

**MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
DE GOIÁS - CÂMPUS VALPARAÍSO**

CURSO DE LICENCIATURA EM MATEMÁTICA

NÚMEROS INTERESSANTES E RESULTADOS ASSOCIADOS

ISRAEL DA SILVA FERNANDES

VALPARAÍSO - GOIÁS

2021

ISRAEL DA SILVA FERNANDES

NÚMEROS INTERESSANTES E RESULTADOS ASSOCIADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Matemática do Instituto Federal de Goiás - IFG - Câmpus Valparaíso, como requisito parcial para obtenção do título de Licenciado em Matemática.

Área de Concentração: Álgebra

Orientadora: M.e Professora Mayra Camelo Madeira de Moura

VALPARAÍSO - GOIÁS

2021

Ficha catalográfica elaborada pelo bibliotecário Helio Lino Delfino (CRB-1/3031),
com os dados fornecidos pelo(a) autor(a).

F363n

Fernandes, Israel da Silva
Números interessantes e resultados associados / Israel
da Silva Fernandes. -- Valparaíso, 2021.
80 f. : il.

Orientadora: Mayra Camelo Madeira de Moura.
TCC (Graduação - Licenciatura em Matemática) -
- Instituto Federal de Goiás, Campus Valparaíso
de Goiás, 2021.

1. Teoria dos números - matemática. 2. Álgebra. 3.
Números interessantes - matemática. I. Moura, Mayra
Camelo Madeira de. II. Título.

CDD 510



INSTITUTO FEDERAL
Goiás

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
SISTEMA INTEGRADO DE BIBLIOTECAS

TERMO DE AUTORIZAÇÃO PARA DISPONIBILIZAÇÃO NO REPOSITÓRIO DIGITAL DO IFG - ReDi IFG

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia de Goiás, a disponibilizar gratuitamente o documento no Repositório Digital (ReDi IFG), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IFG.

Identificação da Produção Técnico-Científica

- | | |
|--|---|
| ☐ Tese | ☐ Artigo Científico |
| ☐ Dissertação | ☐ Capítulo de Livro |
| ☐ Monografia – Especialização | ☐ Livro |
| ☒ TCC - Graduação | ☐ Trabalho Apresentado em Evento |
| ☐ Produto Técnico e Educacional - Tipo: _____ | |

Nome Completo do Autor: Israel da Silva Fernandes

Matrícula: 20171150040185

Título do Trabalho: "Números interessantes e resultados associados."

Autorização - Marque uma das opções

- ☒ Autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso aberto);
- ☐ Autorizo disponibilizar meu trabalho no Repositório Digital do IFG somente após a data ____/____/____ (Embargo);
- ☐ Não autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso restrito).

Ao indicar a opção 2 ou 3, marque a justificativa:

- ☐ O documento está sujeito a registro de patente.
☐ O documento pode vir a ser publicado como livro, capítulo de livro ou artigo.
☐ Outra justificativa: _____

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O/A referido/a autor/a declara que:

- o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
- obteve autorização de quaisquer materiais incluídos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia de Goiás os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
- cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

Volpiano de Goiás 07 05 2021
Local Data

Israel da Silva Fernandes
Assinatura do Autor e/ou Detentor dos Direitos Autorais



INSTITUTO FEDERAL
Goiás

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE GOIÁS
CÂMPUS VALPARAÍSO

Termo de Aprovação

ISRAEL DA SILVA FERNANDES

NÚMEROS INTERESSANTES E RESULTADOS ASSOCIADOS

Trabalho de Conclusão de Curso apresentado a Coordenação do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia de Goiás – Câmpus Valparaíso de Goiás, como parte dos requisitos para a obtenção do título de Licenciado/Licenciada em Matemática.

Monografia defendida e aprovada, em dez de março de 2021, pela banca examinadora constituída pelos seguintes membros:

BANCA EXAMINADORA

Profa. Ma. Mayra Camelo Madeira de Moura
Presidente da banca / Orientador(a)
Instituto Federal de Educação, Ciência e Tecnologia de Goiás

Prof. Dr. Bruno de Paula Miranda
Instituto Federal de Educação, Ciência e Tecnologia de Goiás

Prof. Dr. Hiuri Fellipe Santos dos Reis
Instituto Federal de Educação, Ciência e Tecnologia de Goiás

Valparaíso de Goiás – GO

2021

Documento assinado eletronicamente por:

- Bruno de Paula Miranda, PROFESSOR ENS BASICO TECN TECNOLÓGICO, em 12/03/2021 08:04:51.
- Hiuri Fellipe Santos dos Reis, PROFESSOR ENS BASICO TECN TECNOLÓGICO, em 11/03/2021 19:28:41.
- Mayra Camelo Madeira de Moura, PROFESSOR ENS BASICO TECN TECNOLÓGICO, em 11/03/2021 09:58:46.

Este documento foi emitido pelo SUAP em 09/03/2021. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifg.edu.br/autenticar-documento/> e forneça os dados abaixo:

Código Verificador: 138810

Código de Autenticação: d128a1554c



BR 040, KM 6, Avenida Saia Velha, S/Nº, Área 8, Parque Esplanada V, VALPARAÍSO DE GOIÁS / GO, CEP 72876-601
(61) 3615-9200 (ramal: 9200)

Dedicatória

À meus pais que sempre foram e sempre serão os maiores incentivadores de todas as minhas conquistas.

Agradecimentos

“Tu formaste o íntimo do meu ser e me teceste no ventre de minha mãe. Graças te dou pela maneira extraordinária como fui criado! Pois tu és tremendo e maravilhoso! Sim, minha alma o sabe muito bem.”(BÍBLIA, Salmos, 139, 13-14). Agradeço a Deus pois foi Ele quem me deu forças quando eu pensei que não ia conseguir, me acalmou quando eu não estava bem com tanta coisa para fazer em tão pouco tempo e, em toda minha graduação e vida, sempre foi minha rocha, meu abrigo, foi aquele para quem eu sempre recorri independente se eu estava na melhor ou na pior. E por nunca ter desistido de mim, meu primeiro agradecimento é a Ele.

Palavras me faltam também ao agradecer meus pais Sr. Carlos Alberto e Sra. Francisca Antônia por, em toda a minha vida, nunca terem me deixado faltar nada, sempre terem batalhado muito - MUITO - para que eu sempre tivesse o melhor que eles pudessem me dar. Mas acima de tudo que o dinheiro pode comprar, eu sou grato pelo amor que vocês nunca deixaram faltar e, inclusive, sempre me dão em sobra. Aproveito também para agradecer meus irmãos Ezequiel e Isabela e Ludimila por sempre me ajudarem - mesmo nas coisas mais simples - e manterem nossa família unida sempre com bons jogos e risadas.

Agradeço também a minha orientadora, professora Mayra Madeira, que acreditou em mim e no meu projeto e me ajudou a trilhar toda essa jornada de escrita. Por mais que eu tenha “lerdado”às - muitas - vezes, obrigado por não ter desistido de mim e do meu projeto e por sempre me ajudar a chegar no “glow up”. Desejo muito tornar-me um profissional e uma pessoa como tu és, que faz com que os outros se sintam bem e em paz e apaixonem-se também pelo que estarei ensinando. MUITÍSSIMO obrigado mesmo.

Não poderia deixar de agradecer a meus amigos que sempre estiveram me apoiando, nunca me deixaram desistir (literalmente porque o tanto que eles “brigavam” comigo para continuar, não foi pouco) e sempre estiveram presentes, mesmo que eu estivesse correndo com tudo, sempre mandavam uma mensagem ou apareciam em casa do nada, ou me chamavam para sair para algum lugar. Vocês foram - e são - extremamente fundamentais para mim em todos os meus processos e eu espero nunca perder vocês. Danilo, Bruna, Marthus, Taiane, Matheus, Karol, Ruth, Rute, Jheison, Rayssa, Brenda, Fernando, Giovanna, Júnior, Moura: Obrigado e Amo Vocês!

Por fim, agradeço a todos que, direta ou indiretamente, participaram da minha formação até aqui e a você leitor o meu Muito Obrigado.

Resumo

O presente trabalho tem como objetivo ser um compêndio dos principais resultados e problemas em aberto gerados por determinados números que possuem propriedades interessantes. Os números interessantes selecionados para este trabalho foram os números amigos, números primos gêmeos e os números perfeitos. Para a realização desse compêndio, estudamos conteúdos da teoria dos números que nos serviram de base no desenvolvimento dos resultados. Daí, partimos para o estudo da busca por pares de números amigos, desde fórmulas que geram apenas um par, até as que geram vários. Seguimos estudando os números primos gêmeos e a conjectura em aberto que os permeia assim como os resultados associados a tal conjectura. Terminamos estudando os números perfeitos e os teoremas que utilizam da ideia de tais números em suas demonstrações. Para todos os números interessantes supracitados, foram apresentados teoremas ou conjecturas que necessitam da demonstração dos respectivos números interessantes para que sejam demonstrados ou, ainda, problemas decorrentes do estudo de tais números.

Palavras-chave: Números Interessantes. Números Amigos. Números Primos Gêmeos. Números Perfeitos. Teoria dos Números.

Abstract

The present work aims to be a compendium of the main results and open problems generated by certain numbers that have interesting properties. The interesting numbers selected for this work were friendly numbers, twin prime numbers and perfect numbers. To carry out this compendium, we studied the contents of numbers theory that served as a basis for the development of the results. Hence, we go on to study the search for pairs of friendly numbers, from formulas that generate only one pair, to those that generate several. We continue to study the twin prime numbers and the open conjecture that permeates them as well as the results associated with such a conjecture. We ended up studying the perfect numbers and the theorems that use the idea of such numbers in their statements. For all of the aforementioned interesting numbers, theorems or conjectures were presented that require the demonstration of the respective interesting numbers in order to be demonstrated or, still, problems arising from the study of such numbers.

Keywords: Interesting numbers. Friendly numbers. Twin Prime Numbers, Perfect Numbers. Numbers Theory.

Conteúdo

1	Introdução	1
2	Resultados Essenciais	3
2.0.1	Indução	3
2.0.2	Divisibilidade	4
2.0.3	O Algoritmo da Divisão	4
2.0.4	O Máximo Divisor Comum	5
2.0.5	O Algoritmo de Euclides	8
2.0.6	Números Primos	9
2.0.7	Mínimo Múltiplo Comum	12
2.0.8	Critérios de Divisibilidade	19
2.0.9	Congruência	21
2.0.10	Congruência Linear	26
2.0.11	Soma de divisores	29
2.0.12	Funções Aritméticas	29
2.0.13	Os Teoremas de Euler, Fermat e Wilson	30
3	Números Interessantes e Resultados Associados	34
3.1	Números Amigos	34
3.1.1	Resultados Essenciais	39
3.1.2	Problemas em aberto	48
3.2	Números Primos Gêmeos	50
3.2.1	Resultados Essenciais	52

3.2.2	Problemas em aberto	56
3.3	Números Perfeitos	58
3.3.1	Resultados Essenciais	59
3.3.2	Problemas em aberto	68
4	Conclusão	72
A	Apêndice	78

Introdução

Existem várias formas de analisarmos dados históricos e para que uma análise seja, de fato, uma colaboração teórico relevante, é imprescindível que as fontes analisadas sejam de confiança. Entendemos que quanto mais se aprofunda em estudos de um determinado assunto, mais vai se conhecendo dele e até desmentindo teorias que, até o momento, eram tidas como verdade.

Ainda assim, para encontrarmos a solução de determinado problema é imprescindível que nos apoiemos nos conhecimentos de pessoas que contribuíram antes de nós no intuito de termos uma base na construção de novas afirmações como disse Morman (1992, p 205, apud HANKEL, 1889, P 25): “Na maioria das ciências, uma geração destrói o que a outra havia construído e o que uma estabilizou, a outra desfaz. Na Matemática, uma geração constrói uma nova história para as antigas estruturas.” ou seja, os conhecimentos matemáticos são sempre acrescidos e utilizados nas mais variadas demonstrações e não simplesmente esquecidos.

Segundo José Plínio, o objetivo central da Teoria dos números é o estudo das propriedades dos números inteiros positivos (PLÍNIO, 1998). Assim sendo, o objetivo desse trabalho é fazer um compêndio dos principais resultados associados a determinados números com propriedades interessantes e o objetivo específico é apresentar resultados que buscam solucionar problemas em abertos dos números que serão estudados. Os números interessantes selecionados para aprofundamento neste trabalho foram os números primos gêmeos, números amigos e números perfeitos. Buscamos não somente encontrar os resultados provados que envolvem tais números, como também os principais problemas em aberto de cada um e que já existem teoremas e conjecturas apenas esperando tais provas para serem demonstrados.

Inicialmente, serão abordados conteúdos da teoria dos números que nos servirão de base na compreensão dos próximos resultados. Em seguida, estudaremos os números interessantes selecionados desde a definição até determinadas leis de existência e formação. Apresentamos os principais problemas em aberto de cada um desses números e os teoremas que foram propostos para a resolução de tais problemas incluindo, também, aqueles que dependem da prova dos teoremas em aberto para serem demonstrados.

Os resultados foram obtidos através de uma pesquisa documental em diversos livros e trabalhos acadêmicos, todos disponibilizados online.

Capítulo 1

Resultados Essenciais

1.0.1 Indução

Definição 1 (Princípio da Boa Ordenação - PBO). *Todo conjunto não-vazio de inteiros positivos contém um elemento minimal.*

Proposição 1 (Princípio da Indução Finita). *Seja B um subconjunto dos inteiros positivos. Se B possui as duas seguintes propriedades*

(i) $1 \in B$;

(ii) $k + 1 \in B$ sempre que $k \in B$

ou, podemos reescrever o item (ii) como

(ii) $k + 1 \in B$ sempre que $1, 2, \dots, k \in B$

Então B contém todos os inteiros positivos.

Demonstração. Suponhamos, por contradição, que B não contém todos os inteiros positivos e seja A o conjunto dos inteiros positivos que não pertencem a B . Como valem as propriedades (i) e (ii), então $1 \in B$ logo, pelo PBO, A contém um menor elemento que é maior que 1, que vamos denotar por a_0 . Portanto $a_0 - 1 \in B$, pois a_0 é o menor elemento de A . Então o sucessor de $a_0 - 1$ também deve estar em B . O que é uma contradição. Logo, A tem que ser vazio! □

1.0.2 Divisibilidade

Falaremos agora da divisão entre inteiros e de algumas características e propriedades que a divisibilidade possui. Assim sendo:

Definição 2. *Se a e b são inteiros, dizemos que a divide b , denotando por $a|b$, se existir um inteiro c tal que $b = ac$.*

Proposição 2. *Se a, b e c são inteiros, $a|b$ e $b|c$, então $a|c$.*

Demonstração. Como $a|b$ e $b|c$, por definição, existem inteiros k_1 e k_2 tal que $b = k_1a$ e $c = k_2b$. Substituindo o valor de b na equação $c = k_2b$, teremos $c = k_1k_2a$, o que implica que $a|c$. $\square$

Proposição 3. *Se a, b, c, m e n são inteiros, $c|a$ e $c|b$ então $c|(ma + nb)$.*

Demonstração. Se $c|a$, então $a = k_1c$ e se $c|b$, então $b = k_2c$, por definição. Multiplicando essas equações por m e n respectivamente, teremos $ma = mk_1c$ e $nb = nk_2c$. Somando-as, obteremos $ma + nb = mk_1c + nk_2c = (mk_1 + nk_2)c$. O que implica que $c|(ma + nb)$. $\square$

1.0.3 O Algoritmo da Divisão

Teorema 1. *Dados dois inteiros a e b , com $b > 0$, existe um único par de inteiros q e r , tais que $a = qb + r$, com $0 \leq r < b$ ($r = 0 \Leftrightarrow b|a$) onde q é chamado de quociente e r de resto da divisão de a por b .*

Esse teorema será demonstrado tomando por base o seguinte teorema:

Teorema 2. *(de Eudoxius) Dados dois inteiros a e b , com $b \neq 0$, então a é um múltiplo de b ou se encontra entre dois múltiplos consecutivos de b . Assim, se $b > 0$ temos $qb \leq a < (q + 1)b$ e se $b < 0$ temos $qb \geq a > (q - 1)b$.*

Demonstração. (Teorema 1) O primeiro passo dessa demonstração é a Existência:

Pelo Teorema de Eudoxius, como $b > 0$, existe um q que satisfaz:

$$qb \leq a < (q + 1)b$$

Separando e subtraindo qb em ambos lados, temos que $0 \leq a - qb$ e $a - qb < b$. Assim, chamando $r = a - qb$, o que implica que $a = qb + r$ e temos a existência de um q e um r .

Vamos agora mostrar Unicidade:

Suponhamos que exista um outro par q_1 e r_1 tal que $q_1b + r_1$ também seja igual a esse a tal que:

$$a = q_1b + r_1 \text{ com } 0 \leq r_1 < b$$

Disto temos que

$$\begin{aligned} a - a &= 0 \\ (qb + r) - (q_1b + r_1) &= 0 \\ b(q - q_1) &= r_1 - r \end{aligned}$$

Logo, pela definição de divisibilidade, $b|(r_1 - r)$. Mas, como $0 < r_1 < b$ e $0 < r < b$, temos $|r_1 - r| < b$.

Portanto, se $0 < r_1 - r < b$, então $b \nmid r_1 - r$ pois, suponhamos que $b|r_1 - r$, então deveria existir um k tal que $b.k = r_1 - r$, o que implicaria que $b < r_1 - r$ o que é uma contradição. Assim, uma vez que $0 < r_1 - r < b$, então $b \nmid r_1 - r$, concluímos que

$$r_1 - r = 0$$

O que implica que

$$r_1 = r$$

Assim sendo,

$$\begin{aligned} q_1b &= qb \\ q_1 &= q \text{ (pois } b \neq 0) \end{aligned}$$

Assim sendo, q e r são únicos. □

1.0.4 O Máximo Divisor Comum

Definição 3. *O máximo divisor comum de dois inteiros a e b (a ou $b \neq 0$): denotado por (a, b) , é o maior inteiro que divide a e b .*

Teorema 3. *Seja d o máximo divisor comum de a e b , então existem inteiros n_0 e m_0 tais que $d = n_0a + m_0b$.*

Demonstração. Seja B o conjunto de todas as combinações lineares $(na + mb)$ onde n e m são inteiros distintos. Uma vez que essas combinações podem gerar números negativos e positivos, definiremos um c como sendo o menor inteiro positivo pertencente ao conjunto B e que seja obtido através da combinação linear de n_0 e m_0 , ou seja $c = n_0a + m_0b$. Vamos provar que $c|a$ e $c|b$ (analogamente).

Então, vamos assumir, por contradição, que $c \nmid a$. Pelas regras de divisibilidade, temos que existem q e r tais que $a = qc + r$ com $0 < r < c$. Ou seja,

$$\begin{aligned} a &= qc + r \\ r &= a - qc \\ r &= a - q(n_0a + m_0b) \\ r &= (1 - qn_0)a + (-qm_0)b \end{aligned}$$

Como $(1 - qn_0)$ e $(-qm_0)$ são inteiros, temos que $r \in B$, o que é uma contradição uma vez que $0 < r < c$ e c é o menor elemento positivo de B .

Daí, sabendo que d é um divisor comum de a e b , então existem inteiros k_1 e k_2 tais que $a = k_1d$ e $b = k_2d$, portanto,

$$\begin{aligned} c &= n_0a + m_0b \\ c &= n_0k_1d + m_0k_2d \\ c &= d(n_0k_1 + m_0k_2) \end{aligned}$$

Logo, $d|c$. Do teorema 1 temos que $d \leq c$, e como $d < c$ não é possível (pois d é o máximo divisor comum), então $d = n_0a + m_0b$ □

Teorema 4. *O máximo divisor comum d de a e b é o divisor positivo de a e b o qual é divisível por todo divisor comum.*

Demonstração. Do Teorema anterior podemos concluir que se d_1 é divisor comum de a e b , então $d_1|d$. Assim sendo, d e d_1 possuem a propriedade de serem divisíveis por todo divisor comum, o que implica que $d_1 = d$. □

Proposição 4. Para todo inteiro positivo t , $(ta, tb) = t(a, b)$.

