



VIII

Encontro Cajazeirense de Matemática



Uma década da licenciatura em matemática no IFPB-CZ: tecendo histórias e interligando culturas!
20 a 22 de outubro de 2021

Artimética com o *Sagemath*

Vinicius Martins Teodosio Rocha
Larissa Soares de Sousa
Jose Jorge de Souza Silva

Instituto Federal da Paraíba - Campus Cajazeiras

O Sagemath

- <https://sagecell.sagemath.org/>
- Quase um Python com **muitas** ferramentas extras.
- Missão

Criar uma alternativa viável de código aberto para o Magma, Maple, Mathematica e Matlab

- Licença GPL (GNU General Public License): Livre!
- <https://doc.sagemath.org/html/en/developer/>
- E o que tanto ele faz?
 - ▶ doc.sagemath.org/html/pt/tutorial/
 - ▶ doc.sagemath.org/html/pt/a_tour_of_sage/
 - ▶ doc.sagemath.org/html/en/thematic_tutorials/ só em inglês :(

Gráficos

```
In [4]: 1 plot(sin(x), -pi, pi)
```

Out[4]:

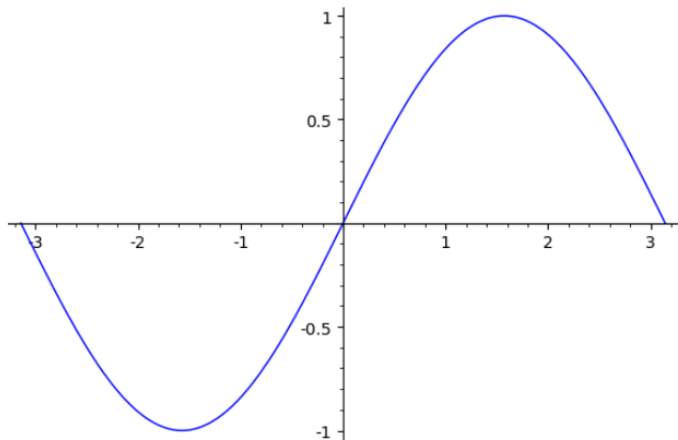


Figure: Gráfico de $\sin(x)$, $x \in [-\pi, \pi]$

Gráficos Interactivos

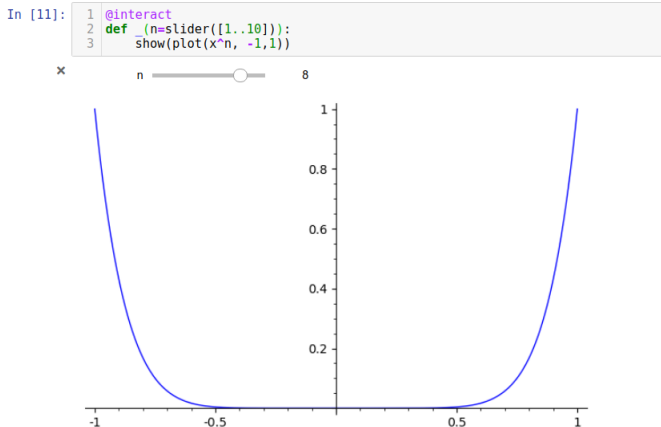
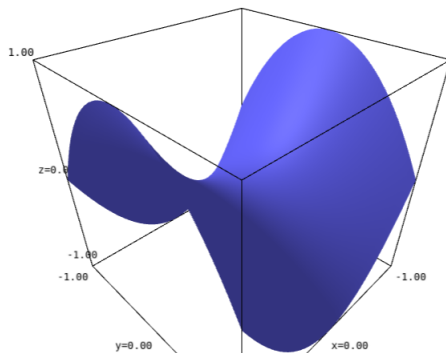


