**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**

**DEPARTAMENTO DE MATEMÁTICA**

**PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA**

**PROFMAT**

**GILBERTO DE PAIVA**

# A MATEMÁTICA DO RESTO: APLICAÇÕES DE CONGRUÊNCIA PARA AS SÉRIES FINAIS DO ENSINO FUNDAMENTAL E MÉDIO

**VITÓRIA**

**2016**

**GILBERTO DE PAIVA**

# A MATEMÁTICA DO RESTO: APLICAÇÕES DE CONGRUÊNCIA PARA AS SÉRIES FINAIS DO ENSINO FUNDAMENTAL E MÉDIO

Trabalho apresentado ao Programa de Pós-Graduação PROFMAT do Departamento de Matemática da Universidade Federal do Espírito Santo, como requisito para obtenção de grau de Mestre em Matemática.

Orientador: Prof. Dr. Florêncio Ferreira Guimarães Filho

**VITÓRIA**

**2016**

*EM BRANCO*

*EM BRANCO*

# AGRADECIMENTOS

*Agradeço à força misteriosa que age sobre todos nós, seja na forma de Deus, seja na forma da vida.*

*A "Seu" Antônio e à Dona Maria pela criação e pelas oportunidades, pelas noites não dormidas para que eu pudesse crescer e pelo apoio incondicional.*

*A Luciana, Gilson, Lucimara, Luciara e Luiza, irmãos que me ensinaram o que é viver em família.*

*A Scheila, pela sua doçura, cobrança e mais do que nunca seu apoio nessa jornada.*

*A Morgana e a Eleonor, as cores dos meus dias e forças de viver.*

*Aos professores do Departamento de Matemática da Universidade Federal do Espírito Santo, em especial ao corpo docente do PROFMAT: Dr. Etereldes Gonçalves Júnior, Dr. Fábio Júlio da Silva Valentim, Dr. Moacir Rosado Filho. e Dr. Valmecir Antônio dos Santos Bayer, por todo conhecimento.*

*Ao meu orientador Prof Dr. Florêncio Ferreira Guimarães Filho, por todas as ideias e pela fonte de inspiração inigualável.*

*Ainda aos colegas de trabalho e alunos da Escola Estadual de Ensino Fundamental e Médio Teófilo Paulino pelo crescimento profissional único.*

*E por fim, a você pela intenção de ler esse texto que com apreço escrevi.*

*Eadem mutata resurgo*

*(Embora mudado, devo me erguer o mesmo).*

*- Jacob Berroulli*

## RESUMO

Este trabalho consiste em propostas de atividades para a utilização no ensino fundamental e médio, abordando Números Inteiros, Equações Diofantinas Lineares, Congruência e suas aplicações, como o Algoritmo Chinês dos Restos e na organização de um calendário. Cada capítulo contém um desenvolvimento teórico contextualizado, exercícios e suas soluções.

## ABSTRACT

This work consists of activities proposed for use in elementary and secondary education, addressing Integers, Linear Diophantine Equations, congruence and its applications, such as Chinese Remainder Theorem and organizing a schedule. Each chapter contains a theoretical development contextualized, exercises and their solutions.

**SUMÁRIO**

# 1 INTRODUÇÃO

O presente trabalho tem como objetivo a obtenção do grau de Mestre em matemática e consolidar o aprendizado dos conteúdos cursados no PROFMAT – Mestrado Profissional em Matemática em Rede Nacional, e mais do que, isso levar aos professores da educação básica aplicações do tão esquecido resto da divisão, encarado eventualmente como um estorvo num universo de múltiplos e resultados exatos.

Durante a construção das atividades aqui propostas, o autor usou com equilíbrio sua atuação em escola pública da rede estadual de ensino, onde lecionou para alunos do oitavo e nono ano, bem como do ensino médio, além de sua experiência com o Programa de Iniciação Cientifica da Olimpíada Brasileira de Matemática das Escolas Públicas. A união dessas tarefas distintas trouxe à luz uma preocupação maior com o rigor que deve ser empregado em atividades diárias da vida estudantil e conceitos abstratos, como números primos, mínimos múltiplos comuns e máximos divisores comuns, mostrando suas utilidades em situações diversas.

A escolha da aritmética modular como pano de fundo desse trabalho deve-se ao fato de que o uso desses conceitos são precariamente citados nos livros didáticos, ou apenas excluídos pela falta de conhecimento de suas aplicações.

No primeiro capítulo, propõe-se uma revisão geral dos conceitos necessários do Conjunto dos Números Inteiros, para em seguida adentrarmos nas Equações Diofantinas, com exercícios que apresentariam certa dificuldade para serem resolvidos sem a ajuda da escrita das soluções dessa classe de problemas.

Em sequência, estudamos o conceito de Congruência Modular e suas propriedades, uma operação simples, porém muito elegante para a verificação de resultados e até para a criação de algoritmos mais rebuscados. Seu conhecimento se faz necessário quando percebemos que deixamos de lado o resto da divisão euclidiana de dois números inteiros, e esses podem ser usados para resolver problemas em que máquinas calculadoras e uso de computadores se tornam inviáveis por sua restrição funcional.

As aplicações decorrentes dos três itens acima - Números Inteiros, Equações Diofantinas e Congruência Modular - permite aos professores diversas formas de apresentar aos alunos conceitos da matemática pura e diversas aplicações no cotidiano, como o modelo das cigarras norte-americanas que possuem um singelo ciclo de vida e exemplificam o Algoritmo Chinês dos Restos, que possui bom emprego na resolução de sistemas de congruências.

No sexto capítulo é mostrado, a partir da organização de um evento esportivo, que a determinação da ordem de turnos pode ser obtida através de resultados numéricos, garantindo equilíbrio dos participantes.

Encerrando este trabalho, é sugerido um algoritmo para a determinação do dia da semana de uma data qualquer, explicando assim como a matemática interferiu na ocorrência dos anos bissextos e na história dos calendários Juliano e Gregoriano.

# 2 NÚMEROS INTEIROS

## 2.1 DIVISIBILIDADE DE NÚMEROS INTEIROS

Seja o conjunto dos Números Inteiros definidos como de costume e representado por $\mathbb{Z}$, logo:

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

Além disso, sejam conhecidas a Adição e a Multiplicação de números inteiros bem como suas propriedades:

1) Comutativa: para cada $a, b \in \mathbb{Z}$

$$a + b = b + a$$

$$a \cdot b = b \cdot a$$

2) Associativa: para cada $a, b, c \in \mathbb{Z}$

$$(a + b) + c = a + (b + c)$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

3) Distributiva: para cada $a, b, c \in \mathbb{Z}$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

4) Elemento Neutro: para cada $a \in \mathbb{Z}$

$$a + 0 = a$$

$$a \cdot 1 = a$$

5) Elemento Simétrico: para cada $a \in \mathbb{Z}$

$$a + (-a) = 0$$

Dados $a, b \in \mathbb{Z}$, dizemos ainda que $a$ é *múltiplo* de $b$, ou $a$ é *divisível* por $b$, quando $b \neq 0$ e existe algum inteiro $c$ tal que:

$$a = b \cdot c$$

Representamos esse fato por $b|a$. Por exemplo, $200$ é múltiplo de $8$, pois $200 = 8 \cdot 25$, ou seja, $8|200$.

Caso contrário, representamos por $b \nmid a$, como por exemplo $3 \nmid 100$, uma vez que não existe inteiro $n$ tal que:

$$100 = 3 \cdot n$$

Assim definido podemos listar as propriedades abaixo, sendo $a, b, c, m, n, x, y \in \mathbb{Z}$

*1)* Se $a|b$ e $b|c$ então $a|c$.

De fato, se $a|b$ e $b|c$, então $b = n \cdot a$ e $c = m \cdot b$ e, logo, $c = m \cdot (n \cdot a)$. Pela propriedade associativa da multiplicação temos:

$$c = (m \cdot n) \cdot a$$

Ou seja, $a|c$.

2) Se $a|b$ e $a|c$ então $a|(b \pm c)$.

De fato, se $a|b$ e $a|c$, então $b = n \cdot a$ e $c = m \cdot a$, logo $b \pm c = n \cdot a \pm m \cdot a = (m \pm n) \cdot a$, pela propriedade distributiva e, logo $a|b \pm c$

3) Se $a|(b + c)$ e $a|b$ então $a|c$;

De fato, se $a|(b+c)$ e $a|b$, então $b = y \cdot a$ e $b + c = x \cdot a$, e portanto, podemos escrever:

$$y \cdot a + c = x \cdot a$$

$$c = x \cdot a - y \cdot a$$

$$c = (x - y) \cdot a$$

Por fim, $a|c$.

**Exercício 2.1:** Verifique, usando a definição, que $1|a$ e $a|a$.

**Solução:** De fato, podemos escrever $a = a \cdot 1$, e pela propriedade comutativa da multiplicação temos $a = 1 \cdot a$ e, logo, $1|a$ e $a|a$.

**Exercício 2.2**: Um tabuleiro quadrado $5 \times 5$ pode ser coberto por dominós $1 \times 2$?

**Solução:** O tabuleiro possui $25$ quadrados, já a peça de dominó sempre ocupará $1 \times 2 = 2$ casas do tabuleiro. Uma quantidade $n$ de peças cobrirá $2n$ quadrados, e logo:

$$25 = 2 \cdot n$$

Porém $2 \nmid 25$, sendo portanto é impossível tal fato.

**Exercício 2.3:** O produto de 22 números inteiros é igual a 1. Mostre que a soma deles não pode ser zero.

**Solução:** Uma vez que apenas $-1$ e $1$ dividem $1$, tal produto é positivo quando a quantidade de números negativos é par. Portanto suponha que existam $n$ números $-1$ nesse conjunto de $22$ números, os demais por sua vez são iguais a $1$. Logo, a soma em questão pode ser expressa por:

$$n \cdot (-1) + (22 - n) \cdot 1 = -n + 22 - n = 22 - 2n$$

Como $n$ é par, o mesmo não é $11$ e, portanto, a soma nunca será igual a zero.

