UNIVERSIDADE DO ESTADO DO PARÁ
DEPARTAMENTO DE MATEMÁTICA, ESTATÍSTICA E INFORMÁTICA
LICENCIATURA EM MATEMÁTICA

CCSE

CENTRO DE CIÊNCIAS SOCIAIS E EDUCAÇÃO

NÚMEROS PRIMOS

Rubens Vilhena Fonseca

Marília Brasil Xavier
REITORA

Prof. Rubens Vilhena Fonseca
COORDENADOR GERAL DOS CURSOS DE MATEMÁTICA

UEPA
UNIVERSIDADE DO ESTADO DO PARÁ

MATERIAL DIDÁTICO

EDITORAÇÃO ELETRONICA

Odivaldo Teixeira Lopes

ARTE FINAL DA CAPA

Odivaldo Teixeira Lopes

REALIZAÇÃO

UEPA
UNIVERSIDADE DO ESTADO DO PARÁ

Belém - Pará - Brasil
- 2011 –

Capítulo 7

NÚMEROS PRIMOS

7.1. Introdução

A noção de número primo foi, muito provavelmente, introduzida por Pitágoras, ± 530 AC, sendo que a mesma desempenhou um papel central tanto na matemática como no misticismo pitagórico.

A escola pitagórica dava grande importância ao número um, que era chamada de unidade (em grego: Monad). Os demais números inteiros naturais – o 2, 3, 4, etc – tinham caráter subalterno, sendo vistos como meras multiplicidades geradas pela unidade e por isso recebiam a denominação de número (em grego: Arithmós).

Entre os pitagóricos a preocupação com a geração dos números não parava por aí. Já o próprio Pitágoras teria atinado que existem dois tipos de arithmós:

- Os protoi arithmós (números primários ou primos), que são aqueles que não podem ser gerados – através da multiplicação – por outros arithmós, como é o caso de 2, 3, 5, 7...
- Os deuterói arithmós (números secundários), podem ser gerados por outros arithmós, por exemplo, 4 = 2.2, 6 = 3.2, etc.

Ainda por influência dos Pitagóricos , por muitos séculos houve polemica a respeito da primalidade do número dois. Os primeiros pitagóricos chamavam-lhe Dyad, atribuíam-lhe caráter especial – embora menos importante que a unidade Monad – e alguns deles não o incluíam entre os arithmós. Consequentemente, muitos pitagóricos não consideravam o dois como primo. É só pela época de Aristóteles, ± 350 AC, que passou a ser considerado como primo, sendo que este costume foi consagrado pelo livro Elementos de Euclides em cerca de ± 300 AC. Cabe mencionar que entre os gregos, principalmente os pitagóricos de várias gerações após Pitágoras, surgiram outras denominações para os númerosprimos, como: retilíneos, lineares e eutimétricos. Contudo, esta nomenclatura teve uso muito restrito e caíram em desuso.

Registros de documentos gregos

Foi supracitado que a noção de primo fora, muito provavelmente, introduzida por Pitágoras. Com efeito, é impossível ter completa segurança nessa atribuição, pois Pitágoras não deixou nenhum registro escrito de seus trabalhos e os documentos mais antigos que temos falando de suas idéias resumem-se a pequenos fragmentos de textos escritos várias gerações após ele. Entretanto, esses fragmentos, apesar de conterem informações muito escassas, são unânimes em afirmar que Pitágoras iniciou o estudo de números primos.

O mais antigo livro de matemática que chegou completo aos nossos dias e que desenvolve sistematicamente o estudo de números primos é Os Elementos de Euclides. Como é sabido, Euclides seguiu muito de perto as orientações matemáticas dos pitagóricos. Assim não é surpreendente que, no capítulo em que trata da teoria dos números, ele defina número primo de um modo absolutamente compatível com as idéias pitagóricas expostas acima. Elementos, Vol. VII, def 11, temos:

“protós arithmós estin monadi mone metroymenos”.

Ou seja: Número primo é todo aquele que só pode ser medido através da unidade.

Surgimento da denominação latina

A arithmetiké do grego Nikomachos, ±100 dC, é o mais antigo livro de Teoria dos Números, posterior a Elementos de Euclides, que chegou aos nossos dias. Trata-se de uma visão de filósofo e letrado em Elementos, sendo que não há uma única demonstração entre os poucos tópicos abordados. Apesar disso, teve grande repercussão na época e foi a base do primeiro livro em latim que se escreveu sobre Teoria do Números: o De Institutione Arithmetica, do romano Boethius ±500 dC.

No livro de Boethius é onde aparece, pela primeira vez, a nomenclatura numerus primus como tradução do tradicional protós arithmós preservada de Euclides por Nikomachos. Além disto, Boethius, sempre seguindo Nikomachos, usa a velha classificação pitagórica dos números naturais: primos incompostos versus secundários ou compostos.

O livro de Boethius foi, durante cerca de seiscentos anos, a única fonte de estudos de Teoria dos Números disponível na Idade Média. Em torno de 1200 dC iniciou o renascimento científico e matemático pela Europa, com o afluxo das obras árabes e a tradução das obras gregas preservadas no Mundo Islamita. É dessa época um dos mais influentes livros de todos os tempos: o Liber Abacci, de Fibonacci. Esse grande matemático, que havia estudado entre os muçulmanos do Norte da África, diz que acha melhor dizer primus em vez do incomposto preferido pelos árabes. Ficou assim, definitivamente, consagrada a denominação número primo na Europa. (http://www.mat.ufrgs.br/~portosil/pqprimo.html)

7.2. Números Primos (do lat. primus, principal. Prime em inglês)

Definição 7.1: Diz-se que um número positivo p > 1 é um número primo ou apenas um primo se, e somente se, 1 e p são seus únicos divisores positivos. Um inteiro maior que 1 e que não é primo diz-se composto.

Teorema 7.1: Se um número primo p não divide um inteiro a, então a e p são relativamente primos (primos entre si).

Demonstração:

Seja d o mdc de a e p. Então d | a e d | p. Da relação d | p, resulta que d = 1 ou d = p, porque p é primos, e como a segunda igualdade é impossível, porque p não divide a, segue-se que d = 1, isto é, o mdc (a , p) = 1. Logo, a e p são relativamente primos. □

Corolário 7.1: Propriedade Fundamental dos Números Primos.

Se p é um primo tal que p | ab, então p | a ou p | b (podendo ser fator de ambos, a e b).

Demonstração:

Se p | a, nada há que demonstrar, e se, ao invés, p não divide a, então, pelo teorema anterior, o mdc (p, a) = 1. logo, pelo teorema 5.4, p | b. □

Nota: *Observemos que esta propriedade necessária dos números primos é também suficiente para que um inteiro positivo n seja primo: Pois, se n = k. s é composto (1< s ≤ k < n) , temos n| k.s porém tanto n | k e n | s .*

Corolário 7.2: Se p é um primo tal que p | $a_1a_2a_3$ ... a_n, então existe um índice k, com 1 ≤ k ≤ n tal que p | a_k.

Demonstração:

Usando Indução, a proposição é verdadeira para n = 1(imediato) e para n = 2 (pelo corolário 5.1). Supondo, pois, n > 2 e que, se p divide um produto com menos de n fatores, então p divide pelo menos um dos fatores (hipótese de indução).

Pelo corolário 7.1, se p|a_1 a_2 . . . a_{n-1}, então p|a_n ou p|a_1 a_2 ... a_{n-1}.

Se p|a_n, a proposição está demonstrada, e se, ao invés, p|a_1 a_2 ... a_{n-1}, então a hipótese de indução assegura que p|a_k, com 1≤ k ≤ n - 1. Em qualquer dos casos, p divide um dos inteiros a_1, a_2, a_3, ..., a_n. □

Corolário7.3: Se os inteiros p, q_1,q_2 ,..., q_n são todos primos e se p | q_1q_2 ... q_n, então existe um índice k, com 1≤ k ≤ n tal que p = q_k.

Demonstração:

De fato, pelo corolário 7.2, existe um índice k, com $1 \leq k \leq n$, tal que $p|q_k$, como os únicos divisores positivos de q_k são 1 e q_k, porque q_k, segue-se que p = 1 ou $p = q_k$. Mas, p > 1, porque p é primo. Logo, $p = q_k$. □

Teorema 7.2: Todo inteiro composto possui um divisor primo.

Demonstração:

Seja a um inteiro composto. Consideremos o conjunto A de todos os divisores positivos de a, exceto os divisores 1 e a, isto é:

$$A = \{ x \mid a; 1 < x < a \}$$

Pelo "Princípio da Boa Ordenação" existe o elemento mínimo p de A. que vamos mostrar ser primo. De fato, se p fosse composto admitiria pelo menos um divisor d tal que 1 < d < p, e então d|p e d|a, o que implica d|a, isto é, p não seria o elemento mínimo de A, se fosse composto. Logo, p é primo. □

7. 3. Teorema Fundamental da Aritmética.

