The Extended Euclidean Algorithm

**Theorem 3:**

a) The Euclidean algorithm computes 
\[ g := \text{gcd}(m, n). \]

b) If \( d \) is a common divisor of \( m \) and \( n \), then \( d | g \).

c) The method of back-substitution yields integers \( x, y \in \mathbb{Z} \) such that 
\[ mx + ny = g. \]

**Historical Remark:**
The extended Euclidean algorithm was called the method of the pulverizer (kut-taka) by the Hindus, particularly by Aryabhata (ca. 500 A.D.) and Brahmagupta (ca. 630 A.D.).

The idea behind the name is the following: by using the right substitution (as prescribed by the Euclidean algorithm), the coefficients of equation (1) are made successively smaller and smaller until they are “pulverized”.

More precisely: if \( m = qn + r \), then the substitution \( x = y', y = x' - q \cdot y' \) in (1) leads to the equation  
\[ nx' + ry' = g. \]