

# Fatoração de um Número

Mário Leite

...

De acordo com as literaturas matemáticas “*Fatoração é um processo que consiste em representar um número ou uma expressão como um produto de fatores*”. Este processo é muito usado para simplificar um polinômio e compactar a expressão. De uma maneira menos formal, pode ser dito que a Fatoração de um número inteiro e positivo é o processo de encontrar números cujo produto reproduz esse número; e neste caso esses números são fatores primos. No ambiente escolar a Fatoração de um número  $N$  é feita fazendo divisões sucessivas de  $N$  por números primos e dos subsequentes quocientes a partir de 2. Deste modo, o produto de todos os divisores será igual a  $N$ , sendo esses divisores chamados de “fatores primos”. O esquema abaixo mostra um exemplo de fatoração do número 372.

$$\begin{array}{r|l} 372 & (2) \\ 186 & (2) \\ 93 & (3) \\ 31 & (31) \\ 1 & \end{array}$$

$$2 \cdot 2 \cdot 3 \cdot 31 = 372$$

Assim pode-se dizer que “*Fatoração é o processo de decompor um número inteiro e positivo em números primos que integram um produto*”. Assim, **2**, **3** e **31** são os números primos que compõem o produto que resulta em **372**, que pode ser escrito do seguinte modo:  **$2^2 \cdot 3 \cdot 31$** .

No método de Criptografia de chave assimétrica RSA, um dos integrantes da chave pública (**e,n**) o número **n** é o produto de dois números primos grandes **p** e **q** (ambos com pelo menos cem dígitos), onde **n** pode ser do conhecimento público, mas os fatores **p** e **q** devem ser preservados. Assim, uma mensagem criptografada (codificada) com este método só poderá ser decodificada se forem conhecidos os números **p** e **q**; e como **n** é o produto destes dois fatores então, teoricamente, bastaria fatorar **n** para obtê-los. O problema é que na fatoração aparecem vários números primos; e como descobrir, com certeza **p** e **q**?! O processo de fatoração de números de até, digamos, 10 dígitos é relativamente rápido; mas, para números muito grandes (acima de trinta dígitos) o tempo de processamento pode ser extremamente longo.

Teoricamente, é sempre possível fatorar um número inteiro e positivo  $N$  ( $N \geq 2$ ); entretanto, a execução de um programa implementado numa linguagem, por mais eficiente que seja, pode exigir um tempo de processamento extremamente grande; se for um número primo muito grande pode levar até milhares de anos, mesmo com um algoritmo bem rápido rodando numa linguagem também muito rápida. O programa “**FatoraNumero**” codificado em **Python** e em **C#** baseado no esquema apresentado no esquema de fatoração de **372** acima, pode ser uma solução bem simples de fatoração. E para testar este programa foram considerados quatro exemplos com dois números compostos e dois números primos, medindo o tempo de processamento para cada exemplo. Observe que os tempos de fatoração nas duas linguagens variam muito; em particular a fatoração do número 2305843009213693951, que é o nono número primo de Mersene. Primeiramente foi apresentado o código-fonte da linguagem e em seguida as saídas do programa naquela linguagem: primeiro em **Python** e depois em **C#**.

## Código do programa em Python

```
'''
Programa "FatoraNumero.py"
Faz a fatoração de um número e exibe seus fatores primos.
Em Python
Autor: Mário Leite & Clesio Matias
E-mail: marleite@gmail.com
-----
'''

#Inicio -----
print("")
import time
import math
from decimal import*
from datetime import datetime

endif = "endif"
endwhile = "endwhile"

#-----
#Função para verificar se o número lido é primo
def VerifPrimo(n):
    if ((n==2) or (n==3)):
        return True
    m = 2
    z = int(n / 2)
    if n > 2 and n % 2 != 0:
        while True:
            m += 1
            if n % m == 0:
                return False
            else:
                z = int(z / m)
                if z <= m:
                    return True
        return False
#-----

Inicio = time.time()
Num = int(input("Digite um número inteiro e positivo: "))
num = Num
Agora = datetime.now()
Agora = Agora.strftime("%d/%m/%y - %H:%M:%S")
print("")
print("Fatores primos de", Num)
if(VerifPrimo(Num)):
    print(Num)
else:
    Divi = 2
    while(Num > 1):
        R = (Num % Divi)
        if((R==0) and (VerifPrimo(Divi))):
            print(Divi)
            Num = int(Num / Divi)
        else:
            if(Num==Divi):
                break
            else:
                Divi = Divi + 1
```