Demonstração. Da demonstração do teorema 3, (ta, tb) é o menor valor positivo das combinações lineares de $mta + ntb$ (com m e n inteiros). Essa combinação é igual a t vezes o menor valor positivo de $ma + nb = t(a, b)$ $\square$

Proposição 5. Se $c > 0$ e a e b são divisíveis por c , então $(\frac{a}{c}, \frac{b}{c}) = \frac{1}{c}(a, b)$

Demonstração. Sabemos que $\frac{a}{c}$ e $\frac{b}{c}$ são inteiros pois a e b são divisíveis por c . Segue da proposição anterior que basta substituímos “ $\frac{a}{c}$ ” por “ a ”, “ $\frac{b}{c}$ ” por “ b ” e tomar $t = \frac{1}{c}$. $\square$

Corolário 1. Se $(a, b) = d$, temos que $(\frac{a}{d}, \frac{b}{d}) = 1$.

Demonstração. Da proposição anterior tínhamos c sendo um divisor comum de a e b . Se tomarmos agora esse c sendo o máximo divisor comum d , então já está demonstrado. $\square$

Definição 4. Os inteiros a e b são relativamente primos quando $(a, b) = 1$

Teorema 5. Para a, b e x inteiros temos $(a, b) = (a, b + ax)$

Demonstração. Sejam $d = (a, b)$ e $f = (a, b + ax)$. Já vimos que existem inteiros n_0 e m_0 tais que $d = n_0a + m_0b$. Sabendo que podemos escrever a expressão acima como

$$d = a(n_0 - xm_0) + (b + ax)m_0,$$

podemos concluir que o máximo divisor de a e de $b + ax$ também divide d .

Mostramos que $f|d$, agora vamos mostrar que $d|f$. Já sabemos que $d|(b + ax)$ e que todo divisor comum de a e de $b + ax$ também é divisor de f . Logo, como temos que esses são inteiros positivos (com $c > 0$) então temos que $f|d$ e $d|f \implies |d| \leq |f|$, então $d = f$. $\square$

Teorema 6. Se $a|bc$ e $(a, b) = 1$, então $a|c$.

Demonstração. Dado que $(a, b) = 1$, do teorema 3, sabemos que existem inteiros n e m tais que $na + mb = 1$. Se multiplicarmos ambos lados por c , temos

$$n(ac) + m(bc) = c$$

Como $a|ac$ e, por hipótese, $a|bc$ então, $a|c$. $\square$

Teorema 7. Se a e b são inteiros e $a = qb + r$ onde q e r são inteiros, então $(a, b) = (b, r)$.

Demonstração. De $a = qb + r$, por proposição, sabemos que todo divisor de b e r também é um divisor de a . Reescrevendo, temos que $r = a - qb$, logo, todo divisor de a e b é um divisor de r . Ou seja, o conjunto dos divisores de a e b é o mesmo conjunto dos divisores de q e r , logo

$$(a, b) = (b, r)$$

□

1.0.5 O Algoritmo de Euclides

O algoritmo da divisão, criado por Euclides, nos garante que se n e d são inteiros com $d \neq 0$, podemos dividir n por d obtendo um único quociente q e um único resto r , em que $0 \leq r < d$. Mas antes de enunciarmos o teorema e o demonstrarmos, vamos dar um exemplo:

Queremos encontrar o MDC de 1126 e 522. Para isso vamos dividir 1126 por 522, após isso, multiplicaremos o dividendo pelo quociente e somaremos ao resto, assim:

$$1126 = 2 \times 522 + 82 \quad 522 = 6 \times 82 + 30$$

E assim sucessivamente até encontrarmos o resto nulo:

$$82 = 2 \times 30 + 22$$

$$30 = 1 \times 22 + 8$$

$$22 = 2 \times 8 + 6$$

$$8 = 1 \times 6 + 2$$

$$6 = 3 \times 2 + 0$$

Assim sendo, da última equação temos que $(6, 2) = 2$ e, pelo teorema anterior, temos que $(8, 6) = (6, 2)$ e, seguindo nesse raciocínio, voltaremos até que $(82, 522) = (522, 1126)$. Assim sendo, o MDC será o último resto não nulo da sequência de igualdades.

Teorema 8. *Sejam $r_0 = a$ e $r_1 = b$ inteiros não-negativos com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_j = q_j \times r_{j+1} + r_{j+2}$$

Para $j = 0, 1, 2, \dots, n-1$ e $r_{n+1} = 0$ então $(a, b) = r_n$ o último resto não-nulo.

Demonstração. Iniciaremos dividindo $r_0 = a$ por $r_1 = b$, obtendo $r_0 = q_1 r_1 + r_2$.

Em seguida, dividiremos r_1 por r_2 obtendo $r_1 = q_2 r_2 + r_3$. E assim sucessivamente até que, come esse processo, encontremos $r_{n+1} = 0$. Teremos então as seguintes sequências de equações:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \text{ com } 0 < r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3 \text{ com } 0 < r_3 < r_2 \\ r_2 &= q_3 r_3 + r_4 \text{ com } 0 < r_4 < r_3 \\ &\dots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \text{ com } 0 < r_n < r_{n-1} \\ r_{n-1} &= q_n r_n + 0 \text{ com } 0 < r_2 < r_1 \end{aligned}$$

Vemos então que o máximo divisor comum de r_n e r_{n-1} é r_n , ou seja,

$$(r_{n-1}, r_{n-2}) = r_n.$$

Então, prosseguindo repetidas vezes, teremos a sequência:

$$r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \dots = (r_1, r_2) = (r_0, r_1) = (a, b)$$

Assim sendo, o máximo divisor comum será o último resto não nulo da sequência de divisões. □

1.0.6 Números Primos

Dentre os vários problemas existentes na teoria dos números, uma area que sempre despertou e desperta muito a atenção de muitos são os números primos e os vários problemas que são desencadeados a partir deles. Vejamos então sua definição:

Definição 5. Um número inteiro n com $(n > 1)$ possuindo somente dois divisores positivos distintos é chamado número primo. Se $n > 1$ não é primo, dizemos que n é composto.

Proposição 6. Se $p|ab$ e p é primo, então $p|a$ ou $p|b$.

Demonstração. Se $p \nmid a$, então $(a, p) = 1$ o que, pelo teorema 6, implica que $p|b$. $\square$

Teorema 9. *(Teorema Fundamental da Aritmética) Todo inteiro maior que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração. Caso n seja primo, não há o que demonstrar. Vamos então supor um n composto.

Seja p_1 ($p_1 > 1$) o menor dos divisores positivos de n . Então p_1 é primo pois, caso contrário, existiria um p tal que $1 < p < p_1$ com $p|n$, o que seria um absurdo dado a escolha do p_1 . Assim sendo, $n = p_1 n_1$. Então, se n_1 for primo, então a prova já está completa.

Mas, se esse n_1 for composto, então tomaremos um p_2 como o menor fator de n_1 . Seguindo o mesmo raciocínio, p_2 é primo, então temos $n = p_1 p_2 n_2$. Repetindo esse processo teremos:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

Agora, para provar a unicidade, utilizaremos a indução em n .

Para $n = 2$ a afirmação é verdadeira. Verifiquemos então para n e para os inteiros maiores que n . Como foi dito, se n é primo, não há nada para provar.

Vamos então pegar um n composto e que seja composto das duas seguintes maneiras:

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_r$$

Vamos provar que $s = r$ e que cada $p_i = q_j$. Sabemos que p_1 divide pelo menos um dos fatores de $q_1 q_2 \dots q_r$ pois divide o produto.

Suponhamos que $p_1 | q_1$. Mas eles são primos, o que implica que $p_1 = q_1$. Logo,

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

E, como $1 < \frac{n}{p_1} < n$, pela hipótese de indução, temos que as duas fatorações serão idênticas. Ou seja, $s = r$ e a menos da ordem as fatorações são iguais. $\square$

Teorema 10. *(Euclides) A sequência de números primos é infinita.*

Demonstração. Suponhamos que a sequência dos primos seja finita. Então, tomemos $p_1, p_2, \dots, p_n$ como sendo a lista de todos os primos e consideremos um $R = p_1 p_2 \dots p_n + 1$. Ora, se R é primo, então entraria na lista dos primos que já tínhamos, mostrando que a sequência pode ser continuada e a prova estaria concluída. Mas se R não é primo então,

pelo teorema fundamental da aritmética, será divisível por um primo. Mas nenhum dos primos da lista o dividiriam, pois sempre sobriaria resto 1. Assim, o primo que dividiria R seria maior do que os já apresentados na lista de primos que tínhamos. Mostrando assim que a sequência de números primos é infinita. $\square$

Teorema 11. *Para qualquer inteiro positivo k , existem k inteiros consecutivos todos compostos. Em outras palavras, existem “saltos” arbitrariamente grandes na sequência dos números primos.*

Demonstração. Como $(k+1)!$ é divisível por todos os k números entre 2 e $k+1$, então a sequência

$$(k+1)! + 2, (k+1)! + 3, \dots, (k+1)! + k, (k+1)! + (k+1)$$

É composta por k números consecutivos compostos. $\square$

Teorema 12. *O produto de qualquer sequência de k inteiros consecutivos é divisível por $k!$*

Demonstração. Consideremos 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:

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

Como o numerador é o produto de k inteiros consecutivos, então temos o resultado para k inteiros. (Se 0 for um elemento da sequência é trivial).

Se a sequência contiver números negativos, no máximo, poderá ocorrer uma troca de sinal continuando a ser um inteiro, o que conclui nossa demonstração. $\square$

Teorema 13. *Se n não é primo, então n possui, necessariamente, um fator primo menor do que ou igual a $\sqrt{n}$.*

Demonstração. Sabemos que n composto se escreve como $n = n_1.n_2$, onde $1 < n_1 < n$ e $1 < n_2 < n$. Suponhamos que $n_1 \leq n_2$. Logo, devemos ter $n_1 \leq \sqrt{n}$, ou teríamos $n = n_1.n_2 > \sqrt{n}.\sqrt{n} = n$, o que é um absurdo.

Assim, pelo teorema fundamental da aritmética, n_1 possui algum fator primo (p) que deve ser menor ou igual a $\sqrt{n}$. Como p será um fator primo de n_1 também será de n , completando assim nossa demonstração. $\square$

A demonstração anterior é muito importante pois nos afirma que, se queremos descobrir se um número é primo, é suficiente procurarmos divisores desse número apenas até $\sqrt{n}$. Por exemplo, se queremos encontrar todos os primos até 100, devemos excluir dentre 2 e 100 todos os múltiplos de 2, 3, 5 e 7 pois estes são os primos $\leq \sqrt{100}$. A esse processo damos o nome de Crivo de Eratóstenes.

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~~

1.0.7 Mínimo Múltiplo Comum

Definição 6. O mínimo múltiplo comum de dois inteiros positivos a e b é o menor inteiro positivo que é divisível por a e b . Vamos denotá-lo por $[a, b]$.

Proposição 7. Se $p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_n^{a_n}$ e $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \dots p_n^{b_n}$ onde $p_1, p_2, \dots, p_n$ são os primos que ocorrem nas fatorações de a e b , então

$$[a, b] = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \dots p_n^{\max\{a_n, b_n\}}$$

Demonstração. Por definição, nenhum dos expoentes p_i deste mínimo pode ter expoente menor que a_i e b_i . Tomando então o maior entre esses dois expoentes p_i teremos o menor múltiplo comum possível. $\square$

Proposição 8. Se x e y são números reais, então

$$\max\{x, y\} + \min\{x, y\} = x + y$$

Demonstração. Se $x = y$ então $\max\{x, y\} = \min\{x, y\} = x = y$. O que é trivial!

Suponhamos que $x < y$. Então $\max\{x, y\} = y$ e $\min\{x, y\} = x$. Concluindo assim a demonstração. $\square$

Teorema 14. Para a e b inteiros positivos temos, $[a, b] \cdot (a, b) = a \cdot b$.

Demonstração. Suponhamos que a e b tenham fatorações como da proposição 7. Então:

$$(a, b) = \prod_{i=1}^n p_i^{\min\{a_i, b_i\}}$$

e

$$[a, b] = \prod_{i=1}^n p_i^{\max\{a_i, b_i\}}$$

Então, é imediato da proposição anterior. $\square$

Proposição 9. Sejam a e b inteiros positivos relativamente primos. Então se d é um divisor positivo de ab , existe um único par de divisores positivos d_1 de a e d_2 de b tais que $d = d_1 d_2$. Reciprocamente, se d_1 e d_2 são divisores positivos de a e b , respectivamente, então $d = d_1 d_2$ é um divisor positivo de ab .

Demonstração. Consideremos as seguintes fatorações de a e b :

$$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_n^{a_n} \text{ e } b = q_1^{b_1} q_2^{b_2} q_3^{b_3} \dots q_n^{b_n}$$

Como $(a, b) = 1$ sabemos que os conjuntos $(p_1, p_2, \dots, p_n)$ e $(q_1, q_2, \dots, q_n)$ são disjuntos logo, a fatoração de d será:

$$d = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m} \text{ onde } 0 \leq \alpha_i \leq a_i, i = 1, 2, \dots, n \text{ e } 0 \leq \beta_j \leq b_j, j = 1, 2, \dots, m.$$

Então, podemos definir d_1 e d_2 como

$$d_1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \text{ e } d_2 = q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m}$$

onde $(d_1, d_2) = 1$ e $d_1 d_2 = d$.

Para mostrar a recíproca, vamos considerar que d_1 e d_2 são divisores positivos de a e b , respectivamente.

Logo, dados

$$d_1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}, 0 \leq \alpha_i \leq a_i, i = 1, 2, \dots, n$$

e

$$d_2 = q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m}, 0 \leq \beta_i \leq b_j, j = 1, 2, \dots, m$$

É fácil ver que

$$d = d_1 d_2 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m}$$

É um divisor de ab . □

Teorema 15. *Seja b um inteiro positivo maior do que 1. Então todo inteiro positivo n pode ser representado de maneira única da seguinte forma:*

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0 \quad (1.1)$$

Onde $k \in \mathbb{Z}^+, a_k \neq 0$ e $0 \leq a_i < b, i = 0, 1, 2, \dots, k$.

Este teorema, demonstraremos de duas formas

Demonstração. (1) Iniciaremos provando a existência.

Vamos começar dividindo n por b obtendo um quociente q_0 e resto a_1 . Logo após, dividiremos q_0 por b e assim, sucessivamente. Assim:

$$\begin{aligned} n &= bq_0 + a_0 \\ q_0 &= bq_1 + a_1 \\ q_1 &= bq_2 + a_2 \\ &\dots \\ q_{k-2} &= bq_{k-1} + a_{k-1} \\ q_{k-1} &= b \cdot 0 + a_k \end{aligned}$$

onde $0 \leq a_j < b, j = 0, 1, 2, \dots, k$

Substituiremos então na primeira equação o valor de q_0 encontrado na segunda e assim

sucessivamente:

$$\begin{aligned}
n &= bq_0 + a_0 \\
n &= b(bq_1 + a_1) + a_0 \\
n &= b^2q_1 + ba_1 + a_0 \\
n &= b^2(bq_2 + a_2) + a_1b + a_0 \\
n &= b^3q_2 + a_2b^2 + a_1b + a_0 \\
n &= b^3(bq_3 + a_3) + a_2b^2 + a_1b + a_0 \\
n &= b^4q_3 + a_3b^3 + a_2b^2 + a_1b + a_0 \\
&\dots \\
n &= b^kq_{k-1} + a_{k-1}b^{k-1} + \dots + a_2b^2 + a_1b + a_0 \\
n &= a_kb^k + a_{k-1}b^{k-1} + \dots + a_1b + a_0
\end{aligned}$$

Basta-nos, agora, mostrar unicidade.

Chamaremos de $d_b(n)$ o número de representações de n na base b . Queremos mostrar que $d_b(n)$ é sempre igual a 1.

Suponhamos que n possa ser representado da seguinte forma:

$$n = a_kb^k + a_{k-1}b^{k-1} + \dots + a_sb^s$$

onde $n = a_k$ e a_s representam os que podem conter termos nulos. Logo:

$$\begin{aligned}
n - 1 &= a_kb^k + a_{k-1}b^{k-1} + \dots + a_sb^s - 1 \\
n - 1 &= a_kb^k + a_{k-1}b^{k-1} + \dots + (a_s - 1)b^s + b^s - 1 \\
n - 1 &= a_kb^k + a_{k-1}b^{k-1} + \dots + (a_s - 1)b^s + (b - 1) \sum_{j=0}^{s-1} b^j
\end{aligned}$$

uma vez que $b^s - 1 = (b - 1) \sum_{j=0}^{s-1} b^j$. Ou seja, para cada representação de n na base b é possível encontrar, na base b , uma representação para $n - 1$.

Disso temos que $d_b(n) \leq d_b(n - 1)$.

Então, se $m \leq n$, então:

$$d_b(m) \leq d_b(m - 1) \leq d_b(m - 2) \leq \dots \leq d_b(n + 1) \leq d_b(n)$$

Logo, como $n > 1$ e $d_b(n) \geq 1$, obtemos $1 \leq d_b(n) \leq d_b(1) = 1$. O que nos garante que $d_b(n) = 1$, o que conclui essa demonstração. $\square$

Demonstração. (2) Usaremos indução em n .

Para $n = 1$ tomamos $k = 0$ e $a_0 = 1$. Então é válido para $n = 1$. Para todo inteiro menor que n , assumiremos que o teorema é válido.

Como $b > 1, n > 0$, n então se encontra entre dois números da seguinte sequência de consecutivos:

$$b^0, b^1, b^2, \dots, b^k, \dots$$

Assim sendo, fica claro que existe um único inteiro k , tal que $b^k \leq n < b^{k+1}$. Assim, pelo teorema dos consecutivos vistos anteriormente, temos:

$$n = a_k b^k + r, 0 \leq r < b^k$$

Claro que $0 < a_k < b$. Então se $r = 0$, temos:

$$n = a_k b^k + 0.b^{k-1} + \dots + 0.b + 0$$

Se $r \neq 0$, pela hipótese de indução:

$$r = c_t b^t + \dots + c_1 b + c_0, 1 < k$$

onde $0 \leq c_i < b$. Dessa forma:

$$n = a_k b^k + c_t b^t + \dots + c_1 b + c_0$$

O que já verificamos em 1.1 ficando, assim, provado a existência.

Agora vamos provar a unicidade através da existência da seguinte representação:

$$n = d_m d^m + \dots + d_1 b + d_0 \text{ com } m \geq 0, d_m \neq 0 \text{ e } 0 \leq d_i < b.$$

Se a_i e d_i não são iguais então, da equação que enuncia este teorema e da equação anterior, obteremos:

$$0 = h_s b^s + \dots + h_1 b + h_0$$

onde s é o maior valor de i nos quais $a_i \neq b$.

Logo, $h_s \neq 0$.

Se $s = 0$ temos uma contradição do fato de estarmos assumindo que a equação que enuncia este teorema e a equação anterior são diferentes. E se $s > 0$, então:

$$\begin{aligned} |h_i| &= |a_i - d_i| \leq b - 1, i = 0, \dots, s - 1 \\ h_s b^s &= -(h_{s-1} b^{s-1} + \dots + h_0) \end{aligned}$$

Assim

$$\begin{aligned} b^s &\leq |h_s b^s| = |h_{s-1} b^{s-1} + \dots + h_0| \\ b^s &\leq |h_s b^s| \leq (b - 1)(b^{s-1} + \dots + b + 1) = b^s - 1 \end{aligned}$$

O que também é uma contradição. Assim, concluímos que $a(s)$ e $d(s)$ são iguais, ou seja, $k = m, a_i = d_i, i = 0, 1, \dots, k$ e têm representação é única. $\square$

Definição 7. *Um número da forma*

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

é chamado de número de Fermat.

