$\mathbb{U}_p$, $\mathbb{U}_{p^k}$, and $\mathbb{U}_{2p^k}$ are cyclic

Matthew Li and Zack Yu

July 2023

Table of Contents

Definitions

Set of Generators

A set of generators $(g_1, \ldots, g_n)$ is a set of elements of a group G such that performing the group operation on themselves and on each other is capable of producing all the elements in the group.

Definitions

Set of Generators

A set of generators $(g_1, \ldots, g_n)$ is a set of elements of a group G such that performing the group operation on themselves and on each other is capable of producing all the elements in the group.

Cyclic Group

A cyclic group is a group that is generated by a single generator.

Motivating Example

Let us observe an example of $\mathbb{U}_p$. We will try to see if it is cyclic.

Motivating Example

Let us observe an example of $\mathbb{U}_p$. We will try to see if it is cyclic.

Example

Consider $\mathbb{U}_5$. The elements of $\mathbb{U}_5$ are 1, 2, 3, and 4. One can see that 2 is a generator of $\mathbb{U}_5$ because

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

Thus, $\mathbb{U}_5$ is cyclic.

Another Example

Not convinced? Let's consider a bigger p.

Another Example

Not convinced? Let's consider a bigger p.

Example

Consider $\mathbb{U}_{13}$. We claim that 2 is a generator of $\mathbb{U}_{13}$.

$$\begin{array}{cccc} 2^1 = 2 & 2^4 = 3 & 2^7 = 11 & 2^{10} = 10 \\ 2^2 = 4 & 2^5 = 6 & 2^8 = 9 & 2^{11} = 7 \\ 2^3 = 8 & 2^6 = 12 & 2^9 = 5 & 2^{12} = 1 \end{array}$$

Proof Sketch of $\mathbb{U}_p$ Cyclic

We need a couple of important results before starting.

Proof Sketch of $\mathbb{U}_p$ Cyclic

We need a couple of important results before starting.

Lagrange's Theorem

For a degree n polynomial mod p, it has at most n roots.

Proof Sketch of $\mathbb{U}_p$ Cyclic

We need a couple of important results before starting.

Lagrange's Theorem

For a degree n polynomial mod p, it has at most n roots.

Lemma 1

If $u \in \mathbb{U}_p$ has order d, then there exists $x \in \mathbb{U}_p$ such that $\mathrm{ord}_p(x) = k$, where k is a divisor of d.

Proof Sketch of $\mathbb{U}_p$ Cyclic

We need a couple of important results before starting.

Lagrange's Theorem

For a degree n polynomial mod p, it has at most n roots.

Lemma 1

If $u \in \mathbb{U}_p$ has order d, then there exists $x \in \mathbb{U}_p$ such that $\mathrm{ord}_p(x) = k$, where k is a divisor of d.

Lemma 2

If $\mathrm{ord}_p(a) = r$, $\mathrm{ord}_p(b) = s$, and $\gcd(r, s) = 1$, then $\mathrm{ord}_p(ab) = rs$.

Proof Sketch of $\mathbb{U}_p$ Cyclic

- We wish to show there is $u \in \mathbb{U}_p$ of order $p - 1$.

Proof Sketch of $\mathbb{U}_p$ Cyclic

- We wish to show there is $u \in \mathbb{U}_p$ of order $p-1$.
- $p - 1 = q_1^{e_1} \cdots q_k^{e_k}$

Proof Sketch of $\mathbb{U}_p$ Cyclic

- We wish to show there is $u \in \mathbb{U}_p$ of order $p-1$.
- $p-1 = q_1^{e_1} \cdots q_k^{e_k}$
- There is $w \in \mathbb{U}_p$ such that $w^{\frac{p-1}{q_i}} \neq 1$ in $\mathbb{U}_p$.

