Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática
em Rede Nacional PROFMAT

Números Primos e o Postulado de Bertrand [†]

por

Antonio Eudes Ferreira

sob orientação do

Prof. Dr. Napoleón Caro Tuesta

Dissertação apresentado ao Corpo Docente do Mestrado Profissional em Rede Nacional PROFMAT - CCEN - UFPB, como requisito parcial para a obtenção do título de Mestre em Matemática.

Agosto/2014
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

Números Primos e o Postulado de Bertrand

por

Antonio Eudes Ferreira

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática

Aprovada por:

Prof. Dr. Napoleón Caro Tuesta -UFPB (Orientador)

Prof. Dr. Antônio de Andrade e Silva - UFPB

Prof. Dr. Diogo Diniz Pereira da Silva e Silva - UFCG

Agosto/2014

Agradecimentos

A Deus, por ser um Pai tão presente em minha vida e me proporcionar esta grande conquista.

A minha mãe, Maria de Fátima Ferreira Barbosa, por fazer papel de pai e mãe ao mesmo tempo, estando sempre ao meu lado em todos os momentos, me incentivando e acreditando que sou capaz de fazer sempre o melhor. Agradeço por sempre fazer seu papel de mãe protetora da forma mais linda que existe e comparilhar de todos os sentimentos por mim vividos, além de ser o principal motivo por eu querer sempre ir mais longe.

Aos meus irmãos, Elifábio Ferreira Barbosa e Maria Elizângela Ferreira Barbosa, que mesmo ausentes, sempre participaram ativamente na minha formação, a quem devo todo meu carinho, respeito e amor.

Aos meus primos - irmãos, Menezes Matias Ferreira e Antonia Elinaíde Ferreira Dantas, por se fazerem sempre presentes na minha vida, alegrando todos os meus dias, apoiando e me incentivando em todas as minhas decisões.

A todos os meus amigos e familiares.

A todos professores que contribuíram com seus conhecimentos e foram de grande importância na minha formação, em especial, ao Professor Napoleón Caro Tuesta pelos ensinamentos e por me orientar de forma significativa e plausível, tornando possível a realização deste sonho.

Aos meus colegas de curso, que estiveram juntos comigo nessa caminhada tão árdua.

Dedicatória

A minha inestimável avó Antonia Avelina de Jesus (in memorian), que sempre torceu pelo meu sucesso e ao meu pai Elesbão Ferreira Barbosa (in memorian).

Resumo

Este trabalho apresenta um estudo sobre os números primos, como estão distribuídos, quantos números primos existem entre 1 e um número real x qualquer, fórmulas que geram primos, além de uma generalização para o Postulado de Bertrand. São abordadas seis demonstrações que mostram que existem infinitos números primos usando redução ao absurdo, Números de Fermat, Números de Mersenne, Cálculo Elementar e Topologia.

Palavras-chaves: Números Primos, Primos de Fermat, Primos de Mersenne, Postulado de Bertrand.

Abstract

This work presents a study of prime numbers, how they are distributed, how many prime numbers are there between 1 and a real number x, formulas that generate primes, and a generalization to Bertrand's Postulate. Six proofs that there are infinitely many primes using reductio ad absurdum, Fermat numbers, Mersenne numbers, Elementary Calculus and Topology are discussed.

Keywords: Prime Numbers, Fermat primes, Mersenne primes, Bertrand Postulate.

Sumário

1 Números Primos **1**
1.1 Prova 1 2
1.2 Prova 2 3
1.3 Prova 3 4
1.4 Prova 4 5
1.5 Prova 5 7
1.6 Prova 6 8

2 Postulado de Bertrand **11**

3 Coeficientes binomiais (quase) nunca são potências **16**

A Primos em certas progressões aritméticas **21**

B Euler, um Gigante da Matemática **23**

C Legendre **24**
C.1 Teorema de Lagrange 25

D Estimativa via integrais **28**
D.1 Estimativas para fatoriais - fórmula de Stirling 29

E Topologia **31**

F Demonstração do Postulado de Bertrand via Ramanujan **33**

G Estimativas para coeficientes binomiais **37**

H A função zeta de Riemann **39**

I Criptografia **41**

Referências Bibliográficas **44**

Introdução

Os números primos são conhecidos pela humanidade há muito tempo. Esses números desempenham papel fundamental na Aritmética e a eles estão associados muitos problemas famosos cujas soluções têm resistido aos esforços de várias gerações de matemáticos. Os gregos foram os pioneiros no estudo dos números primos e as suas propriedades. Entre os gregos, principalmente entre gregos pitagóricos de várias gerações depois de Pitágoras, surgiram outras denominações para os números primos, como: retilíneos, lineares e eutimétricos. Contudo, elas tiveram uso muito restrito e cairam no desuso. Matemáticos da escola de Pitágoras (500 a 300 A.C.) tinham bastante inte-resse nos números pelas suas propriedades numerológicas e místicas. O conjunto dos números primos possui uma definição bastante simples, porém com uma aritmética muito complexa. O matemático grego Euclides provou que os números primos eram infinitos, mesmo assim, problemas envolvendo números primos mantiveram ocupados quase todos os matemáticos desde a antiguidade: como saber se um número é primo ou não, ou pre-ver a sua existência em um conjunto de números, ou ainda encontrar uma fórmula para definí-los. Muitas dessas questões continuam sem resposta. Neste trabalho apresentaremos seis demonstrações da infinitude dos números primos. A primeira, mais antiga e clássica, foi apresentada por Euclides, a segunda usando números de Fermat, a terceira usando números de Mersenne, a quarta usando Cálculo Elementar, a quinta usando Topologia e a última, foi graças ao grande Paul Erdős. Estudaremos o Postulado de Bertand e mostraremos que coeficientes binomiais (quase) nunca são potências.

Capítulo 1

Números Primos

"À Matemática é a rainha das ciências e a Teoria dos Números é a rainha da Matemática".

Karl. F. Gauss.

Neste capítulo serão dadas seis demonstrações sobre a infinitude dos números primos. Mas, antes lembremos algumas noções básicas.

Definição: Um número natural maior do que 1 e que só é divisível por 1 e por si próprio é chamado de **número primo.**

Da definição acima, dados dois números primos p e q e um número natural a qualquer, decorrem os seguintes fatos:

I) Se $p \mid q$, então $p = q$.
De fato, como $p \mid q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

□

II) Se $p \nmid a$, então $\text{mdc}(p, a) = 1$.
De fato, se $\text{mdc}(p, a) = d$, temos que $d \mid p$ e $d \mid a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$.

□

Um número maior do que 1 e que não é primo será chamado de **composto**. Portanto, se um número n é composto, existirá um divisor n_1 de n tal que $n_1 \neq 1$ e $n_1 \neq n$. Logo, existe um número natural n_2 tal que

$$n = n_1 n_2, \text{ com } 1 < n_1 < n \text{ e } 1 < n_2 < n$$

Por exemplo, 2, 3, 5, 7, 11 e 13 são números primos, enquanto que 4, 6, 8, 9, 10 e 12 são compostos.
Do ponto de vista da estrutura multiplicativa dos naturais, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais, conforme afirma o *Teorema Fundamental da Aritmética* que mostra que todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.

Teorema: *Existem infinitos números primos.*

Nas seguintes demonstrações iremos considerar $\mathbb{N} = \{0, 1, 2, 3, ...\}$ como o conjunto dos números naturais, $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ o conjunto dos números inteiros e $\mathbb{P} = \{2, 3, 5, 7, 11, ...\}$ como o conjunto dos números primos. Usaremos também o fato que os números naturais são infinitos e que todo número natural pode ser escrito como o produto de números primos.

1.1 Prova 1

Euclides viveu em Alexandria cerca de 300 a. C., sendo um do três maiores matemáticos da Antiguidade grega e, sem dúvida, de todos os tempos. Pouco se sabe da sua verdadeira biografia. Considerado *pai da Geometria*, tendo em vista os seus avanços feitos nesta área, Euclides, teve uma participação significativa e notória no âmbito da Teoria do Números. Euclides de Alexandria publicou *Os Elementos*, cerca de 300 a.C., provando vários resultados sobre números primos. A demonstração que há infinitos números primos aparece no livro IX de *Os Elementos*, onde, pela primeira vez na história da matemática, uma demonstração é feita a partir do uso da redução ao absurdo.

Prova: Suponhamos que o conjuntos dos números primos $\mathbb{P}$ é finito, isto é, $\mathbb{P} = \{p_1, p_2, ..., p_r\}$ onde $p_1 = 2 < p_2 = 3 < p_3 = 5 < ...$ e considere $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r + 1$. Então, n possui um divisor primo p. Mas p não é um dos p_i : caso contrário p seria um divisor de n e do produto $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r$, e assim também da diferença $n - p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r = 1$, o que é impossível. Portanto, o conjunto $\mathbb{P}$ não é finito.

□

A demonstração apresentada por Euclides serve de espelho para mostrar que em uma determinada progressão aritmética existem infinitos números primos. Para saber mais, leia o texto "Primos em certas progressões aritmética" que se encontra no apêndice A.

1.2 Prova 2

Na seguinte demonstração, usaremos os números de Fermat ($F_n = 2^{2^n} + 1$, com $n = 0, 1, 2, ...$). Pierre de Fermat (1601 - 1665), jurista francês e matemático amador, é considerado, após Euclides e Eratóstenes, o primeiro matemático a contribuir para o desenvolvimento da Teoria dos Números do ponto de vista teórico. Filho de Dominique de Fermat - rico mercador de peles - teve uma educação privilegiada, inicialmente no mosteiro franciscano de Grandselve e depois na Universidade de Toulouse. Fermat teve contribuições significativas na matemática. Conjecturou e demonstrou o chamado *Pequeno Teorema de Fermat* que possui o seguinte enunciado:

"Se p é um número primo, então para todo natural a, $a^p \equiv a \ (mod\ p)$".

Atualmente este teorema é a base de muitos resultados da Teoria dos Números e de métodos para determinação de números primos, utlizados em larga escala na computação e na criptografia. Essa conjectura foi provada por Euler (veja B do apêndice), em 1736.
Os resultados de Fermat foram divulgados por meio de sua correspondência, principalmente com o padre Marin Mersenne, que desempenhava o papel de divulgador da Matemática. Numa de suas cartas de 1640, Fermat enunciou o seu Pequeno Teorema, dizendo que não escreveria a demonstração por ser longa demais. A sua contribuição mais marcante foi a anotação deixada na margem do Problema 8, do Livro 2, de sua cópia de Bachet da *Aritmética* de Diofanto, onde se encontravam descritas as infinitas soluções da equação pitagórica $x^2 + y^2 = z^2$, dizia:

"Por outro lado, é impossível separar um cubo em dois cubos, ou uma biquadrada em duas biquadradas, ou, em geral, uma potência qualquer, exceto um quadrado em duas potências semelhantes. Eu descobri uma demonstração verdadeiramente maravilhosa disto, que todavia esta margem não é suficientemente grande para cabê-la."

