A Property of the Modulo Operation in Number Theory

SOHAM PURKAIT

In this short note, I describe a result in number theory which I have discovered. Here is the statement.

Theorem. *Let x, a, k be integers, $k > 0$, such that the following is true:*

$$x \equiv a \pmod{k}.$$

Then the following is true for any positive integer b:

$$x^{k^b} \equiv a^{k^b} \pmod{k^{b+1}}.$$

Remark. Before proceeding, please note that x^{k^b} means $x^{\left(k^b\right)}$ and **not** $(x^k)^b$ (which is simply x^{kb}). Here, we follow the convention that any expression enclosed within brackets is evaluated first.

Example. To illustrate the theorem, let us start with the statement $5 \equiv 2 \pmod{3}$. Here $x = 5$, $a = 2$, and $k = 3$. We now observe the following relations which may be checked by actual calculation.

- Take $b = 1$. We have:

$$5^3 \equiv 2^3 \pmod{3^2}.$$

- Take $b = 2$. We have:

$$5^{3^2} \equiv 2^{3^2} \pmod{3^3}.$$

Proof. Suppose that $x \equiv a \pmod{k}$. We will build the proof of the statement in stages. Observe that:

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

Keywords: Modulo, congruence, divisible, divisibility, number theory

Next, note the following relations which all follow from $x \equiv a \pmod{k}$ (note that the last relation is trivially true):

$$\begin{aligned}
x^{k-1} &\equiv a^{k-1} \pmod{k},\\
x^{k-2}a &\equiv a^{k-1} \pmod{k},\\
x^{k-3}a^2 &\equiv a^{k-1} \pmod{k},\\
&\cdots\cdots\cdots\cdots\cdots\\
x^1 a^{k-2} &\equiv a^{k-1} \pmod{k},\\
a^{k-1} &\equiv a^{k-1} \pmod{k}.
\end{aligned}$$

Therefore, by addition of the corresponding sides, we obtain, since $ka^{k-1} \equiv 0 \pmod{k}$:

$$x^{k-1} + x^{k-2}a + x^{k-3}a^2 + \cdots + a^{k-1} \equiv 0 \pmod{k}.$$

This is the same thing as saying that k divides $x^{k-1} + x^{k-2}a + x^{k-3}a^2 + \cdots + a^{k-1}$. Since k also divides $x - a$, it follows that k^2 divides $x^k - a^k$, i.e.,

$$x^k - a^k \equiv 0 \pmod{k^2}.$$

We have thus proved the case $b = 1$ of the theorem.

To prove the case $b = 2$, we build on what we have just proved. Thus, we consider:

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

Next, note the following relations which all follow from $x \equiv a \pmod{k}$ (as earlier, note that the last relation is trivially true):

$$\begin{aligned}
x^{k(k-1)} &\equiv a^{k(k-1)} \pmod{k},\\
x^{k(k-2)}a^k &\equiv a^{k(k-1)} \pmod{k},\\
x^{k(k-3)}a^{2k} &\equiv a^{k(k-1)} \pmod{k},\\
&\cdots\cdots\cdots\cdots\cdots\\
x^k a^{k(k-2)} &\equiv a^{k(k-1)} \pmod{k},\\
a^{k(k-1)} &\equiv a^{k(k-1)} \pmod{k}.
\end{aligned}$$

Therefore, by addition of the corresponding sides, we obtain, since $ka^{k(k-1)} \equiv 0 \pmod{k}$:

$$x^{k(k-1)} + x^{k(k-2)}a^k + x^{k(k-3)}a^{2k} + \cdots + a^{k(k-1)} \equiv 0 \pmod{k}.$$

That is, k divides $x^{k(k-1)} + x^{k(k-2)}a^k + x^{k(k-3)}a^{2k} + \cdots + a^{k(k-1)}$. Since k^2 also divides $x^k - a^k$, it follows that k^3 divides $x^{k^2} - a^{k^2}$, i.e.,

$$x^{k^2} - a^{k^2} \equiv 0 \pmod{k^3}.$$

We have thus proved the case $b = 2$ of the theorem.

The general case can now be proved inductively, using exactly the same line of reasoning. As each step is exactly of the same kind, we omit the details here.

SOHAM PURKAIT is currently a student in Class 10 of Sarada Vidyapith, West Bengal. He has a passion for problem solving in mathematics and physics. He also has a keen interest in Rubik's cube, coding, and sketching. He has qualified for Indian National Mathematical Olympiad (INMO) 2020. He secured a gold medal in the Kangaroo Mathematical Olympiad, and a silver medal in the Southeast Asian Mathematical Olympiad. He may be contacted at mathematicsandfun1729@gmail.com.