Celebration 2 Presentation

Selina Gu, Henry Yao, Stephanie Yao

Ross Mathematics Program

October 11, 2023

Table of Contents

1. Definition of cyclic groups and generators
2. Proof of $\mathbb{U}_p$ is cyclic
3. Proof of $\mathbb{U}_{p^k}$ is cyclic
   - Inductive Case: $\mathbb{U}_{p^k}$
   - Base Case: $\mathbb{U}_{p^2}$
4. Proof of $\mathbb{U}_{2p^k}$ is cyclic for odd primes p

Is it possible to get all the other elements in a group from one specific element? And how?

example: $(\mathbb{U}_5, \cdot)$ is a group
try 2 and $\cdot$
$2^1 = 2$ $2^2 = 4$ $2^3 = 3$ $2^4 = 1$
so 2 is such a specific element
in fact, 3 is also such an element

Definition of cyclic groups and generators

Definition

A group is **cyclic** iff there is some element $g \in G$ such that
$G = \{g^n, n \in \mathbb{Z}\}$
We call g the **generator** of G.

$\mathbb{U}_p$ is cyclic

Example

$\mathbb{U}_2$ 1 is a generator
$\mathbb{U}_3$ 2 is a generator
$\mathbb{U}_4$ 3 is a generator
$\mathbb{U}_5$ 2 is a generator
$\mathbb{U}_6$ 5 is a generator
$\mathbb{U}_7$ 3 and 5 are generators
$\mathbb{U}_8$ no generator
$\mathbb{U}_9$ 2 is a generator

Conjecture

$\mathbb{U}_p$ is always cyclic.

$\mathbb{U}_p$ is cyclic

$\mathbb{U}_p$ is cyclic $\Leftarrow$ find a generator g

infinite powers of g and finite elements $\Rightarrow$ the powers of g must repeat

Definition of ord

$\text{ord}_p(g) =$ minimal length of the period
example: in $\mathbb{U}_5$
$\text{ord}_5(1) = 1$
$\text{ord}_5(2) = 4$

some properties of ord:
$g^{\text{ord}_p(g)} = 1$
$\text{ord}_p(g)$ is the smallest x such that $g^x = 1$
if $g^y = 1$ then $\text{ord}_p(g) \mid y$
the ord of any element in$\mathbb{U}_p$ are divisors of $p - 1$
if $\text{ord}_p(a) = r$ and $\text{ord}_p(b) = s$, then $\text{ord}(ab) = rs$ when $\gcd(r, s) = 1$.

WTS: $\mathrm{ord}_p(g) = p - 1$

Tthink about the properties of ord:
the 4th property
(let g be the product of some integers and also factorize $p - 1$)
let $p - 1 = q_1^{e_1} q_2^{e_2} q_3^{e_3} \cdots q_n^{e_n}$
now, we need to find $a_1, a_2, \cdots, a_n$ such that $\mathrm{ord}_p a_1 = q_1^{e_1}$, $\mathrm{ord}_p a_2 = q_2^{e_2}$,$\cdots$,$\mathrm{ord}_p a_n = q_n^{e_n}$ then $g = a_1 a_2 \ldots a_n$
stuck

go back to the beginning

we notice $\mathrm{ord}_p(g) = p - 1$
What's related to $p - 1$? FLT!
FLT: If $gcd(x, p) = 1$,then $x^{p-1} \equiv 1 mod$ p
in $\mathbb{U}_p$, all the elements are coprime to p
so $m \in \mathbb{U}_p$, $m^{p-1} \equiv 1 mod$ p so there are $p - 1$ solutions

in $\mathbb{Z}$, if we have n solutions $x_1, x_2, \ldots, x_n$ to $x^k = 1$, we can write $x^k - 1$ as $(x - x_1)(x - x_2) \cdots (x - x_n)$
check: in $\mathbb{U}_p$, the same
so $x^{p-1} - 1 = (x - 1)(x - 2) \cdots (x - (p - 1))$

recall: $p-1 = q_1^{e_1} q_2^{e_2} q_3^{e_3} \cdots q_n^{e_n}$

we know $q_i^{e_i}$ |p-1

so $x^{q_i^{e_i}} - 1$ |$x^{p-1} - 1$

so $x^{q_i^{e_i}} - 1$ can be written as $(x - c_1)(x - c_2) \cdots (x - c_{q_i^{e_i}})$