Em especial, há números inteiros positivos que possuem apenas dois divisores positivos. Estes são denominados *números primos* e fazem parte pela multiplicação da formação, dos demais números inteiros chamados de *números compostos.* Os únicos divisores positivos de um número primo são $1$ e ele mesmo.

Por exemplo, os números $2$, $3$ e $7$ são números primos, enquanto $10 = 2 \cdot 5$ é composto.

## 2.2 DIVISÃO EUCLIDIANA

Dados os inteiros $a$ e $b$, com $b \neq 0$, podemos enunciar o algoritmo da Divisão Euclidiana de $a$ por $b$. Vamos definir inicialmente o conhecido Principio da Boa Ordem, estabelece que:

“Todo subconjunto não vazio de números inteiros não negativos possui um menor elemento”.

Se $A$ é um subconjunto, não vazio, de inteiros não negativos dizemos que $a$ é o menor elemento de $A$ quando satisfaz simultaneamente as propriedades:

i) $a \in A$;

ii) para todo $n$ pertencente a $A$, tem-se que $a \leq n$

**Divisão Euclidiana:** Sejam $a$ e $b$ dois números inteiros, com $0 < a < b$. Existem dois únicos números inteiros não negativos $q$ e $r$ tais que

$$b = a \cdot q + r, \text{ com } 0 \leq r < a.$$

Os inteiros $q$ e $r$ são chamados de quociente e resto da divisão euclidiana de a por $b$, respectivamente.

**Demonstração:**

Suponha que $b > a$ e considere nos inteiros não negativos, o conjunto $S$ tal que

$$S = \{b, \quad b - a, \ b - 2a, \quad \ldots, \quad b - n \cdot a, \quad \ldots\}$$

Pela Principio da Boa Ordem, o conjunto $S$ tem um menor elemento $r = b - q \cdot a$. Como $r \in S$, então $r \geq 0$. Vamos provar que $r < a$.

Vamos mostrar que não pode ocorrer $r \geq a$. De fato, se isso fosse verdade, existiria um número inteiro não negativo $s < r$ tal que $r = a + s$. Consequentemente, sendo $r = s + a = b - q \cdot a$, teríamos

$$s = b - (q + 1) \cdot a \in S, \text{ com } s < r,$$

o que contradiz o fato de $r$ ser o menor elemento de $S$. Portanto, temos que $b = a \cdot q + r$ com $0 \leq r < a$, o que prova a existência de $q$ e $r$.

Agora vamos provar a unicidade. Dados dois elementos distintos de $S$, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de $a$, é pelo menos igual a $a$. Logo, se $r_1 = b - a \cdot q_1$ e $r_2 = b - a \cdot q_2$, com $r_1 < r_2 < a$, teríamos $r_2 - r_1 \geq a$, o que acarretaria $r_2 \geq r_1 + a \geq a$, absurdo. Portanto, $r_1 = r_2$.

Daí segue-se que $b - a \cdot q_1 = b - a \cdot q_2$, o que implica que $a \cdot q_1 = a \cdot q_2$ e, portanto, $q_1 = q_2$.

**Exercício 2.4:** Determine o quociente e o resto da divisão de:

a) 210 por 6

b) 587 por 3

c) 9514 por 2

d) 1080 por 13

**Solução:**

a) $210 = 6 \cdot 35 + 0$

b) $587 = 3 \cdot 195 + 2$

c) $9514 = 2 \cdot 4757 + 0$

d) $1080 = 13 \cdot 83 + 1$

## 2.3 MÁXIMO DIVISOR COMUM

Quando observamos os inteiros $10$ e $26$ conseguimos perceber que $2|10$ e $2|26$, ou seja, $2$ é um *divisor comum* de $10$ e $26$. Assim, dados dois números inteiros $a$ e $b$, não simultaneamente nulos, dizemos que o número $d$ é um *divisor comum* de $a$ e $b$ se $d|a$ e $d|b$.

Podemos citar como exemplo ainda os números $1, 2, 3$ e $6$ que são divisores comuns de $30$ e $72$.

Em especial podemos definir um número positivo $d$ como sendo o *máximo divisor comum* (mdc) de $a$ e $b$ se esse for o maior divisor comum de $a$ e $b$.

Assim $mdc(30, 72) = 6$, pois $6|30$ e $6|72$, além de ser 6 o maior divisor de $30$ e $72$.

Precisamos de um algoritmo para descobrir o $mdc$ de inteiros $a$ e $b$. Para tanto vamos verificar o conhecido Lema de Euclides:

**Lema de Euclides:** Se $d = mdc(a, b)$ então $mdc(a, b - na) = d$

**Demonstração:** Pela definição do máximo divisor comum, temos que $d|a$ e $d|b$. Tem-se $d|b - na$ pelas propriedades da divisibilidade, uma vez que podemos escrever $a = dx$ e $b = dy$ com $x, y \in \mathbb{Z}$ e logo, $b - na = dy - ndx = d(y - nx)$. Assim, $d$ é um divisor comum de $a$ e $b - na$. Seja $c$ outro divisor comum de $a$ e $b - na$, então $c|a$ e $c|b - na$. Logo $c|b$ e, portanto $c \leq d$. Isso prova que $mdc(a, b - na) = d$.

**Exercício 2.5:** Calcular o $mdc$ de $84$ e 30.

**Solução:** Pelo lema de Euclides temos que:

$$mdc(84,30) = mdc(30,84 - 2 \cdot 30)$$

$$mdc(84,30) = mdc(30,24)$$

Repetindo o processo:

$$mdc(30,24) = mdc(24,30 - 24)$$

$$= mdc(6,24) = 6$$

Portanto, $mdc(84,30) = mdc(30,24) = mdc(24,6) = 6$

Tal procedimento pode ser representado pelo algoritmo de Euclides para $mdc$, em que na primeira linha aparece o quociente da divisão dos dois números iniciais da linha do meio, e na última constará o resto da divisão do mesmo. Assim:

| | 2 | 1 | 4 |
|---|---|---|---|
| 84 | 30 | 24 | 6=mdc(84,30) |
| 24 | 6 | 0 | |

Ao observar a sistematização acima conseguimos formar duas equações que originam os restos das divisões:

$$6 = 30 - 1 \cdot 24$$

$$24 = 84 - 2 \cdot 30$$

Substituindo a segunda equação na primeira, temos que:

$$6 = 30 - 1 \cdot (84 - 2 \cdot 30)$$

$$6 = 3 \cdot 30 - 1 \cdot 84$$

**Exercício 2.6:** Calcular o $mdc$ de $180$ e $24$.

**Solução:**

Pelo algoritmo de Euclides para o $mdc$, podemos sistematizar da seguinte forma:

| | **7** | **2** |
|---|---|---|
| **180** | 24 | 12 |
| **12** | 0 | |

Ou seja, $mdc(180{,}24) = 12$.

Ao observar a sistematização acima conseguimos formar uma equação no qual figura o $mdc$ como igualdade:

$$12 = 180 + 24 \cdot (-7)$$

A equação em questão que aparece no final dos dois exemplos anteriores é conhecida como **Relação de Bézout.**

**Relação de Bézout:** Dados dois números inteiros positivos $a$ e $b$, não nulos simultaneamente, existem dois inteiros $m$ e $n$ tais que:

$$a \cdot m + b \cdot n = mdc(a, b)$$

Vale a observação de que dois inteiros $a$ e $b$ tais que $mdc(a, b) = 1$ são denominados *primos entre si*.

Observe que um divisor comum de $a$ e $b$, divide $am + bn = mdc(a, b)$, ou seja, qualquer outro divisor comum do $a$ e $b$, também é divisor de $mdc(a, b)$.

**Demonstração:**

Sejam $a$ e $b$ números inteiros positivos. Aplicando o algoritmo de Euclides temos:

$$\begin{aligned}
\boldsymbol{a} &= bq_1 + r_1 && 0 \leq r_1 < b \\
\boldsymbol{b} &= r_1 q_2 + r_2 && 0 \leq r_2 < r_1 \\
\boldsymbol{r_1} &= r_2 q_3 + r_3 && 0 \leq r_3 < r_2 \\
&\vdots \quad \vdots && \vdots
\end{aligned}$$

$$\boldsymbol{r_{n-3}} = \quad r_{n-2}q_{n-1} \; + \; r_{n-1} \qquad\qquad 0 \leq r_{n-1} < r_{n-2}$$

$$\boldsymbol{r_{n-2}} = \quad r_{n-1}q_{n} \; + \; r_{n} \qquad\qquad 0 \leq r_{n} < r_{n-1}$$

$$\boldsymbol{r_{n-1}} = \quad r_{n}q_{n+1} \; + \; 0$$

para algum $r_n$ que divida $r_{n-1}$ . E assim, pelo algoritmo de Euclides $mdc(a,b) = r_n$.

Podemos escrever as seguintes equações:

$$r_{n-2} - r_{n-1}q_n = r_n$$

$$r_{n-3} - r_{n-2}q_{n-1} = r_{n-1}$$

$$r_{n-4} - r_{n-3}q_{n-2} = r_{n-2}$$

$$\vdots$$

$$r_1 - r_2q_3 = r_3$$

$$b - r_1q_2 = r_2$$

$$a - bq_1 = r_1$$

Substituindo essas equações nessa ordem, teremos:

$$a \cdot m + b \cdot n = mdc(a,b)$$

**Exercício 2.6:** Mostre que se $a|b \cdot c$ e $mdc(a,b) = 1$, então $a|c$.

**Solução:** Como $a|b \cdot c$ então existe um inteiro $x$ tal que $b \cdot c = a \cdot x$ e, pela Relação de Bézout, podemos afirmar que existem $m, n \in \mathbb{Z}$ tais que:

$$a \cdot m + b \cdot n = 1$$

Multiplicando a equação acima por $c$ ficamos com:

$$a \cdot c \cdot m + b \cdot c \cdot n = c$$

Substituindo $b \cdot c = a \cdot x$ teremos:

$$a \cdot c \cdot m + a \cdot x \cdot n = c$$

Ou seja:

$$c = a \cdot (c \cdot m + x \cdot n)$$

Portanto, $a|c$.

