Order Formula and its Applications

Günthner

Winter 2024

Contents

1 Introduction

In this paper we will be examining the following order formula:

$$\operatorname*{ord}_{\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times}(n) = \operatorname*{ord}_{\left(\mathbb{Z}/p\mathbb{Z}\right)^\times}(n) \cdot p^{\max(0, k - k_p(n))}$$

for p and odd prime, k a natural number and $k_p(n)$ a special function.

2 Proving the Order Formula

This first proof only targets $p \neq 2$. We will see a modified proof later which will clarify the situation for $p = 2$.

Before we tackle the formula directly, we should start by understanding $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$.

We know from Gauss' work that the group $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ is cyclic [1], meaning that

$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times \cong \mathbb{Z}/\varphi(p^k)\mathbb{Z}$$

with $\varphi(p^k)$ the Euler-φ-Function which counts the number of coprime integers smaller than the number. The value is $\varphi(p^k) = (p-1)p^k$ and we get:

$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times \cong \mathbb{Z}/(p-1)p^{k-1}\mathbb{Z}$$

Next we would like to simplify $\mathbb{Z}/(p-1)p^{k-1}\mathbb{Z}$ for which we can use the Chinese Remainder Theorem which tells us that for two coprime integers a, b we get

$$\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$$

Now we can write

$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^{\times} \cong \mathbb{Z}/(p-1)p^{k-1}\mathbb{Z} \cong \left(\mathbb{Z}/(p-1)\mathbb{Z}\right) \oplus \left(\mathbb{Z}/p^{k-1}\mathbb{Z}\right) \tag{1}$$

This is still quite abstract so let's find subgroups of $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^{\times}$ that correspond to the summands. Define the projection onto $(\mathbb{Z}/p\mathbb{Z})^{\times}$:

$$\pi_k : \left(\mathbb{Z}/p^k\mathbb{Z}\right)^{\times} \to (\mathbb{Z}/p\mathbb{Z})^{\times}$$

with

$$\pi_k(n) = n \bmod p$$

One of the interesting subgroups is

$$\ker(\pi_k) = \left\{\, n \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^{\times} \,:\, \text{The last digit of n is } 1 \,\right\}$$

The order of this group is $\#\ker(\pi_k) = p^{k-1}$. Now since equation (1) $\ker(\pi_k)$ must lie entirely inside $\mathbb{Z}/p^{k-1}\mathbb{Z}$, because its order is coprime to that of $\mathbb{Z}/(p-1)\mathbb{Z}$. Now since

$$\#\ker(\pi_k) = \#\mathbb{Z}/p^{k-1}\mathbb{Z}$$

and one of the groups is contained in the other, the groups are equal and we can rephrase equation (1):

$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^{\times} \cong \mathbb{Z}/(p-1)\mathbb{Z} \oplus \ker(\pi_k)$$

Substituting $(\mathbb{Z}/p\mathbb{Z})^{\times}$ for $\mathbb{Z}/(p-1)\mathbb{Z}$ gives us

Lemma 1. *Decomposition of* $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^{\times}$

$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^{\times} \cong (\mathbb{Z}/p\mathbb{Z})^{\times} \oplus \ker(\pi_k)$$

2.1 Applications to the formula

What can we learn from Lemma 1?

Lemma 2. *Multiplicativity of* ord

$$\underset{\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times}{\operatorname{ord}}(n) = \underset{(\mathbb{Z}/p\mathbb{Z})^\times}{\operatorname{ord}}(n) \cdot \underset{\ker(\pi_k)}{\operatorname{ord}}(n)$$

Which we will prove using the more general

Lemma 3. *Let A, B be arbitrary finite groups and $(a, b) \in A \oplus B$*

$$\underset{A\oplus B}{\operatorname{ord}}(a, b) = \operatorname{lcm}\left(\underset{A}{\operatorname{ord}}(a),\ \underset{B}{\operatorname{ord}}(b)\right)$$

The proof of which will be deferred to the Appendix in Proof of Lemma 3.

