Orders and Primitive Roots

Markus Farnebäck[†], Isak Fleig, Sixten Georgsson and Oskar Ådahl
Minervagymnasium

May 2022

Contents

[†]Berzeliusskolan

0 Prerequisites

To fully understand the theory described in this document, we strongly recommend that the reader is familiar with fundamental concepts in number theory, such as divisibility, primes and basic modular arithmetic.

An explanation of the above mentioned concepts can be found in most books on elementary number theory, see for example [5].

1 Introduction

In this document we introduce orders and primitive roots, two closely related concepts in number theory that are often useful in problems where one has integer powers modulo some integer.

Each section begins with some theory and discussion and is followed by one or more worked-through example problems that demonstrate how the theory can be applied. But remember that the best way to get better at problem solving is by doing. For that reason, we have tried to include numerous exercises for the reader, both at the end of each section and in the section *Exercises* at the end of this document. For some of the exercises there is a hint available in the section *Hints*. We recommend that one only uses a hint if one has not achieved any progress on a problem in more than 10 minutes.

In the section named *Further Reading*, the interested reader can find external material with more problems and information about orders, primitive roots, as well as other related concepts.

2 Orders Modulo a Prime

As mentioned in the introduction, orders are related to integer powers modulo some integer. More specifically, we are interested in when some power of an integer is 1 modulo another integer.

Definition 2.1 (Orders Modulo a Prime)**.** Given a prime p, the order of an integer a modulo p, $p \nmid a$, is the smallest positive integer d, such that $a^d \equiv 1 \pmod{p}$. This is denoted $\text{ord}_p(a) = d$.

Now, a relevant question is: Does the order always exist? One could imagine that we could keep multiplying a by itself and never get 1 modulo p. But, the expression $a^d \equiv 1 \pmod{p}$ should remind us of something, namely Fermat's Little Theorem. (If the reader is not familiar with this theorem one can learn about it in [5].) It tells us that $a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$. Thus, we know not only that the order always exists, but we also know that it is smaller than p. In fact, we can reduce the possible values of the order even further.

Consider the following table with the values of the orders of the integers 1 to 10 modulo 11.

a	$\text{ord}_{11}(a)$
1	1
2	10
3	5
4	5
5	5
6	10
7	10
8	10
9	5
10	2

Table 1: Orders modulo 11

All the orders in the table above have one thing in common – they are divisors of $10 = 11 - 1$. This is nothing unique for the prime 11. We have, in fact, the following useful theorem.

Theorem 2.1 (Fundamental Theorem of Orders)**.** *If p is a prime and a is an integer, $p \nmid a$, we have*

$$a^n \equiv 1 \pmod{p} \iff \text{ord}_p(a) \mid n$$

The proof of this theorem is not very difficult and is left as an exercise for the reader. The importance of *Theorem 2.1.* cannot be stressed enough; it is used in almost all applications of orders. This should not come as a surprise since it has the word "fundamental" in its name.

But enough theory now. What can we even use this for? It turns out that orders are a very powerful tool in many problems. Consider the following classic problem.

Example 2.1. *Determine all n such that $n \mid 2^n - 1$.*

In general, most problems where one is asked to find all n that satisfy some condition, tend to only have small solutions that are easy to find, and the tricky part is to show that no other values of n work. After testing some small values, we observe that $n = 1$ is a solution since $1 \mid 2^1 - 1 = 1$, we also guess that this is the only solution. So, from now on we only care about $n > 1$.

Since $2^n - 1$ is odd, it follows that n must be odd as well (Why?). We notice that

$$2^n \equiv 1 \pmod{n}$$

looks like something we could use orders to work with. But we do not necessarily know that n is prime. For that reason we instead consider a prime p that divides n. We have

$$2^n \equiv 1 \pmod{p}$$

and

$$2^{p-1} \equiv 1 \pmod{p} \quad \text{(Fermat's Little Theorem)}$$

This, together with the Fundamental Theorem of Orders, gives us that

$$\mathrm{ord}_p(2) \mid n \quad \text{and} \quad \mathrm{ord}_p(2) \mid p-1$$

Since $\gcd(2,p) = 1$ we know that the order must exist. This does not look like it will help us since we still have several possible candidates for $\mathrm{ord}_p(2)$. Unless we choose p to be the smallest prime dividing n. Then, we cannot have any other number than 1 dividing both n and $p-1$ and we have

$$\mathrm{ord}_p(2) = 1$$

$$\iff 2^1 \equiv 1 \pmod{p}$$

which is impossible. Hence, the only solution is $n = 1$. □

The above solution illustrates some of the main ideas used in most problems involving orders, especially the idea of choosing the smallest prime factor, which is worth remembering.