**Exercício 2.7:** Mostre que se $mdc(a, b) = 1$, $a|c$ e $b|c$, então $a \cdot b|c$.

**Solução:** Como $a|c$ e $b|c$ então existem inteiros $x$ e $y$ tais que $c = a \cdot x$ e $c = b \cdot y$.

Pela Relação de Bézout existem $m, n \in \mathbb{Z}$ tais que:

$$a \cdot m + b \cdot n = 1$$

Multiplicando a equação por $c$ ficamos com:

$$a \cdot c \cdot m + b \cdot c \cdot n = c$$

Substituindo $c = a \cdot x$ e $c = b \cdot y$ teremos:

$$a \cdot b \cdot y \cdot m + b \cdot a \cdot x \cdot n = c$$

Ou seja:

$$c = ab \cdot (y \cdot m + x \cdot n)$$

Portanto $a \cdot b|c$.

## 2.4 MÍNIMO MÚLTIPLO COMUM

Quando um aluno das séries iniciais consulta a tabuada não é raro perceber que certos resultados se repetem algumas vezes, como o $24$ que aparece quando multiplicamos $3 \cdot 8$ e $4 \cdot 6$. Dessa forma, o número 24 é um *múltiplo comum* de $3$ e de $4$.

Em especial, podemos definir um número inteiro $m$ como sendo o *mínimo múltiplo comum* $(mmc)$ de $a$ e $b$, não ambos nulos, quando $m$ é o menor número positivo que é múltiplo simultâneo de $a$ e $b$.

**Exercício 2.8:** Um ciclista dá a volta em uma pista circular em 12 minutos e um atleta em 18 minutos. Os dois partem ao mesmo tempo às 8 horas. A que horas voltam a se encontrar no ponto de partida e quantas voltas dá cada um?

**Solução:** Observamos que o ciclista retornará ao ponto de partida nos múltiplos de 12 minutos, ou seja, voltará em: 24 min; 36 min; 48 min e assim por diante.

Já o atleta retornará ao ponto de partida nos múltiplos de 18 minutos, ou seja, voltará em: 36 min; 54 min; 72 min e assim por diante.

O primeiro encontro ocorrerá aos $mmc(12,18) = 36$ minutos e logo, os ciclistas se encontrarão às 8:36. O primeiro terá dado 3 voltas, enquanto o segundo terá percorrido 2 voltas.

Uma primeira observação acerca do $mmc$ nos diz que se $a$ e $b$ são números inteiros positivos e $a$ é múltiplo de $b$, então $mmc(a,b) = a$.

**Teorema 2.2:** Se $a$ e $b$ são números inteiros positivos, então

$$mmc(a,b) = \frac{ab}{mdc(a,b)}$$

Seja $m = \frac{ab}{mdc(a,b)}$ e $d = mdc(a,b)$. Existem inteiros $a'$ e $b'$ tais que $a = a'd$ e $b = b'd$.

Por sua vez, podemos escrever $m$ como:

$$m = \frac{a}{d} \cdot b = a \cdot \frac{b}{d}$$

$$m = a'b = ab'$$

Logo, $m$ é múltiplo comum de $a$ e $b$.

Seja $M$ um múltiplo comum positivo de $a$ e $b$. Então $M = ap = bq$ com $p, q \in \mathbb{Z}$. Substituindo nessa última igualdade $a = a'd$ e $b = b'd$ temos:

$$M = a'dp = b'qd$$

Simplificando:

$$\frac{M}{d} = a'p = b'q$$

Sabemos, pela relação de Bézout, que existem inteiros $x$ e $y$ tais que:

$$ax + by = d$$

Por sua vez, podemos escrever:

$$a'dx + b'dy = d$$

Simplificando:

$$a'x + b'y = 1$$

Multiplicando todos os membros dessa última igualdade por $p$, temos:

$$a'px + b'py = p$$

Mas $a'p = b'q$ e logo:

$$b'qx + b'py = p$$

Ou seja, $b'|p$ e logo $ab'|ap$. Podemos ainda observar que $m = ab'$ e $M = ap$, ou seja, $m|M$. Portanto, $m \leq M$ e, logo, $m = mmc(a, b)$.

**Teorema 2.3:** Sejam $a$ e $b$ inteiros não nulos e $m = mmc(a, b)$. Se $M$ é um múltiplo comum de $a$ e $b$, então $m|M$.

**Demonstração:** Pela divisão euclidiana, existem $q$ e $r$ tais que $M = mq + r$, com $0 \leq r < m$. Além disso, $a|M$ e $a|m$, logo $a|(M - mq)$, isto é, $a|r$. Analogamente, $b|r$. Por fim, $r$ é um múltiplo comum não negativo de $a$ e $b$ que deve ser menor do que $m$, ou seja, $r = 0$.

**Exercício 2.9:**

Um feirante levava sempre a mesma quantidade $N$ de laranjas para serem vendidas na feira. Quando ele dividia as $N$ laranjas em sacolas contendo 4 laranjas cada uma, não sobrava nenhuma laranja. Quando dividia as $N$ laranjas em sacolas de 5 laranjas cada uma e quando as dividia em sacolas de 6 laranjas cada uma, também não sobrava nenhuma laranja. Destaque-se que esse feirante nunca levava mais de 400 laranjas para a feira.

Determine

a) os possíveis valores de $N$ com base apenas nos dados acima.

Solução: Como o número $N$ não possui resto quando dividido por 4, 5 e 6, as opções viáveis são os múltiplos comuns de $4, 5$ e $6$: 60, 120, 180, 240, 300, 360.

b) o valor de $N$, sabendo ainda que, no dia em que o feirante dividiu as N laranjas em sacolas de 7 laranjas cada uma, sobraram 3 laranjas.

Pela divisão euclidiana, vemos que apenas o 360, dentre os números destacados no item anterior, pode ser escrito como $7q + 3$.

# 3. EQUAÇÕES DIOFANTINAS

No ensino médio, é comum os alunos assumirem que a equação $ax + by = c$ representa uma reta no plano e mais do que isso se faz uma ligação com uma função afim. Porém quando restringimos os possíveis valores das variáveis $x$ e $y$ para os números inteiros os métodos de solução ensinados para a geometria não são úteis, restando apenas a tentativa e o erro. Equações como acima, com $a, b, x, y \in \mathbb{Z}$ são conhecidas como Equações Diofantinas, homenagem a Diofanto de Alexandria, considerado o maior algebrista grego, que tratou de resolver vários problemas em seu livro Aritmética.

**Teorema 3.1:** A equação $ax + by = c$, com $a, b, c \in \mathbb{Z}$ admite solução se, e somente se, $mdc(a, b)|c$.

**Demonstração:**

Suponha que $x_0$ e $y_0$ sejam soluções da equação. Então, $ax_0 + by_0 = c$. Como $mdc(a, b)$ divide $a$ e $b$, segue que ele divide $ax_0 + by_0$ e logo, $mdc(a, b)$ divide $c$.

Reciprocamente, vamos supor que $mdc(a, b)$ divide $c$, ou seja existe um inteiro $d$ tal que $c = mdc(a, b) \cdot d$. Entretanto, sabemos que quaisquer $m, n \in \mathbb{Z}$ tais que $mdc(a, b) = a \cdot m + b \cdot n$, como nos diz a Relação de Bezout. Multiplicando tal igualdade por $d$ temos:

$$c = d \cdot mdc(a, b) = (a \cdot m + b \cdot n) \cdot d$$

$$c = a \cdot (md) + b \cdot (nd)$$

Basta tomar como solução da equação $x = md$ e $y = nd$.

Ainda temos que mostrar qual será a forma das soluções de uma equação diofantina, se esta possuir solução. Para tanto seja o teorema abaixo enunciado.

**Teorema 3.2**: Seja $d = mdc(a, b)$. Seja $x_0$ e $y_0$ uma solução particular, arbitrariamente conhecida, da equação $ax + by = c$. Então as soluções da equação são da forma $x = x_0 + \frac{b}{d}t$ e $y = y_0 - \frac{a}{d}t$, para $t$ variando em $\mathbb{Z}$

**Demonstração:**

Se $(x_0, y_0)$ é uma solução particular da equação $ax + by = c$ e $(x_1, y_1)$ uma solução qualquer dessa equação, então:

$$ax_1 + by_1 = c = ax_0 + by_0$$

É evidente que ficamos com:

$$a(x_1 - x_0) = b(y_0 - y_1)$$

Como $d|a$ e $d|b$ existem inteiros $r$ e $s$, com $mdc(r, s) = 1$, tais que $a = dr$ e $b = ds$, logo:

$$dr(x_1 - x_0) = ds(y_0 - y_1)$$

$$r(x_1 - x_0) = s(y_0 - y_1)$$

Ou seja, $r|s(y_0 - y_1)$. Como $mdc(r, s) = 1$, então $r|y_0 - y_1$(Veja o Exercício 2.6, na página 21),e logo existe um inteiro $t$ tal que:

$$y_0 - y_1 = rt$$

$$y_1 = y_0 - \frac{a}{d}t$$

Portanto, temos:

$$r(x_1 - x_0) = srt$$

$$x_1 - x_0 = st$$

$$x_1 = x_0 + \frac{b}{d}t$$

Então, para todo inteiro $t$, temos que as soluções de uma equação diofantina podem ser escritas como:

$$x = x_0 + \frac{b}{d}t \text{ e } y = y_0 - \frac{a}{d}t$$

**Exercício 3.1:**

De quais maneiras podemos comprar carimbos de cinco e de sete reais, de modo a gastar duzentos reais?