Todo inteiro positivo n > 1 é igual a um produto de fatores primos.

Demonstração:

Mostraremos a existência da fatoração por indução. Se *n* é primo não há o que provar (escrevemos $m = 1$, $p_1 = n$). Se n é composto podemos escrever n = ab, a, b ∈ N , 1 < a < n, 1 < b < n. Por hipótese de indução, a e b se decompõem como produto de primos. Juntando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n. □

Nota: *Este teorema (como qualquer outro teorema chamado de "fundamental") não deveria ser aplicado sem a devida precaução. Existem inúmeros sistemas numéricos nos quais a fatoração não é única. Por exemplo, imagine um sistema que tenha apenas inteiros pares com a adição e multiplicação usual e denominemos um número de "e-primo" se ele não for o produto de dois outros números pares. Neste caso, alguns "e-primos" são 2, 6, 10, 14, 18, ... Observe que neste sistema, 36 possui duas fatorações diferentes, 6x 6 e 2 x 18. (http://primes.utm.edu/)*

Corolário 7.4: A decomposição de um inteiro positivo n > 1 como produto de fatores primos é única, a menos da ordem dos fatores.

Demonstração:

Suponha que

$$n = p_1 \dots p_m = q_1 \dots q_r$$

com, $p_1 \leq \dots \leq p_m$, $q_1 \leq \dots \leq q_r$. Como $p_1 | q_1 \dots q_r$ temos $p_1 | q_i$ para algum valor de i, donde, como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas por hipótese de indução

$$\frac{n}{p_1} = p_2 \dots p_m = q_2 \dots q_r$$

admite uma única fatoração, donde m = r e $p_i = q_i$ para todo i. □

Corolário 7.5: Todo inteiro positivo n > 1 admite uma única decomposição da forma

$$n = p_1^{k1} p_2^{k2} \dots p_r^{kr}$$

onde, para i =1,2,... , r cada k_i é um inteiro positivo e cada p_i é um primo, com

$$p_1 < p_2 < \dots < p_r,$$

denominada decomposição canônica do inteiro positivo n > 1.

Demonstração:

Pelo teorema Fundamental da Aritmética, n é um produto de fatores primos $q_1 . q_2 \dots q_m$, com $q_1 \leq q_2 \leq \dots \leq q_m$ ($m \geq 1$). Agrupando-se os fatores primos repetidos na forma de potências de primos, temos a representação enunciada neste corolário e, pelo Teorema Fundamental da aritmética, tal representação é única.

Nota: *Conhecidas as decomposições canônicas de dois inteiros positivos a > 1 e b > 1, o mdc (a, b) é o produto dos fatores primos comuns às duas decomposições canônicas tomados cada um com o menor expoente, e o mmc (a, b) é o produto dos fatores primos comuns e não comuns às duas decomposições canônicas tomados cada um com o maior expoente.*

Corolário 7.6: Se $p_1.p_2 \dots p_n$ divide a^r, então $p_1 . p_2 \dots p_n$ divide a, onde $p_1 p_2 \dots p_n$ é o produto de n primos e n e r são inteiros positivos.

Demonstração:

Se $p_1\ p_2 \ldots p_n$ não divide a, então a não é nenhum dos primos $p_1p_2 \ldots p_n$ Seja p_i, $1 \leq i \leq n$, um desses primos. Então, p_i também não é fator primo de a^r e, desta forma, não existe p_i, $1 \leq i \leq n$, que divida a^r, o que implica que $p_1 . p_2 \ldots p_n$ não divide a^r. Por contraposição, temos a demonstração pedida.

Observação: O fato de que os expoentes dos primos p_i sejam 1 é essencial. Por exemplo $4 = 2^2$ divide $6^2 = 36$, mas 4 não divide 6.

7.4. A Seqüência dos Números Primos

Teorema 7.4: (de Euclides): Há um número infinito de primos.

Demonstração:

Suponha por absurdo que p_1, p_2, ..., p_m fossem *todos* os primos. O número $P = p_1 . p_2 \ldots p_m + 1 > 1$ não seria divisível por nenhum primo, o que contradiz o teorema fundamental da aritmética. □

Proposição 7.1. Para o n-ésimo número primo p_n vale a estimativa $p_n \leq 2^{2^{n-1}}$.

Demostração:

Para n = 1 é verdade que $2 = p_1 \leq 2^{2^{1-1}} = 2^1 = 2$. Suponhamos já provadas as desigualdades

$$p_2 \leq 2^{2^1}$$
$$p_3 \leq 2^{2^2}$$
$$\ldots$$
$$p_n \leq 2^{2^{n-1}}$$

Se q é primo tal que $q \mid p_1 . p_2 \ldots p_n + 1$, então $q > p_n$, particularmente $q \geq p_{n+1}$.

Então,

$$p_{n+1} \leq p_1 . p_2 \ldots p_n \leq 2^{1+2+2^2+\cdots+2^{n-1}} + 1 = 2^{2^n-1} + 1 \leq 2^{2^n-1} + 2^{2^n-1} = 2^{2^n}.$$ □

Esta estimativa é exageradamente fraca, no geral p_n é significativamente menor que $2^{2^{n-1}}$ por exemplo $2^{2^{4-1}} = 256$ e p_4 é apenas 7. Uma estimativa melhor para p_n, postulada por Bertrand e, demonstrada por Chebychev, é dada pelo teorema seguinte:

Teorema 7.5 (de Chebychev): Para todo inteiro $m \geq 2$ existe um primo p com $m < p < 2m$. A demonstração deste teorema está fora de nosso contexto. Um outro fato provado é que entre dois cubos consecutivos existe sempre um primo.

Com esse Teorema podemos afirmar que $p_{n+1} < 2p_n$ (para $n \geq 1$)

Corolário 7.6. Para o n-ésimo número primo p_n vale a estimativa $p_n \leq 2^n$.

Demonstração:

Temos $2 = p_1 \leq 2^1$ e pelo teorema de Chebychev: Para todo inteiro positivo n, tem-se $p_n < p_{n+1} < 2 . p_n$. De $p_n \leq 2^n$ segue que $p_{n+1} \leq 2. 2^n = 2^{n+1}$. □

Ao estudarmos a sequência de números primos percebemos que existem infinitos primos em subconjuntos particulares dos inteiros, como, por exemplo, na sucessão aritmética: {4q + 3; q inteiro e $q \geq 0$} = {3, 7, 11, 15, 19, ...}.

Esse resultado foi generalizado pelo matemático alemão Peter Gustav Le-jeune Dirichlet (1805-1859).

Teorema 7.6 (de Dirichlet). Sejam a e b inteiros primos entre si, isto é, mdc (a, b) = 1.

Existem infinitos primos da forma an + b, onde n é inteiro positivo.

A demonstração deste Teorema exige avançados conhecimentos de Análise Matemática.

Exemplos:

Na sequência 3n + 1, temos os primos 7, 13, 19, 31, 37, 43, 61, 67, 73, 97, 103, ...

Na sequência 9n + 4 temos os primos 13, 31, 67, 103, 139, 157, 193, 211, ...

O resultado de Dirichlet diz não só que o número de primos é infinito, mas também que, se considerarmos subconjuntos particulares de inteiros, como as sucessões aritméticas acima, teremos já nesses subconjuntos uma infinidade de primos.

Uma aplicação do Teorema de Dirichlet leva-nos a um resultado obtido pelo matemático polonês W. Sierpinski , que nos mostra, mais uma vez, a forma surpreendente como os primos se distribuem nos inteiros.

Teorema 7.7 (de Sierpinski). Dado um inteiro *m* maior que 1, existe um primo p tal que $|p \pm 1|$, $|p \pm 2|$, ..., $|p \pm m|$ são compostos.

Exemplo: Seja m = 10 e p = 19. Temos:

19+1, 19+2, 19+3, 19-4, 19+5, 19+6, 19+7, 19+8, 19+9 e 19-10. Os resultados são todos números compostos: 20, 21, 22, 15, 24, 25, 26, 27, 28 e 9.

Observe que se tivéssemos escolhido o primo 17, não seria possível construir uma sequência de compostos com m = 10, pois 17 + 6 = 23 e 17 – 6 = 11, ambos primos.

Demonstração:

Vejamos, em primeiro lugar, que existe um primo p tal que p + 1, p + 2, ..., p + m sejam compostos. Para cada m dado, o Teorema 1 garante, em particular, que existe um inteiro primo q maior do que m. Seja a = (q + 1) • (q + 2) • (q + 3) ... (q + m).