Exercise 2.1. *Given a prime p. Show that any prime factor q of $p^p - 1$ that is larger than p is congruent to 1 modulo p.*

Exercise 2.2. *Prove the Fundamental Theorem of Orders.*

Exercise 2.3. *Let $p > 3$ be a prime, prove that any prime divisor of $2^p + 1$ is either 3 or on the form $2kp + 1$, for some non-negative integer k.*

3 Euler's Phi Function

Prior to introducing general orders and primitive roots, we must briefly mention Euler's phi function, denoted φ (for a more complete description, see for example [1]). If this section feels too technical, it is not essential to fully understand it. Most of this document can be understood anyway. Though, it is important to know that for a prime p, $\varphi(p) = p - 1$. The phi function is defined as follows.

Definition 3.1 (Euler's Phi Function)**.** $\varphi(1) = 1$. For a positive integer $n > 1$ $\varphi(n)$ is the number of positive integers smaller than n that are relatively prime to n.

For the purpose of this document, only two properties regarding this function are necessary to know. These are Euler's Theorem, the general case of Fermat's Little Theorem, as well as Euler's Product Formula, an efficient way to calculate the value of the function. For the sake of brevity, these results are stated without proof, but proofs can easily be found online.

Theorem 3.1 (Euler's Theorem)**.** *If n and a are relatively prime, then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Theorem 3.2 (Euler's Product Formula)**.**

$$\varphi(n) = n\prod_{p|n}(1-\frac{1}{p})$$

Where the product is over the distinct primes dividing n.

The above formula is easier understood through an example.

Example 3.1. *Calculate $\varphi(20)$.*

We have $20 = 2^2 \cdot 5$, so, the distinct primes dividing 20 are 2 and 5. Now, by Euler's Product Formula,

$$\varphi(20) = 20(1-\frac{1}{2})(1-\frac{1}{5}) = 20 \cdot \frac{1}{2} \cdot \frac{4}{5} = 8.$$

Going back to the definition of φ, we find that the 8 numbers smaller than and relatively prime to 20 are $1, 3, 7, 9, 11, 13, 17$, and 19. □

Here are some exercises to get more familiar with the phi function.

Exercise 3.1. *Using Euler's Theorem, calculate*

(a) $5^{17} \pmod{12}$

(b) $13^{82} \pmod{60}$

(c) $2^{128} \pmod{49}$

Exercise 3.2. *Using Euler's Product Formula, calculate*

(a) $\varphi(30)$

(b) $\varphi(100)$

(c) $\varphi(p^k)$*, where p is a prime and k is a positive integer.*

Exercise 3.3. *Show that the function φ is multiplicative, i.e. if a and b are relatively prime then $\varphi(ab) = \varphi(a)\varphi(b)$.*

Exercise 3.4. *Using the results from Exercise 3.2. part (c) and Exercise 3.3., find another version of Euler's product formula for $\varphi(n)$ based on the prime factorization of n.*

4 General Orders

Earlier, we discussed orders where the modulo base was a prime. But we can easily generalize the concept of orders to work for all modulo bases. General orders work almost the same as prime orders, with the obvious difference that the modulo base need not be a prime (to clarify, prime orders are a special case of general orders). This has implications for which numbers have an order for a given modulo base.

Definition 4.1 (General Orders)**.** Given two relatively prime integers a and $n > 0$, the order of a modulo n is the smallest positive integer d such that $a^d \equiv 1 \pmod{n}$.

So, only integers that are relatively prime to the modulo base can have an order, and the existence of this order follows from Euler's Theorem. Just as the existence of prime orders follows from Fermat's Little Theorem, as described earlier. To explain this more intuitively, we consider the modulo base n which has a factor $k \neq 1$, and the integer a which also has the factor k. If for some $d > 0$, $a^d \equiv 1 \pmod{n}$ then, $n \mid a^d - 1$. Since $k \mid n$ and $k \mid a$, then k must divide 1 which is impossible.

It should be noted that most properties of prime orders also apply to general orders. Most importantly, the Fundamental Theorem of Orders holds for general orders as well. General orders are more seldom used in problem solving but do still appear occasionally, for example in the following problem from the Saint Petersburg Mathematical Olympiad.

