O crivo de Eratóstenes

Praciano-Pereira, Tarcisio *

24 de fevereiro de 2023
préprints da Sobral Matemática
no. 2023.01
Editor Tarcisio Praciano-Pereira
tarcisio@sobralmatematica.org

Resumo

Eratóstenes foi um sábio grego que resolveu alguns problemas interessantes dos quais estou fazendo aqui a lembrança de dois, Um deles era muito comum no Ensino Médio brasileiro, o *crivo de Eratóstenes* um arquivo contendo alguns dos primeiros números primos, aqui estou mostrando os primeiros 24 no meu *crivo de Eratóstenes*. Mostro uma aplicação deste algoritmo, criptografia. O segundo foi genial, o cálculo da circunferência terrestre e numa época em que poucos acreditavam que Terra seria redonda.

palavras chave: circunferência da Terra, crivo de Eratóstenes, criptografia.

Eratosthenes was a Greek sage who solved some interesting problems of which I am remembering two here. One of them was very common in Brazilian High School, the *Sieve of Eratosthenes* a file containing some of the first prime numbers, here I am showing the first 30 in my *Eratosthenes sieve*. I am showing an application of this algorithm, cryptography. The second was brilliant, the calculation of the terrestrial circumference and in a a time when very few believed that the Earth was round.

keywords: cryptography, Eratosthenes sieve, Perimeter of the Earth.

*tarcisio@sobralmatematica.org

1 Eratóstenes e o seu crivo

Eratóstenes , foi um sábio grego que produziu o crivo de Eratóstenes que é uma listagem em sequência dos números primos até um certo ponto, uma vez que o conjunto dos números primos é infinito...

Aqui você tem o meu *crivo de Eratóstenes* contendo os primeiros 30 números primos.

crivo de Eratóstenes

1	2	3	5	7	11
13	17	19	23	31	37
41	43	47	53	59	61
67	71	73	79	83	89
97	101	103	107	109	113
127	131	137	139	149	151

Os alunos do *Ensino Médio* brasileiro, lembro-me de minha época de estudante, tinhamos em geral nas bolsas escolares, entre outros livros, um *livro de tabelas* em que estavam uma *tabela de logarítmos*, tabelas das *diversas funções trigonométricas* e, entre outras, o *crivo de Eratóstenes* bem mais significativo do que este que estou apresentando acima. Como não haviam máquinas de calcular e nem acesso a *Internet*, livros com tabelas eram essenciais para o trabalho escolar, inclusive com os *logaritmos* que eram a *máquina de calcular* da época e que no atrazo em que vivem as Escolas ainda ensinam *logaritmos* como um método para fazer contas...

Aqui eu construí o *crivo de Eratóstenes* com auxilio do `fator` até 151 em que você pode ver alguns dos fatos curiosos, os números primos gêmeos , que são os números primos seguidos pela soma de dois: (3, 5), (5, 7), (11, 13),(17, 19),(29, 31),(41, 43),(59, 61), (71,73), (101, 103), (107, 109), (137, 139), (149, 151) ...

`fator` é um programa que vem junto com as distribuições LinuX.

Segundo a Wikipédia, [1], existem cerca de mil números primos gêmeos abaixo de cem mil e oito mil abaixo de um milhão.

Os números primos foram e continuam sendo alvo de pesquisa, para aumentar a tabela dos primos conhecidos que hoje se encontra na casa dos bilhões havendo aglomerados de computadores que ficam dedicados nos finais de semana nesta busca. Por exemplo, a questão dos gêmeos merece atenção com problemas abertos envolvendo a sua distribuição.

Os números primos são importantes em criptografia por uma razão bem simples, que os restos na divisão por um número primo forma uma álgebra finita muito parecida com álgebra dos números inteiro positivos ou o corpo dos números racionais. Esta possibilidade algébrica permite um processo simples de encriptação que foi usado pelos alemães na segunda guerra com sua máquina de encriptação, *enigma*, cujo segredo foi desvendado pelo matemático inglês Alan Turin. Na tabela operatória dos restos por um número primo, a multiplicação por qualquer número primo, provoca uma permutação dos elementos da linha representando assim um método algébrico que pode ser usado num programa de computação, para produzir permutações e portanto encriptar dados. Observe

nas tabelas que apresento abaixo, cada coluna, ou linha, nestas tabelas contém uma permutação do conjunto dos restos, é uma propriedade fundamental da teoria dos grupos.