Proof Sketch of $\mathbb{U}_p$ Cyclic

- We wish to show there is $u \in \mathbb{U}_p$ of order $p-1$.
- $p-1 = q_1^{e_1} \cdots q_k^{e_k}$
- There is $w \in \mathbb{U}_p$ such that $w^{\frac{p-1}{q_i}} \neq 1$ in $\mathbb{U}_p$.
- For sake of contradiction, assume all $w \in \mathbb{U}_p$ satisfy above. Then, we get contradiction from Lagrange.

Proof Sketch of $\mathbb{U}_p$ Cyclic

- We wish to show there is $u \in \mathbb{U}_p$ of order $p-1$.
- $p-1 = q_1^{e_1} \cdots q_k^{e_k}$
- There is $w \in \mathbb{U}_p$ such that $w^{\frac{p-1}{q_i}} \neq 1$ in $\mathbb{U}_p$.
- For sake of contradiction, assume all $w \in \mathbb{U}_p$ satisfy above. Then, we get contradiction from Lagrange.
- So order of w should not divide $\frac{p-1}{q_i}$. Thus, all orders must be divisible by $q_i^{e_i}$.

Proof Sketch of $\mathbb{U}_p$ Cyclic

- We wish to show there is $u \in \mathbb{U}_p$ of order $p-1$.
- $p - 1 = q_1^{e_1} \cdots q_k^{e_k}$
- There is $w \in \mathbb{U}_p$ such that $w^{\frac{p-1}{q_i}} \neq 1$ in $\mathbb{U}_p$.
- For sake of contradiction, assume all $w \in \mathbb{U}_p$ satisfy above. Then, we get contradiction from Lagrange.
- So order of w should not divide $\frac{p-1}{q_i}$. Thus, all orders must be divisible by $q_i^{e_i}$.
- Thus, there is $x \in \mathbb{U}_p$ of order $q_i^{e_i}$ by Lemma 1.

Proof Sketch of $\mathbb{U}_p$ Cyclic

- We wish to show there is $u \in \mathbb{U}_p$ of order $p-1$.
- $p - 1 = q_1^{e_1} \cdots q_k^{e_k}$
- There is $w \in \mathbb{U}_p$ such that $w^{\frac{p-1}{q_i}} \neq 1$ in $\mathbb{U}_p$.
- For sake of contradiction, assume all $w \in \mathbb{U}_p$ satisfy above. Then, we get contradiction from Lagrange.
- So order of w should not divide $\frac{p-1}{q_i}$. Thus, all orders must be divisible by $q_i^{e_i}$.
- Thus, there is $x \in \mathbb{U}_p$ of order $q_i^{e_i}$ by Lemma 1.
- We repeat this process for all i so $\mathrm{ord}_p(w_i) = q_i^{e_i}$ for all i.

Proof Sketch of $\mathbb{U}_p$ Cyclic

- We wish to show there is $u \in \mathbb{U}_p$ of order $p-1$.
- $p - 1 = q_1^{e_1} \cdots q_k^{e_k}$
- There is $w \in \mathbb{U}_p$ such that $w^{\frac{p-1}{q_i}} \neq 1$ in $\mathbb{U}_p$.
- For sake of contradiction, assume all $w \in \mathbb{U}_p$ satisfy above. Then, we get contradiction from Lagrange.
- So order of w should not divide $\frac{p-1}{q_i}$. Thus, all orders must be divisible by $q_i^{e_i}$.
- Thus, there is $x \in \mathbb{U}_p$ of order $q_i^{e_i}$ by Lemma 1.
- We repeat this process for all i so $\mathrm{ord}_p(w_i) = q_i^{e_i}$ for all i.
- Then, by Lemma 2, $\mathrm{ord}_p(w_1 \cdots w_i) = p - 1$, as desired.

Examples

It is not immediately obvious that $\mathbb{U}_{p^k}$ is cyclic for all odd primes p.

Examples

It is not immediately obvious that $\mathbb{U}_{p^k}$ is cyclic for all odd primes p.

