UNIVERSIDADE FEDERAL DE ALFENAS

MANUEL MESSIAS DA SILVA

TEOREMA CHINÊS DO RESTO, MODELAGENS, SOLUÇÕES E APLICAÇÕES A LINGUAGEM WOLFRAM ALPHA

ALFENAS/MG

2025

MANUEL MESSIAS DA SILVA

TEOREMA CHINÊS DO RESTO, MODELAGENS, SOLUÇÕES E APLICAÇÕES A LINGUAGEM WOLFRAM ALPHA

Dissertação apresentada ao Programa de Pós-Graduação em Mestrado Profissional em Matemática - PROFMAT pela Universidade Federal de Alfenas-MG como parte dos requisitos para obtenção do título de Mestre em Matemática. Área de concentração: Matemática na Educação Básica.

Orientador: Prof. Dr. Marcelo Moreira da Silva

Coorientador: Prof. Dr. José Paulo Carvalho dos Santos

ALFENAS/MG

2025

Sistema de Bibliotecas da Universidade Federal de Alfenas
Biblioteca Central

Silva, Manuel Messias da.
Teorema Chinês do Resto, Modelagens, Soluções e Aplicações a Linguagem Wolfram Alpha / Manuel Messias da Silva. - Alfenas, MG, 2026.
119 f. : il. -

Orientador(a): Marcelo Moreira.
Dissertação (Mestrado em Matemática em Rede Nacional) - Universidade Federal de Alfenas, Alfenas, MG, 2026.
Bibliografia.

1. Teoria dos Números. 2. Teorema Chinês dos Restos. 3. Wolfram Alpha. 4. Modelagem Matemática. I. Moreira, Marcelo, orient. II. Título.

Ficha gerada automaticamente com dados fornecidos pelo autor.

MANUEL MESSIAS DA SILVA

TEOREMA CHINÊS DOS RESTOS: MODELAGENS, SOLUÇÕES E APLICAÇÕES À LINGUAGEM WOLFRAM ALPHA

O Presidente da banca examinadora abaixo assina a aprovação da Dissertação apresentada como parte dos requisitos para a obtenção do título de Mestre em Matemática pela Universidade Federal de Alfenas. Área de concentração: (51) Ciências e Humanidades para a Educação Básica

Aprovada em: 16 de MARÇO de 2026.

Prof. Dr. Marcelo Moreira da Silva

Presidente da Banca Examinadora

Instituição: Universidade Federal de Alfenas

Prof. Dr. Maurício Minchillo

Instituição: Instituto Federal Sul de Minas

Profa. Dr. José Carlos de Souza Júnior

Instituição: Universidade Federal de Alfenas

AGRADECIMENTOS

É inspirador ver como o apoio familiar, a dedicação dos professores motivadores e o empenho dos alunos podem transformar vidas e comunidades. A trajetória que eu tive descreve, desde os esforços de meus pais e de meus irmãos mais velhos que nos anos 80, privilegiaram os estudos meus e de meus irmãos que somos os mais novos da família até o meu ápice que foi a criação da Olimpíada de Matemática das Instituições Federais (OMIF) em 2017, o que evidencia o poder transformador da educação.

A OMIF, desde sua primeira edição em 2018, tem sido um marco significativo na rede federal de educação técnica de nível médio. Ela não apenas incentiva a excelência acadêmica, mas também promove a colaboração e o desenvolvimento pessoal entre estudantes e educadores de todo o país. O envolvimento de alunos como Bruno Januário, Lívia de Souza e Vinícius Lambardozi Nascimento nos grupos de estudos preparatórios visando olimpíadas de matemática no IFSULDEMINAS Campus Muzambinho entre 2014 e 2017 demonstra o impacto positivo dessas iniciativas. Esses grupos não só motivaram os discentes do campus, mas também inspiraram estudantes do ensino fundamental de escolas da região a buscar oportunidades no Campus Muzambinho, visando aprimorar seus conhecimentos e conquistar medalhas em diversas olimpíadas.

A colaboração entre professores dedicados, como Carlos Renato Soares, Guilherme Gonçalves Alves, Mauricio Minchillo, Renato Machado Pereira e eu, foi fundamental para a formulação e implementação da OMIF: Olimpíadas de Matemática das Instituições Federais. Essa iniciativa tem sido essencial para preparar os estudantes para os desafios dos vestibulares e concursos futuros, contribuindo para seu crescimento acadêmico e pessoal.

Que essa história continue a inspirar futuras gerações a valorizar a educação e a buscar sempre novos horizontes por meio de raciocínios lógicos e matemáticos como os encontrados na Teoria dos Números e em especial no Teorema Chinês dos Restos.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

RESUMO

No decorrer de minha experiência no magistério, especialmente nas séries do segundo ciclo do Ensino Fundamental, verifiquei a relevância de se promover, de forma sistemática, a assimilação dos conceitos e conteúdos básicos da Matemática, a fim de possibilitar que os estudantes, ao longo de sua trajetória escolar, desenvolvam-se de maneira consistente e em consonância com suas necessidades formativas. Por isso que neste trabalho, propõe-se o desenvolvimento de tópicos da Teoria dos Números, ramo da Matemática dedicado ao estudo das propriedades dos números inteiros, abrangendo conteúdos fundamentais como Números Primos, Divisibilidade, Equações Diofantinas, Congruências Modulares e o Teorema Chinês dos Restos. Trata-se de uma área central da Matemática, tanto por sua relevância teórica quanto por suas aplicações práticas, especialmente no campo da criptografia, elemento essencial à segurança digital contemporânea. Destaca-se, ainda, que os dois primeiros conteúdos mencionados Números Primos e Divisibilidade constituem base fundamental para o desenvolvimento cognitivo nas séries iniciais do segundo ciclo do Ensino Fundamental e ajudando em todo o desenvolvimento da Matemática em todos os níveis seguintes. Nesse contexto, busca-se evidenciar conceitos estruturantes dessa teoria, articulando-os em uma abordagem que culmina na Modelagem Matemática, com ênfase na aplicação ao sistema criptográfico RSA. Considerando o cenário atual, marcado pela crescente digitalização, pela validação eletrônica de dados e segurança de dados, explora-se também o uso do aplicativo Wolfram Alpha como ferramenta computacional de apoio à resolução, verificação e representação gráfica de resultados. Ademais, observa-se, de modo particular, a contribuição do Teorema Chinês dos Restos para a simplificação e otimização de cálculos envolvendo congruências, favorecendo a eficiência dos procedimentos e ampliando sua acessibilidade didática a professores e estudantes das séries finais do Ensino Fundamental e do Ensino Médio.

