# Math 446 - Homework # 5

1. List the elements of $\mathbb{Z}_7^\times$. For each element find it's multiplicative inverse.

   **Solution:** $\mathbb{Z}_7^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$

   We have that $\overline{1}^{-1} = \overline{1}$.

   $\overline{2}^{-1} = \overline{4}$ since $\overline{2} \cdot \overline{4} = \overline{8} = \overline{1}$.

   $\overline{3}^{-1} = \overline{5}$ since $\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$.

   $\overline{4}^{-1} = \overline{2}$ since $\overline{2} \cdot \overline{4} = \overline{8} = \overline{1}$.

   $\overline{5}^{-1} = \overline{3}$ since $\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$.

   $\overline{6}^{-1} = \overline{6}$ since $\overline{6} \cdot \overline{6} = \overline{36} = \overline{1}$.

2. List the elements of $\mathbb{Z}_8^\times$. For each element find it's multiplicative inverse.

   **Solution:** $\mathbb{Z}_8^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$

   We have that $\overline{1}^{-1} = \overline{1}$.

   $\overline{3}^{-1} = \overline{3}$ since $\overline{3} \cdot \overline{3} = \overline{9} = \overline{1}$.

   $\overline{5}^{-1} = \overline{5}$ since $\overline{5} \cdot \overline{5} = \overline{25} = \overline{1}$.

   $\overline{7}^{-1} = \overline{7}$ since $\overline{7} \cdot \overline{7} = \overline{49} = \overline{1}$.

3. List the elements of $\mathbb{Z}_{15}^\times$. For each element find it's multiplicative inverse.

   **Solution:** $\mathbb{Z}_{15}^\times = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$

   We have that $\overline{1}^{-1} = \overline{1}$.

   $\overline{2}^{-1} = \overline{8}$ since $\overline{2} \cdot \overline{8} = \overline{16} = \overline{1}$.

   $\overline{4}^{-1} = \overline{4}$ since $\overline{4} \cdot \overline{4} = \overline{16} = \overline{1}$.

   $\overline{7}^{-1} = \overline{13}$ since $\overline{7} \cdot \overline{13} = \overline{91} = \overline{1}$.

   $\overline{8}^{-1} = \overline{2}$ since $\overline{2} \cdot \overline{8} = \overline{16} = \overline{1}$.

   $\overline{11}^{-1} = \overline{11}$ since $\overline{11} \cdot \overline{11} = \overline{121} = \overline{1}$.

   $\overline{13}^{-1} = \overline{7}$ since $\overline{7} \cdot \overline{13} = \overline{91} = \overline{1}$.

   $\overline{14}^{-1} = \overline{14}$ since $\overline{14} \cdot \overline{14} = \overline{196} = \overline{1}$.

4. Find all of the primitive roots for $\mathbb{Z}_7^\times$. How many are there?

**Solution:** $\mathbb{Z}_7^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$.

$\overline{2}$ is not a primitive root because the positive powers of $\overline{2}$ do not give us all of $\mathbb{Z}_7^\times$. Here are the first few positive powers of $\overline{2}$:

$$\begin{array}{rcl} \overline{2}^1 & = & \overline{2} \\ \overline{2}^2 & = & \overline{4} \\ \overline{2}^3 & = & \overline{1} \\ \overline{2}^4 & = & \overline{2} \\ \overline{2}^5 & = & \overline{4} \\ \overline{2}^6 & = & \overline{1} \\ \vdots & & \vdots \end{array}$$

Note how the powers keep repeating $\overline{2}$, $\overline{4}$, and $\overline{1}$ forever.

On the other hand, $\overline{3}$ is a primitive root because we get all of the elements of $\mathbb{Z}_7^\times$ from the positive powers of $\overline{3}$ as we see below:

$$\begin{array}{rcl} \overline{3}^1 & = & \overline{3} \\ \overline{3}^2 & = & \overline{2} \\ \overline{3}^3 & = & \overline{6} \\ \overline{3}^4 & = & \overline{4} \\ \overline{3}^5 & = & \overline{5} \\ \overline{3}^6 & = & \overline{1} \end{array}$$

$\overline{4}$ is not a primitive root because the positive powers of $\overline{4}$ do not give us all of $\mathbb{Z}_7^\times$. Here are the first few positive powers of $\overline{4}$:

$$\begin{array}{rcl} \overline{4}^1 & = & \overline{4} \\ \overline{4}^2 & = & \overline{2} \\ \overline{4}^3 & = & \overline{1} \\ \overline{4}^4 & = & \overline{4} \\ \overline{4}^5 & = & \overline{2} \\ \overline{4}^6 & = & \overline{1} \\ \vdots & & \vdots \end{array}$$

Note how the powers keep repeating $\overline{4}$, $\overline{2}$, and $\overline{1}$ forever.