$(c_1, c_2, \cdots, c_{q_i^{e_i}} \in \mathbb{U}_p)$

$\mathrm{ord}_p c_j$ |$q_i^{e_i}$

we want | here to be $=$, which means we need to rule out $\mathrm{ord}_p c_j < q_i^{e_i}$

so find a solution to $x^{q_i^{e_i}} \equiv 1 \mod pbutnotsolutionstox^{q_i^{e_i-1}} \equiv 1 \mod p(mustexists)$

then $\mathrm{ord}_p c_j \nmid q_i^{e_i-1}$

so $\mathrm{ord}_p c_j = q_i^{e_i}$

Conclusion

Factorization of $p - 1$
FLT
factorization of $x^{p-1} - 1$
factorization of $x^{q_i^{e_i}} - 1$
find a solution a_i to $x^{q_i^{e_i}} \equiv 1 \mod p butnotsolutionstox^{q_i^{e_i - 1}} \equiv 1 \mod p$
$\mathrm{ord}_p c_j = q_i^{e_i}$
$g = a_1 a_2 \dots a_n$
$\mathbb{U}_p$ is cyclic

$\mathbb{U}_{p^k}$ is cyclic

Conjecture

If $\mathbb{U}_{p^k}$ is cyclic, then $\mathbb{U}_{p^{k+1}}$ is also cyclic.

$\mathbb{U}_{p^k}$ is cyclic

Conjecture

If $\mathbb{U}_{p^k}$ is cyclic, then $\mathbb{U}_{p^{k+1}}$ is also cyclic.

Lemma

If $a \equiv 1 \pmod{p^{k+1}}$, then $a \equiv 1 \pmod{p^k}$.

$\mathbb{U}_{p^k}$ is cyclic

Proof Outline:

1. Suppose g is a generator in $\mathbb{U}_{p^{k-1}}$, we claim that g is also a generator in $\mathbb{U}_{p^k}$.

$\mathbb{U}_{p^k}$ is cyclic

Proof Outline:

1. Suppose g is a generator in $\mathbb{U}_{p^{k-1}}$, we claim that g is also a generator in $\mathbb{U}_{p^k}$.
2. Let $\mathrm{ord}_{p^k}(g) = d$, then $\varphi(p^{k-1}) \mid d \mid \varphi(p^k)$.

$\mathbb{U}_{p^k}$ is cyclic

Proof Outline:

1. Suppose g is a generator in $\mathbb{U}_{p^{k-1}}$, we claim that g is also a generator in $\mathbb{U}_{p^k}$.
2. Let $\mathrm{ord}_{p^k}(g) = d$, then $\varphi(p^{k-1}) \mid d \mid \varphi(p^k)$.
3. If $d = \varphi(p^k)$, then we are done.

$\mathbb{U}_{p^k}$ is cyclic

Proof Outline:

1. Suppose g is a generator in $\mathbb{U}_{p^{k-1}}$, we claim that g is also a generator in $\mathbb{U}_{p^k}$.
2. Let $\mathrm{ord}_{p^k}(g) = d$, then $\varphi(p^{k-1}) \mid d \mid \varphi(p^k)$.
3. If $d = \varphi(p^k)$, then we are done.
4. If $d = \varphi(p^{k-1})$, then find a $n \in \mathbb{Z}_p$ with $\mathrm{ord}_{p^k}(g + np^{k-1}) = \varphi(p^k)$.

