Choose an arbitrary prime number p and any integer z ; then *Fermat's Little Theorem* says

$$z^p \equiv z \ \mathbf{mod}\ p\ , \quad \text{and if } p \text{ does not divide } z \text{ then } z^{p-1} \equiv 1 \ \mathbf{mod}\ p\ .$$

This is Theorem 5 on p. 145 of the text, which proves the theorem on p. 149 ex. 14 - 17 by first proving *Wilson's Theorem* : $(p-1)! \equiv p-1 \ \mathbf{mod}\ p$. What follows are two more direct proofs of Fermat's Little Theorem. The first was recommended by Prof. Ken Ribet.

First, recall the *Binomial Theorem* : $(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} \cdot x^k \cdot y^{p-k}$ in which the combinatorial coefficient $\binom{p}{k} = p\cdot(p-1)\cdot(p-2)\cdot(\ldots)\cdot(p-k+2)\cdot(p-k+1)/k!$, and observe that $\binom{p}{k} \equiv 0 \ \mathbf{mod}\ p$ for $0 < k < p$. Consequently $(x + y)^p \equiv (x^p + y^p) \ \mathbf{mod}\ p$ for all integers x and y . We shall use this congruence to prove Fermat's Little Theorem by *Mathematical Induction* :

Evidently the assertion " $z^p \equiv z \ \mathbf{mod}\ p$ " is true when $z = 0$ and when $z = \pm 1$. If the assertion were ever false the smallest integer $Z > 1$ for which it was false would have to exist though the assertion is true for $0 \le z < Z$. But then we could set $x := Z-1 < Z$ and $y := 1 < Z$, whence $x^p \equiv x \ \mathbf{mod}\ p$ and $y^p \equiv y \ \mathbf{mod}\ p$, and then find $Z^p = (x + y)^p \equiv (x^p + y^p) \equiv (x + y) \equiv Z \ \mathbf{mod}\ p$; this would prove the assertion true for $z = Z$ too contradicting the characterization of Z as the smallest integer for which the assertion was false. Therefore the assertion can never be false for any positive integer z ; and the identity $z^p = (-1)^p\cdot(-z)^p$ propagates the assertion to negative integers, confirming the theorem's first congruence. When z is not a multiple of prime p an integer $z^{-1} \ \mathbf{mod}\ p$ exists; multiplying the theorem's first congruence by that inverse yields the second. End of first proof.

Second proof: Suppose $0 < k < p$ and consider the multiples $\{k, 2k, 3k, \ldots, (p-1)k\}$; evidently no two of these can be congruent $\mathbf{mod}\ p$ nor can any be congruent to $0 \ \mathbf{mod}\ p$. Therefore these multiples must be congruent $\mathbf{mod}\ p$ to $\{1, 2, 3, \ldots, p-1\}$ in some order. The product of all these congruences implies $k^{p-1}\cdot(p-1)! \equiv (p-1)! \ \mathbf{mod}\ p$, and since the prime p does not divide $(p-1)!$ we can find its integer inverse $\mathbf{mod}\ p$ and multiply by it to conclude that $k^{p-1} \equiv 1 \ \mathbf{mod}\ p$, which confirms the theorem's second congruence for all $z \equiv k \ \mathbf{mod}\ p$. Multiply by z to confirm the first congruence, which holds also when $z \equiv 0 \ \mathbf{mod}\ p$. End of second proof.

Fermat's Little Theorem is most often applied in the $z^{p-1} \equiv 1 \ \mathbf{mod}\ p$ form. For example, if the congruence " $z^{n-1} \equiv 1 \ \mathbf{mod}\ n$ " is dissatisfied when tested for some z and n , then n is certainly not a prime even if its factors are unknown. Unfortunately the converse is untrue; that congruence can be satisfied by some z but not others when n is what is called a "pseudoprime". Worse, infinitely many *Carmichael Numbers* n satisfy that congruence for all integers z for which $\mathrm{GCD}(z, n) = 1$ though these non-primes n are very rare. Still, as tests for non-primes go, this test is relatively cheap because modular exponentiation is so fast; *cf.* text p. 163 ex. 14.

Fermat's Little Theorem justifies posting two integers n and e on your web site by which you can be sent an enciphered message that nobody else who intercepts it can read. The sender first encodes his message into an integer $M < n$, then encrypts it into $C := M^e \ \mathbf{mod}\ n$ and sends you C . You decrypt $M = C^d \ \mathbf{mod}\ n$ by using your secret key $d := e^{-1} \ \mathbf{mod}\ (p-1)\cdot(q-1)$ where p and q are the two secret huge prime factors of $n := p\cdot q$, and you have chosen e to satisfy $\mathrm{GCD}(e, (p-1)\cdot(q-1)) = 1$. Why does this work? Unless $p|M$ or $q|M$, in which case extra argument is needed, $M^{p-1} \equiv 1 \ \mathbf{mod}\ p$ and $M^{q-1} \equiv 1 \ \mathbf{mod}\ q$. Then, since $d\cdot e = 1 + k\cdot(p-1)\cdot(q-1)$ for some integer k , $C^d = M^{de} = M^{1+k(p-1)(q-1)} \equiv M \ \mathbf{mod}\ p$ and $\mathbf{mod}\ q$. Therefore $C^d \equiv M \ \mathbf{mod}\ pq$. *Cf.* text p. 147.

This document was created with FrameMaker 4.0.4