Fermat's Little Theorem From the Multinomial Theorem

Thomas J. Osler (osler@rowan.edu), Rowan University, Glassboro, NJ 08028

Fermat's Little Theorem [**1**] states that $n^{p-1} - 1$ is divisible by p whenever p is prime and n is an integer not divisible by p. This theorem is used in many of the simpler tests for primality. The so-called multinomial theorem (described in [**2**]) gives the expansion of a multinomial to an integer power $p > 0$,

$$(a_1 + a_2 + \cdots + a_n)^p = \sum_{k_1+k_2+\cdots+k_n=p} \binom{p}{k_1, k_2, \ldots, k_n} a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}. \tag{1}$$

Here the multinomial coefficient is calculated by

$$\binom{p}{k_1, k_2, \ldots, k_n} = \frac{p!}{k_1!\,k_2! \cdots k_n!}. \tag{2}$$

This is a generalization of the familiar binomial theorem to the case where the sum of n terms $(a_1 + a_2 + \cdots + a_n)$ is raised to the power p. In (1), the sum is taken over all nonnegative integers $k_1, k_2, \ldots, k_n$ such that $k_1 + k_2 + \cdots + k_n = p$.

In this capsule, we show that Fermat's Little Theorem can be derived easily from the multinomial theorem. The following steps provide the derivation.

1. All the multinomial coefficients (2) are positive integers. This is clear from the way in which they arise by repeated multiplication by $(a_1 + a_2 + \cdots + a_n)$ in (1).
2. There are n values of the multinomial coefficient that equal 1. These occur when all but one of the indices $k_r = 0$, so that the remaining index equals p. For example, $\binom{p}{0,\ldots,0,p,0,\ldots,0} = \frac{p!}{0!\cdots 0!\,p!\,0!\cdots 0!} = 1$.
3. With the exception of the n coefficients just listed above, all of the remaining coefficients are divisible by p if p is a prime number. This follows from the fact that (2) is an integer, so the denominator $k_1!\,k_2! \cdots k_n!$ divides the numerator $p!$. Since $k_r < p$ for $r = 1, 2, \ldots, n$, the factor p never occurs in the prime factorization of the denominator $k_1!\,k_2! \cdots k_n!$. Therefore, $k_1!\,k_2! \cdots k_n!$ must divide $(p-1)!$ and so p divides the multinomial coefficient.
4. Let each $a_r = 1$ for $r = 1, 2, \ldots, n$ in (1). Then from step 2 above,

$$(1 + 1 + \cdots + 1)^p = 1^p + 1^p + \cdots + 1^p + \sum \binom{p}{k_1, \cdots k_n}. \tag{3}$$

Note, from step 3, that all the multinomial coefficients in the sum are divisible by p. And since $1 + 1 + \cdots + 1 = n$ in (3), we get

$$n^p = n + \{\text{number divisible by } p\}.$$

It follows that $n^p - n = n(n^{p-1} - 1)$ is divisible by p. Finally, $n^{p-1} - 1$ is divisible by p if n is not divisible by p.

The author wishes to thank James Smoak for correspondence that motivated this capsule.

References

1. David M. Burton, *Elementary Theory of Numbers*, (4th ed.), McGraw-Hill, 1997, pp. 91–92.
2. R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, 1989, pp. 166–172.