Lifting The Exponent

The "**lifting the exponent**" (LTE) lemma is a useful one about the largest power of a prime dividing a difference or sum of n^{th} powers. Here are some sample problems whose solutions use the lemma.

1. Let n be a squarefree integer. Show that there is no pair of coprime positive integers (x, y) such that
$$(x+y)^3 | (x^n + y^n).$$
2. Show that 2 is a primitive root mod 3^k for all positive k.
3. Find all solutions in positive integers to $3^n = x^k + y^k$, where $\gcd(x, y) = 1, k \geq 2.$
4. Suppose a and b are positive real numbers such that $a - b, a^2 - b^2, a^3 - b^3, \ldots$ are all positive integers. Show that a and b must be positive integers.

Contents

LTE Lemma Statement

DEFINITION

Let p be a prime and n a nonzero integer. Then we define $v_p(n)$ to be the exponent of p in the prime factorization of n. That is,
$$v_p(n) = k \Leftrightarrow p^k | n \text{ and } p^{k+1} \nmid n.$$

THEOREM

Let p be a prime, x and y integers, n a positive integer, and suppose that $p | (x - y)$ but $p \nmid x$ and $p \nmid y$. Then
(1) if p is odd,
$$v_p(x^n - y^n) = v_p(x - y) + v_p(n);$$
(2) for $p = 2$ and even n,
$$v_2(x^n - y^n) = v_2(x - y) + v_2(n) + v_2(x + y) - 1.$$

Notice that if n is odd, we can substitute $-y$ for y in (1) to obtain
$$v_p(x^n + y^n) = v_p(x + y) + v_p(n)$$
if $p | (x + y)$.

EXAMPLE

Use the LTE lemma to find the largest power of 3 dividing $5^{18} - 2^{18}$.

By LTE,
$$v_3(5^{18} - 2^{18}) = v_3(5 - 2) + v_3(18) = 1 + 2 = 3.$$
So the answer is 3^3.

Without LTE, the problem can be solved by factoring
$$\begin{aligned} 5^{18} - 2^{18} &= (5^9 - 2^9)(5^9 + 2^9) \\ &= (5^3 - 2^3)(2^6 + 2^3 5^3 + 5^6)(5^9 + 2^9) \\ &= (5 - 2)(2^2 + (2)(5) + 5^2)(2^6 + 2^3 5^3 + 5^6)(5^9 + 2^9). \end{aligned}$$

The first factor has one 3 and the fourth factor has no 3s, and some careful mod-9 analysis shows that the second and third factors are divisible by 3 but not 9, so the total number of factors of 3 is 3. This is quite a bit more complicated (but note that it also indicates how an inductive proof of LTE might proceed). $\square$

This lemma gives a practical way to solve many problems involving the largest power of a prime that divides certain expressions. In particular, the solutions to the problems in the introduction all use LTE in an essential way.

As a warmup, here is a typical Diophantine equation that can be tackled using the LTE Lemma.

TRY IT YOURSELF

Find all positive integers x, y and positive prime numbers p such that

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

Enter your answer as the sum $\sum(p_i + x_i + y_i)$, where the sum runs over the solutions (p, x, y) to the equation.

Submit your answer

Solution to Problem 1

Assume $(x+y)^3|(x^n+y^n)$ with $\gcd(x,y)=1$. We will derive a contradiction.

First, suppose n is even. If there is an odd prime $p|(x+y)$, then $x^n+y^n \equiv x^n+(-x)^n \equiv 2x^n \bmod p$, so $p|x$, so $p|y$, contradiction. Since x and y are positive, the only possible way that there is no odd prime p dividing $x+y$ is if $x+y$ is a power of 2. In this case, x and y are both odd since they are coprime, so since n is even x^n and y^n are both $1 \bmod 8$, so $v_2(x^n+y^n)=1$, but $v_2\left((x+y)^3\right) \geq 3$, so again we get a contradiction.