O teorema seguinte nos fornece uma segunda prova da infinitude dos números primos.

Teorema 16. *Quaisquer dois números de Fermat distintos F_n e F_m são relativamente primos.*

Demonstração. Primeiramente vamos provar por indução que

$$F_0 F_1 \dots F_{n-1} = F_n - 2$$

Como para $n = 1$ é fácil ver, ou seja, $F_0 = F_1 - 2$, vamos supor que vale para n e mostrar que também vale para $n + 1$.

$$\begin{aligned} F_0 F_1 \dots F_n &= (F_0 F_1 \dots F_{n-1}) F_n \\ &= (F_n - 2) F_n \\ &= (2^{2^n} + 1 - 2)(2^{2^n} + 1) \\ &= (2^{2^n} - 1)(2^{2^n} + 1) = 2^{(2^{n+1})} - 1 \\ &= 2^{2^{n+1}} + 1 - 2 = F_{n+1} - 2 \end{aligned}$$

Suponhamos que $n < m$ então temos:

$$F_0 F_1 F_2 \dots F_n \dots F_{m-1} = F_m - 2$$

o que implica que

$$F_m - F_0 F_1 F_2 \dots F_n \dots F_{m-1} = 2$$

Então se um número d divide F_n e F_m então também divide 2. Como F_n é ímpar, $d \neq 2$, logo $(F_n, F_m) = 1$. E finalizamos aqui a demonstração. $\square$

Daqui concluímos que existem infinitos números primos pois, como existem infinitos números de Fermat e não possuem fatores primos em comum, o conjunto deve ser infinito.

Teorema 17. *Existem infinitos primos da forma $6k + 5$*

Demonstração. Pelo algoritmo da divisão sabemos que, ao dividirmos um número por 6, os possíveis restos são 0, 1, 2, 3, 4 e 5. Ou seja, pode ser escrito como $6k, 6k + 1, 6k + 2, 6k + 3, 6k + 4$ e $6k + 5$. Então se p é primo será, ou da forma $6k + 1$ ou $6k + 5$.

Mostraremos então que existem infinitos primos da forma $6k + 5$. Suponhamos por absurdo que esses primos são finitos.

Seja $p_0 = 5, p_1, p_2, \dots, p_r$ esse conjunto. Considere:

$$P = 6p_1 p_2 \dots p_r + 5$$

Da proposição 3, sabemos que esse número não é divisível por nenhum dos primos $p_0, p_1, p_2, \dots, p_r$. Temos que P possui um fator primo da forma $6k + 5$ pois, caso contrário, seria da forma $6k + 1$ (pois o produto de primos $6k + 1$ é $6k + 1$).

Logo, ou P é primo ou possui um fator primo da forma $6k + 5$, provando que existem infinitos primos da forma $6k + 5$. Concluindo a demonstração. $\square$

Provamos aqui um caso especial do Teorema de Dirichlet chamado “Teorema dos Primos em Progressão Aritmética” que diz: Se a e b são inteiros relativamente primos, então a progressão aritmética $an + b, n = 1, 2, 3, \dots$ contém um número infinito de primos.

1.0.8 Critérios de Divisibilidade

Por 2

É “a mais fácil”. Todo inteiro pode ser escrito na forma $10k + j$, onde j representa as unidades. Assim sendo, como 10 é divisível por dois, o produto dele com qualquer inteiro também o será. Logo, toda vez que j for par, ou seja, toda vez que j for múltiplo de 2, todo o número também o será.

Exemplo 1. 5973 não é divisível por 2 pois pode ser reescrito da forma $10 \times 597 + 3$ e 3 não é divisível por 2 (ou seja, não é par).

Exemplo 2. 5974 é divisível por 2 pois pode ser reescrito da forma $10 \times 597 + 4$ e 4 é divisível por 2 (ou seja, é par).

Por 3 e por 9

Consideremos um número n com 5 dígitos $abcde$ na base 10. Ele pode ser escrito assim:

$$n = a \times 10^4 + b \times 10^3 + c \times 10^2 + d \times 10 + e$$

Reescreveremos

$$10 = 9 + 1$$

$$100 = 99 + 1$$

$$1000 = 999 + 1$$

$$10000 = 9999 + 1$$

Assim

$$n = a(9999 + 1) + b(999 + 1) + c(99 + 1) + d(9 + 1) + e$$

$$n = (9999a + 999b + 99c + 9d) + (a + b + c + d + e)$$

$$n = 9(1111a + 111b + 11c + d) + (a + b + c + d + e)$$

Então, se $3|n$, então como $3|9(1111a + 111b + 11c + d)$, 3 deve dividir $(a + b + c + d + e)$.

Da mesma forma, se $3|(a + b + c + d + e)$, então $3|n$ uma vez que $3|9(1111a + 111b + 11c + d)$.

Concluimos assim que:

“Um número é divisível por 3 se, e somente se, a soma de seus dígitos é divisível por 3.”

O mesmo critério vale para o 9:

“Um número é divisível por 9 se, e somente se, a soma de seus dígitos é divisível por 9.”

Exemplo 3. 4578 é divisível por 3 pois $(4 + 5 + 7 + 8) = 24$ e 24 é divisível por 3.

Exemplo 4. 4578 não é divisível por 9 uma vez que a soma de seus dígitos é igual a 24 e 24 não é divisível por 9.

Por 4

Consideraremos um número na forma $n = 100k + ab$ onde “ ab ” são os dois últimos dígitos de n . Assim, como 100 é um múltiplo de 4, basta verificarmos se $4|ab$.

Exemplo 5. 72548 é divisível pois pode ser reescrito como $725x100 + 48$ e 48 é divisível por 4.

Exemplo 6. 72514 não é divisível pois pode ser reescrito como $725x100 + 14$ e 14 não é divisível por 4.

Por 7

De uma forma geral, ao tomarmos um número muito grande, iremos retirando o último número e subtraindo pelo dobro do número retirado. Esse processo será repetido até que encontremos um número suficientemente pequeno ao ponto que seja fácil ver que é divisível por 7. Conforme o exemplo:

$$59325 \implies 5932 - 10 = 5922$$

$$5922 \implies 592 - 4 = 588$$

$$588 \implies 58 - 16 = 42$$

Assim, temos que a fórmula geral seria $10k + i$ o que nos geraria uma segunda equação $r = k - 2i$ e assim sucessivamente.

Demonstração. Temos dois casos:

1º) Se $10k + 1$ for múltiplo de 7, então sabemos que existe um inteiro m tal que

$$10k + i = 7m$$

Portanto

$$k - 2i = k - 2(7m - 10k)$$

$$k - 2i = k - 14m + 20k$$

$$k - 2i = 21k - 14m$$

$$k - 2i = 7(3k - 2m)$$

Ou seja, $k - 2i$ é um múltiplo de 7.

2º) Se $k - 2i$ é múltiplo de 7, então existe um inteiro n tal que

$$k - 2i = 7n$$

Portanto

$$10k + i = 10(7n + 2i) + i$$

$$10k + i = 70n + 20i + i$$

$$10k + i = 70n + 21i$$

$$10k + i = 7(10n + 3i)$$

Ou seja, $10k + i$ é múltiplo de 7, o que conclui nossa demonstração.

□

1.0.9 Congruência

Definição 8. Se a e b são inteiros dizemos que a é congruente a b módulo m ($m > 0$) se $m|(a-b)$. Denotamos isto por $a \equiv b(\text{mod } m)$. Se $m \nmid (a-b)$ dizemos que a é incongruente a b módulo m e denotamos por $a \not\equiv b(\text{mod } m)$.

Exemplo 7. $11 \equiv 3(\text{mod } 2)$ pois $2|(11-3)$.

Exemplo 8. Como $5 \nmid 6$ e $6 = 17 - 11$ temos que $17 \not\equiv 11(\text{mod } 5)$.

Proposição 10. Se a e b são inteiros, temos que $a \equiv b(\text{mod } m)$ se, e somente se, existir um inteiro k tal que $a = b + km$.

Demonstração. Da definição, sabemos que se $a \equiv b \pmod{m}$ se, e somente se, $m|(a-b)$, ou seja, existe um inteiro k tal que

$$a - b = km \implies a = b + km$$

□

Proposição 11. *Se a, b, m e d são inteiros, $m > 0$, as seguintes sentenças são verdadeiras:*

- i) $a \equiv a \pmod{m}$*
- ii) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$*
- iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$ então $a \equiv c \pmod{m}$*

Aqui mostraremos que a congruência é (i) reflexiva, (ii) comutativa e (iii) distributiva, respectivamente.

Demonstração. i) Como $m|0$, então $m|(a-a)$, o que implica que $a \equiv a \pmod{m}$.

ii) Se temos $a \equiv b \pmod{m}$, então $a = b + k_1m$ para algum inteiro k_1 . Ou seja, $b = a - k_1m$ o que implica que $b \equiv a \pmod{m}$.

iii) Dizer que $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$ é dizer que existem inteiros k_1 e k_2 tais que $a - b = k_1m$ e $b - c = k_2m$. Somando, membro a membro, obteremos $a - c = (k_1 + k_2)m$, ou seja $a \equiv c \pmod{m}$.

□

Teorema 18. *Se a, b, m e d são inteiros positivos tais que $a \equiv b \pmod{m}$, então*

- i) $a + c \equiv b + c \pmod{m}$*
- ii) $a - c \equiv b - c \pmod{m}$*
- iii) $ac \equiv bc \pmod{m}$*

Demonstração. i) Como $a \equiv b \pmod{m}$ é o mesmo que $a - b = km$ que pode ser reescrito como $(a + c) - (b + c) = km$ temos que $a + c \equiv b + c \pmod{m}$.

ii) Da mesma forma, $(a - c) - (b - c) = (a - b)$ e como, por hipótese, temos que $a - b = km$, então $a - c \equiv b - c \pmod{m}$.

iii) Do mesmo modo, como $a - b = km$, então $ac - bc = ckm$, ou seja $m|(ac - bc)$, logo, $ac \equiv bc \pmod{m}$.

□

Teorema 19. Se a, b, c, d e m são inteiros positivos tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

i) $a + c \equiv b + d \pmod{m}$

ii) $a - c \equiv b - d \pmod{m}$

iii) $ac \equiv bd \pmod{m}$

Demonstração. i) De $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ temos que $a - b = km$ e $c - d = k_1m$. Se somarmos, membro a membro, teremos $(a + c) - (b + d) = (k + k_1)m$ e isso implica que $a + c \equiv b + d \pmod{m}$

ii) De $a - b = km$ e $c - d = k_1m$, se subtrairmos, membro a membro, teremos $(a - b) - (c - d) = (a - c) - (b - d) = (k - k_1)m$, o que implica $a - c \equiv b - d \pmod{m}$

iii) Dados $a - b = km$ e $c - d = k_1m$, multiplicando por c e b , respectivamente, temos $ac - bc = ckm$ e $bc - db = bk_1m$. Somando ambos lados da igualdade, temos $ac - bc + bc - db = (ck + bk_1)m$, o que implica $ac \equiv bd \pmod{m}$

□

Teorema 20. Se a, b, c e m são inteiros positivos e $ac \equiv bc \pmod{m}$, então $a \equiv b \pmod{\frac{m}{d}}$ onde $d = (c, m)$

Demonstração. De $ac \equiv bc \pmod{m}$ temos que $ac - bc = c(a - b) = km$. Dividindo ambos membros por d (essa divisão por d pode ser efetuada pois d é divisor comum entre c e m logo, a divisão de ambos os membros está bem definida), então temos que $(\frac{c}{d})(a - b) = k(\frac{m}{d})$. Assim $\frac{m}{d} | \frac{c}{d}(a - b)$ e como d é o mdc entre m e c , isso implica que $(\frac{m}{d}, \frac{c}{d}) = 1$, então $\frac{m}{d} | (a - b)$. O que implica $a \equiv b \pmod{\frac{m}{d}}$. □

Definição 9. Se h e k são dois inteiros com $h \equiv k \pmod{m}$, dizemos que k é um resíduo de h módulo m .

Definição 10. O conjunto dos inteiros $r_1, r_2, \dots, r_s$ é um sistema completo de resíduos módulo m se

- i) $r_i \not\equiv r_j \pmod{m}$ para $i \neq j$
- ii) Para todo inteiro n existe um r_i tal que $n \equiv r_i \pmod{m}$.

Teorema 21. Se k inteiros $r_1, r_2, \dots, r_k$ formam um sistema completo de resíduos módulo m então $k = m$.

Demonstração. Demonstraremos primeiro que os inteiros $t_0, t_1, \dots, t_{m-1}$, com $t_i = i$ formam um sistema completo de resíduos módulo m . Sabemos que $r_i \not\equiv r_j \pmod{m}$ com $i \neq j$. Se $r_i \equiv r_j \pmod{m} \implies m \mid r_i - r_j$ o que gera um absurdo pois $r_i - r_j < m$. Sabemos também pelo teorema fundamental da Aritmética que, para cada n , existe um único par de inteiros q e s tal que $n = mq + s$, $0 \leq s < m$.

Assim sendo, $n \equiv s \pmod{m}$ para $i \neq j$. Logo o conjunto $\{t_0, t_1, \dots, t_{m-1}\}$ é um sistema completo de resíduos módulo m .

Daí é fácil ver que cada r_i é congruente a um t_i , logo, $k \leq m$. E como o conjunto $r_0, r_1, \dots, r_k$ forma, por hipótese, um sistema completo de resíduos módulo m , temos também que cada t_i é congruente a um r_j , o que nos dá que $m \leq k$. Dessa forma, $k = m$. $\square$

Exemplo 9. $\{0, 1, 2, \dots, m-1\}$ é um sistema completo de resíduos módulo m .

Teorema 22. Se $r_1, r_2, \dots, r_m$ é um sistema completo de resíduos módulo m , e a e b são inteiros com $(a, m) = 1$, então

$$ar_1 + b, ar_2 + b, \dots, ar_m + b$$

Também é um sistema completo de resíduos módulo m .

Demonstração. Partindo do resultado do teorema anterior, mostraremos então que quaisquer dois inteiros do conjunto $ar_1 + b, ar_2 + b, \dots, ar_m + b$ não são congruentes módulo m . Suponhamos que $ar_i + b \equiv ar_j + b \pmod{m}$. Do teorema 18, temos que $ar_i \equiv ar_j \pmod{m}$

e do teorema 20, temos que $d = (a, m) = 1$, o que implica que $r_i \equiv r_j \pmod{m}$. E isso implica que $i = j$ uma vez que $\{r_1, r_2, \dots, r_m\}$ forma um sistema completo de resíduos módulo m . $\square$

Proposição 12. *Se a, b, k e m são inteiros positivos com $k > 0$ e $a \equiv b \pmod{m}$, então $a^k \equiv b^k \pmod{m}$.*

Demonstração. Segue diretamente do teorema 20. Temos que

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \dots + ab^{k-2} + b^{k-1})$$

Se $a \equiv b \pmod{m}$, então temos que $a = b + km$ para algum $k \in \mathbb{Z}$, o que implica que $a - b = km$. Portanto, temos que $m | (a - b)$, o que implica que $m | (a - b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \dots + ab^{k-2} + b^{k-1}) = a^k - b^k$. Logo, temos que $rn = a^k - b^k$ para algum $r \in \mathbb{Z}$ e, consequentemente

$$a^k \equiv b^k \pmod{m}$$

$\square$

Teorema 23. *Se $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m_k}$, onde $a, b, m_1, m_2, \dots, m_k$ são inteiros com m_i positivos, $i = 1, 2, \dots, k$ então*

$$a \equiv b \pmod{[m_1, m_2, \dots, m_k]}$$

onde $[m_1, m_2, \dots, m_k]$ é o mínimo múltiplo comum de $m_1, m_2, \dots, m_k$.

Demonstração. Seja a seguinte fatoração em primos

$$m_i = p_1^{x_{1i}} p_2^{x_{2i}} \dots p_n^{x_{ni}} \text{ com } 1 \leq i \leq k \text{ (tal que alguns } x_{ij} \text{ podem ser nulos).}$$

onde p_n o maior primo da fatoração de $m_1, m_2, \dots, m_k$.

Como $m_i | (a - b)$, $i = 1, 2, \dots, k$ então teremos que $p_j^{i_j} | (a - b)$, $i = 1, 2, \dots, k$ e $j = 1, 2, \dots, n$.

Portanto se tomarmos o máximo $x_i = \max_{1 \leq j \leq k} \{x_{ij}\}$ de cada m_i , teremos

$$p_1^{x_1} \cdot p_2^{x_2} \cdot \dots \cdot p_n^{x_n} | (a - b)$$

Mas,

$$p_1^{x_1} \cdot p_2^{x_2} \cdot \dots \cdot p_n^{x_n} = [m_1, m_2, \dots, m_k]$$

O que implica

$$a \equiv b \pmod{[m_1, m_2, \dots, m_k]}$$

□

1.0.10 Congruência Linear

Definição 11. Chamamos de congruência linear em uma variável a uma congruência da forma $ax \equiv b \pmod{m}$ onde x é uma incógnita.

Observação 1. Uma equação da forma $ax + by = c$, onde a, b e c são inteiros é chamada equação diofantina linear.

Teorema 24. Sejam a e b inteiros positivos e $d = (a, b)$. Se $d \nmid c$ então a equação $ax + by = c$ não possui nenhuma solução inteira. Se $d|c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por

$$x = x_0 + \left(\frac{b}{d}\right)k$$

$$y = y_0 - \left(\frac{a}{d}\right)k$$

onde k é um inteiro.

Demonstração. Se $d|a$ e $d|b$, d deve dividir c já que c é uma combinação linear de a e b , implicando assim que se $d \nmid c$ então a equação $ax + by = c$ não possui solução.

Suponhamos que $d|c$. Então existem inteiros n_0 e m_0 tais que

$$an_0 + bm_0 = d$$

E também existe um k tal que $c = kd$. Multiplicando a equação acima por k , teremos

$$a(n_0k) + b(m_0k) = kd = c$$

Ou seja, que o par (x_0, y_0) com $x_0 = n_0k$ e $y_0 = m_0k$ é uma solução de $ax + by = c$. É fácil ver que os pares abaixo são soluções

$$x = x_0 + \left(\frac{b}{d}\right)k$$

$$y = y_0 - \left(\frac{a}{d}\right)k$$

Uma vez que

$$\begin{aligned}
ax + by &= a[x_0 + (\frac{b}{d})k] + b[y_0 - (\frac{a}{d})k] \\
ax + by &= ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k \\
ax + by &= ax_0 + by_0 = c
\end{aligned}$$

Ou seja, se conhecemos uma solução particular, podemos gerar infinitas soluções. Vamos agora mostrar que toda solução da equação $ax + by = c$ é da forma $x = x_0 + (\frac{d}{a})k$, $y = y_0 - (\frac{a}{d})k$.

Suponhamos que (x, y) seja uma solução.

