Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional

Semigrupos Numéricos e suas Características

Leonardo Alcântara Portes

Goiânia

2013

sibi sistema de bibliotecas ufg

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR AS TESES E DISSERTAÇÕES ELETRÔNICAS (TEDE) NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **Trabalho de Conclusão de Curso de Mestrado Profissional**

2. Identificação da Tese ou Dissertação

Autor (a):	LEONARDO ALCÂNTARA PORTES		CPF: 71215042191		
E-mail:	leoallcan2@hotmail.com				
Seu e-mail pode ser disponibilizado na página?	[x]Sim	[ ] Não			
Vínculo empregatício do autor	PROFESSOR DO ENSINO MÉDIO E SUPERIOR				
Agência de fomento:	Coord. De Aperf. Pessoal de Nível Superior			Sigla:	CAPES
País: BRASIL	UF: GO		CNPJ:		
Título:	Semigrupos Numéricos e suas Características				
Palavras-chave:	Semigrupos, Número de Frobenius, Geradores e Sequências.				
Título em outra língua:	Numerical Semigroups and their Features				
Palavras-chave em outra língua:	Semigroups , Number of Frobenius , Generators and Sequences .				
Área de concentração:	Matemática do Ensino Básico.				
Data defesa: (dd/mm/aaaa)	01/10/2013				
Programa de Pós-Graduação:	MESTRADO				
Orientador (a):	Prof. Dr. RONALDO ANTÔNIO GARCIA				
E-mail:	ronaldoagarcia@gmail.com				
Co-orientador (a):*					
E-mail:					

*Necessita do CPF quando não constar no SisPG

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC da tese ou dissertação.

O sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses e ou dissertações, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.

Leonardo Alcântara Portes

Assinatura do (a) autor (a)

Data: 09 / 12 / 14

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

Leonardo Alcântara Portes

Semigrupos Numéricos e suas Características

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.
Área de Concentração: Matemática do Ensino Básico
Orientador: Prof. Dr. Ronaldo Alves Garcia

Goiânia

2013

Ficha catalográfica elaborada
automaticamente com os dados fornecidos pelo(a) autor(a).

Portes, Leonardo Alcântara
Semigrupos numéricos e suas características [manuscrito] / Leonardo Alcântara Portes. - 2013.
62 f.: il.

Orientador: Prof. Ronaldo Alves Garcia.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME) , Programa de Pós-Graduação em Matemática, Goiânia, 2013.
Bibliografia. Apêndice.
Inclui símbolos, lista de figuras.

1. Semigrupos. 2. Número de Frobenius. 3. Geradores e sequência. I. Garcia, Ronaldo Alves, orient. II. Título.

Leonardo Alcântara Portes

Semigrupos Numéricos e suas Características

Trabalho de Conclusão de Curso defendido no Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFG, do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática, área de concentração Matemática do Ensino Básico, aprovado no dia 01 de outubro de 2013, pela Banca Examinadora constituída pelos professores:

Prof. Dr. Ronaldo Alves Garcia
Instituto de Matemática e Estatística-UFG
Presidente da Banca

Prof. Dr. Flávio Raimundo de Souza
IFG/Goiânia

Prof. Dr. Jesus Carlos da Mota
Instituto de Matemática e Estatística-UFG

Leonardo Alcântara Portes graduou-se em Matemática pela Universidade Estadual de Goiás em 2005. Atualmente é professor da Secretaria Municipal de Educação em Goiânia, Colégio Unus , Colégio Metropolitano e outros.

Dedico esse trabalho à minha mãe que com honestidade , empenho e muito trabalho fez com que eu fosse o homem que sou hoje, além de sempre me apoiar nos estudos e cuidar para que eu pudesse chegar até aqui.

Agradecimentos

A Deus em primeiro lugar por estar sempre ao meu lado , me conduzindo pelos caminhos certos e mesmo quando tortuosos me fez chegar ao fim.

À minha mãe por ser a verdadeira representação de um anjo do Senhor ao meu lado, sempre me amando em todos os momentos de minha vida.

À minha esposa que foi quem me apoiou e me incentivou a começar essa batalha e não permitiu que eu a abandonasse nos momentos mais difíceis dessa luta.

À minha querida , amada e falecida irmã que, com certeza, onde quer que esteja está olhando por mim e sabida de ser minha eterna inspiração para continuar caminhando.

Ao amigo Dilermano Honório de Arruda por se fazer não só um amigo mas um verdadeiro pai me apoiando nos estudos e contribuindo para meu crescimento.

À minha querida amiga Eliane Cristina que foi quem me indicou a esse mestrado, me deu apoio e força para termina-lo e sempre acreditou em mim. Sem ela isso não seria possivel.

Aos demais colegas de PROFMAT pelas constantes ajudas e paciência que tiveram comigo, especialmente minha colega e amiga Viviane Kfouri.

Aos meus coordenadores e patrões pela disposição em me ajudar sempre que necessário.

Ao meu orientador, professor Dr. Ronaldo Alves Garcia, pelo seu conhecimento e paciência comigo, demonstrando sempre boa vontade em me ensinar e ajudar.

À CAPES pelo incentivo financeiro e à UFG por permitir que esse sonho se realizasse.

Resumo

O objetivo deste trabalho é mostrar a estrutura de semigrupos numéricos e suas características, mostrando a finalização destes em uma $P.A.$ (progressões aritméticas).Em seguida mostrar a curiosidades de alguns semigrupos e realizar muitos exemplos para facilitar o entendimento desta estrutura. Por fim mostramos a estrutura para generalizar o número de Frobenius em alguns semigrupos e para a quantidade de elementos presente nos semigrupos até a chegada deste número.

Palavras-chave Semigrupos, Número de Frobenius, Geradores e sequência.

Abstract

The objective of this work is to show the structure of numerical semigroups and their characteristics, showing the completion of these in a *P.A.* (arithmetic progressions).

Then we show the curiosities of some semigroups and many examples to facilitate understanding of this structure is presented.

Keywords Semigroups, Frobenius number, sequence and generators.

Lista de Figuras

Sumário

1 Introdução

Acostumados com os conteúdos de teoria de números e com as estruturas algébricas de grupo este trabalho visa dar ao leitor uma introdução básica sobre semigrupos numéricos.

Este trabalho visa mostrar a estrutura simples de um semigrupo e sua criação a partir de uma sequência definida ou a partir de geradores, usando apenas a operação de soma.

Os semigrupos tem grandes aplicações na matemática apesar de sua estrutura simples, porém nosso enfoque nesse texto é mostrar a estrutura e exemplos de semigrupos gerados por 2 ou 3 geradores. Além disso, queremos mostrar que a estrutura de semigrupos se desemboca em uma $P.A.$, o que torna esse conteúdo facilmente aplicado nos conteúdos de ensino médio.

Na primeira parte do trabalho fazemos uma introdução à álgebra, passando por conteúdos necessários ao entendimento de semigrupos e a outras partes bastante interessantes da álgebra como o Teorema de Fermat e as congruências lineares.

Na segunda parte mostraremos as estruturas de semigrupos e vários exemplos, além de mostrar algumas características importantes de semigrupos, alguns Teoremas, etc.

2 Seções de desenvolvimento do trabalho

Neste capítulo estudaremos as congruências lineares módulo m e algumas de suas aplicações. Estas equações são fundamentais para defirnirmos alguns conceitos necessários para a explicação dos semigrupos numéricos, que veremos adiante. Este capítulo foi baseado nas referências [1],[2],[5], [6],[7].

2.1 Congruências

Sejam $a,\ b,\ n \in \mathbb{Z}$. Dizemos que a é congruente a b módulo n, e escrevemos

$$a \equiv b(mod\ n)$$

se n divide $a - b$ deixam o mesmo resto na divisão por n.

Por exemplo temos que $7 \equiv 2(mod\ 5)$ ou que $31 \equiv 7(mod\ 6)$.
Com relação as congruências temos que elas possuem algumas propriedades:

- Reflexivas: $x \equiv x\ (mod\ w)$;
- Simétricas: $x \equiv y\ (mod\ w)$, então $x \equiv y\ (mod\ w)$;
- Transitivas: $x \equiv y\ (mod\ w)$, e $y \equiv a\ (mod\ w)$, então $x \equiv a\ (mod\ w)$;
- Compatíveis com a soma e a diferença :

$$\begin{cases} x \equiv y(mod\ w) \\ \\ a \equiv b(mod\ w) \end{cases} \Longrightarrow \begin{cases} x + a \equiv (x + b)(mod\ w) \\ \\ x - a \equiv (y - b)(mod\ w) \end{cases}$$

- Compatíveis com o produto :

$$\begin{cases} x \equiv y(mod\ w) \\ \qquad\qquad e \\ a \equiv b(mod\ w) \end{cases}$$

- Cancelamento : Se $\text{mdc}(c, w) = 1$ então

$$xc \equiv yc(mod\ w) \longleftrightarrow x \equiv y(mod\ w).$$

Exemplo 1. *Demonstrar que* $7 \mid 3^{15} - 6$.
Solução: Demonstrar que $7 \mid 3^{15} - 6$ *é o mesmo que provar que* $3^{15} \equiv 6(mod\ 7)$. *Observemos que :* $3^2 \equiv 2(mod\ 7)$.

Então temos $(3^2)^7 \equiv 2^7(mod\ 7)$ *e portanto* $(3^2)^7 \equiv 2(mod\ 7)$. *Isto é o mesmo que dizer que* $3^{14} \equiv 2(mod\ 7)$.

Multiplicando os dois membros por 3 *(o que não altera pois o* $mdc(3, 7) = 1$*) temos:* $3^{15} \equiv 6(mod\ 7)$, *como queríamos demonstrar.*

Exemplo 2. *Vamos determinar o resto da divisão de* 5^{300} *por* 122.

Solução: Temos que $5^{300} \equiv 3(mod\ 122)$

Então $(5^3)^{10} \equiv 3^{10}(mod\ 122) \longleftrightarrow (5^3)^{10} \equiv 59049(mod\ 122)$.

Como $59049 \equiv 1(mod\ 122)$, *temos que* $(5^3)^{10} \equiv 1(mod\ 122)$, *que é o mesmo que* $5^{30} \equiv 1(mod\ 122)$.

Elevando os dois membros a 10 *temos que* $(5^{30})^{10} \equiv 1^{10}(mod\ 122)$ *ou seja,*

$5^{300} \equiv 1(mod\ 122)$.

Então 122 *divide* $(5^{300} - 1)$, *ou seja, o resto da divisão de* 5^{300} *por* 122 *é* 1.

Exemplo 3. *Mostre que se a equação* $x^3 - 117$ *é múltiplo de* 9, *então qualquer solução inteira deve satisfazer*

$$x^3 - 117y^3 = 5(mod\ 9)$$

Solução: Observamos que x *só pode deixar resto de* 0 *a* 8 *na divisão por* 9. *Analisando estes casos temos:*

$x\ mod\ 9$	*0 1 2 3 4 5 6 7 8*
$x^3\ mod\ 9$	*0 1 2 3 4 5 6 7 8*

Ou seja, $x^3 \equiv 5(mod\ 9)$ *é impossível e a equação não possui raízes inteiras.*

Exemplo 4. *Mostre que* $13 \mid 5^{12} - 1$ *é o mesmo que provar que* $5^{12} \equiv 1(mod\ 13)$.

Solução:

Sabemos que $5^{12} \equiv -1(mod\ 13)$.

Portanto $5^{12} \equiv 1(mod\ 13)$, como queríamos demonstrar.

O exemplo 4 é um clássico do pequeno Teorema de Fermat que estudaremos adiante. Nesta parte do capítulo estudaremos as equações do tipo:

$$f(x) = 0(mod\ m)$$

na variável x, onde $f(x)$ é um polinômio com coeficientes inteiros. Para isso enunciaremos antes o *Teorema de Fermat* e a *Função de Euler*.

2.2 Teorema de Fermat e a Função de Euler

Para Estudar o Teorema de Fermat e a função de Euler precisamos antes definir o que é um sistema completo de restos (que chamaremos de scr) . Dizemos que um conjunto de n números inteiros $a_1, \ldots, a_n$ forma um sistema de restos módulo n (scr) se ele contém todos os possíveis restos da divisão por n , ou seja, $scr = 0, 1, 2, ..., n-1$.

Isto é, se os a_i representam todas as classes de congruência módulo n, temos, por exemplo, na divisão de um número qualquer n por 9 , que o conjunto $0, 1, 2, \ldots, 8$ formam um scr módulo 9. Equivalentemente, podemos dizer que $a_1, \ldots, a_n$ formam um scr módulo n se, e somente se, $a_i \equiv a_j (\text{mod } n)$ implicar $i = j$.

