78.1 A (Very) Short Proof of Fermat's Little Theorem
Author(s): Stephen P. Kennedy
Source: *The Mathematical Gazette*, Vol. 78, No. 481 (Mar., 1994), p. 48
Published by: The Mathematical Association
Stable URL: http://www.jstor.org/stable/3619430
Accessed: 24/03/2010 21:12

Notes

78.1 A (very) short proof of Fermat's little theorem

Fermat's little theorem states that if a and p are positive integers, p a prime which does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$. The standard textbook proofs rely on complicated divisibility results or ring theory. A little combinatorics makes the proof very simple, and emphasises the hypotheses. The key is the following lemma, whose straightforward proof is left to the reader.

Lemma. If w is a string of arbitrary symbols of length p, a prime, and w is not a single symbol repeated p times, then the cyclic permutations of p are distinct.

For example, if w is the string *abbab*, then w and its cyclic permutations *bbaba*, *babab*, *ababb*, and *babba* are distinct. On the other hand, the string abab and its cyclic permutations *baba*, *abab*, and *baba* are not distinct. All strings with non-distinct cyclic permutations are of this form – the concatenation of some number of copies of a shorter substring. Notice that the length of the repeated substring must then divide the length of the original string.

Theorem. If a and p are positive integers and p is prime, then p divides $a^p - a$.

Let $A = \{x_1, x_2, x_3, \ldots, x_a\}$ be a set of arbitrary symbols. Form all possible strings of length p of elements of A, with repetition allowed. There are a^p such strings. Some of them are special – the strings which consist of a single symbol repeated p times, e.g. $x_1 x_1 x_1 \ldots x_1$. There are a such trivial strings, and, hence, $a^p - a$ other strings. Each of these non-trivial strings has length p, a prime, and therefore has p distinct cyclic permutations. Partition the set of non-trivial strings into cyclic permutation classes. each class contains p elements, and each element is in a unique class. Therefore, p must divide $a^p - a$.

Fermat's little theorem follows by dividing both sides of the congruence $a^p \equiv a \pmod{p}$, by a. It is a pleasure to acknowledge helpful conversations with Matthew Stafford on this topic.

STEPHEN P. KENNEDY

Department of Mathematics, Saint Olaf College, Northfield, MN 55057 USA.