Figure: Gráfico de x^n , $x \in [-1, 1]$, $n = 1, 2, \dots$

Gráficos 3D

```
In [33]: 1 var('y')  
2 plot3d(x^2 - y^2, (x,-1,1),(y,-1,1))
```

Out[33]:

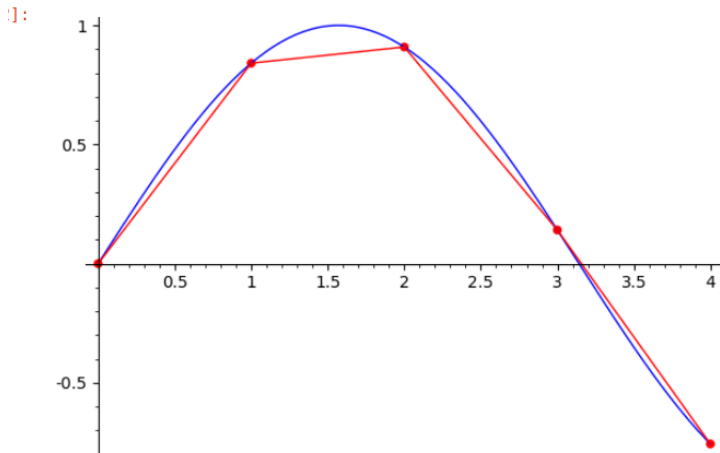


```
In [33]: 1 D1 = plot(sum([print(a, sin(a)) color='red' size=20) for a in [0, 411])
```

Figure: Um parabolóide hiperbólico.

Muitos gráficos juntos!

```
1 P1 = plot(sum([point((n,sin(n)),color='red',size=30) for n in [0..4]]))
2 P2 = plot(sin(x),0,4)
3 P3 = line([(n,sin(n)) for n in [0..4]],color='red')
4 P1+P2+P3
5
```



Cálculo Diferencial e Integral

Cálculo Diferencial e Integral

In [42]:

```
1 f(x) = (3*x^2 - x + 2)/(5*x - 4)
2 show(lim(f,x=1))
```

$$x \mapsto 4$$

In [49]:

```
1 show(f.derivative())
```

$$x \mapsto \frac{6x-1}{5x-4} - \frac{5(3x^2-x+2)}{(5x-4)^2}$$

In [52]:

```
1 show(f.integral(x))
```

$$x \mapsto \frac{3}{10}x^2 + \frac{7}{25}x + \frac{78}{125}\log(5x-4)$$

Figure: Derivadas e integrais

Cálculo Diferencial e Integral

edos, series,?

Matrizes

```
In [67]: 1 A = matrix([[1,2,4],  
2               [2,3,1],  
3               [3,1,5]])  
4 show(A)
```

$$\begin{pmatrix} 1 & 2 & 4 \\ 2 & 3 & 1 \\ 3 & 1 & 5 \end{pmatrix}$$

```
In [57]: 1 show(det(A))  
-28
```

```
In [88]: 1 show("A^(-1) = ", A.inverse(), " ; A na forma escalonada: ", A.echelon_form())
```

$$A^{(-1)} = \begin{pmatrix} -\frac{1}{2} & \frac{3}{14} & \frac{5}{14} \\ \frac{1}{4} & \frac{1}{4} & -\frac{1}{4} \\ \frac{1}{4} & -\frac{5}{28} & \frac{1}{28} \end{pmatrix} ; A \text{ na forma escalonada: } \begin{pmatrix} 1 & 0 & 18 \\ 0 & 1 & 7 \\ 0 & 0 & 28 \end{pmatrix}$$

Figure: Manipulando matrizes

Álgebra Linear

```
In [120]: 1 show("Polinômio Car.: ", A.charpoly())  
          2 show("Polinômio Min.: ", A.minpoly())
```