Então dizemos que a função de Euler $\varphi(n)$ é o número de inteiros positivos menores ou igual a n que são primos com n e denotaremos da seguinte maneira:

$$\varphi(n) = \{x \in \mathbb{N} / 1 \leq x \leq n, \text{mdc}(x, n) = 1\}$$

Exemplo 5.

n	1	2	3	4	5	6	7	8	9	10
φ (n)	1	1	2	2	4	2	6	4	6	4

$\varphi(1) = 1$ por que o único inteiro positivo menor ou igual a 1 é o próprio 1 e mdc (1,1) = 1.

Exemplo 6. *Para exemplificar o Teorema acima vamos calcular $\varphi(9)$. Veja o número de elementos do conjunto.*

$$\{x \in \mathbb{N} \ / \ 1 \leq x \leq 9 \ / \ mdc(x,9) = 1\} = \{1,2,4,5,7,8\}$$

Como o número de elementos do conjunto é 6*, então* $\varphi(9) = 6$.

Montar o conjunto φ para um certo η e contar seu número de elementos utilizando esse método é fácil apenas se este η for relativamente pequeno. Esta tarefa torna-se complicada com η relativamente grande, por exemplo $\eta = 12960$.

Mas se η for primo, simplesmente $\varphi(\eta) = \eta$ - 1, tendo em vista que todos os inteiros positivos menores que η primo são primos com o mesmo.

Vejam na tabela do exemplo 5

$$\varphi(2) = 1, \varphi(3) = 2, \varphi(5) = 4, \varphi(7) = 6,$$

e assim por diante .

Sendo η um inteiro positivo qualquer, como calcular $\varphi\ (\eta)$?

Para responder essa pergunta utilizaremos a propriedade de que a função de Euler é uma função aritmética multiplicatica, ou seja, se a e b são inteiros positivos tais que $\text{mdc}(a, b) = 1$, então

$$\varphi(ab) = \varphi(a).\varphi(b)$$

Para demonstrar a afirmação acima utilizaremos o Lema abaixo.

Lema 1. *Dados os inteiros positivos k, a e b, com mdc $(a, b) = 1$, então os restos das divisões dos a inteiros*

$$k, k + b, k + 2b, ..., k + (a - 1)b$$

por a , são todos diferentes.

Demonstração. Observe a desigualdade $0 \leq s, t < a$. Suponhamos por absurdo, que $\kappa + sb$ e $\kappa + tb$ deixem o mesmo resto na divisão por a. Assim, $\kappa + sb = aq + r$ e $\kappa + tb = aq' + r$. Então veja que a divide o produto $(s - t)b$:

$$(\kappa + sb) - (\kappa + tb) = (aq + r) - (aq' + r) \Rightarrow (s - t)b = a(q - q') \Rightarrow (q - q') = \frac{(s - t)b}{a}.$$

Por hipótese, $\text{mdc}(a, b) = 1$, logo a divide $(s - t)$, o que é impossível porque foi imposto que $0 \leq s, t < a$.

Concluímos então que os restos são todos diferentes. □

Corolário 1. *Se a não divide um número p qualquer, então o resto r $(0 \leq r < a)$ tem exatamente uma quantidade a de inteiros positivos, tal que estes dispostos em ordem são $0, 1, 2, ...a - 1$.*

Teorema 1. *A função de Euler é uma função aritmética multiplicativa.*

O que faremos é provar que $\varphi(ab) = \varphi(a).\varphi(b)$, desde que $\text{mdc}(a, b) = 1$.

Demonstração. Se $a = 1$ ou $b = 1$, o teorema é válido, pois

$$\varphi(1.b) = \varphi(b) = 1.\varphi(b) = \varphi(a).\varphi(b)$$
$$\varphi(a.1) = \varphi(a) = \varphi(a).1 = \varphi(a).\varphi(b)$$

Sejam, então $a > 1$ e $b > 1$. Vamos agora dispor todos os inteiros $1, 2, ..., ab$ em a linhas e b colunas, para daí tirar algumas conclusões.

0b+1	0b+2	.....	0b+k	....	1b
1b+1	1b+2	.....	1b+k	.....	2b
2b+1	2b+2	.....	2b+k	.....	3b
.....	.....	.....	.....	.....	.....
(a-1)b+1	(a-1)b+2	.....	(a-1)b+k	.....	ab

Os inteiros da κ-ésima coluna serão primos com b apenas se κ for primo com b.

De fato, pois, de modo inverso, b divide $qb + \kappa$, apenas se κ for múltiplo de b.

Suponhamos que a κ-ésima coluna seja uma destas $\varphi(b)$ colunas. Pelo Lema 1, os restos das divisões dos a inteiros desta coluna por a são $1, 2, ...a - 1$. Como sabemos, $\varphi(a) = 1, 2, ..., a - 1$. Logo o número de inteiros da κ-ésima coluna que são primos com a é $\varphi(a)$.

Portanto, em cada coluna (em um total de $\varphi(b)$ de inteiros onde todos são primos com b, vamos ter $\varphi(a)$ inteiros que são primos com a.

Logo, o número de inteiros da matriz $a \times b$ que são primos com a e b é $\varphi(a)\varphi(b)$. É claro que todo número que não tem fatores primos com a e b também não terão com o produto ab. Assim, $\varphi(a).\varphi(b)$ também é a quantidade de inteiros positivos menores que, e primos, com ab.
Conclusão : $\varphi(\text{ab}) = \varphi(a)\varphi(b)$.

□

Corolário 2. *Se os inteiros positivos $a_1, a_2, \ldots, a_n = a, b, c, ..., z$ respectivamente , e $a, b, ..., z$ são dois a dois primos entre si, então*

$$\varphi(a_1, a_2, a_3, \ldots, a_n) = \varphi(a_1)\varphi(a_2)\varphi(a_3)\ldots\varphi(a_n)$$

ou

$$\varphi(a, b, c, \ldots, z) = \varphi(a)\varphi(b)\varphi(c)\ldots\varphi(z)$$

Esta generalização do teorema é uma propriedade comum à todas as funções aritméticas multiplicativas.

Agora já sabemos que se $n = p$ é primo, então $\varphi(p) = p - 1$. Então dado $a \in \mathbb{N}$, com $a \geq 1$, vamos estabelecer a fórmula para o cálculo de $\varphi(p^a)$.

Teorema 2. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

Demonstração. Os inteiros menores que p^a e que são primos com p

$$t.p = p^\alpha \Rightarrow t = p^{\alpha-1}$$

Então como t indica a quantidade de inteiros menores que p^α que não são primos com p^α, a quantidade de inteiros que são menores que p e primos com p^α são exatamente $p^\alpha - p^{\alpha-1}$. Assim, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

□

Associando a propriedade multiplicativa da função de Euler e o Teorema 2, conseguimos calcular $\varphi(n)$ para qualque inteiro positivo n .

Exemplo 7. *Calcular* $\varphi(5625000)$.

Primeiro passo: Fatorar $n = 5625000$*, ou seja,* $n = 2^3.3^2.5^7$

Segundo passo: Calcular $\varphi(p^a) = p^a - p^{a-1}$.

$$\varphi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$$

$$\varphi(3^2) = 3^2 - 3^1 = 9 - 3 = 6$$

$$\varphi(5^7) = 5^7 - 5^6 = 78125 - 15625 = 62500$$

Por último, aplicamos a propriedade multiplicativa de $\varphi(n)$.

$\varphi(5625000) = \varphi(2^3.3^2.5^7) = 4.6.62500 = 1500000$

O **último teorema de Fermat**, afirma que não existe nenhum conjunto de inteiros positivos x , y , z e n com n maior que 2 que satisfaça

$$x^n + y^n = z^n.$$

2.3 Equações módulo m

Se $\text{mdc}(a, m) = 1$, como a é invertível módulo m, a equação

$$ax \equiv b(mod\, m),$$

tem solução única módulo m, dada por

$$x \equiv a^{\varphi(m)-1}b(mod\, m).$$

Utilizando o Teorema de Fermat temos que todas as soluções da equação acima são da forma

$$x \equiv a^{\varphi(m)-1}b + km(mod\, m),$$

onde $k \in \mathbb{Z}$

Temos que na congruência linear do tipo

$$ax \equiv b(mod\, m),$$

um inteiro x será uma solução se existir $y \in \mathbb{Z}$ tal que $ax - b = my$.

Logo, se $d = \text{mdc}(a, m)$, então para que exista solução devemos ter que $d|b$ pois $b = ax - my$

Por outro lado, sabemos que existem inteiros x_0 e y_0 tais que

$$ax_0 + my_0 = d$$

x_0 e y_0 podem ser encontrados através do algorítmo de Euclides, com o qual se calcula d.

Então, se $d|b$, temos que

$$ax_0\frac{b}{d} + my_0\frac{b}{d} = b$$

e vemos que a equação modular tem a solução $x = x_0\dfrac{b}{d}$ (ou a classe de congruência deste número).

Para analisar a existência de outras soluções, supomos que z e w satisfazem igualmente $az - mw = b$; então

$az - mw = ax - my \Leftrightarrow a(a - x) = m(w - y) \Leftrightarrow \dfrac{a}{d}(z - x) = \dfrac{m}{d}(w - y)$

mas, como $\dfrac{a}{d}$ e $\dfrac{m}{d}$ são primos entre si, isso implica que

$$\frac{m}{d}|(z-x)$$

ou seja

$$z = x + k.\frac{m}{d}, k \leq d$$

Duas soluções desta forma serão congruentes módulo m se $d|k$. Temos, portanto, d soluções distintas, correspondentes aos valores $0 \leq k < d$.

Logo, daí, temos a seguinte proposição

Proposição 1. *Para $m \in \mathbb{N}$, $a \in \mathbb{Z}$ e $d = mdc(a, m)$ a equação*

$$ax \equiv b(mod\ m)$$

tem d soluções distintas se $d \mid b$ e não tem soluções se $(d \nmid b)$(que é o mesmo que dizer que d não divide b).

Se x_0 e y_0 são inteiros satisfazendo $ax_0 + my_0 = d$, as soluções do primeiro caso são

$$x_0\frac{b}{d} + k\frac{m}{d}, 1 \leq k < d$$

Neste caso o número de soluções distintas módulo m da equação é exatamente o $\text{mdc}(a, m)$.

Exemplo 8. *Agora vamos resolver a equação $12x \equiv 28(mod\ 8)$*

Observe que o $mdc(12, 8) = 4$ e como $4|28$, logo pelo Teorema acima sabe-se que esta equação tem 4 soluções.

Testando, encontramos como soluções $3, 5, 7$ e 9. Qualquer outra solução é congruente a uma dessas, módulo 8.

Exemplo 9. *Encontrando a solução da equação $10x \equiv 11(mod\ 9)$*

Observe que o $mdc(10, 9) = 1$, e como $1 \mid 9$ a equação tem uma única solução.

Podemos ver que a solução é 2; qualquer outra solução é congruente a essa, módulo 9.

Para resolvermos um sistema de congruências lineares, podemos usar o Teorema chinês do resto, que garante a existência de solução para este tipo de sistemas.

