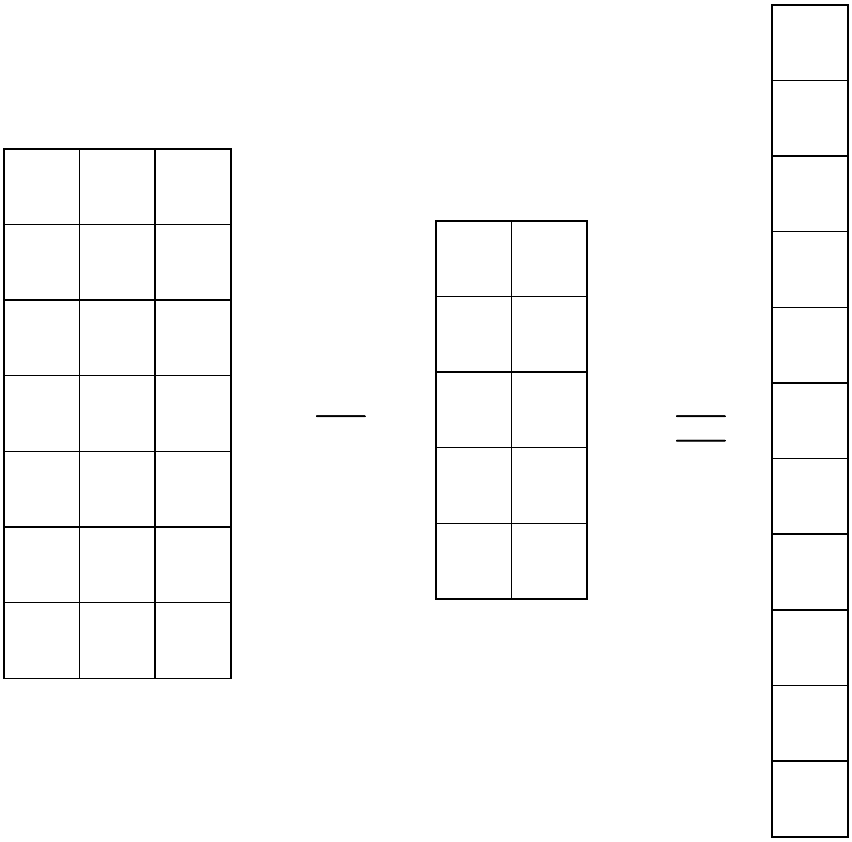
eric campos bastos guedes



Fórmulas para $\mathbb{N}$úmeros $\mathbb{P}$rimos

Eric Campos Bastos Guedes

Fórmulas para Números Primos

Ficha catalográfica

G 924 Guedes, Eric Campos Bastos

Fórmulas para números primos: / Eric Campos Bastos Guedes. – Rio de Janeiro: Sociedade Brasileira de Matemática, 2008.

89p.

ISBN: ____________________

1. Números primos. 2 Teoria dos números. 3 Matemática-fórmulas. I. Título

CDD: 512.72

Em memória de meu pai

Agradeço ao professor Jorge Petrúcio Viana
pelo apoio e incentivo.

Prefácio

Uma fórmula para primos é uma função cuja imagem é um conjunto de números primos. Certa vez, mostrei a um grupo heterogêneo de estudantes e professores de Matemática um exemplo de função que produzia todos os primos, e somente primos. A primeira reação foi o espanto de quem sempre ouviu falar que não existiam tais fórmulas. Em seguida, os mais experientes esclareceram que existem infinitas fórmulas para primos. Havendo infinitas, quais serão especialmente elegantes? Breves? Engenhosas? Quais suscitarão questões de interesse? Que conjecturas surgirão de modo natural? Como caracterizar os números primos de modo não trivial? Como construir uma fórmula para primos usando essa caracterização? Essas questões vão sendo respondidas ao longo deste livro, através de exemplos acompanhados de demonstrações. O bom leitor terá a oportunidade de responder a questões que o desenvolvimento das idéias do texto proporciona.

