Lifting the Exponent Lemma

Ida Grimheden, Erik Hedin*, Alvin Palmgren and Emil Sandberg

Norra Real

Contents

*Gymnasieskolan Spyken

0 Notation

- $n \mid a$ means that n divides a and $n \nmid a$ means that n doesn't divide a.
- $a \equiv b \pmod{n}$ means that a and b are congruent modulo n.
- $a \perp b$ means that a and b are relatively prime.
- In this text $\mathbb{N}$ will denote the set of positive integers and $\mathbb{N}_0$ will denote the set of non-negative integers.

1 Is It Worth It?

Let us imagine that you are studying numbers of the form 11^n. You might find that these numbers all have 1 as their last digit so you conclude that numbers of the form $11^n - 1$ always end with a 0, but will they ever have more than one 0 at the end, and how many trailing zeroes could they have? You might try calculating a few of these numbers and find:

$$11^2 - 1 = 120$$

$$11^3 - 1 = 1330$$

$$11^4 - 1 = 14640$$

These numbers all have 1 trailing zero and it is already becoming a little tedious to do the arithmetic; you are considering giving up. After all, this question is not that relevant and when thinking about delving deeper into the problem you ask yourself:

"Is it worth it?"

If you are going to find something interesting you cannot keep trying larger and larger n, you must do something a bit more clever. You might realise that the number of trailing zeroes of a number is equal to the number of times you can factor out 10 from it. Since $10 = 2 \cdot 5$ you want to find the number of times that 2 and 5 occur in the prime factorisation of $11^n - 1$. This is a useful insight that will be crucial for answering the question, but the solution still seems far away so you might again ask yourself:

"Is it worth it?"

You keep going and you remember that you can factor $11^n - 1$, exactly what you need!

$$11^n - 1 = (11 - 1) \cdot \left(1 + 11 + 11^2 + \ldots + 11^{n-1}\right).$$

Now you see that the number has 10 as a factor but the other factor looks even more intimidating than what you started with and once more you ask yourself:

"Is it worth it?"

2 Building Towards the Lemma

2.1 The p-adic valuation

It is clear that we are interested in the number of times that a prime number occurs in the prime factorization of a number. To describe this idea succinctly, we will introduce some terminology and notation.

Definition 2.1. Let $a \in \mathbb{Z}$ and let p be a prime. Then the *p-adic valuation* of a, denoted $\nu_p(a)$, is the number of times that p occurs in the prime factorization of a. In other words, it is the largest number $n \in \mathbb{N}_0$ such that $p^n \mid a$. By convention we usually let $\nu_p(0) = \infty$.

Some fundamental properties of the p-adic valuation are provided below:

- $\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b)$
- $\nu_p(a + b) \geq \min\{\nu_p(a), \nu_p(b)\}$
- $\nu_p(a) \leq \log_p|a|$, for $a \neq 0$. (equality when a is a power of p)

Proof. The proofs of these properties are left as an exercise for the reader. □

Hint. Rewrite the numbers a and b on the form $k \cdot p^n$.

If we could find $\nu_2(11^n - 1)$ and $\nu_5(11^n - 1)$ we would be able to answer our original question. If possible we would like to be more general than just looking at the numbers 11 and 1. Therefore, we will now look at the expression $\nu_p(x^n - y^n)$ where p is a prime that divides $x - y$, but does not divide the integers x or y. Using the factorization

$$x^n - y^n = (x - y) \cdot \left(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1}\right)$$

as well as the property $\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b)$, we obtain

$$\nu_p\left(x^n - y^n\right) = \nu_p(x - y) + \nu_p\left(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1}\right).$$

The first term is independent of n and simple to evaluate for small values of x and y. The second term is trickier, however. We will therefore begin by studying a specific case in which the second term becomes trivial.