Palavras-chave: teoria dos números; teorema chinês do resto; wolfram alpha; modelagem matemática.

ABSTRACT

Throughout my experience in teaching, especially in the upper elementary grades (second cycle of Brazilian Ensino Fundamental), I have observed the relevance of systematically promoting the assimilation of fundamental concepts and contents of Mathematics, in order to enable students, throughout their school trajectory, to develop consistently and in accordance with their formative needs. For this reason, this work proposes the development of topics in Number Theory, a branch of Mathematics dedicated to the study of the properties of integers, covering fundamental content such as Prime Numbers, Divisibility, Diophantine Equations, Modular Congruences, and the Chinese Remainder Theorem. This is a central area of Mathematics, both for its theoretical relevance and its practical applications, especially in the field of cryptography, an essential element of contemporary digital security. It is also noteworthy that the first two mentioned contents — Prime Numbers and Divisibility — constitute a fundamental basis for cognitive development in the early years of the upper elementary grades and aid the entire development of Mathematics at all subsequent levels. In this context, we seek to highlight structuring concepts of this theory, articulating them in an approach that culminates in Mathematical Modeling, with an emphasis on the application to the RSA cryptosystem. Considering the current scenario, marked by increasing digitalization, electronic data validation, and data security, we also explore the use of the Wolfram Alpha application as a computational tool to support solving, verification, and graphical representation of results. Furthermore, we particularly observe the contribution of the Chinese Remainder Theorem to the simplification and optimization of calculations involving congruences, favoring the efficiency of procedures and expanding its didactic accessibility to teachers and students in the final years of elementary school and high school.

Keywords: number theory; chinese remainder theorem; wolfram alpha; mathematical modeling.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A temática deste trabalho se relaciona com o Teorema Chinês dos Restos, este teorema se aplica no caso de determinar um certo número de tal forma que na divisão dele por outros números ele deixa certos restos desde que esses outros números sejam primos entre si dois a dois. Esse algoritmo matemático é atribuído primeiramente ao matemático chinês Sun Tzu Suan Ching , tendo uma de suas primeiras aparições no "Manual de Aritmética", do mestre Sun. O Teorema Chinês dos Restos teve sua origem em aplicações práticas ao longo da história, como indicam relatos sobre os generais chineses na antiguidade. Estes líderes militares utilizavam métodos criativos para calcular suas perdas após uma batalha. Uma estratégia comum envolvia organizar as tropas sobreviventes em formações específicas e contar quantas formações completas poderiam ser formadas. Esse método eficiente permitia estimar o número de tropas remanescentes. Por exemplo, se um general quisesse determinar quantos soldados sobreviveram a uma batalha, poderia ordenar que se alinhassem em fileiras com um número específico de soldados não alocados para formação completa. Um caso hipotético envolve um general chinês com 1700 tropas no início da batalha. Ao final, ele comandava que se alinhassem de 5 em 5, resultando em 3 soldados não alocados; depois de 6 em 6, gerando 4 soldados não utilizados; e por último de 7 em 7, deixando 5 soldados sem formação completa. A pergunta final era: quantas tropas restaram afinal? Embora não exista evidência definitiva que confirme, é provável que problemas semelhantes tenham ocorrido na China antiga ou em outras civilizações.

O objetivo deste trabalho é o desenvolver uma sequência didática que apresente modelagem com Criptografia RSA com o uso do Teorema Chinês dos Restos e um aplicativo computacional para alunos da Educação Básica, em especial aos dos anos finais Ciclo Dois do Ensino Fundamental e Ensino Médio. Visto que, o Teorema Chinês dos Restos está relacionado com vários conteúdos matemáticos da BNCC, como por exemplo divisibilidade, multiplicidade, divisões com restos, números primos e operações com números inteiros.

A BNCC apresenta os conteúdos básicos a serem trabalhados. Indicando quais são as habilidades e competências (gerais e específicas), as habilidades e as aprendizagens essenciais que todos os alunos devem desenvolver durante cada etapa da educação básica – Ensino Fundamental, como por exemplo, classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade. A BNCC também determina que essas competências, habilidades e conteúdos devem ser os mesmos, independentemente de

onde as crianças, os adolescentes e os jovens moram ou estudam. A Base não deve ser vista como um currículo, mas como um conjunto de orientações que irá nortear as equipes pedagógicas na elaboração dos currículos locais. Esse documento deve ser seguido tanto por escolas públicas quanto particulares.

As aplicações da BNCC não devem limitar a só uma maneira de apresentação com coerência do começo, meio e fim. Por isso, vejo necessário que a escola mostre resoluções diferentes e que tenham um mesmo objetivo e que ambas apresentem soluções corretas de uma mesma questão. No livro "Na vida dez e na escola zero" (Carraher; Carraher; Schliemann, 1988), mostram exatamente a discrepância que acontece com as crianças que conseguem fazer muitos cálculos do seu dia-a-dia, vendendo os seus objetos nas feiras livres, mas que não os reproduzem no papel com os algoritmos. Por isso aproveitarmos os conhecimentos que os alunos já possuem dos seus ambientes de convívio e valorizar os raciocínios dos estudantes na formalização matemática, o que pode tanto facilitar seus entendimentos e auxiliá-los na compreensão da aplicação e ainda observarem pontos de vistas diferentes. Assim sendo escolhi a Teoria dos Números com foco principal no Teorema Chinês dos Restos e apresentações de soluções com um aplicativo computacional para apresentar uma sequência didática sobre uma modelagem sobre criptografia.