Example 4.1 (Saint Petersburg Mathematical Olympiad)**.** *Prove that for all positive integers $a > 1$ and n we have $n \mid \varphi(a^n - 1)$*

We have not mentioned any method for calculating φ of something like $a^n - 1$, so this suggests that we might not need to calculate it. Maybe we could use Euler's Theorem instead. For any x, we have

$$x^{\varphi(a^n-1)} \equiv 1 \pmod{a^n - 1}$$

Now, this looks like something where we could use orders. We would like to have some x such that $\operatorname{ord}_{a^n-1}(x) = n$, by the Fundamental Theorem of Orders,

$$n = \operatorname{ord}_{a^n-1}(x) \mid \varphi(a^n - 1)$$

The question is what this x might be, if it even exists. To begin with, we must have $(a^n - 1) \mid (x^n - 1)$. This is obviously true for $x = a$. But if $x = a$ should work we must, for all $d < n$, have

$$a^d \not\equiv 1 \pmod{a^n - 1}$$

which is equivalent to

$$(a^n - 1) \nmid (a^d - 1)$$

But we know this is true since $a^n - 1$ is larger than $a^d - 1$. We also know that the order exists since $\gcd(a, a^n - 1) = 1$. Thus $x = a$ works, and we are done. □

Exercise 4.1. *Determine whether the order exists in the following cases and calculate it if it does.*

(a) $\operatorname{ord}_{10}(5)$

(b) $\text{ord}_{12}(7)$

(c) $\text{ord}_{15}(2)$

Exercise 4.2. *Given positive integers n and a, and a prime p such that $a^p \equiv -1 \pmod{n}$, $n \nmid a-1$, and $a+1$ and n are relatively prime. Find $ord_n(a)$.*

5 Primitive Roots

As it turns out, often, the most useful and interesting case is when the order of some integer g modulo n is $\varphi(n)$. This case is so important that it even has a special name.

Definition 5.1 (Primitive Roots)**.** Given a positive integer n. If $\text{ord}_n(g) = \varphi(n)$ then g is a primitive root modulo n. (For a prime p, $\varphi(p) = p-1$.)

For example, looking at *Table 1*, we see that $2, 6, 7$ and 8 have order $10 = \varphi(11)$. So, they are the primitive roots modulo 11.

The natural question now, as with orders, is: Does there always exist a primitive root modulo n? We encourage the reader to investigate for what n there exist primitive roots and come up with an own conjecture before we spoil the answer in the following theorem.

Theorem 5.1 (Existence of Primitive Roots)**.** *A primitive root exists modulo n if and only if $n = 1, n = 2, n = 4$ or if n is in the form p^k or $2p^k$ for some positive integer k and odd prime p.*

The proof of this result is difficult and out of the scope for this document. The main takeaway from this theorem is that primitive roots exist for all primes. This case is by far the most used.

Now, one very important and useful fact regarding primitive roots is the following.

Theorem 5.2. *Given a prime p and a primitive root g modulo p, the set $\{g^1, g^2, g^3, \ldots, g^{p-1}\}$ forms a complete set of residues modulo p. (This is equivalent to saying that all g^i are different modulo p.)*

Proof. There are $p-1$ possible values of g^i. So, if all are not different then, by the pigeonhole principle, there must exist some $i, j, 0 < i < j < p$, such that

$$g^i \equiv g^j \pmod{p}$$

Then,

$$g^{j-i} \equiv 1 \pmod{p}$$

But this is impossible, since $j - i < p - 1$ and $\text{ord}_p(g) = p - 1$. Hence such i, j do not exist and all g^i are different modulo p. □

One should note that this theorem has an analog for general primitive roots. Proving that analog theorem is *Exercise 5.3.* at the end of this section. Now, let us move on to some applications of primitive roots.

Example 5.1 (Wilson's Theorem, one direction)**.** *Given a prime p, then*

$$(p-1)! \equiv -1 \pmod{p}$$

.