Apesar de não demonstrada por ele, acabou sendo chamada de Último Teorema de Fermat e foi demonstrada em 1995, pelo matemático inglês, Andrew Wiles.
Há muito era procurado por matemáticos fórmulas que gerassem números primos. Fermat propôs que a fórmula $2^{2^n} + 1$ com $n \in \mathbb{N}$ produzia números primos. Para $n = 0, 1, 2, 3$ e 4, temos:

$$\begin{aligned} n &= 0 \rightarrow F_0 = 3 \\ n &= 1 \rightarrow F_1 = 5 \\ n &= 2 \rightarrow F_2 = 17 \\ n &= 3 \rightarrow F_3 = 257 \\ n &= 4 \rightarrow F_4 = 65537 \end{aligned}$$

são números primos. Apesar de não ter um prova convicta do seu resultado, sua crença foi posteriormente demonstrada como falsa com a apresentação de uma fatoração de $2^{2^5}+1$ proposta por Leonard Euler. Os números de Fermat primos são chamados de *primos de Fermat*. Até hoje, não se sabe se existem outros primos de Fermat além dos cinco primeiros. Um importante resultado acerca desses números, afirma que quaisquer dois primos de Fermat são relativamentes primos, o que nos leva a mais uma demonstração de que há infinitos números primos, pois cada número de Fermat tem pelo menos um divisor primo e esses divisores primos são todos distintos.

Prova: Consideremos os números de Fermat, $F_n = 2^{2^n}+1$ para $n = 0, 1, 2, 3, \cdots$. Vamos mostrar a seguinte recorrência:

$$\prod_{k=0}^{n-1} F_k = F_n - 2 \qquad (n \geq 1),$$

Usemos indução sobre n. Para n = 1, temos $F_0 = 3$ e $F_1 - 2 = 3$. Por indução concluímos que:

$$\prod_{k=0}^{n} F_k = (\prod_{k=0}^{n-1} F_k)F_n = (F_n - 2).F_n = (2^{2^n}-1)(2^{2^n}+1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2$$

Segue-se da fórmula anterior, que dois números de Fermat diferentes são relativamentes primos. Com efeito, se d é um divisor de F_k e F_n $(k < n)$, então d divide 2 e consequentemente d = 1 ou d = 2. Mas, d = 2 é impossível, já que todo número de Fermat é ímpar. Portanto, como existem infinitos números de Fermat, todos coprimos dois a dois, conluímos que existem infinitos números primos.

□

1.3 Prova 3

Para a seguinte prova, usaremos os números de Mersenne ($M_p = 2^p - 1$, com p primo). Marin Mersenne, nascido em 1588, foi um matemático, teórico musical, padre mínimo, teólogo e filósofo francês. Mersenne era o centro da divulgação científica, correspondendo-se com os maiores cientistas, seus conteporâneos, como Descartes, Galileu, Fermat, Pascal e Torricelli. Mersenne organizava também encontros entre estes cientistas e viajava com frequência pela Europa para se encontrar com alguns deles. Também teve sua contribuição na área da teoria dos números.

Assim como Fermat, Mersenne propôs uma fórmula para se obter números primos. Usando a relação $M_p = 2^p - 1$, onde p é um número primo e $2 \leq p \leq 5000$ os números de Mersenne que são primos, chamados de *primos de Mersenne*, correspondem aos seguintes valores de p: 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 1279, 2203, 2281, 3217, 4253 e 4423. Mersenne sabia que se n é composto, então M_n também o é. Já se n é primo, nem sempre M_n é primo ($2^{11} - 1 = 2047 = 23 \cdot 89$ é composto). Até dezembro de 2001, o maior primo de Mersenne conhecido era $M_{13466917}$, que possui no sistema decimal 4053946 dígitos, e é o trigésimo nono primo de Mersenne conhecido.

Prova: Suponhamos que $\mathbb{P}$ é finito. Seja p o maior número primo. Consideremos o *número de Mersenne* $2^p - 1$. Mostraremos que qualquer fator primo q de $2^p - 1$ seja maior do que p, o que nos levará a uma contradição e consequentemente, concluiremos que $\mathbb{P}$ é infinito. Seja q um primo que divide $2^p - 1$, de forma que $2^p \equiv 1 \bmod q$. Uma vez que p é primo, significa que o elemento 2 tem ordem p no grupo multiplicativo $\mathbb{Z}_q \backslash \{0\}$ do corpo Z_q. Esse grupo tem $q - 1$ elementos. Pelo teorema de Lagrange (veja C.1 do apêndice), sabemos que a ordem de cada elemento divide a ordem do grupo, ou seja, $p | q - 1$, e daí, $p < q$.

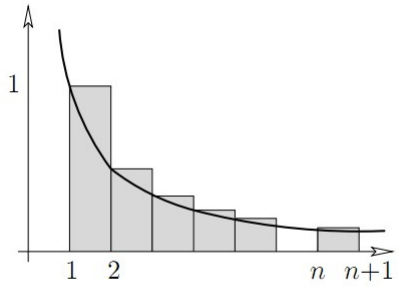
□

1.4 Prova 4

Gauss, assim como outros matemáticos, sempre buscou responder perguntas relacionadas a distribuição dos números primos, como por exemplo: Quantos números primos existem entre 1 e um número x qualquer? Gauss trabalhou com uma função, que posteriormente foi denotada por $\pi(x)$, definida como o número de primos que são menores que ou iguais ao número real x, $\pi(x) := \#\ \{p \leq x : p \in \mathbb{P}\}$, chamada de *função de contagem dos números primos.* Assim temos, por exemplo: $\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(5) = 3$, $\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(\sqrt{2}) = 0$, $\pi(e) = 1$, etc. Assim, a proporção de números primos entre 1 e x é dada por $\dfrac{\pi(x)}{x}$. Matemáticos buscaram achar boas aproximações para $\pi(x)$ por funções contínuas. Em 1972, Gauss conjeccturou que $\pi(x)$ era assintoticamente aderente a função integral logarítmica ($f(x) = \int_2^x \frac{dt}{\ln t}$), sendo provada em 1896 por Hadamard e De La Vallée Poussin. Conhecido como Teorema do Número Primo que afirma que o $\lim\limits_{x \to \infty} \dfrac{\pi(x)}{x/\ln x} = 1$.
Gauss quando conjecturou a aproximação de $\pi(x)$ pela função integral logarítmica, contava apenas com 15 anos de idade. Em 1798, inspirado pelo Teorema do Número Primo, Legendre conjecturou que $\pi(x) \sim \dfrac{x}{\ln x - 1,08366}$. Sendo demonstrada como falsa, por Tschebycheff, quarenta anos mais tarde. Vejamos a demonstração que

existe infinitos números primos usando Cáculo Elementar.

Prova: Consideremos $\pi(x) := \#\{p \leq x : p \in \mathbb{P}\}$. Enumeremos os primos $\mathbb{P} = \{p_1, p_2, ...\}$ em ordem crescente. Considere o logaritmo natural $\log x$, definido como $\log x = \int_1^x \frac{1}{t} dt$. Iremos comparar a área abaixo do gráfico de $f(t) = \frac{1}{t}$ com uma função escada superior (para esse método, veja D do apêndice). Assim, para $n \leq x \leq n+1$ nós temos:



Degraus acima da função $f(t) = \frac{1}{t}$

$$\log x \leq 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n-1} + \frac{1}{n} \leq \sum \frac{1}{m}$$

onde a soma se estende para todo natural m que tenha apenas divisores primos $p \leq x$. Uma vez que cada m pode ser escrito de forma única como um produto da forma $\prod_{p \leqslant x} p^{k_p}$, vemos que a última soma é igual a

$$\prod_{p \in \mathbb{P},\ p \leqslant x} \Big(\sum_{k \geq 0} \frac{1}{p^k} \Big).$$

O somatório é uma série geométrica com razão $\frac{1}{p}$, de onde

$$\log x \leq \prod_{p \in \mathbb{P},\ p \leqslant x} \frac{1}{1 - \frac{1}{p}} = \prod_{p \in \mathbb{P},\ p \leqslant x} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

Como $p_k \geq k+1$, temos:

$$\frac{p_k}{p_{k-1}} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k}$$

e portanto

$$\log x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1.$$

Sabemos que $\log x$ não é limitado, daí concluímos que $\pi(x)$ é ilimitado e assim conclui-se que há um número infinito de primos.

□

1.5 Prova 5

Uma outra demonstração de que existem infinitos números primos está relacionada à Topologia - ramo da Matemática no qual são estudadas, com grande generalidade, as noções de limites, de continuidade e as ideias com elas relacionadas. Tal demonstração foi proposta por Frustenberd, matemático israelense, muito respeitado pelos resultados que obteve na teoria de probabilidade e teoria ergódica, que ficou famoso logo no começo da carreira ao publicar, em 1955, quando ele era apenas um aluno de graduação, uma demonstração da infinitude dos primos usando apenas a definição de topologia e algumas propriedades de sequências infinitas de números inteiros. Essa demonstração ficou famosa, pois ela está bem longe das demonstrações rotineiras da área de topologia: trata-se de uma técnica topológica aplicada à teoria dos números! Por isso mesmo é considerada muito estranha e fascinante. Para tal entendimento, é importante conhecermos alguns conceitos e resultados utilizados em tal prova (veja E do apêndice).

Prova: Vamos introduzir uma topologia no conjunto dos números inteiros $\mathbb{Z}$. Para $a, b \in \mathbb{Z}, b > 0$, façamos

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}.$$

Dizemos que um conjunto $O \subseteq \mathbb{Z}$ é *aberto* se O é vazio ou se, para cada $a \in O$, existe algum $b > 0$ com $N_{a,b} \subseteq O$. Claramente a união de conjuntos abertos é também um conjunto aberto. Se O_1, O_2 são abertos e $a \in O_1 \cap O_2$ com $N_{a,b_1} \subseteq O_1$ e $N_{a,b_2} \subseteq O_2$, então $a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. Então concluímos que quaquer intersecção de um número finito de conjuntos abertos é um conjunto aberto. Assim, essa família de conjuntos abertos induz uma topologia em $\mathbb{Z}$. Convém observar dois fatos:

a) Qualquer conjunto aberto não vazio é infinito.

b) Qualquer conjunto $N_{a,b}$ também é fechado.