Se q divide a, então q divide q + i, e, portanto, q divide i, o que é impossível para $0 < i \leq m < q$. Então a e q são primos entre si. Pelo teorema de Dirichlet, existe um primo p na sequência an + q. Seja p = (q +1) • (q + 2) • ... • (q + m) • n + q este primo. Então os números p + 1, p + 2, ..., p + m são m números compostos. Para ampliar este resultado, observemos que, por motivos análogos aos de cima,

a' = (q - m).[q - (m- 1)]...(q - 1)...(q + m)

é primo com q e se p' for um primo da sequência a'n + q, isto é,

p' = (q - m) ... (q - 1) . (q + 1) ... (q + m) . n + q

os números p' – m, ... p' – 1, p' + 1, ... p' + m serão compostos. Assim o número primo p' se encontra na sucessão dos inteiros, "isolado" por m compostos de cada lado. (RPM 11)

7.5. O Crivo de Eratóstenes.

Eratóstenes, matemático, astrônomo, historiador, geógrafo e filósofo grego, nasceu em Cirene por volta de 276 a.C. e passou grande parte de sua juventude em Atenas. Com aproximadamente 40 anos, foi convidado pelo rei Ptolomeu III do Egito para ser bibliotecário da Universidade de Alexandria.

Ficou conhecido como Beta, e a respeito dessa alcunha existem algumas hipóteses. Alguns acreditam que, por causa de seu saber, foi elevado à condição de um segundo Platão. Outros, dizem que tal apelido lhe fora dado por ter sido o segundo bibliotecário da Universidade de Alexandria. Uma terceira explicação sugere que, apesar de ser talentoso, Eratóstenes não conseguiu ser o primeiro de seu tempo em nenhum ramo de estudo, em outras palavras, foi sempre o segundo. Por fim, o historiador James Gow sugeriu que talvez Beta indicasse simplesmente o número (grego) 2 referente a um gabinete ou a uma sala de leitura da universidade.

Escreveu diversas obras, mas muitas se perderam, inclusive o tratado Sobre a medida da Terra. Eratóstenes morreu em Alexandria, em 194 a.C.

(http://www.moderna.com.br/moderna/didaticos/ef2/matematica/erato/bio_eratostenes.htm)

Teorema 7.8: Se um inteiro positivo a > 1 é composto, então a possui um divisor primo $p \leq \lfloor \sqrt{a} \rfloor$.

Demonstração:

Com efeito, se o inteiro positivo a > 1 é composto, então:

$$a = bc, \text{ com } 1 < b < a \text{ e } 1 < c < a$$

Portanto, supondo $b \leq c$, teremos:

$$b^2 \leq bc = a \Rightarrow b \leq \sqrt{a}\,. \square$$

O teorema 7.8 fornece um processo que permite reconhecer se um dado inteiro a >1 é primo ou é composto, para o que basta dividir a sucessivamente pelos primos que não excedem o valor $\lfloor \sqrt{a} \rfloor$. Tal resultado é a base do chamado Crivo de Eratóstenes que veremos em seguida.

Uma questão natural sobre os números primos é a de determinar, dentre os inteiros positivos, todos os números primos até certo número dado. Esta questão também foi resolvida na antiguidade por Eratóstenes. A ele devemos o chamado *Crivo de Eratóstenes*. Com o crivo de Eratóstenes podem-se

determinar, sem auxílio de máquinas, todos os números primos até 200, 400 ou 500, por exemplo. Com o auxílio de computadores, o crivo de Eratóstenes, convenientemente adaptado, permite determinar os números primos até limites bem altos. Mesmo antes dos computadores, já haviam sido determinados os números primos até 10.000.000. Isto ocorreu por volta de 1914, por obra do matemático americano D. N. Lehmer. Dois outros matemáticos (Bays e Hudson) calcularam, em 1976, (usando computadores, evidentemente!), a tabela dos números primos até 12×10^{11}. Além disso, há tabelas de números primos em determinados intervalos de inteiros e conhecem-se também números primos bem grandes, como o número $2^{44497} - 1$, que possui 13395 algarismos! (RPM 19)

A construção de uma tabela de números primos que não excedam um dado inteiro n usando o Crivo de Eratóstenes consiste no seguinte: escrevem-se na ordem natural todos os inteiros a partir de 2 até n e, em seguida, eliminam-se todos os inteiros compostos que são múltiplos dos primos p tais que $p \leq \lfloor \sqrt{a} \rfloor$ isto é, 2p, 3p, 4p, ...

Exemplo: Construir a tabela de números primos menores que 200.

Solução: Como $\lfloor \sqrt{200} \rfloor = 14$, basta eliminar sucessivamente da tabela os números que são múltiplos dos primos p menores que 14, ou seja, 2, 3, 5, 7, 11 e 13.

.	**2**	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100
101	102	**103**	104	105	106	**107**	108	**109**	110
111	112	**113**	114	115	116	117	118	119	120
121	122	123	124	125	126	**127**	128	129	130
131	132	133	134	135	136	**137**	138	**139**	140
141	142	143	144	145	146	147	148	**149**	150
151	152	153	154	155	156	**157**	158	159	160
161	162	**163**	164	165	166	**167**	168	169	170
171	172	**173**	174	175	176	177	178	**179**	180

181	182	183	184	185	186	**187**	188	189	190
191	192	**193**	194	195	196	**197**	198	**199**	200

Os valores em vermelho são os números primos que não foram "riscados" da tabela.

Listamos a seguir a os 199 primeiros números primos:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 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, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213 ,1217.

Nota: *Podemos fazer um crivo mais econômico, já que não é possível evitar completamente o fato de que alguns números são riscados várias vezes. Podemos proceder da seguinte maneira: Primeiro escrevemos uma lista com os ímpares de 3 até n. Como queremos riscar os números de p em p é claro que os múltiplos de p que são múltiplos de primos menores que p já foram riscados da lista. Então, nesta etapa, podemos começar a riscar de p em p a partir do menor múltiplo de p, que não é múltiplo de um primo menor que p; isto é, a partir de* p^2*. Isto evita muitas duplicações.[Coutinho]*

3, 5, 7, 32, 11, 13, 15, 17, 19, 21 23, 52, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 72, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99.

Definição 7.2: Para qualquer número real $x > 0$, seja $\pi(x)$ o número de primos $p \leq x$, isto é, $\pi(x)$ é quantidade dos números primos menores que ou iguais a x.

Tabela dos 20 primeiros valores inteiros da Função p (x)

x	π(x)
1	0
2	1
3	2

4	2
5	3
6	3
7	4
8	4
9	4
10	4
11	5
12	5
13	6
14	6
15	6
16	6
17	7
18	7
19	8
20	8

De acordo com o Teorema de Chebychev podemos afirmar que

$$\pi(2n) - \pi(n) \geq 1 \text{ (para } n \geq 2)$$

Nota: *Um problema prático, onde as propriedades dos números primos têm reflexos importantes, é o problema do reconhecimento da fala por computadores que exige o desenvolvimento de algoritmos tão rápidos quanto possível para a decomposição de sons nas suas frequências fundamentais, uma técnica conhecida como Análise de Fourier. A velocidade teórica máxima desses algoritmos esta diretamente relacionada com a função $\pi(x)$ que fornece o numero de primos menores que ou iguais a x.*

Fórmula de Minác: Dado um inteiro $m \geq 2$, J. Minác estabeleceu uma fórmula para a contagem dos números primos $\pi(m)$:

$$\pi(m) = \sum_{k=2}^{m} \left\lfloor \frac{(k-1)! + 1}{k} - \left\lfloor \frac{(k-1)!}{k} \right\rfloor \right\rfloor$$

Demonstração: Será vista após estudarmos o Teorema De Wilson.

Exemplo:

$$\pi(6) = \left[\frac{1!+1}{2} - \left\lfloor\frac{1!}{2}\right\rfloor\right] + \left[\frac{2!+1}{3} - \left\lfloor\frac{2!}{3}\right\rfloor\right] + \left\lfloor\frac{3!+1}{4} - \left\lfloor\frac{3!}{4}\right\rfloor\right\rfloor + \left\lfloor\frac{4!+1}{5} - \left\lfloor\frac{4!}{5}\right\rfloor\right\rfloor + \left\lfloor\frac{5!+1}{6} - \left\lfloor\frac{5!}{6}\right\rfloor\right\rfloor$$

$\pi(6) = 1 + 1 + 0 + 1 + 0 = 3$. Resultado que nos diz que existem três primos antes do número seis.