$\overline{5}$ is a primitive root because we get all of the elements of $\mathbb{Z}_7^\times$ from the positive powers of $\overline{5}$ as we see below:

$$\begin{aligned}
\overline{5}^1 &= \overline{5}\\
\overline{5}^2 &= \overline{4}\\
\overline{5}^3 &= \overline{6}\\
\overline{5}^4 &= \overline{2}\\
\overline{5}^5 &= \overline{3}\\
\overline{5}^6 &= \overline{1}
\end{aligned}$$

$\overline{6}$ is not a primitive root because the positive powers of $\overline{6}$ do not give us all of $\mathbb{Z}_7^\times$. Here are the first few positive powers of $\overline{6}$:

$$\begin{aligned}
\overline{6}^1 &= \overline{6}\\
\overline{6}^2 &= \overline{1}\\
\overline{6}^3 &= \overline{6}\\
\overline{6}^4 &= \overline{1}\\
\overline{6}^5 &= \overline{6}\\
\overline{6}^6 &= \overline{1}\\
\vdots & \quad \vdots
\end{aligned}$$

Note how the powers keep repeating $\overline{6}$, $\overline{1}$ forever.

Therefore, the only primitive roots in $\mathbb{Z}_7^\times$ are $\overline{3}$ and $\overline{5}$.

5. Find all of the primitive roots for $\mathbb{Z}_{14}^\times$. How many are there?

   **Solution:** $\mathbb{Z}_{14}^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}\}$.

   The primitive roots are $\overline{3}$ and $\overline{5}$.

6. Find all of the primitive roots for $\mathbb{Z}_9^\times$. How many are there?

   **Solution:** $\mathbb{Z}_9^\times = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$.

   The primitive roots are $\overline{2}$ and $\overline{5}$.

7. Find all of the primitive roots for $\mathbb{Z}_{20}^\times$. How many are there?

**Solution:** Recall that there exists a primitive root of $\mathbb{Z}_n^\times$ if and only if $n$ is of the form $n = 2, 4, p^k,$ or $2p^l$ where $p$ is an odd prime. Here we have that $n = 20 = 2^2 \cdot 5$. Therefore, $\mathbb{Z}_{20}^\times$ has no primitive roots.

8. Reduce $\overline{7}^{103}$ in $\mathbb{Z}_{13}$.

   **Solution:** Note that 13 is prime. Therefore, by Fermat's theorem, since $\gcd(7, 13) = 1$ we have that $\overline{7}^{12} = \overline{7}^{13-1} = \overline{1}$ in $\mathbb{Z}_{13}$. Dividing 12 into 103 gives $103 = 8 \cdot 12 + 7$. Hence

$$\begin{aligned}
\overline{7}^{103} &= \overline{7}^{8\cdot 12+7} \\
&= (\overline{7}^{12})^8 \cdot \overline{7}^{2+2+2+1} \\
&= \overline{1} \cdot \overline{49} \cdot \overline{49} \cdot \overline{49} \cdot \overline{7} \\
&= \overline{10} \cdot \overline{10} \cdot \overline{10} \cdot \overline{7} \\
&= \overline{7000}
\end{aligned}$$

   Note that $7000 = 538 \cdot 13 + 6$. Hence

$$\overline{7}^{103} = \overline{7000} = \overline{538} \cdot \overline{13} + \overline{6} = \overline{538} \cdot \overline{0} + \overline{6} = \overline{6}$$

9. Reduce $\overline{5}^{127}$ in $\mathbb{Z}_{12}$.

   **Solution:** Note that

$$\phi(12) = |\mathbb{Z}_{12}^\times| = |\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}| = 4.$$

   By Euler's theorem, since $\gcd(5, 12) = 1$, we have that $\overline{5}^{\phi(12)} = \overline{5}^4 = \overline{1}$ in $\mathbb{Z}_{12}$. Dividing 4 into 127 gives $127 = 31 \cdot 4 + 3$. Hence

$$\begin{aligned}
\overline{5}^{127} &= \overline{5}^{31\cdot 4+3} \\
&= (\overline{5}^4)^{31} \cdot \overline{5}^3 \\
&= \overline{1} \cdot \overline{125} \\
&= \overline{125}
\end{aligned}$$

   Note that $125 = 10 \cdot 12 + 5$. Hence

$$\overline{5}^{127} = \overline{125} = \overline{10} \cdot \overline{12} + \overline{5} = \overline{10} \cdot \overline{0} + \overline{5} = \overline{5}$$

10. (a) Let $p$ be a prime and let $\overline{x} \in \mathbb{Z}_p^\times$. Prove that $\overline{x}^{p-2}$ is the multiplicative inverse of $\overline{x}$ in $\mathbb{Z}_p^\times$.