O primeiro fato decorre da definição. Quanto do segundo, observe que:

$$N_{a,b} = \mathbb{Z} \backslash \bigcup_{i=1}^{b-1} N_{a+i,b}$$

o que prova que $N_{a,b}$ é o complementar de um conjunto aberto e, portanto, fechado. Até agora os números primos não entraram em cena, mas ei-los aqui. Uma vez

que qualquer número $n \neq 1, -1$ tem um divisor primo p e, consequentemente, está contido em $N_{0,p}$, concluímos então que

$$\mathbb{Z}\backslash\{1,-1\} = \bigcup_{p\in\mathbb{P}} N_{0,p}$$

Agora se $\mathbb{P}$ fosse finito, então $\bigcup_{p\in\mathbb{P}} N_{0,p}$ seria uma união finita de conjuntos fechados (por b), e portanto fechado. Consequentemente, $\{-1, 1\}$ seria um conjunto aberto, em contradição com (a). Portanto, $\mathbb{P}$ é infinito.

□

1.6 Prova 6

Nossa prova final dá um considerável passo adiante e demonstra não somente que há infinitos números primos, mas também que a série $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverge. A primeira prova desse resultado importante foi dada por Euler (e é interessante em si mesma), mas nossa prova, concebida por Erdős, é de uma beleza irresistível.

Paul Erdős (1913 - 1996) foi um matemático húngaro. De origem judaica, mas não praticante, era filho único. Filho de pais matemáticos, mostrou desde cedo aptidão para a atividade matemática. Extremamente prolífico e de notável excentricidade, publicou 1475 artigos, alguns de extrema importância, o que é um número superior a qualquer outro matemático na história, trabalhando com centenas de colaboradores. Trabalhou em problemas de análise combinatória, teoria dos grafos, teoria dos números, teoria dos conjuntos, análise matemática e teoria das probabilidades. Aos quatro anos de idade conseguiu descobrir sozinho algumas propriedades dos números primos. Apesar das restrições que existiam na Hungria impedindo os Judeus de entrar na universidade, Erdős conseguiu entrar em 1930. Recebeu o doutoramento em 1934. As contribuições de Erdős para a Matemática são numerosas e variadas. Mas não era um grande teórico; preferia resolver problemas. Acreditava que as sofisticadas teorias matemáticas não podem cobrir toda a matemática, e que há muitos problemas que não podem ser atacados por meio delas, mas que podem ser resolvidos por métodos elementares. Os problemas que mais o atraiam eram problemas de análise combinatória, teoria dos grafos e teoria dos números. Não resolvia problemas de qualquer maneira, queria resolvê-los de uma forma simples e elegante. Para Erdős, a prova tinha que explicar por que o resultado é verdadeiro, e não ser apenas uma sequência de passos sem ajudar a entender o resultado. Profissionalmente, Erdős é mais conhecido pela sua capacidade

de resolver problemas extraordinariamente difíceis. O seu estilo característico consistia em resolver problemas de uma forma elegante e visionária. Recebeu o Prémio Cole da Sociedade Americana de Matemática em 1951 pelos seus muitos artigos em teoria dos números, e em particular pelo artigo "On a new method in elementary number theory which leads to an elementary proof of the prime number theorem", publicado nos Proceedings of the National Academy of Sciences em 1949. Erdős ocupou oficialmente posições em várias universidades de Israel, Estados Unidos e Reino Unido. Essas posições eram apenas formais. Na realidade ele era um nómada sem objetivos definidos, viajando pelas universidades mais prestigiadas. Trabalhava obsessivamente, dormia 4 a 5 horas por dia e tomava anfetaminas para manter a capacidade de trabalho. A dada altura, um amigo desafiou-o a não tomar a droga durante um mês; ele queixou-se mais tarde que durante esse mês a sua produtividade baixara imensamente. Erdős recebeu muitos prêmios, incluindo o Prêmio Wolf de Matemática de 1983. No entanto, devido ao seu estilo de vida, precisava de pouco dinheiro. Por isso ajudou estudantes talentosos e ofereceu prémios pela resolução de problemas propostos por ele . Morreu em Varsóvia, Polónia a 20 de setembro de 1996.

Demonstração: Seja $p_1, p_2, p_3, ...$ a sequência de números primos em ordem crescente e assumiremos que $\sum_{p\in\mathbb{P}} \frac{1}{p}$ converge. Então deve existir um número natural k tal que $\sum_{i>k+1} \frac{1}{p_i} < \frac{1}{2}$. Chamaremos $p_1, ..., p_k$ de *primos pequenos* e $p_{k+1}, p_{k+2}, ...$ de *primos grandes*. Para um natural arbitrário N nós encontraremos a seguinte desigualdade

$$\sum_{i\geq k+1} \frac{N}{p_i} < \frac{N}{2}. \tag{1.1}$$

Seja N_b o número de inteiros positivos $n \leq N$ que são divisíveis por pelo menos um primo grande e N_s o número de inteiros positivos $n \leq N$ que tem somente divisores primos pequenos. Mostremos que para um N adequado, $N_b + N_s < N$, que será nossa contradição, uma vez que, por definição, $N_b + N_s$ teria que ser igual a N. Para estimar N_b note que $\lfloor \frac{N}{p_i} \rfloor$ conta os inteiros positivos $n \leqslant N$ que são múltiplos de p_i. Daí por (1.1) nós obtemos

$$N_b \leq \sum_{i\geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2}. \tag{1.2}$$

Vamos olhar para N_s. Escrevemos cada $n \leq N$ que tem somente divisores primos pequenos da forma $n = a_n b_n^2$, onde a_n é a parte livre de quadrados. Todo a_n é portanto, um produto de diferentes primos pequenos e nós concluímos que há precisamente 2^k diferentes partes livres de quadrados. Além disso, como $b_n \leq \sqrt{n} \leq$

$\sqrt{N}$, descobrimos que são no máximo $\sqrt{N}$ partes quadradas e assim $N_s \leq 2^k\sqrt{N}$. Como (1.2) vale para qualquer N, resta encontrar um número N com $2^k\sqrt{N} \leq \frac{N}{2}$ ou $2^{k+1} \leq \sqrt{N}$, assim $N = 2^{2k+2}$.

□

Capítulo 2

Postulado de Bertrand

Já vimos que a sequência de números primos 2, 3, 5, 7, ... é infinita. Para ver que o tamanho das lacunas entre um primo e outro não é limitado, vamos usar $N := 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p$ para denotar o produto de todos os primos que são menores que $k+2$, e verificar que nenhum dos k números

$$N+2, N+3, N+4, \cdots, N+(k+1)$$

é primo, uma vez que, para $2 \leq i \leq k+1$, sabemos que i tem um fator primo que é menor que $k+2$, e esse fator também divide N e, cosequentemente, também divide $N+i$. Com essa receita, encontramos, por exemplo, para $k = 10$, que nenhum dos dez números

$$2.312, 2.313, 2.314, \ldots, 2.321$$

é primo.
Mas também existem limitantes superiores para as lacunas na sequência de números primos uma famosa estimativa estabelece que "a lacuna até o próximo primo não pode ser maior que o número com o qual iniciamos nossa busca".'Ela é conhecida como *postulado de Betrand*, uma vez que foi conjecturada e verificada empiricamente para $n < 3.000.000$ por Bertrand. Joseph Louis Bertrand (1822-1900) foi um dos mais importantes matemáticos e geômetras da França, com importantes trabalhos publicados em geometria diferencial e teoria das probabilidades. Foi considerado um gênio precoce, pois aos nove anos de idade ele entendeu álgebra e geometria elementar, bem como foi capaz de falar latim fluentemente. Dois anos depois, quando tinha onze anos, ele recebeu permissão para assistir a palestras na Escola Politécnica. Defendeu sua tese de doutorado em termodinâmica com dezessete anos de idade, sendo admitido em seguida como professor da Escola Politécnica. No Collège de France, instituição mais prestigiosa do país, ensinou física e matemática durante quase cinquenta anos. Também lecionou na Escola de Minas e na Escola Normal Superior. Entrou para a história da matemática ao formular e resolver o

chamado "problema de Bertrand" e ao descrever as propriedades daquelas que passaram a ser conhecidas como "curvas de Bertrand". Em 1856 foi eleito membro da Academia de Ciências, tornando-se seu secretário perpétuo a partir de 1874. Em 1884 tornou-se membro também da Academia Francesa no lugar de Jean-Baptiste Dumas. Essas altas posições acadêmicas, combinadas com sua erudição, sua eloquência e seu charme, colocaram-no em uma posição de grande proeminência no cenário francês na segunda metade do século XIX. Reuniu em torno de si um círculo cultural de grande prestígio. Foi membro da Legião de Honra. De 1865 até sua morte, Bertrand editou o "Journal des Savants". Escreveu inúmeros artigos de divulgação e de história da ciência, bem como sobre vida e obra de cientistas como Lavoisier, Comte, D'Alembert, Pascal, entre outros. Bertrand publicou muitos trabalhos sobre geometria diferencial e teoria da probabilidade. Ele escreveu uma série de notas sobre a teoria da probabilidade na redução dos dados de observações. Ele publicou estas notas começando por volta de 1875 e, após uma breve pausa de três anos a partir de 1884, ele começou a publicar notas adicionais em probabilidade. O postulado foi provado pela primeira vez para todo n por Pafnuty Chebyshev em 1850. Uma prova muito mais simples foi dada pelo gênio indiano Ramanujam (veja F do apêndice). Nossa prova se deve a Paul Erdős e foi extraída do primeiro artigo por ele publicado, que apareceu em 1932, quanto tinha 19 anos.

Postulado de Betrand

Para cada $n \geq 1$, existe algum número primo p com $n < p \leq 2n$.

Prova. Vamos fazer uma estimativa do tamanho do coeficiente binomial $\binom{2n}{n}$ de maneira cuidadosa o suficiente para ver que, se ele não tivesse nenhum fator primo no intervalo $n < p \leq 2n$, então ele seria "muito pequeno". Nosso argumento será feito em cinco etapas.

(1) Provemos primeiro o postulado de Bertrand para $n < 4.000$. Para isso, não é preciso checar 4.000 casos: é suficiente (este é o "truque de Landau") checar que

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1.259, 2.503, 4.001$$

é uma sequência de números primos onde cada um é menor que duas vezes o anterior. Em consequência, cada intervalo $\{y : n < y \leq 2n\}$, com $n \leq 4.000$, contém um desses 14 primos.

