U_p Cyclic Proof

Sean Xiao

(Dated: June 2024)

Proof.
We'll first go through several lemmas.

Lemma 1 *If m is a prime, then a polynomial of degree n has at most n roots in $\mathbb{Z}_m[x]$. (Lagrange's theorem on roots of polynomials)*

Proof.
We use induction. Suppose the polynomial is:

$$f(x) = \sum_{i=0}^{n} a_i x^i (\mathrm{m} \nmid \mathrm{a_n})$$

When $n = 0$, since $m \nmid a_0$, then $f(x) \equiv 0 \pmod{m}$ has no solutions. Therefore the proposition holds for every polynomial whose degree is 0.
Now assume the proposition holds for every polynomial whose degree is smaller than n. Then we assume that there exists a polynomial $f(x)$ whose degree is n such that $f(x) \equiv 0 \pmod{m}$ has $n+1$ solutions $x_i (i \in [0, n])$ in $\mathbb{Z}_m[x]$.
Next we can assume there's another polynomial $g(x)$ such that $f(x) - f(x_0) = (x - x_0)g(x)$, so $\deg(g(x)) \leq n-1$. Hence, we have:

$$(x_i - x_0)g(x_i) \equiv f(x_i) - f(x_0) \equiv 0 \pmod{m}$$

for every $1 \leq i \leq n$.
But we know that $x_i \not\equiv x_0 \pmod{m}$, so $g(x_i) \equiv 0 \pmod{m}$, so $g(x) \equiv 0 \pmod{m}$ has at least n solutions, which contradicts the proposition. □

Lemma 2 *Let $p > 2$ be a prime, and let $p - 1 = \prod_{i=1}^{r} q_i^{e_i}$ be the prime factorization of $p - 1$ into powers of distinct primes. Then for each i there's an element $a_i \in \mathbb{U}_p$ of order $q_i^{e_i}$.*

Proof.
First, we need to prove that if $a \in \mathbb{U}_m$ has order k, then $k \mid \varphi(m)$.
By Euler's theorem, we can know that $a^{\varphi(m)} \equiv 1 \pmod{m}$. We know that $a^{\mathrm{ord}(a)} \equiv 1$, and by definition, $k \mid \varphi(m)$. And by UFT, we can know that if $p > 2$ is a prime, $p - 1 = q_1^{e_1} \cdots q_r^{e_r}$ is the prime factorization of $p-1$ into powers of distinct primes. Then we can know that the order of each element $a \in U_p$ is $q_1^{c_1} \cdots q_r^{c_r}$ where $c_i \leq e_i$ for each i.
Next we will prove that: Let $p > 2$ be a prime, and let $p - 1 = q_1^{e_1} \cdots q_r^{e_r}$ be the prime factorization of $p-1$ into powers of distinct primes. Then for each i there is an element $a_i \in \mathbb{U}_p$ whose order is a multiple of $q_i^{e_i}$.
We prove this for $i = 1$, the argument for general i is similar. So suppose the lemma fails for $i = 1$. Then every element of U_p has order $q_1^{c_1} \cdots q_r^{c_r}$ with $c_1 \leq e_1 - 1$ and $c_j \leq e_j$ for $j > 1$. In other words, every element has order dividing $\frac{p-1}{q_1} = q_1^{e_1 - 1} \cdots q_r^{e_r}$. Let $d = \frac{p-1}{q_1}$. Then every element of U_p is a root of $x^d - \overline{1}$. However, by Lagrange's

theorem on roots of polynomials, there are at most d roots. This is a contradiction since $\mathbb{U}_p$ has $p-1$ elements and $p-1 > d$. And since we've proved that there is an element $b_i \in \mathbb{U}_p$ of order $q^{e_i}k$ for some k, let $a_i = b_i * k$, then a_i has the order $q_i^{e_i}$. □

Now, We will move on to prove that $\mathbb{U}_p$ is cyclic.
The problem is the same as: Let p be a prime, then U_p has an element of order $\varphi(p) = p-1$.

1. $p = 2$
   The result is trivial since $\varphi(2) = 1$.

2. $p > 2$
   We will first need to prove a lemma:

   (a) theorem
   Suppose $a \in \mathbb{U}_m$ has order k_1 and $b \in \mathbb{U}_m$ has order k_2. If $(k_1, k_2) = 1$ then ab has order k_1k_2.

   (b) proof
   Let k bWe will first need to prove that ife the order of ab. First in $\mathbb{Z}_m$, we observe that:

$$(ab)^{k_1k_2} = (a)^{k_1k_2}(b)^{k_1k_2} = \left(a^{k_1}\right)^{k_2}\left(b^{k_2}\right)^{k_1} = (1)^{k_2}(1)^{k_1} = 1$$

   So we have $k \mid k_1k_2$.
   Next in $\mathbb{Z}_m$, we also observe that:

$$(ab)^{k_1k} = (a)^{k_1k}(b)^{k_1k} = \left(a^{k_1}\right)^{k}(b)^{k_1k} = (1)^{k_2}(b)^{k_1k} = (b)^{k_1k}$$

$$(ab)^{k_1k} = \left(ab^{k}\right)^{k_1} = 1^{k_1} = 1$$

   So $(b)^{k_1k} = 1$. Again, we know that $1, k_2 \mid k_1k$. Since $(k_1, k_2) = 1$, it follows that $k_2 \mid k$. Similarly, $k_1 \mid k$.
   Since $k_1 \mid k$ and $k_2 \mid k$, and since $(k_1, k_2) = 1$, it follows that $k_1k_2 \mid k$.
   Since $k_1k_2 \mid k$ and $k \mid k_1k_2$, it follows that $k = k_1k_2$.

   Then we can generate the lemma from two variables to r variables. We can use induction to prove this. Assume there are t variables. When $t = 2$, we've proved that the proposition holds. Suppose when $t = r-1 (r \in \mathbb{Z}^+$ and $r \geq 4)$ the proposition still holds, as we suppose $a_1, \cdots, a_r \in \mathbb{U}_m$ have orders $n_1, \cdots, n_r$ respectively and the n_i are pairwise relatively prime. Then when $t = r$, since we know $\gcd(\prod_{i=0}^{r-1} n_i, n_r) = 1$, the situation is the same as there are two variables which are $\prod_{i=0}^{r-1} n_i$ and n_r. Hence it still holds when $t = r$, which means that $\prod_{i=1}^{r} a_i$ has order $\prod_{j=1}^{r} n_i$.
   Now we let $p-1 = q_1^{e_1} \cdots q_r^{e_r}$ be the prime factorization of $p-1$ into powers of distinct primes. By P9 in this set there is, for each i, an element $a_i \in \mathbb{U}_p$ of order $q_i^{e_i}$.
   By the lemma we know that the element $\prod_{i=1}^{r} a_i$ has order $p-1$.

   □