Mas como $ax_0 + by_0 = c$, subtraindo, membro a membro, obtemos

$$ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0$$

Isso implica que $a(x - x_0) = b(y_0 - y)$ e como $d = (a, b)$ temos que

$$(\frac{a}{d}, \frac{b}{d}) = 1$$

Portanto, dividindo a penúltima igualdade por d , temos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$$

Então,

$$\frac{b}{d} | (x - x_0)$$

Portanto, existe um inteiro k tal que

$$x - x_0 = k(\frac{b}{d}), \text{ ou seja, } x = x_0 + (\frac{b}{d})k$$

Substituindo esse valor na equação dividida por d acima, teremos

$$y = y_0 - (\frac{a}{d})k$$

O que conclui a demonstração. □

Teorema 25. *Sejam a, b e m inteiros tais que $m > 0$ e $(a, m) = d$. No caso em que $d \nmid b$ a congruência $ax \equiv b \pmod{m}$ não possui nenhuma solução e quando $d | b$, possui exatamente d soluções incongruentes módulo m .*

Demonstração. Sabemos que $ax \equiv b(\text{mod } m)$ tem x como solução se, e somente se, houver um y tal que $ax = b + my$ que é o mesmo que $ax - my = b$. Sabemos também que se $d \nmid b$ a equação não tem nenhuma solução e que se $d|b$ tem infinitas soluções dadas por $x = x_0 - (\frac{m}{d})k$ e $y = y_0 - (\frac{a}{d})k$ no qual (x_0, y_0) é uma solução particular de $ax - my = b$. Assim a congruência $ax \equiv b(\text{mod } m)$ possui infinitas soluções dadas por $x = x_0 - (\frac{m}{d})k$. Estamos tentando encontrar o número de soluções incongruentes, então vamos tentar descobrir sobre que condições

$$x_1 = x_0 - (\frac{m}{d})k_1$$

e

$$x_2 = x_0 - (\frac{m}{d})k_2$$

são congruentes módulo m . Se $x_1 \equiv x_2$ então

$$x_0 - (\frac{m}{d})k_1 \equiv x_0 - (\frac{m}{d})k_2(\text{mod } m)$$

o que implica que

$$(\frac{m}{d})k_1 \equiv (\frac{m}{d})k_2(\text{mod } m)$$

e como $(\frac{m}{d})|m$ então $(\frac{m}{d}, m) = \frac{m}{d}$. Assim, pelo teorema 20, temos que

$$k_1 \equiv k_2(\text{mod } d) \text{ e que } d|b.$$

[Uma vez que $d = \frac{m}{\frac{m}{d}}$].

Ou seja, possui exatamente d soluções incongruentes módulo m que são dadas por

$$x = x_0 - (\frac{m}{d})k$$

onde k é um sistema completo de resíduos módulo d , o que conclui a demonstração $\square$

Definição 12. Dizemos que uma solução x_0 de $ax \equiv b(\text{mod } m)$ é única módulo m quando qualquer outra solução x_1 for congruente a x_0 módulo m .

Definição 13. Uma solução $\bar{a}$ de $ax \equiv 1(\text{mod } m)$ é chamada de um inverso de a módulo m .

Teorema 26. Seja p um número primo. O inteiro a é o seu próprio inverso módulo p se, e somente se, $a \equiv 1(\text{mod } p)$ ou $a \equiv -1(\text{mod } p)$.

Demonstração. Dizer que a é seu próprio inverso, é dizer que $a^2 \equiv 1 \pmod{p}$ o que implica que $p \mid (a^2 - 1)$. Mas como p é primo, então se $p \mid (a - 1)(a + 1)$ logo ou $p \mid (a - 1)$ ou $p \mid (a + 1)$ o que implica que $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$.

A recíproca é imediata visto que se $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$ então ou $p \mid (a - 1)$ ou $p \mid (a + 1)$. Assim sendo, $p \mid (a - 1)(a + 1)$ o que implica que $a^2 \equiv 1 \pmod{p}$. $\square$

1.0.11 Soma de divisores

Definição 14. *Seja n um inteiro positivo. Indicaremos por $\sigma(n)$ a soma dos divisores positivos de n .*

Exemplo 10. *Os divisores positivos de 60 são 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 e 60, logo*

$$\sigma(60) = 1 + 2 + 3 + 4 + 5 + 6 + 10 + 12 + 15 + 20 + 30 + 60 = 168.$$

Os divisores positivos de 13 são 1 e 13, logo

$$\sigma(13) = 1 + 13 = 14$$

O que implica que 13 é primo.

1.0.12 Funções Aritméticas

Definição 15. *Chama-se função aritmética toda função f definida no conjunto $\mathbb{N}$ dos inteiros positivos e com valores no conjunto $\mathbb{Z}$ dos inteiros, isto é, toda função f de $\mathbb{N}$ em $\mathbb{Z}$ ($f : \mathbb{N} \rightarrow \mathbb{Z}$)*

Utilizaremos das seguintes funções aritméticas de $\mathbb{N}$ em $\mathbb{N}$ ($d, \sigma : \mathbb{N} \rightarrow \mathbb{N}$) em nosso trabalho:

Definição 16. *Denotaremos por d o conjunto de todos divisores inteiros de um número.*

Definição 17. *Denotaremos por σ o conjunto que possui apenas os divisores próprios de um número, ou seja, todos os divisores de n exceto n mesmo.*

Definição 18. *(Funções Aritméticas Multiplicativas). Uma função aritmética f diz-se uma função aritmética multiplicativa se*

$$f(rs) = f(r)f(s),$$

para todo par de inteiros positivos r e s tais que $\text{mdc}(r, s) = 1$.

Teorema 27. A função $\sigma(n)$ é uma função aritmética multiplicativa.

Demonstração. Sejam u e v dois inteiros positivos com $\text{mdc}(u, v) = 1$, ou seja, coprimos. Se $u = 1$ ou $v = 1$, então teríamos $\sigma(uv) = \sigma(u)\sigma(v)$. Então, suponhamos que ambos sejam maiores que um e tenham a seguinte decomposição canônica

$$u = p_1^{k_1} \cdot p_2^{k_2} \dots p_i^{k_i} \text{ e } v = q_1^{h_1} \cdot q_2^{h_2} \dots q_i^{h_i}.$$

Uma vez que são coprimos, cada $p_x \neq q_y$, logo, o produto entre eles será

$$uv = p_1^{k_1} \cdot p_2^{k_2} \dots p_i^{k_i} \cdot q_1^{h_1} \cdot q_2^{h_2} \dots q_i^{h_i}$$

Logo, a soma dos divisores do produto será igual ao produto da soma dos divisores, ou seja

$$\sigma(uv) = \sigma(u)\sigma(v)$$

de modo que σ é uma função aritmética multiplicativa. □

1.0.13 Os Teoremas de Euler, Fermat e Wilson

Teorema 28. (de Wilson) p é primo se, e somente se, $(p-1)! \equiv -1 \pmod{p}$.

Demonstração. Como $(2-1)! \equiv 1 \equiv -1 \pmod{2}$ então o resultado é válido para $p = 2$.

Pelo teorema 25, $ax \equiv 1 \pmod{p}$ tem uma única solução para todo a no conjunto $(1, 2, 3, \dots, p-1)$. Mas, como desses elementos, só 1 e $p-1$ são seus próprios inversos módulo p então, conforme o exemplo 9, podemos agrupar os que sobraram em $\frac{p-3}{2}$ pares dos quais os produtos são congruentes a 1 módulo p . Multiplicando todos esses pares, teremos

$$2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-2) \equiv 1 \pmod{p}$$

E multiplicando ambos lados por $(p-1)$, teremos

$$2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-2) \cdot (p-1) \equiv (p-1) \pmod{p}$$

O que implica que $(p-1)! \equiv -1 \pmod{p}$ uma vez que $p-1 \equiv -1 \pmod{p}$.

Vejam os então a recíproca. Suponhamos que $(n-1)! \equiv -1 \pmod{n}$, ou seja, que $n \mid [(n-1)! + 1]$ e que esse n , por contradição, não seja primo. Logo, n seria da forma $n = rs$,

$1 < r < n$ e $1 < s < n$.

É fácil ver que n deveria dividir $(n-1)!$ e, como r é um divisor de n , r também o deveria dividir $r|[(n-1)!+1]$ uma vez que a diferença é igual a 1. Isso é um absurdo já que $r > 1$. Assim sendo, n deve ser primo. $\square$

Teorema 29. (*Pequeno Teorema de Fermat*) Seja p primo e $a \in \mathbb{Z}$. Se $p \nmid a$ então $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração. Já sabemos que o conjunto formado pelos p números $0, 1, 2, \dots, (p-1)$ constitui um sistema completo de resíduos módulo p . Ou seja, qualquer conjunto que contenha no máximo p elementos incongruentes pode ser colocado em correspondência biunívoca com esse subconjunto. Consideremos os números $a, 2a, 3a, \dots, (p-1)a$. Como $(a, p) = 1$ então nenhum dos números ia , $1 \leq i \leq p-1$ será divisível por p . Isso significa que nenhum deles será congruente a 0 módulo p . Quaisquer dois deles serão incongruentes módulo p quando $aj \equiv ak \pmod{p} \implies j \equiv k \pmod{p}$ o que só é possível se $j = k$ uma vez que j e k são positivos e menores que p . Assim sendo, cada elemento desse conjunto de $p-1$ elementos incongruentes módulo p e não divisíveis por p será congruente a exatamente um dos elementos de $1, 2, 3, \dots, p-1$. Multiplicando então, membro a membro, teremos dessas congruências

$$a(2a)(3a)\dots(p-1)a \equiv 1.2.3. \dots .(p-1) \pmod{p}$$

O que implica que $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Mas como $[(p-1)!, p] = 1$, podemos cancelar o valor $(p-1)!$ Em ambos lados, gerando

$$a^{p-1} \equiv 1 \pmod{p}$$

O que conclui a demonstração. $\square$

Corolário 2. Se p é um primo e a é um inteiro positivo, então $a^p \equiv a \pmod{p}$.

Demonstração. Se $p|a$, então $p|[a(a^{p-1}-1)]$, logo $a^p \equiv a \pmod{p}$.

Se $p \nmid a$, $p|(a^{p-1}-1)$, ou seja, $p|(a^p-a)$.

Logo, em ambos casos, $p|(a^p-a)$. $\square$

Definição 19. Se n é um inteiro positivo, a função ϕ de Euler, denotada por $\phi(n)$, é definida como sendo o número de inteiros positivos menores ou iguais a n que são relativamente primos com n .

Definição 20. Um sistema reduzido de resíduos módulo m é um conjunto de $\phi(m)$ inteiros $r_1, r_2, \dots, r_{\phi(m)}$, tais que cada elemento do conjunto é relativamente primo com m , e se $i \neq j$, então $r_i \not\equiv r_j \pmod{m}$.

Exemplo 11. O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7\}$ é um sistema completo de resíduos módulo 8. O conjunto $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8.

Ou seja, para obtermos um sistema reduzido de um sistema completo de resíduos, basta retirarmos todos que são relativamente primos com o módulo.

Teorema 30. Seja a um inteiro positivo tal que $(a, m) = 1$. Se $r_1, r_2, \dots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m , então $ar_1, ar_2, \dots, ar_{\phi(m)}$ é, também, um sistema reduzido de resíduos módulo m .

Demonstração. Sabemos que a sequência $ar_1, ar_2, \dots, ar_{\phi(m)}$ tem $\phi(m)$ elementos.

Vamos provar que todos são relativamente primos com m e, dois a dois, são incongruentes módulo m .

Como $(a, m) = 1$ e $(r_i, m) = 1$ então $(ar_i, m) = 1$. Assim, resta-nos mostrar que $ar_i \not\equiv ar_j \pmod{m}$ se $i \neq j$. Mas como $(a, m) = 1$, então de $ar_i \equiv ar_j \pmod{m}$ temos que $r_i \equiv r_j \pmod{m} \implies i = j$ uma vez que $r_1, r_2, \dots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m . O que conclui a demonstração. $\square$

Teorema 31. (de Euler) Se m é um inteiro positivo e a um inteiro com $(a, m) = 1$, então

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Demonstração. Já vimos que $ar_1, ar_2, \dots, ar_{\phi(m)}$ é um sistema reduzido de resíduos módulo m se $(a, m) = 1$ e $r_1, r_2, \dots, r_{\phi(m)}$ for um sistema reduzido de resíduos módulo m . Ou seja, ar_1 é congruente a exatamente um dos r_j , $1 \leq j \leq \phi(m)$. Isso implica que os produtos dos ar_i deve ser congruente ao produto dos r_j , módulo m , isto é

$$ar_1 \cdot ar_2 \cdot \dots \cdot ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdot \dots \cdot r_{\phi(m)} \pmod{m}$$

Ou seja

$$a^{\phi(m)} r_1 . r_2 . \dots . r_{\phi(m)} \equiv r_1 . r_2 . \dots . r_{\phi(m)} (\text{mod } m)$$

E como de

$$(\prod_{i=1}^{\phi(m)} r_i, m) = 1$$

Podemos cancelar em ambos lados

$$\prod_{i=1}^{\phi(m)} r_i$$

Então obteremos $a^{\phi(m)} \equiv 1 (\text{mod } m)$. Concluindo assim nossa demonstração. $\square$

Capítulo 2

Números Interessantes e Resultados Associados

2.1 Números Amigos

Os filósofos gregos acreditavam que uma amizade perfeita entre duas pessoas significava que, com as partes de uma, era possível construir a outra, e que valia o contrário. Essa crença levou os pitagóricos a pensarem no que, hoje, conhecemos como números amigos, e que estão totalmente relacionados a essa crença de amizade dos filósofos gregos. Vejamos então a definição de números amigos:

Definição 21. *Um par de números inteiros positivos (M, N) são chamados números amigos se M é a soma dos divisores próprios de N e N é a soma dos divisores próprios de M .*

Observação 2. *Da definição acima, é imediato que a soma dos divisores de M é igual a $N + M$ assim como a soma dos divisores de N resultam em $M + N$.*

Exemplo 12. *220 e 284 é o primeiro par de números amigos uma vez que os divisores próprios de 220 são 1, 2, 4, 5, 10, 20, 11, 22, 44, 55, 110 que somam 284 ao passo que os divisores próprios de 284 são 1, 2, 4, 71, 142 que somam 220.*

Se, ao invés de tomarmos os divisores próprios, tomarmos os divisores de cada um dos

números acima, teremos que os divisores de 220 somam 504 que também é soma dos divisores de 284. Logo, como visto na observação anterior $\sigma(N) = M + N = \sigma(M)$.

Mas todo esse algebrismo é algo recente, muito antes o matemático árabe Thabit Ibn Qurra propôs que

Teorema 32. *(de Thabit Ibn Qurra) Seja k um número inteiro positivo. Se*

$$\begin{aligned} p &= 3 \cdot 2^{k-1} - 1 \\ q &= 3 \cdot 2^{k-1} \\ r &= 9 \cdot 2^{2k-1} - 1 \end{aligned}$$

são todos primos, então

$$(M, N) = (2^k pq, 2^k r)$$

é um par de amigos.

Porém começou-se a especular as condições sobre as quais p , q e r são satisfeitas de modo que m e n são amigos - que mostraremos no teorema 33. Questionou-se também para quais valores de k p , q e r seriam primos e os estudiosos, matemáticos e filósofos da época, foram desenvolvendo cálculos sobre tal questionamento de maneira que chegaram numa resposta que seria para $k = 2, 4, 7$. Porém, tal resposta só pode obter 3 conjuntos diferentes de p , q e r calculados naquela época. E mesmo depois de vários estudos sobre esse questionamento dos valores de k , os pitagóricos não conseguiram mostrar nenhum. Até que em 1636 Fermat pôde encontrar mais um par nesse formato. O tempo foi passando até que Euler propôs o seguinte teorema:

Teorema 33. *Se p, q, r são primos ímpares e distintos de modo que*

$$n = 2^k pq \text{ e } m = 2^k r$$

são amigos. Então existem números naturais t e k tais que $t \leq k$ o que satisfaz as igualdades

$$\begin{aligned} p &= 2^k + 2^{k-t} - 1 \\ q &= 2^k + 2^{k+t} - 1 \\ r &= [2^{2k-t}(2^{t+1} + 2^{2t} + 1)] - 1 \end{aligned}$$

Demonstração. Sabemos, pelo teorema fundamental da aritmética, que os divisores de n são

$$1, 2, \dots, 2^k, p, 2p, \dots, 2^k p, q, 2q, \dots, 2^k q, pq, 2pq, \dots, 2^k pq$$

então, a soma dos divisores próprios de n é dada por

$$(1 + 2 + \dots + 2^k) + p(1 + 2 + \dots + 2^k) + q(1 + 2 + \dots + 2^k) + pq(1 + 2 + \dots + 2^k)$$

Podemos entender $(1 + 2 + \dots + 2^k)$ como $2^{k+1} - 1$ e $(1 + p + q + pq)$ como o produto notável $(p + 1)(q + 1)$. Assim, os divisores próprios de n é

$$(2^{k+1} - 1)(p + 1)(q + 1).$$

Ainda pelo teorema fundamental da aritmética, temos que os divisores de m são

$$1, 2, \dots, 2^k, r, 2r, \dots, 2^k r$$

E que podemos representar sua soma como

$$\begin{aligned} (1 + 2 + \dots + 2^k) + r(1 + 2 + \dots + 2^k) &= \\ (r + 1)(1 + 2 + \dots + 2^k) &= \\ (r + 1)(2^{k+1} - 1) \end{aligned}$$

Por hipótese, n e m são amigos, então

$$S(n) = S(m)$$

e

$$S(m) = S(n)$$

onde S representa a soma dos divisores próprios.

Se somarmos n e m , respectivamente nas equações acima, teremos que

$$\begin{cases} \sigma(n) = m + n \\ \sigma(m) = n + m \end{cases} \quad (2.1)$$

Subtraindo as equações, temos que

$$\sigma(n) - \sigma(m) = 0$$

o que implica que

$$\sigma(n) = \sigma(m)$$

Logo temos

$$\begin{aligned}(2^{k+1} - 1)(p + 1)(q + 1) &= (2^{k+1} - 1)(r + 1) \\ (p + 1)(q + 1) &= (r + 1) \\ pq + p + q &= r\end{aligned}$$

De (2.1) temos que $n + m = \sigma(n)$. Ou seja,

$$(1 + p + q + pq)(2^{k+1} - 1) = n + m = 2^k pq + 2^k r$$

Mas reescrevendo r como acima, temos

$$(1 + p + q + pq)(2^{k+1} - 1) = 2^k pq + 2^k (pq + p + q)$$

E tomando $(2^{k+1} - 1) = 2^k 2 - 1$, teremos

$$\begin{aligned}(1 + p + q + pq)(2^k 2 - 1) &= 2^k 2 + 2^k 2pq + 2^k 2p + 2^k 2q - 1 - p - q - pq = \\ &= 2^k (2 + 2pq + 2p + 2q) - (1 + pq + p + q)\end{aligned}$$

Igualando então a equação acima com a equação na qual reescrevemos o r , teremos

$$2^k (2 + 2pq + 2p + 2q) - (1 + pq + p + q) = 2^k pq + 2^k (pq + p + q)$$

Operando então ambas, teremos

$$2^k (2 + p + q) = (1 + pq + p + q) \tag{2.2}$$

Se definirmos agora um $P = p + 1$ e um $Q = q + 1$, então

$$1 + p + q + pq = PQ$$

e

$$p + q + 2 = P + Q$$

Assim sendo, podemos reescrever (2.2) como

$$2^k (P + Q) = PQ$$

Se somarmos $2^{2k} - 2^k (P + Q)$, teremos

$$2^{2k} = PQ + 2^{2k} - 2^k(P + Q)$$

Assim, sabendo que $2^{2k} = 2^k 2^k$, podemos reescrever a equação acima como

$$2^{2k} = (P - 2^k)(Q - 2^k)$$

Então $(P - 2^k) > 0$ e $(Q - 2^k) > 0$. Como 2 é primo, pelo teorema fundamental da aritmética, temos que

$$(P - 2^k) = 2^h$$

e

$$(Q - 2^k) = 2^d$$

Sabemos que se h e d são inteiros tais que $h + d = 2k$, então existe um número t menor ou igual a k tal que $h = k - t$ e $d = k + t$. Assim sendo, chegamos que

$$P = 2^k + 2^{k-t}$$

e

$$Q = 2^k + 2^{k+t}$$

Destarte

$$p = P - 1 = 2^k + 2^{k-t} - 1$$

e

$$q = Q - 1 = 2^k + 2^{k+t} - 1$$

Assim, lembrando que $r = p + q + qp$, então temos que

$$r = PQ - 1 = (2^k + 2^{k-t})(2^k + 2^{k+t}) - 1 = [2^{2k-t}(2^{t+1} + 2^{2t} + 1)] - 1$$

o que conclui nossa demonstração. □

Agora que temos o teorema acima estruturado, voltemos para a demonstração do teorema de Thabit Ibn Qurra que é a análise do caso particular $t=1$, do teorema que acabamos de demonstrar.