(2) Em seguida provemos que

$$\prod_{p \leq x} p \leq 4^{x-1} \tag{2.1}$$

para todo real $x \geq 2$, onde nossa notação – aqui e no que segue – é entendida como implicando que o produto é tomado sobre todos os números primos

$p \leq x$. A prova que apresentamos para essa fato não vem do artigo original de Erdős, mas também é dele, e é uma prova digna d'Olivro [1]. Primeiro notamos que, se q é o maior número primo com $q \leq x$, então

$$\prod_{p \leq x} p = \prod_{p \leq q} p \text{ e } 4^{q-1} \leq 4^{x-1}.$$

Assim basta chegar que (2.1) para o caso em que $x = q$ é um número primo. Para $q = 2$, temos "$2 \leq 4$", de forma que nosso procedimento será considerar números primos $q = 2m + 1$. Para esses números, vamos decompor o produto e computar

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \cdot \prod_{m+1 < p < 2m+1} p \leq 4^m \binom{2m+1}{m} \leq 4^m 2^{2m} = 4^{2m}.$$

Todas as partes dessa "computação de uma linha" são fáceis de ver. De fato,

$$\prod_{p \leq m+1} p \leq 4^m$$

pela indução. A desigualdade

$$\prod_{m+1 < p \leq 2m+1} p \leq \binom{2m+1}{m}$$

segue da observação de que $\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$ é um inteiro, onde os primos que consideramos são todos fatores do numerador $(2m+1)!$, mas não do denominador $m!(m+1)!$. Finalmente,

$$\binom{2m+1}{m} \leq 2^{2m}$$

vale, pois

$$\binom{2m+1}{m} \text{ e } \binom{2m+1}{m+1}$$

são duas parcelas (iguais!) que aparecem em

$$\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}.$$

[1] O Livro (em inglês, The Book) refere-se a um livro imaginário no qual Deus teria escrito as mais belas demonstrações de todos teoremas. O conceito foi criado por Paul Erdős que dizia que um matemático poderia não acreditar em Deus, mas teria que acreditar n'O Livro. Depois da morte de Erdős foi publicado o livro Proofs from THE BOOK contendo 32 demonstrações de teoremas de diversas áreas da matemática, sugeridas por Erdős.

(3) Do teorema de Legendre (veja C do apêndice), obtemos que $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ contém o fator primo p exatamente

$$\sum_{k\geq 1}\Big(\Big\lfloor\frac{2n}{p^k}\Big\rfloor - 2\Big\lfloor\frac{n}{p^k}\Big\rfloor\Big)$$

vezes. Aqui, cada parcela é no máximo 1, já que ela satisfaz

$$\Big\lfloor\frac{2n}{p^k}\Big\rfloor - 2\Big\lfloor\frac{n}{p^k}\Big\rfloor < \frac{2n}{p^k} - 2\Big(\frac{n}{p^k} - 1\Big) = 2$$

é inteira. Além disso, as parcelas anulam-se sempre que $p^k > 2n$. Assim, $\binom{2n}{n}$ contém p exatamente

$$\sum_{k\geq 1}\Big(\Big\lfloor\frac{2n}{p^k}\Big\rfloor - 2\Big\lfloor\frac{n}{p^k}\Big\rfloor\Big) \leq max\{r : p^r \leq 2n\}$$

vezes. Daí segue que a maior potência de p que divide $\binom{2n}{n}$ não é maior que $2n$. Em particular, os números primos $p > \sqrt{2n}$ aparecem no máximo uma vez em $\binom{2n}{n}$. Além do mais – e isso, de acordo com Erdős, é o fato-chave para sua prova –, números primos p que satisfazem $\frac{2}{3}n < p \leq n$ não dividem $\binom{2n}{n}$ de forma alguma! De fato, $3p > 2n$ implica (para $n \geq 3$ e, consequentemente, $p \geq 3$) que p e $2p$ são os únicos múltiplos de p que aparecem como fatores no numerador de $\frac{(2n)!}{n!n!}$, ao passo que temos dois p - fatores no denominador.

(4) Agora estamos prontos para estimar $\binom{2n}{n}$. Para $n \geq 3$, usando uma estimativa (veja G do apêndice) para a cota inferior, obtemos

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq \prod_{p\leq\sqrt{2n}} 2n \cdot \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \cdot \prod_{n<p\leq 2n} p$$

e assim, uma vez que não há mais que $\sqrt{2n}$ primos $p \leq \sqrt{2n}$,

$$4^n \leq (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \cdot \prod_{n<p<2n} p \quad \text{para} \quad n \geq 3 \tag{2.2}$$

(5) Vamos assumir agora que não existe primo p com $n < p \leq 2n$, de forma que o segundo produto em (2.2) é 1. Substituindo (2.1) em (2.2) obtemos

$$4^n \leq (2n)^{1+\sqrt{2n}} 4^{\frac{2}{3}n}$$

ou

$$4^{n/3} \leq (2n)^{1+\sqrt{2n}} \tag{2.3}$$

que é falso para n suficientemente grande! De fato, usando $a+1<2^a$ (que vale para todo $a\geq 2$ por indução), obtemos

$$2n=(\sqrt[6]{2n})^6<\left(\left\lfloor\sqrt[6]{2n}\right\rfloor+1\right)^6<2^{6\lfloor\sqrt[6]{2n}\rfloor}\leq 2^{6\sqrt[6]{2n}}, \tag{2.4}$$

e assim, para $n\geq 50$ (e consequentemente $18<2\sqrt{2n}$), obtemos, de (2.3) e (2.4),

$$2^{2n}\leq(2n)^{3(1+\sqrt{2n})}<2^{\sqrt[6]{2n}(18+18\sqrt{2n})}<2^{20\sqrt[6]{2n}\sqrt{2n}}=2^{20(2n)^{2/3}}.$$

Isso implica que $(2n)^{1/3}<20$ e, assim, $n<4.000$. Podemos extrair ainda mais dessa prova: de (2.2), o mesmo tipo de estimativa que acabamos de usar prova que

$$\prod_{n<p\leq 2n} p\geq 2^{\frac{1}{30}n}\quad\text{para}\quad n\geq 4.000$$

e, assim, que existem no mínimo

$$\log_{2n}\left(2^{\frac{1}{30}n}\right)=\frac{1}{30}\frac{n}{\log_2 n+1}>\frac{1}{30}\frac{n}{\log_2 n}$$

primos entre n e $2n$. Até que essa estimativa não é tão má assim: o número "verdadeiro" de primos nesse intervalo é aproximadamente $n/\log n$. Isto decorre do famoso "teorema do número primo", que estabelece que o limite

$$\lim_{n\to\infty}\frac{\#\{p\leq n:\text{p é primo}\}}{n/\log n}$$

existe e é igual a 1. Isso foi provado primeiro por Hadamard e de la Vallée-Poussin em 1986; Selberg e Erdős encontraram uma prova elementar (sem as ferramentas de análise complexa, mas ainda assim longa e intrincada) em 1948. A respeito do teorema do número primo propriamente, parece que a palavra final ainda não foi dada: por exemplo, uma prova da hipótese de Riemann (veja H do apêndice), um dos maiores problemas abertos em matemática, também daria uma melhora substancial nas estimativas do teorema do número primo. Também para o postulado de Bertrand se poderiam esperar aperfeiçoamentos dramáticos. De fato, o seguinte é um problema não resolvido:

Sempre extiste um primo entre n^2 *e* $(n+1)^2$?

Capítulo 3

Coeficientes binomiais (quase) nunca são potências

James Joseph Sylvester (1814-1897) foi um matemático inglês. Contribuiu fundamentalmente no desenvolvimento da teoria matricial, teoria dos invariantes, teoria dos números e análise combinatória. Desempenhou papel fundamental no desenvolvimento da matemática nos Estados Unidos na segunda metade do século XIX, quando professor da Universidade Johns Hopkins e fundador do American Journal of Mathematics. Sylvester frequentou duas escolas em Londres, a primeira sendo um internato em Highgate que ele frequentou até 1827, depois ele realizou um estudo mais aprofundado em 18 meses em uma escola em Islington. Em 1828, com a idade de 14 anos, ele entrou no University College de Londres e começou seus estudos no primeiro ano que o Colégio recebeu alunos. Ele também tinha o ta-lentoso De Morgan como seu professor de matemática. Foi ele quem inventou a palavra totiente, pela qual é reconhecida a Função totiente de Euler, usada em Teoria dos Números e criptografia RSA (veja I do apêndice), a qual foi usada por Leonhard Euler para provar o Pequeno Teorema de Fermat.
Existe um epílogo para o postulado de Bertrand que leva a um belo resultado sobre os coeficientes binomiais. Em 1892, Sylvester reforçou o postulado de Bertrand do seguinte modo:

Se $n \geq 2k$, então no mínimo um dos números $n, n-1, ..., n-k+1$ tem um divisor primo maior do que k.

Note que para $n = 2k$, obtemos precisamente o postulado de Bertrand. Em 1934, Erdős deu uma curta e elementar prova d'O Livro do resultado de Sylvester, na mesma linha de sua prova do postulado de Bertrand. Existe

uma maneira equivalente de enunciar o teorema de Sylvester:

O coeficiente binomial

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \quad (n \geq 2k)$$

sempre tem um fator primo $p > k$.

Com essa observação em mente, vamos nos voltar para uma outra das jóias de Erdős. Quando $\binom{n}{k}$ é igual a uma potência m^l? É fácil ver que exitem infinitas soluções para $k = l = 2$, ou seja, da equação $\binom{n}{2} = m^2$. De fato, se $\binom{n}{2}$ é um quadrado, então $\binom{(2n-1)^2}{2}$ também o é. Para ver isso, faça $n(n-1) = 2m^2$. Segue-se que

$$(2n-1)^2((2n-1)^2-1) = (2n-1)^2 4n(n-1) = 2(2m(2n-1))^2$$

e, consequentemente,

$$\binom{(2n-1)^2}{2} = (2m(2n-1))^2.$$

Começando com $\binom{9}{2} = 6^2$ obtemos assim infinitas soluções – a próxima é $\binom{289}{2} = 204^2$. Convém observar que isso não produz todas as soluções. Por exemplo, $\binom{50}{2} = 35^2$ começa uma outra série, da mesma forma como $\binom{1.682}{2} = 1.189^2$. Para $k = 3$, sabe-se que $\binom{n}{3} = m^2$ tem a solução única $n = 50$, $m = 140$. Mas agora estamos no fim da linha. Para $k \geq 4$ e qualquer $l \geq 2$, não existem soluções, e isso foi o que Erdős provou através de um argumento engenhoso.

Teorema: *A equação $\binom{n}{k} = m^l$* não tem soluções inteiras com $l \geq 2$ e $4 \leq k \leq n-4$.

Prova: Note primeiro que podemos assumir $n \geq 2k$ porque $\binom{n}{k} = \binom{n}{n-k}$. Suponha que o teorema é falso, e que $\binom{n}{k} = m^l$. A prova, por redução ao absurdo, procede nos seguintes quatro passos.

(1) Pelo teorema de Sylvester, existe um fator primo p de $\binom{n}{k}$ maior do que k, de forma que p^l divide $n(n-1)...(n-k+1)$. Claramente, somente um dos fatores $n-i$ pode ser um múltiplo de p (por causa de $p > k$), e concluímos que $p^l | n-i$, e daí

$$n \geq p^l > k^l \geq k^2$$

(2) Considere qualquer fator $n-j$ do numerador e escreva-o na forma $n-j = a_j m_j^l$, onde a_j não é divisível por qualquer l- ésima potência não trivial. Notamos de **(1)** que a_j tem somente divisores primos menores ou iguais a k. Queremos mostrar em seguida que $a_i \neq a_j$ para $i \neq j$. Suponha por absurdo que $a_i = a_j$ para algum $i < j$. Então $m_i \geq m_j + 1$ e

$$\begin{aligned} k &> (n-i)-(n-j) = a_j(m_i^l - m_j^l) \geq a_j((m_j+1)^l - m_j^l \\ &> a_j l m_j^{l-1} \geq l(a_j m_j^l)^{1/2} \geq l(n-k+1)^{1/2} \\ &\geq l(\frac{n}{2}+1)^{1/2} \geq n^{1/2}, \end{aligned}$$

que contradiz $n > k^2$ acima.

