Math 333 Problem Set 4
Due: 03/02/16

Be sure to list EVERYONE in the that you talk to about the homework!

1. Compute $([a]_2 + [b]_2)^2$ for any $a, b \in \mathbb{Z}$.

   We have $([a]_2+[b]_2)^2 = [a]_2^2+2[a]_2[b]_2+[b]_2^2 = [a]_2^2+[b]_2^2$ since $2[a]_2[b]_2 = [0]_2$.

2. Which of $[0], [1], [2], [3]$ is $[5^{627}]$ equal to in $\mathbb{Z}/4\mathbb{Z}$?

   We have $[5]_4 = [1]_4$, so $[5^{627}]_4 = [5]_4^{627} = [1]_4^{627} = [1]_4$. This relies on the following lemma.

   Lemma 1. *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$. If $[a]_n = [b]_n$ then $[a]_n^k = [b]_k$ for all $k \in \mathbb{Z}_{\geq 1}$.*

   Proof. We prove this by induction with the base case being $k = 1$, which is true by assumption. Assume that for some $m \in \mathbb{Z}_{\geq 1}$ we have $[a]_n^m = [b]_n^m$. We have $[a]_n^{m+1} = [a]_n^m[a]_n = [b]_n^m[b]_n = [b]_n^{m+1}$. Thus, the lemma follows by induction. $\square$

3. (a) Prove or disprove: If $[a]_n[b]_n = [a]_n[c]_n$ in $\mathbb{Z}/n\mathbb{Z}$ with $[a]_n \neq [0]_n$, then $[b]_n = [c]_n$.

   This is not true. Let $n = 6$, $a = 2, b = 4$ and $c = 1$. Then $[2]_6[4]6 = [8]_6 = [2]_6 = [2]_6[1]_6$ but $[4]_6 \neq [1]_6$.

   (b) Prove or disprove: If $[a]_p[b]_p = [a]_p[c]_p$ in $\mathbb{Z}/p\mathbb{Z}$ with $[a]_p \neq [0]_p$, then $[b]_p = [c]_p$ for p a prime number.

   Note that if $[a]_p \neq [0]_p$ then $p \nmid a$, i.e., $\gcd(a, p) = 1$. Thus, there exists $m, n \in \mathbb{Z}$ so that $am+pn = 1$, i.e., $[a]_p[m]_p = [1]_p$. Suppose that $[a]_p[b]_p = [a]_p[c]_p$. Multiplying both sides by $[m]_p$ we obtain

$$\begin{aligned}
[b]_p &= [1]_p[b]_p \\
&= ([m]_p[a]_p)[b]_p \\
&= [m]_p([a]_p[b]_p) \\
&= [m]_p([a]_p[c]_p) \\
&= ([m]_p[a]_p)[c]_p \\
&= [1]_p[c]_p \\
&= [c]_p.
\end{aligned}$$

4. Write out addition and multiplication tables for $\mathbb{Z}/6\mathbb{Z}$.

Note I omit the $[\cdot]_6$ here to save typing.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	5	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

5. (a) Show that $10^n \equiv 1 \pmod 9$ for every positive integer n.

   Proof. Observe we have $10 \equiv 1 \pmod 9$, so $10^n \equiv 1^n \pmod 9 \equiv 1 \pmod 9$ where we use the lemma above again. □

   (b) Prove that every positive integer is congruent to the sum of its digits modulo 9. (For example, $38 \equiv 11 \pmod 9$.)

Proof. Let $m \in \mathbb{Z}_{>0}$ and write $m = a_n a_{n-1} \cdots a_1 a_0$ with $a_i \in \{0, 1, \ldots, 9\}$. Then we have

$$\begin{aligned} m &= \sum_{j=0}^{n} a_j 10^j \\ &\equiv \sum_{j=0}^{n} a_j 10^j \pmod 9 \\ &\equiv \sum_{j=0}^{n} a_j \cdot 1 \pmod 9 \\ &\equiv \sum_{j=0}^{n} a_j \pmod 9. \end{aligned}$$

□

6. Find all units and zero divisors in $\mathbb{Z}/6\mathbb{Z}$.

   The units are $[1]_6$ and $[5]_6$ and the zero divisors are $[2]_6, [3]_6$, and $[4]_6$.

7. How many solutions does the equation $[6]_8 x = [4]_8$ have in $\mathbb{Z}/8\mathbb{Z}$?

   One can just plug in every value of $\mathbb{Z}/8\mathbb{Z}$ to see the solutions are $[2]_8$ and $[6]_8$ as $[6]_8[2]_8 = [12]_8 = [4]_8$ and $[6]_8[6]_8 = [36]_8 = [4]_8$.

8. Let $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$. Prove that if $[a]_n$ is a unit then the equation $[a]_n x = [b]_n$ has a unique solution in $\mathbb{Z}/n\mathbb{Z}$.

   Proof. Let $[a]_n$ be a unit, i.e., there exists $[c]_n \in \mathbb{Z}/n\mathbb{Z}$ so that $[a]_n[c]_n = [1]_n$. If we set $x = [cb]_n$ then we have

$$\begin{aligned} [a]_n x &= [a]_n [cb]_n \\ &= [ac]_n [b]_n \\ &= [1]_n [b]_n \\ &= [b]_n. \end{aligned}$$

Thus, $[cb]_n$ is a solution. Now suppose $[d]_n$ is another solution. Then we have

$$\begin{aligned}[d]_n &= [1]_n[d]_n \\ &= [ac]_n[d]_n \\ &= [c]_n[a]_n[d]_n \\ &= [c]_n[b]_n \\ &= [cb]_n \\ &= x.\end{aligned}$$

Thus, the solution is unique. $\square$

9. Almost every item sold has a UPC number $d_1 d_2 \cdots d_{11} d_{12}$. The last digit d_{12} is a check digit chosen so that

$$3 \sum_{j=0}^{5} d_{2j+1} + \sum_{j=1}^{6} d_{2j} \equiv 0 \pmod{10}.$$

If the congruence does not hold, an error has been made and the item must be scanned again or the UPC code entered by hand. Is 040293673034 a possible UPC code?

To be a valid UPC code we must have

$$3(0+0+9+6+3+3) + (4+2+3+7+4) \equiv 0 \pmod{10}.$$

Observe the left hand side is equal to 83, so this is not a valid UPC code.