A tabela seguinte é da multiplicação dos restos na divisão por 7 em que cada linha é uma permutação da primeira obtida pela multiplicação pelo resto que se encontra na primeira coluna.

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

A próxima é a tabela da adição dos restos na divisão por 7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Usando estas duas tabelas você pode resolver qualquer equação, cujos coeficientes se encontrem neste conjunto de restos, apenas usando as propriedades fundamentais da aritmética dos números racionais, como existência do neutro multiplicativo ou neutro aditivo, existência do inverso aditivo ou multiplicativo e a propriedade associativa,

$$4x + 3 = 2$$

$$4 * x + 3 = 2 \tag{1}$$

$$4 * x + 3 + 4 = 2 + 4 \quad \Rightarrow \quad 4 * x + 0 = 2 + 4 = 6 \tag{2}$$

$$4 * x = 6 \tag{3}$$

$$2 * (4 * x) = 2 * 6 = 5 \tag{4}$$

$$2 * (4 * x) = (2 * 4) * x = 5 \tag{5}$$

$$1 * x = x = 5 \text{ a solução da equação} \tag{6}$$

$$\text{testando } 4 * 5 + 3 = 6 + 3 = 2 \quad \Leftarrow \quad 4 * x + 3 = 2 \tag{7}$$

Considere um exercício identificar onde foi usada, cada uma das propriedades, para obter a linha seguinte no sistema de equações (eq. 1)-(eq. 7).

Este exemplo lhe mostra que o conjunto finito dos restos na divisão por 7 tem as *mesmas propriedades* que o conjunto dos números racionais ou dos reais: todo

número tem um inverso aditivo ou multiplicativo, adição e multiplicação são comutativas e associativas e existe um elemento neutro para adição e outro para a multiplicação. Com isto eu posso resolver qualquer equação *com coeficientes dentro do conjunto dos restos na divisão por* 7.

Mas também se pode *encriptar* ou *desencriptar* qualquer informação baseada nesta tabela de multiplicação e adição dos restos na divisão por 7.

Aqui você a importância de descobrir números inteiros primos muito grandes: eles permitem uma álgebra mais generosa o que justifica a *generosidade* de certos financiadores que garantem computadores para matemáticos fazerem a pesquisa de números primos muito grandes. Não é exatamente porque os *rentistas* sejam *mecenas* da ciência ...

As tabelas da adição e multiplicação módulo 7 foram construídas por um programa em `C++` que vou voltar a usar para construir a maior tabela que for possível colocar na página que é a tabela seguinte, da adição dos inteiros módulo 19, foi produzida por um programa em `C++` que calculou os dados da tabela e construiu o layout da tabela em LaTeX .

A tabela da adição módulo 19

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3
5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4
6	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5
7	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6
8	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7
9	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8
10	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9
11	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10
12	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13
15	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
16	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
18	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

A tabela do produto módulo 19

*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	2	4	6	8	10	12	14	16	18	1	3	5	7	9	11	13	15	17
3	3	6	9	12	15	18	2	5	8	11	14	17	1	4	7	10	13	16
4	4	8	12	16	1	5	9	13	17	2	6	10	14	18	3	7	11	15
5	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14
6	6	12	18	5	11	17	4	10	16	3	9	15	2	8	14	1	7	13
7	7	14	2	9	16	4	11	18	6	13	1	8	15	3	10	17	5	12
8	8	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11
9	9	18	8	17	7	16	6	15	5	14	4	13	3	12	2	11	1	10
10	10	1	11	2	12	3	13	4	14	5	15	6	16	7	17	8	18	9
11	11	3	14	6	17	9	1	12	4	15	7	18	10	2	13	5	16	8
12	12	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7
13	13	7	1	14	8	2	15	9	3	16	10	4	17	11	5	18	12	6
14	14	9	4	18	13	8	3	17	12	7	2	16	11	6	1	15	10	5
15	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4
16	16	13	10	7	4	1	17	14	11	8	5	2	18	15	12	9	6	3
17	17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	6	4	2
18	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Um programa como este pode ser usado para encriptar dados com um valor grande para o número primo p, mas 19 foi o maior número primo que eu pude usar para que ainda fosse possível apresentar, de maneira decente, estas tabelas,

