# A nice and tricky lemma (lifting the exponent)

**Santiago Cuellar, Jose Alejandro Samper**

This article presents a powerful lemma which is useful in solving olympiad problems.

**Lemma:** Let $p$ be an odd prime. For two different integers $a$ and $b$ with $a \equiv b(\bmod p)$ and a positive integer $n$, the exponent of $p$ in $a^n - b^n$ is equal to the sum of the exponent of $p$ in $a - b$ and the exponent of $p$ in $n$.

Let us introduce notation $p^a || n \iff p^a | n$ and $p^{a+1} \nmid n$, where $a, p, n \in \mathbb{Z}$. It allows us to state the lemma as follows

Let $p$ be an odd prime and let $a, b, n \in \mathbb{Z}$. Then $p^\alpha || a - b$ and $p^\beta || n$ implies $p^{\beta+\alpha} || a^n - b^n$.

**Proof:** Let us prove that if $a \equiv b(\bmod p)$ and $p^\beta || n$ then $p^\beta || \dfrac{a^n - b^n}{a - b}$. It is clear that the lifting lemma will follow, because with the condition $p^\alpha || a - b$ we have $p^{\alpha+\beta} || a^n - b^n$.

Assume $n = p^\beta k$. We fix $k$ and proceed by mathematical induction on $\beta$. The base case is $\beta = 0$. It follows that $p \nmid n$ and we have

$$\begin{aligned}
a^k &\equiv b^k (\bmod p)\\
a^k b^{n-k-1} &\equiv b^{n-1} (\bmod p)\\
\sum_{k=0}^{n-1} a^k b^{n-k-1} &\equiv \sum_{k=0}^{n-1} b^{n-1} (\bmod p)\\
&\equiv n b^{n-1} (\bmod p)\\
&\not\equiv 0 (\bmod p)
\end{aligned}$$

Because $\dfrac{a^n - b^n}{a - b} = \displaystyle\sum_{i=0}^{n-1} a^{n-i-1} b^i$ we get $\dfrac{a^n - b^n}{a - b}$ is not multiple of $p$.

Assume that $p^\beta || \dfrac{a^n - b^n}{a - b}$. We want to prove that $p || \dfrac{a^{np} - b^{np}}{a^n - b^n}$. As $p | a - b$, we have $a = b + xp$ and $a^k \equiv b^k + k b^{k-1} xp (\bmod p^2)$

$$\begin{aligned}
\frac{a^{np} - b^{np}}{a^n - b^n} &= \sum_{i=0}^{n-1} a^{n(p-i-1)} b^i\\
&\equiv \sum_{i=0}^{n-1} \left( b^{n(p-i-1)} + ixpb^{n(p-i-1)-1} \right) b^i (\bmod p^2)
\end{aligned}$$

From it is clear that $p||\dfrac{a^{np}-b^{np}}{a^n-b^n}$. Therefore

$$p^\beta \cdot p\ ||\frac{a^n-b^n}{a-b}\cdot\frac{a^{np}-b^{np}}{a^n-b^n} \Leftrightarrow p^{\beta+1}||\frac{a^{np}-b^{np}}{a-b}.$$

The lemma is proven.

**A special case of the lemma,** $p=2$**.**

Let $a,b,n\in\mathbb{Z}$ such that $2^\alpha||\dfrac{a^2-b^2}{2}$ and $2^\beta||n$. Then

$$2^{\beta+\alpha}||a^n-b^n.$$

**Proof:** Again it is enough to prove that if $2|\dfrac{a^2-b^2}{2}$ and $2^\beta||n$, $\beta\geq 1$, then $2^{\beta-1}||\dfrac{a^n-b^n}{a^2-b^2}$.