**Solution:** Suppose that $\overline{x} \in \mathbb{Z}_p^\times$. By Fermat's theorem, we have that $\overline{x}^{p-1} = \overline{1}$. Hence $\overline{x} \cdot \overline{x}^{p-2} = \overline{1}$. Therefore, the multiplicative inverse of $\overline{x}$ is $\overline{x}^{p-2}$.

(b) Use (10a) to find the multiplicative inverse of $\overline{2}$ in $\mathbb{Z}_7$.

**Solution:** By (10a), the multiplicative inverse of $\overline{2}$ is

$$\overline{2}^{7-2} = \overline{2}^5 = \overline{32} = \overline{4} \cdot \overline{7} + \overline{4} = \overline{4} \cdot \overline{0} + \overline{4} = \overline{4}.$$

(c) Use (10a) to find the multiplicative inverse of $\overline{3}$ in $\mathbb{Z}_{11}$.

**Solution:** By (10a), the multiplicative inverse of $\overline{3}$ is

$$\begin{aligned} \overline{3}^{11-2} &= \overline{3}^9 = \overline{3}^3 \cdot \overline{3}^3 \cdot \overline{3}^3 = \overline{27} \cdot \overline{27} \cdot \overline{27} = \overline{5} \cdot \overline{5} \cdot \overline{5} \\ &= \overline{125} = \overline{11} \cdot \overline{11} + \overline{4} = \overline{0} \cdot \overline{0} + \overline{4} = \overline{4} \end{aligned}$$

11. Let $p$ be a prime and let $m$ and $n$ be positive integers. Let $\overline{a} \in \mathbb{Z}_p^\times$. Prove that if $m \equiv n (\text{mod } p-1)$, then $\overline{a}^m = \overline{a}^n$ in $\mathbb{Z}_p^\times$.

**Solution:** Let $\overline{a} \in \mathbb{Z}_p^\times$. By Fermat's theorem, $\overline{a}^{p-1} = \overline{1}$ in $\mathbb{Z}_p^\times$. Since $m \equiv n (\text{mod } p-1)$ we have that $m = n + (p-1)k$ for some integer $k$. Therefore

$$\overline{a}^m = \overline{a}^{n+(p-1)k} = \overline{a}^n \cdot (\overline{a}^{p-1})^k = \overline{a}^n \cdot \overline{1}^k = \overline{a}^n.$$

Hence $\overline{a}^m = \overline{a}^n$.

12. Prove that $a^{6k} - 1$ is divisible by 7 for any positive integer $a$ with $\gcd(a, 7) = 1$.

**Solution:** Let $a$ be an integer with $\gcd(a, 7) = 1$. Since 7 is prime, by Fermat, we have that $\overline{1} = \overline{a}^{7-1} = \overline{a}^6$. Hence

$$\overline{a^{6k} - 1} = (\overline{a}^6)^k + \overline{-1} = \overline{1} + \overline{-1} = \overline{0}.$$

Thus $\overline{a^{6k} - 1} = \overline{0}$ in $\mathbb{Z}_7^\times$. Therefore, 7 divides $a^{6k} - 1$.

13. Prove that 19 is not a divisor of $4n^2 + 4$ for any integer $n$.

**Solution:** Suppose that 19 is a divisor of $4n^2+4$. We will show that this leads to a contradiction. Since 19 divides $4n^2+4$ we have that $4n^2+4 \equiv 0 (\text{mod } 19)$. In $\mathbb{Z}_{19}$ this gives us that

$$\overline{4n^2+4} = \overline{0}.$$

Hence

$$\overline{4} \cdot \overline{n}^2 + \overline{4} = \overline{0}.$$

Adding $\overline{15}$ to both sides we have that

$$\overline{4} \cdot \overline{n}^2 = \overline{15}.$$

Multiplying both sides by $\overline{4}^{-1} = \overline{5}$ we have that

$$\overline{5} \cdot \overline{4} \cdot \overline{n}^2 = \overline{5} \cdot \overline{15}.$$

So

$$\overline{20} \cdot \overline{n}^2 = \overline{75}.$$

Thus

$$\overline{n}^2 = \overline{3 \cdot 19 + 18}.$$

So

$$\overline{n}^2 = \overline{3} \cdot \overline{19} + \overline{18} = \overline{3} \cdot \overline{0} + \overline{18} = \overline{18}.$$

We now show that $\overline{n}^2 = \overline{18}$ has no solutions in $\mathbb{Z}_{19}$. Here is the check:

$$\begin{aligned}
\overline{1}^2 &= \overline{1} \\
\overline{2}^2 &= \overline{4} \\
\overline{3}^2 &= \overline{9} \\
\overline{4}^2 &= \overline{16} \\
\overline{5}^2 &= \overline{6} \\
\overline{6}^2 &= \overline{17} \\
\overline{7}^2 &= \overline{11} \\
\overline{8}^2 &= \overline{7} \\
\overline{9}^2 &= \overline{5} \\
\overline{10}^2 &= \overline{5} \\
\overline{11}^2 &= \overline{7} \\
\overline{12}^2 &= \overline{11} \\
\overline{13}^2 &= \overline{17} \\
\overline{14}^2 &= \overline{6} \\
\overline{15}^2 &= \overline{16} \\
\overline{16}^2 &= \overline{9} \\
\overline{17}^2 &= \overline{4} \\
\overline{18}^2 &= \overline{1}
\end{aligned}$$

Thus we have a contradiction.