Demonstração. (do teorema de Thabit Ibn Qurra) Temos que

soma dos divisores de $n = (2^{k+1} - 1)(p + 1)(q + 1)$

ou seja

$$S(n) = (2^{k+1} - 1)(p + 1)(q + 1) - 2^k pq$$

da mesma forma, temos que

$$\sigma(m) = (2^{k+1} - 1)(r + 1)$$

que é o mesmo que

$$S(m) = (2^{k+1} - 1)(r + 1) - 2^k r$$

mas já vimos na demonstração do teorema anterior que

$$(r + 1) = (p + 1)(q + 1)$$

Logo,

$$S(n) = (2^{k+1} - 1)(r + 1) - 2^k pq = S(m)$$

Ou seja, a soma dos divisores de n é igual a soma dos divisores de m , o que implica que n e m são amigos. $\square$

2.1.1 Resultados Essenciais

Diversos outros teoremas foram mais tarde enunciados com o propósito de encontrar pares de números amigos. Então, como pretendemos que este trabalho seja um compêndio dos resultados relacionados a números interessantes, do teorema 35 ao teorema 49 encontraremos resultados que já foram provados na direção de encontrar pares de números amigos atendendo determinadas condições. Devido ao grau de complexidade, as demonstrações desses resultados serão omitidas mas podem ser encontradas em [16].

Teorema 34. *Sejam (M, N) números amigos e seja g um inteiro positivo tal que $g|M$ e $g|N$. Se*

$$\text{mdc}(g, \frac{M}{g}) = \text{mdc}(g, \frac{N}{g}) = 1$$

e se $h \neq g$ é um número inteiro positivo tal que

$$\frac{\sigma(h)}{g} = \frac{\sigma(g)}{g}$$

e

$$\text{mdc}(h, \frac{M}{g}) = \text{mdc}(h, \frac{N}{g}) = 1$$

então

$$(h\frac{M}{g})(h\frac{N}{g})$$

são números amigos.

Teorema 35. *Sejam M e N números inteiros positivos. Se*

$$\begin{cases} N = \sigma(M) - M \\ t = \sigma(N) - N \end{cases}$$

então (M, N) é um par de amigos.

O teorema a seguir é análogo ao teorema de Thabit.

Teorema 36. *Seja k um número inteiro positivo e seja $0 < x < k$ tal que*

$$p = 2^x g - 1$$

é um número primo, onde $g = 2^{k-x} + 1$. Seja $0 < y < k$ tal que

$$\begin{cases} q = 2^y + (2^{k+1} - 1)g \\ r = 2^{k-y} g q - 1 \\ s = 2^{k-y+x} g^2 q - 1 \end{cases}$$

se q, r e y são primos, então

$$(M, N) = (2^k p q r, 2^k q s)$$

é um par de amigos.

O teorema a seguir também é análogo ao teorema de Thabit e foi proposto por Lee.

Teorema 37. *Seja k um número inteiro positivo. Se*

$$\begin{cases} p = 3 \cdot 2^{k-1} - 1 \\ q = 35 \cdot 2^{k+1} - 29 \\ r = 7 \cdot 2^{k-1} - 1 \\ s = 15 \cdot 2^{k+1} - 13 \end{cases}$$

são números primos, então

$$(M, N) = (2^k pq, 2^k rs)$$

é um par de amigos.

Teorema 38. *Sejam k, m e n números inteiros positivos com $k < m$. Sejam*

$$\begin{cases} f = 2^k + 1 \\ g = 2^{m-k} f^2 \end{cases}$$

se

$$\begin{cases} r_1 = f 2^{m-k} - 1 \\ r_2 = f 2^m - 1 \\ p = g(2^{m+1} - 1) + 1 \\ q_1 = p^n [(2^m - 1)g + 2] - 1 \\ q_2 = 2^m p^n g [(2^m - 1)g + 2] - 1 \end{cases}$$

são todos primos, então

$$(M, N) = (2^m p^n r_1 r_2 q_1, 2^m p^n q_2)$$

é um par de amigos.

Teorema 39. *(Regra de Borho). Sejam b_1 e b_2 inteiros positivos e seja p um primo que não divide nem b_1 nem b_2 tais que*

$$\frac{p}{p-1} = \frac{b_1}{\sigma(b_1)} + \frac{b_2}{\sigma(b_2)}$$

Se para algum inteiro positivo k e para $i = 1, 2, \dots$

$$q_i = \frac{p^k (p-1) (b_1 + b_2)}{\sigma(b_i)} - 1$$

é um primo que não divide $b_i p$, então $(M, N) = (b_1 p^k q_1, b_2 p^k q_2)$ é um par de amigos.

Teorema 40. (*Método de Lee*). Sejam $A_1 = \sigma(a_1)$ e $A_2 = \sigma(a_2)$. Sabendo que podemos escrever todo par de amigos como $(M, N) = (a_1 p q, a_2 r)$, se tivermos

$$\begin{cases} A_1(p+1)(q+1) = A_2(r+1) = a_1 p q + a_2 r \\ r = \frac{A_1(p+1)(q+1)}{A_2} - 1 \\ [a_1 A_2 - A_1(A_2 - a_2)] p q - A_1(A_2 - a_2)(p + q) = a_2 A_2 + A_1(A_2 - a_2) \\ p = \frac{X + A_1(A_2 - a_2)}{a_1 A_2 - A_1(A_2 - a_2)} \\ q = \frac{Y + A_1(A_2 - a_2)}{a_1 A_2 - A_1(A_2 - a_2)} \end{cases} \quad (2.3)$$

Onde X e Y são um par de fatores tais que

$$XY = A_2[a_1 a_2 A_2 + A_1(a_1 - a_2)(A_1 - a_2)] \quad (2.4)$$

então, do determinante de p e q se deduz a seguinte condição

$$\frac{a_1}{A_1} + \frac{a_2}{A_2} > 1 \quad (2.5)$$

Daí, tomando a_1 e a_2 sujeitos a 2.5, das desigualdades 2.3 podemos obter todos os possíveis valores de p, q e r tais que

$$(M, N) = (a_1 p q, a_2 r)$$

são números amigos.

Observação 3. O problema desse teorema é que é muito difícil encontrar a_1 e a_2 tais que p, q e r sejam inteiros. Isso foi resolvido por Herman J. J te Riele, que propôs a partir de números amigos já conhecidos.

Teorema 41. (*Análogo ao Método de Lee*). Seja $(M_1, N_1) = (a_1 p, a_2 q)$ um par de números amigos com

$$\begin{cases} p, q \text{ primos} \\ \text{mdc}(a_1, p) = \text{mdc}(a_2, q) = 1 \end{cases} \quad (2.6)$$

Selecionando (a_1, a_2) para encontrar uma solução (q_1, q_2) da equação bilinear Diofantina

$$Aq_1q_2 - B(q_1 + q_2) = C$$

o equivalente a

$$(Aq_1 - B)(Aq_2 - B) = AC + B^2 = W$$

onde

$$\begin{cases} A_1 = \sigma(a_1) \\ A_2 = \sigma(a_2) \\ B_1 = \sigma(a_1) - a_1 \\ B_2 = \sigma(a_2) - a_2 \\ A = a_1a_2 - B_1B_2 \\ B = B_1A_2 \\ C = a_1A_1 + B_1A_2W = AC + B^2 \end{cases}$$

Escrevendo W de todas as formas possíveis de um produto $W = UV$, temos

$$\begin{cases} U = Aq_1 - B \\ V = Aq_2 - B \end{cases}$$

o que implica que

$$\begin{cases} q_1 = \frac{U+B}{A} \\ q_2 = \frac{V+B}{A} \end{cases}$$

onde q_1 e q_2 satisfazem

$$\begin{cases} q_1 \text{ e } q_2 \text{ são primos} \\ q_1 \neq q_2 \\ \text{mdc}(a_2q_1, q_2) = 1 \end{cases} \quad (2.7)$$

calculando p_1 , tal que

$$\begin{cases} p_1 = \frac{a_2 q_1 q_2 - A_1}{B_1} \\ p_1 \text{ é primo} \\ \text{mdc}(a_1, p_1) = 1 \end{cases} \quad (2.8)$$

Assim sendo, se satisfazem as condições 2.6, 2.7 e 2.8, então

$$(M, N) = (a_1 p_1, a_2 q_1 q_2)$$

é um par de números amigos.

Teorema 42. (Regra de te Riele). Seja $(M_1, N_1) = (au, ap)$ um par de números amigos com $\text{mdc}(a, u) = \text{mdc}(a, p) = 1$, onde p é primo. Se existe um par de números primos r e s com $p < r < s$ e $\text{mdc}(a, rs) = 1$, que satisfaça

$$(r - p)(s - p) = \frac{\sigma(a)}{a} \sigma(u)^2$$

e existe um primo q com $\text{mdc}(au, q) = 1$ e

$$q = r + s + u,$$

então

$$(M, N) = (auq, ars)$$

é um par de amigos.

Teorema 43. Seja $w > 1$ um número inteiro dado, e seja u e v números inteiros tais que $w^2 = uv$ e $1 < u \leq v$. Sejam $A = \sigma(w) - w$ e $B = 2w - \sigma(w)$. Se

$$\begin{cases} p = \frac{u+A}{B} \\ q = \frac{v+A}{B} \\ s = p.q + p + q \end{cases}$$

são primos distintos, e

$$\text{mdc}(w, p) = \text{mdc}(w, q) = \text{mdc}(w, s) = 1$$

então

$$(M, N) = (wpq, ws)$$

é um par de amigos.

Teorema 44. *Seja a_1 e a_2 dois números inteiros positivos dados. Sejam*

$$\begin{cases} A = \sigma(a_1)[\sigma(a_2) - a_2] \\ B = a_1\sigma(a_2) - \sigma(a_1)[\sigma(a_2) - a_2] \end{cases}$$

e sejam u e v números naturais tais que

$$\left\{ uv = \sigma(a_2)[a_1a_2\sigma(a_2) + \sigma(a_1)(a_1 - a_2)(\sigma(a_2) - a_2)] \right.$$

se

$$\begin{cases} p = \frac{u+A}{B} \\ q = \frac{v+A}{B} \\ s = \frac{\sigma(a_1)(pq+p+q+1)}{\sigma(a_2)} - 1 \end{cases}$$

são primos diferentes, e

$$\text{mdc}(a_1, p) = \text{mdc}(a_1, q) = \text{mdc}(a_2, s) = 1$$

então

$$(M, N) = (a_1pq, a_2s)$$

é um par de amigos.

Teorema 45. *Sejam m e n dois números inteiros positivos distintos tais que*

$$\sigma(m) = \sigma(n) \neq m + n$$

se existe outro números inteiro $w > 1$ tal que

$$\begin{cases} \text{mdc}(m, w) = \text{mdc}(n, w) = 1 \\ \frac{\sigma(w)}{w} = \frac{m+n}{\sigma(m)} \end{cases}$$

então

$$(M, N) = (wm, wn)$$

é um par de amigos.

Para os próximos enunciados, usaremos a seguinte definição:

Definição 22. Um par de números inteiros positivos (a_1, a_2) é chamado breeder ou criador se a equação

$$a_1 + a_2x = \sigma(a_1) = \sigma(a_2)(x + 1)$$

tem uma solução inteira positiva.

Proposição 13. Sejam (a_1, a_2) um par criador. Se x é um número primo que não divide a_2 e é solução da equação da definição de criador, então (a_1, a_2x) é um par de números amigos.

Assim sendo, da definição, os pares criadores também poderão ser encontrados da forma $(i, 1)$ onde i é a quantidade de fatores primos distintos e com $i \geq 1$.

Teorema 46. (Regra de Borho). Seja (au, a) um par criador, com solução inteira x da equação da definição de criador. Se existe um par de números primos distintos r e s com $\text{mdc}(a, rs) = 1$, satisfazendo

$$q = r + s + u$$

Então

$$(M, N) = (auq, ars)$$

é um par de amigos.

Observação 4. Se assumirmos a regra de Riele (au, ap) como um par amigável, fazendo a substituição temos que (au, a) é um criador e obtemos a forma geral.

Teorema 47. Sejam a_1 e a_2 números inteiros positivos. Se

$$\sigma(a_1)(r_1 + 1) = a_1r_1 + a_2r_2 = \sigma(a_2)(r_2 + 1)$$

tem uma solução de inteiros positivos r_1 e r_2 , e $\text{mdc}(a_1, r_1) = \text{mdc}(a_2, r_2) = 1$, então

$$(M, N) = (a_1 r_1, a_2 r_2)$$

É um par de amigos.

Os primeiros números amigos da forma (7,1) - ou seja, o par de amigos com mesmos fatores primos iniciais mas que, um é multiplicado por 7 primos e o outro por apenas um - foram encontrados por García e foram:

$$2 \cdot 5^2 \cdot 19 \cdot \begin{cases} p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \cdot p_6 \cdot p_7 \\ q \end{cases}$$

onde

$$\begin{cases} p_1 = 23 \\ p_2 = 2203 \\ p_3 = 256661 \\ p_4 = 20053673 \\ p_5 = 872652329 \\ p_6 = 227581730937820119934248943 \\ p_7 = 2177018379078405763792563767026726112056503960079 \\ q = (p_1 + 1)(p_2 + 1)(p_3 + 1)(p_4 + 1)(p_5 + 1)(p_6 + 1)(p_7 + 1) - 1 \end{cases}$$

do método descrito acima, e utilizando o teorema que enunciaremos abaixo, podem-ser obter 1224444006400 casos possíveis de números amigos, e com o par (8, 2) que é da forma:

$$2 \cdot 5^2 \cdot 19 \cdot \begin{cases} p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \cdot p_6 \cdot p_7 \cdot p_8 \\ q_1 \cdot q_2 \end{cases}$$

foi possível gerar números com primos de até 102 dígitos cada.

Teorema 48. *Sejam m, n números inteiros positivos tais que*

$$\sigma(m)\sigma(n) = n[m + \sigma(m) - 1]$$

e $\text{mdc}(m, n) = 1$. Se

$$\begin{cases} p \\ q \\ r = \sigma(m)(p+1)(q+1) - 1 \end{cases}$$

são primos tais que não dividem nem m nem n e que satisfazem a equação

$$(p - m + 1)(q - m + 1) = m(m - 1) + 1$$

então

$$(M, N) = (mnpq, nr)$$

é um par de números amigos.

2.1.2 Problemas em aberto

Como problemas em aberto nos números amigos, temos buscas por áreas específicas dentro deles. Já existem teoremas propostos, mas ainda não provados, a cerca de tais números. São eles:

- 1 Pares de números amigos ímpares não divisíveis por 3

Era tido como um problema em aberto a existência de tais números até que, em 1988, S. Battiato e W. Borho apresentaram uma lista que continha 15 desses pares. O interessante é que todos tinham como fatores comuns $5^4 \cdot 7^3 \cdot 11^3 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 61^2 \cdot 97 \cdot 307$.

- 2 Números amigos com menor fator primo distinto

Também de descoberta recente, em 30 de janeiro de 2016, Sergei Chernykh apresentou uma lista que continha 7 desses pares.

As listas apresentadas por Battiato e Borho e por Chernykh, encontram-se no apêndice deste trabalho.

- 3 Existem pares de números amigos coprimos?

Ainda não se tem certeza pelo fato de que todos têm, ao menos, um divisor comum maior que um. Supõe-se que os teoremas que se utilizarão para provar serão:

Teorema 49. *Se (M, N) é um par de números amigos relativamente primos (coprimos), então MN têm mais de 20 fatores primos;*

Teorema 50. *Se (M, N) é um par de números amigos relativamente primos, então $M > 10^{33}$ e $N > 10^{33}$.*

4 Existem números amigos com paridade oposta?

Paridade oposta quer dizer que um de seus membros será par e, o outro, ímpar. O teorema que se supõe admitir como hipótese na demonstração de existência será o seguinte:

Teorema 51. *Se existir um par de números amigos de paridade oposta, então o membro ímpar é um quadrado e o membro par é o produto de uma potência de 2 por um número quadrado ímpar*

Além dos itens (3) e (4), existem pesquisas também sobre a junção de ambos, ou seja, procura-se a existência de pares de números amigos coprimos e com paridade oposta e supõe-se que usar-se-ão os seguintes resultados para a resolução:

Teorema 52. *Se (M, N) é um par de números amigos coprimos de paridade oposta, então $MN > 10^{121}$;*

Corolário 3. *Se (M, N) é um par de números amigos coprimos de paridade oposta, então $M > 10^{60}$ e $N > 10^{60}$.*

2.2 Números Primos Gêmeos

Os números primos são uma das maiores motivações dos pesquisadores de teoria dos números porém, dentro dos números primos, há vastas áreas de pesquisa. Uma delas é sobre os primos p com $p + 2$ também primo, o que chamamos de par de primos gêmeos. Apesar de ter sido chamado de “número primo gêmeo” apenas em 1916, sua definição informal já era usada desde bem antes. A definição que utilizamos hoje é a seguinte:

Definição 23. *Se p e q são primos com $|p - q| = 2$, então dizemos que p e q são primos gêmeos.*

Em 1849, Polignac conjecturou que, para todo número natural k , existem infinitos pares de primos consecutivos p e p' tais que $p' - p = k$. O caso de $k = 2$ é a conjectura dos primos gêmeos. Um século se passou até que Clement [4], em 1949, caracterizou os números primos gêmeos da seguinte maneira

Teorema 53. *Seja $p \geq 2$. Os inteiros p e $p + 2$ são primos gêmeos se, e somente se:*

$$4[(p - 1)! + 1] + p \equiv 0 \pmod{p^2 + 2p}$$

Demonstração. Seja p e $p + 2$. Do teorema de Wilson

$$(p - 1)! + 1 \equiv 0 \pmod{p}$$

temos que se p é primo tal que satisfaça a equivalência, então $p + 2$ também é primo. Logo, se p e $p + 2$ são primos, então, $p \neq 2$. Assim para p primo:

$$\begin{aligned} \implies (p - 1)! + 1 &\equiv 0 \pmod{p} \\ \implies 4[(p - 1)! + 1] &\equiv 0 \pmod{p} \\ \implies 4[(p - 1)! + 1] &\equiv -p \pmod{p} \end{aligned} \tag{2.9}$$

Similarmente, para $p + 2$ primo, temos:

$$\begin{aligned} (p + 1)! + 1 &\equiv 0 \pmod{p + 2} \\ \implies (p^2 + p)(p - 1)! + 1 &\equiv 0 \pmod{p + 2} \\ \implies [(p + 2)(p - 1) + 2](p - 1)! + 1 &\equiv 0 \pmod{p + 2} \\ \implies 2(p - 1)! + 1 &\equiv 0 \pmod{p + 2} \\ \implies 2[2(p - 1)! + 1] &\equiv 0 \pmod{p + 2} \end{aligned}$$

$$\begin{aligned}
&\implies 2[2(p-1)! + 1] + (p+2) \equiv 0 \pmod{p+2} \\
&\implies 4[(p-1)! + 1] + p \equiv 0 \pmod{p+2} \\
&\implies 4[(p-1)! + 1] \equiv -p \pmod{p+2}
\end{aligned} \tag{2.10}$$

Assim, por (2.9) e (2.10),

$$4[(p-1)! + 1] \equiv -p \pmod{p^2 + 2p}$$

Reciprocamente, se

$$4[(p-1)! + 1] + p \equiv 0 \pmod{p^2 + 2p} \implies 4[(p-1)! + 1] + p \equiv 0 \pmod{p}$$

E uma vez que 4 não pode dividir p, então

$$[(p-1)! + 1] \equiv 0 \pmod{p}$$

e pelo teorema de Wilson, p é primo. Da mesma forma se

$$4[(p-1)! + 1] + p \equiv 0 \pmod{p+2}$$

então

$$4(p-1)! + p + 4 \equiv 2(-1)(-2)(p-1)! + 2 \equiv 2(p+1)! + 2 = 2[(p+1)! + 1] \equiv 0 \pmod{p+2}.$$

Uma vez que p e p+2 são coprimos, então

$$(p+1)! + 1 \equiv 0 \pmod{p+2}$$

então, pelo teorema de Wilson, p+2 também é primo.