**Solução:**

Sejam $x$ e $y$ a quantidade de carimbos de cinco e sete reais, respectivamente. Logo, nossa equação diofantina pode ser escrita como:

$$5x + 7y = 200$$

Uma vez que o $mdc(5,7) = 1|200$, a equação possui solução inteira. Em particular, temos $x = 40$ e $y = 0$. Como demonstramos acima as soluções possíveis dessa igualdade respeitam a forma:

$$x = 40 - 7t \text{ e } y = 5t$$

Como estamos tratando de quantidades, os valores das variáveis estão restringidas a números não negativos. Assim, as soluções possíveis são:

$$(40,0);\ (33,5);\ \ (26,10);\ \ (19,15);\ \ (12,20) \text{ e } (5,25)$$

Portanto, há seis maneiras de comprarmos carimbos de cinco e sete reais gastando duzentos reais.

**Exercício 3.2:** Resolva as equações diofantinas abaixo:

a) $3x - 12y = 7$

b) $21x + 48y = 6$

c) $1990x - 173y = 11$

**Solução:**

a) Como $mdc(3,12) = 3$ e $3 \nmid 7$, a equação não possui soluções inteiras.

b) Uma vez que $mdc(48,21) = 3|6$, então a equação possui solução inteira. Pelo algoritmo de Euclides para $mdc$, temos:

| | 2 | 3 | 2 |
|---|---|---|---|
| 48 | 21 | 6 | 3 |
| 6 | 3 | 0 | |

Logo, podemos escrever a equação

$$6 = 21 \cdot (-2) + 48 \cdot 1$$

Portanto as soluções da equação são:

$$x = -2 + \frac{48}{3}t \text{ e } y = 1 - \frac{21}{3}t$$

$$x = -2 + 16t \text{ e } y = 1 - 7t$$

c) Vamos primeiro calcular o $mdc$ de $1990$ e $173$ pelo algoritmo de Euclides:

| | 11 | 1 | 1 | 86 |
|---|---|---|---|---|
| 1990 | 173 | 87 | 86 | 1 |
| 87 | 86 | 1 | 0 | |

Como $mdc(1990, 173) = 1$ e esse divide $11$, a equação possui solução e, assim, podemos formar as equações:

$$1 = 87 \cdot 1 - 86 \cdot 1$$

$$86 = 173 \cdot 1 - 87 \cdot 1$$

$$87 = 1990 \cdot 1 - 173 \cdot 11$$

Substituindo a segunda equação na primeira teremos:

$$1 = 87 \cdot 1 - (173 \cdot 1 - 87 \cdot 1) \cdot 1$$

$$1 = 87 \cdot 2 - 173 \cdot 1$$

Por fim, substituindo nesta última equação ficamos com:

$$1 = (1990 \cdot 1 - 173 \cdot 11) \cdot 2 - 173 \cdot 1$$

$$1 = 1990 \cdot 2 - 173 \cdot 23$$

Essa última igualdade representa a Relação de Bézout. Multiplicando-a por $11$ ficamos com a igualdade:

$$11 = 1990 \cdot 22 - 173 \cdot 253$$

Portanto, as soluções de tal equação diofantina são representadas por:

$$x = 22 + 173t \text{ e } y = -253 - 1990t$$

**Exercício 3.3:** Uma pessoa foi ao banco para descontar um cheque no valor de $x$ reais e $y$ centavos. O caixa do banco errou na leitura do valor do cheque e pagou $y$ reais e $x$ centavos. A pessoa guardou o dinheiro no bolso sem verificar a quantia.

No caminho, ela gastou cinco centavos e quando chegou em casa verificou que tinha exatamente o dobro do valor do cheque. Sabendo-se que essa pessoa não levou dinheiro nenhum consigo quando foi ao banco, pergunta-se qual era o valor do cheque.

**Solução:** Sabemos que $1$ real equivale a $100$ centavos, e logo o cheque estava preenchido com um total de $100x + y$ centavos. Já o valor pago pelo caixa foi de $100y + x$ centavos. Seguindo o enunciado do problema, sabemos que após gastar cinco centavos a pessoa ainda teria o dobro da quantia inicial, e logo:

$$(100y + x) - 5 = 2(100x + y)$$

Simplificando tal expressão teremos:

$$-199x + 98y = 5$$

Como $mdc(199{,}98) = 1$, tal equação diofantina possui solução. Pelo algoritmo de Euclides para $mdc$ temos:

| | 2 | 32 | 1 | 2 |
|---|---|---|---|---|
| 199 | 98 | 3 | 2 | 1 |
| 3 | 2 | 1 | 0 | |

Ficamos assim com as equações:

$$1 = 1 \cdot 3 - 1 \cdot 2$$

$$2 = 1 \cdot 98 - 3 \cdot 32$$

$$3 = 1 \cdot 199 - 2 \cdot 98$$

Ou seja, podemos escrever $mdc(199{,}98)$ segundo a relação de Bézout como:

$$1 = 1 \cdot 3 - 1 \cdot (1 \cdot 98 - 3 \cdot 32)$$

$$1 = 33 \cdot 3 - 1 \cdot 98$$

$$1 = 33 \cdot (1 \cdot 199 - 2 \cdot 98) - 1 \cdot 98$$

$$1 = 33 \cdot 199 - 67 \cdot 98$$

A equação original da questão é igualada a cinco, logo vamos multiplicar a igualdade por esse valor, ficando com:

$$5 = 165 \cdot 199 - 335 \cdot 98$$

Pelas soluções descritas acima teremos:

$$x = 165 - 98t \text{ e } y = -335 - 199t$$

Como o problema pede em valores de reais e centavos, uma análise rápida é necessária para percebermos que os valores pedidos na questão têm dois dígitos. Para tanto, temos que escolher $t = 2$. Logo:

$$x = -165 + 98 \cdot 2 = 31$$

$$y = -335 + 199 \cdot 2 = 63$$

Assim o valor do cheque em questão era de R$ 31,63.

# 4 CONGRUÊNCIA

Seja $m$ um número inteiro positivo. Dizemos que os números inteiros $a$ e $b$ são côngruos módulo $m$ quando ambos deixam o mesmo resto na divisão por $m$ e representamos esse fato como:

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

Caso contrário, representamos por:

$$a \not\equiv b \ (mod\ m)$$

**Exemplo 4.1:**

1) $21 \equiv 15 \ (mod\ 6)$, pois $21 = 6 \cdot 3 + 3$ e $15 = 6 \cdot 2 + 3$
2) $10 \equiv 17 \ (mod\ 7)$, pois o resto da divisão de ambos por $7$ é $3$.
3) $20 \not\equiv 5 \ (mod\ 4)$, pois o resto da divisão de $20$ por $4$ é $0$, enquanto o resto da divisão de $5$ por $4$ é $1$.

**Teorema 4.1:** $a \equiv b \ (mod\ m)$ se, e somente se, $a - b$ é múltiplo de $m$.

**Demonstração:**

Pelo algoritmo da divisão temos que:

$$a = m \cdot q_a + r_a \text{ e } b = m \cdot q_b + r_b$$

$$\text{Com } q_a, q_b, r_a, r_b \in \mathbb{Z} \text{ e } 0 \leq r_a, r_b < m$$

Assim podemos escrever:

$$a - b = m \cdot (q_a - q_b) + r_a - r_b$$

Podemos afirmar que $a - b$ será múltiplo de $m$ se, e somente se, $r_a - r_b$ for divisível por $m$. Suponha que $r_b \leq r_a$. Então $0 \leq r_a - r_b < m$. Logo, $m$ divide $a - b$ se, e somente se, $r_a - r_b = 0$, ou seja, se, e somente se, $r_a - r_b$.

Podemos, assim, enunciar as seguintes propriedades:

i) $a \equiv a\ (mod\ m)$.

ii) Se $a \equiv b\ (mod\ m)$, então $b \equiv a\ (mod\ m)$.

iii) Se $a \equiv b\ (mod\ m)$ e $b \equiv c\ (mod\ m)$, então $a \equiv c\ (mod\ m)$

Além dessas propriedades, precisamos enunciar algumas operacionalidades sobre as congruências. Entre elas temos:

i) Se $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então $a \pm c \equiv b \pm d\ (mod\ m)$.

**Demonstração:** Temos que $m|(b - a)$ e $m|(d - c)$. Pelas propriedades da divisibilidade podemos afirmar que:

$$m|((b - a) \pm\ (d - c))$$

Assim:

$$m|((b \pm d) - (a \pm c))$$

Ou seja:

$$a \pm c \equiv b \pm d\ (mod\ m)$$

ii) Se $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então $a \cdot c \equiv b \cdot d\ (mod\ m)$.

**Demonstração:** Sabemos que $m|(a - b)$ e $m|(c - d)$. Além disso, podemos perceber que:

$$a \cdot c - b \cdot d = a(c - d) + d \cdot (a - b)$$

Logo, $m|a \cdot c - b \cdot d$, e portanto:

$$a \cdot c \equiv b \cdot d \ (mod\ m)$$

iii) Se $a \equiv b \ (mod\ m)$ e $n$ é inteiro positivo, então $a^n \equiv b^n \ (mod\ m)$.

**Demonstração:**

Basta aplicar $n$ vezes a segunda propriedade que obteremos o resultado esperado.

**Exercício 4.1:** Calcule o resto da divisão de:

a) $12^{12}$ por $5$.

**Solução**: Temos que $12 \equiv 2 \ (mod\ 5)$. Pela segunda operação acima, podemos multiplicar ambos lados da equivalência por um mesmo número, uma vez que $12 \equiv 2 \ (mod\ 5)$. Assim:

$$12^2 \equiv 4 \ (mod\ 5)$$

Elevando a congruência ao quadrado teremos:

$$12^4 \equiv 16 \equiv 1 \ (mod\ 5)$$

Além disso:

$$(12^4)^3 \equiv 1^3 \ (mod\ 5)$$

$$12^{12} \equiv 1 \ (mod\ 5)$$

Logo, o resto da divisão de $12^{12}$ por $5$ é igual ao resto da divisão $1$ por $5$. Portanto o . $12^{12}$ deixa resto $1$ na divisão por $5$.

b) $41^{65}$ por 7

Tem-se:

$$41 \equiv 6\ (mod\ 7)$$

Além disso, vemos que $6 \equiv -1\ (mod\ 7)$, logo:

$$41^{65} \equiv (-1)^{65} \equiv -1(mod\ 7)$$

Assim, o resto da divisão de $41^{65}$ por 7 é igual a $7 - 1 = 6$.

