Formalização do Algoritmo RESSOL utilizando Coq

Bruno Rafael dos Santos
Universidade do Estado de Santa Catarina
`bruniculos2014@gmail.com`

Orientadora: Dra Karina Girardi Roggia
Coorientador: Me Paulo Henrique Torrens

29/11/2024

Sumário

Sumário

- A Teoria dos Números é um ramo da matemática que lida, em sua maior parte, com propriedades de números inteiros;
- É muito presente em temas relacionados a criptografia;
- Envolve definições de diversas relações em $\mathbb{Z}$, sendo duas dessas as relações de divisibilidade e congruência;
- Neste contexto que se apresenta o *símbolo de Legendre*, o qual possui relação com o algoritmo *RESSOL* e está presente na *Lei de Reciprocidade Quadrática*.
- A seguir se apresentam as definições de divisibilidade e congruência.

Definição 1 (*Divisibilidade*)

$\forall d, a \in \mathbb{Z}$, d ***divide*** *a (ou em outras palavras: a é um múltiplo de d) se e somente se a seguinte proposição é verdadeira:*

$$\exists q \in \mathbb{Z}, a = d \cdot q$$

assim, se tal proposição é verdadeira e portanto d divide a, tem-se a seguinte notação que representa tal afirmação:

$$d \mid a$$

caso contrário, a negação de tal afirmação (d não divide a) é representada por:

$$d \nmid a$$

Definição 2 (*Congruência*)

Para todo $a, b, n \in \mathbb{Z}$, *a é congruente a b módulo n se e somente se, pela divisão euclidiana* $\frac{a}{n}$ *e* $\frac{b}{n}$ *(onde* $0 \leq r_a < |n|$ *e* $0 \leq r_b < |n|$*) tem-se*

$$a = n \cdot q_a + r_a$$

e

$$b = n \cdot q_b + r_b$$

com $r_a = r_b$, *o que também equivale a dizer que:*

$$n \mid a - b$$

tal relação entre os inteiros a, b e n é representada por:

$$a \equiv b \pmod{n}$$

Objetivo Geral

Implementar o *símbolo de Legendre* e realizar a formalização de suas propriedades (apresentadas em (BROCHERO et al., 2013)) e da corretude (da função que o implementa).

1. Obter conhecimentos avançados sobre o assistente de provas *Coq*.
2. Realizar o estudo sobre as principais documentações da biblioteca Mathematical Components.
3. Desenvolver a capacidade de realizar provas em *Coq* utilizando as táticas da linguagem de provas *SSReflect*.
4. Estudar conteúdos de Teoria dos Números relacionados ao símbolo de Legendre.
5. Implementar uma função que compute o valor do *símbolo de Legendre* e provar a corretude da mesma se utilizando da biblioteca Mathematical Components.
6. Provar teoremas úteis para manipulação de expressões envolvendo o símbolo de Legendre utilizando-se da biblioteca Mathematical Components.

A seguir serão apresentados os principais teoremas, lemas e definições considerados úteis para a realização do objetivo estabelecido. Esse conteúdo se baseia no livro (BROCHERO et al., 2013) que foi amplamente estudado para realização deste trabalho.

1. (*Reflexividade*) $a \equiv a \pmod{n}$
2. (*Simetria*) $a \equiv b \pmod{n} \Longrightarrow b \equiv a \pmod{n}$
3. (*Transitividade*)

$$a \equiv b \pmod{n} \ \wedge \ b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$$

4. (*Compatibilidade com a soma*)

$$a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a+c \equiv b+d \pmod{n}$$

5. (*Compatibilidade com a diferença*)

$$a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a-c \equiv b-d \pmod{n}$$

6. (*Compatibilidade com o produto*)

$$a \equiv b \pmod{n} \land c \equiv d \pmod{n} \implies a \cdot c \equiv b \cdot d \pmod{n}$$

A partir dessa propriedade, note que, para todo $k \in \mathbb{N}$:

$$a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$$

7. (*Cancelamento*)

$$\mathrm{mdc}(c, n) = 1 \implies (a{\cdot}c \equiv b{\cdot}c \pmod{n} \iff a \equiv b \pmod{n})$$

Definição 3 (Função φ de Euler)

Para quaisquer n inteiro positivo, a função $\varphi(n)$ é definida como:

$$\varphi(n) = |(\mathbb{Z}/(n))^{\times}| \tag{1}$$

Algumas propriedades da função φ de Euler são:

1. $\varphi(1) = \varphi(2) = 1$
2. $\forall\, n, n > 2 \Rightarrow 1 < \varphi(n) < n$
3. $\forall\, p$, se p é primo então $\forall\, k \in \mathbb{N} - \{0\}, \varphi(p^k) = p^k - p^{k-1}$, portanto, $\varphi(p) = p - 1$

4. $\forall n, m \in \mathbb{N} - \{0\}, \text{mdc}(n, m) = 1 \Rightarrow \varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$
5. $\forall n \in \mathbb{N} - \{0\}$, se a fatoração de n em potências de primos distintos é dada por $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, então:

$$\begin{aligned} \varphi(n) &= \prod_{1 \le i \le k} \varphi(p_i^{\alpha_i}) \\ &= \prod_{1 \le i \le k} p_i^{\alpha_i} - p_i^{\alpha_i - 1} \\ &= n \cdot \prod_{1 \le i \le k} \left(1 - \frac{1}{p_i}\right) \end{aligned} \tag{2}$$

Teorema 1 (*Teorema de Euler-Fermat*)

Para todo $a, m \in \mathbb{Z}$, *se* $m > 0$ *e* $\text{mdc}(a, m) = 1$ *então:*

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Teorema 2 (*Pequeno Teorema de Fermat*)

Para todo $a \in \mathbb{N} - \{0\}$, *dado um número primo* p, *tem-se que:*

$$a^{p} \equiv a \pmod{p}$$

- Sendo p um número primo maior que 2 e $a, b, c \in \mathbb{Z}$ números não divisíveis por p, como motivação suponha que se deseje resolver a seguinte equação:

$$a \cdot x^2 + b \cdot x + c \equiv 0 \pmod{p} \tag{3}$$

Manipulando essa equação por meio das propriedades de congruência se obtém:

$$(2 \cdot a \cdot x + b)^2 \equiv b^2 - 4 \cdot a \cdot c \pmod{p} \tag{4}$$

- Realizando a substituição $X = 2 \cdot a \cdot x + b$ e $d = b^2 - 4 \cdot a \cdot c$ na Equação 4, tem-se:

$$X^2 \equiv d \pmod{p} \tag{5}$$

  Portanto, resolver a Equação 3 é equivalente a resolver a Equação 5;

- Sobre a Equação 5, se diz que d é um quadrado perfeito em $\mathbb{Z}/(p)$ e também que d é um *resíduo quadrático módulo p*.

Conforme (BROCHERO et al., 2013), existem $\frac{p+1}{2}$ resíduos quadráticos módulo p, que são:

$$0^2 \bmod p, 1^2 \bmod p, 2^2 \bmod p, \ldots, \left(\frac{p-1}{2}\right)^2 \bmod p \tag{6}$$

pois note que, para todo $x \in \mathbb{Z}$ existe algum $i \in [0, \frac{p-1}{2}]$ tal que $x \equiv i \pmod{p}$ ou $x \equiv -i \pmod{p}$, logo $x^2 \equiv i^2 \pmod{p}$ (usando a propriedade do Item 6) e i^2 está na Lista 6.

Além disso, todos os os valores na Lista 6 são distintos em módulo p, pois para todo $i, j \in \left[0, \frac{p-1}{2}\right]$:

$$
\begin{aligned}
i^2 \equiv j^2 \pmod{p} &\iff p \mid (i^2 - j^2) && (7)\\
&\iff p \mid (i-j)\cdot(i+j) && (8)\\
&\iff p \mid (i-j) \vee p \mid (i+j) && (9)
\end{aligned}
$$

Com isso, dado o intervalo de i e j, então $0 \leq i + j \leq p - 1$, assim existem as seguintes possibilidades:

1. $i = j = 0$ e portanto $i \equiv j \pmod{p}$;
2. $0 < i + j \leq p - 1$, portanto $p \nmid i + j$, e então pela disjunção em 9 resta que $p \mid (i - j)$, o que equivale a $i \equiv j \pmod{p}$, ou seja, i é igual j módulo p se e somente se seus quadrados também são.