Fórmula Para o n-ésimo Número Primo

Devido ao resultado acima podemos escrever uma fórmula que nos retorna o n-ésimo número primo estabelecida por C. P. Willans em 1964:

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \left(\frac{n}{1 + \pi(m)} \right)^{\frac{1}{n}} \right\rfloor$$

Exemplo:

$$p_2 = 1 + \left\lfloor \sqrt{\left(\frac{2}{1 + \pi(1)} \right)} \right\rfloor + \left\lfloor \sqrt{\left(\frac{2}{1 + \pi(2)} \right)} \right\rfloor + \left\lfloor \sqrt{\left(\frac{2}{1 + \pi(3)} \right)} \right\rfloor + \left\lfloor \sqrt{\left(\frac{2}{1 + \pi(4)} \right)} \right\rfloor$$

$$p_2 = 1 + \lfloor \sqrt{2} \rfloor + \lfloor \sqrt{1} \rfloor + \left\lfloor \sqrt{\frac{2}{3}} \right\rfloor + \left\lfloor \sqrt{\frac{2}{3}} \right\rfloor = 1 + 1 + 1 + 0 + 0 = 3$$

Definição 7.3: Para todo número primo p, seja p# o produto de todos os números primos q ≤ p . p# é chamado o *primorial de p*.

Tabela dos 17 primeiros Primoriais

P	p#
2	2
3	6
5	30
7	210
11	2310
13	30030
17	510510
23	9699690
29	223092870
31	6469693230
37	200560490130
41	7420738134810
43	304250263527210
47	13082761331670030
53	614889782588491410
59	32589158477190044730
61	1922760350154212639070

Teorema 7.8: p# +1 não possui nenhum fator primo menor do que ou igual a p.

Demonstração: Suponhamos, por contradição, que p# + 1 seja divisível por um primo q ≤ p . Ou seja, existe um inteiro positivo s tal que tal que p# + 1 = q.s, isto é q.s – p# =1. Como q ≤ p , então q é necessariamente um fator de p#. Logo q divide ambas as parcelas da diferença q.s – p#. Portanto q divide 1, o que é um absurdo uma vez que q é primo. □

Nota: *Veja que resultado interessante:*

$$\lim_{n\to\infty}\left[(p_n\ \#)^{\frac{1}{p_n}}\right] = e$$

Leitura: **A Distribuição dos Números Primos**

Ao contemplar uma tabela de números primos, a primeira impressão que se tem é a de que não há nenhuma ordem entre os números primos: às vezes eles aparecem próximos uns dos outros, às vezes afastados, ora menos, ora mais afastados; enfim, analisando-os individualmente ou em pequenos grupos, não divisamos qualquer regularidade em sua distribuição. Entretanto, a sagacidade de inteligências privilegiadas consegue ver mais fundo, e foi precisamente isso o que aconteceu por obra do matemático francês Adrien - Marie Legendre (1752-1833). Ele se ocupou dessa questão e por volta de 1800 formulou uma conjectura que revela certa ordem no que parecia ser um caos completo. Para explicarmos a conjectura de Legendre, introduzimos o símbolo π (x) como sendo o número de números primos até certo valor x. Assim, π(8) = 4, ou seja, o número de números primos até 8 é 4; π(11) = 5, pois há cinco números primos até 11, precisamente, 2, 3, 5, 7, 11; e assim por diante. Pois bem, o que Legendre conjecturou, empiricamente, analisando tabelas de números primos (em 1797 uma dessas tabelas foi publicada, contendo todos os números primos até 400031), é que π(x) podia ser aproximado pela função $\frac{x}{lnx}$ (o logaritmo que aqui aparece é o logaritmo natural, isto é, na base e ≈ 2,718281...), e que essa aproximação seria tanto melhor quanto maior fosse x. Mas isto deve ser entendido em termos relativos, isto é, o erro que se comete tomando $\frac{x}{lnx}$ em lugar de π (x) torna-se tanto menor quanto maior for x, relativamente a $\frac{x}{lnx}$. Em outras palavras, seja

$$E(x) = \pi(x) - \frac{x}{lnx}\ (1)$$

o erro que se comete ao tomar $\frac{x}{1nx}$ em lugar. de π(x). Pois bem, o que se torna pequeno com o crescer de x é o erro relativo

$$\frac{\frac{E(x)}{x}}{\frac{}{\ln x}}\ (2)$$

Este erro pode ser feito, em valor absoluto, tão pequeno quanto quisermos, desde que façamos x suficientemente grande.

Carl Friedrich Gauss (1777-1855), que é considerado por muitos o maior matemático de todos os tempos, conta, numa carta de 1849, publicada vários anos mais tarde, que quando ainda bem jovem, com apenas 15 anos de idade, pensou muito sobre a distribuição dos números primos, chegando a conjecturar algo equivalente ao que conjecturou Legendre.

Seja como for, essa conjectura logo impressionou os matemáticos como algo notável, pois quem diria que a seqüência dos números primos pudesse ter algo a ver com a função logaritmo!

A descoberta de Legendre e Gauss demorou a ser demonstrada. Embora ela tenha sido objeto da atenção dos melhores matemáticos do século, desafiou a argúcia desses homens por cerca de 100 anos. De fato, foi somente em 1896 que ela foi demonstrada pela primeira vez. E nesse mesmo ano apareceram duas demonstrações, uma pelo matemático francês Jacques Hadamard (1865-1963) e outra, pelo belga Charles de Ia Vallée Poussin (1866-1962). Essas demonstrações, independentes uma da outra, baseavam-se nas idéias de um outro grande matemático do século, Bernhard Riemann (1826-1866). Embora não tenha logrado demonstrar a conjectura de Legendre e Gauss, Riemann, num memorável trabalho intitulado Sobre o número de números primos menores que um certo número, deixou ideias notáveis sobre teoria dos números, que vêm sendo exploradas pelos estudiosos do assunto até os dias de hoje.

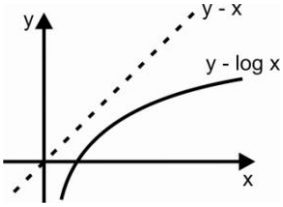
Antes mesmo das demonstrações de Hadamard e de la Vallée Poussin, o matemático russo Pafnutii Chebyshev (1821-1894) provou, por volta de 1850, um resultado próximo à conjectura de Legendre e Gauss. Segundo Chebyshev, existem constantes positivas c e C (c ≈ 0,92, C ≈ 1, 106) tais que

$$c\frac{x}{\ln x} \leq \pi\,(x) \leq C\frac{x}{\ln x} \quad (3)$$

Para bem entendermos o significado da aproximação

$$\pi\,(x) \approx \frac{x}{\ln x} \quad (4)$$

vamos comparar os gráficos das funções y = x e y = log x. Eles nos revelam que ambas as funções crescem com o crescer de x, tendendo a infinito.



No entanto, como podemos ver, claramente, a primeira dessas funções cresce mais depressa que a segunda, distanciando-se mais e mais desta última, à medida que x cresce acima de qualquer número dado. Isto fica mais claro ainda quando levamos em conta que o gráfico do logaritmo tem a concavidade voltada para baixo, significando que, embora esta função esteja crescendo sempre com o crescer de x, trata-se de um crescimento cada vez mais lento, quanto maior for x. Isto quer dizer que o quociente no segundo membro de (4) também cresce, tendendo a infinito com o crescer de x, o que está de acordo com o fato de que existem infinitos números primos, isto é, (x) cresce acima de qualquer número, desde que façamos x suficientemente grande. Não obstante tudo isso, o erro absoluto expresso em (1) pode tornar-se muito grande, mas não o erro relativo expresso em (2); este tende a zero, isto é, pode ser feito menor do que qualquer número positivo dado, desde que façamos x suficientemente grande.

Uma conclusão simples que podemos tirar de (4) é que, em certo sentido, os números primos vão ficando cada vez mais raros, à medida que avançamos na seqüência dos números naturais. Para bem entender o que estamos dizendo, observe que $\frac{x}{1nx}$ significa $x\ \ vezes\ \frac{x}{1nx}$

de sorte que $\frac{x}{1nx}$ é a densidade média dos números primos no intervalo que vai de 1 até x. O fato de que essa densidade decresce com o crescer de x significa precisamente o que dissemos acima: os números primos vão ficando cada vez mais raros, à medida que avançamos na seqüência dos números naturais. (RPM19)

Definição 7.3 Chamam-se primos gêmeos dois inteiros positivos ímpares e consecutivos que são ambos primos. Em outras palavras, dizemos que dois primos ímpares são gêmos quando a diferença entre eles é igual a 2.

Assim, por exemplo, são pares de primos gêmeos:

3 e 5, 5 e 7, 11 e 13, 17 e 19, 29 e 31

Não se sabe até hoje se há um número infinito de pares de primos gêmeos, mas são conhecidos primos gêmeos muito grandes, tais como:

140.737.488.353.507 e 140.737.488.353.509 140.737.488.353.699 e 140.737.488.353.701

Um fato interessante é a existência de apenas um terno de inteiros positivos ímpares e consecutivos que são todos primos: 3, 5 e 7.