2.4 Teorema Chinês dos Restos

Considere o sistema de equações

$$\begin{aligned} K &\equiv c_1 (\text{mod } n_1) \\ K &\equiv c_2 (\text{mod } n_2) \\ K &\equiv c_3 (\text{mod } n_3) \\ &\cdots \\ K &\equiv c_k (\text{mod } n_k) \end{aligned} \tag{1}$$

Teorema 3. *O sistema* (1)*, onde* $mdc(n_i, n_j) = 1$*, para todo* n_i*,* n_j *com* $i \neq j$*, possui uma única solução módulo N, com* $N = n_1 n_2 \dots n_k$*. Tal solução pode ainda ser obtida da seguinte maneira :*

$$X = N_1 Y_1 C_1 + N_2 Y_2 C_2 + ... + N_r Y_r C_r$$

onde $N_i = N/n_i$ *e* y_j *é solução de* $N_i Y \equiv 1 (mod\ n_i)$ *,* $i = 1, 2, ...r$*.*

Demonstração. Vamos inicialmente provar que x é uma solução simultânea do sistema (1). De fato, como $n_i \mid N_i$, se $i \neq j$, e $N_i y_j \equiv 1\ (mod\ n_i)$ segue-se que

$$X = N_1 y_1 c_1 + N_2 y_2 c_2 + \cdots + N_r y_r c_r \equiv N_i y_i c_i (mod\ n_j).$$

Por outro lado, se x' é outra solução do sistema (1), então

$$X \equiv x' (mod\ n_i), \forall i, i = 1, 2, ..., r.$$

Como $\text{mdc}(n_i, n_j) = 1$ (ou podemos dizer apenas $(\text{n}_i,\text{n}_j) = 1$), $i \neq j$, segue-se que o mmc de $n_1, \dots, n_r$, que podemos representar por $[n_1, \dots, n_r]$, é igual a $n_1, \dots, n_r = N$ e , consequentemente, temos que

$$X \equiv x (mod\ N).$$

□

Exemplo 10. *Vamos agora resolver o famoso problema de Sun-Tsu, matemático chinês que viveu no século* 3 *d.C. , que propõe encontrar o número que deixa restos* 2 *,* 3 *e* 2 *quando dividido por* 3*,* 5 *e* 7*, respectivamente.*

Solução : *Resolver o problema de Sun-Tsu é o mesmo que resolver o sistema de congruências*

$$\begin{aligned} K &\equiv 2(mod\ 3) \\ K &\equiv 3(mod\ 5) \\ K &\equiv 2(mod\ 7) \end{aligned} \tag{2}$$

Temos que $N_3 = 3.5.7 = 105$*;* $N_1 = 35$*,* $N_2 = 21$ *e* $N_3 = 15$*.*

Temos também que resolvendo as equações $35Y \equiv 1(mod\ 3)$*,* $21Y \equiv 1(mod\ 5)$ *e* $15Y \equiv 1(mod\ 7)$ *encontramos as soluções* $y_1 = 2$*,* $y_2 = 1$ *e* $y_3 = 1$*, respectivamente. Portanto, uma solução módulo* $N = 105$ *é dada por*

$$X = N_1y_1c_1 + N_2y_2c_2 + N_3y_3c_3 = 233.$$

Como $233 \equiv 23(mod\ 105)$*, então é a solução única, módulo* 105*, do problema de Sun-Tsu e qualquer outra solução é da forma* $23 + \lambda 105$*, com* $\lambda \in \mathbb{N}$*.*

3 Equações Diofantinas

Neste capítulo estudaremos as equações diofantinas e o Pequeno Teorema de Fermat. Esses dois tópicos são usados nos semigrupos gerados por n elementos, que estudaremos logo a seguir. Estes conceitos nos darão condições para provar alguns tópicos em relação aos semigrupos, e foi escrito baseado em [5], [6], [7], [8] e [11]

3.1 Equações Diofantinas

Diofanto, nascido em $221d.C.$, viveu em Alexandria já sobre o domínio romano e faleceu aos 84 anos. Foi um dos únicos matemáticos de renome de sua época que dedicou seu trabalho à teoria dos números.

As equações polinomiais com coeficientes inteiros e soluções inteiras ou racionais são chamadas hoje de Equações Diofantinas.

As equações diofantinas que iremos estudar são do tipo $ax + by = n$, com a,b e $n \in \mathbb{Z}$.

As equações desse tipo só admitem solução se, e se somente se, o $\text{mdc}(a, b) \mid n$. Observe que se x_0 e y_0 é uma solução particular da equação $ax + by = n$ então temos que x e y serão soluções desta mesma equação se, e somente se,

$$x = x_0 + \frac{t.a}{(a, b)}$$

e

$$y = y_0 + \frac{t.a}{(a, b)}$$

para algum $t \in \mathbb{Z}$, em que $(a, b) = \text{mdc}(a, b)$.

Exemplo 11. *Resolver a equação 12x -7y = 9*
Como mdc$(12, 7) \mid 9$ *a equação tem solução. Vamos encontrar a solução* (x_0, y_0) *desta equação.*

Pelo algoritmo euclidiano, temos:

$$12 = 7.1 + 5$$
$$7 = 5.1 + 2$$
$$5 = 2.2 + 1$$

Isolando as equações temos

$$1 = 5 - 2.2 \ (a)$$
$$2 = 7 - 5.1 \ (b)$$
$$5 = 12 - 7.1 (c)$$

Substituindo (c) em (b) obtemos :

$$2 = 7 - 12 + 7 = 7.2 - 12 \ (d)$$

Substituindo (c) e (d) em (a) obtemos :

$$1 = 12 - 7.1 - 2\,(7.2 - 12) = 12 - 7.1 - 7.3 + 12.2$$

Então temos

$$1 = 12.3 - 7.5$$

E, portanto,

$$9 = 12.27 - 7.45$$

Logo, $x_1 = 27$ *e* $y_1 = 45$ *é uma solução particular da equação.*
Vamos agora determinar a solução da equação :

$$x = 27 + t.7 \text{ e } y = 45 - t.12.$$

Encontrando o maior valor de $t \in \mathbb{N}$*, de modo que* $x, y \in \mathbb{N}$*.*
Neste caso, isso ocorre quando $t = 3$*, logo a solução é* $x_0 = 6$ *e* $y_0 = 9$*.*
As soluções da equação são

$$x = 6 + 7t \text{ e } y = 9 + 12t.$$

Depois dos trabalhos de Diofanto a Aritmética ficou muitos anos sem um grande salto. Apesar de algumas descobertas ela só voltou a ter grandes avanços através de Pierre de Fermat, um jurista francês que viveu no séc. $XVII$ e contribuiu com vários teoremas , dentre eles um bastante usado na álgebra, o Pequeno Teorema de Fermat.

3.2 O Pequeno Teorema de Fermat

Teorema 4. *Seja* a *um inteiro positivo e* p *um primo, então*

$$a^p \equiv a(mod\ p).$$

Demonstração. Vamos provar por indução sobre a.

Para $a = 1$ é claro o resultado, pois p divide 0 ($p \mid 0$).

Suponha o resultado válido para a. Iremos provar que ele também vale para $a + 1$. Pela fórmula do Binômio de Newton,

$$(a+1)^p - (a+1) = a^p - a + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1} + ... \begin{pmatrix} p \\ p-1 \end{pmatrix} a \quad . \tag{3}$$

Como os números $\begin{pmatrix} p \\ 1 \end{pmatrix}$ são todos divisíveis por p, sendo p um número primo, então por isso e pela hipótese temos que

$$a^p - a + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1} + ... \begin{pmatrix} p \\ p-1 \end{pmatrix} a \tag{4}$$

é divisível por p. □

Então podemos enunciar o pequeno Teorema de Fermat da seguinte forma:

$$a^p \equiv a(mod\ p)$$

ou

$$a^p - 1 \equiv 1(mod\ p)$$

Exemplo 12. *Vamos agora encontrar o resto da divisão de* 2^{100} *por* 11.

solução : *Pelo teorema acima temos que* $2^{10} \equiv 1(mod\ 11)$.
Elevando ambos os lados da equação por 10 *temos que* $2^{100} \equiv 1(mod\ 11)$ *ou seja, o resto da divisão de* 2^{100} *por* 11 *é* 1.

Exemplo 13. *Calculando agora o resto da divisão de* 7^{213} *por* 17 *:*

solução : *Observe que* $7^{213} = 7^{16.13+5}$
Temos que $7^2 \equiv -2\ (mod\ 17)$ *e* $7^5 \equiv 11(mod\ 17)$
Como $7^2 \equiv -2\ (mod\ 17)$
Elevando os dois lados à quarta potência temos :
$(7^2)^4 \equiv 16\ (mod\ 17)$
Que também pode ser escrito
$7^8 \equiv -1(mod\ 17)$
Elevando os dois lados ao quadrado temos :
$7^{16} \equiv 1(mod\ 17)$

Elevando os dois lados a treze e multiplicando por 7^5 *temos :*
$(7^{16})^{13}$.$(7^5) \equiv (1^{13}).\ 7^5\ (mod\ 17)$
Ou seja, $7^{213} \equiv 7^5 (mod\ 17)$
E como $7^5 \equiv 11 (mod\ 17)$*, logo*
$7^{213} \equiv 11 (mod\ 17)$
Logo o resto dessa divisão é 11.

Observamos que as equações diofantinas não lineares são muito complexas e dariam, por si só, um trabalho sobre elas.

4 Os semigrupos numéricos

Neste capítulo estudaremos os semigrupos gerados por 2 e 3 elementos , além de mostrar algumas de suas características e aplicações.

Estudaremos regularidades de alguns semigrupos, além de mostrar alguns teoremas importantes acerca do estudo destas estruturas. Esse capítulo foi escrito baseado nas referências [8], [10], [12] e [17].

4.1 Semigrupos Numéricos

Subconjuntos S de $\mathbb{N} \cup \{0\}$ são chamados de semigrupos quando 0 pertence a S e quando $x,\ y$ pertencem a $S \Longrightarrow x + y \in S$.

Um semigrupo S é dito de razão r se existe $a_0 \in S$ tal que $S \cap \{a_0, a_0 + r, a_0 + 2r, ...\}$ é igual a $\{a_0, a_0 + r, a_0 + 2r, ...\}$,ou seja, o semigrupo é uma progressão aritmética $(P.A.)$ de razão $r > 0$ a partir de a_0.

Quando esta $P.A.$ for de razão 1 este semigrupo será chamado de *semigrupo aritmético* ou *numérico*.

Dizemos que o menor elemento de S que satisfazer essa condição é chamado de *regularizador aritmético* deste semigrupo e será denotado por $r(S)$.
Os números inteiros l não pertencentes ao semigrupo S são chamados de *lacunas* e o número de lacunas g é chamado de *gênero*.

Exemplo 14. *Seja* $S_1 = \{0, 5, 6, 7, 8, 9, \ldots\}$.

Como S_1 *é um semigrupo, o regularizador de* S_1 *é* 5*, ou seja,* $r(S_1) = \{5\}$

Se temos um semigrupo numérico então $\mathbb{N}\backslash S$ é um conjunto finito e $r(S) = F(S)+1$, em que $F(S)$ é chamado de *número de Frobenius deste semigrupo.*

Ou seja, o conjunto das lacunas de S é denotado por $L_S = \mathbb{N}\backslash S$.

Se em algum caso $L_S = \{l_1 < l_2 < l_s\}$ for finito, dizemos que l_s é a maior lacuna de S.

Exemplo 15. $S_1 = \{0, 5, 6, 7, 8, 9, 10, 11, \}$ *é um semigrupo. Temos* $L_{S_1} = \{1, 2, 3, 4\}$. *Como o conjunto das lacunas de* S_1 *é finito e seu maior elemento é o* 4*, então* $l_s = 4$

Exemplo 16. *O conjunto das lacunas do semigrupo formado pelos números pares* $S = \{0, 2, 4, 6, \ldots, 2k, \ldots\}$ *é* $L_S = \{1, 3, 5, 7, 9, \ldots, 2k + 1, \ldots\}$ *e como este conjunto é infinito ele não possui número de Frobenius e seu regularizador aritmético* $r(S)$ *é o zero.*

Usualmente representamos um semigrupo S na seguinte forma:

$$S = \{0, s_1, s_2, \ldots, s_n, \ldots\}$$

.

Poderia restar dúvidas se os sucessores de s_n, no semigrupo, são todos os naturais maiores que s_n. Para evitar essas dúvidas, passaremos tambémm a expressar um semigrupo por meio de seus geradores.

Definição 1. *Sejam* S *um semigrupo com regularizador* $r(S)$ *e um elemento qualquer* $p \neq 0$ *de* S*. O número de Frobenius é uma unidade a menos que o regularizador , ou seja ,* $F(S) = r(S) - 1$.

Estudaremos agora alguns resultados envolvendo o gênero g e a maior lacuna l_g do semigrupo S.

Sejam $a_1, a_2, \ldots, a_n \in \mathbb{N}$. O semigrupo gerado pelo conjunto $\{a_1, a_2, \ldots, a_n\}$ é dado por: $S :=< a_1, a_2, \ldots, a_n >= \{a_1x_1 + a_2x_2 + \cdots + a_nx_n : \ x_1, x_2, \ldots, x_n \in \mathbb{N} - 0\}$.

S é um semigrupo numérico se, e somente se, mdc$(a_1, a_2, ..., a_n) = 1$.

Existe um conjunto natural que gera um semigrupo.

Tome:

$$s_i = min\{h \in H : h \equiv i(mod\ n_1)\},$$

ou seja, S é gerado por $\{n_1, s_1, \ldots, S_{n_1} - 1\}$ e não se tem necessariamente que o número de geradores de S é o menor possível.

Vamos agora discutir a possibilidade de se obter uma fórmula explícita para o gênero g e para a maior lacuna l_g em função dos geradores do semigrupo S.

Para $S =< a_1, a_2 >$ pode se escrever que $g = \dfrac{(a_2 - 1)}{2}$ e $l_g = (a_1 - 1) - 1$.

Como mdc$(a_1, a_2) = 1$ então existem z e $t \in \mathbb{Z}$ tais que $a_1 z + a_2 t = 1$.