numa página de texto. Estas são as tabela da adição e do produto módulo 19. Testei a tabela para o número primo 23 mas não foi possível apresentá-la na página. O próximo número *primo interessante* no *crivo de Eratóstenes* é 37 e ele já representa um bom número primo para ser usado em encriptação uma vez que com a tabela de multiplicação e adição de $\mathbf{Z}_{37}$ já é possível montar uma máquina de encriptação para todas as letras do alfabeto, 24 mais os 10 algarismos decimais, $24 + 10 = 34 < 37$. Não caberia numa página editada esta tabela mas ela pode ser facilmente produzida para ser usada com um programa de computação a ser utilizado para fazer a encriptação e tudo que você precisa para se comunicar com alguém de forma segura, sem que *google, facebook* e similares possam saber o que você está comunicando para alguém, e tudo que você e seu interlocutor precisam é que a chave de encriptação é 37.

Certo, os algoritmos destes invasores conseguem desencriptar um texto encriptado com este sistema, mas o trabalho que daria somente seria interessante se eles desconfiassem que suas informações seriam valiosas para eles, e eles não teriam tempo para perder com pessoas comuns. Isto também mostra como é importante para os *banqueiros* a pesquisa sobre números primos, embora os *banqueiros* mesmo, não tenham a menor ideia sobre isto, eles nem trabalham nem estudam apenas acumulam renda! Mas tem muita gente que estuda e serve de *capacho para os banqueiros*. Vale a pena estudar o assunto, sobretudo se você quiser virar um *bancário*!

2 Perímetro da Terra

Outro feito de Eratóstenes foi a *medida da circunferência da Terra*

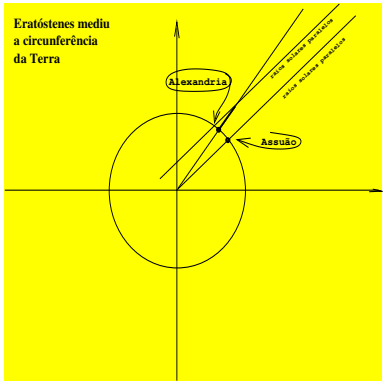

Figura 1:

Na Wikipédia, [1], é estimado que ele tenha cometido um erro entre um por cento a dez por cento e incerteza do erro fica por conta da incerteza do valor da medida de comprimento *estádio* que variava entre os países que a usavam na época. Na figura (fig 1), página 4, você pode a motivação geométrica de Eratóstenes para o cálculo da circunferência da Terra. Ele sabia que no *solstício*, na Grécia, quando os raios solares iluminavam o fundo dos poços e os prédios não tinham sombra ao meio dia, portanto era quando os raios solares chegavam ao meio dia paralelamente com os edifícios, na cidade Assuão que ficava sobre o mesmo paralelo que Alexandria então medindo a sombra dum edifício em Alexandria ele pode determinar o ângulo entre as paralelas consideradas como tal as retas dos raios do Sol o que lhe permitiu a determinação do ângulo central. A medida da circunferência da Terra entre as duas cidades se diz ter sido feito contando

as passadas de soldados marchando a passos cadenciados entre as duas cidades, provavelmente uma das *melhores utilização que se pode ter feito em toda a História da Humanidade de militares*. Conhecendo o comprimento do arco e o comprimento do ângulo central, ele obteve com uma *razão de três* a circunferência da Terra segundo a Wikipédia, 39.700 km, muito semelhante ao valor hoje estimado que é 40.008 km.

Referências

[1] Wikimedia Foundation. Wikipedia, enciclopédia livre na internet. http://www.wikipedia.org.