Order Formula and its Applications

Günthner

Winter 2024

Contents

1 Introduction

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

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

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

2.1 Decomposition of $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$

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

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

with

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

One of the interesting subgroups is

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

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

Lemma 2.1. *Decomposition of* $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$

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

2.2 Applications to the formula

What can we learn from Lemma 2.1?

Lemma 2.2. *Multiplicativity of* ord

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

Which we will prove using the more general

Lemma 2.3. *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 section 5.1.

Well we know that

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

since the orders of their respective groups is coprime. This simplifies the lcm to a product and proves Lemma 2.2. (a, b coprime integers implies that $\operatorname{lcm}(a, b) = ab$)

Now all that remains 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 the Introduction, but with a reduced domain. Now we can prove

Lemma 2.4. *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 $(a)_+ \coloneqq \max(0, a)$:

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

In the proof of this formula we will be using

Lemma 2.5. *$n, l \in \mathbb{N}$, then*

$$\underset{\mathbb{Z}/l\mathbb{Z}}{\operatorname{ord}}(n) = \frac{l}{\gcd(n, l)}$$

This lemma will again be proven in the Appendix in section 5.2.
Now this lemma only deals with the additive group $\mathbb{Z}/p^k\mathbb{Z}$ so let us start here by proving

$$\operatorname{ord}(t) = p^{k-k'_p(t)} \tag{2}$$

with the function k'_p the equivalent of k_p for the additive group

$$k'_p(t) \coloneqq \max\{\, i \in \mathbb{N} : t \equiv 0 \pmod{p^i} \,\}$$

To prove equation (2) we can do a simple calculation (ν_p denotes the p-adic valuation):

$$\begin{aligned}\operatorname{ord}(t) &\overset{2.5}{=} \frac{p^k}{\gcd(p^k, t)} = \frac{p^k}{p^{\min(k,\nu_p(t))}} \\ &= p^{k-\min(k,\nu_p(t))} = p^{k+\max(-k,-\nu_p(t))} \\ &= p^{\max(0,k-\nu_p(t))} = p^{\left(k-\nu_p(t)\right)_+}\end{aligned}$$

But how do we translate equation (2) to the multiplicative group and Lemma 2.4?

Lemma 2.6. *Given the isomorphism*

$$\begin{array}{rccc}\iota: & \mathbb{Z}/p^{k-1}\mathbb{Z} & \to & \ker(\pi_k) \\ & l & \mapsto & g^l\end{array}$$

and $t \in \ker(\pi_k)$*:*

$$k_p(t) = k'_p(\iota^{-1}(t))$$

Proof. We want to show the equality by proving that any exponent—in the set over which k_p is the maximum of—is also a valid exponent for k'_p (and vice versa)
Let $t \in \ker(\pi_k)$ and $i \in \mathbb{N}$ with $t \equiv 1 \pmod{p}^i$

Now ι restricts to an isomorphism $\iota' : \mathbb{Z}/p^{i-1}\mathbb{Z} \to \ker(\pi_i)$. Since neutral elements are mapped to neutral elements by isomorphisms we get

$$\iota^{-1}(t) \equiv 0 \pmod{p^{i-1}}$$

This proof also works with k_p and k'_p switched, giving us the equality. □

Proof of Lemma 2.4.

$$\operatorname*{ord}_{\ker(\pi_k)}(n) = \operatorname*{ord}_{\mathbb{Z}/p^{k-1}\mathbb{Z}}(\iota^{-1}(n)) \overset{2}{=} p^{\left(k-k'_p(\iota^{-1}(n))\right)_+} \overset{2.6}{=} p^{\left(k-k_p(n)\right)_+}$$

□

Now we have almost proved the order formula, all that is missing is the k_p function for all natural numbers:

Definition 2. *Generalized k_p-function*

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

with

$$\theta(n) \coloneqq \operatorname*{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(\pi_k(n))$$

Now we can finish the proof of the formula by calculation:

$$\begin{aligned}\operatorname*{ord}_{(\mathbb{Z}/p^k\mathbb{Z})^\times}(n) &= \theta(n) \cdot \operatorname*{ord}_{(\mathbb{Z}/p^k\mathbb{Z})^\times}(n^{\theta(n)}) = \theta(n) \cdot p^{\left(k-k_p(n^{\theta(n)})\right)_+} \\ &= \theta(n) \cdot p^{\left(k-k_p(n)\right)_+} = \operatorname*{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(n) \cdot p^{\left(k-k_p(n)\right)_+}\end{aligned}$$

3 Proving the Order Formula for $p = 2$

This proof really is almost the same as that in section 2, the only difference lies in the structure of $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$. While $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ is cyclic for $p \neq 2$, it is semicyclic for $p = 2$, it has two generators. (semicyclic for $k \geq 3$)

3.1 Decomposition of $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$

In this subsection k should be assumed to be at least 3.