Suponha que $z \geq a_2$. Pelo algoritmo da divisão de Euclides tem-se que $z = a_2 q + r$ com $q \geq 1$ e $0 \leq r < a_2$. Deste modo $a_1 z + a_2 t = a_1(a_2 q + r) + a_2 t = a_1 r + a_2(a_1 q + t)$.

Chamando $x = r$ e $y = a_1 q + t$ tem-se que $a_1 z + a_2 t = a_1 x + a_2 y$.

Logo podemos considerar a seguinte igualdade $a_1 x + a_2 y = 1$ para todo x e $y \in \mathbb{Z}$ com $0 \leq x < a_2$.

Esta nova representação se torna única. Então para qualquer $n \in \mathbb{N}$ tem-se que $n = n.1 = n(a_1 x + a_2 y) = a_1 nx + a_2 ny$.

Desta maneira $n \in S$ se, e somente se, $a_1 n_x, a_2 n_y \leq 0$. Tome $m = max\{n : n \notin H\}$. Então m é dado por $x = a_2 - 1$ e $y = -1$. Assim $l_g = a_1(a_2 - 1) - a_2 = (a_1 - 1)(a_2 - 1) - 1$. Como $n_g = l_g + 1$ tem-se que $l_g + 1 = (a_1 - 1)(a_2 - 1)$.

Para determinar g deve-se contar até quando $a_1(a_2 - 1) - (a_2 - 1)$ - $na_2 \in S$, ou seja,

$$a_1(a_2 - 1) - na_2 > 0, com\ 0 \leq b \leq a_1 - 1.$$

Então temos que $g = \dfrac{(a_1 - 1)(a_2 - 1)}{2}$

Não conhecemos a resposta deste problema para $n > 2$. No caso em que $n = 3$, e supondo que os geradores são co-primos(primos entre si) , exibiremos uma fórmula que já foi provada por dois matemáticos (Rosales e Sanches-Garcia).

Considere S um semigrupo minimamente gerado por $\{a_1, a_2, a_3\}$ tais que $\text{mdc}(a_i, a_j) = 1$ para todo $i \neq j$ com $1 \leq i, j \leq 3$. Sejam $i,\ j$ e k números inteiros entre 1 e 3 , definimos :

$c_i := min\{n \in \mathbb{N} : na_i \in < a_j, a_k >\}$.

Tem-se que :

$$\begin{cases} c_1a_1 = r_{12}a_2 + r_{13}a_3 \\ c_2a_2 = r_{21}a_1 + r_{23}a_3 \\ c_3a_3 = r_{31}a_1 + r_{32}a_2 \end{cases}$$

Os r_{ij} acima definidos são inteiros positivos.

Os geradores a_1, a_2 e a_3 podem ser reescritos como :

$$\begin{cases} a_1 = r_{12}r_{13} + r_{21}r_{23} + r_{13}r_{32} \\ a_2 = r_{13}r_{21} + r_{21}r_{23} + r_{23}r_{31} \\ a_3 = r_{12}r_{31} + r_{21}r_{32} + r_{31}r_{32} \end{cases}$$

4.2 Alguns Teoremas Importantes

Teorema 5. *[Teorema de Sylvester] Sejam a e b números naturais tais que $mdc(a, b) = 1$ e considere o semigrupo $S(a, b)$ gerado por a e b. A maior lacuna de $S(a, b)$ de $\mathbb{N} \setminus S(a, b)$ é o número (ímpar) de Frobenius $F(a, b)$,*

$$F(a, b) = ab - (a + b) = (a - 1)(b - 1) - 1 = r(S) - 1.$$

O semigrupo $S(a, b)$ é aritmético.

Demonstração. Sejam a e b números inteiros positivos tais que o máximo divisor comum $\text{mdc}(a, b)$ seja igual a 1, isto é, a e b são primos entre si. Equivalentemente, $\text{mdc}(a, b) = 1$ se, e somente se, as progressões aritméticas

$P(a) = \{0, a, 2a, \ldots, ma, \ldots\} = a\mathbb{N}$ e $P(b) = \{0, b, 2b, 3b, \ldots, nb, \ldots\} = b\mathbb{N}$ possuem elementos que diferem de uma unidade inteira.

Portanto existem inteiros positivos $m, n \in \mathbb{N}$ tais que $|ma - nb| = 1$. Assim a equação linear $ax + by = 1$ possui infinitas soluções inteiras. Se (x_0, y_0) for uma solução particular , então todas as demais soulções inteiras são parametrizadas por $x(n) = x_0 + bn$ e $y(n) = y_0 - an$, $n \in \mathbb{Z}$. Quando uma solução (x_0, y_0) da equação

$ax+by=1$ pertence ao primeiro quadrante do plano xy , isto é $x \geq 0$ e $y \geq 0$, dizemos que a soluçao é não negativa . Se $x_0 > 0$ e $y_0 > 0$ a soluçao é positiva.

Para continuar a demonstração usaremos os teoremas e lemas a seguir.

Teorema 6. *Sejam a e b números naturais tais que $mdc(a,b) = 2$.*

Então dizemos que $S(a,b)$ é um semigrupo de razão 2 e o seu regularizador aritmético é o número par ,

$$r(S(a,b)) = \frac{1}{2}.(a-2)(b-2).$$

Devido aos Teoremas 5 e 6 é natural esperar uma generalização para semigrupos $S(a,b)$ com $\text{mdc}(a,b) = k,\ k \geq 3$.

Teorema 7. *Sejam a e b números naturais tais que $mdc(a,b) = k,\ k \geq 3$.*

Então $S(a,b)$, o semigrupo gerado por a e b é um semigrupo de razão k e o seu regularizador aritmético é dado

$$r(S(a,b)) = \frac{1}{k}.(a-k)(b-k).$$

□

Lema 2. *Seja $mdc(a,b) = 1$. Então, a equação diofantina $ax + by = ab + r$ possui soluções inteiras positivas para todo $r \in \mathbb{N}$ e somente as soluções não negativas $(0,a)$ e $(b,0)$ para $r = 0$.*

Demonstração. Primeiro mostramos que o Lema é verdadeiro para $r = 0$.

Temos que a equação $ax + by = ab$ possui soluções particulares $(b,0)$ e $(0,a)$.

As demais soluções são dadas por $x(n) = bn$, $y(n) = a - an$, $n \in \mathbb{Z}$ e nenhuma delas pertence ao primeiro quadrante.

Em seguida, para demonstrar o Lema para r ≥ 1 tomamos uma solução inteira da equação diofantina $ax_0 + by_0 = 1$ com $x_0 < 0$ e $y_0 > 0$.

Consideramos a reta que liga os pontos $(0,0)$ e (x_0, y_0).

A interseção desta reta com a reta $ax+by = ab+r$ é uma solução inteira da equação $ax + by = ab + r$.

De fato este ponto de interseção é exatamente o ponto

$$x_1 = x_0(ab + r), y_1 = y_0(ab + r).$$

Assim as soluções inteiras da equação $ax + by = ab + r$ são dados por

$$x_n = x_1 + b(n-1) = x_0(ab+r) + bn$$

$$y_n = y_1 - an = y_0(ab+r) - a(n-1), n \in \mathbb{Z}.$$

Como a velocidade da reta acima é $\sqrt{a^2+b^2}$, segue que a sequência de pontos (x_n, y_n) deverá visitar o segmento de reta definido pelos pontos extremais $(0, \frac{ab+r}{b})$ e $(\frac{ab+r}{a}, 0)$ que tem comprimento maior que $\sqrt{a^2+b^2}$, portanto a equação diofantina $ax + by = ab + r$ sempre possui solução inteira positiva para todo r ≥ 1, veja figura 1. □

Lema 3. *Seja $mdc(a,b) = 1$. Então a equação diofantina $a_x + b_y = k$ possui soluções inteiras não negativas para todo $k \geq ab - (a+b) + 1 = (a-1)(b-1)$ e $ab - a - b$ não pertence ao semigrupo $S(a,b)$.*

Demonstração. Pelo Lema 2 a equação $ax + by = ab$ possui soluções inteiras positivas (b, 0) e (0, a) e a equação $ax + by = ab + 1$ possui soluções inteiras positivas $(b, 0)$ e $(0, a)$ e a equação $ax + by = ab + 1$ possui soluções inteiras (x_1, y_1) com $x_1 > 0$ e $y_1 > 0$. Portanto $a(x_1 - 1) + (y_1 - 1) = ab - (a+b) + 1 = (a-1)(b-1) \in S(a,b)$.

Da mesma maneira se (x_r, y_r) , com $x_r > 0$ e $y_r > 0$, é solução inteira positiva de $ax + by = ab + r$, $r > 1$, temos que $(x_r - 1, y_r - 1)$ é inteira solução positiva da equação $ax + by = ab - (a+b) + r$, $r > 1$, temos que $(x_r - 1, y_r - 1)$ é uma solução inteira, positiva, da equação $ax + by = ab - (a+b) + r$. A equação $ax + by = ab - a - b$ não possui soluções inteiras não negativas.

Então, seja $(\overline{x}, \overline{y})$ uma solução com $\overline{x} > 0$ e $\overline{y} > 0$, tal que $a\overline{x} + b\overline{y} = ab - a - b$. Logo $(\overline{x} + 1, \overline{y} + 1)$ é uma solução positiva da equação $ax + by = ab$ pois $a(\overline{x} + 1) + b(\overline{y} + 1) = a\overline{x} + b\overline{y} + a + b = ab - a - b + a + b = ab$.

Isto é uma contradição com o fato de que as únicas soluções inteiras não negativas de $ax + by = ab$ serem $(b, 0)$ e $(0, a)$. Portanto o Lema está demonstrado. □

Lema 4. *Seja $mdc(a,b) = 1$. Dado $k \in \mathbb{N}$ tal que $ab > k \geq (a-1)(b-1)$ a equação diofantina $ax + by = k$ possui uma única solução inteira não negativa.*

Demonstração. Pelo Lema 3 sempre temos soluções nas condições do enunciado.Portanto, devemos primeiro estabelecer a unicidade. Demonstraremos então que a equação diofantina $ax + by = ab - 1$ possui uma única solução inteira positiva. Lembramos que a

equação $ax + by = ab$ possui somente as soluções inteiras $(b, 0)$ e $(0, a)$ não negativas. Considere o segmento com vértices $A_1 = (\frac{ab-1}{a}, 0)$ e $A_2 = (0, \frac{ab-1}{b})$.

O seu comprimento é $(1 - \frac{1}{ab})\sqrt{a^2 + b^2} < \sqrt{a^2 + b^2}$. As soluções inteiras da equação $ax + by = ab - 1$ são da forma $x_n = x_0 + b_n$, $y_n = y_0 - an$ onde (x_0, y_0) é uma solução particular a qual podemos supor pertencente ao segundo quadrante.

Logo a sequência $p_n = (x_n, y_n) \in \mathbb{Z} \times \mathbb{Z}$ visita o interior relativo do segmento com vértices A_1 e A_2 uma única vez. Veja figura 1.

Para os demais valores de k a argumentação é análoga, mas não podemos sempre garantir que a solução seja positiva.

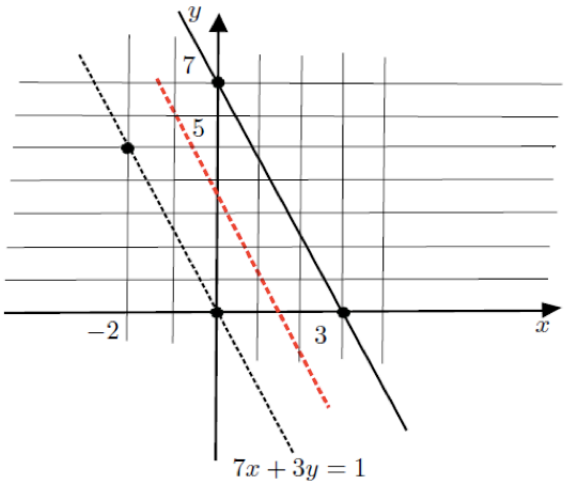

Figura 1: Equação Diofantina Linear $7x + 3y = k$

□

Lema 5. *Seja* $mdc(a, b) = 1$. *O número* $ab - a - b + 1 = (a - 1)(b - 1)$ *é exatamente o dobro do número de pares ordenados inteiros* (m, n) *contidos no interior do triângulo*

de vértices $(0,0)$, $(0,a)$ *e* $(b,0)$.