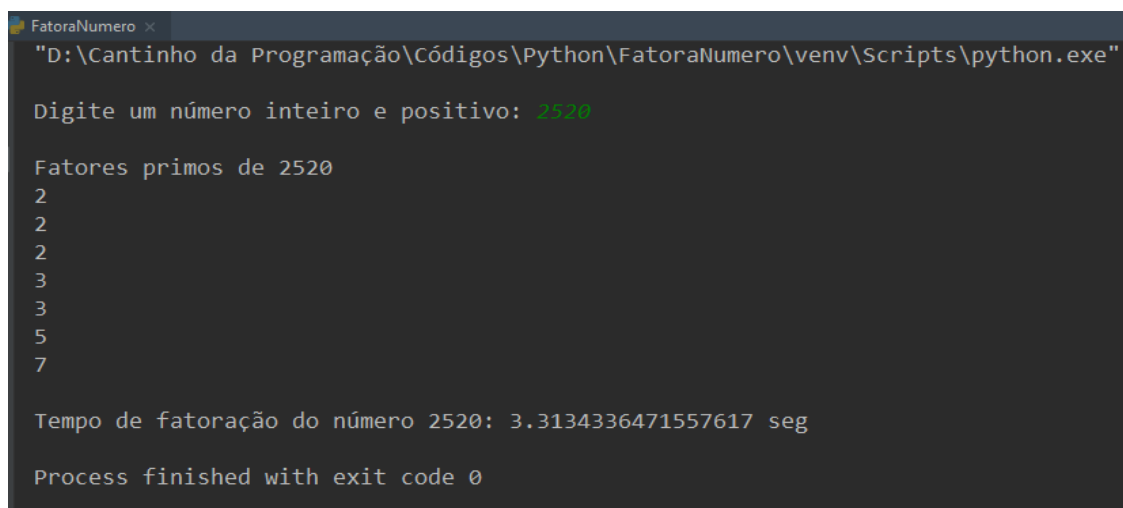
```

        endif
    endif
endwhile
endif

#Computa o tempo de processamento
print("")
Agora = datetime.now()
Agora = Agora.strftime("%d/%m/%y - %H:%M:%S")
Fim = time.time()
Tempo = Fim - Inicio
#Tempo = int(Tempo*100 + 0.50)/100
print(f'Tempo de fatoração do número {num}: {Tempo} seg')
#FimPrograma-----

```

## Saídas do programa em Python



```

FatoraNumero x
"D:\Cantinho da Programação\Códigos\Python\FatoraNumero\venv\Scripts\python.exe"

Digite um número inteiro e positivo: 2520

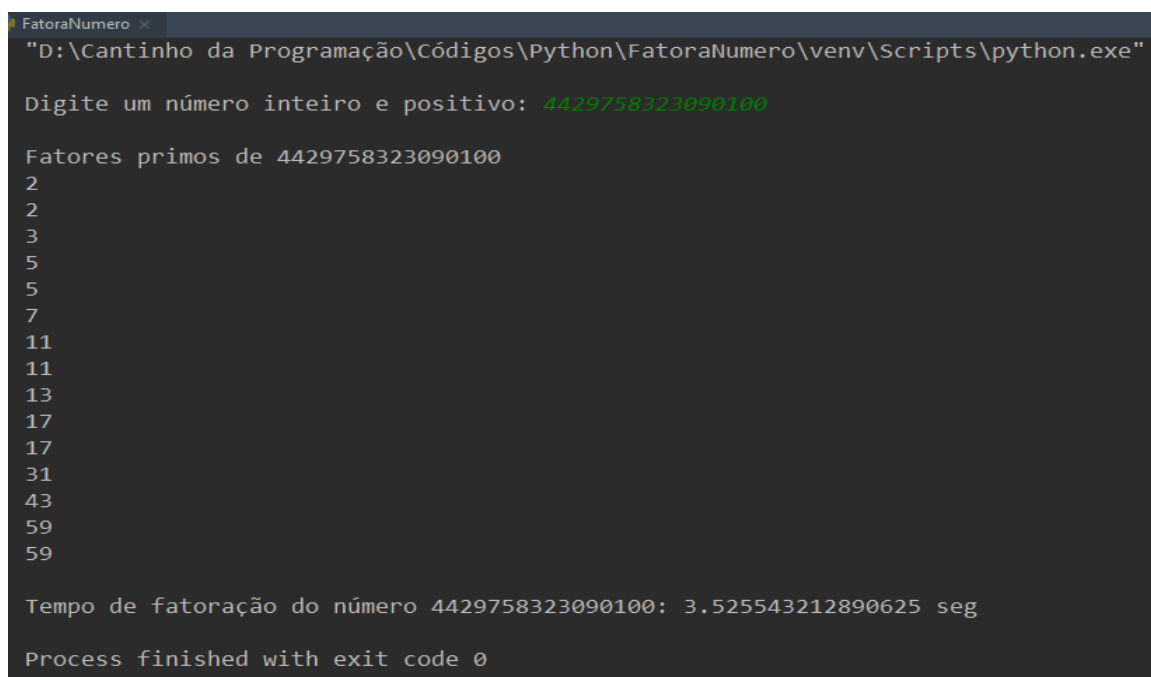
Fatores primos de 2520
2
2
2
3
3
5
7

Tempo de fatoração do número 2520: 3.3134336471557617 seg

Process finished with exit code 0

