Bruno Rafael dos Santos

Formalização do Algoritmo Ressol em Coq

Brasil

15 de julho de 2024

Bruno Rafael dos Santos

Formalização do Algoritmo Ressol em Coq

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, como requisito parcial para a obtenção do grau de Bacharel em Ciência da Computação.

Universidade do Estado de Santa Catarina – UDESC

Bacharelado em Ciência da Computação

Orientador: Karina Girardi Roggia

Coorientador: Paulo Henrique Torrens

Brasil

15 de julho de 2024

Bruno Rafael dos Santos

Formalização do Algoritmo Ressol em Coq

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, como requisito parcial para a obtenção do grau de Bacharel em Ciência da Computação.

Trabalho aprovado. Brasil, 24 de novembro de 2012:

Karina Girardi Roggia
Orientadora (Doutora)

Cristiano Damiani Vasconcelos
Doutor

Rafael Castro Gonçalves
Mestre

Brasil
15 de julho de 2024

"Em cima desse rato
tinha uma pulga...
Será possível?
Uma pulga acordada,
em cima de um rato dormitando,
em cima de um gato ressonando,
em cima de um cachorro cochilando,
em cima de um menino sonhando,
em cima de uma avó roncando,
numa cama aconchegante,
numa casa sonolenta,
onde todos viviam dormindo."
(WOOD, 1999).

1 Introdução

Durante os cursos de Ciência da Computação, são vistas estruturas matemáticas muito diferentes daquelas as quais alunos de ensino médio estão habituados. No geral, grande parte destas estruturas são abstratas por não parecerem uma representação de um objeto real ou por, apesar de parecer, a razão de sua formulação não ser bem motivada de início. A exemplo de tais estruturas temos vetores, matrizes, filas e grafos, utilizados na modelagem de diversos problemas. Apesar destas ferramentas serem extremamente úteis, há um tipo de objeto matemático sempre presente na maioria dos problemas e que muitas vezes são considerados limitados e apenas objetos auxiliares demasiadamente utilizados: estes são os números inteiros. O conjunto dos números inteiros, apesar de ser formado por objetos (números) vistos como simples, possui diversas endorrelações que levam a muitas conclusões e invenções de grande importância, principalmente para o campo da criptografia. Dentre estas relações, duas delas são pilares fundamentais para tais conclusões e invenções mencionadas: a relação de divisibilidade e de congruência. A primeira é definida da seguinte forma (BROCHERO MARTINEZ CARLOS GUSTAVO T. DE A. MOREIRA, 2013):

Referências

BROCHERO MARTINEZ CARLOS GUSTAVO T. DE A. MOREIRA, N. C. S. E. T. F. E. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. 3. ed. Rio de Janeiro : IMPA: IMPA, 2013. (Projeto Euclides). ISBN 978-85-2444-0312-5. Citado na página 5.

WOOD, A. *A Casa Sonolenta*. Original. Estados Unidos América: Editora Ática, 1999. (Abracadabra). ISBN 9788508032761. Citado na página 3.