Demonstração. Segue diretamente do Teorema 9 que relaciona a área de uma poligonal fechada P tendo vértices com ambas coordenadas inteiras com o número de pares ordenados inteiros contidos no interior de P e na sua fronteira. Precisamente, $A(P) = \frac{B}{2} + I - 1$, onde I é o número de pares (x_i, y_i) inteiros contidos no interior de P, e B é o número de pares ordenados inteiros contidos na fronteira de P, incluindo os vértices. No caso do triângulo de vértice $(0,0)$, $(0,a)$ e $(b,0)$ temos que $A(P) = \frac{ab}{2}$ e $B = a+1+b$. Observamos que no interior relativo do segmento com pontos extremais $(0,a)$ e $(b,0)$ não temos pares ordenados inteiros pois $\text{mdc}(a,b) = 1$. Logo

$$I = \frac{ab}{2} - \frac{a+b+1}{2} + 1 = \frac{ab-a-b+1}{2} = \frac{(a-1)(b-1)}{2}$$

Portanto, pelos lemas anteriores , concluímos a demonstração do Teorema 5 [Teorema de Sylvester] □

A partir do Lema 3 temos que $F(a,b) = ab - a - b$ é o maior elemento de $\mathbb{N} \setminus S(a,b) = F(a,b)$. Assim o semigrupo $S(a,b)$ é aritmético e pelo Lema 6 temos que $F(a,b) = (a-1)(b-1) - 1$ é ímpar.

4.3 Demonstração do Teorema 6

Para provar este teorema, inicialmente usaremos uma hipótese provisória (argumento heurístico) na busca de um candidato para o número $r = r(S(a,b))$. Baseado no Teorema 5 , suponhamos uma fórmula da seguinte forma polinomial simétrica nas variáveis (a,b):

$$r(S(a,b)) = x(a+b)^2 + yab + z(a+b) + w, (x,y,z,w) \in \mathbb{Q}^4$$

Assim , fazendo 4 exemplos , obtemos o seguinte sistema linear :

$$r(2,4) = 36x + 8y + 6z + w = 0$$

$$r(4,10) = 196x + 40y + 14z + w = 8$$

$$r(6,8) = 196x + 48y + 14z + w = 12$$

$$r(4,14) = 324x + 56y + 18z + w = 12$$

O sistema acima possui uma solução única $(x, y, z, w) = (0, \frac{1}{2}, -1, 2)$.

Logo a fórmula polinomial procurada , se existir, é :

$$r(S(a,b)) = \frac{1}{2}ab - (a+b) + 2 = \frac{1}{2}(a-2)(b-2).$$

Lema 6. *Sejam a e b inteiros positivos tais que $mdc(a,b) = 2$. Temos que:*

$$r(S(a,b)) = \frac{1}{2}(a-2)(b-2).$$

Demonstração. Sejam a_1 e b_1 tais que $a = 2a_1$, $b = 2b_1$ e $(a_1, b_1) = 1$.

Temos que $S(a,b) \subset S(a_1,b_1)$ e $r(S(a,b)) = 2r(S(a_1,b_1))$.

De fato, pela estrutura do semigrupo $S(a_1,b_1)$ sabemos pelo Teorema 5 que $r(S(a_1,b_1))$ é um número par e $r(S(a,b)) \leq 2r(S(a_1,b_1))$.

Também temos que $2F(a_1,b_1) \notin S(a,b)$, onde $F(a_1,b_1)$ é o número de Frobenius do semigrupo $S(a_1,b_1)$. Logo $2F(a_1,b_1)+1 \notin S(a,b)$, portanto $r(S(a,b)) = 2r(S(a_1,b_1))$. □

Terminamos a demonstração do Teorema 5 observando , de acordo com o Lema 6, que o número

$$r(S(a,b)) = \frac{1}{2}(a-2)(b-2) = \frac{1}{2}(2a_1-2)(2b_1-2) = 2(a_1-1)(b_1-1)$$

é par.

4.4 Demonstração do Teorema 7

Sejam a_1 e b_1 tais que $a = ka_1$, $b = kb_1$ e $(a_1, b_1) = 1$

Temos que $S(a,b) \subset S(a_1,b_1)$ e $r(S(a,b)) = kr(S(a_1,b_1))$. De fato, pela estrutura do semigrupo $S(a_1,b_1)$, sabemos pelo Teorema 5, que $r(S(a_1,b_1))$ é um número par e $r(S(a,b)) \leq kr(S(a_1,b_1))$. Também temos que $kF(a_1,b_1) \notin S(a,b)$. Logo $kF(a_1,b_1)+r \notin S(a,b)$ para todo $1 \leq r < k$ e $kF(a_1,b_1)+k = k(F(a_1,b_1)+1) \in S(a,b)$.

Portanto $r(S(a,b)) = kr(S(a_1,b_1)) = \frac{1}{k}(a-k)(b-k)$.

5 Recíproca do Teorema de Silvester

Dado um número par r determinar todos os pares de inteiros positivos (a, b) tais que $\text{mdc}(a, b) = 1$ e $F(a, b)+1 = ab-(a+b)+1 = r$, isto é, determinar todos os semigrupos S com dois geradores tendo o número $r-1$ como seu número de Frobenius.

Na tabela abaixo estão listados os semigrupos S gerados por 2 números a e b com $\text{mdc}(a, b) = 1$ com seu respectivo regularizador arititmético r e seu número de Frobenius $F(a, b)$.

Por exemplo para $r = 20$ temos 3 semigrupos distintos
$S_1 = (2, 21) = \{0, 2, 4, 6, \ldots, 18, 20, 21, 22, 23, 24, \ldots\}$,
$S_2 = (3, 11) = \{0, 3, 6, 9, 11, 12, 14, 15, 17, 18, 20, 21, 22, \ldots\}$ e
$S_3 = (5, 6) = \{0, 5, 6, 10, 11, 12, 15, 16, 17, 18, 20, 21, 22, 23, 24, \ldots\}$

$r = F(a, b) + 1$	$(a, b) : \text{mdc}(a, b) = 1$
2	(2,3)
4	(2,5)
6	(2,7), (3,4)
8	(2,9), (3,5)
10	(2,11)
12	(2,13), (3,7), (4,5)
14	(2,15), (3,8),
16	(2,17)
18	(2,19), (3,10), (4,7)
20	(2,21), (3,11), (5,6)
22	(2,23)
...	...
50	(2,51), (3,26), (6,11)

Tabela 1: Semigrupos com 2 geradores e com regularizador aritmético dado, formando progressão aritmética de razão 1.

E na tabela a seguir em que temos mais alguns semigrupos com as mesmas características:

$r = F(a,b) + 1$	$(a,b) : mdc(a,b) = 1$
2	(2,3)
...	...
26	(2,27);(3,14)
28	(2,29);(5,8)
30	(2,31);(3,16);(4,11);(6,7)
32	(2,33);(3,17); (5,9)
34	(2,35)
36	(2,37);(3,19); (4,13)
38	(2,39);(3,20)
40	(2,41);(5,11)
42	(2,43);(3,22);(4,15);(7,8)
44	(2,45);(3,23);(5,12)
46	(2,47)
48	(2,49);(3,25);(4,17);(5,13);(7,9)
50	(2,51);(3,26);(6,11)
52	(2,53);(5,14)
54	(2,55);(3,28);(7,10);(4,19)
56	(2,57);(3,29);(8,9)

$r = F(a,b) + 1$	$(a,b) : mdc(a,b) = 1$
58	(2,59)
60	(2,61);(3,31);(5,16);(4,21);(6,13);(7,11)
62	(2,63);(3,32)
64	(2,65);(5,17)
66	(2,67);(3,34);(4,23);(7,12)
68	(2,69);(3,35);(5,18)
70	(2,71);(8,11)
72	(2,73);(3,37);(4,25);(5,19);(7,13);(9,10)
74	(2,75);(3,38)
76	(2,77)
78	(2,79);(3,40);(4,27)
80	(2,81);(3,41);(5,21);(9,11)
82	(2,83)
84	(2,85);(3,43);(4,29);(5,22);(7,15);(8,13)
86	(2,87);(3,44)
88	(2,89);(5,23)
90	(2,91);(3,46);(4,31);(6,19);(7,16);(10,11)
92	(2,93);(3,47);(5,24)
94	(2,95)
96	(2,97);(3,49);(4,33);(7,17);(9,13)
98	(2,99);(3,50);(8,15)
100	(2,101);(5,26)

Podemos também analisar esses semigrupos em pares ordenados e representa-los geometricamente no sistema de coordenadas simples:

O gráfico abaixo mostra a relação entre os semigrupos gerados por $(3, 5)$ e $(4, 7)$.

O semigrupo gerado por $(3, 5) = \{0, 3, 5, 6, 8, 9, 10, \ldots\} = S$, cujo regularizador é 8 e o número de Frobenius é 7.

O semigrupo gerado por $(4, 7) = \{0, 4, 7, 8, 11, 12, 14, 15, 16, 18, 19, 20, 21, \ldots\} = S_1$ cujo regularizador é 18 e o número de Frobenius é 17.

Chamaremos de Q a região delimitado pelo polígono que contém todos os pontos formados pelo produto cartesiano dos números de S e S_1, menores que seus regularizadores, que denotamos por $S \times S_1$, ou seja, o retângulo com vértices em $(0, 0), (0, 8), (18, 0)$ e $(18, 8)$. E chamaremos de R a região, infinita, rosa.

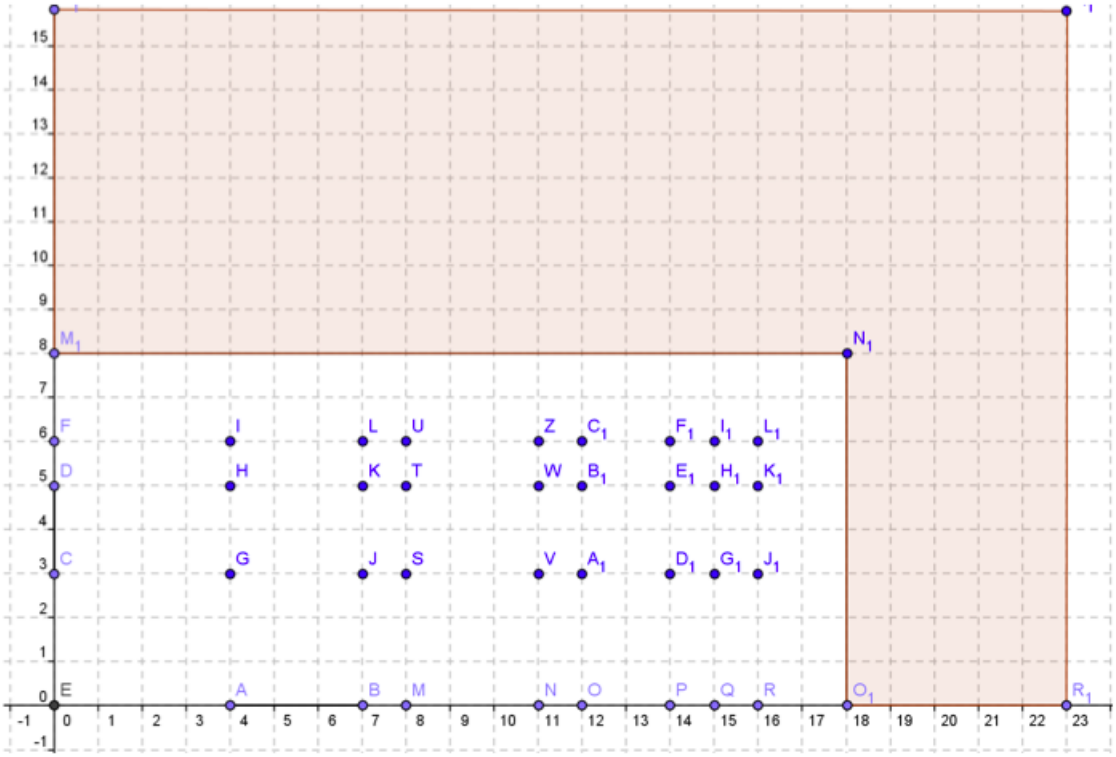

Figura 2: $S \times S_1$

Todos os pares dentro da região R pertencem a $S \times S_1$.

Chamaremos de W a quantidade de pontos fora da região R que pertencem a $S \times S_1$.

Os pontos de azul do polígono Q (incluindo a origem) são pontos que também pertencem a $S \times S_1$.

Observe que a relação de quantidade de pontos fora da região do polígono rosa que

pertence a $S \times S_1$ é $\frac{1}{4}$ de todos os pontos fora dessa região.

Neste exemplo existem 144 pontos fora de Q e destes 36 $\in S \times S_1$.