Polinômio Car.: $x^3 - 9x^2 + 6x + 28$

Polinômio Min.: $x^3 - 9x^2 + 6x + 28$

```
In [121]: 1 A.eigenvalues()
```

Out[121]: [-1.378695206755170?, 2.616358832559789?, 7.762336374195381?]

```
In [123]: 1 show(A.LU())
```

$$\left(\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ \frac{2}{3} & 1 & 0 \\ \frac{1}{3} & \frac{5}{7} & 1 \end{pmatrix}, \begin{pmatrix} 3 & 1 & 5 \\ 0 & \frac{7}{3} & -\frac{7}{3} \\ 0 & 0 & 4 \end{pmatrix} \right)$$

Figure: Polinômios, autovalores e decomposições

Álgebra - Cálculo Simbólico

Álgebra - Cálculo Simbólico

In [127]:

```
1 var('a,b')  
2 show(expand((a+b)^5))
```

$$a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

In [134]:

```
1 show(factor(a^6 - b^6))
```

$$(a^2 + ab + b^2)(a^2 - ab + b^2)(a + b)(a - b)$$

In [139]:

```
1 show(solve([a^2 + a - 1 == 0],a))
```

$$\left[a = -\frac{1}{2} \sqrt{5} - \frac{1}{2}, a = \frac{1}{2} \sqrt{5} - \frac{1}{2} \right]$$

Figure: Manipulando expressões, resolvendo equações

In [162]:

```
1 # interseção do círculo unitário com a parábola y = x^2
2 var('x,y')
3 sol = solve([
4     x^2 + y^2 == 1,
5     y == x^2,
6 ],x,y)
7 show(sol)
```

$$\left[\left[x = -\sqrt{\frac{1}{2} \sqrt{5} - \frac{1}{2}}, y = \frac{1}{2} \sqrt{5} - \frac{1}{2} \right], \left[x = \sqrt{\frac{1}{2} \sqrt{5} - \frac{1}{2}}, y = \frac{1}{2} \sqrt{5} - \frac{1}{2} \right], \left[x = -\sqrt{-\frac{1}{2} \sqrt{5} - \frac{1}{2}}, y = -\frac{1}{2} \sqrt{5} - \frac{1}{2} \right], \left[x = \sqrt{-\frac{1}{2} \sqrt{5} - \frac{1}{2}}, y = -\frac{1}{2} \sqrt{5} - \frac{1}{2} \right] \right]$$

In [180]:

```
1 f(x) = a*x^2 + b*1/x^2
2 show(f(x))
3 show(f(f(x)))
4 show(f(x).subs(a=3,b=2))
```

$$ax^2 + \frac{b}{x^2}$$

$$\left(\left(ax^2 + \frac{b}{x^2} \right)^2 a + \frac{b}{\left(ax^2 + \frac{b}{x^2} \right)^2} \right)^2 a + \frac{b}{\left(\left(ax^2 + \frac{b}{x^2} \right)^2 a + \frac{b}{\left(ax^2 + \frac{b}{x^2} \right)^2} \right)^2}$$

$$3x^2 + \frac{2}{x^2}$$

Álgebra abstrata

Álgebra Abstrata

```
In [187]: 1 G = SymmetricGroup(3)
          2 G.is_abelian()
```

Out[187]: False

```
In [193]: 1 G.multiplication_table(names='elements')
```

Out[193]:

	*	()	(2,3)	(1,2)	(1,2,3)	(1,3,2)	(1,3)
	+-----						
()		()	(2,3)	(1,2)	(1,2,3)	(1,3,2)	(1,3)
(2,3)		(2,3)	()	(1,2,3)	(1,2)	(1,3)	(1,3,2)
(1,2)		(1,2)	(1,3,2)	()	(1,3)	(2,3)	(1,2,3)
(1,2,3)		(1,2,3)	(1,3)	(2,3)	(1,3,2)	()	(1,2)
(1,3,2)		(1,3,2)	(1,2)	(1,3)	()	(1,2,3)	(2,3)
(1,3)		(1,3)	(1,2,3)	(1,3,2)	(2,3)	(1,2)	()

```
In [194]: 1 g = G("(1,2,3)")
          2 g.inverse()
```

Out[194]: (1,3,2)

Figure: Trabalhando com grupos

E muito mais:

- Combinatória, análise numérica, polinômios, grafos, etc
- Tópicos avançados (geometria algébrica, curvas elípticas, formas modulares, etc)
- Interface com outras ferramentas (GP/PARI, GAP, Singular,...)
- L^AT_EX!
- Todo poder do *Python*!
- O principal...