$\mathbb{U}_{p^k}$ is cyclic

Proof Outline:

1. Suppose g is a generator in $\mathbb{U}_{p^{k-1}}$, we claim that g is also a generator in $\mathbb{U}_{p^k}$.
2. Let $\operatorname{ord}_{p^k}(g) = d$, then $\varphi(p^{k-1}) \mid d \mid \varphi(p^k)$.
3. If $d = \varphi(p^k)$, then we are done.
4. If $d = \varphi(p^{k-1})$, then find a $n \in \mathbb{Z}_p$ with $\operatorname{ord}_{p^k}(g + np^{k-1}) = \varphi(p^k)$.
5. Use Euler's Totient Theorem and Binomial expansion to get $g^{\varphi(p^{k-1})} \equiv 1 + np^{k-1} \pmod{p^k}$

Graph

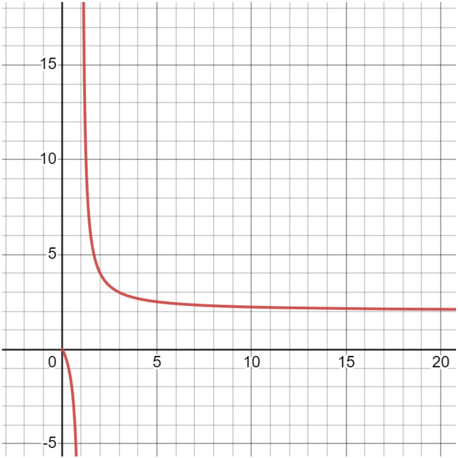

Figure: The graph of the function $k = 2 + \dfrac{2}{a-1}$, so for $k = 3$, it can divide all $(p^{k-2})^a$ when $a \geq 3$.

$\mathbb{U}_{p^k}$ is cyclic

Proof Outline:

1. Suppose g is a generator in $\mathbb{U}_{p^{k-1}}$, we claim that g is also a generator in $\mathbb{U}_{p^k}$.
2. Let $\mathrm{ord}_{p^k}(g) = d$, then $\varphi(p^{k-1}) \mid d \mid \varphi(p^k)$.
3. If $d = \varphi(p^k)$, then we are done.
4. If $d = \varphi(p^{k-1})$, then find a $n \in \mathbb{Z}_p$ with $\mathrm{ord}_{p^k}(g + np^{k-1}) = \varphi(p^k)$.
5. Use Euler's Totient Theorem and Binomial expansion to get $g^{\varphi(p^{k-1})} \equiv 1 + np^{k-1} \pmod{p^k}$ (true for $k > 2$.)

$\mathbb{U}_{p^k}$ is cyclic

Proof Outline:

1. Suppose g is a generator in $\mathbb{U}_{p^{k-1}}$, we claim that g is also a generator in $\mathbb{U}_{p^k}$.
2. Let $\mathrm{ord}_{p^k}(g) = d$, then $\varphi(p^{k-1}) \mid d \mid \varphi(p^k)$.
3. If $d = \varphi(p^k)$, then we are done.
4. If $d = \varphi(p^{k-1})$, then find a $n \in \mathbb{Z}_p$ with $\mathrm{ord}_{p^k}(g + np^{k-1}) = \varphi(p^k)$.
5. Use Euler's Totient Theorem and Binomial expansion to get $g^{\varphi(p^{k-1})} \equiv 1 + np^{k-1} \pmod{p^k}$ (true for $k > 2$.)
6. Contradiction got from $p^k \nmid np^{k-1}$, $g^{\varphi(p^{k-1})} \not\equiv 1 \pmod{p^k}$.

$\mathbb{U}_{p^2}$ is cyclic

Conjecture

If $\mathbb{U}_p$ is cyclic, then $\mathbb{U}_{p^2}$ is also cyclic.

Lemma

$$\mathrm{ord}_{p^2}(1 + p) = p$$

$\mathbb{U}_{p^2}$ is cyclic

Conjecture

If $\mathbb{U}_p$ is cyclic, then $\mathbb{U}_{p^2}$ is also cyclic.

Lemma

$$\mathrm{ord}_{p^2}(1+p) = p$$

Proof Outline:

$\mathbb{U}_{p^2}$ is cyclic

Conjecture

If $\mathbb{U}_p$ is cyclic, then $\mathbb{U}_{p^2}$ is also cyclic.