No exemplo abaixo existem 288 fora de Q e destes 7 $\in S \times S_1$

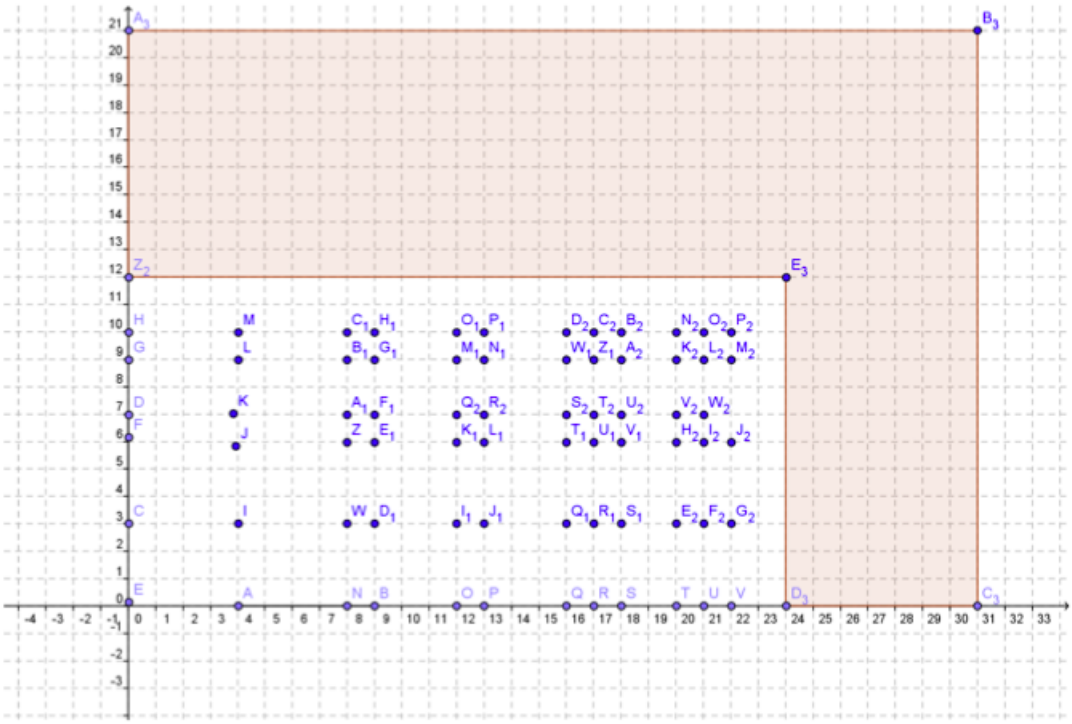

Figura 3: $S \times S_1$

5.1 Semigrupos do tipo $2^n.3$

Analisaremos agora os semigrupos cujo regularizador aritmético $r(S)$ é $2^n.3$. Na tabela abaixo estão lsitados alguns destes semigrupos.

n	$2^n.3$	Semigrupos gerados por $2^n.3$
0	3	ϕ
1	6	(2,7);(3,4)
2	12	(2,13); (3,7) ; (4,5)
3	24	(2,25);(3,13);(4,9);(5,7)
4	48	(2,49);(3,25);(4,17);(5,13);(7,9)
5	96	(2,97);(3,49);(4,33);(7,17);(9,13);
6	192	(2,193);(3,97);(4,65);(5,49);(7,33);(9,25);(13,17)
7	384	(2,385);(3,193);(4,129);(5,97);(7,65);(9,49);(13,33) ;(17,25)
8	768	(2,769);(3,385);(4,257);(5,193);(7,129);(9,97);(13,65);(17,49);(25,33)
9	1536	(2,1537);(3,769);(4,513);(5,385);(7,257);(9,193);(13,129);(17,97);(25,65);(33,48)
10	3072	(2,3073);(3,1537);(4,1025);(5,796);(7,513);(9,385);(13,257);(17,193); (25,129);(33,97);(49,65)

Estes semigrupos possuem características próprias e a tabela acima sugere algumas destas características, mas não podemos garantir que valem para todos os semigrupos existentes.

Regularidades observadas nestes semigrupos

Para cada valor de n , diferente de 0 , temos :

1) O primeiro semigrupo é sempre da forma $(2, K)$ com :

$K = (2^n.3) + 1$;

2) O segundo semigrupo é sempre da forma $(3, M)$ com:

$M = \dfrac{(2^n.3)}{2} + 1$;

3) O terceiro semigrupo, se existir , é sempre da forma $(4, N)$ com:

$N = \dfrac{(2^n.3)}{3} + 1.$

Veja que o segundo elemento de cada semigrupo é sempre da forma $\dfrac{(2^n.3)}{P} + 1$,

onde P é a posição do semigrupo em ordem crescente (para 1^o semigrupo $P = 1$, para o 2^o semigrupo $P = 2$, e assim por diante).

Observe também que o número de semigrupos $f(n)$ da tabela (com exceção de $n = 5$) , com $r(S) = 2^n.3$ e $n \neq 0$, é $n + 1$.

5.2 Estrutura de semigrupos gerados por 2 elementos

Iremos agora descrever a estrutura do semigrupo S gerado por dois números a e b tal que $\text{mdc}(a, b) = 1$.

Definição 2. *Dado um semigrupo aritmético S, com número de Frobenius $F(S) = r(S) - 1$, um inteiro $n \leq F(S)$ é chamado do tipo $(+)$ se $n \in S$ e do tipo $(-)$ se n não pertence a S. O conjugado de n é o número $\overline{n}$ tal que $n + \overline{n} = F(S) = r(S) - 1$.*

Se m e $n = \bar{m}$ são conjugados e m é do tipo $(+)$ então $n = \bar{m}$ é do tipo $(-)$, caso contrário teríamos $m + \bar{m} = r(S) - 1 \in S$. Então temos as seguintes equações sobre a cardinalidade de n :

$$\sharp\{n : n \text{ é do tipo } (+)\} \leq \frac{r(S)}{2}$$

$$\sharp\{n : n \text{ é do tipo}(-)\} \geq \frac{r(S)}{2}.$$

Por exemplo, quando $S = S(a, b)$ todos os elementos das progressões aritméticas $P(a)$ e $P(b)$ estão contidos no conjunto S e portanto são do tipo $(+)$.

Definição 3. *Um número n é chamado do tipo $(-,-)$ se n e $\overline{n}$ forem ambos do tipo $(-)$.*

Assim podemos concluir as seguintes inequações sobre cardinalidade :

$$\sharp\{x : x \text{ é do tipo}(+)\} \leq r(S)/2$$

$$\sharp\{x : x \text{ é do tipo}(-)\} \geq r(S)/2$$

Lema 7. *Sejam a e b inteiros tais que $mdc(a,b)=1$. Na região triangular*

$$R=\{(x,y): x\geq 0, y\geq 0, ax+by\leq F(a,b)\}$$

temos exatamente

$$\frac{(a-1)(b-1)}{2}$$

pontos com ambas coordenadas inteiras.

Demonstração. Observamos que $(-1,a-1)$ e $(b-1,-1)$ são soluções inteiras da equação diofantina $ax+by=ab-a-b=F(a,b)$.

Os pontos com coordenadas inteiras no interior do triângulo retângulo com vértices $(-1,a-1),(b-1,-1)$ e $(-1,-1)$ possuem sempre coordenadas não negativas. Logo, pelo Teorema9 , a quantidade I destes pontos é dado pela equação

$$\frac{ab}{2}=I+\frac{a+b+1}{2}-1$$

Logo, temos

$$I=\frac{(a-1)(b-1)}{2}.$$

□

Seja o semigrupo gerado pelos números 3 e 7 então temos que $(3-1).(7-1)=12$. Logo o número de Frobenius é 11, o regularizador é 12 e a quantidade I de elementos não pertencentes a S antes do regularizador é 6.

$S(3,7)=\{0,3,6,7,9,10,12,13,14...\}$ e $l=\{1,2,4,5,8,11\}$, ou seja $I=6$

Proposição 2. *Sejam a e b inteiros tais que $mdc(a,b)=1$, dizemos que x é do tipo $(+)$ se, e somente se, o seu conjugado $\overline{x}$ é do tipo $(-)$. Portanto temos,*

$$\sharp\{x: x \text{ é do tipo } (+)\}=\sharp\{x: x \text{ é do tipo } (-)\}=\frac{1}{2}r(S(a,b)).$$

Demonstração. Observamos que , de acordo com o Lema 7, na região triangular

$R=\{(x,y): x\geq 0, y\geq 0, ax+by\leq F(a,b)\}$ temos exatamente $\dfrac{(a-1)(b-1)}{2}$

pontos com ambas coordenadas inteiras.

Os pontos de $(m,n)\in R\cap(\mathbb{N}\cup\{0\}\times\mathbb{N}\cup\{0\})$ dão origem aos números $am+bn\in S(a,b)$

que pertecem ao conjunto $\{0, a, b, \ldots, F(a,b)\}$. Logo, no caso de dois geradores, a e b com $mdc(a,b) = 1$, não existe inteiro x tal que x e $\overline{x}$ sejam ambos do tipo $(-)$. Portanto a proposição está demonstrada.

□

Corolário 3. *Sejam a e b inteiros tais que $a < b$ e $mdc(a,b) = 1$. Os números $F(a,b) - k$, $1 \leq k \leq a-1$ são do tipo $(+)$.*

Demonstração. Os números do conjunto $\{1, 2, \ldots, a-1\}$ são do tipo $(-)$. Logo, pela proposição 2, os números $F(a,b) - k, 1 \leq k \leq a-1$, são do tipo $(+)$. □

Lema 8. *Sejam a e b inteiros tais que $a < b$ e $mdc(a,b) = 1$. Seja m_i o menor elemento do conjunto $\{i, i+a, i+2a, \ldots\} \cap \mathcal{S}(a,b)$.*

Seja o conjunto $F(a,b)$ a união de $a-1$ progressões aritméticas finitas do tipo $A_i = \{i, i+a, i+2a, \ldots, m_i - a\}$ com $i = 1, 2, \ldots, a-1$. Além disso o conjunto $\{m_1, m_2, \ldots, m_{a-1}\}$, após reordenação é também uma progressão aritmética de razão b com $m_1 = b$ e $m_{a-1} = (a-1)(b-1)$.

Demonstração. Pela proposição 2, todos os elementos de A_i são do tipo $(-)$, portanto pertencem a $F(a,b)$. Observando que $N = {U_i}^{a-1} = \{i, i+a, i+2a, \ldots\}$, temos, pela definição de m_i , que $m_i \in S(a,b)$ é um múltiplo de b e $m_i - a \in F(a,b)$.

□

Proposição 3. *Sejam a e b inteiros tais que $mdc(a,b) = 1$. Considere os conjuntos finitos $F(a,b)$ e$S_f(a,b)$, tal que $S_f(a,b) = \{0, 1, 2, ..., F(a,b)\} \setminus F(a,b)$. Sejam*

$$f(a,b) = \sum_{x \in_L} x \text{ e } g(a,b) = \sum_{x \in Sf(a,b)} x$$

Então

$$f(a,b) = \frac{1}{12}.(a-1)(b-1)(2ab - a - b)$$

$$g(a,b) = \frac{1}{12}.(a-1)(b-1)(4ab - 5a - 5b + 1).$$

Demonstração. Observamos que

$$\sum_{k=1}^{n} k = \frac{(n+1)n}{2}$$

e

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1).$$

Portanto,

$$\sum_i m_i = \sum_{i=1}^{a-1} n_i = \frac{1}{2}a(a-1)b$$

e

$$\sum_i (m_i)^2 = \sum_{i=1}^{a-1} b^2 i^2 = \frac{1}{6}b^2 a(a-1)(2a-1)$$

Por outro lado a soma dos termos da progressão aritmética
$A_i = \{i, i+a, ...m_i - a\}$ com, $m_i = k_i a + i$ é dada por :

$$\frac{1}{2}(i + m_i - a)k_i = (i + m_i - a)(m_i - \frac{i}{2a}) = (m_i^2 - \frac{i^2}{2a}) - (m_i - \frac{i}{2})$$

Portanto

$$f(a,b) = \sum_{x \in F(a,b)} x = \sum_{i=1}^{a-1} \frac{m_i^2 - i^2}{2a} + \frac{m_1 - i}{2}$$

$$= \frac{1}{2a}\frac{a(a-1)(2a-1)}{6}(b^2-1) - (\frac{1}{4})a(a-1)(b-1)$$

$$= \frac{1}{12}(a-1)(b-1)(2ab - a - b)$$

Analogamente temos que :

$$g(a,b) = \frac{1}{12}(a-1)(b-1)(4ab - 5a - 5b + 1).$$

□

5.3 Semigrupos gerados por 2 elementos com mdc = 2

$r = (a-2)(b-2)/2$	$(a,b) : \text{mdc}(a,b) = 2$
0	(2,4)
2	$\emptyset$
4	(4,6)
6	$\emptyset$
10	$\emptyset$
12	(4,14), (6,8)
14	$\emptyset$
16	(6,10)
18	$\emptyset$
20	(4,22)
22	$\emptyset$
24	(4,26), (6,14), (8,10)
...	...
50	$\emptyset$
...	...
100	(4,102)

Tabela 2: Semigrupos com 2 geradores e com regularizador aritmético dado, formando uma progressão aritmética de razão 2.