Assume $n=2^\beta m$, where $m$ is odd. We fix $m$ and proceed by mathematical induction on $\beta$. The base case is $\beta=1$ or $n=2m$. From $2|\frac{a^2-b^2}{2}$ we get $2|a-b$. Therefore

$$\begin{aligned}
a &\equiv b(\bmod 2)\\
a^{2m-2i-2}b^{2i} &\equiv b^{2m-2}(\bmod 2)\\
\sum_{i=0}^{2m-2} a^{2m-2i-2}b^{2i} &\equiv mb^{2m-2}(\bmod 2)\\
&\equiv 1(\bmod 2)
\end{aligned}$$

Because $\dfrac{a^{2m}-b^{2m}}{a^2-b^2}=\displaystyle\sum_{i=0}^{2m-2}a^{2m-2i-2}b^{2i}$ we get $\dfrac{a^{2m}-b^{2m}}{a^2-b^2}$ is an odd number that is equivalent to $2^0||\dfrac{a^{2m}-b^{2m}}{a^2-b^2}$.

Assume that

$$2^{\beta-1}||\frac{a^n-b^n}{a^2-b^2}.$$

We know that $a$ and $b$ are odd, and $n$ is even, thus

$$\begin{aligned}
a^n &\equiv 1(\bmod 4)\\
b^n &\equiv 1(\bmod 4)\\
a^n+b^n &\equiv 2(\bmod 4)
\end{aligned}$$

It follows that 2 is the greatest power of 2 that divides $a^n + b^n$ or $2||a^n + b^n$. Multiplying this result with the induction hypothesis we obtain

$$2^\beta || \frac{a^n - b^n}{a^2 - b^2} \cdot (a^n + b^n) = \frac{a^{2n} - b^{2n}}{a^2 - b^2} \cdot (a^n + b^n).$$

The special case of the lemma is proven.

*Remark:* Note that if $\beta = 0$ the special case of the lemma is only true if $4|a - b$.

We continue with the problems that are examples how the lemma can be applied.

**Problem 1.** Find the least positive integer $n$ satisfying: $2^{2007}|17^n - 1$.

**Solution:** We have $2^4 || \frac{17^2 - 1}{2}$. Suppose $2^\alpha || n$. The lemma tells us $2^{4+\alpha}||17^n - 1$. We want to have $\alpha + 4 \geq 2007 \Rightarrow \alpha \geq 2003$. This means that $2^{2003}|n$ which implies that $n \geq 2^{2003}$. Using our lemma we obtain $2^{2007}|17^{2^{2003}} - 1$. Thus the minimum value of $n$ is $2^{2003}$.

**Problem 2:** *(Russia 1996)* Let $a^n + b^n = p^k$ for positive integers $a, b$ and $k$, where $p$ is an odd prime and $n > 1$ is an odd integer. Prove that $n$ must be a power of $p$.

**Solution:** We can factor $p^k = a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + ... - ab^{n-2} + b^{n-1})$, because $n$ is odd. Therefore $a + b = p^r$ for some positive integer $r$ less or equal to $k$. Since $a$ and $b$ are positive integers we have $r \geq 1$. Now suppose that $p^\beta||n$. Using our lemma we get $p^{r+\beta}||a^n - (-b)^n = a^n + b^n = p^k$.

This last result is equivalent to $p^{r+\beta}||p^k \Rightarrow \beta = k - r$.

This means that we have to take the least integer $n$ such that $p^\beta||n$ in order to have $a^n + b^n = p^k$, because $a^m + b^m \geq a^n + b^n$ for $m > n$. The least positive integer $n$ such that $p^\beta||n$ is $p^\beta$. Thus $n$ must be a power of $p$ and we are done.

**Problem 3:** *(IMO 1990)* Find all positive integers $n$ such that $n^2|2^n + 1$.

**Solution:** Note that $n$ must be odd because $2^n + 1$ is always odd. Let $p_1$ be the smallest prime divisor of $n$. We have $2^{2n} \equiv 1 (\mathrm{mod}\ p_1)$. Now let $d = \mathrm{ord}_{p_1} 2$. Clearly $d < p_1$, $d|2n$ and $\gcd(n, d) = 1$, because $p_1$ is the least prime that divides $n$. Knowing that we obtain $d|2$, which implies that $d = 1$ or $d = 2$. If $d = 1$ we get $p_1|1$ which is absurd. Thus $d = 2$ and $p_1|3 \Rightarrow p_1 = 3$.