Example

Consider $\mathbb{U}_{3^2}$. The elements of $\mathbb{U}_9$ are 1, 2, 4, 5, 7, and 8. We claim that 5 is a generator.

$$\begin{array}{ll} 5^1 = 5 & 5^4 = 4 \\ 5^2 = 7 & 5^5 = 2 \\ 5^3 = 8 & 5^6 = 1 \end{array}$$

Examples

Consider $\mathbb{U}_{3^3}$. Through some tedious computation we can show 5 is also a generator of $\mathbb{U}_{3^3}$.

Examples

Consider $\mathbb{U}_{3^3}$. Through some tedious computation we can show 5 is also a generator of $\mathbb{U}_{3^3}$.

Example

$$
\begin{array}{cc}
5^1 = 5 & 5^{10} = 22 \\
5^2 = 25 & 5^{11} = 2 \\
5^3 = 17 & 5^{12} = 10 \\
5^4 = 4 & 5^{13} = 23 \\
5^5 = 20 & 5^{14} = 7 \\
5^6 = 19 & 5^{15} = 8 \\
5^7 = 14 & 5^{16} = 13 \\
5^8 = 16 & 5^{17} = 11 \\
5^9 = 26 & 5^{18} = 1
\end{array}
$$

Proof Attempt

- One idea is to try the same approach we used in $\mathbb{U}_p$. What's wrong with this?

Proof Attempt

- One idea is to try the same approach we used in $\mathbb{U}_p$. What's wrong with this?
- Notice that in proving Lagrange's Theorem, we required the property in $\mathbb{Z}_p$ that if $ab = 0$, then $a = 0$ or $b = 0$.

Motivating the Proof

- We know that $|\mathbb{U}_{p^k}| = \varphi(p^k) = p^{k-1}(p-1)$

Motivating the Proof

- We know that $|\mathbb{U}_{p^k}| = \varphi(p^k) = p^{k-1}(p-1)$
- We want to find a generator or an element of order $p^{k-1}(p-1)$

Motivating the Proof

- We know that $|\mathbb{U}_{p^k}| = \varphi(p^k) = p^{k-1}(p-1)$
- We want to find a generator or an element of order $p^{k-1}(p-1)$
- Since $\gcd(p^{k-1}, p-1) = 1$, if we can find find elements of order p^{k-1} and order $p-1$, their product should have order $p^{k-1}(p-1)$

Motivating Example

Example

Consider 4 and $2 \in \mathbb{U}_9$.

$$\begin{array}{ll} 4^1 = 4 & 2^1 = 2 \\ 4^2 = 7 & 2^2 = 4 \\ 4^3 = 1 & 2^3 = 8 \\ & 2^4 = 7 \\ & 2^5 = 5 \\ & 2^6 = 1 \end{array}$$

Therefore $\mathrm{ord}_9(4) = 3 = 3^{2-1}$ and $\mathrm{ord}_9(8) = 2 = (3-1)$.
Then, the product 5 should have order $3^{2-1}(3-1) = 6$ and should be a generator of $\mathbb{U}_{p^2}$. We have already showed this.

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We will first find an element of order $p-1$

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We will first find an element of order $p - 1$
- Consider a generator g of $\mathbb{U}_p$

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We will first find an element of order $p-1$
- Consider a generator g of $\mathbb{U}_p$
- Let us say $\mathrm{ord}_{p^k}(g) = d$

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We will first find an element of order $p-1$
- Consider a generator g of $\mathbb{U}_p$
- Let us say $\mathrm{ord}_{p^k}(g) = d$
- Since we know $g^d \equiv 1 \mod p^k$, we know $g^d \equiv 1 \mod p$, so $p-1 \mid d$