```

**Figura 1 - Fatoração de um número composto pequeno**



```

FatoraNumero x
"D:\Cantinho da Programação\Códigos\Python\FatoraNumero\venv\Scripts\python.exe"

Digite um número inteiro e positivo: 4429758323090100

Fatores primos de 4429758323090100
2
2
3
5
5
7
11
11
13
17
17
31
43
59
59

Tempo de fatoração do número 4429758323090100: 3.525543212890625 seg

Process finished with exit code 0

```

**Figura 2 - Fatoração de um número composto grande**

```
FatoraNumero x
"D:\Cantinho da Programação\Códigos\Python\FatoraNumero\venv\Scripts\python.exe"

Digite um número inteiro e positivo: 2147483647

Fatores primos de 2147483647
2147483647

Tempo de fatoração do número 2147483647: 1.8133130073547363 seg

Process finished with exit code 0
```

**Figura 3 - Fatoração de um número primo pequeno**

```
FatoraNumero x
"D:\Cantinho da Programação\Códigos\Python\FatoraNumero\venv\Scripts\python.exe"

Digite um número inteiro e positivo: 2305843009213693951

Fatores primos de 2305843009213693951
2305843009213693951

Tempo de fatoração do número 2305843009213693951: 6.292205095291138 seg

Process finished with exit code 0
```

**Figura 4 - Fatoração de um número primo grande**

## Código do programa em C#

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Diagnostics;

namespace FatoraNumero
{
    internal class Program
    {
        public const long MAXNUM = 9223372036854775807; //máximo inteiro longo
        static void Main(string[] args)
        {
            /* Tratamento de datas */
            int diaHoje = int.Parse(DateTime.Now.Day.ToString());
            int mesHoje = int.Parse(DateTime.Now.Month.ToString());
            int anoHoje = int.Parse(DateTime.Now.Year.ToString());
            string hora = DateTime.Now.ToString("hh:mm:ss tt");
            string dataHoje = diaHoje + "/" + mesHoje + "/" + anoHoje;
            DateTime objData = new DateTime(anoHoje, mesHoje, diaHoje);
            Stopwatch ObjSw = new Stopwatch(); //cria objeto de controle de tempo
            ObjSw.Start(); //liga o cronômetro
            long num, divi, resto;
            num = 1;
            while ((num < 2) || (num > MAXNUM))
            {
                Console.WriteLine(" Digite o número a ser fatorado [min 2 máx {0}]:", MAXNUM);
                num = long.Parse(Console.ReadLine());
            }
            Console.WriteLine("");
            Console.WriteLine(" Início do processamento: " + dataHoje + " - " + hora);

            Console.WriteLine();
            Console.WriteLine("");
            Console.WriteLine(" Fatores primos de {0}:", num);
            if (VerifPrimo(num))
            {
                Console.WriteLine(" " + num + " é primo");
            }
            else
            {
                divi = 2;
                /* Loop para fazer as divisões sucessivas */
                while (num > 1)
                {
                    resto = (long)(num % divi);
                    if (resto == 0)
                    {
                        Console.WriteLine(" " + divi);
                        num = (num / divi);
                    }
                    else
                    {
                        if (num == divi)
                        {
                            break; //abandona o loop: divisões terminaram
                        }
                        else
                        {
                            divi = divi + 1;
                            if (divi % 2 == 0)
                            {
                                divi++; //garante divisor impar
                            }
                        }
                    }
                }
            }
        }
    }
}
```

```

    }
    }
}

Console.WriteLine();

/* Calcula o tempo de processamento */
ObjSw.Stop(); //desliga o cronômetro
TimeSpan tempo = ObjSw.Elapsed;
Console.WriteLine("");
Console.WriteLine(" Tempo de fatora  o [hh:mm:ss:ms]:{0}{1}",tempo," segundos.");
Console.ReadLine();
} //fim do m  todo principal