2.2 The Case $p \nmid n$

Lemma 2.1. *Let x and y be (not necessarily positive) integers and let p be a prime number such that $p \mid x - y$ and $p \nmid x, y$. If n is a positive integer such that $p \nmid n$, then*

$$\nu_p\left(x^n - y^n\right) = \nu_p(x - y).$$

Proof. By the previous observation, this is equivalent to showing that

$$p \nmid x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}.$$

In fact, since $p \mid x - y \Leftrightarrow x \equiv y \pmod{p}$ we have that neither n nor x are divisible by p. Therefore

$$\underbrace{x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1}}_{n \text{ terms}} \equiv nx^{n-1} \not\equiv 0 \pmod{p}$$

which implies $p \nmid x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}$ as desired. □

With this useful step complete it feels like our effort might soon be worth it. Now we are ready to investigate the situation when n can be any integer, not just one relatively prime to p.

2.3 The Case $n = p$

Now that we know what to do when $p \nmid n$ we want to look at n that are divisible by p. Let us now consider the simplest such case, when n is equal to p. First we look at odd primes p:

Lemma 2.2. *If p is an odd prime with x and y integers, $p \nmid x, y$ and $p \mid x - y$ then:*

$$\nu_p\left(x^p - y^p\right) = \nu_p(x - y) + 1.$$

Proof. This is equivalent to showing that $p \mid x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1}$, whilst $p^2 \nmid x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1}$. Since $p \mid x - y$, let $y = kp + x$ for some integer k. Consider $y^t x^{p-1-t}$ modulo p^2 using the Binomial Theorem:

$$\begin{aligned} y^t x^{p-1-t} &= (kp + x)^t x^{p-1-t} \\ &= x^{p-1-t} \cdot \left(x^t + tkpx^{t-1} + \cancel{p^2 \sum_{i=2}^{t} k^i \binom{t}{i} p^{i-2} x^{t-i}} \right) \\ &\equiv x^{p-1} + tkpx^{p-2} \pmod{p^2}. \end{aligned}$$

Adding together all terms of the form $y^t x^{p-1-t}$ for $0 \leq t \leq p-1$ gives:

$$\begin{aligned} x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1} &= \sum_{t=0}^{p-1} y^t x^{p-1-t} \\ &\equiv \sum_{t=0}^{p-1} \left(x^{p-1} + tkpx^{p-2} \right) \pmod{p^2} \\ &\equiv px^{p-1} + \cancel{k\frac{(p-1)p}{2} px^{p-2}} \pmod{p^2} \\ &\equiv px^{p-1} \not\equiv 0 \pmod{p^2} \end{aligned}$$

Therefore we can conclude both that $p \mid x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1}$ and that $p^2 \nmid x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1}$. Hence we are done. □

This step was quite difficult, but will soon prove very useful. Now what if $p = 2$? They say that 2 is the oddest prime as it is the only one that is even. Unfortunately the above lemma doesn't work when $p = 2$ (can you see why?) but thankfully there is another lemma for this case, which we see below.

Lemma 2.3. *If x, y are odd:*

$$\nu_2\left(x^2 - y^2\right) = \nu_2(x - y) + \nu_2(x + y).$$

Proof. This follows directly from the fact that $\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b)$. □

Now we are ready to witness the fruits of our labour by proving the Lifting the Exponent Lemma, or LTE for short.

3 Lifting the Exponent Lemma

Everything we have done so far has lead us to the Lifting the Exponent lemma. This lemma will, among other things, help us answer the question at the start of the paper. It is also very useful in a wide variety of situations and it would have been a shame had we deemed this endeavor not "worth it" when we first started. The lemma has a couple of cases: when the prime p is odd and when it is even.

3.1 For odd primes

Using lemma 2.3 and a proof by induction we can prove the following:

Theorem 1. *If p is an odd prime with x and y integers such that $p \nmid x, y$ and $p \mid x - y$ then:*

$$\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n).$$

Proof. Write $n = p^k m$ for some non-negative integer k and positive integer $m \perp p \Leftrightarrow p \nmid m$. We will show the theorem by induction on k.