7.6. Seqüência de Inteiros Consecutivos Compostos

Existem, na *sequência dos primos*, primos *consecutivos* "tão afastados quanto se deseje". Ou seja, existem "saltos' arbitrariamente grandes na seqüência dos primos.

Teorema 7.9: Dado um inteiro positivo n >1, é possível determinar n inteiros consecutivos tais que nenhum deles seja primo.

Demonstração:

De fato, é evidente que na sequência:

$$(n + 1)! + 2, (n + 1)! + 3, (n + 1)! + 4, ..., (n + 1)! + (n + 1)$$

os seus n termos são inteiros positivos consecutivos, e cada um deles é *composto*, porque (n +1)! + j é divisível por j se $2 \leq j \leq n + 1$. □

Assim, por exemplo, supondo n = 4, obtemos a sequência:

$$5! + 2, 5! + 3, 5! + 4, 5! + 5$$

Cujos termos são 4 inteiros positivos consecutivos, cada um dos quais é composto, pois, temos:

$$5! + 2 = 122 = 2 \cdot 61, 5! + 3 = 123 = 3 \cdot 41$$
$$5! + 4 = 124 = 4 \cdot 31, 5! + 5 = 125 = 5 \cdot 25$$

Outras sequências de 4 inteiros consecutivos e compostos existem, tais como

24, 25, 26, 27 e 32, 33, 34, 35
54, 55, 56, 57 e 74, 75, 76, 77

Nota: *Em 1984 Samuel Yates iniciou uma lista dos "Maiores Primos Conhecidos" e criou o nome primo titânico para designar qualquer número primo com 1.000 ou mais dígitos decimais. Denominou também de titãs aqueles que provaram a sua primalidade.*

A maioria dos primos são titânicos e dezenas de milhares deles são "conhecidos". Entretanto, na época em que Yates definiu os primos titânicos, tinha-se conhecimento de apenas alguns poucos.

Cerca de dez anos mais tarde, Yates designou como primo gigante todo número primo que possuísse 10.000 ou mais dígitos decimais. E os Megaprimos são números primos que possuam no mínimo um milhão de dígitos decimais.

http://www.numaboa.com.br/criptologia/matematica/primos.php

Corolário 7.7: Dado um inteiro positivo n, existem dois primos consecutivos p_h, p_{h+1} tais que

$$p_{h+1} - p_h > n.$$

Demonstração:

Seja p_h o maior dos primos que são menores que $(n +1)! + 2$.

Então, $p_h \leq (n + 1)! + 1$. Do teorema anterior, temos ainda que

$$p_{h+1} > (n + 1)! + (n + 1)$$

Fazendo a diferença entre ambas as desigualdades, temos

$$p_{h+1} > (n + 1)! + (n + 1)$$

Exemplo: Seja n = 6, de acordo com a demonstração podemos considerar os primos $p_1 = 5039$ e $p_2 = 5059$. Assim, 5059 – 5039 > 6, isto é, 20 > 6.

Teorema 7.10: O produto de qualquer sequência de k inteiros consecutivos é divisível por k!.

Demonstração:

Vamos considerar *n* e *k* inteiros positivos com $k \leq n$. Sabemos que o número de combinações de *n*, tomadas *k* a *k*, é um inteiro dado por:

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{n(n-1)\ldots(n-k+1)}{k!}$$

Sendo o numerador o produto de *k* inteiros consecutivos temos o resultado para uma sequência de *k* inteiros positivos. No caso de zero ser um elemento na seqüência o resultado é trivial, uma vez que zero é divisível por qualquer inteiro não nulo.

Se a sequência contiver só números negativos, a fração do lado direito da igualdade acima sofrerá, no máximo, uma mudança de sinal continuando a ser um inteiro, o que conclui a demonstração.

7.7. Conjecturas

● **Conjectura de Goldbach.**

Em 1742, numa carta a Leonhard Euler (1707-1783), **Christian Goldbach** (1690-1764) expressou a seguinte conjectura:

Todo inteiro n > 5 é a soma de três números primos.

Em resposta, **Leonhard Euler** observou que essa conjectura era equivalente à seguinte:

Todo inteiro par maior que ou igual a 4 *é a soma de dois primos.*

Esta conjectura é conhecida como *conjectura de Goldbach*. Um romance interessantíssimo sobre a dificuldade desse assunto é "*Tio Petros e a Conjectura de Goldbach*" escrito por Apostolos Doxiadis e publicado pela Editora 34.

Exemplos:

4=2+2
6=3+3
8=3+5
10=3+7, 5+5
12=5+7
14=3+11, 7+7
16=3+13, 5+11
18=5+13, 7+11
20=3+17, 7+13
22=3+19, 5+17, 11+11
24=5+19, 7+17, 11+13
26=3+23, 7+19, 13+13
28=5+23, 11+17
30=7+23, 11+19, 13+17
32=3+29, 13+19
34=3+31, 5+29, 11+23, 17+17
36=5+31, 7+29, 13+23, 17+19
38=7+31, 19+19
40=3+37, 11+29, 17+23

Muitos matemáticos continuam tentando encontrar um contra-exemplo ou uma demonstração para essa conjectura. Por exemplo:

- **Georg Cantor** (1845-1918), efetuou em 1894 todas as decomposições possíveis, como soma de dois números primos, de todos os números pares inferiores a 1000.

- **Aubry** estendeu a lista de Cantor até 2000.
- **R. Haussner** em 1897 estendeu essa tabela até 5000.

- Em 1937 o matemático soviético **I.M.Vinogradov** demonstrou, usando somas trigonométricas adequadas, que qualquer número ímpar suficientemente grande é soma de três números primos.

- Em 1966 o matemático chinês Jeng-Run Chen provou que a partir de algum número n, todo par maior que 2 ou é soma de dois primos, ou a soma de um primo com o produto de dois primos. O argumento de Chen não diz qual é esse n; apenas demonstra que ele existe.

Além da Conjectura de Goldbach, em Teoria dos Números, particularmente em Números Primos, existem muitos problemas em aberto. Segue uma lista com algumas conjecturas que, embora já tenham sido testadas para inúmeros casos, ainda não foram demonstradas. Eis algumas:

- ***Todo número ímpar maior que cinco é a soma de três primos***. Esse fato já foi provado, por Vinogradov, para números suficientemente grandes. Em 1956, Borodzkin mostrou que $n > 3^{14348907}$ é suficiente. Esse número foi diminuído, em 1989, para 1043000, por Chen e Wang,

mas ainda é muito grande para que os casos menores possam ser testados com o uso de um computador.
Exemplos:
7 = 3 + 2 + 2; 21 = 11 +7 + 3 ; 41 = 11 + 13 + 17; 49 = 13 + 17 + 19

- ***Existem infinitos primos da forma $k^2 + 1$.***
  Exemplos:
  $5 = 2^2 + 1$; $17 = 4^2 + 1$; $3^7 = 6^2 + 1$.

- ***Existem infinitos pares de primos consecutivos (Primos Gêmeos)*** .
  Exemplos: (3 e 5), (5 e 7), (11 e 13), (17 e 19), (29.879 e 29.881), ...

Em 2000, foi apresentado um par de primos gêmeos cada um com 18075 dígitos. É o par

$$4\,648\,619\,711\,505.\ 2^{60000} \pm 1$$

- **Existe sempre um primo entre dois quadrados consecutivos.**
  Exemplos: 3 entre 1 e 4; 5 e 7 entre 4 e 9; 11 e 13 entre 9 e 16, ...

- **Primos de Sophie Germain.** Um número primo p é um número primo de Sophie Germain se $2p + 1$ é também primo. São famosos porque Sophie Germain provou que o Último Teorema de Fermat é verdadeiro para estes números. A existência de um número infinito de tais números primos é uma uma afirmação ainda não provada. Os primeiros primos de Sophie Germain são 2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233 ...

Nota: Primos em Progressão Aritmética.

Um problema famoso que permaneceu por muito tempo em aberto, era o de provar se existiam progressões aritméticas arbitrariamente longas formadas exclusivamente por primos. Van der Corput já havia provado em 1939 que há uma infinidade de progressões aritméticas formadas por 3 primos. Ben Green do Instituto de Matemática de Vancouver e Terence Tao da Universidade da Califórnia, provaram em 2006, que tais sequências existem. Mas a prova não especifica como encontrá-las ou entre quais primos tais sequências se encontram.
A mais longa progressão aritmética de números primos conhecida até o momento, tem 24 termos. Foi descoberta por Jaroslaw Wroblewski em janeiro de 2007:

$$468395662504823 + 45872132836530.k, \text{ para } k = 0, 1, ..., 23.$$

7.8. Fórmulas que geram alguns números primos

Muitas tentativas têm sido realizadas para encontrar fórmulas aritméticas simples que forneçam somente primos. Nesta seção será apresentada algumas fórmulas famosas sobre primos.