Este trabalho busca dar suporte para os professores e alunos que visam aprimorar seus estudos e pesquisas posteriores nesse conteúdo.

1.1 CONTEXTO HISTÓRICO DO TEOREMA CHINÊS DOS RESTOS

O teorema é atribuído primeiramente ao matemático chinês *Sun Tzu Suan Ching*, tendo uma de suas primeiras aparições no "Manual de aritmética do mestre Sun",[1] um livro chinês que data de 287 d.C. a 473 d.C. Ele foi desenvolvido simultaneamente por gregos e chineses com o intuito de resolver alguns problemas relativos à astronomia. Por um pouco sobre a cronologia seguem alguns personagens em linha do tempo que fizeram trabalhos muito importantes para a Aritmética:

A afirmação mais antiga conhecida do Teorema Chinês dos Restos apresentada como um problema numérico, aparece no livro do século III, Sunzi Suanjing, escrito pelo matemático chinês Sunzi. "Há certas coisas cujo número é desconhecido. Se contá-los por três, restamos dois; aos cinco, temos três sobrando, e aos setes, sobram dois. Quantas coisas existem?" Moder-

Tabela 1 – Principais estudiosos da Teoria dos Números

Matemáticos	**Época**	**Legado**
Pitágoras	569 a 500 a.C.	Ternas Pitagóricas.
Euclides	350 a.C.	Formalização e utilização do algoritmo.
Diofanto	250 d.C.	Soluções de equações indeterminadas com coeficientes inteiros.
Sun	entre 287d.C à 473 d.C.	Análise de contagem de restos em divisões.
Fermat	1661 a 1665	Pequeno Teorema de Fermat.
Euler	1707 a 1783	Teorema de Euler
Gauss	1777 a 1885	Lema de Gauss.
Direchilet	1805 a 1889	Princípio das Casas dos Pombos.

Fonte: Do autor(a)

namente para responder a essa pergunta, deve-se resolver o seguinte sistema de congruências:

$$x \equiv 2 \mod 3$$

$$x \equiv 3 \mod 5$$

$$x \equiv 2 \mod 7$$

Mas para chegar a esta solução há vários procedimentos a serem realizados. Por isso que tais assuntos da forma em que estão aqui sendo tratados neste trabalho de conclusão de curso, deverá servir de apoio para professores e alunos que buscam material suplementares para resolução de problemas.

2 MODELAGEM MATEMÁTICA E RECURSO COMPUTACIONAL

A modelagem matemática é uma estratégia que visa compreender e explicar fenômenos do mundo real por meio da construção de modelos. Esse processo envolve a identificação de exemplos representativos, a previsão de cenários e a aplicação de cálculos e projeções baseados em variáveis, aproximando-se da realidade. Embora os modelos não reproduzam a realidade de forma fiel, fornecem uma visão aproximada que possibilita o entendimento de situações complexas, com o objetivo de minimizar prejuízos e maximizar benefícios.

O processo de modelagem consiste em formular hipóteses que permitam uma compreensão quantitativa de fenômenos reais. Por meio do uso criterioso de dados e da definição de prioridades, a modelagem estimula ideias e experiências, engajando o estudante em sua própria aprendizagem ao demonstrar como a matemática se aplica ao cotidiano.

Na educação matemática, a modelagem valoriza a capacidade dos alunos de desenvolverem, avaliarem e aplicarem modelos matemáticos em diferentes contextos. A reflexão sobre aspectos da realidade leva à seleção de argumentos essenciais, que são formalizados em modelos matemáticos capazes de contemplar as relações envolvidas.

O ponto inicial da modelagem é a coleta de dados experimentais, obtidos de fontes diversas, com destaque para a internet como recurso inicial, complementado por outras fontes à medida que o modelo é refinado. O refinamento, por sua vez, é o núcleo do processo, exigindo conhecimento tanto da matemática quanto da área específica do fenômeno em análise. Assim, a modelagem matemática alia teoria e prática, motivando os estudantes a compreenderem e transformarem a realidade que os cerca.

2.1 RESOLUÇÃO DE PROBLEMAS

A resolução de problemas distingue-se da aplicação de técnicas específicas ao enfatizar o processo de pensamento, e não apenas os resultados.

- Técnica: Refere-se a um procedimento operacional estruturado em passos, aplicado para alcançar uma meta específica, como a resolução de exercícios ou a execução de cálculos matemáticos (ex.: fatoração de números primos);

- Método: Consiste em um percurso reflexivo e organizado que guia a resolução de um problema, demandando pensamento crítico e análise de possibilidades.

Na resolução de problemas, o conhecimento é tratado como um processo contínuo, construído ao longo da vida. O objetivo principal não é a obtenção imediata de resultados, mas a qualidade do entendimento desenvolvido por meio de uma postura investigativa e reflexiva.

O ponto de partida é a interpretação do enunciado, identificando dados e relações. O professor atua como mediador, incentivando a busca por soluções, a análise de hipóteses e a reflexão sobre os resultados. Esse processo fomenta a autonomia do aluno, que aprende a avaliar soluções e justificar escolhas. Além disso, o erro é valorizado como oportunidade de aprendizado.

Procedimentos recomendados incluem:

1. Leitura e interpretação cuidadosa do enunciado;
2. Estímulo à análise conjunta entre professores e estudantes;
3. Desenvolvimento de estratégias de resolução, análise de hipóteses e verificação de resultados.

2.1.1 Diferença entre Problemas e Exercícios

A diferenciação entre problemas e exercícios é essencial no ensino da matemática:

- Problema: Envolve situações abertas, que podem ter várias ou nenhuma solução. Visa engajar o aluno no processo de busca, desenvolvimento de raciocínio e reflexão sobre possibilidades. Os dados geralmente não estão explícitos, demandando investigação e levantamento de informações;

- Exercício: Baseia-se na aplicação de conhecimentos prévios, técnicas e fórmulas já aprendidas, com um único caminho de resolução. O foco está no procedimento, e não na criação de estratégias.