(3) A seguir, vamos provar que os a_i são os inteiros $1, 2, ..., k$ em alguma ordem. (De acordo com Erdős, esse é o ponto crucial da prova.) Uma vez que já sabemos que são todos distintos, basta provar que

$$a_0 a_1 \cdots a_{k-1} \text{ divide } k!.$$

Substituindo $n - j = a_j m_j^l$ na equação $\binom{n}{k} = m^l$, obtemos

$$a_0 a_1 \cdots a_{k-1}(m_0 m_1 \cdots m_{k-1})^l = k! m^l.$$

Cancelar os fatores comuns de $m_0 m_1 \cdots m_{k-1}$ e m produz

$$a_0 a_1 \cdots a_{k-1} u^l = k! v^l$$

com $\text{mdc}(u, v) = 1$. Falta mostrar que $v = 1$. Caso contrário, então v contém um divisor primo de p. Uma vez que $\text{mdc}(u, v) = 1$, p deve ser um divisor primo de $a_0 a_1 \cdots a_{k-1}$ e consequentemente é menor que ou igual a k. Pelo teorema de Legendre (veja C do apêndice) nós sabemos que $k!$ contém p elevado a $\sum_{i \geq 1} \left\lfloor \frac{k}{p_i} \right\rfloor$. Vamos agora fazer uma estimativa do expoente de p em $n(n-1)\cdots(n-k+1)$. Seja i um inteiro positivo e sejam $b_1 < b_2 < \ldots b_s$ os múltiplos de p_i entre $n, n-1, \ldots, n-k+1$. Então $b_s = b_1 + (s-1)p^i$ e consequentemente,

$$(s-1)p^i = b_s - b_1 \leq n - (n-k+1) = k-1,$$

o que implica

$$s \leq \left\lfloor \frac{k-1}{p^i} \right\rfloor + 1 \leq \left\lfloor \frac{k}{p^i} \right\rfloor + 1$$

Dessa forma, para cada i, o número de múltiplos de p^i dentre $n, ..., n-k+1$ e, consequentemente, dentre os a_j, é limitado por $\lfloor \frac{k}{p_i} \rfloor + 1$. Isso implica que o expoente de p em $a_0 a_1 \cdots a_{k-1}$ é no máximo

$$\sum_{i=1}^{l-1} \Big(\Big\lfloor \frac{k}{p^i} \Big\rfloor + 1 \Big),$$

com o argumento que usamos para o teorema de Legendre no Cap. 2. A única diferença é que dessa vez a soma pára em $i = l-1$, uma vez que os a_j não contêm potências l-ésimas. Juntando as duas contas, achamos que o expoente de p em v^l é, no máximo,

$$\sum_{i=1}^{l-1} \Big(\Big\lfloor \frac{k}{p^i} \Big\rfloor + 1 \Big) - \sum_{i \geq 1} \Big\lfloor \frac{k}{p^i} \Big\rfloor \leq l-1,$$

e temos nossa desejada contradição, uma vez que v^l é uma l-ésima potência. Isso já é suficiente para decidir o caso $l = 2$. De fato, uma vez que $k \geq 4$, um dos a_i deve ser igual a 4, mas os a_i não contêm quadrados. Dessa forma, vamos agora assumir que $l \geq 3$.

(4) Uma vez que $k \geq 4$, devemos ter $a_{i_1} = 1$, $a_{i_2} = 2$, $a_{i_3} = 4$ para alguns i_1, i_2, i_3, ou seja,

$$\begin{aligned} n - i_1 &= m_1^l, \\ n - i_2 &= 2m_2^l, \\ n - i_3 &= 4m_3^l. \end{aligned}$$

Afirmamos que $(n-i_2)^2 \neq (n-i_1)(n-i_3)$. Caso contrário, faça $b = n - i_2$ e $n - i_1 = b - x$, $n - i_3 = b + y$, onde $0 < |x|, |y| < k$. Daí,

$$b^2 = (b-x)(b+y) \text{ ou } (y-x)b = xy,$$

onde $x = y$ é evidentemente impossível. Agora temos, da parte **(1)**,

$$|xy| = b|y-x| \geq b > n-k > (k-1)^2 \geq |xy|,$$

o que é absurdo. Assim, temos que $m_2^2 \neq m_1 m_3$, onde estamos assumindo $m_2^2 > m_1 m_3$ (sendo o outro caso análogo) e procedemos nossa última cadeia de desigualdades. Obtemos

$$\begin{aligned} 2(k-1)n &> n^2-(n-k+1)^2 > (n-i_2)^2-(n-i_1)(n-i_3) \\ &= 4[m_2^{2l}-(m_1m_3)^l] \geq 4[(m_1m_3+1)^l-(m_1m_3)^l] \\ &\geq 4lm_1^{l-1}m_3^{l-1}. \end{aligned}$$

Uma vez que $l \geq 3$ e $n > k^l \geq k^3 > 6k$, resulta

$$\begin{aligned} 2(k-1)nm_1m_3 &> 4lm_1^lm_3^l = l(n-I_1)(n-i_3) \\ &> l(n-k+1)^2 > 3(n-\frac{n}{6})^2 > 2n^2. \end{aligned}$$

Agora, uma vez que $m_i \leq n^{1/l} \leq n^{1/3}$, fnalmente obtemos que

$$kn^{2/3} \geq km_1m_3 > (k-1)m_1m_3 > n,$$

ou $k^3 > n$. Com essa contradição, a prova está completa.

Apêndice A

Primos em certas progressões aritméticas

Os números primos sempre encantaram os matemáticos de todos os tempos. Sempre se buscou saber como esses números estavam distribuídos, quantos números primos existiam entre 1 e um número real x qualquer, fórmulas que gerassem números que fossem primos, e etc.
Mesmo quando um número natural a não divide o número natural b, Euclides, nos seus elementos, utiliza sem enunciá-lo explicitamente, o fato de que é sempre possível efetuar a divisão de b por a, com o resto. Este resultado é um importante instrumento na obra de Euclides e conhecido pelo algoritmo da divisão de Euclides. Empossados desse algoritmo, vamos fazer algumas observações relacionadas às várias maneiras que os números primos podem ser escritos. Sabemos pelo algoritmo da divisão que todo inteiro pode ser escrito da seguinte maneira:

$$4n, 4n+1, 4n+2, 4n+3.$$

É claro que $4n$ e $4n+2$ são sempre números pares. Então, os números inteiros primos estão em duas progressões:

a) $4n+1$
$1, 5, 9, 13, 17, 21, ...$

b) $4n+3$
$3, 7, 15, 19, 23, 27, 31...$

Como podemos ver, as progressões contêm números primos. Um questão que surge é:

Quantos números primos existem em tais progressões?

Para responder tal pergunta, faremos uma demonstração utilizando um raciocínio análogo ao de Euclides usado para demonstrar que há infinitos números primos. Mostraremos primeiro, que o produto de dois ou mais inteiros da forma $4n+1$ é da mesma forma. Para isso, considere $a = 4n+1$ e $b = 4m+1$, tendo em vista que é suficiente considerar o produto apenas para dois inteiros. Multiplicando-os, temos:

$$a \times b = (4n+1) \times (4m+1) = 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1.$$

Como queríamos demonstrar. Mostremos agora que existem infinitos números primos da forma $4n+3$ e, em particular, que existem infinitos números primos.

Teorema: Existem infinitos números primos da forma $4n+3$.

Demonstração: Suponha, por contradição, que existem finitos números primos da forma $4n+3$. São eles: $p_1, p_2, p_3, ..., p_r$. Considere N tal que:

$$N = 4p_1p_2p_3...p_r - 1 = 4p_1p_2p_3...p_r - 1 - 4 + 4 = 4(p_1p_2p_3...p_r - 1) + 3$$

Sendo $N = r_1r_2r_3...r_t$ sua fatoração em números primos. Como N é primo, temos que $r_k \neq 2, \forall k$, então cada r_k é da forma $4n+1$ ou $4n+3$. Já vimos anteiromente que o produto de dois números inteiros da forma $4n+1$ é da mesma forma, como N é da forma $4n+3$, temos que algum r_k é da forma $4n+3$, mas r_k não pode ser igual a algum dos $p_1, p_2, ..., p_r$, caso contrário $r_k \mid 1$, o que é um absurdo.

Portanto, existe infinitos números primos da forma $4n+3$.

□

Gauss conjecturou que dados dois números naturais coprimos (que possuem o máximo divisor igual a 1) a e b, existem infinitos primos da forma $an+b$. Essa conjectura foi demonstrada em 1837, por Johann Dirichlet (1805 - 1859), um matemático alemão, a quem se atribui a moderna definição formal de função. O teroema de Dirichlet sobre progressões aritméticas é um resultado da teoria analítica dos números. A demonstração do teorema é muita complexa e não será apresentada aqui, pois utiliza de certas funções multiplicativas (conhecidas como funções L de Dirichlet) e vários resultados sobre aritmética de números complexos.

Apêndice B

Euler, um Gigante da Matemática

Leonhard Euler, nasceu em 15 de abril de 1707, e morreu em 18 de setembro de 1783. Foi o matemático mais prolífico na história. Os 866 livros e artigos dele representam, aproximadamente, um terço do corpo inteiro de pesquisa em matemática, teorias físicas, e engenharia mecânica publicadas entre 1726 e 1800. Nasceu na Suíça, perto da cidade de Basiléia. Seu pai, um pastor, queria que o filho seguisse os passos dele e o enviou para a Universidade da Basiléia, onde foi aluno de Johann Bernoulli, com quem teve a sua verdadeira iniciação à matemática.
Um de seus primeiros grandes sucessos em matemática foi calcular, em 1735, o valor exato da soma infinita

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots$$

Euler teve grandes contribuições na Teoria dos Números. Demonstrou o "Pequeno Teorema de Fermat" utilizando indução matemática e recursos elementares. Euler escreveu sobre os mais variados assuntos, tais como, teoria das funções, cálculo diferencial e integral, números complexos, acústica, música, teoria dos números, teoria das partições e mecânica, entre muitos outros, ocupando, indiscutivelmente, um lugar entre os maiores matemáticos de todos os tempos. Na teoria dos números, a sua demonstração que há infinitos números primos mostra, também, uma prova que a série $\sum_{p \in \mathbb{P}} \frac{1}{p}$ diverge.