For the base case $k = 0$, we have that

$$\nu_p\left(x^{p^0 m} - y^{p^0 m}\right) = \nu_p\left(x^{1 \cdot m} - y^{1 \cdot m}\right) = \nu_p(x - y) + 0$$

by Lemma 2.1 as desired.

Next consider the induction step. From the induction hypothesis the theorem holds when the exponent is $p^{k-1}m$. Note $p \mid x - y \Rightarrow p \mid x^p - y^p$ and $p \nmid x, y \Rightarrow p \nmid x^p, y^p$. Therefore we get that

$$\begin{aligned}\nu_p\left(x^{p^k m} - y^{p^k m}\right) = \nu_p\left((x^p)^{p^{k-1} m} - (y^p)^{p^{k-1} m}\right) &= \nu_p\left(x^p - y^p\right) + (k - 1) \\ &= \nu_p(x - y) + 1 + (k - 1)\end{aligned}$$

with the last step being due to Lemma 2.2. Since $1 + (k - 1) = k = \nu_p(n)$ this completes the induction step and therefore the proof. □

3.2 For $p = 2$

When $p = 2$ we will get something slightly different. In fact, we usually split the $p = 2$ case into two separate theorems depending on the parity of the exponent. Luckily, when the exponent is odd we can refer back to Lemma 2.1.

Theorem 2. *If x and y are odd and n is even then*

$$\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(x + y) + \nu_2(n) - 1.$$

Proof. This proof will be very similar to the proof of Theorem 1. Write $n = 2^k m$ for some positive integers k and m with m odd. We will show the theorem by induction on k.

For the base case $k = 1$, note that x, y are odd and therefore so are x^2 and y^2. Therefore we get that

$$\nu_2\left(\left(x^2\right)^m - \left(y^2\right)^m\right) = \nu_2\left(x^2 - y^2\right) = \nu_2(x - y) + \nu_2(x + y) + \nu_2(n) - 1$$

by Lemma 2.3 as desired.

Next consider the induction step. From the induction hypothesis the theorem holds when the exponent is $2^{k-1}m$. Therefore we get that

$$\begin{aligned}\nu_2\left(\left(x^2\right)^{2^{k-1}m} - \left(y^2\right)^{2^{k-1}m}\right) &= \nu_2\left(x^2 - y^2\right) + \nu_2\left(x^2 + y^2\right) + \nu_2\left(2^{k-1}m\right) - 1 \\ &= \nu_2(x - y) + \nu_2(x + y) \cancel{+1} + \nu_2(n) \cancel{-1} - 1\end{aligned}$$

noting that $\nu_2\left(x^2 + y^2\right) = 1$ because $x^2, y^2 \equiv 1 \pmod 4$, and also $\nu_2(n) - 1 = \nu_2\left(2^{k-1}m\right)$. This completes the induction step and therefore the proof. □

This paper started with a simple question that barely seemed worth studying, but by trying to answer this question and by making generalisations when possible we were able to prove some very powerful theorems that we would never have found without curiosity and persistence. The process of proving these theorems has also taught us that it is sometimes necessary to look at simpler and more specific cases before proving a general result. The theorems and lemmas in this chapter are known collectively as the Lifting The Exponent (LTE) lemma. This will be discussed further in the next section.

4 Applications

Now we will look at how one can apply the LTE-lemma to solve some problems. There are four sections below each dealing with different aspects of applying LTE. Each section includes some examples, some exercise problems and some comments relating to the different ideas presented.

4.1 Choosing the prime p

For some problems it is easy to guess that the LTE-lemma may be helpful. Then the difficulty often lies in figuring out which prime(s) to look at. Consider the following problem:

Example 4.1. Prove that the number $a^{a-1} - 1$ is never square-free[1] for all integers $a > 2$.

The problem is equivalent to finding a prime which divides $a^{a-1} - 1$ twice. The expression looks very well suited for LTE, but we do not yet know which prime to consider. So in the rudest way possible suppose we consider *any* prime p which divides $a - 1$. Then if p is odd: $\nu_p(a^{a-1} - 1) = \nu_p(a - 1) + \nu_p(a - 1) = 2\nu_p(a - 1)$, which finishes immediately. A complete proof for this example may look like the one below.