1) *Fórmula de Fermat:*
Fermat fez sua famosa conjectura de que os números da forma

$$F_n = 2^{2^n} + 1$$

são primos.
Para n = 1, 2, 3, 4 obtemos:

$$F_1 = 2^2 + 1 = 5$$
$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$$
$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$$
$$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65.537$$

todos primos. Porém em 1732, Euler descobriu a fatoração

$$2^{2^5} + 1 = 4294967297 = (641).(6700417)$$

portanto, F(5) não é primo. Até este momento (05 /2005) o maior primo de Fermat conhecido é F_4

2) *Fórmula de Euler:*
Em 1772 Leonhard Euler descobriu um polinômio tendo uma longa sucessão de valores primos, dado por

$$F(n) = n^2 + n + 41$$

que fornece primos para n = 1, 2, ..., 39. Entretanto, para n = 40 o valor é composto:

$$F(40) = 402 + 40 + 41 = 40.\ (40 + 1) + 41 = 40.41 + 41 = 41.(40 + 1) = 41.41.$$

3) *Fórmula de Mersenne:*
Marin Mersenne em 1644 fez a seguinte afirmação: "Todo natural $M_p = 2^p - 1$ é primo para os primos p = 2, 3, 5, 7, 13, 17, 19, 31, **67**, 127 e **257**, e é composto para todos os outros primos p < 257".

Entretanto, esta afirmação é incorreta, pois, segundo o site http://www.mersenne.org/ prime.htm, até setembro de 2006 já eram conhecidos, 44 primos de Mersene, para os primos p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 1213 ,19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 30402457 e 32582657. Esse último primo tem 9.808.358 dígitos.

Como se pode ver, Mersenne cometeu duas falhas: Incluiu p= 67, 257 na sua lista de primos e excluiu dessa lista p= 61, 89, 107.

Somente em 1947 (mais de 300 anos depois) a lista correta p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 e 127 onde p < 257, ficou pronta..

4) Outras fórmulas que geram alguns primos são:

$F(n) = n^2 - n + 41$ para n = 1, 2, 3, 4, ..., 40

$F(n) = n^2 - 79n + 1601$ para n = 0, 1, 2, ..., 79

$F(n) = n^2 + n + 17$ para n = 0, 1, 2, ..., 15

$F(n) = 3n^2 + 3n + 23$ para n = 0, 1, 2, ..., 21

$F(n) = 6n^2 + 6n + 31$ para n = 0, 1, 2, ..., 28

Cabe agora a pergunta: Existe algum polinômio (não-constante), com coeficientes inteiros, que forneça a sequência dos números primos ou apenas números primos? Infelizmente a resposta é não!

Teorema 7.11: Não existe polinômio algum $P(x) = a_n x^n + a_{n-1}x^{x-1} + ... + a_0$, $a_0 \neq 0$ com coeficientes a_k, $0 \leq k \leq n$, todos inteiros, cujos valores numéricos sejam sempre primos para valores inteiros da variável x. (VER RPM 45)

Demonstração: Suponhamos, por contradição, que o polinômio *P(x)*, nas condições do teorema, produz sempre primos para valores inteiros da variável x. Então, para x = j, sendo j um inteiro fixo, *P*(j) = p é um primo, e qualquer que seja o inteiro s, temos:

$$P(j + ps) = a_n (j + ps)^n + na_{-1} (j + ps)^{n-1} + ... + a_2 (j + ps)^2 + a_1 (j + ps) + a_0$$

Desenvolvendo cada uma das potências pela fórmula do binômio e agrupando os primeiros termos de cada desenvolvimento, temos:

$$P(j + ps) = (a_n j^n + a_{n-1} j^{n-1} + ... + a_2 j^2 + a_1 j + a_0) + pg(s) = P(j) + pg(s) = p + pg(s)$$

onde *g(s)* indica um certo polinômio não constante em *s* com coeficientes inteiros, de grau n, logo:

$$P(j + ps) = p(1 + g(s))$$

Então, p| P(j + ps). Se P(j + ps) é *primo* devemos ter $P(j + ps) = \pm p$, donde $1+ g(s) = \pm 1$, para todo *s*. Temos uma contradição, pois *g(s)* não é constante. □

Nota: *O teorema anterior refere-se a polinômios numa variável. Os trabalho de Putnam, Davis, Robison e Matijasevic conduziram a uma surpreendente conclusão:* ***Existe um polinômio de coeficientes inteiros, tal que o conjunto dos números primos coincide com o conjunto dos valores positivos assumidos por esse polinômio, quando as variáveis percorrem o conjunto***

> ***dos inteiros positivos.***
> *Jones, Sato, Wada e Wiens (1976) foram os primeiros a escrever, explicitamente, um polinômio desse tipo, de grau 25 e com 26 varáveis. [Ribombim]*

Leitura: **Uma Fórmula que Fornece todos os Números Primos**

Sejam x e y números naturais, $y \neq 0$ e $a = x(y + 1) - (y!+ 1)$.

A fórmula que dá todos os números primos e somente esses é:

f(x, y) = $\frac{y-1}{2}\ [|a^2 - 1| - (a^2 - 1)] + 2.$

Por exemplo:

Se x = 1 e y = 1, então a = 0 e f(1,1) = 2;

Se x = 1 e y = 2, então a = 0 e f(1,2) = 3;

Se x = 1 e y = 3. então a = –3 e f(1,3) = 2;

e, atribuindo-se a x e a y mais alguns valores, percebe-se logo que a função f tem uma predileção muito grande pelo número primo 2. Mas ela fornece **todos** os números primos:

5 = f (5,4); 7 = f (103,6); 11= f (329891,10); 13 = f (36846377, 12); ....

Como foram achados os pares (x,y) acima? A resposta é simples: para obter o número primo p, calcule f(x,y) para

$$x = \frac{(p-1)! + 1}{p} \ e \ y = p - 1$$

Assim, para obter 13, fizemos

$$x = \frac{(13-1)! + 1}{13} = 36846277 \ e \ y = 13 - 1 = 12$$

Como se vê, a fórmula existe, mas não é nada prática, uma vez que envolve cálculos com números muito grandes(RPM 37).

A demonstração dessa fórmula será vista após estudarmos o Teorema de Wilson.

7.9. Decomposição do Fatorial em Fatores Primos

Mostraremos como achar a fatoração em números primos de *n*! onde *n* é um número natural arbitrário.

Proposição 7.2: Sejam $a \geq 0$ e $b, c > 0$. Temos que

$$\left\lfloor \frac{\frac{a}{b}}{c} \right\rfloor = \left\lfloor \frac{a}{bc} \right\rfloor$$

Demonstração: Sejam.

$$q_1 = \left\lfloor \frac{a}{b} \right\rfloor \quad e \quad q_2 = \left\lfloor \frac{\frac{a}{b}}{c} \right\rfloor$$

Logo,

$$a = bq_1 + r_1 \text{ , com } r_1 \leq b - 1$$

e

$$\left\lfloor \frac{a}{b} \right\rfloor = q_1 = cq_2 + r_2 , \qquad com \ r_2 \leq c - 1$$

portanto,

$$a = bq_1 + r_1 = b(cq_2 + r_2) + r_1 = bcq_2 + br_2 + r_1$$

como

$$br_2 + r_1 \leq b(c - 1) + b - 1 = bc - 1$$

segue-se que é o quociente da divisão de a por bc, ou seja,

$$q_2 = \left\lfloor \frac{a}{bc} \right\rfloor$$

Dados um número primo *p* e um número natural m, vamos definir por $E_p\,(m)$ o expoente da maior potência de *p* que divide m, ou seja, é o expoente da potência de *p* que aparece na fatoração de *m* em fatores primos.
Em particular, $E_p\,(n!)$ representará a potência de *p* que aparece na fatoração de *n!* em fatores primos.

Teorema de Legendre. Sejam m um número natural e *p* um número primo. Então

$$E_p\,(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ ...$$

Demonstração: Note, inicialmente, que a soma acima é finita, pois existe um número natural *r* tal que $p^i > n$ para todo i > r portanto $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$, se i ≥ r

Vamos demonstrar o resultado por indução sobre n . A fórmula vale trivialmente para $n = 0$. Suponha que o resultado vale para qualquer natural *m* com $m < n$ Sabemos que os múltiplos de *p* entre 1 e *n* são:

$$p, 2p, ..., \left\lfloor \frac{n}{p} \right\rfloor p$$

Portanto, pela hipótese de indução, temos que

$$E_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + E_p\left(\left\lfloor \frac{n}{p} \right\rfloor !\right)$$

O resultado, agora, decorre da preposição 7.2.
Para calcular E_p (n!) faz-se uso do seguinte algoritmo:

$$n = pq_1 + r_1$$

$$q_1 = pq_2 + r_2$$

.....

$$q_{s-1} = pq_s + r_s$$

Como $q_1 > q_2 > ...$, seguem-se que, para alguns *s*, tem-se que. Portanto, seguem-se que.