Niterói, maio de 2006.

Eric Campos Bastos Guedes

Sumário

Os Números Primos e seus Desafios....................13
Uma Função de Variável Matricial que Produz Números Primos....................25
Funções que Geram Números Primos....................32
Quatro Fórmulas Relacionadas que Produzem Números Primos....................39
Outras Fórmulas Relacionadas que Produzem Números Primos....................43
Uma Aplicação da Análise à Teoria dos Números....................46
Relacionando Números Primos e Binomiais....................52
Uma Função que Produz Infinitos Números Primos....................58
Uma Função para o enésimo Número Primo....................64
Números Primos e Séries Formais....................67
Caracterizando Intervalos de Números Primos através de Polinômios....................72
Produzindo Números Primos por Iteração....................78
Uma Constante para os Números Primos....................81
Primalidade e Número de Divisores....................84
Outras Fórmulas e Conjecturas....................86
Tábua de Números Primos....................89
Referências Bibliográficas....................94

1

Os Números Primos e seus Desafios

Divisibilidade

Seria difícil falar em números primos sem mencionar o conceito de divisibilidade. Se a e b são inteiros quaisquer, então dizemos que b é *divisível* por a sempre que existir um número inteiro q satisfazendo $b=aq$. Dizer que b é divisível por a é o mesmo que dizer: "b é *múltiplo* de a", "a é *divisor* de b", "*a divide b*", ou, em símbolos $a|b$. Escreve-se $a|b$ para significar que b deixa resto zero na divisão por a, isto é, a divisão de b por a é exata. Quando não o for escreveremos $a \nmid b$ (lê-se "a não divide b"). Exemplos: $2|6$, $6|60$, $5 \nmid 6$.

Estando claro o conceito de divisibilidade, podemos falar no conjunto de divisores positivos de um inteiro. Por exemplo, os divisores positivos de 12 são 1, 2, 3, 4, 6 e 12; os de 8 são 1, 2, 4 e 8. Os divisores *comuns* a 12 e 8 são 1, 2 e 4. O maior deles é o 4, e por isto é chamado de *m*áximo *d*ivisor *c*omum de 8 e 12, o que em símbolos se escreve mdc(8,12)=4 ou (8,12)=4, quando não houver ambigüidade.

Tem-se m = mdc(a, b) sempre que cumprirem-se as propriedades seguintes:

(i) $m|a$ e $m|b$

(ii) se $d|a$ e $d|b$ então $d|m$

(iii) $m > 0$

A propriedade (i) diz que o mdc de dois números é um divisor comum desses números; (ii) nos diz que todo divisor comum de a e b também divide seu mdc; se m satisfaz (i) e (ii), então $-m$ também satisfaz (i) e (ii), de modo que, para evitar ambigüidade, (iii) nos diz para tomarmos sempre o valor positivo.

Essas questões são fundamentais e precisamos delas para prosseguir. Este é o motivo pelo qual as menciono aqui. Qualquer livro de introdução a Teoria dos Números traz logo no início essas informações.

Inteiros coprimos

Dois números inteiros são ditos *coprimos*, ou *relativamente primos* ou ainda *primos entre si* sempre que seu máximo divisor comum for igual a 1. Assim, 27 e 80 são coprimos, porque mdc(27, 80)=1. Entretanto 48 e 33 não são relativamente primos, uma vez que mdc(48, 33)=3≠1.

Definindo números primos

Os números primos são os números naturais que têm exatamente dois divisores positivos. Esta não é uma definição citada com freqüência, mas é a que me parece, aqui, a mais adequada. Existem outras definições equivalentes. A mais popular diz que número primo é um inteiro maior que 1 cujos únicos divisores positivos são 1 e ele mesmo. Assim, 7 é primo, pois seus únicos divisores são 1 e 7; mas 9 não é primo pois tem três divisores: 1, 3 e 9.