14. Let $n$ be an integer with $n \geq 2$.

(a) Let $a$ be an integer with $\gcd(a, n) = 1$. Suppose that $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c}$ in $\mathbb{Z}_n$. Prove that $\overline{b} = \overline{c}$.

**Solution:** Suppose that $\gcd(a, n) = 1$ and $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c}$. Since $\gcd(a, n) = 1$ we know that $\overline{a} \in \mathbb{Z}_n^{\times}$. Therefore, $\overline{a}^{-1}$ exists. So, $\overline{a}^{-1} \cdot \overline{a} \cdot \overline{b} = \overline{a}^{-1} \cdot \overline{a} \cdot \overline{c}$. Thus, $\overline{b} = \overline{c}$.

(b) Let $a$ be an integer with $\gcd(a, n) = 1$. Prove that

$$\overline{a} \cdot \mathbb{Z}_n = \{\overline{a} \cdot \overline{0}, \overline{a} \cdot \overline{1}, \overline{a} \cdot \overline{2}, \cdots, \overline{a} \cdot \overline{(n-1)}\}$$

is equal to $\mathbb{Z}_n$.

**Solution:** Since $\gcd(a, n) = 1$ we know that $\overline{a}^{-1}$ exists in $\mathbb{Z}_n$. We now show that $\overline{a} \cdot \mathbb{Z}_n = \mathbb{Z}_n$. We do this by showing that $\overline{a} \cdot \mathbb{Z}_n \subseteq \mathbb{Z}_n$ and $\mathbb{Z}_n \subseteq \overline{a} \cdot \mathbb{Z}_n$.

Let $\overline{x} \in \overline{a} \cdot \mathbb{Z}_n$. Then $\overline{x} = \overline{a} \cdot \overline{y}$ where $\overline{y} \in \mathbb{Z}_n$. Then $\overline{x} = \overline{a \cdot y} \in \mathbb{Z}_n$. Hence $\overline{a} \cdot \mathbb{Z}_n \subseteq \mathbb{Z}_n$.

Let $\overline{s} \in \mathbb{Z}_n$. Since $\overline{s} = \overline{a} \cdot (\overline{a}^{-1} \cdot \overline{s})$ and $\overline{a}^{-1} \cdot \overline{s} \in \mathbb{Z}_n$ we have that $\overline{s} \in \overline{a} \cdot \mathbb{Z}_n$. Hence $\mathbb{Z}_n \subseteq \overline{a} \cdot \mathbb{Z}_n$.

(c) Give an example showing that if $\gcd(a, n) \neq 1$ then one can have $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c}$ in $\mathbb{Z}_n$, but $\overline{b} \neq \overline{c}$.

**Solution:** $\overline{2} \cdot \overline{4} = \overline{2} \cdot \overline{1}$ in $\mathbb{Z}_6$.

15. Prove that if $a \equiv b (\bmod\ n)$ then $\gcd(a, n) = \gcd(b, n)$.

**Solution:** Since $a \equiv b (\bmod\ n)$ we have that $a = b + qn$ for some integer $q$. Let $d = \gcd(a, n)$ and $d' = \gcd(b, n)$.

Since $d' = \gcd(b, n)$ we have that $d'|b$ and $d'|n$. Hence $d'k_1 = b$ and $d'k_2 = n$ for some integers $k_1, k_2$. Thus $a = b + qn = d'k_1 + qd'k_2 = d'(k_1 + qk_2)$. So $d'|a$. So $d'$ is a common divisor of $a$ and $n$. Since $\gcd(a, n) = d$ we must have that $d' \leq d$.

Since $d = \gcd(a, n)$ we have that $d|a$ and $d|n$. Hence $dt_1 = a$ and $dt_2 = n$ for some integers $t_1, t_2$. Thus $b = a - qn = dt_1 - qdt_2 = d(t_1 - qt_2)$. So $d|b$. So $d$ is a common divisor of $b$ and $n$. Since $\gcd(b, n) = d'$ we must have that $d \leq d'$.

Since $d' \leq d$ and $d \leq d'$ we have that $d = d'$.