Com essas conclusões (de que a Lista 6 contém todos os resíduos quadráticos módulo p e que todos os valores dela são distintos em módulo p) pode ser provado o seguinte lema:

Lema 1

Seja $p > 2$ um número primo, existem exatamente $\frac{p+1}{2}$ resíduos quadráticos módulo p e $\frac{p-1}{2}$ resíduos não quadráticos módulo p.

Definição 4 (Símbolo de Legendre)

Seja $p > 2$ um número primo e $a \in \mathbb{Z}$, se define o símbolo de Legendre por:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \textit{ se } p \nmid a \textit{ e } a \textit{ é um resíduo quadrático módulo } p \\ 0, \textit{ se } p \mid a \\ -1, \textit{ caso contrário (} a \textit{ não é um resíduo quadrático)} \end{cases}$$

Uma maneira de se computar o valor de um *símbolo de Legendre* é por meio do *Critério de Euler*, descrito a seguir:

Teorema 3 (*Critério de Euler*)

Para todo $a \in \mathbb{Z}$, seja $p > 2$ um número primo, então:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Para a se realizar a prova do *Critério de Euler* são necessários as definições, lemas e teoremas dados a seguir:

Definição 5 (*Inverso multiplicativo módulo n*)

Dados $a, m, n \in \mathbb{Z}$, *se* $a \cdot m \equiv 1 \pmod{n}$, *se diz que* m *é um inverso de* a *módulo* n, *e pode ser denotado por* a^{-1}.

Lema 2

Para todo $a, n \in \mathbb{Z}$, *se* $n > 0$, *então, existe* $b \in \mathbb{Z}$ *tal que* $a \cdot b \equiv 1 \pmod{n}$ *se, e somente se,* $\mathrm{mdc}(a, n) = 1$.

Lema 3 (*Unicidade de inverso multiplicativo módulo p*)

Dado um número primo p*, seja* $a \in [1, p-1]$*, existe* $k \in [1, p-1]$ *tal que* $a \cdot k \equiv 1 \pmod{p}$ *e* k *é portanto o único inverso multiplicativo de módulo* p *de* a *no intervalo* $[1, p-1]$*.*

Lema 4

Seja $a \in [1, p-1]$ *em que* p *é um número primo maior que 2, se* $x^2 \equiv a \pmod{p}$ *não tem solução, então para todo* $h \in [1, p-1]$ *existe* $k \in [1, p-1]$*, tal que:*

$$h \neq k \wedge h \cdot k \equiv a \pmod{p}$$

Lema 5

Seja $a, h, k, k^{'} \in [1, p-1]$, *se* $k \cdot h \equiv a \pmod{p}$ *e* $k^{'} \cdot h \equiv a \pmod{p}$ *então* $k = k^{'}$ *(*k *é único).*

Lema 6

Seja $p > 2$ *um número primo, para todo* $a \in \mathbb{Z}$, *se* $\mathrm{mdc}(a, p) = 1$ *e* $x^2 \equiv a \pmod{p}$ *não tem solução então:*

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Lema 7

Seja p um número primo, então para quaisquer soluções de $x^2 \equiv 1 \pmod{p}$ têm-se que $x \equiv 1 \pmod{p}$ ou $x \equiv -1 \pmod{p}$. Portanto para qualquer outro valor y que não é uma solução, $y \not\equiv y^{-1} \pmod{p}$.

Teorema 4 (*Teorema de Wilson*)

Seja número composto um número que pode ser escrito como a multiplicação de dois outros números menores então, dado $n > 1$:

$$(n-1)! \equiv \begin{cases} -1 \pmod{n} \text{ se } n \text{ é primo} \\ 0 \pmod{n} \text{ se } n \text{ é composto e } n \neq 4 \end{cases}$$

Com esses itens apresentados pode ser realizada a prova do *Critério de Euler*, qual é por sua vez o teorema mais importante para a formalização do algoritmo *RESSOL*.

Obs.: todos esses itens junto ao *Critério de Euler* não estão implementados na biblioteca Mathematical Components, portanto constituem uma etapa intermediária para que se alcance o objetivo deste trabalho.

- O símbolo foi implementado por meio da seguinte função:

```
Definition legendre_symb {p : int} (pL2 : (2 < p)%R)
    (pP : primez.primez p) (a : int) :=
        if (p %| a)%Z then 0%Z else if (resz_quad p a)
        then 1%Z else (-1)%Z.
```

onde `resz_quad`

Referências

BROCHERO, F. E. et al. *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.