Enquanto os problemas promovem a construção de raciocínio crítico, os exercícios reforçam habilidades específicas. Ambos são importantes, mas devem ser planejados com base nos objetivos de aprendizagem e no nível cognitivo dos estudantes.

2.2 SEQUÊNCIA DIDÁTICA

A sequência didática é definida como um conjunto ordenado e estruturado de atividades planejadas para atingir objetivos educacionais. Ela deve ser concebida de forma a promover a progressão gradual das capacidades dos estudantes, partindo do conhecimento prévio e aumentando a complexidade em etapas.

Para ser eficaz, uma sequência didática deve apresentar:

- Conexão entre as atividades e os objetivos propostos;

- Planejamento detalhado e dinâmico, alinhado às necessidades dos estudantes;

- Intervenções pedagógicas que estimulem o aprendizado ativo e a autonomia dos alunos.

Por meio da sequência didática, o professor conduz o processo de ensino-aprendizagem de maneira estruturada, ampliando as habilidades dos estudantes e favorecendo a construção de conhecimento significativo.

3 LINGUAGEM WOLFRAM ALPHA

O Wolfram Alpha é chamado de *computational knowledge engine* (motor de conhecimento computacional), pois, em vez de apenas buscar páginas na internet, ele processa dados e conhecimentos estruturados para gerar respostas computadas. Não se trata de um buscador comum de repostas, pois ele faz cálculos, interpreta dados e gera respostas. A sua utilidade está em vários campos como por exemplo:

1. Matemática: resolução de equações, integrais, derivadas, estatística etc.
2. Ciências:
    (a) Química: estruturas moleculares.
    (b) Física: unidades e fórmulas.
    (c) Biologia: dados sobre organismos.
3. Engenharia: cálculos elétricos, mecânicos e simbólicos.
4. Finanças e economia: análise de dados e cálculos financeiros.
5. Computação: manipulação de imagens, gráficos e programação.

Os itens acima podem nos indicar o seu uso educacional mo ensino médio, certos conceitos matemáticos podem ser mais facilmente compreendidos quando os alunos têm a oportunidade de interagir e manipular conhecimentos com o apoio de tecnologias apropriadas. É sempre bom lembrarmos que o uso de ferramentas tecnológicas não deve substituir os métodos tradicionais — como cálculos feitos com papel e lápis —, mas sim se integrar de maneira equilibrada a outros métodos, incluindo o cálculo mental. É fundamental que os alunos estejam preparados para interagir de forma crítica e inteligente com as ferramentas tecnológicas disponíveis.

Com os avanços tecnológicos, torna-se cada vez mais necessário que os estudantes tenham contato e saibam utilizar, de maneira correta e crítica, as novas tecnologias que estão cada vez mais acessíveis no dia a dia. Essas ferramentas oferecem a professores e alunos novas formas de explorar conceitos centrais da matemática, especialmente nas áreas de funções, geometria analítica e álgebra, tanto no ensino médio quanto no universitário.

3.1 HISTÓRIA DO WOLFRAM ALPHA

A história do Wolfram Alpha está diretamente ligada ao trabalho do cientista Stephen Wolfram, que idealizou um motor de conhecimento capaz de calcular respostas a partir de dados estruturados. Lançado em 2009, o Wolfram Alpha se diferencia dos motores de busca tradicionais, que apenas fornecem listas de páginas da web, ao oferecer respostas calculadas e detalhadas.

3.1.1 Origem e desenvolvimento

A trajetória começa com a fundação da Wolfram Research por Stephen Wolfram em 1987. A empresa ficou conhecida pelo desenvolvimento do Mathematica, uma plataforma de computação técnica amplamente utilizada em universidades e centros de pesquisa. O Wolfram Alpha foi construído sobre a tecnologia e a linguagem do Mathematica, o que lhe deu a capacidade de realizar cálculos complexos. A ideia de tornar o conhecimento do mundo computável era uma visão de longa data de Stephen Wolfram, concretizada com o lançamento do projeto. Após uma transmissão ao vivo em 15 de maio de 2009, o serviço foi lançado oficialmente em 18 de maio de 2009. O início foi marcado por grande tráfego, chegando a gerar sobrecargas. Sua proposta inovadora de fornecer respostas diretas em vez de links fez do Wolfram Alpha um pioneiro na busca semântica.

3.1.2 Evolução e expansões

- 2012: Lançamento do Wolfram Alpha Pro, versão paga com recursos adicionais, como soluções passo a passo, upload de arquivos e personalização de gráficos.
- 2014: Apresentação da Wolfram Language, linguagem de programação que sustenta o Mathematica e o Wolfram Alpha, tornando-se disponível para um público mais amplo.