Apêndice C

Legendre

Legendre (1752-1833) nasceu em Paris. Teve uma educação de qualidade superior no Collége Mazarim em Paris, elaborando sua tese em física e matemática em 1770. Muitas de suas obras foram completada por outros, como por exemplo, seu trabalho sobre raízes polinomiais que, inspirou a teoria de Galois. Na teoria dos números, Legendre proporcionou uma demonstração do Último Teorema de Fermat para o expoente $n = 5$, o que foi comprovado por Dirichlet em 1828. Ainda na teoria dos números, conjecturou a lei da reciprocidade quadrática, utilizando como notação o conhecido símbolo de Legendre:

$$\left(\frac{p}{q}\right) = \pm 1$$

se o inteiro p co-primo com q seja (no caso positivo) ou não (no caso negativo) o resto da congruência $x^2 \equiv p \ (\mathrm{mod} p)$. Legendre também estabeleceu uma conjectura sobre a distribuição dos números primos e demonstrou que não existe função algébrica racional que fornece sempre números primos.

Teorema de Legendre: *O número n! contém o fator primo p exatamente* $\sum_{k\geq 2} \left\lfloor \frac{n}{p^k} \right\rfloor$ *vezes* .

Demonstração: Exatamente $\left\lfloor \frac{n}{p} \right\rfloor$ dos fatores de $n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot n$ são divisíveis por p, o que fornece $\left\lfloor \frac{n}{p} \right\rfloor$ fatores p. Em seguida, $\left\lfloor \frac{n}{p^2} \right\rfloor$ dos fatores de $n!$ são divisíveis por p^2, o que nos dá os seguintes $\left\lfloor \frac{n}{p^2} \right\rfloor$ fatores primos p e $n!$, etc.

□

Exemplos como

$$\begin{aligned}\binom{26}{13} &= 2^3.5^2.7.17.19.23\\ \binom{28}{14} &= 2^3.3^3.5^2.17.19.23\\ \binom{30}{15} &= 2^4.3^2.5.17.19.23.29\end{aligned}$$

ilustram que fatores primos "muito pequenos" $p < \sqrt{2n}$ podem aparecer com expoentes mais altos em $\binom{2n}{n}$, primos "pequenos" com $\sqrt{2n} < p \leq \frac{2}{3}n$ aparecem no máximo uma vez, ao passo que fatores $\frac{2}{3}n < p \leq n$ não aparecem de todo.

C.1 Teorema de Lagrange

Grupos e subgrupos

Definição 1: Um sistema matemático constiuído de um conjunto não vazio G e uma operação $(x, y) \mapsto x * y$ sobre G é chamado *grupo* se essa operação se sujeita aos seguintes axiomas:

- *Associatividade*

  $(a * b) * c = a * (b * c)$, quaisquer que sejam $a, b, c \in G$;

- *Existência de elemento neutro*

  Existe um elemento $e \in G$ tal que $a * e = e * a = a$ qualquer que seja $a \in G$;

- *Existência de simétricos*

  Para todo $a \in G$ existe algum elemento $a' \in G$ tal que $a * a' = a' * a = e$.

  Se, além disso, ainda se cumprir o axioma da

- **Comutatividade**

  $a * b = b * a$ quaisquer que sejam $a, b \in G$,

  o grupo recebe o nome de *grupo comutativo ou abeliano.*

Exemplos:

1. *Grupo aditivo dos inteiros (comutativo)*

   Sistema formado pelo conjunto dos inteiros e a adição usual sobre esse conjunto. Motivo: a adição usual é um operação sobre $\mathbb{Z}$, associativa e comutativa. Mais: há um elemnto neutro para ela (o número 0), e o oposto $-a$ de um elemento $a \in \mathbb{Z}$ também pertencente a esse conjunto.

2. *Grupo aditivo dos racionais (comutativo)*

   Sistema formado por $\mathbb{Q}$ e a adição usual sobre esse conjunto. O porquê é o mesmo do exemplo anterior.

3. *Grupo aditivo dos reais (comutativo)*

   Sistema formado por $\mathbb{R}$ e a adição usual sobre esse conjunto. O porquê é o mesmo do primeiro exemplo.

Definição 2: Seja $(G, *)$ um grupo. Diz-se que um subconjunto não vazio $H \subset G$ é um *subgrupo* de G se:

- H é fechado para a operação $*(isto, se$ a, b $\in H$ então $a * b \in H$;
- $(H, *)$ também é um grupo (aqui o símbolo $*$ indica a restrição da operação do G aos elementos de H).

Se e indica o elemento neutro de G, então obviamente $\{e\}$ é um subgrupo de G. É imediato, também, que o próprio G é um subgrupo de si mesmo. Esses dois subgrupos, ou seja, $\{e\}$ e G, são chamados *subgrupos triviais* de G.

Exemplos:

- os subgrupos de $\mathbb{Z}$ são os conjuntos $n\mathbb{Z}$ dos múltiplos de n, para cada $n \in \mathbb{Z}$.
- $(\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Q}, +)$.

Teorema de Lagrange: Se G é um grupo (multiplicativo) finito e U é um subgrupo, então $|U|$ divide $|G|$.

Demonstração: Considere a relação binária $a \sim b :\Leftrightarrow ba^{-1} \in U$. Segue-se, dos axiomas de grupo, que $\sim$ é uma relação de equivalência. A classe de equivalência

contendo um elemento a é precisamente a classe lateral $Ua = \{xa : x \in U\}$. Uma vez que claramente $|Ua| = |U|$, temos que $|G|$ se decompõe em classes de equivalência, todas de tamanho $|U|$ e, consequentemente, $|U|$ divide $|G|$.

□

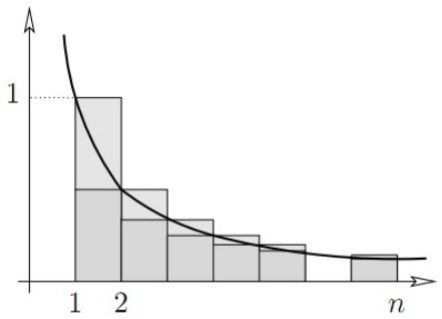
Apêndice D

Estimativa via integrais

Existe um método do tipo "simples-mas-efetivo" para estimar somas por meio de integrais (como vimos anteriormente). Para estimar os *números harmônicos*

$$H_n = \sum_{k-1}^{n} \frac{1}{k}$$

desenhamos a figura abaixo



e dela derivamos que

$$H_n - 1 = \sum_{k=2}^{n} \frac{1}{k} < \int_1^n \frac{1}{t} dt = \log n$$

pela comparação da área abaixo do gráfico de $f(t) = \frac{1}{t}$ $(1 \leq t \leq n)$ com a área dos retângulos sombreados, e

$$H_n - \frac{1}{n} = \sum_{k=1}^{n-1} \frac{1}{t} dt = \log n$$

comaprando com a área dos retângulos grandes (incluindo as partes fracamente sombreadas). Tomadas conjuntamente, isso resulta em

$$\log n + \frac{1}{n} < H_n < \log n + 1.$$

Em particular, $\lim_{n\to\infty} H_n \to \infty$, e a ordem de crescimento de H_n é dada por $\lim_{n\to\infty} \frac{H_n}{\log n} = 1$. Porém, estimativas muito melhores são conhecidas tais como

$$H_n = \log n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} + O\Big(\frac{1}{n^6}\Big),$$

onde $\gamma \approx 0,5772$ é a "constante de Euler".

Observação: Aqui $O\Big(\frac{1}{n^6}\Big)$ denota uma função $f(n)$ tal que $f(n) \leq c\frac{1}{n^6}$ verifica-se para alguma constante c.

D.1 Estimativas para fatoriais - fórmula de Stirling

O mesmo método aplicado a

$$\log(n!) = \log 2 + \log 3 + \cdots + \log n = \sum_{k=2}^{n} \log k$$

fornece

$$\log((n-1)!) < \int_1^n \log t dt < \log(n!)$$

onde a integral é facilmente calculada:

$$\int_1^n \log t dt = [t\log t - t]_1^n = n\log n - n + 1$$

Assim, obtemos uma cota inferior para $n!$

$$n! > e^{n\log n - n + 1} = e\Big(\frac{n}{e}\Big)^n$$

e ao mesmo tempo uma cota superior

$$n! = n(n-1)! < ne^{n\log n - n + 1} = en\Big(\frac{n}{e}\Big)^n$$

Nesse ponto, uma análise mais cuidadosa é necessária para se obter um aproximação assintótica para $n!$, conforme dada pela *fórmula de Stirling*

$$n! \sim \sqrt{2\pi n}\Big(\frac{n}{e}\Big)^n.$$

E, novamente, existem versões mais precisas disponíveis, tais como

$$n! \sim \sqrt{2\pi n}\Big(\frac{n}{e}\Big)^n\Big(1+\frac{1}{12n}+\frac{1}{288n^2}-\frac{139}{5140n^3}+O\Big(\frac{1}{n^4}\Big)\Big).$$

Observação: Aqui, estamos usando $f(n) \sim g(n)$ para significar que $\lim_{n\to\infty}\dfrac{f(n)}{g(n)} = 1$.

Apêndice E

Topologia

Definição: Se E é um conjunto, uma *topologia* em E é um conjunto $\mathcal{T} \subset \mathcal{P}(\mathsf{E})$ tal que

1. $\emptyset, \mathsf{E} \in \mathcal{T}$;
2. se $(\mathsf{A}_j)_{j\in\mathsf{J}}$ for uma família de elementos de $\mathcal{T}$, então $\bigcup_{j\in\mathsf{J}} \mathsf{A}_j \in \mathcal{T}$;
3. se $(\mathsf{A}_j)_{j\in\mathsf{J}}$ for uma família de elementos de $\mathcal{T}$ e se J for finito, então $\bigcap_{j\in\mathsf{J}} \mathsf{A}_j \in \mathcal{T}$.

Um *espaço topológico* é um par ordenado $(\mathsf{E}, \mathcal{T})$, sendo E um conjunto e $\mathcal{T}$ uma topologia em E.

Definição: Seja $(\mathsf{E}, \mathcal{T})$ um espaço topológico e seja $\mathsf{X} \subset \mathsf{E}$. Diz-se que X é *aberto* se $\mathsf{X} \in \mathsf{E}$; diz-se que X é *fechado* se $\mathsf{X}^{\complement} \in \mathcal{T}$.

Dado um conjunto X e uma topologia $\mathcal{T}$ sobre X, dizemos que todo $\mathsf{U} \in \mathcal{T}$ é um aberto de X. Tendo isso em mente, podemos dizer também que um espaço topológico é um conjunto X junto a uma coleção de abertos de X, onde $\emptyset$ e X são abertos, qualquer união de abertos é aberto, e intersecções finitas de abertos são abertos.