Proof Example 4.1. Since $a > 2$ there must exist some prime p which divides $a-1$. For odd p, the LTE-lemma gives: $\nu_p(a^{a-1}-1) = \nu_p(a-1)+\nu_p(a-1) \geq 2$, so $p^2 \mid a^{a-1} - 1$ as desired. If $p = 2$ then $a - 1$ must be even which gives: $\nu_2(a^{a-1} - 1) = \nu_2(a - 1) + \nu_2(a + 1) + \nu_2(a - 1) - 1 \geq 2$ as desired. □

While it worked here, it will often NOT be the case that choosing any random prime will work. Still, it often is helpful to look at the exponents and bases. For these next problems choosing suitable primes may require some attention.

Exercise 4.1. Let k be a positive integer. What is the smallest positive integer n so that $11^n - 1$ has k trailing zeroes?

Exercise 4.2 (Ireland 1996)**.** Let p be a prime number. Show that $2^p + 3^p$ cannot be a perfect power[2].

Exercise 4.3 (Iran 2008)**.** Fix $a \in \mathbb{N}$. Suppose $4(a^n + 1)$ is a perfect cube for all $n \in \mathbb{N}$. Prove that $a = 1$.

In the exercises above choosing a relevant prime for LTE may have been a little tricky, especially for exercise 4.3. If you have not solved exercise 4.3 yet we encourage you to push on, because it is a very neat problem!

Nevertheless the relevant primes should not be too difficult to find. Indeed, let us consider a substantially more challenging problem:

Example 4.2. Let $k > 1$ be an integer. Show that there exists infinitely many positive integers n such that

$$n \mid 1^n + 2^n + \cdots + k^n.$$

[1] An integer n is said to be square-free if there does not exist a positive integer $b \neq 1$ such that $b^2 \mid n$.

[2] A perfect power is a natural number that can be expressed as a^m for integers $a, m > 1$.

In these kinds of problems one often falls into the trap of trying to fill *all* possible values of n which work. However, this is often not feasible to study and is unlikely to reveal any coherent patterns. Instead we should restrict ourselves to only study *nice* values of n. *Nice* values could mean anything: squares of integers, odd multiples of 2023, Fermat primes, etc., but preferably something that makes the problem easier to analyse. In this example we will see that it is beneficial to study prime powers.

Proof Example 4.2. Note that either k or $k+1$ will be odd, and therefore have an odd prime divisor p. We will show that taking $n = p^m$ will work for all $m \in \mathbb{N}$. Firstly, if k is even then $k+1$ is odd. Therefore $p \mid a + (k+1-a)$ for all $a \in \{1, 2, \ldots, \frac{k}{2}\}$. For $p \mid a \Rightarrow p \mid k+1-a$ we have

$$\nu_p\left(a^n + (k+1-a)^n\right) \geq \min\{\nu_p(a^n), \nu_p\left((k+1-a)^n\right)\} \geq n = p^m > m.$$

And for $p \nmid a \Rightarrow p \nmid k+1-a$ LTE gives that

$$\nu_p\left(a^n + (k+1-a)^n\right) = \nu_p(a + (k+1-a)) + \nu_p(n) > \nu_p(n) = \nu_p(p^m) = m.$$

Considering these two cases together we have that $p^m \mid a^n + (k+1-a)^n$ for all $a \in \{1, 2, \ldots, \frac{k}{2}\}$. Therefore we have that $n \mid 1^n + 2^n + \cdots + k^n$ as desired.

Secondly, if k is odd then we have already concluded that $n \mid 1^n + 2^n + \cdots + (k-1)^n$. Left to note is that $p \mid k$ which implies that $p^m \mid k^n$ since $m < p^m = n$. Therefore we have that $n \mid 1^n + 2^n + \cdots + k^n$ as desired. □

Another idea for finding a good prime not mentioned thus far is looking at the smallest/largest prime factors of some expression. One should also always test small primes, like 2, 3, 5 and 7, to see if they yield some helpful constraints.