A tabela abaixo também contém semigrupos com as mesmas características.

$r = F(a,b) + 1$	$(a,b) : mdc(a,b) = 2$
12	(4,14);(6,8)
14	ϕ
16	(4,18);(6,10)
18	ϕ
20	(4,22)
22	ϕ
24	(4,26);(6,14);(8, 10)
28	(4,30);(6,16)
32	(4,34)
36	(4,38);(6,20);(8,14)
40	(4,42);(6,22);(10,12)
44	(4,46)
48	(4,50);(6,26);(8,18);(10,14)
52	(4,54);(6,28)
56	(4,58);(10,16)
60	(4,62);(6,32);(8,22);(12,14)
64	(4,66);(6,34);(10,18)
68	(4,70)
72	(4,74);(6,38)
76	(4,78);(6,40)
80	(4,82);(10,22)
84	(4,86);(6,44)
88	(4,90);(6,46);(10,24)
92	(4,94)

Nestes semigrupos também temos algumas regularidades baseadas na tabela.

Observamos que para todo $r = 2, 6, 10, ...$, ou seja , uma *P.A.* de razão 4 com primeiro termo igual a 2 , o número de semigrupos igual a *zero*.

Observe que o primeiro semigrupo gerado por cada r é $(4, x)$, em que $x = r + 2$.

Observe que todos os r que possuem semigrupos gerados por $(6, y)$, tem y= $(\frac{r}{2})$+2

6 Estrutura de semigrupos gerados por 3 elementos

Seja o semigrupo $S = S(a, b, c) = \{p = ma + nb + rc,\ (m, n, r) \in \mathbb{N}^3\}$ tal que $\text{mdc}(a, b, c) = 1$ e seja $F(a, b, c)$ o *número de Frobenius* de S, isto é, $F(a, b, c)$ é o maior inteiro que não pertence a S. O *regularizador aritmético* de S é o número natural $r(S) = F(a, b, c) + 1$.

Relembramos, veja definição 2, que um número $n \in \{0, 1, ..., F(a, b, c)\}$ é chamado do tipo $(+)$ se $n \in S$ e do tipo $(-)$ se $n \notin S$. O conjugado de n é o número $\overline{n}$ tal que $n + \overline{n} = F(a, b, c)$.

Claramente se n é do tipo $(+)$ então $\overline{n}$ é do tipo $(-)$, então

$$\#\ \{n : n \text{ é do tipo}(+)\} \leq (1 + F(a, b, c))/2$$
$$\text{e}$$
$$\#\ \{n : n \text{ é do tipo}(-) \geq (1 + F(a, b, c))/2$$

Relembramos também, veja definição 3, que um número $n \leq F(a, b, c)$ é chamado do tipo$(-, -)$ se n e $\overline{n}$ forem ambos do tipo $(-)$.

Proposição 4. *Nas condições acima temos:*

$$\#\{(+)\} = \tfrac{F(a,b,c)+1-\#\{(-,-)\}}{2}$$
$$e$$
$$\#\{(-)\} = \tfrac{F(a,b,c)+1+\#\{(-,-)\}}{2}$$

Em particular se F(a,b,c) for par temos que # {(-,-)} > 0.

Demonstração. Observamos que o número total de pares $(n, \overline{n})$ no conjunto $\{0, 1, 2, \ldots, F(a, b, c)\}$ é igual a $F(a, b, c) + 1$. Portanto,

$$F(a, b, c) + 1 = \#\{(+, -)\} + \#\{(-, +)\} + \#\{(-, -)\}.$$

$$\#\{(+)\} = \#\{(+,-)\} = \#\{(-,+)\}$$

e

$$\#\{(-)\} = \#\{(+,-)\} = \#\{(-,-)\}$$

Consequentemente,

$$\#\{(+)\} + \#\{(-)\} = F(a,b,c) + 1 = \#\{(-)\} - \#\{(+)\} = \#\{(-,-)\}$$

Logo temos,

$$\{(+)\} = \frac{F(a,b,c) + 1 - \#(-,-)}{2}$$

$$\{(-)\} = \frac{F(a,b,c) + 1 + \#(-,-)}{2}.$$

□

Exemplo 17. $S(4,9,19) = 0,4,8,9,12,13,16,17,18,19,...$

Observe que depois do 16 *todos os naturais pertencem ao semigrupo* S.

O conjunto dos elementos do tipo $(-,-)$ *é:*

$\{(-,-\} = \{(1,14),(4,11),(5,10)\}$.

A cardinalidade do conjunto $\{(-,-)\}$ *é* 6.

Exemplo 18. *Seja o semigrupo* $S(21,31,45)$ *relatado abaixo, temos que* $F(21,31,45) = 227$ *e* 24 *são elementos do tipo* $(-,-)$.

Mostrando o semigrupo :

$S(21,31,45) = \{0,21,31,42,45,52,62,63,66,73,76,83,84,87,90,94,97,104,105,107,108,111,114,115,118,121,124,125,126,128,129,132,135,136,138,139,142,145,146,147,149,150,152,153,155,156,157,159,160,163,166,167,168,169,170,171,173,174,176,177,178,180,181,183,184,186,187,188,189,190,191,192,194,195,197,198,199,200,201,202,204,205,207,208,209,210,211,212,213,214,215,216,217,218,219,220,221,222,223,225,226,228,\ldots,\}$.

Observamos que depois do 228 *, todos os naturais pertencem ao semigrupo* S. *Para comprovar isto basta listar o semigrupo até o elemento* $228 + 21 = 249$.

O conjunto dos elementos do tipo $(-,-)$ *é:*

$\{(-,-\} = \{(3,224),(24,203),(34,193),(48,179),(55,172),(65,162),(69,158),(79,148),(86,141),(96,131),(100,127),(110,117)\}$.

A cardinalidade do conjunto $\{(-,-)\}$ *é* 24.

A representação geométrica do conjunto dos elementos $(-,-)$ *é :*

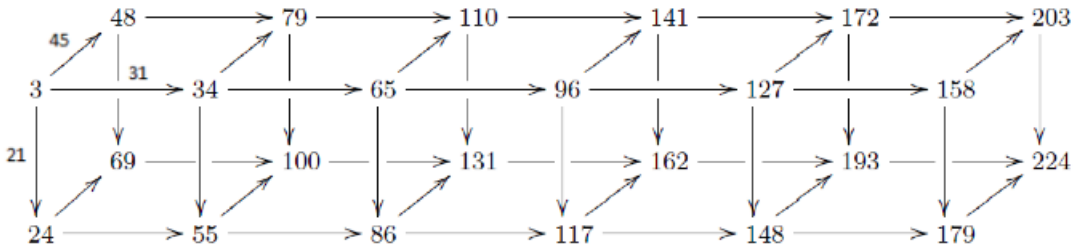

Figura 4: Representação geométrica do conjunto dos elementos $(-,-)$ do semigrupo $S(21,31,45)$

No sólido acima (figura 4) cada direção das setas revela uma P.A. e a razão de cada uma delas é um dos geradores do semigrupo ($\rightarrow$ *é a P.A de razão* 31; $\downarrow$ *é a P.A. de razão*21 ; $\nearrow$ *é a P.A. de razão* 45*).*

Exemplo 19. *Seja o semigrupo :*

$(29,37,51) = \{0,29,37,51,58,66,74,80,87,88,95,102,103,109,111,116,117,124,125,131,132,138,139,140,145,146,148,153,154,160,161,162,167,168,169,174,175,176,177,182,183,185,189,190,191,196,197,198,199,203,204,205,206,211,212,213,214,218,219,220,222,225,226,227,228,232,233,234,235,236,240,241,242,243,248,249,250,251,254,255,256,257,259,261,262,263,264,265,268,269,270,271,272,273,276,277,278,279,280,283,284,285,286,287,288,290,291,292,293,294,296,298,299,300,301,302,305,306,307,308,309,310,312,313,314,315,316,317,319,320,321,322,323,324,325,327,328,329,330,331,333,334,335,336,337,338,339,341,342,343,344,345,346,347,348,349,350,353,352,353,354,355,356,357,358,359,360,361,362,364,365,366,367,368,370...\}$.

A partir do 370 *temos todos os números*

O número de Frobenius é 369.

Temos então 175 *números que são do tipo* $(+)$ *e* 195 *numeros que são do tipo*$(-)$

Temos então os números do tipo $(-,-)$ *:*

$(43, 326), (65, 304), (72, 297), (94, 275), (122, 247), (123, 246), (130, 239), (152, 217), (159, 210), (181, 188)$

10 *pares, ou seja ,* 20 *números do tipo* $(-,-)$

Confirmando as fórmulas temos:

$$\{(+)\} = \frac{(369 + 1 - 20)}{2} = 175$$

e

$$\{(-)\} = \frac{(369 + 1 + 20)}{2} = 195$$

Exemplo 20. *Seja o semigrupo abaixo:*

$$(7, 11, 15) = \{0, 7, 11, 14, 15, 18, 21, 22, 25, 26, 28, 29, 30, 32, 33, 35, 36, 37, 39, ...\}$$

A partir do 39 *temos todos os números naturais.*

O número de Frobenius é 38.

Temos então 18 *números que são do tipo* $(+)$ *e* 21 *numeros que são do tipo* $(-)$

Temos então os números do tipo $(-,-)$ *:*

$(4, 34)$,$(19, 19)$, 2 *pares, ou seja ,* 3 *números do tipo* $(-,-)$ *que são* $4, 19$ *e* 34*, formando uma P.A. de razão* 15.

Confirmando as fórmulas temos:

$$\{(+)\} = \frac{(38 + 1 - 3)}{2} = 18$$

$$\{(-)\} = \frac{(38 + 1 + 3)}{2} = 21$$

Exemplo 21. $(5, 8, 14, 22) = \{0, 5, 8, 10, 13, 14, 15, 16, 18, 19, 20, 21, 22, ...\}$

$F(5, 8, 14, 22) = 17$*;* $\{(+)\} = 8$*,* $\{(-) = 10$ *e* $\{(-,-)\} = (6, 11)$ *ou seja* 2 *números.*

Pela conjectura 1 $\{(+)\} = \frac{17+1-2}{2} = 8$ *e* $\{(-)\} = \frac{17+1+2}{2} = 10$

Exemplo 22. $(8, 13, 31, 44) = \{0, 8, 13, 16, 21, 24, 26, 29, 31, 32, 34, 37, 39, 40, 42, 44,$
$45, 47, 48, 50, 52, 53, 55, 56, 57, 58, 60, 61, 63, 64, 65, 66, 68, 69, 70, 71, 72,$
$73, 74, 75, ...\}$

$F(8, 13, 31, 44) = 67$ *;* $\{(+)\} = 32$*,* $\{(-)\} = 36$ *e* $\{(-,-)\} = (5, 62); (18, 49)$ *ou seja,* 4 *números.*

Pela conjectura 1 $\{(+)\} = \frac{67+1-4}{2} = 32$ *e* $\{(-)\} = \frac{67+1+4}{2} = 36$

Teorema 8. *Seja* $x \in \{0, 1, \ldots, F(a, b, c)\}$*e suponha que* $p < x < r$ *onde* p *e* r *são do tipo* $(-,-)$*. Se* $r - x \in \{(+)\}$ *e* $x - p \in \{(+)\}$ *então* x *é do tipo* $(-,-)$*.*

Demonstração. Sendo $r = x + (r - x)$, se x for do tipo $(+)$, como por hipótese $r - x \in \{(+)\}$, então r também seria do tipo $(+)$, o que não é verdade pois estamos supondo $r \in \{(-)\}$. Por outro lado, como $x + \overline{x} = F(a, b, c)$ e $p + \overline{p} = F(a, b, c)$ temos que $x + \overline{x} = p + \overline{p}$ e assim obtemos que $\overline{p} = \overline{x} + (x - p)$. Como $(x - p) \in \{(+)\}$ e $\overline{p} \in \{(-)\}$, temos obrigatoriamente que $\overline{x}$ é do tipo $(-)$.
Assim, $x + \overline{x}$ são ambos do tipo $(-)$, ou seja, x é do tipo $(-,-)$.