Lemma

$$\mathrm{ord}_{p^2}(1+p) = p$$

Proof Outline:

1. Use binomial expansion, $(1+p)^p \equiv 1 \pmod{p^2}$.

$\mathbb{U}_{p^2}$ is cyclic

Conjecture

If $\mathbb{U}_p$ is cyclic, then $\mathbb{U}_{p^2}$ is also cyclic.

Lemma

$$\mathrm{ord}_{p^2}(1+p) = p$$

Proof Outline:

1. Use binomial expansion, $(1+p)^p \equiv 1 \pmod{p^2}$.
2. $\mathrm{ord}_{p^2}(1+p) = p$ or 1.

$\mathbb{U}_{p^2}$ is cyclic

Conjecture

If $\mathbb{U}_p$ is cyclic, then $\mathbb{U}_{p^2}$ is also cyclic.

Lemma

$$\mathrm{ord}_{p^2}(1+p) = p$$

Proof Outline:

1. Use binomial expansion, $(1+p)^p \equiv 1 \pmod{p^2}$.
2. $\mathrm{ord}_{p^2}(1+p) = p$ or 1.
3. If $\mathrm{ord}_{p^2}(1+p) = 1 \implies$ impossible.

$\mathbb{U}_{p^2}$ is cyclic

Conjecture

If $\mathbb{U}_p$ is cyclic, then $\mathbb{U}_{p^2}$ is also cyclic.

Lemma

$$\mathrm{ord}_{p^2}(1+p) = p$$

Proof Outline:

1. Use binomial expansion, $(1+p)^p \equiv 1 \pmod{p^2}$.
2. $\mathrm{ord}_{p^2}(1+p) = p$ or 1.
3. If $\mathrm{ord}_{p^2}(1+p) = 1 \implies$ impossible.
4. $\mathrm{ord}_{p^2}(1+p) = p$. □

Proof Outline:

1. For the same reason, we have d either be p or $(p-1)p$.
2. If $d = (p-1)p \implies$

$\mathbb{U}_{p^2}$ is cyclic

Proof Outline:

1. For the same reason, we have d either be p or $(p-1)p$.
2. If $d = (p-1)p \implies$ Nice!

$\mathbb{U}_{p^2}$ is cyclic

Proof Outline:

1. For the same reason, we have d either be p or $(p-1)p$.
2. If $d = (p-1)p \implies$ Nice!
3. If $d = p - 1$, then we need another element that have order $p(p-1)$.

$\mathbb{U}_{p^2}$ is cyclic

Proof Outline:

1. For the same reason, we have d either be p or $(p-1)p$.
2. If $d = (p-1)p \implies$ Nice!
3. If $d = p - 1$, then we need another element that have order $p(p-1)$.
4. Use the fact: if $\mathrm{ord}_m(a) = r, \mathrm{ord}_m(b) = s$, $\gcd(r, s) = 1 \implies \mathrm{ord}_m(ab) = rs$.

$\mathbb{U}_{2p^k}$ is cyclic for odd primes p

Since $\mathbb{U}_{p^k}$ is cyclic, because p^k and $2p^k$ are similar. Instead of starting from scratch, we should definitely try to find if such a similarity between $\mathbb{U}_{2p^k}$ and $\mathbb{U}_{p^k}$'s generators exists as well.

Let's start out by working a couple of numerical examples to give us some idea of some possible patterns or conjectures we can make.

$$\mathbb{U}_5 - 2, 3$$
$$\mathbb{U}_{10} - 3, 7$$

$\mathbb{U}_{2p^k}$ is cyclic for odd primes p

$$\begin{array}{ll} \mathbb{U}_5 - 2, 3 & \mathbb{U}_7 - 3, 5 \\ \mathbb{U}_{10} - 3, 7 & \mathbb{U}_{14} - 3, 5 \end{array}$$

$\mathbb{U}_{2p^k}$ is cyclic for odd primes p

$$\begin{array}{ccc} \mathbb{U}_5 - 2,3 & \mathbb{U}_7 - 3,5 & \mathbb{U}_9 - 2,5 \\ \mathbb{U}_{10} - 3,7 & \mathbb{U}_{14} - 3,5 & \mathbb{U}_{18} - 5,11 \end{array}$$

