UCLA Math Circle

James Toche (and family)

9 August 2020
(Last revision: August 8, 2020)

Abstract

Notes on modular arithmetic from the UCLA Math Circle Intermediate-2 for Summer Session 2020, August 9nd.

Fermat's Little Theorem

Fermat's little theorem may be stated in two ways. The easiest to remember: For any prime number p,

$$a^p \equiv a \pmod{p}, \quad \forall a \in \mathbb{N}$$

Typically more useful is the equivalent statement:

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

Problem 1

Calculate $128^{129} \pmod{17}$

With a view to applying Fermat's little theorem, we seek to write 128^{129} in the form $\ldots^{17}$ or $\ldots^{16}$. To this end, consider $16 \times 8 = 128$ and $17 \times 7 = 119$.

$$\begin{aligned} 128^{129} &= 128^{16\times 8+1} \\ &= 128 \cdot (128^8)^{16} \\ &\equiv 128 \\ &\equiv 17 \times 7 + 9 \pmod{17} \\ &\equiv 9 \pmod{17} \end{aligned}$$

Problem 2

Calculate the remainder of $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ divided by 7. Consider each power separately:

$$
\begin{aligned}
2^{20} &= (2^3)^6 \cdot 2^2 \equiv 4 \pmod 7 \\
3^{30} &= (3^5)^6 \equiv 1 \pmod 7 \\
4^{40} &= 2^{80} = (2^{13})^6 \cdot 2^2 \equiv 4 \pmod 7 \\
5^{50} &= (5^8)^6 5^2 \equiv 25 \pmod 7 \equiv 7 \cdot 3 + 4 \pmod 7 \equiv 4 \pmod 7 \\
6^{60} &= (6^{10})^6 \equiv 1 \pmod 7
\end{aligned}
$$

Add up:

$$
\begin{aligned}
2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} &\equiv 4 + 1 + 4 + 4 + 1 \pmod 7 \\
&\equiv 2 \cdot 7 \pmod 7 \\
&\equiv 0 \pmod 7
\end{aligned}
$$

Problem 3

Let the sequence a_n be defined by $a_n = 4^{a_{n-1}}$ and $a_0 = 1$. Show by induction that $a_n \equiv 4 \pmod 7$, for all $n \in \mathbb{N}$ and $n \geq 1$.

Suppose the following holds for some fixed $n \in \mathbb{N}$.

$$P(n): \qquad a_n \equiv 4 \pmod 7$$

Base Case:

$$\begin{aligned} P(1): \qquad a_1 &= 4^{a_0} \\ &= 4^1 \\ &\equiv 4 \pmod 7 \end{aligned}$$

Induction Step:

Show that the left-hand side of $P(n+1)$ is congruent to 4 modulo 7.

$$P(n+1): \qquad a_{n+1} \equiv 4 \pmod 7$$

A very natural way to start is to use the property that a_n is congruent to 4 modulo 7, which may be written as $a_n = 7k + 4$ for some $k \in \mathbb{N}$. Unfortunately, that does not lead directly to a proof:

$$\texttt{lhs} = a_{n+1} = 4^{a_n} = 4^{7k+4} = (4^k)^7 \cdot 2^6 \cdot 2^2 \equiv 4^k \cdot 4 \pmod 7$$

and there is no obvious way to deal with the 4^k term.

The above steps suggest that if a_n were written as a multiple of 6 instead of 7, the 4^k term would be made to vanish. So this is what we seek. The result below delivers.

$$4^a \equiv 4 \pmod 6, \quad \forall a \in \mathbb{N}$$

implies that $4^{a_n} \equiv 4 \pmod 6$. This congruence may be used as follows:

$$\begin{aligned} \texttt{lhs} = a_{n+1} = 4^{a_n} = 4^{6k+4} &= (4^k)^6 \cdot 4^4 \\ &\equiv 4^4 \pmod 7 \\ &\equiv 4 \pmod 7 \\ &= \texttt{rhs} \qquad \square \end{aligned}$$

The difficult step in the above demonstration was to see that $4^a \equiv 4 \pmod 6$ for all $a \in \mathbb{N}$. This too can be shown by induction. The base case ($a = 1$) is obvious. The induction step goes:

$$\begin{aligned} 4^{a+1} &= 4 \cdot 4^a \\ &\equiv 4 \cdot 4 \pmod 6 \\ &\equiv 16 - 2 \cdot 6 \\ &\equiv 4 \pmod 6 \qquad \square \end{aligned}$$

Problem 4

Find all integers such that $x^{86} \equiv 6 \pmod{29}$.

Since 29 is prime, we can apply Fermat's little theorem to reduce the exponent on x. Using $28 \times 3 = 84$ yields

$$\begin{aligned} x^{86} &= (x^3)^{28} \cdot x^2 \\ &\equiv x^2 \pmod{29} \end{aligned}$$

We now write 6 as a square modulo 29 (by adding 29 to 6 repeatedly until we get a perfect square).

$$\begin{aligned} 6 &\equiv 6 + 2 \times 29 \pmod{29} \\ &\equiv 64 \pmod{29} \\ &\equiv 8^2 \pmod{29} \end{aligned}$$

Putting it together yields the equation:

$$x^2 \equiv 8^2 \pmod{29}$$

with solutions:

$$\begin{cases} x \equiv 8 \pmod{29} \\ x \equiv -8 \pmod{29} \equiv 21 \pmod{29} \end{cases}$$

Thus the equation has two integer solutions modulo 29: 8 and 21.

Problem 5

Show by induction that $x^p \equiv x \pmod{p}$, for all $x \in \mathbb{N}$, where p is any prime number. Hint: Use $(x+1)^p \equiv x^p = 1 \pmod{p}$ in the inductive step.

Recall that for any a, b, the binomial expansion formula is:

$$(a+b)^n = a^n + na^{n-1}b + \ldots + \binom{n}{k}a^{n-k}b^k + \ldots + nab^{n-1} + b^n$$

where the binomial coefficient is:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Let p denote any prime number. Suppose the following holds for some fixed $n \in \mathbb{N}$.

$$P(n): \qquad n^p \equiv n \pmod{p}$$

Base Case:

$$P(1): \qquad 1^p \equiv 1 \pmod{p}$$

Induction Step:

$$P(n+1): \qquad (n+1)^p \equiv (n+1) \pmod{p}$$

Show that the left-hand side of $P(n+1)$ is congruent to the right-hand side:

$$\begin{aligned}
\texttt{lhs} = (n+1)^p &= n^p + p\, n^{p-1} + \ldots + \binom{p}{k}n^{p-k} + \ldots + p + 1 \\
&= n^p + p \underbrace{\left(n^{p-2} + \ldots + p^{-1}\frac{p!}{k!(p-k)!} + \ldots + 1\right)}_{\in\mathbb{N}} + 1 \\
&\equiv n^p + 1 \pmod{p} \\
&\equiv n + 1 \pmod{p} \\
&= \texttt{rhs} \qquad \square
\end{aligned}$$

In the above we used the well-known result that

$$n^k \equiv n \pmod{k} \quad \forall n, k \in \mathbb{N}^2$$