Exercise 4.4. Find all positive integers n such that

$$2^{n^2} - n^n = 6n^{n+1} - 1.$$

4.2 Using LTE

While LTE is a useful tool in and of itself, it is very often combined with other tools. Some examples of other helpful tools which we will explore in this section are: Fermat's Little Theorem, Modulo and Orders[3]. Other relevant tools not discussed in this text include Wilsson's Theorem and Euler's Theorem.

Example 4.3 (Swedish Training-camp 2023)**.** Let p be a prime. Find all positive integers n with the following property: if $x^n - 1$ is divisible by p for some integer x, then $x^n - 1$ is also divisible by p^2.

[3]For some good material regarding orders we would like to recommend: `https://static1.squarespace.com/static/5fe101b108d85d5e817a934a/t/62b4964e8a2c88240860a5bc/1656002143465/Orders_and_Primitive_Roots_Minerva.pdf`

Since this problem gives a lot of freedom in the choice of x, a good way to gain intuition will be to try to construct some x such that the condition does not hold. For this problem one can refer back to Lemma 2.1 which gives that $\nu_p(x^n-1) = \nu_p(x-1)$ if $p \mid x-1$ and $p \nmid n$. From there it is not difficult to guess that the answer will be all n divisible by p.

Proof Example 4.3. Assume $p \nmid n$. Choosing $x = p+1$ gives $p = x-1 \mid x^n - 1$, but by LTE $\nu_p(x^n-1) = \nu_p(x-1) = 1$ which means that $p^2 \nmid x^n - 1$.

Assume instead that $p \mid n$ and let $n = pm$ for some positive integer m. We must show that the implication holds for all x. By Fermat's Little Theorem we have that $x^n = (x^m)^p \equiv x^m \pmod{p}$. Therefore $p \mid x^n - 1 \Rightarrow p \mid x^m - 1$. Now LTE finishes immediately:

$$\nu_p(x^n-1) = \nu_p((x^m)^p - 1) = \nu_p(x^m - 1) + \nu_p(p) \geq 1 + 1 = 2.$$

□

Exercise 4.5. Let a, n be two positive integers and let p be an odd prime number such that:

$$a^p \equiv 1 \pmod{p^n}.$$

Prove that

$$a \equiv 1 \pmod{p^{n-1}}.$$

Exercise 4.6. Let a, b, c be positive integers such that $c \mid a^c - b^c$. Prove that $c \mid \frac{a^c - b^c}{a-b}$.

Example 4.4 (IMO 1990 P3)**.** Determine all integers $n > 1$ such that

$$\frac{2^n + 1}{n^2}$$

is an integer.

Proof Example 4.4. Note that n cannot be even since $2 \nmid 2^n + 1$. Consider the smallest prime factor p of n. Note that $p \mid 2^n + 1 \Rightarrow 2^n \equiv -1 \pmod{p} \Rightarrow 4^n \equiv 1 \pmod{p}$. Therefore $\mathrm{ord}_p(4) \mid n$ and $\mathrm{ord}_p(4) \mid \phi(p) \Rightarrow \mathrm{ord}_p(4) \mid \gcd(n, \phi(p)) = 1$, with the last step following from that p is the smallest prime factor of n and therefore also it's smallest proper factor. This implies $\mathrm{ord}_p(4) = 1 \Rightarrow 4^1 \equiv 1 \pmod{p} \Rightarrow p = 3$. Now write $n = 3m$. By LTE we now get

$$\nu_3(2^n + 1) = \nu_3(2+1) + \nu_3(n).$$

However, we must have $1 + \nu_3(n) = \nu_3(2^n + 1) \geq \nu_3(n^2) = 2\nu_3(n)$, which implies $\nu_3(n) \leq 1 \Rightarrow 3 \nmid m$.

