid n=7k \text{ where } k\in\mathbb{Z}\}.$$

   ← Include *negative* integers.

   (b) Describe all integers n such that $n=2$ in $\mathbb{Z}_7$.

   Solution. They are 2 more than a multiple of 7, i.e., the elements of the set

   $$\{n\in\mathbb{Z}\mid n=7k+2 \text{ where } k\in\mathbb{Z}\}.$$

3. For each pair a and b, determine whether or not $a=b$ in $\mathbb{Z}_7$.

   ← These should be done *without* a calculator.

   (a) $a=16$ and $b=30$

   Solution. YES, because 30 is $14=7\cdot 2$ more than 16.

   (b) $a=3258$ and $b=3288$

   Solution. NO, the difference between a and b is 30, which is *not* a multiple of 7.

   (c) $a=-710$ and $b=-731$

   Solution. YES, because -731 is $21=7\cdot 3$ less than 710.

   (d) $a=98765123406$ and $b=98765123476$

   Solution. YES, because b is $70=7\cdot 10$ more than a.

4. Given a, $b\in\mathbb{Z}$, describe how you can determine whether or not $a=b$ in $\mathbb{Z}_7$. Can you do this *without* first simplifying each of a and b in $\mathbb{Z}_7$?

   Solution. We have $a=b$ in $\mathbb{Z}_7$ when the difference between a and b is a multiple of 7; equivalently, when $7\mid(a-b)$, i.e., 7 is a divisor of $a-b$.

5. Consider $\mathbb{Z}_7=\{0,1,2,3,4,5,6\}$ again. Recall that 3 is a multiplicative inverse of 5 because $3\cdot 5=1$. (And vice versa, i.e., 5 is a multiplicative inverse of 3.) Find all other elements of $\mathbb{Z}_7$ that have multiplicative inverses.

   Ans: All of them except 0.

   Solution. All elements of $\mathbb{Z}_7$, except 0, have multiplicative inverses. The *inverse pairs* (i.e., pairs a and b such that $a\cdot b=1$) are...

   $$1\cdot 1=1,\quad 2\cdot 4=1,\quad 3\cdot 5=1,\quad 6\cdot 6=1.$$

6. Now switch gears and consider the number system $\mathbb{Z}_5=\{0,1,2,3,4\}$. Which one of these elements have multiplicative inverses?

   Ans: All of them except 0.

   Solution. All elements except 0. The inverse pairs are $1\cdot 1=1$, $2\cdot 3=1$, and $4\cdot 4=1$.

7. (a) Repeat Problem #6 with $\mathbb{Z}_6$, with $\mathbb{Z}_{10}$, and with $\mathbb{Z}_{15}$. Any conjectures?

   Solution. The table below contain data for $\mathbb{Z}_6$, $\mathbb{Z}_{10}$, and $\mathbb{Z}_{15}$, and for $\mathbb{Z}_7$ and $\mathbb{Z}_5$.

$\mathbb{Z}_m$	Elements with inverses
$\mathbb{Z}_5$	1, 2, 3, 4
$\mathbb{Z}_6$	1, 5
$\mathbb{Z}_7$	1, 2, 3 ,4, 5, 6
$\mathbb{Z}_{10}$	1, 3, 7, 9
$\mathbb{Z}_{15}$	1, 2, 4, 7, 8, 11, 13, 14

   Looking at $\mathbb{Z}_{15}$, for instance, we see that the elements with inverses are precisely those that are *relatively prime* to 15. In other words...

   - If $\gcd(a, 15) = 1$, then a has an inverse in $\mathbb{Z}_{15}$.
   - If $\gcd(a, 15) \neq 1$, then a does not have an inverse in $\mathbb{Z}_{15}$.

   (b) In $\mathbb{Z}_{35}$, does 8 have a multiplicative inverse? What about 10? How do you know? ← You're *not* being asked to find these inverses.

   Solution. Applying the conjecture from part (a), we have...

   - Since $\gcd(8, 35) = 1$, we believe 8 has an inverse in $\mathbb{Z}_{35}$.
   - Since $\gcd(10, 35) \neq 1$, we believe 10 does not have an inverse in $\mathbb{Z}_{35}$.

8. (a) In $\mathbb{Z}_{2584}$, does 2583 have a multiple inverse? If so, find it. If not, explain why not.

   Solution. YES. In $\mathbb{Z}_{2584}$, we have $2583 = -1$. Thus, $2583 \cdot 2583 = -1 \cdot -1 = 1$, so that 2583 is its own multiplicative inverse.

   (b) Generalize your result from part (a).

   Solution. In $\mathbb{Z}_m$, we have $m - 1 = -1$. Thus, $(m-1) \cdot (m-1) = -1 \cdot -1 = 1$, so that $m - 1$ is its own multiplicative inverse.

9. (a) **True or False:** In $\mathbb{Z}_m$, if $a \cdot b = 0$, then $a = 0$ or $b = 0$.

   Solution. False. For a counterexample, consider $a = 2$ and $b = 4$ in $\mathbb{Z}_8$. We have $a \cdot b = 0$, but neither a nor b is equal to 0 in $\mathbb{Z}_8$.

   (b) The statement in part (a) is true for which values of m? false for which values of m?

   Solution. It is true if m is a prime number.

   (c) *Justify* your conjectures from part (b).

10. In $\mathbb{Z}_7$, compute 6^{231}. Also compute 2^{101}. **Ans:** $2^{101} = 4$.

11. **(Some Food for Thought)** Compute

$$a^6 + a^5 + a^4 + a^3 + a^2 + a + 1$$

    for each $a \in \mathbb{Z}_7$ with $a \neq 1$. Can you explain what's going on and why?