□

Existem 17 pares de primos gêmeos compreendidos entre 0 e 250. São eles (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), (149, 151), (179, 181), (191, 193), (197, 199), (227, 229), (239, 241).

Coincidentemente, com exceção do par (3, 5), todos os 17 pares citados podem ser escritos como $(6k-1, 6k+1)$ para algum $k \in \mathbb{Z}$ usando a classe dos restos da divisão por 6. Esse par $(6k-1, 6k+1)$ é a única forma, das classes dos restos da divisão por 6, nas quais um número pode ser primo – e nem todos são – uma vez que os outros são múltiplos ou de 2 ou de 3.

2.2.1 Resultados Essenciais

Proposição 14. *Se o par $(p, p+2)$ é de primos gêmeos, então*

$$2^{p+2} \equiv 3p + 8 \pmod{p^2 + 2p}$$

Demonstração. Se p é primo e $p \neq 2$ então, pelo Pequeno Teorema de Fermat, temos que

$$2^{p-1} \equiv 1 \pmod{p} \implies 2^{p+2} \equiv 8 \equiv 3p + 8 \pmod{p}$$

Da mesma forma, se $p + 2$ for primo, temos que

$$2^{p+1} \equiv 1 \pmod{p+2} \implies 2^{p+2} \equiv 2 \equiv 2 + 3(p+2) = 3p + 8 \pmod{p}$$

Com p e $p + 2$ coprimos. □

Antes de prosseguirmos, vale ressaltar apenas uma definição que será utilizada também na demonstração do próximo Lema.

Definição 24. *Os números de Catalan são definidos como:*

$$C_n = \frac{1}{n+1} \binom{2n}{n} = \frac{(2n)!}{(n+1)!n!}$$

Para $n \geq 0$.

Lema 1. *Se p é um primo ímpar, então $(-1)^{\frac{p-1}{2}} C_{\frac{p-1}{2}} \equiv 2 \pmod{p}$.*

Demonstração. Temos que $p - i \equiv -i \pmod{p}$ para qualquer inteiro i . Então

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left(\frac{p-1}{2}\right) \cdot \left(p - \frac{p-1}{2}\right) \cdot \left(p - \frac{p-1}{2} - 1\right) \cdot \dots \cdot (p-1) \equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p} \implies$$

$$C_{\frac{p-1}{2}} \equiv (p+1) C_{\frac{p-1}{2}} = 2 \binom{p-1}{\frac{p-1}{2}} = 2 \left(\frac{(p-1)!}{\left[\left(\frac{p-1}{2}\right)!\right]} \right)^2 \equiv 2(-1)^{\frac{p-1}{2}} \pmod{p}$$

O que conclui nossa demonstração. □

Proposição 15. *Se os números $(p, p+2)$, são primos gêmeos, então*

$$8(-1)^{\frac{p-1}{2}} C_{\frac{p-1}{2}} \equiv 7p + 16 \pmod{p^2 + 2p}$$

Demonstração. Conforme visto no lema anterior,

$$8(-1)^{\frac{p-1}{2}} C_{\frac{p-1}{2}} \equiv 2 \cdot 8 \equiv 7p + 16 \pmod{p}$$

Da mesma forma,

$$C_{\frac{p-1}{2}} = \frac{p+3}{4p} C_{\frac{p+1}{2}}$$

Logo, temos que

$$\begin{aligned} 8(-1)^{\frac{p-1}{2}} C_{\frac{p-1}{2}} &= 8(-1)^{\frac{p-1}{2}} \left(\frac{p+3}{4p}\right) C_{\frac{p+1}{2}} \\ 8(-1)^{\frac{p-1}{2}} \left(\frac{p+3}{4p}\right) C_{\frac{p+1}{2}} &\equiv \frac{-2}{4p} (-1)^{\frac{p-1}{2}} 2p C_{\frac{p+1}{2}} \\ \frac{-2}{4p} (-1)^{\frac{p-1}{2}} 2p C_{\frac{p+1}{2}} &\equiv -4 \frac{p+3}{p} \\ -4 \frac{p+3}{p} \equiv 2 &\equiv 2 + 7(p+2) = \\ &7p+16 \pmod{p+2} \end{aligned}$$

Uma vez que

$$-4(p+3) \equiv 2p \pmod{p+2}$$

Logo,

$$8(-1)^{\frac{p-1}{2}} C_{\frac{p-1}{2}} \equiv 7p + 16 \pmod{p^2 + 2}$$

□

Podemos também encontrar algumas equivalências aos teoremas anteriormente mostrados. Elas provam, em seus resultados, a existência ou localização de alguns pares de números primos gêmeos. Tais resultados não serão demonstrados neste trabalho, apenas serão enunciados. São eles:

Equivalência 1. *Os números $(p, p+2)$ são primos gêmeos se, e somente se,*

$$2\left[\left(\frac{p-1}{2}\right)!\right]^2 + (-1)^{\frac{p-1}{2}} (5p+2) \equiv 0 \pmod{p^2 + 2p}$$

Baseando-se também na função de Euler, temos o seguinte resultado:

Equivalência 2. *Os números $(p, p+2)$ são primos gêmeos se, e somente se,*

$$\phi(p) + \phi(p+2) = 2p$$

Equivalência 3. *Os números $(p, p+2)$ são primos gêmeos se, e somente se,*

$$\sigma_a(p) + \sigma_a(p+2) = 2 + p^a + (p+2)^a$$

para algum inteiro a , com $a \geq 1$.

Equivalência 4. *Seja $n = pq$, então (p, q) são primos gêmeos se, e somente se,*

$$\phi(n)\sigma(n) = (n-3)(n+1)$$

Equivalência 5. *Os números $(p, p+2)$ são primos gêmeos se, e somente se,*

$$\sum_{i=1}^p i^a \left(\left\lfloor \frac{p+2}{i} \right\rfloor + \left\lfloor \frac{p}{i} \right\rfloor \right) = 2 + p^a + \sum_{i=1}^p i^a \left(\left\lfloor \frac{p+1}{i} \right\rfloor + \left\lfloor \frac{p-1}{i} \right\rfloor \right)$$

Para $a \geq 0$, onde $\lfloor x \rfloor$ denota a parte inteira de x .

Mostraremos agora um teorema que utiliza os números primos gêmeos em sua demonstração. Mas, antes, lembremos como é escrita a série harmônica:

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \dots$$

Apesar de parecer convergente - afinal, os termos estão decrescendo à zero - temos que é divergente visto que, se substituirmos, após os dois primeiros termos, um a um, por menores ou iguais e equivalentes a eles, teremos uma série menor ainda, divergindo, o que implica que a série harmônica também divergirá. Em outras palavras:

$$\begin{aligned} S &= 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \dots \\ S &= 1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \dots \\ S &= 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \dots = \infty \end{aligned}$$

Logo, como S é divergente e $S \leq \sum_{n=1}^{\infty} \frac{1}{n} \implies \sum_{n=1}^{\infty} \frac{1}{n}$ é divergente.

O teorema de Euler, que mostraremos abaixo, nos mostra que a soma dos inversos de todos os primos diverge.

Teorema 54 (Euler). *A série seguinte é divergente.*

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

onde $\mathbb{P}$ é o conjunto dos primos.

Demonstração. Comparemos com a série harmônica que mostramos anteriormente. Fixemos, então, um $t \in \mathbb{N}$ arbitrário. Do teorema fundamental da aritmética, sabemos que para cada $n \in \mathbb{N}$, $2 \leq n \leq t$, a fração $\frac{1}{n}$ é o produto de frações do tipo $\frac{1}{p^q}$ onde p é primo, $p \leq n \leq t$ e $q \in \mathbb{N}$. Logo, $\frac{1}{n}$ é apenas uma parcela do produto

$$\prod_{p \in \mathbb{P}, p \leq t} \left(\sum_{k=0}^{\infty} \frac{1}{p^k} \right) = \prod_{p \in \mathbb{P}, p \leq t} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots \right) = \prod_{p \in \mathbb{P}, p \leq t} \frac{1}{1 - \frac{1}{p}}, \text{ onde } \mathbb{P} \text{ é o conjunto dos primos.}$$

O que faz com que tenhamos

$$\sum_{n=1}^t \frac{1}{n} \leq \prod_{p \in \mathbb{P}, p \leq t} \frac{1}{1 - \frac{1}{p}}$$

tomando, então, os logaritmos, temos

$$\log \left(\sum_{n=1}^t \frac{1}{n} \right) \leq \sum_{p \in \mathbb{P}, p \leq t} \log \left(\frac{1}{1 - \frac{1}{p}} \right)$$

Fixando o $p \in \mathbb{P}$ que mencionamos anteriormente, como $\frac{1}{p} \leq 1$, a expansão em séries de potência da função logarítmica, nos faz deduzir que

$$\begin{aligned} \log \left(\frac{1}{1 - \frac{1}{p}} \right) &= -\log \left(1 - \frac{1}{p} \right) = - \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} \left(\frac{1}{p} \right)^n \leq \sum_{n=1}^{\infty} \frac{1}{np^n} \leq \sum_{n=1}^{\infty} \frac{1}{p^n} = \\ &= \frac{1}{p} + \frac{1}{p^2} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots \right) = \frac{1}{p} + \frac{1}{p^2 \left[1 - \frac{1}{p} \right]} = \frac{1}{p} + \frac{1}{p(p-1)} \end{aligned}$$

Destarte

$$\log \left(\sum_{n=1}^t \frac{1}{n} \right) \leq \sum_{p \in \mathbb{P}, p \leq t} \frac{1}{p} + \sum_{p \in \mathbb{P}, p \leq t} \frac{1}{p(p-1)} \leq \sum_{p \in \mathbb{P}, p \leq t} \frac{1}{p} + \sum_{n=1}^t \frac{1}{n(n-1)}$$

Assim, tomando os limites de $t \rightarrow \infty$, temos

$$\log \left(\sum_{n=1}^{\infty} \frac{1}{n} \right) \leq \sum_{p \in \mathbb{P}} \frac{1}{p} + \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1 + \sum_{p \in \mathbb{P}} \frac{1}{p}$$

já que

$$\sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n} \right) = 1$$

o que implica que a série

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

é divergente uma vez que $\sum_{n=1}^{\infty} \frac{1}{n}$ é divergente. □

Observação 5. A demonstração acima implica que existem infinitos primos uma vez que, $\sum_{n=1}^{\infty} \frac{1}{n} = +\infty$. Caso os primos fossem finitos, então série convergiria, o que não acontece.

O próximo teorema, que enunciaremos porém não demonstraremos, devido ao grau de complexidade de sua demonstração, é o teorema de Brun que diz:

Teorema 55 (Brun). $\sum_{p, p+2 \in \mathbb{P}} \left(\frac{1}{p} + \frac{1}{p+2} \right) < \infty$

A demonstração de Brun estende a soma para todos os primos p tais que $p+2$ também seja primo e mostra que essa soma é convergente. Isso implica que, ainda que existam infinitos primos gêmeos, eles se encontrarão cada vez mais afastados uns dos outros.

2.2.2 Problemas em aberto

Algumas conjecturas utilizam, de alguma forma, a seguinte conjectura:

Conjectura 1. *Os números primos gêmeos são infinitos.*

Essa conjectura é conhecida como conjectura dos números primos gêmeos e as seguintes dependem da demonstração dela para serem provadas:

Conjectura 2. *Todo número par é a diferença de dois números primos consecutivos, em um número infinito de maneiras.*

Caso seja possível provar tal conjectura, com diferença igual a 2, obteremos, também, a conjectura dos primos gêmeos. Ou seja, é ainda mais forte do que a conjectura dos números primos gêmeos.

Conjectura 3. *Seja $s \geq 1$ e $f_i(X) = b_i X + a_i$, onde $i = 1, \dots, s$ com $a_i, b_i \in \mathbb{Z}$ e $b_i \geq 1$.*

Além disso, admitamos que não existe um inteiro $n > 1$ que divida todos os produtos $\prod_{j=1}^s f_j(k)$ para cada inteiro k . Então existe uma infinidade de números naturais m tais que cada um dos inteiros $f_1(m), \dots, f_s(m)$ é um número primo.

Essa tem, como caso particular, tanto a conjectura dos primos gêmeos quanto a conjectura dos primos de Sophie Germain

Definição 25. *Chamamos de primos de Sophie Germain os primos p tais que $2p + 1$ também é primo.*

Exemplo 13. $(3, 7), (5, 11), (23, 47), \dots$

Conjectura 4. *Existem infinitos números primos de Sophie Germain.*

E a última conjectura, que enunciaremos a seguir, é a generalização da conjectura de de Hardy-Littlewood (também conhecida como k-tupla conjectura), a qual afirma que o número assintótico de constelações de primos - ou seja, um número muito grande de primos bem organizados como uma constelação e não como toda a Via Láctea - pode ser calculado explicitamente

Conjectura 5. *Seja $0 < m_1 < m_2 < \dots < m_k$ então, sendo $\pi_{m_1, m_2, \dots, m_k}(x)$ o número de primos $p \leq x$ tais que $p + 2m_1, p + 2m_2, \dots, p + 2m_k$ são todos primos, satisfaz*

$$\pi_{m_1, m_2, \dots, m_k}(x) \sim C(m_1, m_2, \dots, m_k) \int_2^x \frac{dt}{(\log t)^{k+1}}$$

onde $C(m_1, m_2, \dots, m_k) = 2^k \prod_q \frac{1 - \frac{w(q; m_1, m_2, \dots, m_k)}{q}}{(1 - \frac{1}{q})^{k+1}}$ o produto é tomado sobre todos os primos ímpares q e $w(q; m_1, m_2, \dots, m_k)$ é o número de distintos resíduos $0, m_1, \dots, m_k \pmod{q}$.

2.3 Números Perfeitos

Os últimos dos números interessantes que veremos são os números perfeitos que são estudados desde bem antes de 300 a.C. Os Pitagóricos já admiravam tais números pelas mistificadas de cada um. Acreditavam que 6 era número perfeito uma vez que, biblicamente, Deus criou o mundo em 6 dias. Também afirmaram que a lua leva 28 dias para dar a volta na Terra, logo também consideravam 28 como um número perfeito. Assim sendo, definamos então número perfeito.

Definição 26. *Se um número n é tal que $\sigma(n) = n$, então esse número é dito perfeito.*

Observação 6. *Alguns autores, ao invés de tomar $\sigma(n)$ como os divisores próprios, tomam todos os divisores, por conseguinte, obtém-se que os números perfeitos são da forma:*

$$\sigma(n) = 2n$$

Exemplo 14. *Os divisores próprios de 6 são $1 + 2 + 3 = 6$. Logo, por definição, 6 é perfeito. Já os divisores próprios de 8 são $1 + 2 + 4 = 7$. Logo, 8 não é perfeito.*

Observação 7. *8 será chamado deficiente ou defectivo uma vez que a soma de seus divisores próprios resultam em um número menor que o mesmo. Caso resultasse em um número maior, seria chamado de abundante, é o caso do 12 pois a soma dos seus divisores próprios é $1 + 2 + 3 + 4 + 6 = 16$.*

Os primeiros resultados dos quatro primeiros números perfeitos foram registrados por Euclides em seu livro "Os Elementos de Euclides", na proposição 36 do livro IX, que enuncia: "Se tantos números quanto quisermos, a partir da unidade, forem postos continuamente, em proporção dupla, até que a soma de todos seja um número primo e se multiplicarmos pelo último membro da soma, o produto será um número perfeito.". Isso é, se tomarmos a sequência 1, 2, 4, 8, ... tal que obtenhamos um primo e multipliquemos pelo último número que somamos, poderemos ter um número perfeito. Observe:

$$6 = (1 + 2) \cdot 2$$

$$28 = (1 + 2 + 4) \cdot 4$$

$$496 = (1 + 2 + 4 + 8 + 16) \cdot 16$$

Apesar de, a primeira vista, aparentar que os cálculos crescerão exponencialmente, mais tarde - em 1747 -, Euler mostrou que não só todo número dessa forma será perfeito (como Euclides tinha mostrado) como mostrou que todo número perfeito par será dessa forma - ou seja, a recíproca é verdadeira. Então a busca é pelos seguintes números:

Definição 27. *Os inteiros da forma $2^n - 1$ serão chamados número de Mersenne*

Observação 8. *Lembrando que a soma das n primeiras potências de 2 é dada por $2^n - 1$*

Logo, a busca por números perfeitos pares se resume a encontrar números de Mersenne. Mais especificamente, os números da forma:

$$2^{n-1}(2^n - 1)$$

onde se $2^n - 1$ é primo, então n também o é. Como mostra o teorema abaixo:

Teorema 56. *Se $2^n - 1$ é primo, então n é primo*

Demonstração. Suponhamos que n seja composto. Logo, n é da forma $n = ab$ com $a, b > 1$. Como $2^a - 1 > 1$, temos que

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 \equiv 1^b - 1 = 0 \pmod{2^a - 1}$$

mostrando assim que $2^n - 1$ é composto (uma vez que $2^a | 2^n$).

Diante disso, se $2^n - 1$ é composto, então n também o é, e se $2^n - 1$ for primo, n também o será. □

2.3.1 Resultados Essenciais

Teorema 57. *(Euclides) Se $2^k - 1$ é primo ($k > 1$), então o número natural $n = 2^{k-1}(2^k - 1)$ é um número perfeito.*

Demonstração. Seja $2^k - 1 = p$ um primo com ($k > 1$) e consideremos o número natural $n = 2^{k-1}p$. Sabemos que o $\text{mdc}(2^{k-1}, p) = 1$ e que $\sigma(n)$ é uma função aritmética

multiplicativa. Daí, temos:

$$\begin{aligned}
\sigma(n) &= \sigma(2^{k-1}p) \\
&= \sigma(2^{k-1})\sigma(p) \\
&= \frac{2^{k-1+1} - 1}{2 - 1}(p + 1) \\
&= (2^k - 1)(2^k - 1 + 1) \\
&= (2^k - 1)2^k \\
&= (2^k - 1)2 \frac{2^k}{2} \\
&= 2 \cdot 2^{k-1}(2^k - 1) \\
&= 2n
\end{aligned}$$

logo, por definição, n é perfeito. □

Nichomachus, baseando-se nos estudos de Euclides, também propôs o seguinte teorema que segue da aplicação direta do teorema anterior:

Teorema 58. *Se $n = 2^{k-1}(2^k - 1)$ é um número perfeito euclidiano, então:*

- i) se $k = 2$ então $n = 6$;*
- ii) se $k \equiv 1 \pmod{4}$ então $n \equiv 6 \pmod{10}$*
- iii) se $k \equiv 3 \pmod{4}$ então $n \equiv 28 \pmod{100}$*

Demonstração. i) se $k = 2$ então $n = 6$

Segue imediato da definição. Logo, se $k = 2$, temos que $n = 2^{2-1}(2^2 - 1) = 6$

ii) se $k \equiv 1 \pmod{4}$ então $n \equiv 6 \pmod{10}$

Seja $k \equiv 1 \pmod{4}$, ou seja, $k = 4n + 1 \Leftrightarrow k - 1 = 4n$.