Teoria dos Números

A rainha da matemática



Figure: Carl F. Gauss

Por quê?

*“Associado ao pensamento computacional, **cumprе salientar a importância dos algoritmos e de seus fluxogramas**, que podem ser objetos de estudo nas aulas de Matemática. Um algoritmo é uma sequência finita de procedimentos que permite resolver um determinado problema. [...] A linguagem algorítmica tem pontos em comum com a linguagem algébrica, sobretudo em relação ao conceito de variável. **Outra habilidade relativa à álgebra que mantém estreita relação com o pensamento computacional é a identificação de padrões para se estabelecer generalizações, propriedades e algoritmos.**”*

Brasil (2017). Base nacional comum curricular. Ministério da Educação e Cultura

Computador não é o suficiente!

31	é primo
331	é primo
3331	é primo
33331	é primo
333331	é primo
3333331	é primo
33333331	é primo
333333331	é composto

$$333333331 = 17 \times 19607843$$

Computador não é o suficiente!

31	é primo
331	é primo
3331	é primo
33331	é primo
333331	é primo
3333331	é primo
33333331	é primo
333333331	é composto

$$333333331 = 17 \times 19607843$$

Computador não é o suficiente!

31	é primo
331	é primo
3331	é primo
33331	é primo
333331	é primo
3333331	é primo
33333331	é primo
333333331	é composto

$$333333331 = 17 \times 19607843$$

Computador não é o suficiente!

31	é primo
331	é primo
3331	é primo
33331	é primo
333331	é primo
3333331	é primo
33333331	é primo
333333331	é composto

$$333333331 = 17 \times 19607843$$

Computador não é o suficiente!

31	é primo
331	é primo
3331	é primo
33331	é primo
333331	é primo
3333331	é primo
33333331	é primo
333333331	é composto

$$333333331 = 17 \times 19607843$$

Computador não é o suficiente!

31	é primo
331	é primo
3331	é primo
33331	é primo
333331	é primo
3333331	é primo
33333331	é primo
333333331	é composto

$$333333331 = 17 \times 19607843$$

Computador não é o suficiente!

31	é primo
331	é primo
3331	é primo
33331	é primo
333331	é primo
3333331	é primo
33333331	é primo
333333331	é composto

$$333333331 = 17 \times 19607843$$

Computador não é o suficiente!

31	é primo
331	é primo
3331	é primo
33331	é primo
333331	é primo
3333331	é primo
33333331	é primo
333333331	é composto

$$333333331 = 17 \times 19607843$$

Computador não é o suficiente!

31	é primo
331	é primo
3331	é primo
33331	é primo
333331	é primo
3333331	é primo
33333331	é primo
333333331	é composto

$$333333331 = 17 \times 19607843$$

Computador não é o suficiente!

31	é primo
331	é primo
3331	é primo
33331	é primo
333331	é primo
3333331	é primo
33333331	é primo
333333331	é composto

$$333333331 = 17 \times 19607843$$

Onde aprender?