Ainda há uma definição importante de número primo. Ela diz que um inteiro $p>1$ é primo quando $p|a$ ou $p|b$, para *quaisquer* inteiros a e b tais que $p|ab$. Logo, quando um primo divide um produto, necessariamente divide algum dos fatores.

A seqüência dos primos

Os dez primeiros números primos são 2, 3, 5, 7, 11, 13, 17, 19, 23 e 29. Esta lista pode ser estendida indefinidamente, conforme mostraremos ainda neste capítulo. Então, existe uma *sucessão* ou *seqüência* de números primos. Faz sentido, portanto, falar num primeiro número primo, que é o 2; num segundo primo (o 3) e mais geralmente num n-ésimo número primo, que ocupa a posição n na sucessão e é denotado por p_n. Assim, por exemplo, $p_{10} = 29$, ou seja, o décimo primo é 29.

Algumas notações

O conceito de número primo está fortemente ligado ao de *divisibilidade*. Dado um inteiro positivo *n*, seu *número de divisores positivos* é representado por $\mathrm{d}(n)$. Assim, um número natural *p* é primo quando $\mathrm{d}(p)=2$. Por exemplo, os divisores de 127 são 1 e 127; então $\mathrm{d}(127)=2$ e portanto 127 é primo. Por outro lado, os divisores de 128 são 1, 2, 4, 8, 16, 32, 64 e 128 em número de 8; logo $\mathrm{d}(128)=8\neq 2$ e portanto 128 não é primo.

Vimos duas notações: p_n designa o *n*-ésimo primo e $\mathrm{d}(n)$ a quantidade de divisores de *n*. Usaremos essas designações em todo livro. Elas são empregadas com bastante freqüência pelos matemáticos e se consagraram pela tradição. Uma outra função comum em Teoria dos Números é a σ_k. Representa-se por $\sigma_k(n)$ a soma das *k*-ésimas potências dos divisores positivos de *n*. Note o leitor que para qualquer inteiro *n*, tem-se $\sigma_0(n)=\mathrm{d}(n)$. Além disso, denotando por $\mathrm{s}(n)$ a soma dos divisores de *n*, vale $\sigma_1(n)=\mathrm{s}(n)$. Então, pode-se usar uma ou outra notação conforme for conveniente.

Uma primeira fórmula

Já se pode, com o que vimos até aqui, escrever uma fórmula para primos. Basta notar que:

(i) Dado *n*>1, a sucessão $\sigma_{-1}(n),\sigma_{-2}(n),\sigma_{-3}(n),\ldots$ converge para 1;

(ii) A sucessão $\sqrt[-1]{\sigma_{-1}(n)-1},\sqrt[-2]{\sigma_{-2}(n)-1},\sqrt[-3]{\sigma_{-3}(n)-1},\ldots$ converge para o menor divisor maior que 1 de *n*;

(iii) De modo mais geral $\lim\limits_{\alpha\to-\infty}\sqrt[\alpha]{\sigma_\alpha(n)-1}$ é o menor divisor maior que 1 de *n*;

(iv) Dado qualquer inteiro *n*>1, seu menor divisor maior que 1 é primo;

(v) Logo, $f(n)=\lim\limits_{\alpha\to-\infty}\sqrt[\alpha]{\sigma_\alpha(n)-1}$ produz todos os primos, e somente primos sendo, portanto, uma fórmula para primos.

Alguns leitores podem ficar um pouco desapontados com este primeiro exemplo. Para calcular o valor de $f(n)$ é necessário conhecer os divisores n. Mais que isto: é preciso que conheçamos a soma das α-ésimas potências dos divisores de n (quando α tende a $-\infty$ (!)). É muito complicado usar esta fórmula para calcular primos.

Não obstante, ela é bonita! É concisa, não trivial e faz exatamente o que dela se pede: produz (todos os) primos e somente primos, embora de modo computacionalmente ineficaz. Neste livro não nos prenderemos meramente a questão estética das fórmulas. Também serão levantadas questões teóricas, conjecturas sugeridas explicita ou implicitamente. Não é nosso objetivo aqui medir a rapidez das fórmulas ou sua *complexidade computacional*, embora esta questão interesse a muitos matemáticos de renome.