**Exercício 4.2:** Se o resto da divisão de um inteiro $n$ por $5$ é igual a $3$, qual é o resto da divisão de $n^2$ por $5$?

**Solução:** Podemos escrever $n \equiv 3\ (mod\ 5)$. Elevando ambos lados da congruência ao quadrado temos:

$$n^2 \equiv 9 \equiv 4\ (mod\ 5)$$

Logo, o resto da divisão de $n^2$por $5$ é igual a $4$.

**Exercício 4.3:** Mostre que nenhum quadrado perfeito tem o algarismo das unidades igual a 2, 3, 7 ou 8.

**Solução:** Seja $n$ um número inteiro, então o mesmo pode ser escrito por $10n_1 + n_0$, sendo $n_0$ o algarismo das unidades de $n$. Assim:

$$n \equiv 10n_1 + n_0\ (mod\ 10)$$

$$n \equiv n_0\ (mod\ 10)$$

Logo $n^2 \equiv n_0^2 \ (mod\ 10)$ e, portanto, o algarismo das unidades de $n^2$ é o mesmo de $n_0^2$. Observando os possíveis valores para $n_0$ temos:

| $n_0$ | $n_0^2$ |
|---|---|
| **0** | 0 |
| **1** | 1 |
| **2** | 4 |
| **3** | 9 |
| **4** | 16 |
| **5** | 25 |
| **6** | 36 |
| **7** | 49 |
| **8** | 64 |
| **9** | 81 |

Assim os possíveis resultados para o algarismo das unidades de $n^2$ são 0, 1, 4, 5, 6 ou 9, que é equivalente ao pedido.

## 4.1 INVERSOS MODULARES

Voltemos agora à Relação de Bezout para $a$ e $b$ inteiros positivos e primos entre si. Neste caso, existem $x$ e $y$ inteiros tais que $ax + by = 1$. Aplicando a congruência módulo $b$ nessa igualdade chegamos a:

$$ax \equiv 1 \ (mod \ b)$$

Dizemos então que $a$ é invertível módulo $b$, ou ainda, $a$ possui inverso módulo $b$ uma vez que existe inteiro $x$ para a congruência acima. A decorrência desse fato é de suma importância para o desenvolvimento de algoritmos de criptografia e para a solução de sistemas de congruências que resolvem diversos problemas.

**Exercício 4.4:** Mostre que se $a$ é invertível módulo $m$, então $mdc(a, m) = 1$.

**Solução**: Suponha que $a$ possua inverso módulo $m$, e que esse seja $x$, logo:

$$ax \equiv 1 \ (mod \ m)$$

Donde podemos escrever:

$$ax - 1 = my$$

para algum inteiro $y$. Logo:

$$ax + m(-y) = 1$$

Essa última é a relação de Bézout para $a$ e $m$. Logo, $mdc(a, m) = 1$.

**Exercício 4.5:** Mostre que $n - 1$ é sempre seu próprio inverso módulo $n$.

**Solução**: Observe que:

$$(n-1) \cdot (n-1) \equiv n^2 - 2n + 1 \equiv 1 \ (mod \ n),$$

como queríamos demonstrar.

# 5. PERIODICIDADE DAS CIGARRAS E OS ALINHAMENTOS ORBITAIS

No ensino médio é comum vários problemas resultarem em um sistema linear, sendo solucionados pelos alunos por um dos diversos métodos ensinados. Desse mesmo modo, podemos usar interseções de progressões aritméticas para solucionarmos problemas mais específicos, como o exemplo abaixo.

**Exemplo 5.1**

No ano de 2001, duas espécies de cigarras norte-americanas fizeram seus rituais de acasalamento, entre elas a Onondaga Brood que irá repetir esse feito somente em intervalos de 17 anos. Já a segunda espécie, Baton Rouge Brood, irá aparecer em períodos de 13 anos. Qual será o próximo ano que ambas irão se reproduzirem juntas?

**Solução:** De fato, a primeira irá se reproduzir nos anos 2018, 2035,... formando uma progressão aritmética de razão igual a $17$. Enquanto a Baton Rouge se reproduziu no ano 2014 e voltará se reproduzir nos anos 2027, 2040... formando uma progressão aritmética de razão igual a $13$. Em qualquer apresentação simultânea das duas espécies terá havido um intervalo de anos que é múltiplo de 13 e 17. Mas todo número que é múltiplo comum de $13$ e $17$ é múltiplo do $mmc(13,17)$ que é $221$, conforme o teorema 2.2.

Logo, a próxima apresentação será no ano $2001 + 221 = 2222$. Vale observar que todas as próximas apresentações ocorrerão a cada $221$ anos.

As cigarras periódicas são curiosidades que só ocorrem na América do Norte e tem sido objeto de estudo pelos entomólogos por vários anos. Este exemplo e os demais

que virão a seguir podem ser encontrados em [5]. A curiosidade matemática fica maior quando percebemos que essas cigarras respeitam os ciclos de intervalos de 13 ou 17 anos, que são números primos. Esse fato é explicado pelo escritor Stephen Jay Gould contido na mesma referência (APUD Nachbin e Tabak, 1997, p. 38-39):

> Os predadores em potencial vivem em ciclos de 2 a 5 anos. Esses ciclos não originaram por causa das cigarras! Afinal, os predadores têm vários picos (populacionais) durante os anos de não-emergência das cigarras. Por exemplo, se as cigarras viessem à superfície a cada 15 anos, elas poderiam ser abatidas por um pico dos predadores. Como o seu ciclo é um primo muito grande, as chances de uma coincidência são mínimas. Ciclos de treze ou dezessete anos muito raramente vão coincidir com ciclos de poucos anos.

É preciso chamar a atenção que a escolha de números primos para definir os ciclos está ligada à indivisibilidade dos mesmos.

Caso as cigarras escolhessem outro primo, menor do que esses, os predadores poderiam retardar ou adiantar seus picos populacionais.

Outra consequência do período da cigarra ser longo é a enorme quantidade de cigarras em relação ao número de predadores. Este comportamento provoca uma estratégia de sobrevivência das espécies pela saciedade do predador. O objetivo é saciar a maior parte dos predadores nas primeiras horas de aparição e garantir a sobrevivência das demais cigarras, tornando possível a reprodução.

O problema das cigarras se torna realmente interessante quando supomos que nenhuma aparição simultânea das duas espécies seja conhecida. O exemplo a seguir apresenta um método para determinar a data em que duas espécies voltam a aparecer juntas a partir do conhecimento de cada espécie.

**Exemplo 5.2**

A cigarra Great Eastern Brood possui um ciclo de 17 anos, tendo sua última reprodução no ano de 2004. Já a cigarra Great Southern Brood fez sua última aparição no ano de 2011 e possui um ciclo de 13 anos. Qual será a próximo ano que ambas as espécies surgirão juntas?

**Solução:** Ao usarmos o pensamento do exemplo 5.1 percebemos que o mesmo se torna inconclusivo, pois não temos uma primeira data para iniciar o emparelhamento. Assim é necessário outro artifício para solucionarmos essa questão.

Seja $x$ o próximo ano em que ambas as espécies irão surgir simultaneamente. Pelo ciclo de cada uma das espécies podemos escrever as duas congruências abaixo:

$$x \equiv 2004 \ (mod\ 17)$$

$$x \equiv 2011 \ (mod\ 13)$$

Como $2004 = 17 \cdot 117 + 15$ e $2011 = 13 \cdot 154 + 9$, então:

$$x \equiv 15 \ (mod\ 17)$$

$$x \equiv 9 \ (mod\ 13)$$

Nossa primeira congruência afirma que $x$ deixa resto $15$ na divisão por 17, logo

$$x = 17y + 15, \text{com } y \in \mathbb{Z} \qquad \text{(I)}$$

Substituindo o valor $x$ na segunda congruência do sistema, obtemos:

$$17y + 15 \equiv 9 \ (mod\ 13)$$

Daí,

$$4y \equiv 7\ (mod\ 13)$$

Como $mdc(4,13) = 1$ (Veja o exercício 4.5 na página 39), o número $4$ possui inverso módulo $13$, ou seja, existe um inteiro $a$ tal que $4a \equiv 1\ (mod\ 13)$. Observando os múltiplos de 4, podemos afirmar que $a = 10$. Logo:

$$40y \equiv 70\ (mod\ 13)$$

$$y \equiv 5\ (mod\ 13)$$

Ou seja, $y = 13t + 5$, com $t \in \mathbb{Z}$. Substituindo o valor de $y$ em (I) temos que:

$$x = 17(13t + 5) + 15$$

$$x = 221t + 100$$

Como o exemplo pede um ano maior do que 2011, o valor de $t$ deve ser $9$, ou seja:

$$x = 221 \cdot 9 + 100 = 2089$$

A próxima aparição simultânea das espécies Eastern Brood e Southern Brood será no ano 2089.

Observe que: $2089 \equiv 15\ (mod\ 17)$ e $2089 \equiv 9\ (mod\ 13)$ satisfazem nossas condições iniciais.

**Exercício 5.3:** Resolver o sistema de congruências abaixo

$$x \equiv 2(mod\ 3)$$

$$x \equiv 1\ (mod\ 5)$$

$$x \equiv 4\ (mod\ 7)$$

**Solução:** Esquecendo a última equação por alguns instantes, podemos resolver o sistema formado pelas duas primeiras congruências, da mesma maneira que resolvemos o exemplo anterior.