- Comput. Math. with SageMath
 - ▶ <http://sagebook.gforge.inria.fr/english.html>
- Sage for undergraduates
 - ▶ people.vcu.edu/~clarson/bard-sage-for-undergraduates-2014.pdf
- Grátis (inglês/francês/alemão)

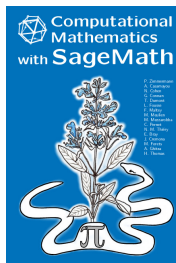


Figure: Comput. Math. with SageMath

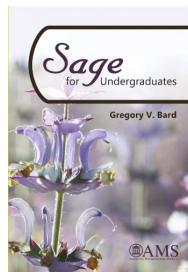
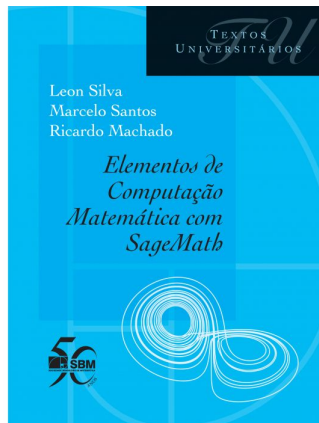


Figure: Sage for undergraduates

Em português

- Elementos de comput. matemática com o Sagemath
 - ▶ <https://loja.sbm.org.br/index.php/elementos-de-computac-html>
- Outros: sagemath.org/library-publications.html#books



Como usar?

- Baixando e instalando.
 - ▶ www.sagemath.org/download.html
 - ▶ Windows, Mac e Linux
 - ▶ Não recomendável (pelo menos inicialmente)
 - ▶ Terminal e Jupyter
- Cocalc
 - ▶ cocalc.com/
 - ▶ Colaborativo e interativo (mostro já!)
 - ▶ Nuvem
- SageMathCell
 - ▶ sagecell.sagemath.org/
 - ▶ Usaremos esse aqui!
 - ▶ Desvantagem: Não salva seu trabalho.

Tipos de dados †

- Números:
 - ▶ Inteiros `ZZ`
 - ▶ Racionais `QQ`
 - ▶ Reais `RR`
 - ▶ Complexos `CC`
- Booleanos: Verdadeiro/Falso (True/False)
- Strings (textos!)
- \rightarrow Listas \leftarrow
 - ▶ Sequências indexadas por $0, 1, 2, \dots$
 - ▶ Não são exatamente conjuntos... mas servem

$$\{x^2 \mid x \in \{1, \dots, 5\}\}$$

```
[ x^2 for x in [1..5]]
```

- Operações e funções

Finalmente...

Teorema (Divisão euclidiana)

Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Existem $q, r \in \mathbb{Z}$ únicos tais que

$$a = bq + r, r \in \{0, 1, \dots, b - 1\}$$

- Método `.quo_rem()` (**Q**uotient e **R**emainder — Quociente e resto)
- Uso: `a.quo_rem(b)`
- Retorna o par `(q, r)`
- **Cuidado!** Para $b < 0$ o comportamento é diferente.

Divisores

- Se o resto for zero dizemos que b *divide* a . A notação é $b \mid a$.
- No sage isso se verifica com o método `b.divides(a)`.
- Vamos criar uma lista com os divisores de a . †
- **Desafio:** Um natural n é *perfeito* se é a soma de seus divisores próprios, e.g.

$$6 = 1 + 2 + 3 \text{ e } 28 = 1 + 2 + 4 + 7 + 14$$

Encontre mais um número perfeito (Dica: Existe a função `sum`!)

- **Dever de casa 1:** Um teorema de Euclides/Euler classifica os perfeitos pares. Pesquise-o e encontre os 10 primeiros
- **Dever(?) de casa 2:** Encontre um número perfeito ímpar.

Divisores

- Se o resto for zero dizemos que b *divide* a . A notação é $b \mid a$.
- No sage isso se verifica com o método `b.divides(a)`.
- Vamos criar uma lista com os divisores de a . †
- **Desafio:** Um natural n é *perfeito* se é a soma de seus divisores próprios, e.g.

$$6 = 1 + 2 + 3 \text{ e } 28 = 1 + 2 + 4 + 7 + 14$$

Encontre mais um número perfeito (Dica: Existe a função `sum`!)