Let us apply our lemma: $3||2 - (-1)$ and we suppose that $3^\beta||n$. Therefore $3^{\beta+1}||2^n - (-1)^n = 2^n + 1^n$. We want now $3^{2\beta}|3^{\beta+1}||2^n + 1$. This means that $2\beta \leq \beta + 1 \iff \beta \leq 1$. Thus $3||n$ and we can write $n = 3n'$ with $\gcd(3, n') = 1$.

Let $p_2$ be the smallest prime that divides $n'$. We have $2^{6n'} \equiv 1 (\mathrm{mod} p_2)$. Letting $d_2 = \mathrm{ord}_{p_2} 2$ we get $d_2 < p_2$ and $d_2 | 6n'$. But $\gcd(d_2, n') = 1$, thus $d_2 | 6$. Clearly $d_2$ can't be 1 or 2 as we proved before. It follows that $d_2 = 3$ or $d_2 = 6$.

If $d_2 = 3$ we have $p_2 | 7 \Rightarrow p_2 = 7$. If $d_2 = 6$ we have $p_2 | 63 = 7 \cdot 9 \Rightarrow p_2 | 7$, hence $p_2 = 7$. Note that $2^3 \equiv 1 (\mathrm{mod} 7) \Rightarrow 2^{k+3} \equiv 2^k (\mathrm{mod} 7)$. Observe that $2^1 \equiv 2 (\mathrm{mod} 7)$ and $2^2 \equiv 4 (\mathrm{mod} 7)$. This means $2^k \equiv -1 (\mathrm{mod} 7)$ does not have solution in integers. Thus $7 \not| 2^{7k} + 1 \forall k$, and $p_2$ does not exist.

Finally we obtain that the only prime divisor of $n$ is 3 and $3||n \Rightarrow n = 3$. It follows that the only solutions are $n = 1$ and $n = 3$.

**Problem 4:** *(IMO 2000)* Does there exist a positive integer $n$ such that $n$ has exactly 2000 prime divisors and $n$ divides $2^n + 1$?

**Solution:** We will prove by induction on $k$ that there exists $n$ with exactly $k$ prime divisors such that $n | 2^n + 1$. Before we start the induction, we observe that the divisors of $n$ will be odd, because $2^n + 1$ is odd for all positive integers n.

The base case is $n = 2$. 9 has just one prime divisor and $9 | 2^9 + 1 = 513$. It also happens that $19 | 513$. Suppose that for $k = t$ there is $n_t$ such that $n_t | 2^{n_t} + 1$ and there exists $p_t$ such that $p_t | 2^{n_t} + 1$, $\gcd(n_t, p_t) = 1$. We will prove that there exist $n_{t+1}$ with $t + 1$ prime divisors such that $n_{t+1} | 2^{n_{t+1}} + 1$ and that there is also a prime $p_{t+1}$ such that $p_{t+1} | 2^{n_{t+1}} + 1$ and $\gcd(n_{t+1}, p_{t+1}) = 1$. We will also prove that $n_{t+1} = n_t p_t$. As $\gcd(n, p_t) = 1 \Rightarrow n_t p_t | 2^{n_t} + 1 | 2^{n_t p_t} + 1$, thus $n_{t+1} = n_t p_t$ works. We will apply our lemma to prove that $p_{t+1}$ exists. Let $q$ be a prime divisor of $n_t$. Suppose $q^\alpha || 2^{n_t} + 1$ and we have $q^0 || p_t$. The lemma tells us that $q^\alpha || 2^{n_{t+1}} + 1$. Now suppose that $p_t^\beta || 2^{n_t} + 1$ and we know $p_t || p_t$. The lemma tells us that $p_t^{\beta+1} || 2^{n_{t+1}} + 1$. This means that all we have to prove

$$p_t(2^{n_t} + 1) < 2^{n_{t+1}} + 1 = (2^{n_t} + 1)(2^{n_t(p_t-1)} - 2^{n_t(p-2)} + ... - 2^{n_t} + 1).$$