$\mathbb{U}_{2p^k}$ is cyclic for odd primes p

$$\begin{array}{cccc} \mathbb{U}_5 - 2,3 & \mathbb{U}_7 - 3,5 & \mathbb{U}_9 - 2,5 & \mathbb{U}_{25} - 2,3,8,12,13,17,22,23 \\ \mathbb{U}_{10} - 3,7 & \mathbb{U}_{14} - 3,5 & \mathbb{U}_{18} - 5,11 & \mathbb{U}_{50} - 3,13,17,23,27,13,37,47 \end{array}$$

By now, we can notice a certain pattern. It seems that for all odd generators g of $\mathbb{U}_{p^k}$, g is also a generator in $\mathbb{U}_{2p^k}$. And for all even generators g of $\mathbb{U}_{p^k}$, $g + p^k$ is a generator in $\mathbb{U}_{2p^k}$

Let's try and prove that this pattern holds in general.

$\mathbb{U}_{2p^k}$ is cyclic for odd primes p

x - generator of $\mathbb{U}_{2p^k}$, need $\mathrm{ord}_{2p^k}(x) = \varphi(2p^k)$ and $x \in \mathbb{U}_{2p^k}$.

y - generator of $\mathbb{U}_{p^k}$, need $\mathrm{ord}_{p^k}(y) = \varphi(p^k)$ and $y \in \mathbb{U}_{p^k}$.

We're trying to find the generators of $\mathbb{U}_{2p^k}$ from $\mathbb{U}_{p^k}$'s generators

Then can we relate $\varphi(p^k)$ and $\varphi(2p^k)$?

Since $\varphi(2) = 1$, this gives us the idea of proving that φ is multiplicative which would allow us to derive that:

Since gcd(2, p^k) $= 1$ (because p^k is odd for odd primes p), then by the multiplicity of φ, $x^{\varphi(2p^k)} = x^{\varphi(2)\varphi(p^k)}$, and since $\varphi(2) = 1$, we just need for $\mathrm{ord}_{2p^k}(x) = x^{\varphi(p^k)}$ in order to show x is a generator of $\mathbb{U}_{2p^k}$.

$\mathbb{U}_{2p^k}$ is cyclic for odd primes p

Claim

φ is multiplicative, meaning for a,b with gcd(a,b)=1, $\varphi(a)\varphi(b) = \varphi(ab)$

Proof: Recall that $\varphi(n)$ is the number of numbers a with $1 \leq a \leq n$ and gcd(a,n)=1.

Relation between $\varphi(ab)$and$\varphi(a)\varphi(b)$?

Let $a = p^n$, and $b = q^m$, p and q different primes.

Step 1: Take some u counted in $\varphi(p^n)$.

Step 2: Take some v counted in $\varphi(q^m)$.

Step 3: gcd(p,q)=1 $\implies$ gcd(p^n,q^m)=1

Step 4: p^n is coprime to q^m so use CRT

Step 5: Then gcd(w,p^n)=1, gcd(w,q^m)=1. Then clearly gcd(w,$p^n q^m$)=1.

We have shown for every pair of elements, one in $\varphi(p^n)$, and one in $\varphi(q^m)$, we always have an element in $\varphi(p^n q^m)$.

So $\varphi(p^n q^m) \geq \varphi(p^n)\varphi(q^m)$.

$\mathbb{U}_{2p^k}$ is cyclic for odd primes p

Can we do something similar to show $\varphi(p^n)\varphi(q^m) \geq \varphi(p^n q^m)$, the converse??

Step 1: Take some w counted by $\varphi(p^n q^m)$

Step 2: gcd(w,$p^n q^m$)=1 $\implies$ gcd(w,p^n)=1, gcd(w,q^m)=1.

Step 3: Reducing w mod p^n, and mod q^m we get:

Then for every w we have in $\varphi(p^n q^m)$ we can get a pair of elements, one in $\varphi(p^n)$ and the other in $\varphi(q^m)$.