If $m = 1$ we can check that the condition holds. Now suppose $m > 1$. We will then consider the smallest prime factor q dividing m and note that $q \mid 2^n + 1 = 8^m + 1 \Rightarrow 8^m \equiv -1 \pmod{q} \Rightarrow 64^m \equiv 1 \pmod{q}$. Therefore $\mathrm{ord}_q(64) \mid m$ and $\mathrm{ord}_q(64) \mid \phi(q) \Rightarrow \mathrm{ord}_q(64) \mid \gcd(m, \phi(q)) = 1$, with the last step following from that q is the smallest prime factor of m and therefore also it's smallest

proper factor. This implies $\text{ord}_q(64) = 1 \Rightarrow 64^1 \equiv 1 \pmod{q} \Rightarrow q \mid 63 = 3^2 \cdot 7$. Therefore $q = 7$ since $q \mid m$ but $3 \nmid m$. However this is impossible as $8^m + 1$ cannot be divisible by 7 since it is congruent to 2 modulo 7.

In conclusion the only n for which $n^2 \mid 2^n + 1$ is $n = 3$. □

4.3 The case $p = 2$

It can often be easy to forget that p can be 2. Then the statement of the main LTE-lemmas are slightly different, and one has to divide into cases based on if the exponent is even or odd. This section is here to serve as a reminder to always check if p can be 2, and if so to deal with it separately.

Exercise 4.7. Show that a number with binary representation $111\ldots1$ cannot be a perfect power.

Exercise 4.8 (Romania TST 2009)**.** Let $a, n \geq 2$ be integers, which have the following property: there exists an integer $k \geq 2$, such that n divides $(a-1)^k$. Prove that n also divides $a^{n-1} + a^{n-2} + \cdots + a + 1$.

Exercise 4.9. Find all positive integers n such that $2^n \mid 3^n - 1$.

4.4 Inequalities and Bounding

It may sound surprising at first, but creative use of LTE can lead to some very powerful inequalities. In fact in recent years problems[4] at the highest level of competition for high-school students, the International Mathematical Olympiad (IMO), have relied on bounding $\nu_p(n!)$ and $\nu_p(x^k - y^k)$ using the lemma[5] $v_p(n!) = \frac{n - \tau_p(n)}{p-1}$ and LTE respectively.

Example 4.5 (Bulgaria 1997)**.** For some integer $n \geq 2$, the number $3^n - 2^n$ is a perfect power of a prime. Prove that n is a prime.

Proof Example 4.5. Assume that n is not prime but $3^n - 2^n$ is a power of a prime. Let this prime be p and the power be p^w. Note that $w > 0$ since $3^n - 2^n > 1$ for $n \geq 2$. Therefore $p \mid 3^n - 2^n$. Since neither 2 nor 3 divides $3^n - 2^n$, we can conclude that $p \neq 2, 3$.

Since n is composite, we can let $n = ab$ for some positive integer $a, b \geq 2$. Since $3^a - 2^a \mid 3^{ab} - 2^{ab}$ we must have that $3^a - 2^a$ is also a power of p. Now we can apply LTE and notice that

$$\begin{aligned} \nu_p\left((3^a)^b - (2^a)^b\right) &= \nu_p(3^a - 2^a) + \nu_p(b) \\ \Rightarrow 3^{ab} - 2^{ab} &= (3^a - 2^a) \cdot p^{\nu_p(b)} \leq (3^a - 2^a)b \\ \Rightarrow \underbrace{3^{a(b-1)} + 3^{a(b-2)}2^a + \cdots + 3^a 2^{a(b-2)} + 2^{a(b-1)}}_{\text{sum of } b \text{ integers greater than 1}} &\leq b \end{aligned}$$

which is a contradiction. Hence our assumption that n was composite must be false. Therefore we can conclude that n is a prime as desired. □

[4] See IMO 2022 P5 and IMO 2019 P4.