3.1.3 Utilização e impacto

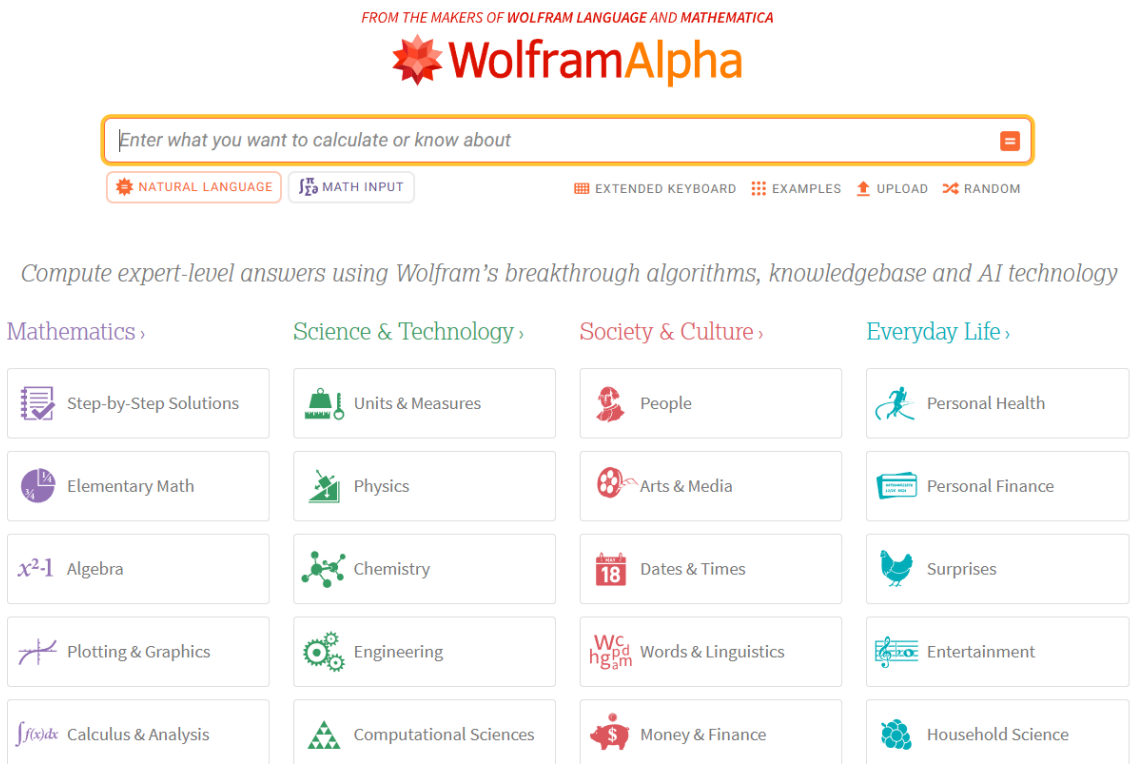
Desde então, o Wolfram Alpha tem sido amplamente utilizado por estudantes, profissionais e pesquisadores em áreas como matemática, física, engenharia e estatística, além de explo-

ração de dados computacionais. Ele compila dados de diversas fontes acadêmicas e comerciais, como o The World Factbook (CIA) e a Dow Jones, e utiliza processamento de linguagem natural (PLN) para compreender consultas dos usuários. A partir delas, aplica uma vasta biblioteca de algoritmos para gerar respostas detalhadas, incluindo fatos, gráficos e visualizações.

3.2 TELAS DE USO

No navegador do seu computador, digitamos https://www.wolframalpha.com/ e obtemos a tela principal do Wolfram Alpha que está a seguir. Vale também lembrar que dependendo do navegador que usarmos podemos traduzir a página.

Figura 1 – Tela Principal



A primeira página do site Wolfram Alpha é extensa. Tem mais informações rolando a página para baixo, como podemos ver na próxima figura:

Observamos tópicos de vários assuntos. Olhando a coluna da Mathematics (Tradução: Matemática) na cor roxa, onde é a primeira coluna de conteúdos, temos a última opção chamada *More Topics* (Tradução: Mais Tópicos). Quando clicamos em *More Topics*, aparece a tela com vários conteúdos de Matemática. Esta página é muito extensa. Por isso ela foi dividida em quatro telas na sequência.