The case of $p = 2$ is obvious, so from now on we assume p is an odd prime. Let g be a primitive root modulo p.

$$\begin{aligned}
(p-1)! &= 1 \cdot 2 \cdot 3 \cdots (p-1) \\
&\equiv g^1 \cdot g^2 \cdot g^3 \cdots g^{p-1} \pmod{p} \quad \text{(Theorem 5.2.)} \\
&= g^{1+2+3+\cdots+(p-1)} \\
&= g^{\frac{p(p-1)}{2}} \quad \text{(Sum of arithmetic sequence)} \\
&\equiv g^{\frac{p-1}{2}} \pmod{p} \quad \text{(Fermat's Little Theorem, strong form)}
\end{aligned}$$

It is important to note that in the second step, the numbers $1, 2, 3, \ldots, p-1$ do not necessarily correspond to the powers of g in the specific order they are written. Now,

$$g^{p-1} \equiv 1 \pmod{p} \quad \text{(Fermat's Little Theorem)}$$

$$\iff p \mid g^{p-1} - 1 = (g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1)$$

However, from the definition of primitive roots, $p \nmid g^{\frac{p-1}{2}} - 1$. So, we must have

$$p \mid g^{\frac{p-1}{2}} + 1$$

$$\implies (p-1)! \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

□

Why did we take care of the case $p = 2$ in the beginning?

Exercise 5.1. *Prove the other direction of Wilson's Theorem, i.e. if $(p-1)! \equiv -1 \pmod{p}$, then p is a prime.*

We continue with another example which is also a useful result in its own right.

Example 5.2 (Sum of Powers Modulo n)**.** *Let p be a prime and x be a positive integer. Find all residues the sum*

$$1^x + 2^x + 3^x + \cdots + (p-1)^x$$

can give when divided by p.

If $p-1 \mid x$, then we have, for some k, $x = k(p-1)$. Now, by Fermat's Little Theorem,

$$\begin{aligned} 1^x + 2^x + 3^x + \cdots + (p-1)^x &= 1^{k(p-1)} + 2^{k(p-1)} + 3^{k(p-1)} + \cdots + (p-1)^{k(p-1)} \\ &\equiv 1^k + 1^k + 1^k + \cdots + 1^k \pmod{p} \quad \text{(Fermat's Little Theorem)} \\ &= p-1 \end{aligned}$$

So, from now on, we assume that $p-1 \nmid x$. Let g be a primitive root modulo p. Then we can write the given sum as

$$\begin{aligned} 1^x + 2^x + 3^x + \cdots + (p-1)^x &\equiv g^x + g^{2x} + g^{3x} + \cdots + g^{(p-1)x} \pmod{p} \quad \text{(Theorem 5.2.)} \\ &= g^x \cdot \frac{g^{(p-1)x} - 1}{g^x - 1} \quad \text{(Sum of geometric sequence)} \\ &= g^x \cdot \frac{(g^x)^{p-1} - 1}{g^x - 1} \\ &\equiv g^x \cdot \frac{1-1}{g^x - 1} \pmod{p} \quad \text{(Fermat's Little Theorem)} \\ &= 0 \end{aligned}$$

Note that is only valid if the denominator $g^x - 1$ is not 0 modulo p. But, since g is a primitive root and $p-1 \nmid x$, it follows from the Fundamental Theorem of Orders that we cannot have $g^x - 1 \equiv 0 \pmod{p}$.

Thus, the sum can only give the residues 0 and $p-1$ when divided by p. □

Exercise 5.2. *Find all primitive roots in the following modulo bases.*

(a) 10

(b) 30

(c) 17

Exercise 5.3. *Given an integer n for which there exists a primitive root g modulo n. Prove that the set $\{g^1, g^2, \ldots, g^{\varphi(n)}\}$, when considered modulo n, contains all integers relatively prime to n.*

Exercise 5.4. *Let p be a prime and let g be a primitive root modulo p. Given that $g^2 \equiv g+1 \pmod{p}$, show that $g-1$ is also a primitive root modulo p.*

6 Miscellaneous Examples

In this section, we solve two challenging problems using the theory presented in the previous sections.

Example 6.1 (Fermat's Christmas Theorem)**.** *Let p be an odd prime. Then there exists an integer n such that $p \mid n^2 + 1$ if and only if $p \equiv 1 \pmod{4}$.*

This is an interesting problem, because we can use orders for proving one direction and primitive roots for the other. We start by assuming that there exists an integer n such that $p \mid n^2 + 1$. This immediately reminds us of orders, because this is

$$n^2 \equiv -1 \pmod{p}$$

And, as a result,

$$n^4 \equiv 1 \pmod{p}$$

Thus, $\text{ord}_p(n)$ divides 4, but it does not divide 2, and we must have $\text{ord}_p(n) = 4$. And, by Fermat's Little Theorem and the Fundamental Theorem of Orders, we have

$$4 = \text{ord}_p(n) \mid p - 1$$

Hence, $p - 1 = 4k$, for some positive integer k and $p \equiv 1 \pmod{4}$ as desired.