□

Conjectura 1. *(Arnold) Considere um semigrupo* $S(a, b, c)$*,* $mdc(a, b, c) = 1$*.*
Seja $M = max\{(-,-)\}$ *e* $m = mim\{(-,-)\}$*. Então* $M - m \in \{(+)\} \subset S(a, b, c)$*.*

O seguinte semigrupo com 4 geradores, veja [9], mostra que a conjectura acima é específica para 3 geradores.

Considere o semigrupo S gerado por $(4, 6, 13, 15)$.

Temos que

$$S(4, 6, 13, 15) = \{0, 4, 6, 8, 10, 12, 13, 14, 15, 16, 17, 18, ...\}$$

O conjunto das lacunas é $\{(-)\} = \{1, 2, 3, 5, 7, 9, 11\}$. O seu número de Frobenius é 11 e $\{(-,-)\} = \{2, 9\}$.

Aqui o maior elemento de $(-,-)$ é $M = 9$ e o menor elemento de $(-,-)$ é $m = 2$. No entanto $M - m = 9 - 2 = 7$ não pertence a $S(4, 6, 13, 15)$, ou seja, não é do tipo $\{(+)\}$.

Exemplo 23. *Considere o semigrupo gerado por* $(15, 21, 25)$.

Temos que:

$(15, 21, 25) = \{0, 15, 21, 25, 30, 36, 40, 42, 45, 46, 50, 51, 55, 57, 60, 61, 63, , 65, 66,$
$67, 70, 71, 72, 75, 76, 78, 80, 81, 82, 84, 85, 86, 87, 88, 90, 91, 92, 93, 95, 96, 97, 99,$
$100, 101, 102, 103, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117,$
$118, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134,$
$135, ...\}$

$F(15, 21, 25) = 119$*;* $\{(+)\} = 60$*;* $\{(-)\} = 60$ *e* $(-, -) = 0$

Pela conjectura 1 $\{(+)\} = \dfrac{119 + 1 - 0}{2} = 60$ *e* $\{(-)\} = \dfrac{119 + 1 + 0}{2} = 60.$

Conforme mostrado nos exemplos, os semigrupos com 3 geradores nem sempre tem a propriedade: $n \in \mathbb{N}$, então $n \in S$ ou $(F(a, b, c) - n) \in$ S.

Os semigrupos que possuem a propriedade acima são chamados *semigrupos simétricos*.

A tabela a seguir mostra alguns exemplos de semigrupos gerados por 3 números. Estes semigrupos são mais difíceis de definir porém alguns exemplos a seguir são facilmente visíveis e o ponto de ? nos semigrupos do tipo$(a, b, ?)$ representa um elemento qualquer maior que b (pois a e b já geram o semigrupo).

$r = F(a,b,c) + 1$	$(a,b,c) : mdc(a,b,c) = 1$
2	ϕ
3	(3,4,5)
4	(2,5,?)
5	(3,5,7)
6	(2,7,?) ; (3,7,8)
7	ϕ
8	(2,9,?) ; (3,5,?)
9	(3,10,11)
10	(2,11,?)
11	(3,8,13)
12	(2,13,?) ; (3,7,?);(3,13,14)
13	(5,8,9)
14	(2,15,?) ; (3,8,?)
15	(3,6,17)
16	(2,17,?)
17	(3,17,19)
18	(2,19,?);(3,19,20)
19	(4,11,13)
20	(2,21,?)
21	(3,22,23)

Quando o regularizador $r(S)$ for múltiplo de 3 , então um semigrupo gerado para este número será $(3, a, b)$ em que a e b são os primeiros dois números maiores que $r(S)$.

Na figura abaixo encontramos mais semigrupos que obedecem as mesmas características dos semigrupos da tabela.

r = F (a,b,c) + 1	(a,b,c) : mdc(a,b,c) = 1	r = F (a,b,c) + 1	(a,b,c) : mdc(a,b,c) = 1
2	Ø	**29**	(3,29,31)
3	(3,4,5)	**30**	(3,31,32)
4	(2,5,?)	**31**	(4,17,35)
5	(3,5,7)	**32**	(3,32,34)
6	(3,7,8)	**33**	(3,34,35)
7	Ø	**34**	(4,15,37)
8	(2,9,?) ; (3,5,?)	**35**	(3,35,37)
9	(3,10,11)	**36**	(3,37,38)
10	(2,11,?)	**37**	(4,13,?)
11	(3,8,13)	**38**	(3,38,40)
12	(3,13,14)	**39**	(3,40,41)
13	(5,8,9)	**40**	(4,14,?)
14	(2,15,?) ; (3,8,?)	**41**	(3,41,43)
15	(3,6,17)	**42**	(3,43,44) ; (5,12,43)
16	(2,17,?)	**43**	
17	(3,17,19)	**44**	(3,44,46)
18	(3,19,20)	**45**	(3,46,47)
19	(4,11,13)	**46**	
20	(2,21,?)	**47**	(3,47,49)
21	(3,22,23)	**48**	(3,49,50)
22		**49**	
23	(3,23,25) ; (5,8,27)	**50**	(3,50,52)
24	(3,25,26)	**51**	(3,52,53)
25	(5,11,18)	**...**	...
26	(3,23,28)	**100**	(7,18,101)
27	(3,28, 29)	**...**	...
28	(6, 11 ,14)	**135**	(8,21,139)

Figura 5: Semigrupos do tipo (a, b, c) com $\text{mdc}(a, b, c) = 1$

Notas

Podemos observar alguns estudos muito interessantes com a utilização dos semigrupos como por exemplo aplicação e utilização de semigrupos na confecção de redes sociais,geometria dinâmica, topologia, equações diferenciais entre outras.

Em vários sites podemos ler alguns artigos referentes a estes estudos e sobre algumas aplicações dos semigrupos numéricos.

Alguns destes sites estão relacionados abaixo e podem ser uma grande inspiração para o começo do estudo acerca destas estruturas tão importantes e interessantes.

http://pendientedemigracion.ucm.es/info/pecar/Articulos/Boyd.pdf

http://posugf.com.br/biblioteca/?word=Semigrupos

http://www.teses.usp.br/teses/disponiveis/45/45132/tde-31082010-093717/pt-br.php

http://mtm.ufsc.br/pos/ementaMTM510002.html

http://www.ufsj.edu.br/portal2-repositorio/File/demat/PASTA-PROF/raposo/volume-32.pdf

7 Considerações finais

O estudo de semigrupos com uma quantidade finita de elementos , apesar da simplicidade, é rico em detalhes, havendo inúmeras propriedades que relacionam seus elementos. Os semigrupos possuem características próprias podendo até gerar um estudo só para eles, como no caso dos semigrupos do tipo $2^n.3$. Algumas características, como o mdc entre seus geradores, o número de geradores, entre outras, podem ser estendidas para todos os semigrupos.

Analisando a quantidade de elementos dos semigrupos S e sua relação com o número de Frobenius, temos um vasto campo de estudo no ensino médio no qual podemos trabalhar o raciocínio lógico matemático além de conteúdos como funções e progressões aritméticas.

Num campo mais avançado ,os semigrupos também tem várias aplicações em geometria algébrica, em particular na geometria e topologia de curvas planas singulares.

Devemos também ressaltar a importância do Teorema de Sylvester nos estudos destes semigrupos, não só por fazer parte determinante nas demonstrações, mas também por exercer um importante papel na determinação de muitos destes semigrupos.

Já existem vários trabalhos envolvendo semigrupos gerados por 3 ou mais elementos envolvendo sistemas dinâmicos e criação de redes sociais, o que nos leva a entender mais ainda a importância do estudo deste assunto nos dias de hoje.

Porém, a intenção deste trabalho era mostrar um pouco de semigrupos, um assunto bastante interessante, para despertar o interesse dos estudantes e dos colegas em relação à esse assunto.

8 Apêndices

Teorema 9. *[Teorema de Pick] Dado um polígono simples P, sejam B o número de pontos da fronteira e I o número de pontos interiores, então a área $A(P)$ desse polígono é dada por*

$$A(P) = \frac{1}{2}B + I - 1$$

Exemplos do Teorema de Pick:

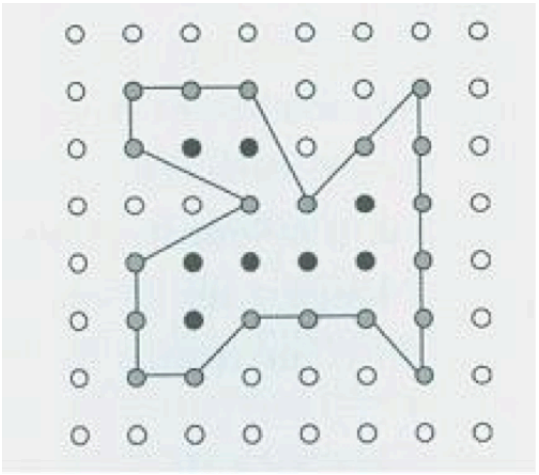

Figura 6: Teorema de Pick

Exemplo 24. *Na figura 6, $B = 20$ e $I = 8$, portanto a área é $\frac{1}{2}$ x $20 + 8 - 1 = 17$ unidades quadradas.*

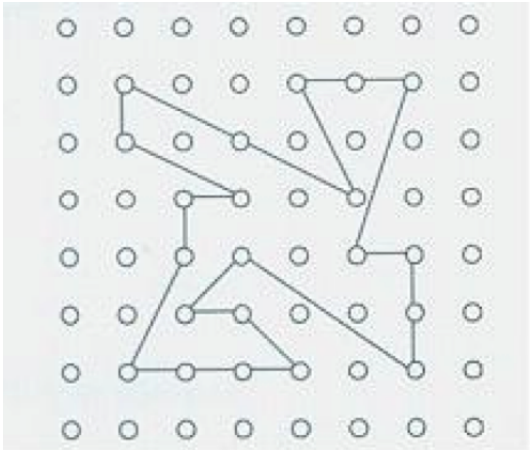

Figura 7: Teorema de Pick

Exemplo 25. *Na figura 7,* $B = 21$ *e* $I = 5$*, portanto a área é* $\frac{1}{2}$ *x 21 + 5 - 1 = 14,5 unidades quadradas.*

9 Referências Bibliográficas

Referências

[1] Monteiro, Antonio e Matos, Isabel. Álgebra, um primeiro curso. Escolar 1995.

[2] Abramo, Hefez. Irreducible Plane Curve Singularities. In Real and Complex Singularities. D. Mond and M. J. Saia, Editors, Lecture Notes in Pure and Applied Math. Vol. 232, Marcel Dekker, 1-120, 2003.

[3] Abramo, Hefez. Elementos da Aritmética, SBM,2011.

[4] Lima, Elon Lages. Análise Real Vol 1 , 2ª edição , Coleção Matemática Universitária , IMPA 2003.

[5] Lima, Elon Lages. Análise Real Vol 2, 5ª edição , Coleção Matemática Universitária , IMPA 2010.

[6] Domingues, Hygino H e Iezzi, Gelson. Álgebra Moderna , 4ª edição , Editora Atual (Grupo Saraiva) , 2006.

[7] Durbin, John R. Modern Algebra - an introduction, John Wiley e Sons, 1995.

[8] Garcia, Ronaldo Alves, Dinâmica e Geometria, 2^o Colóquio de Matemática da Região Nordeste, UFPI, 2012.

[9] Garcia, Ronaldo Alves, Semigrupos Numéricos e o Teorema de Sylvester, Revista da Olimpíada de Matemática do Estado de Goiás, vol.8: paginas 47-66, UFG, 2013.

[10] Wasserman, S.Y.K.F. Social Network Analysis. Methods and applications. Cambridge University Press, Cambridge, 1994.

[11] Singh, Simon. O Último Teorema de Fermat,Record ,1998.

[12] Arnold, V., Arithmetical turbulence of selfsimilar fluctuations statistics os large Frobenius numbers of additive semigroups of integers. Moscow Math. Journal 7:173-193, (2007).

[13] Arnold, V., On additive semigroups starting parts. Funct. Anal. Other Math., 2:81-86, (2008).

[14] Disponível em: <http://pendientedemigracion.ucm.es/info/pecar/Articulos/Boyd.pdf. Acesso em 10 de Junho de 2013.

[15] Documento-semigrupos-numericos-e-corpos-de-funcoes-algebricas,Disponível em < http://elementos.ufac.br/proplan/elementos/edicoes/ > Acesso em : 10 de junho de 2013.

[16] Disponível em: < http://link.springer.com/article/10.1007/s11853-011-0048-9 > Acesso em 15 de julho de 2013.

[17] Disponível em: < Disponível em: < http://www.mat.ufmg.br/ anacris/Rafael2.pdf> Acesso em : 15 de julho de 2013.