A primeira congruência fornece

$$x = 3q_1 + 2$$

Substituindo essa equação na segunda congruência e somando 3 de ambos as lados obtemos

$$3q_1 \equiv 4\ (mod\ 5)$$

Multiplicando ambos os lados por $2$ e observando que $6 \equiv 1\ (mod\ 5)$ e $8 \equiv 3\ (mod\ 5)$,

$$q_1 \equiv 3\ (mod\ 5)$$

Logo, $q_1 = 5q_2 + 3$ e, portanto,

$$x = 3(5q_2 + 3) + 2 = 15q_2 + 11$$

Agora, basta substituirmos o valor de $x$ obtido acima na terceira congruência ainda não utilizada

$$15q_2 + 11 \equiv 4\ (mod\ 7)$$

Ou seja:

$$q_2 \equiv 0\ (mod\ 7)$$

Logo $q_2$ é da forma $7t$, com $t \in \mathbb{Z}$.

Finalmente obtemos

$$x = 15(7t) + 11$$

$$x = 105t + 11$$

que satisfaz todas as congruências dadas.

**Exercício 5.4:** Ao tentar formar grupos de trabalho numa turma, conclui-se que se os grupos tiverem 3 elementos restarão dois alunos de fora, se tiverem quatro ficará 1 de fora, mas ao formar grupos de 5 elementos, desde que o professor faça parte de um deles, não restará nenhum aluno sem grupo. Qual é o número mínimo de alunos que essa turma possui?

**Solução:** Suponha que nessa sala haja $a$ alunos, logo podemos formar o sistema de congruências:

$$a \equiv 2(mod\ 3)$$

$$a \equiv 1\ (mod\ 4)$$

$$a + 1 \equiv 0\ (mod\ 5)$$

Somando $1$ em ambos os lados da primeira congruência, obtemos $a + 1 \equiv 0\ (mod\ 3)$. Portanto $a + 1$ é múltiplo de $3$ e de $5$ (pela terceira congruência). Assim $a + 1$ é múltiplo de $15$. Logo $a = 15t - 1$, com $t \in \mathbb{Z}$. Substituindo na segunda congruência obtemos

$$15t - 1 \equiv 1\ (mod\ 4)$$

$$-t \equiv 2\ (mod\ 4)$$

Consequentemente

$$t = 4k + 2, \text{com } k \in \mathbb{Z}$$

Portanto

$$a = 15(4k + 2) - 1 = 60k + 29$$

Como estamos tratando de número mínimo de alunos, esse valor é alcançado com $k = 0$, ou seja, $29$ alunos.

**Exercício 5.3:** Três satélites passarão sobre o Vitória à noite. O primeiro à uma hora da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã. Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra; o segundo, 15 horas e, o terceiro, 19 horas. Determine quantas horas decorrerão, a partir da meia-noite, até que os três satélites passem ao mesmo tempo sobre Vitória.

**Solução:** Podemos escrever as informações acima como um sistema de congruências onde $x$ é o número de horas em que os três satélites passaram juntos sobre Vitória.

$$x \equiv 1 \ (mod\ 13)$$

$$x \equiv 4 \ (mod\ 15)$$

$$x \equiv 8 \ (mod\ 19)$$

Podemos resolver pelo método do Exercício 5.1, porém observe que somando $11$ em ambos os lados das duas últimas congruências, obtemos que $x + 11$ é múltiplo de $15$ e $19$, e logo $x + 11 = 15 \times 19t = 285t$, com $t \in \mathbb{Z}$.

Substituindo na primeira congruência obtemos

$$285t - 11 \equiv 1 \ (mod\ 13)$$

$$(22 \times 13 - 1)t \equiv -1 \ (mod\ 13)$$

Consequentemente,

$$t = 13k + 1, \text{ com } k \in \mathbb{Z}$$

Portanto,

$$x = 285(13k + 1) - 11 = 3705k + 274$$

Quando $k = 0$, obtemos $x = 274$. Assim, após 274 horas, ou seja, após 11 dias e 10 horas, os três satélites passarão simultaneamente por Vitória.

Após esses exemplos, o aluno deve perceber que tal Algoritmo só funcionou pois os números que representam os módulos das congruências são dois a dois primos entre si. Além disso, as soluções do sistema de congruências são números inteiros onde a diferença entre dois consecutivos é o produto dos módulos das congruências.

# 6. HORÁRIOS DE TORNEIOS

O ensino médio de uma escola quer preparar uma competição interclasse de futebol de salão, sendo que cada turma terá um time representante. O torneio será de um único turno, em que cada confronto entre dois times acontece uma única vez, e com pontos corridos, ou seja, cada time enfrentará todos os outros.

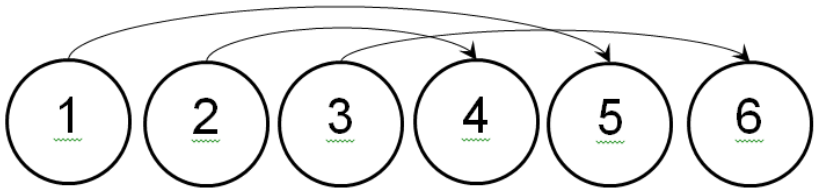
A dificuldade de se montar uma tabela de um campeonato é garantir o seguinte:

- O time oponente não é o próprio time.
- Times diferentes têm oponentes diferentes numa mesma rodada.
- O mesmo time em rodadas diferentes tem oponentes diferentes.

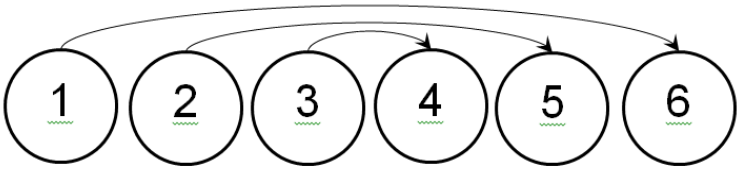
**Exemplo 6.1**

Suponha que a escola tenha seis times para disputar tal campeonato. Atribuiremos a cada time um número de 1 a 6.

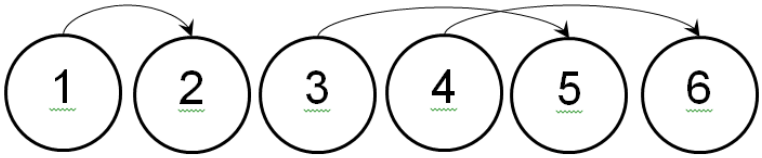
Na primeira rodada iremos definir os confrontos de forma que a soma dos números dos oponentes seja 6. Assim o time 1 enfrentará o time 5, o time 2 enfrentará o time 4. Porém, o time 3 seria seu próprio oponente e, para evitar isso, definimos o último jogo sendo o time 3 contra o time 6.



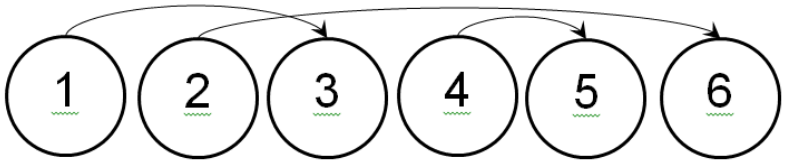

Já na segunda rodada, serão oponentes os times cuja soma seja 7. Assim o time 1 enfrenta o time 6. O time 2 enfrenta o time 5. Por fim, o time 3 enfrenta o time 4.



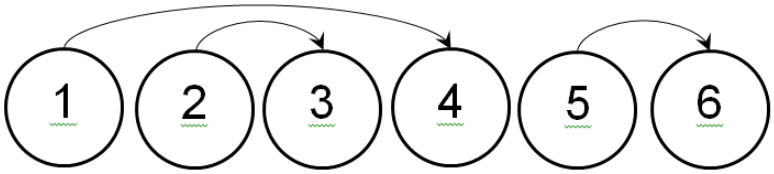

Para o terceira rodada queremos que a soma seja 8, ou ainda, um número que deixa resto 3 na divisão por 5. O esquema abaixo, mostra os combates:




Para a quarta rodada teremos:




Já na última rodada:




Observe que tal feito respeita as condições impostas acima.

Vamos assumir que existam $N$ classes de ensino médio. Devemos ficar atentos no caso de $N$ ser ímpar, pois assim a cada rodada um time diferente não deve jogar, mantendo a igualdade de descanso entre os participantes. Neste último caso, acrescentaremos um time fictício $B_0$ denominado Banco e tomamos a quantidade $N+1$ que, por sua vez, é par. Quando um time é escalado para jogar com o Banco significa que ele descansa nessa rodada. Feito isso, podemos supor que $N$ seja par. Vamos nomear os times pelos números $1, 2, 3, \cdots, N-1, N$.

Cada time irá jogar um total de $N-1$ partidas. Inicialmente, vamos supor que $1 \leq x \leq N-1$, isto é, $x \neq N$. Vamos denominar o oponente do time $x$ na rodada $r$ por $y_r$, determinado pela congruência:

$$x + y_r \equiv r \ (mod\ N-1)$$

Devemos verificar que cada time terá um oponente diferente numa mesma rodada. Note que:

$$x + y_r \equiv r \equiv x' + y_r \ (mod\ N-1)$$

implicando diretamente em:

$$x \equiv x' \ (mod\ N-1)$$

Dessa última congruência retiramos duas possibilidades:

- $x - x' \neq 0$ seja um múltiplo não nulo de $N-1$
- Ou $x - x' = 0$.

Como os possíveis valores de $x$ estão entre $1$ e $N-1$, a primeira opção é impossível, restando apenas $x = x'$.

Logo, times diferentes terão adversários diferentes em uma mesma rodada.