O crivo de Eratóstenes

Se estivéssemos interessados em determinar rapidamente todos os primos menores que um número dado, seria insensato usar a fórmula que vimos. Em vez disso, usaríamos o crivo. Ele consiste num *algoritmo* devido ao matemático grego Eratóstenes (276 a.C–194 a.C), o mesmo que fez a primeira estimativa para a circunferência da Terra. O crivo consiste em, dado um inteiro $n>3$, determinar todos os números primos menores que n mediante as seguintes etapas:

Etapa 1: Escrevemos os números ímpares do intervalo aberto $]2, n[$ em ordem crescente numa tabela;

Etapa 2: Circulamos o menor número não circulado e não cortado (este número é primo);

Etapa 3: Chamamos de c o maior número circulado. Se $n>c^2$ passamos para a etapa 4. Caso contrário encerramos o algoritmo e os números primos menores que n são exatamente aqueles que não foram cortados (os circulados também são primos) e também o inteiro 2.

Etapa 4: Iniciando por c^2, vamos cortando os números da tabela de c em c, isto é, cortamos c^2, c^2+c, c^2+2c etc. (cortamos estes números pois eles não são primos, por serem múltiplos de c; não precisamos cortar nenhum múltiplo de c

menor que c^2 pois eles já foram cortados antes). Nesta etapa é como se estivéssemos *peneirando* nossa tabela de números, por isso o nome *crivo*. Neste momento retorna-se à etapa 2.

O crivo é um meio rápido de decidir quais números menores que um inteiro dado são primos, e quais não são. Os que não são primos se escrevem como produto de primos (com exceção de 1) e por isto chamam-se *compostos*. O número 1 não é considerado nem primo nem composto. É interessante notar que para os gregos antigos 1 não era nem sequer um número (veja p.1 de [15]).

As funções π, teto, chão e parte fracionária

Voltemos ao crivo. Como ele nos mostra todos os primos menores que um inteiro *n*, é natural nos perguntarmos *quantos* primos há até *n*. Representa-se por $\pi(n)$ a quantidade de números primos menores *ou iguais* a *n*. Assim, $\pi(1)=0$ pois não há primos no intervalo $[1,1]=\{1\}$; $\pi(11)=5$, porque no intervalo $[1,11]$ existem 5 números primos, a saber, 2, 3, 5, 7 e 11.

Sabemos que primalidade está relacionada com divisibilidade. E quando nos questionamos a respeito de divisibilidade, estamos procurando informações a respeito de alguma divisão. Por outro lado, números primos são sempre *inteiros*, mas muitos valores de funções *não* são números inteiros. Então precisamos, algumas vezes, "converter" números reais em inteiros. Por isso, duas funções que aparecem com freqüência quando se buscam fórmulas para primos são a *chão* e a *teto*. O chão de *x* é denotado por $\lfloor x \rfloor$ e é o maior inteiro $\leq x$. O teto de *x* é denotado por $\lceil x \rceil$ e é o menor inteiro $\geq x$. Os números $\lfloor x \rfloor$ e $\lceil x \rceil$ são os únicos *inteiros* que satisfazem $x-1<\lfloor x \rfloor \leq x \leq \lceil x \rceil < x+1$. Note que chamar $\lfloor x \rfloor$ de o *chão* de *x* e $\lceil x \rceil$ de o *teto* de *x* está em conformidade com o que é sugerido graficamente por estes símbolos.

Assim, por exemplo, $\lfloor 7,8 \rfloor = 7$ e $\lceil 20,2 \rceil = 21$. Com números negativos tem-se $\lfloor -7,42 \rfloor = -8 = \lceil -8,17 \rceil$. Quando *x* é inteiro, tanto o chão quanto o teto de *x* igualam-se a *x*.