Math 446 - Homework # 5

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

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

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

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

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

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

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

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

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

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 $\mathbb{Z}_p^\times$.

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

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

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 $m \equiv n (\mathrm{mod}\ p-1)$, then $\overline{a}^m = \overline{a}^n$ in $\mathbb{Z}_p^\times$.

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

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

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 $\overline{b} = \overline{c}$.

(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 $\mathbb{Z}_n$.

(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 $\overline{b}\neq\overline{c}$.

15. Prove that if $a\equiv b(\text{mod } n)$ then $\gcd(a,n)=\gcd(b,n)$.