Assim sendo, temos que $2^{k-1} = 2^{4n}$. Logo, $2^{4n} = (2^4)^n = 16^n \equiv 6^n \pmod{10}$. Só que $6 \equiv 6 \pmod{10}$ e $6^2 = 36 \equiv 6 \pmod{10}$ o que, por indução, é possível provar que para todo n natural, $6^n \equiv 6 \pmod{10}$ - pela proposição 12. Isso implica que

$$2^{k-1} = 2^{4n} = (2^4)^n = 16^n \equiv 6^n \equiv 6 \pmod{10}$$

Mas $2^k - 1 = 2 \cdot 2^{k-1} - 1 \equiv 2 \cdot 6(-1) = 11 \equiv 1 \pmod{10}$. Logo, se $k \equiv 1 \pmod{4}$, $n = 2^{k-1}(2^k - 1) \equiv 6 \cdot 1 = 6 \pmod{10}$.

iii) se $k \equiv 3 \pmod{4}$ então $n \equiv 28 \pmod{100}$

Seja $k \equiv 3 \pmod{4}$, isto é, $k = 4n + 3 \Leftrightarrow k - 1 = 4n + 2$.

Assim sendo, temos que $2^{k-1} = 2^{4n+2} = 2^{4n} \cdot 2^2 = 4^{2n} \cdot 4 \equiv 0 \pmod{4}$, o que implica que $4|2^{k-1}$. Então, pelo critério de divisibilidade por 4, o número formado pelos dois últimos algarismos de 2^{k-1} é divisível por 4.

Mas, do item anterior, temos que $2^{4n} \equiv 6 \pmod{10}$ então $2^{k-1} = 2^{4n+2} = 2^{4n} \cdot 2^2 \equiv 6 \cdot 4 = 24 \equiv 4 \pmod{10}$ o que mostra que o últimos algarismo de 2^{k-1} é 4.

Logo, $2^{k-1} \equiv 10a + 4 \pmod{100}$ para algum $a \in \mathbb{N}_0$. Sabendo que $4|2^{k-1}$, então $4|(10a + 4)$. E como é certeza que, por definição, $4|4$, então $4|10a$, o que implica que $a \in 0, 2, 4, 6, 8$

Então, $2^{k-1} \equiv 4, 24, 44, 64 \text{ ou } 84 \pmod{100}$. E como $2^k - 1 = 2 \cdot 2^{k-1} - 1$, então temos que $2 \cdot 2^{k-1} - 1 \equiv 2 \cdot 4 - 1 = 7 \pmod{100}$ ou $2 \cdot 2^{k-1} - 1 \equiv 2 \cdot 24 - 1 = 47 \pmod{100}$ ou $2 \cdot 2^{k-1} - 1 \equiv 2 \cdot 44 - 1 = 87 \pmod{100}$ ou $2 \cdot 2^{k-1} - 1 \equiv 2 \cdot 64 - 1 = 127 \equiv 27 \pmod{100}$ ou $2 \cdot 2^{k-1} - 1 \equiv 2 \cdot 84 - 1 = 167 \equiv 67 \pmod{100}$.

Logo, $2^k - 1 \equiv 7, 47, 87, 27 \text{ ou } 67 \pmod{100}$.

Portanto,

$$n = 2^{k-1}(2^k - 1) \equiv 4 \cdot 7, 24 \cdot 47, 44 \cdot 87, 64 \cdot 27 \text{ ou } 84 \cdot 67 \pmod{100}$$

ou seja

$$n \equiv 28, 1128, 3828, 1728 \text{ ou } 5628 \pmod{100}.$$

O que prova que $n \equiv 28 \pmod{100}$

□

A recíproca do teorema de Euclides sobre os números perfeitos foi provada, muito tempo depois por Euler, e é a seguinte

Teorema 59. (Euler) Se n é um número perfeito par, então, $n = 2^{k-1}(2^k - 1)$, onde $2^k - 1$ é um primo.

Demonstração. Seja n um número perfeito par. Assim sendo, n pode ser escrito como $n = 2^{k-1} \cdot m$ onde m é um número inteiro ímpar e $k \geq 2$. Então, temos que $\sigma(n) = \sigma(2^{k-1} \cdot m)$. E como σ é uma função multiplicativa, que pode ser utilizada uma vez que 2^{k-1} e m são coprimos, então temos que $\sigma(n) = \sigma(2^{k-1} \cdot m) = \sigma(2^{k-1})\sigma(m)$. Porém, também sabemos que $\sigma(2^{k-1}) = \frac{(2^{k-1+1}-1)}{2-1} = 2^k - 1$. Assim sendo, $\sigma(n) = (2^k - 1)\sigma(m)$. Como n é perfeito, então $\sigma(n) = 2n = 2 \cdot 2^{k-1} \cdot m = 2^k \cdot m$. Então temos, por um lado, que $\sigma(n) = (2^k - 1)\sigma(m)$ e, por outro, $\sigma(n) = 2^k \cdot m$, o que implica que

$$2^k \cdot m = (2^k - 1)\sigma(m)$$

Assim sendo, $(2^k - 1) | (2^k \cdot m)$. Mas, uma vez que $2^k - 1$ e 2^k são coprimos, por Euclides, temos que $2^k - 1 | m$.

Seja $m = (2^k - 1)M$. Assim,

$$2^k \cdot m = (2^k - 1)\sigma(m) \Leftrightarrow 2^k(2^k - 1)M = (2^k - 1)\sigma(m) \Leftrightarrow 2^k M = \sigma(m)$$

E já que $m | m$ e $M | m$, temos que

$$2^k M = \sigma(m) \geq m + M = (2^k - 1)M + M = 2^k M$$

Logo, $\sigma(m) = m + M$.

Então, m tem dois divisores, o que implica que m é primo, e seus divisores são m e 1, ou seja, $M = 1$.

Concluindo, temos que $m = (2^k - 1)M = (2^k - 1) \cdot 1 = 2^k - 1$ e como m é primo, é imediato que $2^k - 1$ é primo. □

Teorema 60. *Um número perfeito par termina em 6 ou 8. Equivalentemente, $n \equiv 6 \pmod{10}$ ou $n \equiv 8 \pmod{10}$.*

Demonstração. Seja n um número perfeito par tal que n possa ser representado como $2^{k-1}(2^k - 1)$ onde $2^k - 1$ é primo. De acordo com o teorema 57 dessa sessão, k também deve ser primo. Se $k = 2$, então $n = 6$ e o resultado é válido. Podemos então limitar nossa atenção para o caso de $k > 2$. Para isso, dividiremos essa prova em duas partes: (i) com k da forma $4m + 1$ e (ii) com k da forma $4m + 3$.

i) Se k for da forma $4m + 1$, então

$$n = 2^{4m}(2^{4m+1} - 1)$$

$$n = 2^{8m+1} - 2^{4m}$$

$$n = 2 \cdot 16^{2m} - 16^m$$

Usando a indução, é claro que $16^t \equiv 6 \pmod{10}$ para todo inteiro positivo t . Dessa congruência, temos

$$n \equiv 2 \cdot 6 - 6 \equiv 6 \pmod{10}$$

ii) Se k for da forma $4m + 3$, então

$$n = 2^{4m+2}(2^{4m+3} - 1)$$

$$n = 2^{8m+5} - 2^{4m+2}$$

$$n = 2 \cdot 16^{2m+1} - 4 \cdot 16^m$$

E recorrendo ao fato de que $16^t \equiv 6 \pmod{10}$ para todo inteiro positivo t , vemos que

$$n \equiv 2 \cdot 6 - 4 \cdot 6 \equiv -12 \equiv 8 \pmod{10}$$

Consequentemente, todo número perfeito termina em 6 ou 8. □

Observação 9. Chamamos de *raiz digital* de um número inteiro não negativo o resto da sua divisão por 9. Ou seja, somando-se seus algarismos e obtendo um número maior que nove, repete até que seja menor ou igual à 9. Se for igual a 9, então a raiz é zero, se for entre 0 e 9, então será a raiz digital do número. Uma propriedade especial, nesse caso, é que a raiz digital de qualquer número perfeito, sempre será 1.

Exemplo 15. A raiz digital de $256 = 2 + 5 + 6 = 13 \implies 1 + 3 = 4$ Logo, a raiz digital de 256 é igual a raiz digital de $13 = 4$.

A raiz digital de $28 = 2 + 8 = 10 \implies 1 + 0 = 1$ Logo, a raiz digital do número perfeito 8 é igual a raiz digital de 10 que é igual a 1 .

Teorema 61. *Somando os dígitos de qualquer número perfeito par (exceto 6), em seguida, somar os algarismos do número restante, e repetindo este processo até chegar um único dígito, então este dígito será sempre 1.*

Demonstração. Suponhamos que p seja um primo ímpar. Da proposição 12 temos que $2^{p-1} \equiv (-1)^{p-1} = 1 \pmod{3}$ uma vez que $p-1$ é par. Mas, uma vez que $p-1$ é par, temos que $2^{p-1} \equiv 1 \pmod{3}$, o que implica que

$$2^{p-1} = 3k + 1$$

para algum k inteiro. Multiplicando a equação acima por 2, teremos $2^p = 6k + 2$ logo, subtraindo 1 na igualdade, obteremos $2^p - 1 = 6k + 1$. Assim sendo,

$$\begin{aligned} 2^{p-1}(2^p - 1) &= \\ (3k + 1)(6k + 1) &= \\ 18k^2 + 9k + 1 &= \\ 9(2k^2 + k) + 1 &= \\ 9K + 1 &\equiv 1 \pmod{9} \end{aligned}$$

com $K = 2k^2 + k$. Assim sendo, a raiz digital de um número perfeito par (diferente de 6) é 1. □

Observação 10. *Para 6 não é válido pois, usando a fórmula $2^{p-1}(2^p - 1)$, teremos $p = 2$.*

Por consequência do nível de elementaridade das demonstrações de 63 a 69, uma vez explicados os conceitos necessários, podem ser aplicadas até em ensino fundamental e médio como atividades e desafios.

Teorema 62. *Um primo não pode ser um número perfeito.*

Demonstração. Seja p um primo. Então, $d(p) = p + 1$, onde d representa os divisores de p . Se p for um número perfeito, então $\sigma(p) = p$. Logo, teríamos que

$$p + 1 = p \implies 1 = p - p \implies 1 = 0$$

o que é uma contradição. Logo, um primo não pode ser um número perfeito. □

Teorema 63. *Todo número perfeito par, maior que 6, é múltiplo de 4.*

Demonstração. Seja n um número perfeito da seguinte forma $n = 2^{k-1}(2^k - 1)$. Já vimos que, então, k é um primo ímpar (pois não analisaremos o caso de $n = 6$). Assim, temos: (i) $k = 4t + 1$ ou (ii) $k = 4t + 3$ Ambos com $t \in \mathbb{N}$. Analisemos cada caso:

$$\begin{aligned} \text{i)} \quad n &= 2^{4t}(2^{4t+1} - 1) \\ n &= 4^{2t}(2^{4t+1} - 1) \\ n &= 4 \cdot (4^{2t-1}) \cdot (2^{4t+1} - 1) \end{aligned}$$

$$\begin{aligned} \text{ii)} \quad n &= 2^{4t+2}(2^{4t+3} - 1) \\ n &= 2^{4t} \cdot 2^2(2^{4t+3} - 1) \\ n &= 4 \cdot (2^{8t+3} - 2^{4t}) \end{aligned}$$

Assim, todo número perfeito é múltiplo de 4 para todo k primo $\neq 2$, □

Teorema 64. *Todo número perfeito par, maior que 6, pode ser escrito como uma diferença de dois quadrados perfeitos.*

Demonstração. Seja n um número perfeito par maior que 6. Do teorema anterior, temos que $n = 4k$, para algum $k \in \mathbb{N}$. Mas $4k$ pode ser reescrito como

$$n = (k + 1)^2 - (k - 1)^2$$

O que prova esse teorema. □

Antes de enunciarmos o próximo teorema, lembremos da seguinte proposição dos números naturais que diz:

Proposição 16. *Se p e q são números naturais tal que $\text{mdc}(p, q) = 1$, então todo número natural maior que ou igual a $pq - p - q + 1$ é obtido através de uma combinação linear $mp + nq$, com m e n inteiros não-negativos.*

Agora vamos ao teorema.

Teorema 65. *Qualquer número maior que 28 pode ser representado como a soma de, pelo menos, dois números perfeitos.*

Demonstração. Sabendo que o $\text{mdc}(3, 14) = 1$, então todo natural maior que $3 \cdot 14 - 3 - 14 + 1 = 26$ pode ser representado pela combinação linear $3x + 14y$ com $x, y \geq 0$. Multiplicando, convenientemente, por 2, obtemos que todo número par maior que 52, pode ser representado através da combinação linear de $6x + 28y$, inclusive, todo par perfeito com $n > 28$. $\square$

Teorema 66. *A soma dos inversos de todos os divisores de um número perfeito par (incluindo ele próprio) é igual a 2.*

Demonstração. Se n é um número perfeito par e $d_1, d_2, \dots, d_r$ são os divisores não triviais de n , então teremos:

$$\frac{1}{1} + \frac{1}{d_1} + \frac{1}{d_2} + \frac{1}{d_3} + \dots + \frac{1}{n} = \frac{n + \dots + d_3 + d_2 + d_1 + 1}{n}$$

Mas, como n é perfeito, então temos que $1 + d_1 + d_2 + d_3 + \dots = n$, então a soma será:

$$\frac{n+n}{n} = \frac{2n}{n} = 2.$$

$\square$

Observação 11. *Chamaremos de número triangular aqueles que são obtidos através da soma de consecutivos, ou seja*

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2} = T_n$$

Teorema 67. *Números perfeitos pares são triangulares.*

Demonstração. Suponhamos que P seja um número perfeito. Então, P será da forma

$$P = 2^{m-1}(2^m - 1) = \frac{(2^m - 1)2^m}{2}$$

Então, tomando $2^m - 1 = n$, teremos $2^m = n + 1$. Substituindo na equação, temos

$$p = \frac{n(n+1)}{2}.$$

O que é a forma de número triangular, como queríamos. $\square$

Teorema 68. *Se n é um número perfeito par, então $8n + 1$ é um quadrado perfeito.*

Demonstração. Seja n um número perfeito par, ou seja, $n = 2^{k-1}(2^k - 1)$. Então

$$\begin{aligned}
8n + 1 &= 8[2^{k-1}(2^k - 1)] + 1 \\
&= 2^3[2^{k-1+k} - 2^{k-1}] + 1 \\
&= 2^{3+k-1+k} - 2^{3+k+1} + 1 \\
&= 2^{2k+2} - 2^{k+2} + 1 \\
&= 2^{2(k+1)} - 2^{k+1+1} + 1 \\
&= (2^{k+1})^2 - 2 \cdot 2^{k+1} + 1 \\
&= (2^{k+1} - 1)^2
\end{aligned}$$

O que implica que $8n + 1$ é um quadrado perfeito uma vez que n é perfeito. $\square$

Teorema 69. *Seja $A(n)$ o conjunto de divisores primos de $n > 1$. Se n é um número perfeito par, então temos que*

$$A(n) = A(\sigma(n)).$$

Demonstração. Suponhamos que $p \in A(n)$. Então, pelo teorema 13, temos que

$$p \leq \sqrt{n} \leq \sqrt{2}\sqrt{n} = \sqrt{2n} \implies p \in A(2n)$$

Logo,

$$A(n) \subseteq A(\sigma(n))$$

Já que, por hipótese, n é um número perfeito par. De forma recíproca, se

$$p \in A(\sigma(n)) = A(2n) \implies p|2n \implies p|2 \text{ ou } p|n$$

Então, ou $p|2$, ou $p|n$, uma vez que n é perfeito. Logo, $p \in A(n)$. $\square$

Teorema 70. *Seja $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ um número natural em sua decomposição em fatores primos. Se k_i é um expoente par, onde $1 \leq i \leq r$, então $a = \sigma(p_i^{k_i})$ é ímpar.*

Demonstração. Suponhamos que o expoente seja um número par. Então, para $k = 2\alpha$, com $\alpha \in \mathbb{Z}$, temos

$$\sigma(p^k) = \frac{p^{k+1}-1}{p-1} = \frac{p^{2\alpha+1}-1}{p-1} = \frac{p^{2\alpha+1} \cdot p-1}{p-1} = \frac{p^{2\alpha+1} \cdot p-p+1}{p-1} = \frac{p^{2\alpha} \cdot p-p}{p-1} + \frac{p-1}{p-1} = \frac{p(p^\alpha+1) \cdot (p^\alpha-1)}{p-1} + 1$$

E como

$$\frac{p^\alpha - 1}{p - 1} = p^{\alpha-1} + p^{\alpha-2} + \dots + p + 1$$

então

$$a = p(p^\alpha + 1) \cdot (p^{\alpha-1} + p^{\alpha-2} + \dots + p + 1) + 1$$

E para $p = 2 \implies a = 2k + 1$, o que implica que a é ímpar. Já para $p > 2$, o fator $p^\alpha + 1$ é par. Logo, $a = 2k_1 + 1$, que também é ímpar. Portanto, para k par, o fator $\frac{p^{k+1}-1}{p-1}$ sempre terá resultado ímpar. $\square$

Teorema 71. *Um quadrado perfeito não pode ser um número perfeito.*

Demonstração. Se $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ é um quadrado perfeito em sua decomposição, então os expoentes k_i serão todos pares. Do teorema anterior, então todos os fatores de $\sigma(n)$ são ímpares. Sabendo que a multiplicação de ímpares, resulta em um ímpar, como propôs Euclides no livro IX: "Caso um número ímpar, tendo multiplicado um número ímpar, faça algum, o produzido será ímpar.", então a soma dos divisores de um número quadrado sempre será ímpar, ou seja, não será da forma $2n$ o que implica que não será um número perfeito. $\square$

2.3.2 Problemas em aberto

Como dito no início dessa sessão, Nichomachus apresentou em seu livro no século 100 d.C., cinco resultados não demonstrados (na época) acerca dos números perfeitos. São eles

- 1 O enésimo número perfeito têm n algarismos;

Esse, porém, já foi provado como não verdade. Apesar dessa regra valer para os quatro primeiros números perfeitos, a partir do quinto, já não vale uma vez que o quinto número perfeito - que é 33.550.336 - tem 8 dígitos.

- 2 Todos os números perfeitos são pares;

Esse ainda não possui demonstração uma vez que ainda não foi provada a existência ou inexistência dos números perfeitos ímpares.

3 Todos os números perfeitos terminam em 6 ou 8, alternadamente;

Apesar de termos provado anteriormente nessa seção que todos os números perfeitos pares terminam em 6 ou 8, essa terminação não é alternada como proposto nesse resultado. Um par que é contra-exemplo é o sexto e o sétimo número perfeito (respectivamente 33.550.336 e 8.589.869.056) que terminam em 6. Outro contra-exemplo seria o oitavo e o nono número perfeito (respectivamente 137.438.691.328 e 2.305.843.008.139.952.128) que são terminados em 8. Note também que, nesses casos, a regra do item 1 também não é válida.

4 Todo número perfeito é da forma $2^{k-1}(2^k - 1)$, $\forall$ inteiro $k > 1$, com $2^k - 1$ primo;

5 Existem infinitos números perfeitos.

Outro importante pesquisa dentro dos números perfeitos - e, mais especificamente, dos números de Mersenne - é a tentativa de provar que os primos de Mersenne são infinitos, ou seja, que existam p suficientemente grandes. Isso tem implicância direta nos números perfeitos uma vez que, buscar números de Mersenne, é também, procurar condições de números perfeitos. Conjectura-se que exista esse p e que p_n seja o n ésimo primo, tendo

$$0 < A < \frac{\log p_n}{n} < B < +\infty$$

tais que A e B são constantes. Outras conjecturas buscam uma precisão maior quando ao valor de

$$\lim_{n \rightarrow \infty} \sqrt[n]{p_n}$$

Esse limite é motivo de discussões uma vez que, para Eberhart, seja igual a 3, enquanto para Wagstaff, seja $2e^{-7} \approx 1,4757613971$.