Well we know that

$$\underset{(\mathbb{Z}/p\mathbb{Z})^\times}{\operatorname{ord}}(n) \text{ and } \underset{\ker(\pi_k)}{\operatorname{ord}}(n) \text{ coprime}$$

since the orders of their respective groups is coprime. This simplifies the lcm to a product and proves Lemma 2. (a, b coprime integers implies that $\operatorname{lcm}(a, b) = ab$)

Now all that is open is $\underset{\ker(\pi_k)}{\operatorname{ord}}(n)$, for this we will need the following definition:

Definition 1. *For p prime and $n \in \ker(\pi_k)$, meaning that $n \equiv 1 \pmod p$*

$$k_p(n) \coloneqq \max\{\, i \in \mathbb{N} : n \equiv 1 \pmod{p^i} \,\}$$

This is almost the function from section 1, but with a reduced domain. Now we can prove

Lemma 4. *For p prime and $n \in \ker(\pi_k)$*

$$\underset{\ker(\pi_k)}{\operatorname{ord}}(n) = p^{\max(0, k - k_p(n))}$$

Let us rewrite that using $(a)_+ \coloneqq \max(0, a)$:

$$\underset{\ker(\pi_k)}{\operatorname{ord}}(n) = p^{\left(k - k_p(n)\right)_+}$$

Proof by induction over k.

For $1 \le k \le k_p(n)$: $p^{k - k_p(n)} = 1$. And since $n \equiv 1 \pmod{p^{k_p(n)}}$: $\operatorname{ord}(n) = 1$.

For the induction it will be helpful to define the following map:

$$\begin{array}{cccc} \psi: & \ker(\pi_{k+1}) & \to & \ker(\pi_k) \\ & l & \mapsto & l \bmod p^k \end{array}$$

Now assume that $k \geq k_p(n)$ and $\operatorname{ord}(n) = p^{\left(k-k_p(n)\right)_+}$. Now let us show the following relation:

$$\underset{\ker(\pi_{k+1})}{\operatorname{ord}}(n) = p \cdot \underset{\ker(\pi_k)}{\operatorname{ord}}(n)$$

$$\Lambda_k := \mathbb{Z}/p^k\mathbb{Z}$$

$$\begin{array}{cccc} \lambda_k: & \Lambda_k & \to & ker(\pi_k) \\ & l & \mapsto & g^l \end{array}$$

$$\underset{\ker(\pi_{k+1})}{\operatorname{ord}}(n) = p^{k+1-\nu_p(n)} = p \cdot p^{k-\nu_p(n)} = \underset{\ker(\pi_k)}{\operatorname{ord}}(n)$$

□

3 Appendix

3.1 Proof of Lemma 3

Lemma 3. *Let A, B be arbitrary finite groups and $(a,b) \in A \oplus B$*

$$\underset{A\oplus B}{\operatorname{ord}}(a,b) = \operatorname{lcm}\left(\underset{A}{\operatorname{ord}}(a),\ \underset{B}{\operatorname{ord}}(b)\right)$$

Proof.
Let o_a, o_b denote $\underset{A}{\operatorname{ord}}(a), \underset{B}{\operatorname{ord}}(b)$ respectively and let o_{ab} denote $\underset{A\oplus B}{\operatorname{ord}}(a,b)$.
$o_a \mid o_{ab}$, since $n^{o_{ab}} = e$ (Same for o_b). This gives us $\operatorname{lcm}(o_a, o_b) \mid o_{ab}$.
$o_{ab} \mid \operatorname{lcm}(o_a, o_b)$, since $(a,b)^{\operatorname{lcm}(o_a,o_b)} = (a^{\operatorname{lcm}(o_a,o_b)}, b^{\operatorname{lcm}(o_a,o_b)}) = (e,e)$ □

3.2 Unused proof

To prove Lemma 4 we will first show the easier inequality

$$\underset{\ker(\pi)}{\operatorname{ord}}(n) \leq p^{\left(k-k_p(n)\right)_+}$$

Proof. Let $n \equiv 1 \pmod{p^{k_p(n)}}$
$\operatorname{ord}(n)$ in $\ker(\pi)$ is the number of distinct elements in the subgroup generated

by n, well but how many elements can be generated by n? Well for all $\eta = n^l$ we know that $\eta \equiv 1 \pmod{p^{k_p(n)}}$. However we also have

$$\#\{\, \eta \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^{\times} : \eta \equiv 1 \pmod{p^{k_p(n)}} \,\} = p^{k-k_p(n)}$$

$\square$

References

[1] Carl Gauss. *Disquisitiones Arithmeticae.*