Devemos também evitar que o time $x$ seja igual ao seu adversário $y_r$, dessa forma, temos:

$$x + y_r \equiv x + x \equiv r\ (mod\ N-1)$$

$$2 \cdot x \equiv r\ (mod\ N-1)$$

Como $x$ está entre $1,2,\cdots,N-1$, esse fato só ocorre quando:

$$2 \cdot x \equiv r \equiv 2 \cdot x'(mod\ N-1)$$

$$2 \cdot (x - x') \equiv 0\ (mod\ (N-1)$$

Como determinamos inicialmente que $N$ será par, temos que:

$$x \equiv x'(mod\ N-1)$$

uma vez que $2$ é invertível módulo $N-1$, que por sua vez é ímpar. Dessa forma, a única solução da equação $2 \cdot x \equiv (r\ mod\ N-1)$ será:

$x = \frac{r}{2}$, quando $r$ for par,

$x = \frac{r+N-1}{2}$, quando $r$ for ímpar.

Para cada um desses casos, o seu adversário que satisfaz a equação $2 \cdot x \equiv r\ (mod\ N-1)$ será o time que recebeu o índice $N$.

Por fim, temos que mostrar que, em rodadas diferentes, teremos adversários diferentes para cada um dos times. Para o time $N$, teremos o caso específico informado acima. Assim, vamos supor que tem-se rodadas distintas, ou seja, $r \neq s$, de forma que o time adversário de $N$ será $x_0$ na rodada $r$ e $x_1$ na rodada $s$ que satisfaz:

$$2 \cdot x_1 \equiv s \ (mod\ N-1)$$

Como não podemos ter $x_0 = x_1$, temos:

$$2 \cdot x_0 \equiv 2 \cdot x_1 \equiv r \equiv s \ (mod\ N-1)$$

então $r = s$.

Vamos considerar os oponentes entre os times com índice $1,2,\cdots,N-1$. O time $x$ que é o oponente do time $N$ na rodada $r$ será definido por:

$$2 \cdot x \equiv r \ (mod\ N-1)$$

logo:

$$x + y_r \equiv r \ (mod\ N-1) \text{ e } x + y_s \equiv s \ (mod\ N-1)$$

Assim, se $r = s$, então $y_r = y_s$. Logo $y_r \neq y_s$

**Exercício 6.1:** Construa a tabela para $N = 8$ times.

A tabela abaixo mostra em qual rodada dois times se enfrentarão

| **Times** | **Times** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
|---|---|---|---|---|---|---|---|---|---|
| **1** | | | 3ª | 4ª | 5ª | 6ª | 7ª | 1ª | 2ª |
| **2** | | | | 5ª | 6ª | 7ª | 1ª | 2ª | 4ª |
| **3** | | | | | 7ª | 1ª | 2ª | 3ª | 6ª |

| | | | | | |
|---|---|---|---|---|---|
| **4** | | 2ª | 3ª | 4ª | 1ª |
| **5** | | | 4ª | 5ª | 3ª |
| **6** | | | | 6ª | 5ª |
| **7** | | | | | 7ª |

**Exercício 6.2:** Mostre que na segunda rodada os times $1, 2, \cdots, N$ jogaram com $N, N-1, \cdots, 2, 1$, respectivamente.

**Solução:** Observe que na segunda rodada teremos a seguinte congruência:

$$x + y_2 \equiv 2 \ (mod\ N-1)$$

é o mesmo que $x + y_2 - 2 \equiv 0 \ (mod\ N-1)$, ou seja $x + y_2 - 2$ é múltiplo de $N-1$. Em especial $x + y_2$, é igual a $N-1$, pois os valores máximos determinados aos times são $N$, e como $x \neq y_2$como já vimos na demonstração acima, tem-se:

$$x + y_2 - 2 < 2 \cdot (N-1).$$

Assim:

$$x + y_2 - 2 = N - 1$$

$$x + y_2 = N + 1$$

Essa última soma só é possível quando somamos os valores iniciais de $x$ com seus possíveis valores finais.

**Exercícios 6.3:** Por que o time $N-1$ sempre joga com o time $r$ na rodada $r$, exceto quando $r = N-1$?

**Solução:** Suponha $r \neq N-1$, observando a congruência: $N-1+y_r \equiv r\ (mod\ N-1)$ podemos reduzir para $y_r \equiv r\ (mod\ N-1)$. Logo, o adversário do time $N-1$ será o time $r$, quando esse não coincide com ele próprio.

# 7. SOBRE CALENDÁRIOS

## 7.1. Calendário Gregoriano

A necessidade de contar o tempo se deu por motivos como agricultura, religião e viagens marítimas, além da necessidade de recordar e de prever uma data.

Diversos calendários foram criados ao logo da história da humanidade, em sua maioria usando as seguintes subdivisões:

i. **Dia**: intervalo de tempo entre os períodos luminosos.
ii. **Semana:** período artificial de sete dias, difundido através da Mesopotâmia.
iii. **Ano:** período que a Terra gasta para fazer uma revolução completa em torno do Sol.

Esse último, conhecido como ano tropical, tem duração de 365,2422 dias terrestres, trazendo consigo algumas questões. O calendário romano inicialmente possuía 365 dias, iniciando no mês de março e finalizando no mês de fevereiro, onde este último possuía 30 dias. O primeiro dia de cada mês era denominado *calenda*.

Com a finalidade de corrigir a diferença entre os anos, o imperador Júlio César em 46 a.C., a partir do conselho do astrônomo Soségenes de Alexandria, decidiu que a cada 4 anos fevereiro teria duas vezes o dia 24, isto é, o sexto dia antes do fim do ano seria contado duas vezes. Daí a denominação de ano bissexto, erroneamente denominado pelos dois seis do número 366. Dessa forma, um ano no calendário juliano possuía:

$$365 + \frac{1}{4} = 365{,}25 \text{ dias}$$

tendo uma diferença de $-0{,}0078$ dias a cada ano em relação ao ano tropical, o que à primeira vista poderia ser irrisória. Consequentemente, a cada $128$ anos esse calendário atrasaria um dia em relação ao ano tropical. Esse atraso influenciou diretamente na data de início das estações climáticas e, portanto, em datas religiosas, como a Páscoa, que é celebrada no primeiro domingo de lua cheia após o equinócio de primavera no hemisfério norte.

Em 1582, aceitando proposta dos astrônomos Aloysius Lilius e Cristovão Clavius, o papa Gregório XIII autorizou uma mudança no calendário para corrigir a defasagem de 10 dias em relação à passagem da Terra pelo seu ponto vernal - o ponto da esfera celeste determinado pela posição do Sol quando este, movendo-se pela eclíptica, cruza o equador celeste, que normalmente ocorre no dia 20 ou 21 de março. Assim, os cidadãos católicos europeus foram dormir na noite de 4 de outubro de 1582 e acordaram em 15 de outubro do mesmo ano. Vale lembrar que alguns países, como a Rússia só acataram essa mudança no século XX.

Os anos bissextos tiveram suas regras alteradas para os anos múltiplos de 4, porém não múltiplos de 100 e além disso, anos múltiplos de 400 são bissextos. Dessa forma, um ano no calendário gregoriano possui:

$$365 + \frac{1}{4} - \frac{1}{100} + \frac{1}{400} = 365{,}2425 \text{ dias},$$

e será necessário corrigir os calendários apenas a cada 3334 anos aproximadamente. Ou seja, 4880 ou 4884 não terá um dia acrescido.

**Exercício 7.1:** Verifique quais anos abaixo são bissextos:

a) 1564

b) 1700

c) 2000

d) 2450

**Exercício 7.2**: Determine quantos anos bissextos houveram entre a independência do Brasil e a morte de Ayrton Senna.

**Solução:** Ou seja, quantos anos bissextos houve entre 1822 e 1994? Temos $1824 = 456 \times 4$ e $1992 = 498 \times 4$. Logo, houve $498 - 456 + 1 = 43$ anos múltiplos de 4. Nesse período, apenas o ano de 1900 foi múltiplo de 100 e logo, devemos descontar, uma vez que não foi bissexto. Assim, houveram 42 anos bissextos.

## 7.2. Determinação do dia da semana

Uma questão interessante é determinar o dia da semana de uma data no calendário gregoriano usando apenas os numerais que formam o dia, o mês e o ano. Para tanto, suponhamos que o ano tivesse apenas 364 dias e as semanas 7 dias. Assim, como 364 é múltiplo de 7, uma pessoa que nasceu numa segunda-feira sempre irá comemorar seu aniversário em uma segunda-feira. Portanto, seria simples descobrir a qual dia da semana está relacionado uma certa data, independentemente do ano dado.

Como

$$365 \equiv 1 \ (mod\ 7)$$

E em anos bissexto, temos:

$$366 \equiv 2 \ (mod\ 7)$$

Uma dificuldade que poderíamos encontrar é o fato de que o mês de março depende da duração de fevereiro para iniciar, e mesmo fevereiro, que possui durações

distintas conforme o ano, bissexto ou não. Para sanar essa dificuldade, vamos organizar nossos meses iniciando em março e terminando em fevereiro do ano seguinte (conforme o calendário juliano). Logo teremos a ordem:

| | |
|---|---|
| 1 Março | 7 Setembro |
| 2 Abril | 8 Outubro |
| 3 Maio | 9 Novembro |
| 4 Junho | 10 Dezembro |
| 5 Julho | 11 Janeiro |
| 6 Agosto | 12 Fevereiro |

Uma fórmula simples usando congruência para determinar o dia da semana de uma data, no formato $d/m/N$ onde $N = 100C + Y$, no calendário gregoriano é dada por:

$$W \equiv d + \left[\frac{13M - 1}{5}\right] + Y + \left[\frac{Y}{4}\right] + \left[\frac{C}{4}\right] - 2 \cdot C \ (mod\ 7)$$

onde $M$ é a ordem do mês $m$ apresentada na tabela acima. Na fórmula acima $[\frac{a}{b}]$ é igual ao quociente da divisão euclidiana de $a$ por $b$. Além disso, $W = 0$ corresponde a domingo, $W = 1$ segunda,..., $W = 6$ sábado.

