# Homework 5

1. Let $m \geq 2$ and set $\mathbb{Z}_m^* := \{k \in \mathbb{Z}_m : \gcd(k, m) = 1\}$.

   a. First we show that every element of $\mathbb{Z}_m^*$ generates $\mathbb{Z}_m$. We want to show there are $m$ distinct cosets in the cyclic subgroup generated by $k$. Let $n$ be the smallest positive integer such that $nk + m\mathbb{Z} = m\mathbb{Z}$. Then $nk$ is the least common multiple of $k$ and $m$. But since $\gcd(k, m) = 1$, we must have $nk = mk$ and $n = m$. Then $k$ generates $\mathbb{Z}_m$.

      Now take some element $l$ such that $\gcd(l, m) > 1$. Then there is some $r$ such that $m = nr$ and $l = pr$. Then $nl$ is a multiple of both $l$ and $m$, and $n < m$. Then $n$ is the order of $l$, and $l$ does not generate $\mathbb{Z}_m$.

   b. We will show $\mathbb{Z}_m^*$ is a group under multiplication. Clearly it contains the identity 1 since $\gcd(1, m) = 1$. To show inverses, let $n \in \mathbb{Z}_m^*$. Then by applying the euclidean algorithm, there are integers $a$ and $b$ such that $an + bm = 1$ and thus $an = 1 - bm$. Then we have $an + m\mathbb{Z} = 1 + m\mathbb{Z}$, and inverse of $a$ is $n$ in $\mathbb{Z}_m^*$.

      Finally suppose $a, b \in \mathbb{Z}_m^*$. If $p$ is a prime which divides $m$ and $ab$, then $p$ must divide either $a$ or $b$. But this is impossible. Then $ab \in \mathbb{Z}_m^*$.

   c. Suppose $\gcd(a, m) = 1$. Then any element of $a + m\mathbb{Z}$ is also relatively prime with $m$, and thus $a + m\mathbb{Z}$ generates $\mathbb{Z}_m^*$. Then the cyclic group generated by $a + m\mathbb{Z}$ under multiplication must be at most order $m$, and thus $(a + m\mathbb{Z})^{\varphi(m)} = 1 + m\mathbb{Z}$, where $\varphi(m)$ is the order of $\mathbb{Z}_m^*$. But $(a + m\mathbb{Z})^{\varphi(m)} = a^{\varphi(m)} + m\mathbb{Z} = 1 + m\mathbb{Z}$, and we have $a^{\varphi(m)} \equiv m \mod m$.

   d. Suppose $\gcd(a, b) = 1$. Then $\mathbb{Z}_a \times \mathbb{Z}_b$ is a group of order $ab$. Moreover, the order of the element $(1_a, 1_b)$ is the least common multiple of the orders $a$ and $b$ of $1_a$ and $1_b$, which must be $ab$. We have shown $(1, 1)$ generates $\mathbb{Z}_a \times \mathbb{Z}_b$, and thus $\mathbb{Z}_a \times \mathbb{Z}_b$ is a cyclic group isomorphic to $\mathbb{Z}_{ab}$.

      Then $\mathbb{Z}_a \times \mathbb{Z}_b$ has the same number of generators as $\mathbb{Z}_{ab}$. Let $p \in \mathbb{Z}_a$ and $q \in \mathbb{Z}_b$ both be generators with order $a$ and $b$ respectively. By homework 2 problem 3, the order of $(p, q)$ is the least common multiple of $a$ and $b$, $ab$. Then $(p, q)$ generates $\mathbb{Z}_a \times \mathbb{Z}_b$, along with every other pair of generators. Then there are $\varphi(a)\varphi(b)$ generators of $\mathbb{Z}_a \times \mathbb{Z}_b$ and thus of $\mathbb{Z}_{ab}$. Finally, we have shown that this number is precisely $\varphi(ab)$, so that $\varphi(ab) = \varphi(a)\varphi(b)$.

      Let $p$ be a prime number. Then the only divisors of $p$ are itself and one. Then every number $1, 2, \dots, p-1$ is relatively prime with $p$ and $\varphi(p) = p - 1$.

      To calculate $\varphi(p^n)$, note that if we have $\gcd(m, p^n) > 1$ for some $1 \leq m \leq p^n$, then $m$ must be a multiple of $p$ less than or equal to $p^n$. There are $p^{n-1}$ such numbers. Then the remaining $p^n - p^{n-1}$ numbers are relatively prime to $p^n$ and $\varphi(p^n) = p^n - p^{n-1}$.

      Combining the above results, let $m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$. In the above result, notice that $\varphi(p^n) = p^n - p^{n-1} = p^n(1 - \frac{1}{p})$. Then we can write

      $$\varphi(m) = \prod_{i=1}^{n} \varphi(p_i^{a_i}) = \prod_{i=1}^{n} p_i^{a_i}(1 - \frac{1}{p_i}) = m \prod_{i=1}^{n}(1 - \frac{1}{p_i}).$$

      Let $a \in \mathbb{Z}$ and let $p$ be prime. If $a$ is a multiple of $p$, we have

      $$a^p \equiv 0 \bmod p = a \bmod p.$$

      Otherwise, $a$ is relatively prime with $p$, and we have $a^{\varphi(p)} = a^{p-1} = 1 \bmod p$ and thus

      $$a^p = a \bmod p.$$