82.6 A Generalisation of Euler's Theorem
Author(s): Thomas Koshy
Published by: The Mathematical Association
Stable URL: http://www.jstor.org/stable/3620158
Accessed: 24/03/2010 21:12

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at http://www.jstor.org/page/info/about/policies/terms.jsp. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at http://www.jstor.org/action/showPublisher?publisherCode=mathas.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

The Mathematical Association is collaborating with JSTOR to digitize, preserve and extend access to The Mathematical Gazette.
A generalisation of Euler's theorem

One of the celebrated results in number theory is Euler's theorem:

If \( m \) is a positive integer and \( a \) any integer with \( (a, m) = 1 \), then \( a^{\phi(m)} \equiv 1 \pmod{m} \), where \( (a, m) \) denotes the gcd of \( a \) and \( m \). This result can be generalised to a finite number of positive integers \( m_i \), as the next theorem shows, where \( [a, b] \) denotes the lcm of the positive integers \( a \) and \( b \).

Its proof employs the fact that if \( a \equiv b \pmod{m_i} \), where \( 1 < i < k \), then \( a \equiv b \pmod{[m_1, m_2, \ldots, m_k]} \). For example, \( 293 \equiv 113 \pmod{6} \) and \( 293 \equiv 113 \pmod{9} \), so \( 293 \equiv 113 \pmod{[6, 9]} \), that is, \( 293 \equiv 113 \pmod{18} \).

**Theorem** Let \( m_1, m_2, \ldots, m_k \) be any positive integers and \( a \) any integer such that \( (a, m_i) = 1 \) for \( 1 \leq i \leq k \). Then

\[
a^{[\Phi(m_1), \Phi(m_2), \ldots, \Phi(m_k)]} \equiv 1 \pmod{[m_1, m_2, \ldots, m_k]}
\]

**Proof:** Let \( M_k = [\Phi(m_1), \Phi(m_2), \ldots, \Phi(m_k)] \). By Euler's theorem, \( a^{\Phi(m_i)} \equiv 1 \pmod{m_i} \) for every integer \( i \), where \( 1 \leq i \leq k \). Since \( \Phi(m_i) \mid M_k \), it follows that \( M_k \mid \Phi(m_i) \) is a positive integer, and

\[
a^{M_k} = \left[a^{\Phi(m_i)}\right]^{M_k/\Phi(m_i)} \equiv 1 \pmod{[m_1, m_2, \ldots, m_k]}
\]

By the above result, this yields the desired conclusion, \( a^{M_k} \equiv 1 \pmod{[m_1, m_2, \ldots, m_k]} \).

It is worth noting that Phythian's extension [1] of Fermat's Little Theorem follows from the above theorem when each \( m_i \) is a distinct prime.

**Reference**


THOMAS KOSHY

*Framingham State College, Framingham, MA 01701-9101, USA*

**82.7 Equal sums of squares**

**Two squares**

If you want to find all integer solutions of the equation \( 6p + 15q = 0 \), you first divide by 3 to get \( 2p + 5q = 0 \) and then, since 2 and 5 are coprime, you can argue that \( p \) is an integer multiple of 5 and \( q \) the same multiple of 2 but of opposite sign. The result is \( p = 5n \) and \( q = -2n \). The argument fails unless you first remove the highest common factor of 6 and 15.

This leads naturally to the following procedure. To find all solutions in integers of the equation

\[
ap + bq = 0
\]

you work out \( m = (a, b) \), set \( a = mf, b = mg \) so that (1) becomes

\[
fp + gq = 0.
\]