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We will first find an element of order $p-1$
- Consider a generator g of $\mathbb{U}_p$
- Let us say $\operatorname{ord}_{p^k}(g) = d$
- Since we know $g^d \equiv 1 \mod p^k$, we know $g^d \equiv 1 \mod p$, so $p-1 \mid d$
- Then, by one of our earlier lemma's, we know there must exist an element with order $p-1$

Proving $\mathbb{U}_{p^k}$ is Cyclic

- Now, let us find an element of order p^{k-1}

Proving $\mathbb{U}_{p^k}$ is Cyclic

- Now, let us find an element of order p^{k-1}
- For some motivation, first consider $\mathbb{U}_{p^2}$

Proving $\mathbb{U}_{p^k}$ is Cyclic

- Now, let us find an element of order p^{k-1}
- For some motivation, first consider $\mathbb{U}_{p^2}$
- Assume x is the order of $p+1$ in $\mathbb{U}_{p^2}$, then $(p+1)^x \equiv 1 \mod p^2$

Proving $\mathbb{U}_{p^k}$ is Cyclic

- Now, let us find an element of order p^{k-1}
- For some motivation, first consider $\mathbb{U}_{p^2}$
- Assume x is the order of $p+1$ in $\mathbb{U}_{p^2}$, then $(p+1)^x \equiv 1 \mod p^2$
- By expanding $(p+1)^x$ with binomial theorem, we get

$$(p+1)^x = \binom{x}{0}p^x + \binom{x}{1}p^{x-1} + \cdots + \binom{x}{x-1}p + \binom{x}{x}1$$

Proving $\mathbb{U}_{p^k}$ is Cyclic

- Now, let us find an element of order p^{k-1}
- For some motivation, first consider $\mathbb{U}_{p^2}$
- Assume x is the order of $p+1$ in $\mathbb{U}_{p^2}$, then $(p+1)^x \equiv 1 \mod p^2$
- By expanding $(p+1)^x$ with binomial theorem, we get

$$(p+1)^x = \binom{x}{0}p^x + \binom{x}{1}p^{x-1} + \cdots + \binom{x}{x-1}p + \binom{x}{x}1$$

- Thus, we have $(p+1)^x \equiv px + 1 \mod p^2$ since all terms with p^2 disappear

Proving $\mathbb{U}_{p^k}$ is Cyclic

- Now, let us find an element of order p^{k-1}
- For some motivation, first consider $\mathbb{U}_{p^2}$
- Assume x is the order of $p+1$ in $\mathbb{U}_{p^2}$, then $(p+1)^x \equiv 1 \mod p^2$
- By expanding $(p+1)^x$ with binomial theorem, we get

$$(p+1)^x = \binom{x}{0}p^x + \binom{x}{1}p^{x-1} + \cdots + \binom{x}{x-1}p + \binom{x}{x}1$$

- Thus, we have $(p+1)^x \equiv px + 1 \mod p^2$ since all terms with p^2 disappear
- Then, we get $x \equiv 0 \mod p$ or $p \mid x$

Proving $\mathbb{U}_{p^k}$ is Cyclic

- Now, let us find an element of order p^{k-1}
- For some motivation, first consider $\mathbb{U}_{p^2}$
- Assume x is the order of $p+1$ in $\mathbb{U}_{p^2}$, then $(p+1)^x \equiv 1 \mod p^2$
- By expanding $(p+1)^x$ with binomial theorem, we get

$$(p+1)^x = \binom{x}{0}p^x + \binom{x}{1}p^{x-1} + \cdots + \binom{x}{x-1}p + \binom{x}{x}1$$

- Thus, we have $(p+1)^x \equiv px + 1 \mod p^2$ since all terms with p^2 disappear
- Then, we get $x \equiv 0 \mod p$ or $p \mid x$
- Since x is the order of $p+1$ and $p \mid x$, there is another element h with order p

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We construct a set $A = \{k \in \mathbb{Z}^+ \mid \text{the order of } p+1 \text{ in } \mathbb{U}_{p^k} \text{ is not } np^{k-1} \text{ for an integer } n\}$