- **Dever de casa 1:** Um teorema de Euclides/Euler classifica os perfeitos pares. Pesquise-o e encontre os 10 primeiros
- **Dever(?) de casa 2:** Encontre um número perfeito ímpar.

Divisores

- Se o resto for zero dizemos que b *divide* a . A notação é $b \mid a$.
- No sage isso se verifica com o método `b.divides(a)`.
- Vamos criar uma lista com os divisores de a . †
- **Desafio:** Um natural n é *perfeito* se é a soma de seus divisores próprios, e.g.

$$6 = 1 + 2 + 3 \text{ e } 28 = 1 + 2 + 4 + 7 + 14$$

Encontre mais um número perfeito (Dica: Existe a função `sum`!)

- **Dever de casa 1:** Um teorema de Euclides/Euler classifica os perfeitos pares. Pesquise-o e encontre os 10 primeiros
- **Dever(?) de casa 2:** Encontre um número perfeito ímpar.

Primos

- Um natural $p > 1$ é primo seus divisores positivos são 1 e p .
- Como decidir se um dado n é primo?
- Testar se n é divisível por algum inteiro > 1 menor que ele. †
- **Dever de casa:** Otimize o algoritmo acima.
- No sage: `is_prime()`
- Pseudoprimos.
- Outras funções envolvendo primos. †

Primos

- Um natural $p > 1$ é primo seus divisores positivos são 1 e p .
- Como decidir se um dado n é primo?
- Testar se n é divisível por algum inteiro > 1 menor que ele. †
- **Dever de casa:** Otimize o algoritmo acima.
- No sage: `is_prime()`
- Pseudoprimos.
- Outras funções envolvendo primos. †

Primos

- Um natural $p > 1$ é primo seus divisores positivos são 1 e p .
- Como decidir se um dado n é primo?
- Testar se n é divisível por algum inteiro > 1 menor que ele. †
- **Dever de casa:** Otimize o algoritmo acima.
- No sage: `is_prime()`
- Pseudoprimos.
- Outras funções envolvendo primos. †

MDC

- Maior divisor comum
- `max([k for k in divisors(a) if k in divisors(b)])`
- Algoritmo de Euclides: **Lema:** $\text{mdc}(a, b) = \text{mdc}(b, a - kb)$
- r resto da divisão de a por $b \Rightarrow \text{mdc}(a, b) = \text{mdc}(b, r)$
- Divisões euclidianas sucessivas: †

	a		b		
1001	$=$	$9 \times$	109	$+ 20$	$\text{mdc}(1001, 109) = \text{mdc}(109, 20)$
109	$=$	$5 \times$	20	$+ 9$	$\text{mdc}(109, 20) = \text{mdc}(20, 9)$
20	$=$	$2 \times$	9	$+ 2$	$\text{mdc}(20, 9) = \text{mdc}(9, 2)$
9	$=$	$4 \times$	2	$+ 1$	$\text{mdc}(9, 2) = \text{mdc}(2, 1)$
2	$=$	$2 \times$	1	$+ 0.$	$\text{mdc}(2, 1) = \text{mdc}(1, 0) = 1$

Algoritmo de Euclides Estendido

- **T. Bézout:** Existem $x, y \in \mathbb{Z}$ tais que $ax + by = \text{mdc}(a, b)$.
- As divisões sucessivas do Alg. de Euclides fornecem x e y .
- † Uma solução elegante: Seja $M = (m_{ij}) \in M_{3 \times 2}(\mathbb{Z})$, dada por

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ a & b \end{pmatrix}.$$

Se $m_{32} \neq 0$, tome $q = \lfloor m_{31}/m_{32} \rfloor$ e substitua

$$M \longleftarrow M \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}.$$

Enquanto $m_{32} \neq 0$ repita esse processo. Quando $m_{32} = 0$ teremos que $m_{31} = \text{mdc}(a, b)$ e $x = m_{11}$ e $y = m_{21}$ satisfazem $ax + by = \text{mdc}(a, b)$

