A proof of Fermat’s little theorem

Jayadev Misra

September 5, 2021

The following theorem, known as Fermat’s little theorem, is a fundamental result in number theory. The theorem has many applications. Pratt [3] uses the theorem to certify that a number is prime. It is used in cryptographic protocols, such as the Diffie-Hellman key exchange [1].

**Theorem 1** For any natural number \( n \) and prime number \( p \), \( n^p - n \) is a multiple of \( p \).

There are several ways to prove this theorem, e.g. using induction on \( n \). A proof using the pigeon-hole principle is as follows. For positive integers \( i \) and \( j \), and prime \( p \) it can be shown that \( i \cdot n \equiv j \cdot n \pmod{p} \) if and only if \( i \equiv j \pmod{p} \). Then \( \{i \cdot n \pmod{p} | 1 < i < p\} = \{j | 1 < j < p\} \). The product of the elements of the sets in this equation are identical, so, \( \Pi(\{i \cdot n | 1 < i < p\}) \equiv \Pi(\{j | 1 < j < p\}) \pmod{p} \), or \( n^p - 1 \equiv (p-1)! \pmod{p} \). Since prime \( p \) does not divide \( (p-1)! \), cancel \( (p-1)! \) from both sides to get \( n^p \equiv 1 \pmod{p} \). This is equivalent to \( n^p - n \) is a multiple of \( p \).

Dijkstra[2] gives a beautiful proof using elementary graph theory. The proof given here is based on Dijkstra’s constructions though it does not use graph theory.

**Proof of the theorem:** Consider the set of words of length \( p \) over an alphabet of size \( n \). Define an equivalence relation over the words, \( x \) and \( y \) are equivalent if and only if \( x \) is a rotation of \( y \). We count the number and size of the equivalence classes.

Define \( q \) to be a period for \( x \) if \( q \) rotations of \( x \), leftward for positive \( q \) and rightward for negative \( q \), yields \( x \). Clearly, 0 is a period for all \( x \), 1 is a period for \( x \) if and only if all symbols in \( x \) are identical, and given periods \( q \) and \( q' \) for \( x \), \( a \times q + b 	imes q' \), for arbitrary integers \( a \) and \( b \), are also periods for \( x \). In particular, a multiple of a period is a period. A simple period is not a multiple of another period. For simple period \( q \) for \( x \), all \( q \) rotations of \( x \) yield distinct words.

Let \( q \) be a simple period for a given \( x \). We use Bézout’s identity: for integers \( m \) and \( n \), there exist integers \( a \) and \( b \) such that \( a \times m + b \times n = \gcd(m, n) \), where \( \gcd \) is the greatest common divisor. Setting \( m, n = p, q \) in Bézout’s identity, \( \gcd(p, q) \) is a period. Since \( p \) is prime, \( \gcd(p, q) \) is either 1 or \( p \), and since \( q \) is a
simple period, \( q = 1 \) or \( q = p \). If \( q = 1 \), \( x \) consists of identical symbols. There are \( n \) such words so, \( q = p \) for the remaining \( n^p - n \) words. Therefore, each of these words belongs to an equivalence class of size \( p \); so, \( n^p - n \) is a multiple of \( p \).

**Dijkstra’s proof**  The following proof is a rewriting of the proof of Dijkstra [2]. For \( n = 0 \), \( n^p - n \) is 0, hence a multiple of \( p \). For positive integer \( n \), take an alphabet of \( n \) symbols and construct a graph as follows: (1) each node of the graph is identified with a word of \( p \) symbols, and (2) there is an edge from \( x \) to \( y \) if rotating word \( x \) by one place to the left yields \( y \). Observe:

1. No node is on two simple cycles because every node has a single successor and a single predecessor (which could be itself).
2. Each node is on a cycle of length \( p \) because successive \( p \) rotations of a word transforms it to itself.
3. Every simple cycle’s length is a divisor of \( p \), from (2). Since \( p \) is prime, the simple cycles are of length 1 or \( p \).
4. A cycle of length 1 corresponds to a word of identical symbols. So, exactly \( n \) distinct nodes occur in cycles of length 1. The remaining \( n^p - n \) nodes occur in simple cycles of length \( p \).
5. A simple cycle of length \( p \), from the definition of a simple cycle, has \( p \) distinct nodes. From (4), \( n^p - n \) is a multiple of \( p \).

**References**