Exemplos:

1: Topologia Discreta

Seja X um conjunto qualquer. A coleção $\mathcal{T} = \mathcal{P}(\mathsf{X})$ de todos os subconjuntos de X é uma topologia sobre X, conhecida como *topologia discreta*. Qualquer subconjunto de X é aberto na Topologia Discreta.

2: Topologia Caótica

Seja X um conjunto qualquer. A coleção $\mathcal{T} = \{\emptyset, \mathsf{X}\}$ é uma topologia sobre X, conhecida como *topologia caótica*.
Os conjuntos $\emptyset$ e X são os únicos aberto de X na topologia caótica.

3: Topologia do Complemento Finito

Chamamos de *topologia do complemento finito*, a topologia em que todos subconjuntos $\mathsf{U} \subset \mathsf{X}$ tais que, $\mathsf{X} \setminus \mathsf{U}$ ou é vazio ou é finito.

4: Seja $\mathsf{X} = \{a, b, c, d\}$

$\mathcal{T} = \mathcal{P}(\mathsf{X})$ é a topologia discreta sobre X.
$\mathcal{T} = \{\emptyset, \mathsf{X}\}$ é a topologia caótica sobre X.
$\mathcal{T} = \{\emptyset, \{a\}, \{b\}, \{a, b\}, \mathsf{X}\}$ é uma topologia sobre X.
$\mathcal{T} = \{\emptyset, \{a, b\}, \{c, d\}, \mathsf{X}\}$ é uma topologia sobre X.
$\mathcal{T} = \{\emptyset, \{a\}, \{b\}, \{a, b\}, \{c, d\}, \mathsf{X}\}$ **não é** uma topologia sobre X.
$\mathcal{T} = \{\emptyset, \{a\}, \{b\}, \{a, b\}, \{c, d\}, \{a, c, d\}, \{b, c, d\}, \mathsf{X}\}$ é uma topologia sobre X.

Há também a possibilidade de compararmos duas topologias sobre um mesmo conjunto X. Dizemos que $\mathcal{T}'$ é mais fina que $\mathcal{T}$, se $\mathcal{T}$ e $\mathcal{T}'$ são duas topologias sobre X, e $\mathcal{T}' \supset \mathcal{T}$. A grosso modo, comparamos dizendo que uma tem mais aberos que a outra.

Apêndice F

Demonstração do Postulado de Bertrand via Ramanujan

Srinivasa Ramanujan (1887 - 1920) foi um matemático indiano. Nasceu em Erode, pequena localidade da Índia. Aos cinco anos vai para a escola e impressiona todos por sua excepcional inteligência, parece já saber tudo o que é ensinado. Ganha uma bolsa para o Liceu de Kumbakonam, onde desperta admiração nos colegas e mestres. Na adolescência começou a estudar sozinho séries aritméticas e séries geométricas e com 15 anos pôde achar soluções de polinômios de terceiro e quarto grau. Nessa idade, seus colegas conseguiram que a biblioteca lhe emprestasse um livro que foi essencial ao seu desenvolvimento e brilhantismo matemático. Tratava-se de "Synopsis of Elementary Results on Pure Mathematics", obra do autor George Shoobridge Carr (professor da Universidade de Cambridge). O livro apresentava cerca de 6.000 teoremas e fórmulas com poucas demonstrações, o que influenciou a maneira de Ramanujan interpretar a matemática. Demonstrou todas as fórmulas e teoremas, esgotou a geometria, passou a se dedicar à álgebra. Com 17 anos, Ramanujan estudou a série harmónica, $S(\frac{1}{n})$, e calculou a constante de Euler, gamma, até 15 casas decimais. Começou depois a estudar os números de Bernoulli onde fez descobertas importantes. Ramanujam vivia somente para a matemática e parecia não se interessar por outros assuntos, pouco se preocupava com artes e com literatura. Era atraído pelo extraordinário. Em Cambridge criara uma pequena biblioteca com informações sobre fenômenos que desafiavam a razão. Em suas descobertas havia os mais abstratos enigmas a respeito das noções de números, em especial sobre os números primos. Ramanujan continuou a desenvolver as suas ideias e começou a apresentar e a resolver problemas no Jornal da Sociedade Indiana de Matemática. Após a publicação de um brilhante trabalho sobre os números de Bernoulli, Ramanujan conquistou algum reconhecimento. No ano de 1911, pediu ao fundador da Sociedade Indiana de Matemática para lhe aconselhar um possível emprego, tendo no entanto conseguido apenas um posto temporário no Gabinete Geral de Contabili-

dade em Madras. Ramanujan escreveu cartas a Hardy em 1913 contendo resultados fascinantes. Ramanujan resolveu as séries de Riemann, integrais, séries hipergeométricas e equações funcionais da função zeta. Como tinha apenas uma vaga ideia do que é uma demonstração matemática, apesar de muitos resultados brilhantes, alguns dos seus teoremas estavam completamente errados. Tendo sido aquele que mais colaborou com Ramanujan, Hardy tinha uma grande admiração pelo seu talento. Tentou sempre compreender os resultados por ele apresentados, mesmo os mais incompreensíveis. A sua obra está sobretudo ligada à teoria dos números, uma área que tem na sua origem a resolução de problemas com uma formulação relativamente simples. Ramanujan descobriu resultados de Gauss, Kummer e de outros nas séries hipergeométricas. O trabalho sobre as somas parciais e o produto de séries hipergeométricas levaram a grandes desenvolvimentos posteriores. O seu trabalho mais famoso foi porém sobre o número $p(n)$ que significa o número de modos de decompor um inteiro n em somas. A seguir será dada uma demonstração ao postulado de Betrand proposta por Ramanujan em 1919.

Demonstração:

(1) Seja x um número natural maior que 1. Vamos denotar $v(x)$ a soma dos logaritmos de todos os números primos (p) que não excedem x, ou seja:

$$v(x) = \sum_{p \leq x} \log p$$

Vamos considerar as seguintes expressões:

$$\psi(x) = v(x) + v(x^{\frac{1}{2}}) + v(x^{\frac{1}{3}}) + \cdots \tag{F.1}$$

$$\log[x]! = \psi(x) + \psi(\frac{1}{2}x) + \psi(\frac{1}{3}x) + \cdots \tag{F.2}$$

onde $[x]$ denota, como de costume, o maior inteiro em x.
Por F.1 temos:

$$\psi(x) - 2\psi(\sqrt{x}) = v(x) - v(x^{\frac{1}{2}}) + v(x^{\frac{1}{3}}) - \cdots \tag{F.3}$$

e por F.2

$$\log[x]! - 2\log[\frac{1}{2}x]! = \psi(x) - \psi(\frac{1}{2}x) + \psi(\frac{1}{3}x) - \cdots \tag{F.4}$$

Agora lembrando que um $v(x)$ e $\psi(x)$ são funções crescentes, encontramos a partir de F.3 e F.4 que

$$\psi(x) - 2\psi(\sqrt{x}) \leq v(x) \leq \psi(x) \tag{F.5}$$

e

$$\psi(x) - \psi(\frac{1}{2}x) \leq \log[x]! - 2\log[\frac{1}{2}x]! \leq \psi(x) - \psi(\frac{1}{2}x) + \psi(\frac{1}{3}x) \tag{F.6}$$

mas é fácil ver que

$$\log\Gamma(x) - 2\log\Gamma(\frac{1}{2}x + \frac{1}{2}) \leq \log[x]! - 2\log[\frac{1}{2}x]! \leq \log\Gamma(x+1) - 2\log\Gamma(\frac{1}{2} + \frac{1}{3}) \tag{F.7}$$

Agora, usando a aproximação de Stirling deduzimos a partir de F.7 que

$$\log[x]! - 2\log[\frac{1}{2}x]! < \frac{3}{4}x, x > 0; \tag{F.8}$$

e

$$\log[x]! - 2\log[\frac{1}{2}x]! > \frac{2}{3}x, x > 300 \tag{F.9}$$

De F.6, F.8 e F.9 temos que:

$$\psi(x) - \psi(\frac{1}{2}x) < \frac{3}{4}, x > 0; \tag{F.10}$$

e

$$\psi(x) - \psi(\frac{1}{2}x) + \psi(\frac{1}{3}x) > \frac{2}{3}, x > 300; \tag{F.11}$$

Agora arriscando x para $\frac{1}{2}x, \frac{1}{4}x, \frac{1}{8}x, ...$ em F.10 e somando-se todos os resultados, obtemos

$$\psi(x) < \frac{3}{2}x, x > 0 \tag{F.12}$$

novamente, temos:

$$\psi(x) - \psi(\frac{1}{2}x + \psi(\frac{1}{3}x \leq v(x) + 2\psi(\sqrt{x}) - v(\frac{1}{2} + \psi(\frac{1}{3}x) < v(x) - v(\frac{1}{2}x) + \frac{1}{2}x + 3\sqrt{x} \tag{F.13}$$

em virtude de F.5 e F.12.
Resulta de F.11 e F.13 que

$$v(x) - v(\frac{1}{2}x) > \frac{1}{6}x - 3\sqrt{x}, x > 300 \tag{F.14}$$

Mas é óbvio que $\frac{1}{6}x - 3\sqrt{x}, x \geq 324$.
Portanto, temos

$$v(2x) - v(x) > 0, x \geq 162 \tag{F.15}$$

Em outras palavras, existe, pelo menos, um primo entre x e $2x$ se $x \geq 162$. Assim, o postulado de Bertrand é provado por todos os valores de x não inferior a 162, e, por verificação direta, vemos que ela é verdadeira para valores menores.

(2) Denotemos $\pi(x)$ o número de primos que não excede x. Em seguida, uma vez que $\pi(x) - \pi(\frac{1}{2}x)$ é o número de números primos entre x e $\frac{1}{2}x$, e $v(x) - v(\frac{1}{2}x)$ é a soma dos logaritmos dos primos entre x e $\frac{1}{2}x$, é óbvio que:

$$v(x) - v(\frac{1}{2}x) \leq \{\pi(x) - \pi(\frac{1}{2}x)\} \log x, \tag{F.16}$$

para tdos os valores de x. Resulta de F.14 e F.16 que

$$\pi(x) - \pi(\frac{1}{2}x) > \frac{1}{\log x}\frac{1}{6}x - 3\sqrt{x}, x > 300. \tag{F.17}$$

A partir disso, facilmente deduzimos que

$$\pi(x) - \pi(\frac{1}{2}x) \geq 1, 2, 3, 4, 5, ..., x \geq 2, 11, 17, 29, 41, ... \tag{F.18}$$

respectivamente.

□

Apêndice G

Estimativas para coeficientes binomiais

A partir da definição dos coeficientes binomiais $\binom{n}{k}$ como o número de k-suconjuntos de um n-conjunto, sabemos que a sequência $\binom{n}{0}, \binom{n}{1}, ..., \binom{n}{n}$ de coeficiente binomiais:

1. tem soma igual a $\sum_{k=0}^{n} \binom{n}{k} = 2^n$;
2. é simétrica, $\binom{n}{k} = \binom{n}{n-k}$.