Let us begin by finding an element of maximal order in $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$:

Lemma 3.1.

$$\operatorname*{ord}_{(\mathbb{Z}/2^k\mathbb{Z})^\times}(3) = 2^{k-2}$$

Proof by Induction.

For $k = 3$ we can do a simple computation which tells us that $\operatorname{ord}(3) = 2 = 2^{k-2}$.

Now assume that $\operatorname{ord}(3) = 2^{k-2}$ in $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$. Let us try to calculate $3^{(2^{k-2})} \bmod 2^{k+1}$: It is either 1 or $2^k + 1$ as it must be $\equiv 1 \pmod{2^k}$. We can show that it is $2^k + 1$ by proving

$$\nu_2(3^{(2^{k-2})} - 1) = k - 1 \tag{3}$$

If instead the value was 1 the valuation would be larger.

We will prove equation (3) by induction. For $k = 2$ we get

$$\nu_2(3^2 - 1) = \nu_2(2) = 1 = 2 - 1$$

Now assuming that equation (3) holds for k let us compute the value for $k + 1$:

$$\begin{aligned}
\nu_2\left(3^{(2^{k-1})} - 1\right) &= \nu_2\left((3^{(2^{k-2})})^2 - 1^2\right) \\
&= \nu_2\left((3^{(2^{k-2})} - 1)(3^{(2^{k-2})} + 1)\right) \\
&= \nu_2\left(3^{(2^{k-2})} - 1) + \nu_2(3^{(2^{k-2})} + 1\right) \\
&= k - 1 + 1 = k \text{ assuming the right addend is 1}
\end{aligned}$$

Now to prove that

$$\nu_2(3^{(2^{k-2})} + 1) = 1$$

we will simply compute

$$\begin{aligned}
3^{(2^{k-2})} + 1 &\equiv (3^2)^{(2^{k-3})} + 1 \pmod 4 \\
&\equiv 1^{(2^{k-3})} + 1 \equiv 1 + 1 \equiv 2
\end{aligned}$$

□

Next we will prove

Lemma 3.2. *$\{-1, 3\}$ is a generating set of $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$*

Proof. We know from Lemma 3.1 that

$$2 \cdot \text{ord}(3) = 2^{k-1} = \#\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$$

We also know that

$$3^l \equiv \begin{cases} 1 & \text{if } l \bmod 2 = 0 \\ 3 & \text{if } l \bmod 2 = 1 \end{cases} \pmod 8$$

meaning that $3^l \not\equiv -1 \pmod{2^k}$: -1 is not an element of $< 3 >$, so the group $< -1, 3 >$ must have $\text{ord}(-1) \cdot \text{ord}(3) = 2^{k-1}$ elements and must be equal to the entire group. □

Now we can write

$$\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times \cong < -1 > \oplus < 3 > \tag{4}$$

However for the decomposition we would like a different form, like in Lemma 2.1. Define

$$\begin{array}{rccc}
\pi_k : & \left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times & \to & \left(\mathbb{Z}/4\mathbb{Z}\right)^\times \\
& n & \mapsto & n \bmod 4
\end{array}$$

Lemma 3.3. *Decomposition of* $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$ *(for* $k \geq 3$*)*

$$\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times \cong \left(\mathbb{Z}/4\mathbb{Z}\right)^\times \oplus \ker(\pi_k)$$

Proof.

$$\left(\mathbb{Z}/4\mathbb{Z}\right)^\times \cong \mathbb{Z}/2\mathbb{Z} \cong < -1 >$$

For $\ker(\pi_k)$ we will show that $< -3 > \triangleleft \ker(\pi_k)$ and $\#< -3 > = \#\ker(\pi_k)$:

$$\pi_k(-3) \equiv -1 \cdot 3 \equiv -1 \cdot -1 \equiv 1 \pmod 4$$

Now also all powers of -3 will be in the kernel.

$$\begin{aligned} \#< -3 > &= \operatorname{ord}(-3) = \operatorname{lcm}(\operatorname{ord}(-1), \operatorname{ord}(3)) \\ &= 2^{k-2} = \#\ker(\pi_k) \end{aligned}$$

□

3.2 Discussing the remaining proof

The proof that remains is entirely equivalent to the one from section 2, so only an outline of the revised version will be given.

Lemma 3.3 together with Lemma 2.3 gives us the following formula:

$$\underset{\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times}{\operatorname{ord}(n)} = \operatorname{lcm}\left(\begin{array}{cc} \underset{\left(\mathbb{Z}/4\mathbb{Z}\right)^\times}{\operatorname{ord}(n)}, & \underset{\ker(\pi_k)}{\operatorname{ord}(n)} \end{array} \right)$$

This does not—unlike Lemma 2.2—simplify into a product.