Now suppose n is odd. If there is an odd prime $p|(x+y)$, then $3v_p(x+y) \leq v_p(x^n+y^n)$. Then LTE gives

$$3v_p(x+y) \leq v_p(x^n+y^n) = v_p(x+y)+v_p(n) \leq v_p(x+y)+1$$

since n is square-free. Simplifying, we get $v_p(x+y) \leq \frac{1}{2}$, which is impossible since $p|(x+y)$.

As above, the only remaining case is when $x+y$ is a power of 2. But in this case, $v_2(x^n+y^n)=v_2(x+y)$ if n is odd, because x and y are odd and the expansion of

$$\frac{x^n+y^n}{x+y} = x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1}$$

has an odd number of terms, all of which are odd. So it is impossible for $(x+y)^3$ to divide x^n+y^n, since the power of 2 on the left exceeds the power of 2 on the right. $\square$

Solution to Problem 2

We seek the smallest positive n such that $2^n \equiv 1 \bmod 3^k$. If $3^k|(2^n-1)$, first note that $2^n \equiv 1 \bmod 3$, so n is even. Write $n=2m$. So $3^k|(4^m-1)$. Now LTE applies:

$$k \leq v_3(4^m-1^m) = v_3(4-1)+v_3(m) = 1+v_3(m).$$

So $v_3(m) \geq k-1$. The smallest possible such m is 3^{k-1}, so the smallest possible n is $2 \cdot 3^{k-1} = \phi(3^k)$, where ϕ is Euler's totient function. This proves the claim. $\square$

Here is a similar problem to try:

TRY IT YOURSELF

$$3^x = 2^x y + 1$$

Submit your answer

How many pairs of positive integers (x, y) satisfy the equation above?

Solution to Problem 3

If one of x or y is divisible by 3, then they both are, which is a contradiction. So neither is. If k is even, then x^k and y^k are both $1 \bmod 3$, so x^k+y^k is not divisible by any power of 3.

Now suppose k is odd. If $n = 0$, then $x^k + y^k = 1$, and there are no solutions to this in positive integers, so we can exclude this case. Since $n \geq 1$, $3|(x + y)$. Apply LTE:

$$n = v_3(x^k + y^k) = v_3(x + y) + v_3(k).$$

Then

$$x^k + y^k = 3^n = 3^{v_3(x+y)} 3^{v_3(k)} = (x + y)k.$$

The point is that the left side is usually much bigger than the right side, so the result will follow from some routine inequalities.

Suppose $x > y$ without loss of generality. Then dividing through by $x + y$ gives

$$x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1} = k$$
$$(x - y)\left(x^{k-2} + x^{k-4}y^2 + \cdots + xy^{k-3}\right) + y^{k-1} = k.$$

The left side is $\geq x^{k-2}$, so $x^{k-2} \leq k$. So $\ln(x) \leq \frac{\ln(k)}{k-2}$. Recall $k \geq 3, x \geq 2$. By calculus, the right side is decreasing for $k \geq 3$, so $\ln(x) \leq \ln(3)$, so $x \leq 3$. We already ruled out $3|x$, so $x = 2$ and hence $y = 1$.

In that case $2^{k-2} > k$ already unless $k = 3, 4$, but k is odd so $k = 3$. It's easy to check that $x = 2, y = 1, k = 3$ is a solution, as is $x = 1, y = 2, k = 3$ if we relax the $x > y$ assumption, and the above analysis has shown that these are the only ones. $\square$

Solution to Problem 4

Since $a - b \in \mathbb{Z}$ and $a^2 - b^2 \in \mathbb{Z}$, $a + b = \frac{a^2-b^2}{a-b} \in \mathbb{Q}$. But then $a = \frac{1}{2}(a - b) + \frac{1}{2}(a + b)$ and $b = \frac{1}{2}(a + b) - \frac{1}{2}(a - b)$ are rational numbers as well.