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We construct a set $A = \{k \in \mathbb{Z}^+ \mid \text{the order of } p+1 \text{ in } \mathbb{U}_{p^k} \text{ is not } np^{k-1} \text{ for an integer } n\}$
- By WOP, there is a minimum element l of this set

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We construct a set $A = \{k \in \mathbb{Z}^+ \mid$ the order of $p+1$ in $\mathbb{U}_{p^k}$ is not np^{k-1} for an integer $n\}$
- By WOP, there is a minimum element l of this set
- Therefore, the order of $p+1$ in $\mathbb{U}_{p^{l-1}}$ is ap^{l-2}, for some integer a

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We construct a set $A = \{k \in \mathbb{Z}^+ \mid \text{the order of } p+1 \text{ in } \mathbb{U}_{p^k} \text{ is not } np^{k-1} \text{ for an integer } n\}$
- By WOP, there is a minimum element l of this set
- Therefore, the order of $p+1$ in $\mathbb{U}_{p^{l-1}}$ is ap^{l-2}, for some integer a
- We know if $(p+1)^x \equiv 1 \mod p^l$ then $(p+1)^x \equiv 1 \mod p^{l-1}$

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We construct a set $A = \{k \in \mathbb{Z}^+ \mid \text{the order of } p+1 \text{ in } \mathbb{U}_{p^k} \text{ is not } np^{k-1} \text{ for an integer } n\}$
- By WOP, there is a minimum element l of this set
- Therefore, the order of $p+1$ in $\mathbb{U}_{p^{l-1}}$ is ap^{l-2}, for some integer a
- We know if $(p+1)^x \equiv 1 \mod p^l$ then $(p+1)^x \equiv 1 \mod p^{l-1}$
- Then $ap^{l-2} \mid x$ or $x = bap^{l-2}$ for some integer b

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We construct a set $A = \{k \in \mathbb{Z}^+ \mid$ the order of $p+1$ in $\mathbb{U}_{p^k}$ is not np^{k-1} for an integer $n\}$
- By WOP, there is a minimum element l of this set
- Therefore, the order of $p+1$ in $\mathbb{U}_{p^{l-1}}$ is ap^{l-2}, for some integer a
- We know if $(p+1)^x \equiv 1 \mod p^l$ then $(p+1)^x \equiv 1 \mod p^{l-1}$
- Then $ap^{l-2} \mid x$ or $x = bap^{l-2}$ for some integer b
- Now, we can expand $(p+1)^x$ and obtain $xp + 1 \equiv 1 (modp^l)$ from binomial theorem

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We construct a set $A = \{k \in \mathbb{Z}^+ \mid$ the order of $p+1$ in $\mathbb{U}_{p^k}$ is not np^{k-1} for an integer $n\}$
- By WOP, there is a minimum element l of this set
- Therefore, the order of $p+1$ in $\mathbb{U}_{p^{l-1}}$ is ap^{l-2}, for some integer a
- We know if $(p+1)^x \equiv 1 \mod p^l$ then $(p+1)^x \equiv 1 \mod p^{l-1}$
- Then $ap^{l-2} \mid x$ or $x = bap^{l-2}$ for some integer b
- Now, we can expand $(p+1)^x$ and obtain $xp + 1 \equiv 1 (modp^l)$ from binomial theorem
- Thus $x = np^{l-1}$, which contradicts $l \in A$

Proving $\mathbb{U}_{p^k}$ is Cyclic

- We construct a set $A = \{k \in \mathbb{Z}^+ \mid$ the order of $p+1$ in $\mathbb{U}_{p^k}$ is not np^{k-1} for an integer $n\}$
- By WOP, there is a minimum element l of this set
- Therefore, the order of $p+1$ in $\mathbb{U}_{p^{l-1}}$ is ap^{l-2}, for some integer a
- We know if $(p+1)^x \equiv 1 \mod p^l$ then $(p+1)^x \equiv 1 \mod p^{l-1}$
- Then $ap^{l-2} \mid x$ or $x = bap^{l-2}$ for some integer b
- Now, we can expand $(p+1)^x$ and obtain $xp + 1 \equiv 1 (modp^l)$ from binomial theorem
- Thus $x = np^{l-1}$, which contradicts $l \in A$
- Then, there is an element with order p^{k-1}