**Exemplo 7.1** Em qual dia da semana o Brasil foi descoberto?

A data do descobrimento é 22 de abril de 1500. Logo

$$d = 22, M = 2, C = 15, Y = 0$$

Logo:

$$W \equiv 22 + 5 + 0 + 0 + 3 - 30 \equiv 0 \ (mod\ 7)$$

Logo, o Brasil foi descoberto em um domingo.

**Exemplo 7.2:** O brasileiro Rui Barbosa nasceu no dia 5 de novembro de 1849 em Salvador, Bahia. Em qual dia da semana nasceu Rui Barbosa?

Segundo a fórmula apresentada, temos:

$$d = 5, M = 9, C = 18 \, e \, Y = 49$$

Assim:

$$W \equiv 5 + [(13 \cdot 9 - 1)/5] + 49 + [49/4] + [18/4] - 2 \cdot 18 \, (mod \, 7)$$

Logo $W \equiv 57 \, (mod \, 7)$ e $W \equiv 1 \, (mod \, 7)$

Ou seja, Rui Barbosa nasceu em um segunda-feira.

**Demonstração:** Inicialmente vamos determinar o dia da semana do primeiro dia de março de um ano $N = 100 \cdot C + Y$, simbolizado por $d_N$. Assim, suponha que não existam anos bissextos e que saibamos em que dia da semana $d_{1600}$ caiu primeiro de março de 1600. Logo a congruência abaixo faz sentido:

$$d_N \equiv d_{1600} + (100 \cdot C + Y - 1600) \, (mod \, 7)$$

Como estamos lidando com anos bissextos, queremos descobrir quantos anos desse formato houve entre $N$ e 1600, assim:

$$\left[\frac{100C + Y - 1600}{4}\right] = 25C - 400 + \left[\frac{Y}{4}\right]$$

Porém essa quantidade ultrapassa o valor por causa dos anos múltiplos de 100 que não são anos bissextos. Logo devemos subtrair do total a quantidade:

$$C - 16$$

Por fim, devemos contar os múltiplos de 400, por serem bissextos:

$$\left[\frac{C - 16}{4}\right] = \left[\frac{C}{4}\right] - 4$$

Logo considerando todas as expressões e observando que $100 + 25 - 1 = 124 = 7 \times 18 - 2 \equiv -2\ (mod\ 7)$ e também que $1600 + 400 - 16 + 4 = 1988 = 7 \times 284 \equiv 0\ (mod\ 7)$, obtemos:

$$d_N \equiv d_{1600} - 2C + Y + \left[\frac{C}{4}\right] + \left[\frac{Y}{4}\right]\ (mod\ 7)$$

Ainda temos que determinar o valor de $d_{1600}$. Não obstante, sabemos, com um olhar rápido no calendário, que 01/03/2016 cairá em uma terça-feira. Assim:

$$C = 20, \qquad \left[\frac{C}{4}\right] = 4, \qquad Y = 16, \qquad \left[\frac{Y}{4}\right] = 5$$

Logo

$$2 \equiv d_{1600} - 2 \cdot 20 + 16 + \left[\frac{20}{4}\right] + \left[\frac{16}{4}\right]\ (mod\ 7)$$

$$2 \equiv d_{1600} - 40 + 16 + 5 + 4\ (mod\ 7)$$

$$2 \equiv d_{1600} - 15\ (mod\ 7)$$

$$17 \equiv d_{1600}\ (mod\ 7)$$

Temos que $d_{1600} = 3$.

Com isso podemos determinar o dia da semana do primeiro de março de qualquer ano $N$. Contudo queremos determinar quantos dias se passam de outra data específica do mesmo ano $N$ em relação ao primeiro de março. Observe que caso 1º

de março ocorra numa terça-feira, nesse mesmo ano o primeiro dia de abril irá ocorrer numa sexta-feira, uma vez que março possui 31 dias e:

$$31 \equiv 3\ (mod\ 7)$$

Já para o início de maio temos que levar em consideração a duração do mês de abril que possui 30 dias. Como $30 \equiv 2\ (mod\ 7)$, para uma data do mês de maio devemos levar em consideração o total acumulado, $2 + 3 = 5$ dias. Devemos levar em consideração os restos de todos os mês pela divisão por 7: 3, 2, 3, 2, 3, 3, 2, 3, 2, 3 e 3. A tabela abaixo mostra o total acumulado desses restos.

| | |
|---|---|
| I Março 0 | VII Setembro 16 |
| II Abril 3 | VIII Outubro 18 |
| III Maio 5 | IX Novembro 21 |
| IV Junho 8 | X Dezembro 23 |
| V Julho 10 | XI Janeiro 26 |
| VI Agosto 13 | XII Fevereiro 29 |

Para tanto, precisamos de uma expressão que origine os números da tabela acima. É surpreendente que existe uma expressão simples que fornece todos os números da tabela acima, que é dada por:

$$\left[\frac{13M - 1}{5}\right]$$

Unido a expressões teremos a expressão:

$$W \equiv d + \left[\frac{13M - 1}{5}\right] + Y + \left[\frac{Y}{4}\right] + \left[\frac{C}{4}\right] - 2 \cdot C\ (mod\ 7)$$

**Exercício 7.3**: O ano de 2014 começou em uma quarta-feira. Em que dia da semana caiu o último dia desse ano?

**Solução**: Vamos observar que uma semana completa, iniciando numa segunda-feira, terminará em um domingo. Analogamente uma semana completa iniciada numa quarta-feira irá terminar numa terça-feira. Quando observamos que:

$$365 = 364 + 1 = 7 \cdot 52 + 1,$$

Concluímos que 2014 terá 52 semanas completas, terminadas numa terça-feira. Assim, o último dia de 2014 também será numa quarta-feira.

**Exercício 7.4**: O ano de 2014 começou em uma quarta-feira. Em que dia da semana caiu o primeiro dia do ano de 2016?

**Solução:** Pelo Exercício 7.3, 2014 inicia e termina numa quarta-feira. O ano de 2015 inicia e termina numa quinta. Assim, 2016 iniciará numa sexta-feira.

**Exercício 7.5**: O ano de 2014 começou em uma quarta-feira. Em que dia da semana cairá o último dia do ano de 2016?

**Solução:** Pelo Exercício 7.4, conhecemos o primeiro dia do ano de 2016. Além disso, é fácil ver que 2016 é múltiplo de 4 e não de 100 e, logo é bissexto. Usando a mesma ideia do Pelo Exercício 7.3, concluímos que o último dia de 2016 será um domingo.

**Exercício 7.6**: Mostre que os dias 04/04, 06/06, 08/08, 10/10 e 12/12 sempre caem no mesmo dia da semana que o último dia de fevereiro.

**Solução:** Observe que março possui 31 dias, mais 4 dias de abril teremos um total de 35 dias corridos e como esse é múltiplo de 7, temos que o dia da semana de 4 de

abril coincide com o de 28 ou 29 de fevereiro. Seguindo o mesmo procedimento podemos mostrar para as demais datas.

## 8. CONCLUSÃO:

A partir do exposto, pode-se concluir que os conteúdos aqui relacionados – Números Inteiros e suas Propriedades, Mínimo Múltiplo comum, Máximo Divisor Comum e Divisão Euclidiana - são pouco explorados no contexto cotidiano em sala de aula, apesar de sua aplicação simples, e deveria ser mais utilizada pelos alunos, por ser possível percebê-los no mundo, em suas amplas utilidades.

Dessa forma, é visível que o trabalho aqui realizado pode ter seu conteúdo aplicado nas escolas, no dia-a-dia dos profissionais de educação, como fonte de pesquisa e inspiração para as atividades educacionais dos seus alunos, auxiliando na construção de Sequências Didáticas e Projetos Interdisciplinares - uma vez que são pertinentes para alinhar várias disciplinas, colaborando para uma visão ampliada do mundo, justamente o que a proposta de interdisciplinaridade busca e a que se refere.

Tal aplicação nos projetos pedagógicos em Matemática pode envolver Pesquisa Científica, Construção de Modelos, Teste de Hipótese e Resultados, pautados no mundo real e não só em situações abstratas, já tão utilizadas e gastas.

Essa nova abordagem interdisciplinar convida a uma releitura dos conteúdos impressos na atual forma de ensinar, cujo Livro Didático seria seu principal expoente, uma vez que padroniza e engessa os conteúdos, limitando a visão e criando a concepção de uma Matemática restrita e difícil. Ao desconstruir essa visão, podemos ampliar os conteúdos e convidar as pessoas, docentes e discentes, a enxergar a Matemática no cotidiano, de maneira crítica e eficiente, contribuindo não só com os resultados acadêmicos e pontuações, mas com a formação

consciente de cidadãos pensantes, críticos e capazes de questionar, fomentar e utilizar tais conteúdos em suas vidas.

## 9. REFERÊNCIAS:


1. FOMIN, Dmitri; GENKIN, Sergey e ITENBERG, Ilia. **Círculos Matemáticos** – **A Experiência Russa**. 1 ed. Rio de Janeiro: IMPA, 2010.
2. HEFEZ, A. **Elementos de Aritmética.** 2 ed. Rio de Janeiro: SBM, 2006.
3. LIMA NETO, Gastão Bierrenbach. **Notas de Aula – Versão 03/06/2013**. Instituto de Astronomia, Geofísica e Ciências Atmosféricas (IAG). Universidade de São Paulo (USP). Disponível em: http://www.astro.iag.usp.br/~gastao/astroposicao.html.
4. LOVÁSZ, L.; PELIKÁN, J. e VESZTERGOMBI, K. **Matemática Discreta.** 2 ed. Rio de Janeiro: SBM, 2013
5. NACHBIN, André; TABAK, Esteban. **Equações Diferenciais Em Modelagem Matemática Computacional**. 21º Colóquio Brasileiro de Matemática. Rio de Janeiro: IMPA, 1997
7. ORE, Oystein. **Invitation to Number Theory**. 1 ed. Yale University: 1967.
8. POLYA, George. **A Arte de Resolver Problemas**. Rio de Janeiro, RJ: Interciência, 2006.