[5] Here $\tau_p(n)$ is the digit-sum of n in base p.

Exercise 4.10. Find all positive integer solutions to the equation

$$x^{2009} + y^{2009} = 7^z.$$

Exercise 4.11. For a prime p, find all positive integers x, y such that

$$p^x - y^p = 1.$$

Exercise 4.12. For all odd positive integers n, prove that

$$n^2 \mid 2^{n!} - 1.$$

Exercise 4.13 (IMO 2022 P5 Modified)**.** Find all pairs of positive integers a, b such that

$$a^a = b! + a.$$

5 Further Reading

There are several mathematical ideas closely related to the notion of *p-adic valuation* and the result of the Lifting the Exponent Lemma. Some of these we see fit to mention below before concluding this text.

Firstly, for completeness sake we should mention that the *p-adic valuation* can be extended to the rational numbers. The definition is very straightforward: let $\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b)$. Most properties of the *p-adic valuation* mentioned in this text still hold for rational inputs, but some do not. For example the inequality $\nu_p(r) \leq \log_p|r|$ is only universally valid for the integers, excluding zero. Interestingly the LTE lemma itself holds to some degree. The bases x, y can be rational, but the exponent n must still be a positive integer. Specifically, the conditions that $p \nmid x, y$ and $p \mid x - y$ are reformulated as $\nu_p(x) = \nu_p(y) = 0$ and $\nu_p(x - y) > 0$ respectively.

Secondly we should mention two closely related theorems to LTE, namely Zsigmondy's Theorem and Catalan's Conjecture. The second of these is still called a conjecture because it was first proven as recently as 2002 by Preda Mihăilescu after being conjectured all the way back in 1844 by Eugène Charles Catalan. The statements of the two theorems are as follows:

Theorem 3 (Zsigmondy's Theorem)**.** *If $a > b > 0$ are coprime integers, then for any integer n, there exists a prime number p that divides $a^n - b^n$ but does not divide $a^k - b^k$ for any positive integer $k < n$, with the following exceptions:*

- *$n = 1$ and $a - b = 1$,*
- *$n = 2$ and $a + b$ is a power of 2,*
- *$n = 6$, $a = 2$ and $b = 1$.*

Theorem 4 (Catalan's Conjecture)**.** *The only solution to the equation*

$$x^a - y^b = 1$$

in integers $a, b > 1$, $x, y > 0$ is $(a, b, x, y) = (2, 3, 3, 2)$.

The astute reader may notice that Exercise 4.11. in this text is a special case of Catalan's Conjecture. For the interested, we also refer to an elementary proof[6] of Zsigmondy's Theorem using the LTE lemma and cyclotomic polynomials.

6 Hints

Here are some hints for the exercise problems in section 4.

4.1. For a number to have k trailing zeroes, what does that imply about the number's prime factorisation?

4.2. A perfect power cannot be divisible by a prime exactly once.

4.3. Consider a prime other than 2 dividing $a^m + 1$.

4.4. Prove that n is odd, then apply LTE.

4.5. Use Fermat's Little Theorem.

4.6. Consider the distinct prime factors of c separately and try to use Fermat's Little Theorem.

4.7. A number with a binary representation of 111...1 is one less than a power of 2.

4.8. The condition says that every prime which divides n also divides $a - 1$.

4.9. Divide into cases depending on the parity of the exponent n.

4.10. Note that $(x^{41})^{7^2} + (y^{41})^{7^2} = x^{2009} + y^{2009}$.

4.11. First check $p = 2$. Then use LTE and the fact that $y^p + 1$ is a perfect power of p.

4.12. If $n \neq 1$, for all primes $p \mid n$ we have $p \mid 2^{p-1} - 1 \mid 2^{n!} - 1$ since $n > p - 1$.

4.13. Divide into cases depending on whether a is prime or composite. Also note that $b! < b^b - b$ for $b > 2$.

[6] https://angyansheng.github.io/blog/an-elementary-proof-of-zsigmondys-theorem