This is equivalent to

$$p_t < 2^{n_t(p_t-1)} - 2^{n_t(p-2)} + ... - 2^{n_t} + 1 = 2^{n_t(p-2)} + 2^{n_t(p-4)} + ... + 2^{n_t} + 1.$$

We have $2^{n_t(p_t-1)} - 2^{n_t(p-2)} + ... - 2^{n_t} + 1 > \dfrac{(p_t - 3)}{2} 2^{n_t} + 1 > 2^8(p_t - 3) + 1 > p_t$. This means that there exists a prime $p_{t+1}$ such that $(n_{t+1}, p_{t+1}) = 1$ and $p_{t+1} | 2^{n_{t+1}}$ because $p_t > 3$. The problem is solved.

**Problem 5.** Let $a \geq 3$ be an integer. Prove that there exists an integer $n$ with exactly 2007 prime divisors such that $n|a^n - 1$.

**Solution:** We use mathematical induction on the number of divisors. This problem is interesting, because we need to combine both lemmas.

For the base case we have to prove there exist a prime $p$ such that $p|a-1$ (we will take 2 as the first prime if $a$ is odd). We will prove that there is a power of $p$ such that $a^{p^k} - 1$ has another prime divisor $q$ that is not $p$. If $a$ is even we can apply the lemma directly. We have that the exponent of $p$ in $a^p - 1$ is the exponent of $p$ in $a - 1$ plus one. Thus we need $p = \sum_{i=0}^{p-1} a_i > p$ that is not possible. If $a$ is odd then we have two cases, if $a > 3$ we have that $2|a^2 - 1 = (a-1)(a+1)$ and there is one odd divisor of $a^2 + 1$ because $\gcd(a-1, a+1) = 2$. If $a = 3$ we have that $4|3^4 - 1$ and 5 does also divide it. This completes the base case.

Suppose that $n_k$ has exactly $k$ prime divisors such that $n_k|a^{n_k} - 1$ and there exists $p_k$ such that $p_k|a^{n_k} - 1$ with $\gcd(n_k, p_k) = 1$. This means that $a_k p_k|a^{n_k} - 1|a^{n_k p_k} - 1$. We say that $n_{k+1} = n_k p_k$. Now we have to prove that there exists a prime $p_{k+1}$ such that $\gcd(n_{k+1}, p_{k+1}) = 1$ and $p_{k+1}|a^{n_{k+1}} - 1$. Let us use our lemma. Because we have taken 2 as the first prime (when it was possible) we have no problems with the exponent of 2, as for $k \geq 2$ the exponent of 2 does not increase (from the special case of the lemma). Now for any odd prime divisor of $n_k$ the exponent of $p$ in $a^{n_k} - 1$ and $a^{n_{k+1}} - 1$ are equal except for $p_k$ whose exponent has increased by one. We have

$$a^{n_{k+1}} - 1 = a^{n_k p_k} - 1 = (a^{n_k} - 1)(a^{n_k(p_k-1)} + a^{n_k(p_k-2)} + ... + a^{n_k} + 1)$$

Thus $p_{k+1}$ does not exist whenever $p_k = (a^{n_k(p_k-1)} + a^{n_k(p_k-2)} + ... + a^{n_k} + 1)$ (because the exponent of $p_k$ has increased just by one). But the last equation can not hold, because $a > 1$ and the RHS has $p_k$ added all except one greater than 1. Thus RHS>LHS that proves the existence of $p_{k+1}$ and we are done.

Santiago Cuellar, Jose Alejandro Samper

Colegio Helvetia de Bogota, Colombia