Figura 2 – Tela complementar da primeira página

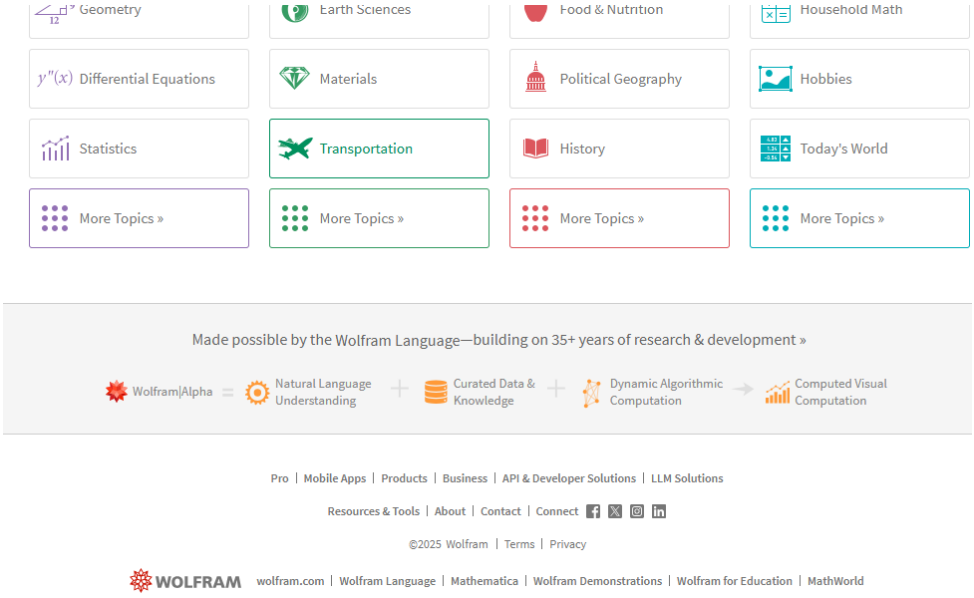


Figura 3 – Parte Dois da Tela de Matemática

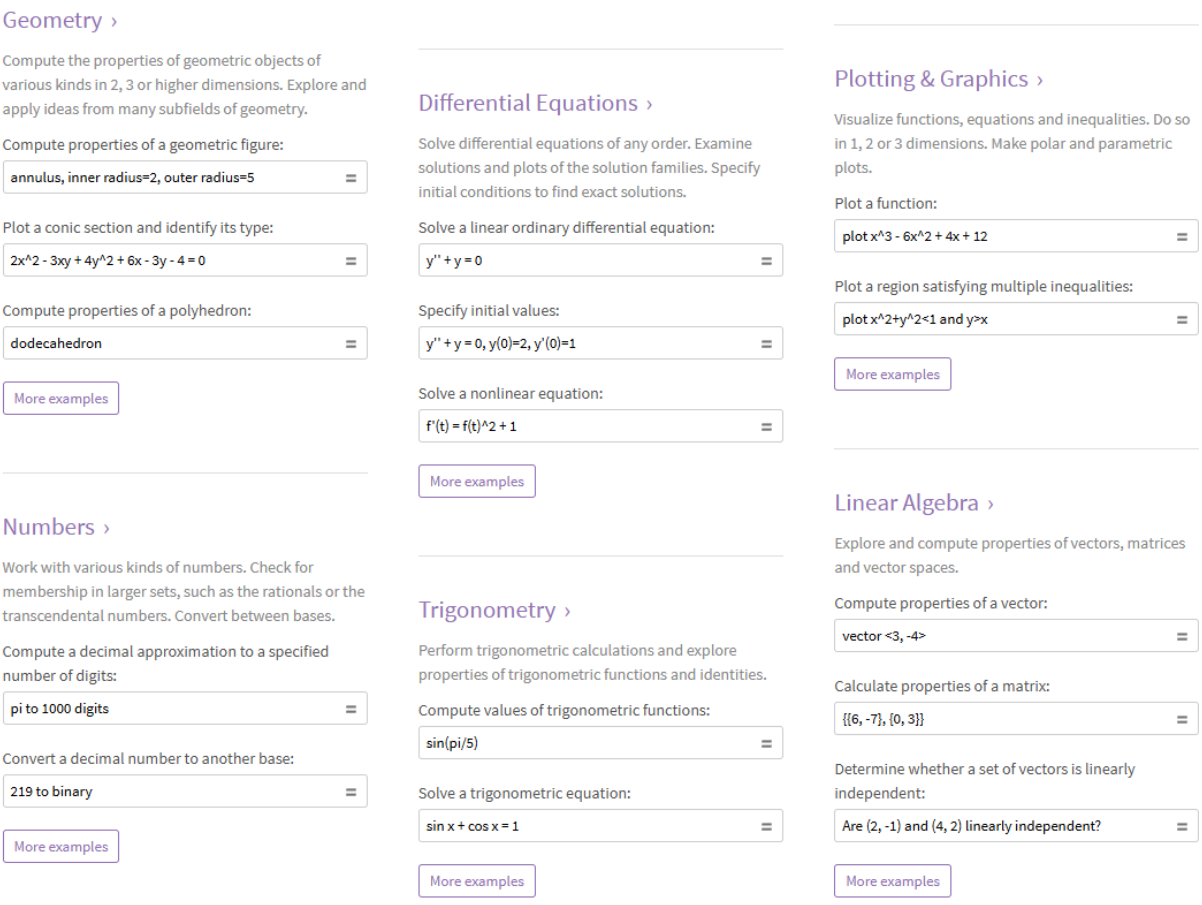


Figura 4 – Parte Três da Tela de Matemática