Finishing the Proof

By multiplying the elements of order p^{k-1} and $p-1$, we obtain an element of order $p^{k-1}(p-1)$, which generates $\mathbb{U}_{p^k}$, yay!

Examples

Let us try to convince ourselves $\mathbb{U}_{2p^k}$ is cyclic for all odd primes p.

Example

Consider $\mathbb{U}_{2.3}$. We know the elements of $\mathbb{U}_6$ are 1 and 5. Clearly, the element 5 generates $\mathbb{U}_6$.

Consider $\mathbb{U}_{2.3^2}$. Then, we claim 5 is a generator.

$$\begin{array}{cc} 5^1 = 5 & 5^4 = 13 \\ 5^2 = 7 & 5^5 = 11 \\ 5^3 = 17 & 5^6 = 1 \end{array}$$

Motivating the Proof

- $\mathbb{U}_{2p^k}$ is not something we are very familiar with, let's see if we can find an isomorphism to something "simpler" that we can work with

Motivating the Proof

- $\mathbb{U}_{2p^k}$ is not something we are very familiar with, let's see if we can find an isomorphism to something "simpler" that we can work with
- Recall that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

Motivating the Proof

- $\mathbb{U}_{2p^k}$ is not something we are very familiar with, let's see if we can find an isomorphism to something "simpler" that we can work with
- Recall that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$
- Since $\gcd(2, p^k) = 1$, we are motivated to see if there is an isomorphism between $\mathbb{U}_2 \times \mathbb{U}_{p^k}$ and $\mathbb{U}_{2p^k}$

Motivating the Proof

- $\mathbb{U}_{2p^k}$ is not something we are very familiar with, let's see if we can find an isomorphism to something "simpler" that we can work with
- Recall that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$
- Since $\gcd(2, p^k) = 1$, we are motivated to see if there is an isomorphism between $\mathbb{U}_2 \times \mathbb{U}_{p^k}$ and $\mathbb{U}_{2p^k}$
- Notice that $\mathbb{U}_2 \times \mathbb{U}_{p^k}$ is very nice to work with since the elements are just $(1, x)$ where x is an element of $\mathbb{U}_{p^k}$

Motivating the Proof

- $\mathbb{U}_{2p^k}$ is not something we are very familiar with, let's see if we can find an isomorphism to something "simpler" that we can work with
- Recall that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$
- Since $\gcd(2, p^k) = 1$, we are motivated to see if there is an isomorphism between $\mathbb{U}_2 \times \mathbb{U}_{p^k}$ and $\mathbb{U}_{2p^k}$
- Notice that $\mathbb{U}_2 \times \mathbb{U}_{p^k}$ is very nice to work with since the elements are just $(1, x)$ where x is an element of $\mathbb{U}_{p^k}$
- Thus, $\mathbb{U}_2 \times \mathbb{U}_{p^k}$ is basically identical to $\mathbb{U}_{p^k}$.