$E\ (n!) = q_1 + q_2 + ... + q_s$

Exemplo: Vamos determinar a decomposição de 10! Em fatores primos.

Para resolvermos o problema, devemos achar $E_p\ (10!)$ para todo primo $p \leq 10$. Sendo

$$E_2(10!) = \left\lfloor \frac{10}{2} \right\rfloor + \left\lfloor \frac{10}{2^2} \right\rfloor + \left\lfloor \frac{10}{2^3} \right\rfloor = 5 + 2 + 1 = 8,$$

$$E_3(10!) = \left\lfloor \frac{10}{3} \right\rfloor + \left\lfloor \frac{10}{3^2} \right\rfloor = 3 + 1 = 4,$$

$$E_5(10!) = \left\lfloor \frac{10}{5} \right\rfloor = 2,$$

$$E_7(10!) = \left\lfloor \frac{10}{7} \right\rfloor = 1,$$

Seguem-se que

$10! = 2^8 3^4 5^2 7$.

Lema 7.1. Sejam $a_1,..., a_m$,*b* inteiros positivos. Tem–se que

$$\left\lfloor \frac{a_1 + a_2 + \cdots + a_m}{b} \right\rfloor \geq \left\lfloor \frac{a_1}{b} \right\rfloor + \cdots + \left\lfloor \frac{a_m}{b} \right\rfloor$$

Demonstração: Sejam q_i e r_i respectivamente o quociente e o resto da divisão de a_i por b para i = 1, ..., m. somando, membro a membro, as igualdade $a_i = bq_i + r_i$ temos que

$$a_1 + ... + a_m = (q_1 + ... + q_m)\, b + r_1 + ... + r_m$$

Segue–se dai que o quociente da divisão de $a_1 + ... + a_m$ por b é maior ou igual do que $q_1 + ... + q_m$ pois $r_1 + ... + r_m$ poderia superar b – 1 . Isto é o que se queria provar.

Corolário 7.8. Se $a_1,..., a_m, b$ são números naturais com $b \neq 0$, então é natural o número

$$\frac{(a_1 + \cdots + a_m)!}{a_1! \ldots a_m!}$$

Demonstração: De fato, pelo Lema 7.1, para todo número primo P e todo número natural i, temos que

$$\left\lfloor \frac{a_1 + \cdots + a_m}{p^i} \right\rfloor \geq \left\lfloor \frac{a_1}{p^i} \right\rfloor + \cdots + \left\lfloor \frac{a_m}{p^i} \right\rfloor$$

Somando, membro a membro, as desigualdades acima, obtemos que

$$E_p\,((a_1 + ... + a_m)!) \geq E_p\,(a_1\,!) + \ ... + E_p\,(a_m)$$

O que prova o resultado.

O próximo resultado relacionará E_p (n!) e a representação p-ádica de n (i.e., a representação relativa à base p)

Teorema 7.12. Sejam *p,n* inteiros positivos, com *p* primo. Suponha que.

$$n = n_r p^r + n_{r-1} p^{r-1} + ... + n_1 p + n_o$$

Seja a representação p – ádica de n . Então.

$$E_p(n!) = \frac{n - (n_0 + n_1 + \cdots + n_r)}{p - 1}$$

Demonstração: Sendo $0 \leq n_i \leq p$, temos que

$$\left\lfloor \frac{n}{p} \right\rfloor = n_r p^{r-1} + n_{r-1} p^{r-2} + \cdots + n_2 p + n_1$$

$$\left\lfloor \frac{n}{p^2} \right\rfloor = n_r p^{r-2} + n_{r-1} p + \cdots + n_2$$

$$\left\lfloor \frac{n}{p^r} \right\rfloor = n_r$$

Portanto,

$$E_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \left\lfloor \frac{n}{p^r} \right\rfloor =$$

$$n_r \frac{p-1^r}{p-1} + n_{r-1} \frac{p^{r-2}-1}{p-1} + \cdots + n_1 =$$

$$\frac{n_r p^r + n_{r-1} p^{r-1} + \cdots + n_{1p} + n_0 - (n_r + n_{r-1} + \cdots + n_1 + n_0)}{p-1} =$$

$$\frac{n - (n_0 + n_1 + \cdots + n_r)}{p-1}$$

Exemplo: Seja determinar a potência de 3 na decomposição de 53! em fatores primos. Primeiramente escrevemos 53 na base 3, isto é:

$53 = (1222)_3$

Aplicando o Teorema 7.12

$$E_3(53!) = \frac{53 - (1+2+2+2)}{3-1} = 23$$

Verificando esse resultado pelo Teorema de Lagrange:

$$E_3(53!) = \left\lfloor \frac{53}{3} \right\rfloor + \left\lfloor \frac{53}{3^2} \right\rfloor + \left\lfloor \frac{53}{3^3} \right\rfloor = 17 + 5 + 1 = 23$$

7.10. Método da Fatoração de Fermat

Até o momento, um dos procedimentos matemáticos mais difíceis é o de fatorar um número arbitrariamente grande e isso às vezes requer um tempo razoável. Para os casos mais simples podemos usar os conhecidos testes de divisibilidade, mas fatorar números grandes é objeto de intensas pesquisas matemáticas. Damos uma aqui um uma ideia desse difícil problema matemático, utilizando o chamado método da Fatoração de Fermat. Em cursos mais avançados outros métodos são apresentados.

Proposição 7.3: Seja *n* > 1 um inteiro ímpar. Há uma correspondência biunívoca entre a fatoração de n e a representação de n como diferença de dois quadrados.

Demonstração:

Se n = a.b, e n ímpar, então a e b são ímpares. Logo a+b e a-b são pares, então $\frac{a+b}{2}$ e $\frac{a-b}{2}$ são inteiros.
Então,

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

Expressa n como a diferença de dois quadrados.
Reciprocamente, suponha n escrito como a diferença de dois quadrados:
$n = s^2 - t^2$, então n = (s-t) . (s+t) é a forma fatorada de n.
Você pode ver que esses dois procedimentos – da fatoração para a diferença e da diferença para a fatoração – determinam uma relação biunívoca.

7.11 – Algoritmo de Fermat

A proposição acima nos permite descrever um algoritmo, que é muito eficiente quando n tem um fator primo que não é muito menor que $\sqrt{n}$.

Para começar vamos supor que n é ímpar, já que se n for par então 2 é um de seus fatores. A idéia do algoritmo de Fermat é tentar achar números inteiros positivos x e y tais que $n = x^2 - y^2$. Supondo que encontramos estes números, temos que

$$n = x^2 - y^2 = (x - y)\,(x + y).$$

Logo x - y e x + y são fatores de n.
O caso mais fácil do algoritmo de Fermat ocorre quando n é um quadrado perfeito; isto é, quando existe algum inteiro r tal que $n = r^2$. Neste caso temos que r é fator de n. Além disso, na notação acima x = r e y = 0. Observe que se y > 0 então

$$x = \sqrt{n + y^2} > \sqrt{n}$$

Isto sugere a seguinte estratégia para encontrar x e y.

Entrada: inteiro positivo ímpar n.

Saída: um fator de n ou uma mensagem indicando que n é primo.

Etapa 1: Comece com $x = \lfloor \sqrt{n} \rfloor$; se $n = x^2$ então x é fator de n e podemos parar.

Etapa 2. Caso contrário incremente x de uma unidade e calcule $y = \sqrt{x^2 - n}$.

Etapa 3. Repita a Etapa 2 até encontrar um valor inteiro para y, ou até que x seja igual a $\frac{(n+1)}{2}$: no primeiro caso n tem fatores x+y e x-y, no segundo n é primo.

Exemplo: Seja n = 1342127 o número obtido como produto de dois primos. A variável x é inicializada com a menor parte inteira da raiz quadrada de n $\left(\left\lfloor\sqrt{1342127}\right\rfloor = 1158\right)$. Mas x^2 = 1158^2 = 1340964 < 1342127 logo passamos a incrementar x de um em um. Fazemos isso até que $\sqrt{x^2 - n}$ seja inteiro, ou x seja igual a $\frac{(n+1)}{2}$, que neste caso valeria 671064. É mais fácil resumir isto em uma tabela

x	$\sqrt{x^2 - n}$
1159	33,97
1160	58,93
1161	76,11
1162	90,09
1163	102,18
1164	113

Obtivemos assim um inteiro no sexto laço. Portanto x = 1164 e y = 113 são os valores desejados. Os fatores correspondentes são x + y = 1277 e x – y = 1051. Logo, 1051 e 1277 são os dois números primos procurados.