Perfeitos ímpares

Outra forte área de pesquisa dentro dos números perfeitos, ainda sem provas, é a busca por números perfeitos ímpares o que, apesar de vários matemáticos, como Descartes, acreditarem na existência de tais números, ainda não pôde ser provada a existência - ou não - dos mesmos. Alguns teoremas foram propostos de maneira a tentar descobrir se tais números existem ou não e ainda na tentativa de traçar um caminho a fim de encontrar

uma solução. Os teoremas que traremos a seguir, apesar de já terem sido demonstrados (vide [7], [1], [8]), não foram capazes de provar ainda o essencial que é a existência e identificação da localização dos números perfeitos ímpares. Os teoremas propostos são os seguintes:

Teorema 72. *Seja $n \in \mathbb{N}$. Se n é ímpar, então n é a diferença de dois quadrados.*

Teorema 73. *Um número natural ímpar que tem pelo menos dois fatores com expoentes ímpares, não pode ser perfeito.*

Diversos matemáticos também propuseram formas e/ou condições da possível existência dos números perfeitos ímpares. Euler, por exemplo, propôs que, se existirem, devem ser da forma $n = p^{4\lambda+1}Q^2$ onde p é um primo da forma $4^n + 1$ o que é semelhante ao resultado de Frenicle (1657) que propôs que deve ser da forma $n = p^\alpha q_1^{2\beta_1} \dots q_r^{2\beta_r}$ tal que $p, q_1, \dots, q_r$ sejam primos distintos e $p \equiv \alpha \equiv 1 \pmod{4}$. Steuerwald ainda provou que os β_i s não podem ser todos 1. Touchard provou que, se existir, o número perfeito ímpar deve ser da forma $12k + 1$ ou $36k + 9$. Stuyvaert afirmou que a soma de dois quadrados será a forma de um perfeito ímpar. Sylvester conjecturou - o que foi provado por Gradshtein em 1925 - que qualquer número perfeito ímpar deve ter, ao menos, seis fatores primos distintos. Hagi provou que tais números devem ter, pelo menos, oito fatores primos distintos (sendo divisível por 15). O que foi aprimorado por Neilsen mostrando que se um perfeito ímpar não for divisível por 3, deve ter, pelo menos, 12 fatores de primos distintos. Mais tarde, Neilsen mostrou que, se um desses números existir, deve ter, ao menos, 9 fatores primos distintos. Catalão também estudou e provou que, se um número perfeito ímpar não é divisível por 3 ou 5 ou 7, então têm, pelo menos, 26 fatores de primos distintos - o que foi estendido para 27 fatores (que já havia mostrado que teria, ao menos, 15). Hare, em 2005, mostrou que para um número perfeito ímpar existir, ele deve ter, ao menos, 75 fatores primos. Com o auxílio de plataformas voltadas para a fatoração, já foi estendido para 101 fatores primos e, não necessariamente, distintos. Iannucci e Jenkins trabalharam para encontrar limites inferiores de um possível número perfeito ímpar. Os três menores fatores devem ser pelo menos 100000007, 10007 e 101. Goto e Ohno resolveram que o maior fator deve ser pelo menos 100000007 usando uma extensão aos métodos de Jenkins. Ochem e Rao, logo em seguida, mostraram que o maior divisor p^a com p primo é maior que 10^{62} .

Yamada determinou que, para o menor fator primo de um número perfeito ímpar com todas as potências pares inferiores a seis, o limite superior será de $\exp(497401.10^{10})$. Já Kishori estabeleceu limites superiores para pequenos fatores de números perfeitos ímpares, mostrando que $p_i < 2^{2^{t-i}}$ tal que $1 \leq i \leq 5$.

Como dissemos anteriormente, a demonstração, de fato, da existência ou não de números perfeitos ímpares ainda é um mistério e, se existirem, serão números extremamente grande - maiores que 10^{1000} .

Conclusão

O fascínio pelas propriedades dos números, como pudemos observar, não começou recentemente e, muito provavelmente, não acabará tão cedo visto a quantidade de resultados que ainda estão a serem provados. Ainda mais pelo fato de que, se desde a antiguidade o homem já tentava desvendar a misticidade de um número - mesmo em meio a tão poucas fontes de informação que se tinha - quanto mais agora que todas as informações estão a alguns cliques de nós.

Então vimos que embora já exista uma fórmula desenvolvida por Thabit Ibn Qurra e aperfeiçoada por outros estudiosos para encontrar pares de números amigos, a solução de encontrar esses pares ainda gerou outros problemas como a busca por pares de números amigos coprimos e/ou com paridade oposta ou ímpares não divisíveis por três entre outras.

Tivemos ainda a busca pela demonstração da conjectura dos números primos gêmeos que procura mostrar a infinitude dos mesmos, assim como dar solução aos teoremas que tem suas demonstrações como consequência direta de tal conjectura.

Por fim, estudamos os números perfeitos e percebemos que, para encontra-los, devemos primeiro encontrar primos de Mersenne que os satisfaçam e que, a prova da infinitude dos números perfeitos pares depende, diretamente, da infinitude dos primos de Mersenne. Além disso, ainda existe a incessante busca por números perfeitos ímpares que, apesar de já terem sido propostas várias formas para os mesmos, ainda assim, não foi possível prová-los.

Diante de todo o apresentado, definiremos ainda outros números considerados interessantes que são:

- de Fermat: são os números da forma $2^{2^n} + 1$ (como citado no capítulo 1)

- defectivos ou defeituosos ou deficientes: são os números nos quais a soma dos seus divisores próprios é menor que o número;
- abundantes: são os números nos quais a soma dos seus divisores próprios é maior que o número;
- sociáveis: são os números que a soma dos divisores do primeiro é igual ao segundo, a soma dos divisores do segundo é igual ao terceiro e, assim, sucessivamente até que a soma dos divisores do último seja igual ao primeiro;

E existem muitos outros nos quais o estudo de suas propriedades os tornam interessantes.

Mais uma vez é importante enfatizar que, ainda que tenhamos mostrado conceitos, em sua maioria, simples, e que geram problemas complicados, a pesquisa sobre isso não está perto do fim. Conforme mostrado nas ultimas partes de cada sessão do capítulo 2, ainda existem diversos problemas em aberto que, precisam de demonstração e desejamos que este trabalho sirva de base e incentivo para futuras pesquisas nas áreas estudadas.

Bibliografia

- [1] BRAUER. A. On the non-existence of odd perfect numbers of form $p^\alpha q_1^2 \dots q_{t-1}^2 q_t^4$, (1943), p. 712-718. Disponível em: <https://projecteuclid.org/journals/bulletin-of-the-american-mathematical-society-new-series/volume-49/issue-10/On-the-non-existence-of-odd-perfect-numbers-of-form/bams/1183505418.full>. Acesso em: 02 fev. 2021
- [2] BURTON, David M. Elementary Number Theory. 6th. ed. New York: McGraw-Hill, 2007. 452 p. Disponível em: https://napocaro.files.wordpress.com/2015/02/david_m_burton_elementary_number_theory_sixth_book_fi-org.pdf. Acesso em: 2 fev. 2021.
- [3] CARAÇA, Bruna Simoni. Um estudo sobre os números especiais. 2013. Trabalho de Conclusão de Curso (Licenciatura em Matemática) - Centro de Ciências Exatas e de Tecnologia, [S. l.], 2013. Disponível em: <https://www.dm.ufscar.br/dm/index.php/component/attachments/download/24>. Acesso em: 11 fev. 2021
- [4] CLEMENT, P. A. “Congruences for Sets of Primes.” The American Mathematical Monthly, vol. 56, no. 1, 1949, pp. 23–25. Disponível em: www.jstor.org/stable/2305816. Acesso em: 04 mai. 2021
- [5] CONG, Lin; LI, Zhipeng. On Wilson’s theorem and Polignac conjecture, Math. Me-dley 32 (2005), 11-16. Disponível em: [arXiv:math/0408018v1](https://arxiv.org/abs/math/0408018v1). Acesso em: 11 fev. 2021.

- [6] COSTA, Tito José Minhava Botelho da. Os números perfeitos e os primos de Mersenne. 2015. Dissertação de Mestrado (Mestrado em Matemática para Professores) - Faculdade de Ciências, [S. l.], 2015. Disponível em: [https : //repositorio.ul.pt/handle/10451/20623](https://repositorio.ul.pt/handle/10451/20623). Acesso em: 2 fev. 2021.
- [7] FERREIRA, Aran Jônatas Lucena. Números Perfeitos. 2014. Trabalho de Conclusão de Curso (Curso de Licenciatura Plena em Matemática) - Centro de Ciências Humanas e Exatas - CCHM, Paraíba, 2014. Disponível em: [http : //dspace.bc.uepb.edu.br/jspui/handle/123456789/10586](http://dspace.bc.uepb.edu.br/jspui/handle/123456789/10586). Acesso em: 7 mar. 2020.
- [8] GREATHOUSE, Charles and Weisstein, Eric W. "Odd Perfect Number."From MathWorld–A Wolfram Web Resource. Disponível em: [https : //mathworld.wolfram.com/OddPerfectNumber.html](https://mathworld.wolfram.com/OddPerfectNumber.html). Acesso em 2 fev. 2021
- [9] HUNTER, J. (1961). G. H. Hardy, and E. M. Wright, An Introduction to the Theory of Numbers (Fourth Edition) (Clarendon Press: Oxford University Press, 1960), 421 pp., 42s. Proceedings of the Edinburgh Mathematical Society, 12(3), 161-161. doi:10.1017/S0013091500002820. Disponível em: [https : //www.cambridge.org/core/journals/proceedings-of-the-edinburgh-mathematical-society/article/g-h-hardy-and-e-m-wright-an-introduction-to-the-theory-of-numbers-fourth-edition-clarendon-press-oxford-university-press-1960-421-pp-42s/B1E4BBA7889BE560D430501B44E9A20A](https://www.cambridge.org/core/journals/proceedings-of-the-edinburgh-mathematical-society/article/g-h-hardy-and-e-m-wright-an-introduction-to-the-theory-of-numbers-fourth-edition-clarendon-press-oxford-university-press-1960-421-pp-42s/B1E4BBA7889BE560D430501B44E9A20A) Acesso em: 02 fev. 2021
- [10] Khan Academy. Prova: série harmônica diverge. (vídeo). Disponível em: [https : //pt.khanacademy.org/math/ap-calculus-bc/bc-series-new/bc-10-6/v/harmonic-series-divergent::text=DemonstraC3A7C3A3o20de20que20a20sC3A9rie,uso20inteligente20da20manipulaC3A7C3A3o20algC3A9brica!](https://pt.khanacademy.org/math/ap-calculus-bc/bc-series-new/bc-10-6/v/harmonic-series-divergent::text=DemonstraC3A7C3A3o20de20que20a20sC3A9rie,uso20inteligente20da20manipulaC3A7C3A3o20algC3A9brica!). Acesso em 11 fev. 2021
- [11] MARTINEZ, Fabio E. Brochero; MOREIRA, Carlos Gustavo T. de A.; SALDANHA, Nicolau C.; TENGAN, Eduardo. Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro. 3. ed. [S. l.: s. n.], 2013. Disponível em: [http : //livrariavirtualimpa.br](http://livrariavirtualimpa.br). Acesso em: 8 jan. 2021.

- [12] PANTOJA, Pedro. Primos Gêmeos e outras Conjecturas. Revista Escolar de la Olimpiada Iberoamericana de Matemática, Portugal, n. 45, p. 1-11, 2012. Disponível em <https://docplayer.com.br/6262505-2-resultados-elementares-2-3-equivalencias-3-4-teorema-de-brun-e-a-conjectura-de-hardy-littlewood-5-5-conjecturas-9-referencias-10.html>. Acesso em 28 dez. 2020.
- [13] PENHA, G. M. de La. Euler e a Teoria dos Números. RPM - Revista Professor de Matemática, NW Washington, 24 fev. 2021. Disponível em: <https://rpm.org.br/cdrpm/4/4.htm>. Acesso em: 11 fev. 2021.
- [14] ROMERO, María G.; VARGAS, Jorge A.. Números Amigos. Revista de educación matemática, [S.l.], v. 11, n. 2, Apr. 2015. ISSN 1852-2890. Disponível em: <https://revistas.psi.unc.edu.ar/index.php/REM/article/view/11025/11601>. Acesso em: 12 Jan. 2021
- [15] RIZEL, Ari Camargo. Números Primos. 2014. Trabalho de Conclusão de Curso (Licenciatura em Matemática) - Instituto de Ciências Exatas, [S. l.], 2014. Disponível em: https://repositorio.ufmg.br/bitstream/1843/EABA-9REL7B/1/monografia_ary.pdf. Acesso em: 4 nov. 2020.
- [16] SANTAMARÍA, Diego Alonso. Números perfectos, multiperfectos y amigos. 2016. Trabajo Fin de Grado (Grado en Matemática) - Facultad de Ciencias, [S. l.], 2016. Disponível em: <http://uvadoc.uva.es/handle/10324/17209>. Acesso em: 21 jan. 2021.
- [17] SANTOS, Adécio da Silva. Demonstração da conjectura do número ímpar imperfeito. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 04, Ed. 05, Vol. 07, pp. 176-185. Maio de 2019. ISSN: 2448-0959. Disponível em: <https://www.nucleodoconhecimento.com.br/matematica/numero-impar>. Acesso em 10 fev. 2021
- [18] SANTOS, José Plínio de Oliveira. Intro: Introdução à Teoria dos Números. Rio de Janeiro: IMPA - Instituto de Matemática Pura e Aplicada, 1998. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4576612/mod_resource/content/1/JoseC

C8120PliCC81nio20de20Oliveira20Santos – IntroducCCA7aCC83o20aCC8020Teoria20dos20NuCC81meros – IMPA2028199829.pdf. Acesso em: 1 dez. 2020.

- [19] SBM. Primos gêmeos constituem um dos mistérios mais intrigantes da aritmética. [S. l.], 16 mar. 2018. Disponível em: <https://www.sbm.org.br/noticias/primos-gemeos-constituem-um-dos-misterios-mais-intrigantes-da-aritmetica>. Acesso em: 25 fev. 2021.
- [20] WEISSTEIN, Eric W. "Thâbit ibn Kurrah Rule." From MathWorld—A Wolfram Web Resource. Disponível em: <https://mathworld.wolfram.com/ThabitibnKurrahRule.html>. Acesso em: 21 jan. 2021.
- [21] WELLS, Diego. Prime Numbers: The Most Mysterious Figures in Math. New Jersey: John Wiley Sons, Inc., Hoboken, 2005. Disponível em: <https://www.arvindguptatoys.com/arvindgupta/primenumbers.pdf>. Acesso em: 12 jan. 2021.

Apêndice

Lista de pares de números amigos ímpares não divisíveis por 3

Todos têm o fator em comum $a = 5^4 \times 7^3 \times 11^3 \times 13^2 \times 17^2 \times 19 \times 61^2 \times 97 \times 307$

$$\begin{aligned} & \begin{cases} a \times 140453 \times 85857199 \\ a \times 56099 \times 214955207 \end{cases} \\ & \begin{cases} a \times 40063 \times 1083014405858114729 \\ a \times 759883871 \times 57100684400759 \end{cases} \\ & \begin{cases} a \times 40127 \times 24316459 \times 8637336284693 \\ a \times 894223226623 \times 9425008441529 \end{cases} \\ & \begin{cases} a \times 40459 \times 79670932151 \times 785235094643 \\ a \times 4071703 \times 621654783217660851119 \end{cases} \\ & \begin{cases} a \times 40459 \times 4075499 \times 11247066371 \\ a \times 6398629999 \times 289840477211 \end{cases} \\ & \begin{cases} a \times 40459 \times 4071703 \times 347952801041 \\ a \times 62791913183 \times 912890522669 \end{cases} \\ & \begin{cases} a \times 40127 \times 24316459 \times 131473538420639 \\ a \times 753760237567 \times 170197428069899 \end{cases} \\ & \begin{cases} a \times 40127 \times 456864935591 \times 2947460281395319 \\ a \times 24317567 \times 2222097774949919253614239 \end{cases} \end{aligned}$$

$$\begin{aligned}
& \begin{cases} a \times 40127 \times 24315667 \times 4668800173953586602539 \\ a \times 1410559270197839 \times 3229592045605749823 \end{cases} \\
& \begin{cases} a \times 40169 \times 43850540160157971076585196343983 \\ a \times 14887001 \times 132233805923 \times 894802182277066859 \end{cases} \\
& \begin{cases} a \times 52937 \times 2215291513690331 \times 134965225980517047468079 \\ a \times 164729 \times 1222569893 \times 78591197135018911142345778143 \end{cases} \\
& \begin{cases} a \times 52937 \times 2215291479910079 \times 1901293905067632711472171 \\ a \times 164729 \times 1222569893 \times 1107136751268199952431099377023 \end{cases} \\
& \begin{cases} a \times 48619 \times 1932038626331293043 \times 101457516345910172512469 \\ a \times 227597 \times 1787122884689 \times 23431070376718989407107294679 \end{cases} \\
& \begin{cases} a \times 40697 \times 7837685559226301 \times 302073366913892362707570079 \\ a \times 2565569 \times 2695609487 \times 13932610455428808648764074706747 \end{cases} \\
& \begin{cases} a \times 48619 \times 290822832708589621439 \times 14139515710202352254726567 \\ a \times 227597 \times 1787121242591 \times 491536226488477432136736101354399 \end{cases}
\end{aligned}$$

Lista de Números Amigos com menor fator primo distinto

$$\begin{aligned}
(445953248528881275, 659008669204392325) &= 5^2 \times 7 \times 13 \times 19 \times 37 \times 73 \times \begin{cases} 3^2 \times 43 \times 439 \times 22483 \\ 571 \times 1693 \times 5839 \end{cases} \\
(1097581690986390225, 1615281291559017775) &= 5^2 \cdot 7^3 \cdot 11^2 \cdot 31 \times \\
&\begin{cases} 3^3 \times 61 \times 4507 \times 4597 \\ 43 \times 2851 \times 409639 \end{cases} \\
(1281431098689616875, 1769164614201263125) &= 5^4 \times 7 \times 11^2 \times 19 \times \\
&\begin{cases} 3 \times 13 \times 373 \times 2503 \times 3499 \\ 31 \times 97 \times 1699 \times 34429 \end{cases} \\
(1993991197249826775, 2901232579265245225) &= 5^2 \times 7 \times 11^2 \cdot 13 \times 307 \times \\
&\begin{cases} 3^2 \times 109 \times 1567 \times 15349 \\ 439 \times 4297 \times 18199 \end{cases} \\
(4438032132485808675, 6288132595256655325) &= 5^2 \times 7^3 \times 13 \times 31 \times 43 \times
\end{aligned}$$

$$\begin{aligned}
& \begin{cases} 3^2 \times 61 \times 1291 \times 42139 \\ 37 \times 103 \times 11103889 \end{cases} \\
& (8265325617300085425, 12234092897366205775) = 5^2 \times 7 \times 13 \times 19 \times 31 \times \\
& \begin{cases} 3^3 \times 151 \times 727 \times 937 \times 2221 \\ 109 \times 1567 \times 1741 \times 30703 \end{cases} \\
& (9759636606249354825, 14162430025984014775) = 5^2 \times 7 \times 11^2 \times 13 \times \\
& \begin{cases} 3^2 \times 139 \times 241 \times 6967 \times 16879 \\ 223 \times 439 \times 7369 \times 71317 \end{cases}
\end{aligned}$$