Now, for the other direction. We assume that $p \equiv 1 \pmod{4}$ and want to find some n such that

$$n^2 \equiv -1 \pmod{p}$$

We know that primitive roots are our best tool to control residues of powers. So, we let g be a primitive root modulo p. Note that in the solution of Wilson's Theorem, we proved that

$$g^{\frac{(p-1)}{2}} \equiv -1 \pmod{p}$$

Maybe we could use this. Then we want

$$n^2 = g^{\frac{p-1}{2}}$$

$$\implies n = \pm g^{\frac{p-1}{4}}$$

And since $p \equiv 1 \pmod{4}$, we know that $\frac{p-1}{4}$ is an integer, and hence is $n = \pm g^{\frac{p-1}{4}}$. So, this construction is indeed possible, and we are done. □

We finish this section with one part of a difficult problem from the Swedish TST 2022 (the other part uses methods that are out of the scope for this document).

Example 6.2 (Sweden TST 2022, modified)**.** *Let p be a prime such that $p^2 \mid 2^{p-1} - 1$. Prove that $p - 1$ has at least two distinct prime factors.*

The cases we want to rule out are if $p - 1$ has less than 2 distinct prime factors, i.e. 0 or 1 distinct prime factors. The only possibility for $p - 1$ to have 0 distinct prime factor is if $p = 2$, but we note that $p = 2$ does not satisfy the divisibility condition given for p, hence we can assume $p > 2$. Then p is odd, so, if $p-1$ has only 1 distinct prime factor, that factor must be 2. Thus $p-1 = 2^k$, for some non-negative integer k.

So, suppose there exists a prime p that satisfies $p^2 \mid 2^{p-1} - 1$ and $p - 1 = 2^k$ for some positive integer k. If k has any odd factor $a > 1$, then, using the factorization of a sum of odd powers, we get

$$\begin{aligned} p &= 2^k + 1 \\ &= (2^{\frac{k}{a}})^a + 1 \\ &= (2^{\frac{k}{a}} + 1)(2^{(\frac{k}{a})^{a-1}} - 2^{(\frac{k}{a})^{a-2}} + \cdots + 1) \end{aligned}$$

The factor $2^{\frac{k}{a}} + 1$ is obviously more than 1 and smaller than p, so, p cannot be prime. This is a contradiction, hence k cannot have any odd factors and must be a power of 2.

When we combine $p^2 \mid 2^{p-1} - 1$ and $p - 1 = 2^k$, we get

$$p^2 \mid 2^{p-1} - 1 = 2^{2^k} - 1$$

Note that the expression $2^{2^k} - 1 = (2^{2^{k-1}})^2 - 1$ is a difference of squares, so, we can factorize it as

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

Now, we can apply the same trick to the left factor, and, by repeating this idea inductively, we get

$$\begin{aligned} 2^{2^k} - 1 &= (2^{2^{k-1}} - 1)(2^{2^{k-1}} + 1) \\ &= (2^{2^{k-2}} - 1)(2^{2^{k-2}} + 1)(2^{2^{k-1}} + 1) \\ &\vdots \\ &= (2^{2^0} - 1)(2^{2^0} + 1)(2^{2^1} + 1) \cdots (2^{2^{k-1}} + 1) \\ &= (2^{2^0} + 1)(2^{2^1} + 1) \cdots (2^{2^{k-1}} + 1) \qquad (1) \end{aligned}$$

Now, we know that $p = 2^k + 1 = 2^{2^m} + 1$ and, since $2^{k-1} \geq k$ for all positive integers k (Why?), one of the factors in (1) must be p. Since p^2 divides the product and p is prime, there must be some other factor that is divisible by p as well.