Now, write $a = \frac{x}{z}$ and $b = \frac{y}{z}$ as quotients of positive integers, with a common denominator. Choose z as small as possible. Then the conditions of the problem imply that

$$z^n | (x^n - y^n) \text{ for all } n.$$

Suppose p is a prime dividing z. Note $z|(x - y)$ so $p|(x - y)$. If $p|x$ then $p|y$ as well, but that violates the choice of z: we could write $a = \frac{\frac{x}{p}}{\frac{z}{p}}, b = \frac{\frac{y}{p}}{\frac{z}{p}}$ to get a smaller common denominator.

So $p \nmid x, y$ and we are set up to apply LTE. If p is odd then

$$n \leq v_p(z^n) = v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

Taking p to both sides gives

$$p^n \leq (x - y)n$$
$$\frac{p^n}{n} \leq (x - y)$$

but this is impossible since the left side goes to infinity as $n \to \infty$, and the right side is a constant independent of n.

If $p = 2$, we get

$$n \leq v_2(z^n) = v_2(x^n - y^n) = v_2(x - y) + v_2(n) + v_2(x + y) - 1,$$

so

$$\frac{2^{n+1}}{n} \leq (x - y)(x + y)$$

and we get a similar contradiction.

The conclusion is that there is no prime p dividing z. So $z = 1$ and a and b are both positive integers. $\square$

Proof of LTE

Here is an outline of the proof for odd primes p; the proof for $p = 2$ is similar. Suppose $p|(x - y)$, $p \nmid x, p \nmid y$.

Step 0: If $p \nmid a$, then $v_p(x^a - y^a) = v_p(x - y)$.

To see this, write $\frac{x^a-y^a}{x-y} = x^{a-1} + x^{a-2}y + \cdots + y^{a-1}$, and since $x \equiv y$ mod p this becomes

$$x^{a-1} + x^{a-1} + \cdots + x^{a-1} \equiv ax^{a-1} \pmod{p},$$

which is nonzero since $p \nmid a$ and $p \nmid x$.

Step 1: Prove it for $n = p$.

In this case, $v_p(x^p - y^p) = v_p(x-y) + v_p(x^{p-1} + x^{p-2}y + \cdots + y^{p-1})$, so the idea is to show that the latter term equals $v_p(p) = 1$.

To do this, write $y = x + pk$ for some k, and expand as a polynomial in p, looking mod p^2 (throwing out terms with p^2 or higher). Eventually we get

$$\begin{aligned} x^{p-1} + x^{p-2}y + \cdots + y^{p-1} &\equiv x^{p-1} + (x^{p-1} + pkx^{p-2}) + (x^{p-1} + 2pkx^{p-2}) \\ &\quad + \cdots + \left(x^{p-1} + (p-1)pkx^{p-2}\right) \\ &\equiv px^{p-1} + \frac{p(p-1)}{2}pkx^{p-2} \\ &\equiv px^{p-1} \pmod{p^2}. \end{aligned}$$

So it is divisible by p but not p^2, as desired.

Step 2: Write $n = p^k a$, $a \nmid p$, and use the previous two steps repeatedly.

That is,

$$\begin{aligned} v_p(x^n - y^n) &= v_p\left(\left(x^{p^k}\right)^a - \left(y^{p^k}\right)^a\right) \\ &= v_p\left(x^{p^k} - y^{p^k}\right) && \text{(Step 0)} \\ &= v_p\left(\left(x^{p^{k-1}}\right)^p - \left(y^{p^{k-1}}\right)^p\right) \\ &= v_p\left(x^{p^{k-1}} - y^{p^{k-1}}\right) + 1 && \text{(Step 1)} \end{aligned}$$

and iterating the last two lines (or using induction) eventually gives $v_p(x-y) + k$, which is $v_p(x-y) + v_p(n)$. $\square$