

211

NÚMEROS DE CARMICHAEL DE ORDEM M. *Leandro Steimez, Vilmar Trevisan (orient.)*
(UFRGS).

O Pequeno Teorema de Fermat garante que quando fixado um primo p , $a^p \equiv a \pmod{p}$ para todo a inteiro. É natural se perguntar se o resultado acima é válido quando p não é primo, isto é, quando p é composto. O primeiro a caracterizar restritivamente o caso em que p é composto foi Korselt, mas não mostrou nenhum exemplo desse tipo de números. O primeiro a encontrar exemplos desse tipo de números foi Carmichael deixando seu nome nos compostos n que satisfazem $a^n \equiv a \pmod{n}$ para todo inteiro a . Há muitas formas de generalizar a noção de números de Carmichael e o objetivo desse trabalho é estudar a generalização recentemente sugerida por Howe em 2005. Um número de Carmichael de ordem m é um composto n livre de quadrados, tal que para todo p primo que divide n , e para todo r com $1 \leq r \leq m$ existe um $i \geq 0$ tal que $n \equiv p^i \pmod{p^r - 1}$. Observa-se que os números de Carmichael surgem no caso particular em que m é igual a 1. Nosso objetivo principal é apresentar um estudo sobre os números de Carmichael de ordem 2, desenvolvendo algoritmos para encontrá-los e compreender a heurística apresentada por Howe que sugere a existência de uma infinidade desses números.