Here we can use orders. Since $p = 2^{2^m} + 1$, we have

$$2^{2^m} \equiv -1 \pmod{p}$$

and thus,

$$2^{2^{m+1}} = (2^{2^m})^2 \equiv 1 \pmod{p}$$

So, $\mathrm{ord}_p(2) \nmid 2^m$ and $\mathrm{ord}_p(2) \mid 2^{m+1}$, implying that $\mathrm{ord}_p(2) = 2^{m+1}$. Now, any of the factors in (1) before $2^{2^m} + 1$ is smaller than p and cannot be divisible by p. Thus, some of the factors larger than p must be. We let one of those factors

be $2^{2^n}+1$. Now we get

$$\begin{aligned} 0 &\equiv 2^{2^n}+1 \pmod{p} \\ &= 2^{2^{m+1}\cdot 2^{n-(m+1)}}+1 \\ &= (2^{2^{m+1}})^{2^{n-(m+1)}}+1 \\ &\equiv 1^{2^{n-(m+1)}}+1 \pmod{p} \\ &= 2 \end{aligned}$$

which is a contradiction, since $p > 2$. Hence, our assumption about the existence of p is false, and we are done. □

7 Exercises

The problems in this section are based on the theory presented in this document and are ordered by (estimated) difficulty. One should not feel disappointed if one does not manage to solve all the problems as some are really difficult. Please give each problem a try before looking at the corresponding hints in the next section. Good luck!

Exercise 7.1. *If $n \mid 2^n+1, n>1$, find the smallest prime factor of 2^n+1.*

Exercise 7.2. *Find all n such that $n^2 \mid 3^n+1$.*

Exercise 7.3. *Suppose that $k \geq 2$ and let $n_1, n_2, \ldots, n_k \geq 1$ be natural numbers having the property that*

$$n_2 \mid 2^{n_1}-1,\ n_3 \mid 2^{n_2}-1,\ \ldots,\ n_k \mid 2^{n_{k-1}}-1,\ n_1 \mid 2^{n_k}-1$$

Show that $n_1 = n_2 = \cdots = n_k = 1$.

Exercise 7.4. *Prove that any prime factor of $2^{2^n}+1$ is congruent to 1 modulo 2^{n+1}.*

Exercise 7.5 (Brazil Iberoamerican TST, Round 3 Problem 1)**.** *Let $p > 10$ be a prime. Prove that there exist positive integers m, n with $m+n<p$, such that $p \mid 5^m 7^n - 1$.*

Exercise 7.6. *Given that there exists a primitive root modulo n. Prove that there exist $\varphi(\varphi(n))$ primitive roots modulo n.*

Exercise 7.7 (Swedish Correspondence Course 2021/2022, Round 3 Problem 2)**.** *The numbers m and n are positive integers, and the number p, $p>n$, is a prime. Given that $pm+n$ divides p^p+1, prove that n divides m.*

8 Hints

2.1. What is $\text{ord}_q(p)$?
2.2. Use Euclid's Division Lemma.
2.3. Set q to be any prime divisor of $2^p + 1$. Use the Fundamental Theorem of Orders.
3.3. Put $n = ab$ into Euler's Product Formula and separate their respective prime factors.
3.4. Split n into the product of its distinct prime factors.
4.2. What number must $\text{ord}_n(a)$ divide? Try then to rule out some candidate values of $\text{ord}_n(a)$ using the given conditions.
5.1. What would happen if p was not prime?
5.3. Use the definition of φ and look at the proof of *Theorem 5.2.*
5.4. Factorize using difference of squares and then assume $g - 1$ is not a primitive root. What would that imply?
7.1. Look at the solution of *Example 2.1.*
7.2. Can n be even? Investigate what happens modulo 4. Then use a standard order argument.
7.3. Let p be the smallest prime factor of any n_i. What is $\text{ord}_p(2)$?
7.4. If p is a prime divisor of $2^{2^n} + 1$, what is $\text{ord}_p(2)$? Look at the solution of *Example 6.2.* for more help.
7.5. Express 5 and 7 as powers of a primitive root g. Express m and n using the exponents of g in a clever way.
7.6. Use the result of *Exercise 5.3.*. How many powers in that set has order $\varphi(n)$?
7.7. Take care of the case $p = 2$. Then, let q be a prime dividing $p^p + 1$. Factor $p^p + 1$. Can q divide both the factors? Find $\text{ord}_q(-p)$.

9 Further Reading

[1] Aditya Khurmi. *Modern Olympiad Number Theory.*
`https://www.academia.edu/44512122/Modern_Olympiad_Number_Theory`

[2] Brilliant. *Order of an Element.*
`https://brilliant.org/wiki/order-of-an-element/`

[3] Brilliant. *Primitive Roots.*
`https://brilliant.org/wiki/primitive-roots/`

[4] Evan Chen. *Orders Modulo a Prime.*
`https://web.evanchen.cc/handouts/ORPR/ORPR.pdf`

[5] Jim Hefferon. *Elementary Number Theory.*
`https://joshua.smcvt.edu/numbertheory/book.pdf`