Fermat's Little Theorem

P. Reany

July 6, 2023

Statement of Fermat's Little Theorem:

Let x be a positive integer and let p be a prime. Then

$$x^p \equiv x \pmod{p}\,, \tag{1}$$

or, alternatively,

$$x^{p-1} \equiv 1 \pmod{p}\,. \tag{2}$$

We choose a proof by induction. For the base case, we obviously need to deal with $x = 1$:

$$1^p \equiv 1 \pmod{p}\,, \tag{3}$$

which is true.

Next, we choose some arbitrary positive integer k and make the induction hypothesis (assumption) that

$$k^p \equiv k \pmod{p}\,, \tag{4}$$

and then show that

$$(k+1)^p \equiv k+1 \pmod{p}\,. \tag{5}$$

Okay, we use the binomial theorem to expand the LHS side of this last equation, to get

$$k^p + \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \cdots + 1\,. \tag{6}$$

Note that in each term except in the first and last, there is a coefficient with a factor of p in it. Therefore, when we reduce this expression modulo p, we have that

$$k^p + 1 \pmod{p}\,. \tag{7}$$

However, from (4) we know that $k^p \equiv k \pmod{p}$. Therefore,

$$(k+1)^p \equiv k^p + 1 \equiv k+1 \pmod{p}\,, \tag{8}$$

which is what we needed to show.