Da equação funcional $\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$ pode-se encontrar facilmente que, para cada n, os coeficientes binomiais $\binom{n}{k}$ formam uma sequência que é simétrica e *unimodal*: ela cresce na direção do meio, de forma que os coeficientes binomiais do meio são os maiores da sequência:

$$1 = \binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil} > \cdots > \binom{n}{n-1} > \binom{n}{n} = 1$$

Aqui, $\lfloor x \rfloor$(respectivamente, $\lceil x \rceil$) denota o número x arredondado para baixo (respectivamente, arredondado para cima) para o inteiro mais próximo.
Das fórmulas assindóticas para fatoriais mencionadas no apêndice, podem-se obter estimativas muito precisas para os tamanhos dos coeficientes binomiais. Contudo precisaremos somente de estimativas muito fracas e simples neste trabalho, tais como: $\binom{n}{k} \leq 2^n$, para todo k, enquanto para $n \geq 2$ temos

$$\binom{n}{\lfloor n/2 \rfloor} \geq \frac{2^n}{n}$$

com a igualdade valendo somente para $n = 2$. Em particular, para $n \geq 1$,

$$\binom{2n}{n} \geq \frac{4^n}{2n}$$

Isso vale uma vez que $\binom{n}{\lfloor n/2 \rfloor}$, um coeficiente binomial do meio, é o maior termo na sequência $\binom{n}{0} + \binom{n}{n}, \binom{n}{1}, \binom{n}{2}, ..., \binom{n}{n-1}$, cuja soma 2^n e cuja média é, portanto, $\frac{2^n}{n}$. Por outro lado, repare na cota superior para coeficientes binomiais

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \leq \frac{n^k}{k!} \leq \frac{n^k}{2^k - 1},$$

que é uma estimativa razoavelmente boa para os coeficientes binomiais "pequenos" nas pontas da sequência, quando n é grande (comparado com k).

Apêndice H

A função zeta de Riemann

A *função zeta de Riemann* $\zeta(s)$ é definida para $s > 1$ real por

$$\zeta(s) := \sum_{n \geq 1} \frac{1}{n^s}.$$

Nossas estimativas para H_n (v. página 25) implicam que a série para $\zeta(1)$ diverge, mas ela converge para qualquer real $s > 1$. A função zeta tem uma continuação canônica no plano complexo inteiro (com um pólo simples em $s = 1$), que pode ser construída usando-se expansão em série de potências. A função complexa restante é da maior importância para a teoria dos números primos. Mencionemos aqui três condições diversas:

(1) A nótavel identidade devida a Euler

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}$$

é uma consequência simples da expansão em série geométrica

$$\frac{1}{1 - p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots$$

(2) O lugar dos zeros complexos da função zeta é o assunto da "hipótese de Riemann": uma das mais famosas e importantes conjecturas não-resolvidas em toda a matemática. Ela afirma que todos os zeros não- triviais $s \in \mathbb{C}$ da função zeta satisfazem

$$Re(s) = \frac{1}{2}.$$

(A função zeta se anula em todos os inteiros negativos pares, os quais são referidos como "zeros triviais".)

Recentemente, Jeff Lagarias mostrou que, surpreendentemente, a hipótese de Riemann equivale à seguinte assertiva elementar: para todo $n \geq 1$,

$$\sum_{d|n} \leq H_n + \exp(H_n)\log(H_n),$$

em que, novamente, H_n é o n-ésimo número harmônico, com igualdade apenas para $n = 1$.

(3) Sabe-se há muito que $\zeta(s)$ é um múltiplo racional de π^s e, portanto, irracional, se s é um inteiro *par* $s \geq 2$. Entretanto, calcular os valores da função ζ para algum valor $s > 1$ é uma tarefa bastante complicada. Euler, em 1735, usando a série de Maclaurin, mostrou que $\zeta(2) = \dfrac{\pi^2}{6}$. Em contraste, a irracionalidade de $\zeta(3)$ foi provada por Róger Apéry somente em 1979.
Apesar de esforços consideráveis, o quadro para $\zeta(s)$ é bastante incompleto quanto aos outros valores ímpares, $s = 2t+1 \geq 5$. A última notícia matemática sobre isso, um artigo de Rivoal, implica que infinitos valores $\zeta(2t + 1)$ são irracionais.

Apêndice I

Criptografia

A criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet. A primeira vista ela até pode parecer complicada, mas para usufruir dos benefícios que proporciona você não precisa estudá-la profundamente e nem ser nenhum matemático experiente. Atualmente, a criptografia já está integrada ou pode ser facilmente adicionada à grande maioria dos sistemas operacionais e aplicativos e para usá-la, muitas vezes, basta a realização de algumas configurações ou cliques de mouse.
Por meio do uso da criptografia você pode:

- proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda;
- criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- proteger seus backups contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- proteger as comunicações realizadas pela Internet, como os e-mails enviados/recebidos e as transações bancárias e comerciais realizadas.

Encaminhar uma mensagem de forma segura é uma preocupação que remonta aos primeiros estrategistas que se têm notícia, na Grécia Antiga. Um exemplo de criptografia foi usado por Júlio César, que foi um grande Imperador de Roma. A chave utilizada por Júlio César era muito simples: desloca-se o alfabeto três letras e troca-as entre si.
Dos métodos criptográficos de chave pública, o RSA (criado em 1978 por de Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman) é o método mais conhecido e, atualmente, o mais usado, sobre todo em aplicações comerciais. Apesar de ser um método de

chave pública, o RSA permite que qualquer usuário codifique mensagens, mas como a chave de decodificação é secreta, só o destinatário legítimo poderá decodificá-la. Para gerar as chaves para o algoritmo RSA, utlizamos o seguinte procedimento:

1. Escolhe-se dois números primos grandes e distintos p e q;
2. Calcula $n = p.q$, onde n será usado como módulo para ambas às chaves públicas e privadas;
3. Calcula $\phi(n) = (p-1).(q-1)$, onde $\phi(n)$ é a função de Euler;
4. Escolha um inteiro e, tal que $1 < e < \phi(n)$ e $m.d.c(e, \phi(n)) = 1$, isto é, e e ϕ são coprimos;
5. Determinar d que é o inverso multiplicatio de e módulo n, ou seja, $d.e \equiv 1(\text{mod}\phi(n))$.

Desta forma geramos o par (n, e) que é a **chave pública do sistema RSA**, e o par (n, d) é a **chave privada do sistema RSA**. Para exemplificar, será escolhido números primos pequenos.

1. Seja $p = 5$ e $q = 7$.
2. Logo, $n = 5.7 = 35$.
3. $\phi(n) = (p-1).(q-1) = (5-1).(7-1) = 4.6 = 24$.
4. $mdc(e, 24) = 1$, observe que 1, 2, 3, 4, 6, 8, 12 e 24 são divisores de 24, para facilitar os cálculos, tomamos o menor valor que não divide 24, ou seja, o menor primo com 24, então $e = 5$.
5. Para determinar d, temos que $d.5 \equiv 1(\text{mod } 24)$, donde concluímos que $d = 5$.

Após os cálculos, temos que o par (35, 5) é a chave pública e também a chave privada.
Para codificar uma mensagem usando o algoritmo RSA,primeiramente devemos converter a mensagem em uma sequência de números. Depois quebrar a mensagem em blocos. Esses blocos devem ser números menores que n. A maneira de escolher os blocos não é única, mas é importante evitar duas situações:

- Nenhum bloco deve começar com o número zero (problemas na decodificação);
- Os blocos não devem corresponder a nenhuma linguística (palavra, letra, etc.)

Assim a decodificação fica impossível.
Para entender tal processo, façamos a codificação da palavra PRIMOS. Para isso considere a tabela abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Utilizando a tabela acima, podemos escrever a palavra PRIMOS como a sequência de números:

$$252718222428$$

Como $n = 21$, podemos dividir a palavra em blocos, de tal forma que cada bloco não exceda n, logo

$$25 - 27 - 18 - 22 - 24 - 28$$

Para codificar, utilizamos a seguinte fórmula:

$$C(b) \equiv b^e (\mathrm{mod} n)$$

onde $C(b)$ é o bloco codificado e $C(b)$ é o resto da divisão de b^e por n. Logo, temos:

$$C(25) \equiv 25^5 \pmod{35}, \text{ o que implica que } C(25) = 30.$$
$$C(27) \equiv 27^5 \pmod{35}, \text{ o que implica que } C(27) = 27.$$
$$C(18) \equiv 18^5 \pmod{35}, \text{ o que implica que } C(18) = 23.$$
$$C(22) \equiv 22^5 \pmod{35}, \text{ o que implica que } C(22) = 22.$$
$$C(24) \equiv 24^5 \pmod{35}, \text{ o que implica que } C(24) = 19.$$
$$C(28) \equiv 28^5 \pmod{35}, \text{ o que implica que } C(28) = 28.$$

Portanto, a palavra criptografada seria: 30-27-23-22-19-18.
Para decodificar a mensagem utilizamos a seguinte fórmula:

$$D(C) \equiv C^d (\mathrm{mod}\ n), \text{ onde } 0 \leq D(C) \leq n$$

e $D(C)$ é o resto da divisão de C^d por n. Por exemplo, se quiséssemos decodificar o bloco 30, teríamos:

$D(30) \equiv 30^5 (\mathrm{mod} 35)$, o que nos daria $D(30) = 25$. Portanto, letra P.

É óbvio que o módulo escolhido no exemplo é muito pequeno para oferecer qualquer segurança real, mas foi escolhido apenas a título de exemplificação. Quando se trata de um exemplo real, devem ser escolhidos números primos maiores para que o algoritmoseja seguro, pois as contas de exponenciação são grandes para serem feitas à mão, por isso, devem ser feitas utilizando um pacote de coputação algébrica.

Referências Bibliográficas

[1] Aigner, M., Ziegner, G., *Proofs from THE BOOK*, Berlin: Ed. Springer. pp.1-13, (1998).

[2] Fernández, Adán José C., Oliveira, Krerley Irraciel M., *Iniciação a Matemática: um curso com problemas e soluções*, 2.ed.-Rio de Janeiro: SBM, 2010.

[3] Filho,Edgar de A., *Teoria Elementar dos Números*. 2. ed.São Paulo: Nobel, 1985. Pitman, (1980).

[4] Hefez, A., *Elementos de Aritmética*, 2. ed. Rio de Janeiro: SBM, 2011.

[5] Iezzi, G., Domingues, Hygino H., *Álgebra Moderna*, vol. único. 4.ed.São Paulo: Atual, 2003.

[6] Lima,Elon L., *Curso de Análise*, v.1. 13.ed.– Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2011.