Evento	Salão UFRGS 2014: SIC - XXVI SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2014
Local	Porto Alegre
Título	Calculando o Inverso Módulo m
Autor	PAOLA ROSSATO BERNARDO
Orientador	VILMAR TREVISAN

Um Domínio Integral K é um anel comutativo com unidade no qual não há divisores de zero. Um Domínio Euclidiano D é um Domínio Integral no qual se pode definir uma função $G: D\backslash\{0\} \rightarrow \mathbb{N}$ tal quer para quaisquer $c, d \in D$, com $b \neq 0$, existem $q, r \in D$, "quociente" e "resto" respectivamente, tais que $c = qd + r$, no qual $r = 0$ ou o grau de r é menor que o grau de d. O principal objetivo desta apresentação é mostrar o cálculo do inverso de a módulo m, no qual m é um Ideal e a um elemento do Domínio Euclidiano. Este é um problema que tem importância prática em muitas aplicações relevantes na aritmética de números inteiros e anéis de polinômios.

A principal ferramenta para a implementação deste método é uma generalização do algoritmo de Euclides, que é considerado o algoritmo mais antigo da ciência moderna. Mostraremos que o cálculo do máximo divisor comum de dois números inteiros, conhecido desde o ensino básico, pode ser generalizado para qualquer Domínio Euclidiano. Além disso, o algoritmo de Euclides estendido é usado para resolver esse problema de maneira eficiente.