So $\varphi(p^n)\varphi(q^m) \geq \varphi(p^n q^m)$

$\mathbb{U}_{2p^k}$ is cyclic for odd primes p

We have shown that:

$$\varphi(p^n q^m) \geq \varphi(p^n)\varphi(q^m) \text{ and } \varphi(p^n)\varphi(q^m) \geq \varphi(p^n q^m)$$
$$\implies \varphi(p^n q^m) = \varphi(p^n)\varphi(q^m).$$

$\mathbb{U}_{2p^k}$ is cyclic for odd primes p

Claim

If g is odd and is a generator of $\mathbb{U}_{p^k}$, then g is also a generator of $\mathbb{U}_{2p^k}$

Proof: First off, since g is a generator in $\mathbb{U}_{p^k}$, $\mathrm{ord}_{p^k}(g) = g^{\varphi(p^k)}$. Note that since g is odd, then $g \in \mathbb{U}_{2p^k}$.

By Euler's Totient Theorem, we know that $g^{\varphi(2p^k)} \equiv 1 \pmod{2p^k}$.

Since we showed $g^{\varphi(2p^k)} = g^{\varphi(p^k)}$, we get that $g^{\varphi(p^k)} \equiv 1 \pmod{2p^k}$.

And since g is a generator of $\mathbb{U}_{p^k}$, we also know that $g^{\varphi(p^k)} \equiv 1 \pmod{2p^k}$.

$\mathbb{U}_{2p^k}$ is cyclic for odd primes p

Let $\text{ord}_{2p^k}(g) = y$.

We know $y \mid \varphi(p^k) \implies$ y$\leq \varphi(p^k)$. But we know that y cannot be less than $\varphi(p^k)$ as if we assume otherwise:

So y cannot be less than $\varphi(p^k)$.

Then using the fact that $y \leq \varphi(p^k)$ combined with the fact that y cannot be less than $\varphi(p^k)$, gives us that $y = \text{ord}_{2p^k}(g) = \varphi(p^k)$. So we have proven our claim.

Claim

If g is even and is a generator of $\mathbb{U}_{p^k}$, then $g + p^k$ is a generator of $\mathbb{U}_{2p^k}$.

Proof: First, note that for an even g, $g + p^k \in \mathbb{U}_{2p^k}$. Since p^k is odd so $g + p^k$ is odd, $2 \nmid g + p^k$. Also, $p \nmid g$ so $p \nmid g + p^k$ so gcd($g + p^k$,$2p^k$)=1.

Also, since g is a generator in $\mathbb{U}_{p^k}$, we know $\mathrm{ord}_{p^k}(g) = g^{\varphi(p^k)}$.

Step 1: Euler's Totient Theorem

Step 2:$\mathrm{ord}_{2p^k}(g + p^k) \mid \varphi(p^k)$.

Which implies that $\mathrm{ord}_{2p^k}(g + p^k) \leq \varphi(p^k)$.

$\mathbb{U}_{2p^k}$ is cyclic for odd primes p

But, we know that $\operatorname{ord}_{2p^k}(g+p^k)$ cannot be less than $\varphi(p^k)$, as if we assume otherwise $(\operatorname{ord}_{2p^k}(g+p^k) < \varphi(p^k))$:

Letting $\operatorname{ord}_{2p^k}(g+p^k) = z$:

But this since $z < \varphi(p^k)$, this a contradiction to $\operatorname{ord}_{p^k}(g) = g^{\varphi(p^k)}$.

Then once again using the fact that $z \leq \varphi(p^k)$ combined with the fact that z cannot be less than $\varphi(p^k)$, gives us that $z = \operatorname{ord}_{2p^k}(g+p^k) = \varphi(p^k)$. So we have proven our claim.

$\mathbb{U}_{2p^k}$ is cyclic for odd primes p

Therefore we have shown that for all generators in $\mathbb{U}_{p^k}$, we can construct a generator in $\mathbb{U}_{2p^k}$. So since $\mathbb{U}_{p^k}$ is cyclic, so is $\mathbb{U}_{2p^k}$.