//-----
public static bool VerifPrimo(long num)
{
    /* Verificar se o n  mero lido    primo */
    long m, z;
    if ((num == 2) || (num == 3))
    {
        return true;
    }
    m = 2;
    z = (int) (num / 2);
    if ((num > 2) && (num % 2 != 0))
    {
        while (true)
        {
            m += 1;
            if (num % m == 0)
                return false;
            else
            {
                z = (int) (z / m);
                if (z <= m)
                {
                    return true;
                }
            }
        }
    }
    return false;
}
}
}
}

```

```

D:\Livros\Livro10\Projetos\PrFatoracao\PrFatoracao\bin\Debug\PrFatoracao...
Digite o n  mero a ser fatorado [m  n 2 m  x 9223372036854775807]:2520
In  cio do processamento: 25/9/2022 - 02:46:12

Fatores primos de 2520:
2
2
2
3
3
5
7

Tempo de fatora  o [hh:mm:ss:ms]: 00:00:00.0513578 segundos.

```

Figura 5 - Fatora  o de um n  mero composto pequeno

```
D:\Livros\Livro10\Projetos\PrFatoracao\PrFatoracao\bin\Debug\PrFatoracao.exe
Digite o número a ser fatorado [min 2 máx 9223372036854775807]:4429758323090100
Início do processamento: 25/9/2022 - 02:48:33

Fatores primos de 4429758323090100:
2
2
3
5
5
7
11
11
13
17
17
31
43
59
59

Tempo de fatoração [hh:mm:ss.ms]: 00:00:00.0016475 segundos.
```

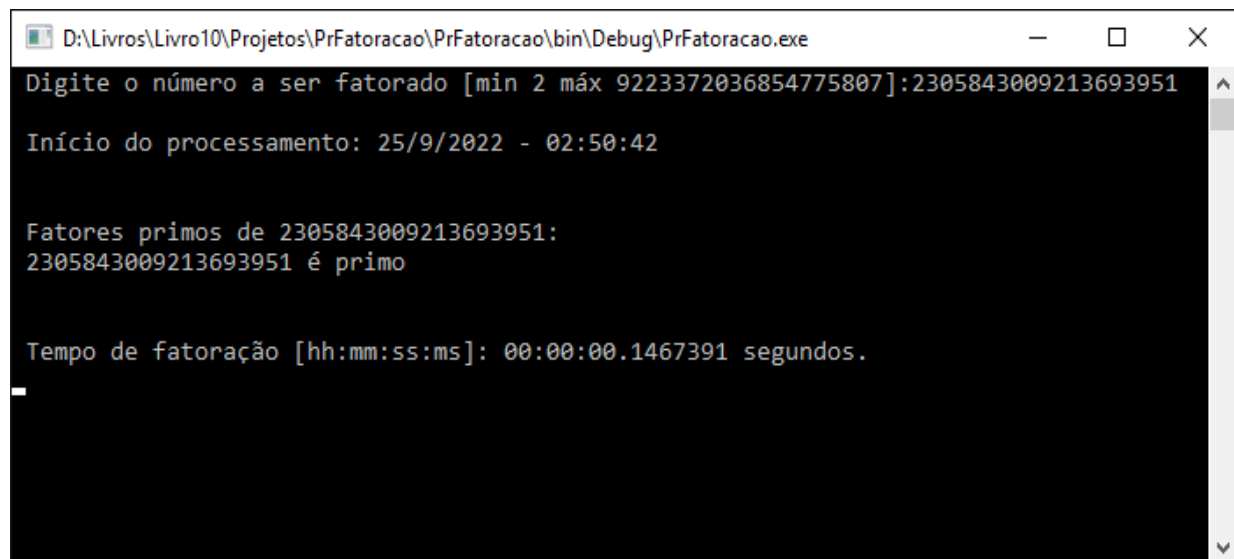
Figura 6 - Fatoração de um número composto grande

```
D:\Livros\Livro10\Projetos\PrFatoracao\PrFatoracao\bin\Debug\PrFatoracao.exe
Digite o número a ser fatorado [min 2 máx 9223372036854775807]:2147483647
Início do processamento: 25/9/2022 - 02:49:33

Fatores primos de 2147483647:
2147483647 é primo

Tempo de fatoração [hh:mm:ss.ms]: 00:00:00.0006668 segundos.
```

Figura 7 - Fatoração de um número primo pequeno



```
D:\Livros\Livro10\Projetos\PrFatoracao\PrFatoracao\bin\Debug\PrFatoracao.exe
Digite o número a ser fatorado [min 2 máx 9223372036854775807]:2305843009213693951
Início do processamento: 25/9/2022 - 02:50:42

Fatores primos de 2305843009213693951:
2305843009213693951 é primo

Tempo de fatoração [hh:mm:ss:ms]: 00:00:00.1467391 segundos.
```

Figura 8 - Fatoração de um número primo grande