Algoritmo de Euclides Estendido

- **T. Bézout:** Existem $x, y \in \mathbb{Z}$ tais que $ax + by = \text{mdc}(a, b)$.
- As divisões sucessivas do Alg. de Euclides fornecem x e y .
- † Uma solução elegante: Seja $M = (m_{ij}) \in M_{3 \times 2}(\mathbb{Z})$, dada por

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ a & b \end{pmatrix}.$$

Se $m_{32} \neq 0$, tome $q = \lfloor m_{31}/m_{32} \rfloor$ e substitua

$$M \longleftarrow M \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}.$$

Enquanto $m_{32} \neq 0$ repita esse processo. Quando $m_{32} = 0$ teremos que $m_{31} = \text{mdc}(a, b)$ e $x = m_{11}$ e $y = m_{21}$ satisfazem $ax + by = \text{mdc}(a, b)$

Algoritmo de Euclides Estendido

- **T. Bézout:** Existem $x, y \in \mathbb{Z}$ tais que $ax + by = \text{mdc}(a, b)$.
- As divisões sucessivas do Alg. de Euclides fornecem x e y .
- † Uma solução elegante: Seja $M = (m_{ij}) \in M_{3 \times 2}(\mathbb{Z})$, dada por

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ a & b \end{pmatrix}.$$

Se $m_{32} \neq 0$, tome $q = \lfloor m_{31}/m_{32} \rfloor$ e substitua

$$M \longleftarrow M \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}.$$

Enquanto $m_{32} \neq 0$ repita esse processo. Quando $m_{32} = 0$ teremos que $m_{31} = \text{mdc}(a, b)$ e $x = m_{11}$ e $y = m_{21}$ satisfazem $ax + by = \text{mdc}(a, b)$

Fatoração Única

Teorema (Fundamental da Aritmética)

Todo inteiro $n > 1$ pode ser escrito de forma única como produto de primos

$$n = p_1 p_2 \cdots p_k,$$

com $p_1 \leq p_2 \leq \cdots \leq p_k$.

- Forma mais natural: Testar todos os primos! †
- No sage: `factor`
- Aplicação Importante: Criptografia!

Mini-Projeto: 1º dia

$$\frac{\#\{n \in \mathbb{N} \mid n \leq N \text{ e } p \mid n\}}{\#\{n \in \mathbb{N} \mid n \leq N\}} \rightarrow \frac{1}{p}, \text{ quando } N \rightarrow \infty$$

- Prob. de um inteiro ser divisível por p é $1/p$.
- Prob. de dois inteiros serem divisíveis por p é $1/p^2$.
- Prob. de dois inteiros não serem simultaneamente divisíveis por p é $1 - \frac{1}{p^2}$
- Prob. de dois inteiros não serem simultaneamente divisíveis por qualquer primo p (i.e. serem coprimos!)

$$\prod_{p \in P} \left(1 - \frac{1}{p^2}\right) = \cdots = \frac{6}{\pi^2}$$

- Tarefa: Escreva um código que dê aproximações para π tomando pares de inteiros arbitrários e verificando se são coprimos.

Ideia:

- Escolha um limite K e uma quantidade de repetições N .
- Crie um contador C para guardar os casos coprimos.
- Para $n = 1, \dots, N$
 - ▶ Escolha a, b aleatórios em $\{1, \dots, K\}$
 - ▶ Se $\text{mdc}(a, b) = 1$, aumente o valor no contador ($C \leftarrow C + 1$)
- Para N e K grandes devemos ter $\alpha := C/N \approx 6/\pi^2$.
- Isole o π na relação acima.
- Exiba uma aproximação para π usando α .
- Varie K e N e veja o efeito na aproximação.