Motivating the Proof

- $\mathbb{U}_{2p^k}$ is not something we are very familiar with, let's see if we can find an isomorphism to something "simpler" that we can work with
- Recall that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$
- Since $\gcd(2, p^k) = 1$, we are motivated to see if there is an isomorphism between $\mathbb{U}_2 \times \mathbb{U}_{p^k}$ and $\mathbb{U}_{2p^k}$
- Notice that $\mathbb{U}_2 \times \mathbb{U}_{p^k}$ is very nice to work with since the elements are just $(1, x)$ where x is an element of $\mathbb{U}_{p^k}$
- Thus, $\mathbb{U}_2 \times \mathbb{U}_{p^k}$ is basically identical to $\mathbb{U}_{p^k}$.
- So, we know $\mathbb{U}_2 \times \mathbb{U}_{p^k}$ is cyclic and if $\mathbb{U}_2 \times \mathbb{U}_{p^k} \cong \mathbb{U}_{2p^k}$, we know $\mathbb{U}_{2p^k}$ is cyclic

Establishing the Isomorphisms

- First, we show that $\mathbb{U}_{2p^k} \cong \mathbb{U}_2 \times \mathbb{U}_{p^k}$

Establishing the Isomorphisms

- First, we show that $\mathbb{U}_{2p^k} \cong \mathbb{U}_2 \times \mathbb{U}_{p^k}$
- We claim the mapping $f : \mathbb{U}_{2p^k} \to \mathbb{U}_2 \times \mathbb{U}_{p^k}$ defined by $[a]_{2p^k} \mapsto ([a]_2, [a]_{p^k})$ is bijective and satisfies $f(ab) = f(a)f(b)$.

Establishing the Isomorphisms

- First, we show that $\mathbb{U}_{2p^k} \cong \mathbb{U}_2 \times \mathbb{U}_{p^k}$
- We claim the mapping $f : \mathbb{U}_{2p^k} \to \mathbb{U}_2 \times \mathbb{U}_{p^k}$ defined by $[a]_{2p^k} \mapsto ([a]_2, [a]_{p^k})$ is bijective and satisfies $f(ab) = f(a)f(b)$.
- Note, to prove bijectivity, we only need to prove injectivity because $|\mathbb{U}_{2p^k}| = |\mathbb{U}_2 \times \mathbb{U}_{p^k}|$.

Establishing the Isomorphisms

- First, we show that $\mathbb{U}_{2p^k} \cong \mathbb{U}_2 \times \mathbb{U}_{p^k}$
- We claim the mapping $f : \mathbb{U}_{2p^k} \to \mathbb{U}_2 \times \mathbb{U}_{p^k}$ defined by $[a]_{2p^k} \mapsto ([a]_2, [a]_{p^k})$ is bijective and satisfies $f(ab) = f(a)f(b)$.
- Note, to prove bijectivity, we only need to prove injectivity because $|\mathbb{U}_{2p^k}| = |\mathbb{U}_2 \times \mathbb{U}_{p^k}|$.
- Now, we show $\mathbb{U}_2 \times \mathbb{U}_{p^k} \cong \mathbb{U}_{p^k}$.

Establishing the Isomorphisms

- First, we show that $\mathbb{U}_{2p^k} \cong \mathbb{U}_2 \times \mathbb{U}_{p^k}$
- We claim the mapping $f : \mathbb{U}_{2p^k} \to \mathbb{U}_2 \times \mathbb{U}_{p^k}$ defined by $[a]_{2p^k} \mapsto ([a]_2, [a]_{p^k})$ is bijective and satisfies $f(ab) = f(a)f(b)$.
- Note, to prove bijectivity, we only need to prove injectivity because $|\mathbb{U}_{2p^k}| = |\mathbb{U}_2 \times \mathbb{U}_{p^k}|$.
- Now, we show $\mathbb{U}_2 \times \mathbb{U}_{p^k} \cong \mathbb{U}_{p^k}$.
- Simply consider the map $f : \mathbb{U}_{p^k} \to \mathbb{U}_2 \times \mathbb{U}_{p^k}$ defined by $x \mapsto (1, x)$

Finishing the Proof

Because $\mathbb{U}_{p^k} \cong \mathbb{U}_2 \times \mathbb{U}_{p^k} \cong \mathbb{U}_{2p^k}$, we know $\mathbb{U}_{2p^k}$ is cyclic, yay!