EXERCÍCIOS

1. Com uma calculadora, achar todos os primos da forma $n^2 - 2$, para $25 \leq n \leq 35$

2. Determine todos os primos que são iguais a diferença de quadrado entre dois primos.

3. De quantos modos podem escrever 497 como a soma de dois números primos?

4. Mostrar que a soma de dois inteiros positivos ímpares e consecutivos nunca é um primo.

5. Em um quadro estão escritos alguns números naturais. Dentre eles, há nove múltiplos de 4, sete múltiplos de 6, cinco múltiplos de 12, três números primos e nada mais. Qual a quantidade mínima de números escritos?

6. Achar todos os primos p e q, tais que $p - q = 3$.

7. Achar todos os primos que são iguais a um quadrado menos 1.

8. Achar todos os primos que são iguais a um cubo menos 1.

9. Escreva os números 55, 83 e 211 como uma soma de três primos.

10. Determinar todos os inteiros positivos n tais que n, n + 2 e n + 4 são todos primos.

11. Determinar todos os primos p tais que 3p + 1 é um quadrado.

12. Com uma calculadora, determinar se são primos os números

    a) 1699
    b) 7429
    c) 21793
    d) 1189

13. Encontre todos os primos p, tais que 17p + 1 é um quadrado.

14. Usando a decomposição em fatores primos dos inteiros 507 e 1287, achar o mdc (507, 1287) e o mmc (507, 1287).

15. Achar o mdc(a, b) e mmc(a, b) sabendo a = 230 . 521 . 19 . 233 e b = 26 . 3 . 74 . 112 . 195 . 237

16. Achar o menor inteiro positivo pelo qual se deve dividir 15! para se obter um quadrado.

    - Qual o menor valor do número natural n que torna n! divisível por 1000?

17. Achar todos os primos que são divisores de 50!.

18. Verifique com uma calculadora, se são primos gêmeos:

    a) 1949 e 1951
    b) 1997 e 1999

19. Achar uma sequência de quatro inteiros positivos consecutivos e compostos.

20. Achar um sequência de 100 inteiros positivos consecutivos e compostos.

21. Mostre que nenhum número inteiro da forma $1+4^n$ é divisível pelo número primo 3.

22. Com uma calculadora, verificar a conjectura de Goldbach para n par, $42 \leq n \leq 100$.

23. Determinar o menor valor positivo do inteiro n tal que $2n^2 + p$, seja um número inteiro composto e p um primo terminado em 7.

24. Demonstrar que todo primo, $p \geq 5$ é da forma 6k – 1 ou 6k + 1, onde k é um inteiro positivo.

25. Demonstrar que todo primo $p \geq 3$, é da forma 4k + 1 ou 4k – 1, onde k é um inteiro positivo.

26. Determine todos os primos $p \geq 5$tais que $8p^4$ - 3003 também seja primo.

27. Mostrar que todo inteiro da forma $n^4 + 4$, com n > 1 não é primo.

28. Mostrar que todo inteiro da forma $8^n + 1$, com n > 1, não é primo.

29. Mostrar que se $n^2 + 2$ é primo então 3 | n, para todo n > 1.

30. Se p > 5 é um primo, então $p^2 + 2$ é composto.

31. Demonstrar as seguintes propriedades:

a) Todo primo da forma 3n + 1 é também da forma 6m + 1.
b) Todo inteiro n > 11 pode ser expresso como a soma de dois inteiros não-primos.
c) Se $p \neq 5$ é um primo ímpar, então $p^2 - 1$ ou $p^2 + 1$ é divisível por 10.
d) Se p > q > 5 e se p e q são ambos primos, então $24 \mid p^2 - q^2$.
e) Todo inteiro da forma 3n + 2 tem um fator primo desta forma.
f) Se p é um primo e se $p \mid a^n$, então $p^n \mid a^n$.

32. Demonstrar que o inteiro positivo a > 1 é um quadrado se e somente se todos os expoentes dos fatores primos da sua decomposição são inteiros pares.

33. Demonstrar que, se o inteiro $k \geq 2$, não é primo, então $2^k - 1$ nunca será primo.

34. Demonstrar que se $2^k - 1$, ($k \geq 2$) é primo, então k também é primo.

35. Seja p o maior fator primo do número $3^{14} + 3^{13} - 12$, então p é igual a:

36. Sejam p, q inteiros positivos. Mostre que $2^p + 1 = q^2$ implica p e q primos e p = q = 3.

37. Mostrar que um inteiro da forma $4^{2n+1} + 1$, onde $n \geq 1$, nunca é primo.

38. Sendo n um inteiro positivo, mostre que $2^{4(n+1)} - 1$ nunca será primo.

39. Mostrar que se n > 4, não é primo, então n divide (n – 1)!.

40. Verificar que todo inteiro pode escrever-se sob a forma 2^k m, onde o inteiro k > 0 e m é um inteiro ímpar.

41. Demonstrar que, se o inteiro n > 2, então existe um primo p tal que n < p < n!.

42. Qual é o menor número primo que um fator da soma $1999^{2002} + 2001^{2002}$?

43. Prove que um triângulo retângulo não pode apresentar as medidas de seus lados sendo números primos.

44. Se p e $8p^2 + 1$ são números primos, prove que p = 3.

45. Mostre que se $n \geq 1$ é natural então, o número $2^{2^{2n+1}}$ não é primo.

46. Sendo n > 1 um inteiro, prove que $4^n + n^4$ não é primo.

47. Mostrar, mediante um exemplo, que a seguinte conjectura é falsa:
"Todo inteiro positivo maior que 1, pode-se escrever sob a forma $a^2 + p$, com a > 0 e p é um inteiro primo ou 1".

48. Determine todos os números primos p e q, para os quais os q números p, p + (q + 1), p + 2 (q + 1), p + 3 (q + 1), . . . , p + (q − 1) (q + 1), também são primos.

49. Demonstrar que existem infinitos primos da forma 4n + 3, com n inteiro positivo.

50. Seja m um intero positivo. Demonstre que não existem números primos da forma $2^{5m} + 2^m + 1$.

51. Determinar o número inteiro positivo n que que é produto dos primos p, q e r, sabendo que r - q = 2p e $rq + p^2 = 676$.

52. Mostre que existem infinitos valores primos p para os quais $8.p^2 + 5$ é divisível por 77.

53. Seja p > 2 um primo. Determine todos os valores inteiros positivos de m e n, tal que $(p - 1)(p^n + 1) = 4m(m + 1)$.

> ➢ Nos problemas que se seguem faça uso de uma calculadora para verificar os resultados e explicite bem os passos utilizados na resolução.

54. Segundo o Teorema de Chebychev, para um inteiro $m \geq 2$, existe um primo p tal que $m < p < 2m$. Determine todos os primos entre 600 e 1200.

55. Segundo o Teorema de Dirichlet, se o mdc (a, b) =1, então existem infinitos primos da forma an+b com n um inteiro positivo. Determine todos os primos p da forma 4n+9, com $88 < 4n + 9 < 388$.

56. Usando o Teorema de Sierpinski, determine um primo p>19 e escreva 20 inteiros compostos.

57. Usando a Fórmula de Minàc, determine $\pi(12)$.

58. Usando a Fórmula do n-ésimo número primo, determine o quarto número primo.

59. Calcule:
a) $\left\lfloor \frac{3\#.5\# + 7\#}{11\#} \right\rfloor$

b) $\left\lfloor \frac{5\#.7\# + 11\#}{13\#} \right\rfloor$

60. Verifique se existem primos gêmeos entre 600 e 700.

61. Determine dois números primos consecutivos tais que a diferença entre eles seja maior que 7.

62. Decomponha 98! Em fatores primos.

63. Determine a potência de 5 na decomposição de 75! em fatores primos, fazendo a decomposição p-ádica de 75.

64. Com quantos zeros termina o número 1000! ? Qual é a potência de 3 que aparece na decomposição de 1000! em fatores primos?

65. Justifique se o número $\frac{93.94.\ldots.112.113}{21!}$ é inteiro. Em caso afirmativo, calcule o seu valor.

66. Encontrar o maior valor do inteiro $n \geq 0$ tal que $\frac{10200!}{504^n}$ seja inteiro.

67. Utilizando o Teorema do Número Primo:

a) Faça uma estimativa (sem muito rigor) de quantos primos de 200 dígitos existem.
b) Mostre que entre os números de k-dígitos, um em cada 2, 3k é primo.

68. Qual o menor valor do número natural n que torna n! divisível por 1000?


UEPA
UNIVERSIDADE DO ESTADO DO PARÁ