Now all steps until Definition 2 will translate naturally (not in the category-theoretic sense). In the definition of k_2 we must replace θ:

Definition 3. *Generalized* k_2*-function*

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

with

$$\theta(n) \coloneqq \underset{\left(\mathbb{Z}/4\mathbb{Z}\right)^\times}{\operatorname{ord}(\pi_k(n))}$$

The last step that may be difficult to simply believe is the final calculation:

$$\begin{aligned}
\underset{(\mathbb{Z}/2^k\mathbb{Z})^\times}{\operatorname{ord}}(n) &\overset{3.2}{=} \underset{(\mathbb{Z}/2^k\mathbb{Z})^\times}{\operatorname{ord}}((-1)^i \cdot 3^j) \\
&= \operatorname{lcm}\left(\begin{array}{c} \underset{(\mathbb{Z}/2^k\mathbb{Z})^\times}{\operatorname{ord}}((-1)^i),\ \underset{(\mathbb{Z}/2^k\mathbb{Z})^\times}{\operatorname{ord}}(3^j) \end{array} \right) \\
&= \operatorname{lcm}\left(\begin{array}{c} \underset{(\mathbb{Z}/4\mathbb{Z})^\times}{\operatorname{ord}}(n),\ \underset{\ker(\pi_k)}{\operatorname{ord}}(3^j) \end{array} \right) \\
&\overset{2.4}{=} \operatorname{lcm}\left(\begin{array}{c} \underset{(\mathbb{Z}/4\mathbb{Z})^\times}{\operatorname{ord}}(n),\ 2^{\left(k-k_2(3^j)\right)_+} \end{array} \right) \\
&\overset{?}{=} \operatorname{lcm}\left(\begin{array}{c} \underset{(\mathbb{Z}/4\mathbb{Z})^\times}{\operatorname{ord}}(n),\ 2^{\left(k-k_2(n)\right)_+} \end{array} \right)
\end{aligned}$$

Now to verify that last question mark we have to show that $k_2((-1)^i \cdot 3^j) = k_2(3^j)$ which we can do with

$$k_2(3^{2j}) = k_2(3^j)$$

We show this by relating indices admissible for one side to those on the other side:
Let $l \in \mathbb{N}$ with $3^j \equiv 1 \pmod{2^l}$, then also $3^{2j} \equiv 1$.

Let $l \in \mathbb{N}$ with $3^{2j} \equiv 1 \pmod{2^l}$, then

$$3^j \equiv \begin{cases} -1 \\ 1 \end{cases}$$

as those are the only square roots of 1, however in the proof of Lemma 3.2 we showed that no $3^j \equiv -1$ and hence $3^j \equiv 1$. □

Now we have proved the order formula for $k \geq 3$, but the reader may verify that the formula is also valid for $k = 2$. Now we can formulate the main result of this paper:

4 The Order Formula

Theorem 1. *For p prime and $k, n \in \mathbb{N}$ the following equation holds:*

$$\operatorname*{ord}_{(\mathbb{Z}/p^k\mathbb{Z})^\times}(n) = \begin{cases} \theta_p(n) \cdot p^{\left(k-k_p(n)\right)_+} & \text{if } p \neq 2 \\ \operatorname{lcm}\left(\alpha_k \cdot \theta_p(n), 2^{\left(k-k_2(n)\right)_+}\right) & \text{if } p = 2 \end{cases}$$

with

$$\theta_p(n) = \begin{cases} \operatorname*{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(n) & \text{if } p \neq 2 \\ \operatorname*{ord}_{(\mathbb{Z}/4\mathbb{Z})^\times}(n) & \text{if } p = 2 \end{cases}$$

and

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

further

$$\alpha_k = \begin{cases} 1 & \text{if } k \neq 1 \\ \frac{1}{2} & \text{if } k = 1 \end{cases}$$

5 Appendix

5.1 Proof of Lemma 2.3

Lemma 2.3. *Let A, B be arbitrary finite groups and $(a, b) \in A \oplus B$*

$$\operatorname*{ord}_{A\oplus B}(a,b) = \operatorname{lcm}\left(\operatorname*{ord}_A(a),\ \operatorname*{ord}_B(b)\right)$$

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

□

5.2 Proof of Lemma 2.5

Lemma 2.5. *$n, l \in \mathbb{N}$, then*

$$\operatorname*{ord}_{\mathbb{Z}/l\mathbb{Z}}(n) = \frac{l}{\gcd(n,l)}$$

Proof. A number x is equal to $\text{ord}(n)$ exactly if it is the smallest number such that $l \mid nx$. Now $n \cdot \text{ord}(n) = \text{lcm}(n, l)$. The smallest multiple of n that is divisible by l. Now calculate

$$n \cdot \frac{l}{\gcd(n, l)} = \frac{nl}{\gcd(n, l)} = \text{lcm}(n, l)$$

telling us that $\frac{l}{\gcd(n,l)} = \text{ord}(n)$ □

References

[1] Carl Gauss. *Disquisitiones Arithmeticae.*