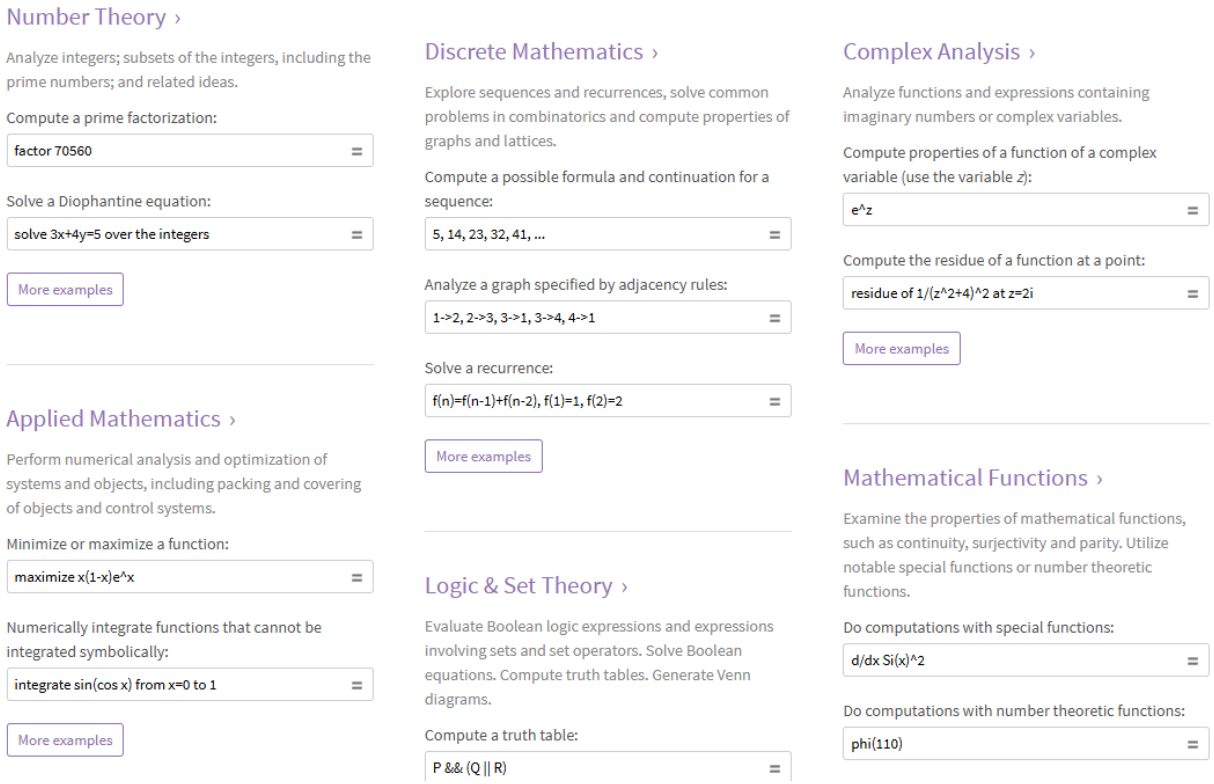
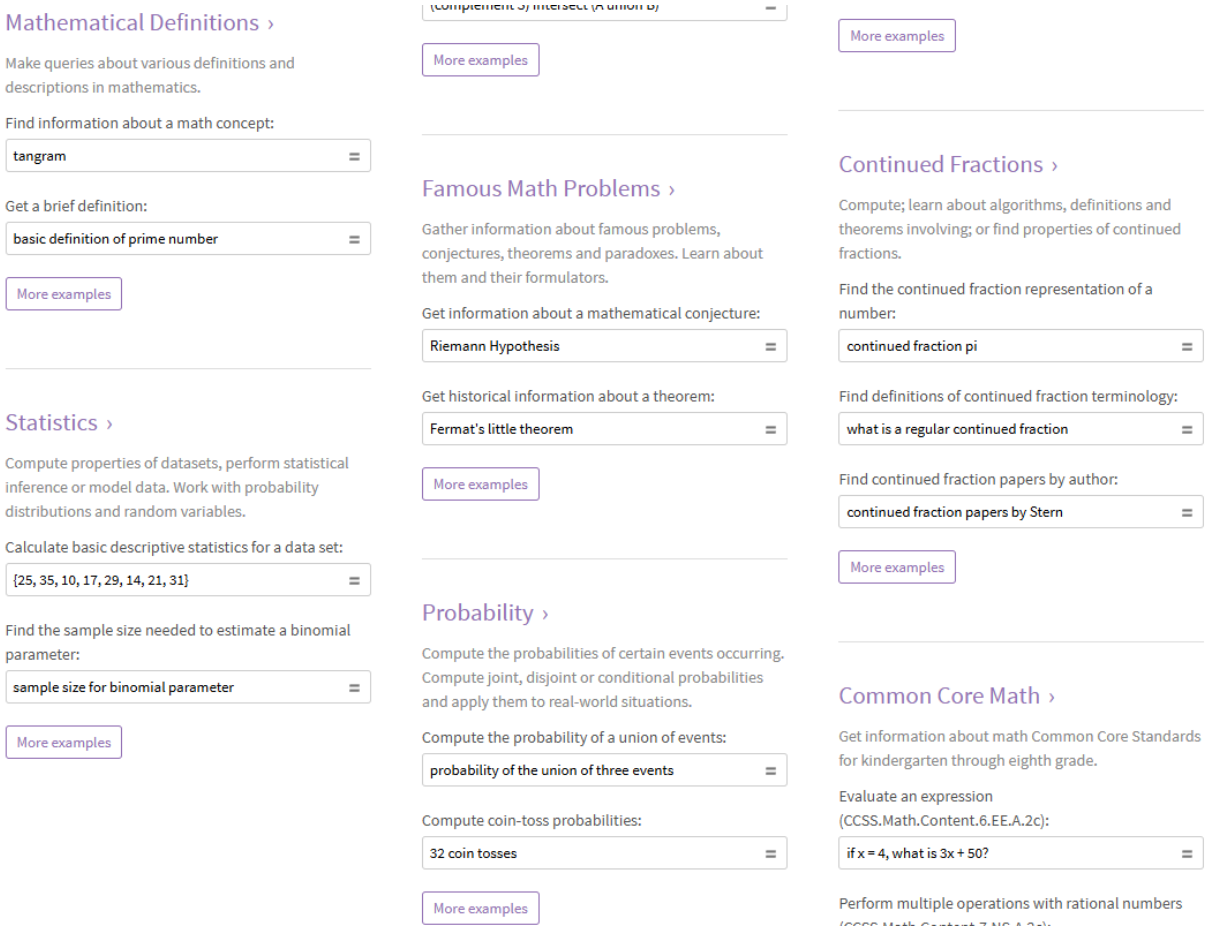


Figura 5 – Parte Quatro da Tela de Matemática



Nessa seção *Mathematics*, clicando no recurso *Number Theory*, apresenta a seguinte tela:

Figura 6 – Parte Um de Teoria dos Números

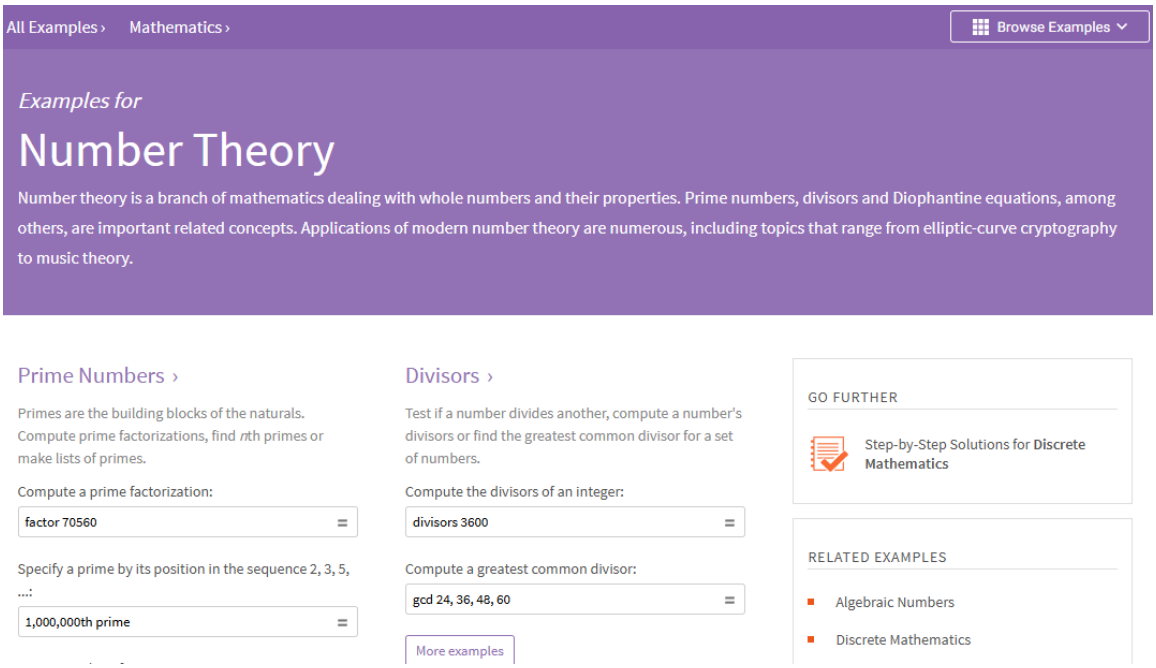
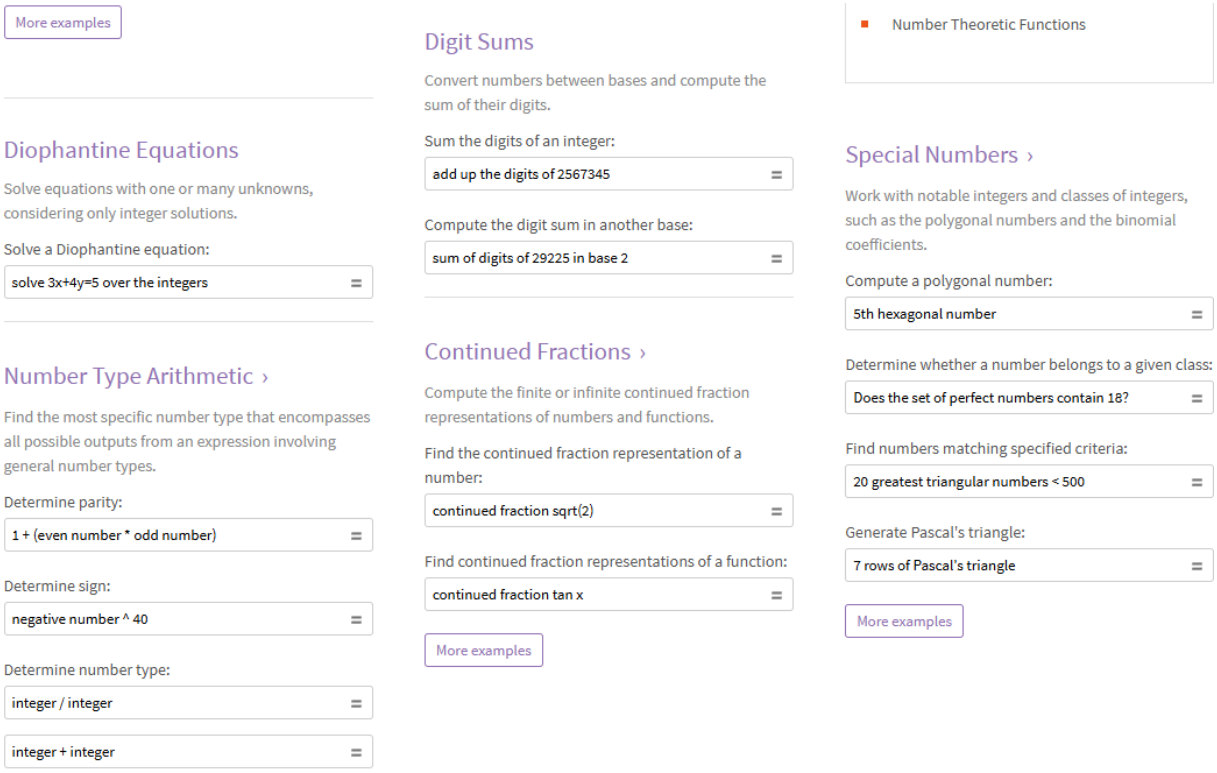


Figura 7 – Parte Dois de Teoria dos Números



Desvendando a potencialidade do Wolfram Alpha, podemos navegar ainda mais na área. Agora, dentro do *Number Theory*, exatamente no assunto *Diophantine Equations*, clicando no comando *solve* $3x+4y=5$ *over the integers*:

Figura 8 – Parte Um do Comando Solve em Equações Diofantinas

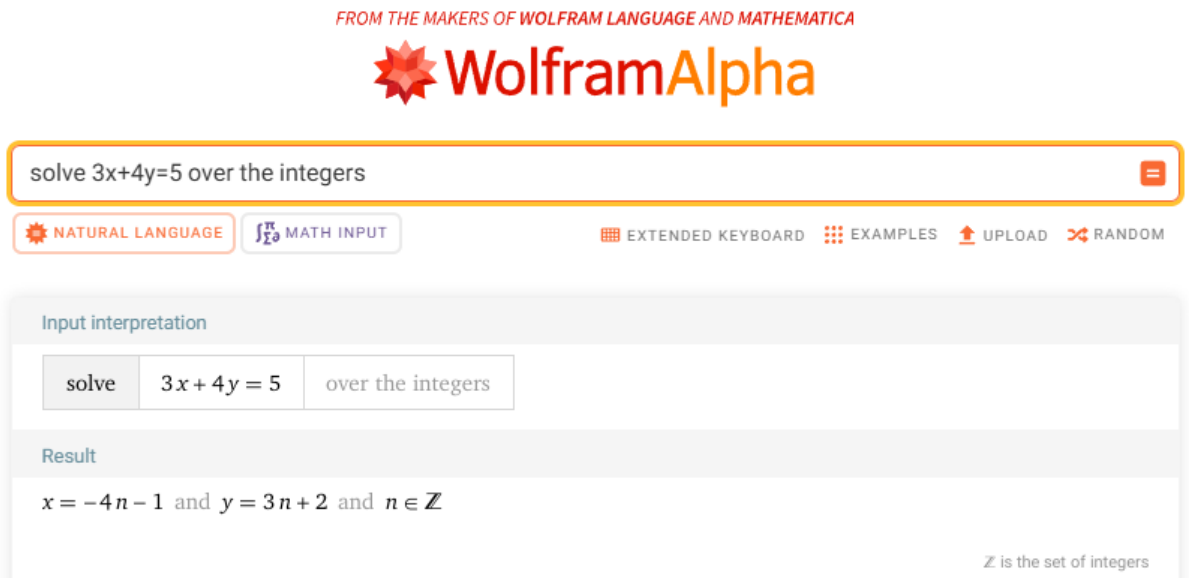
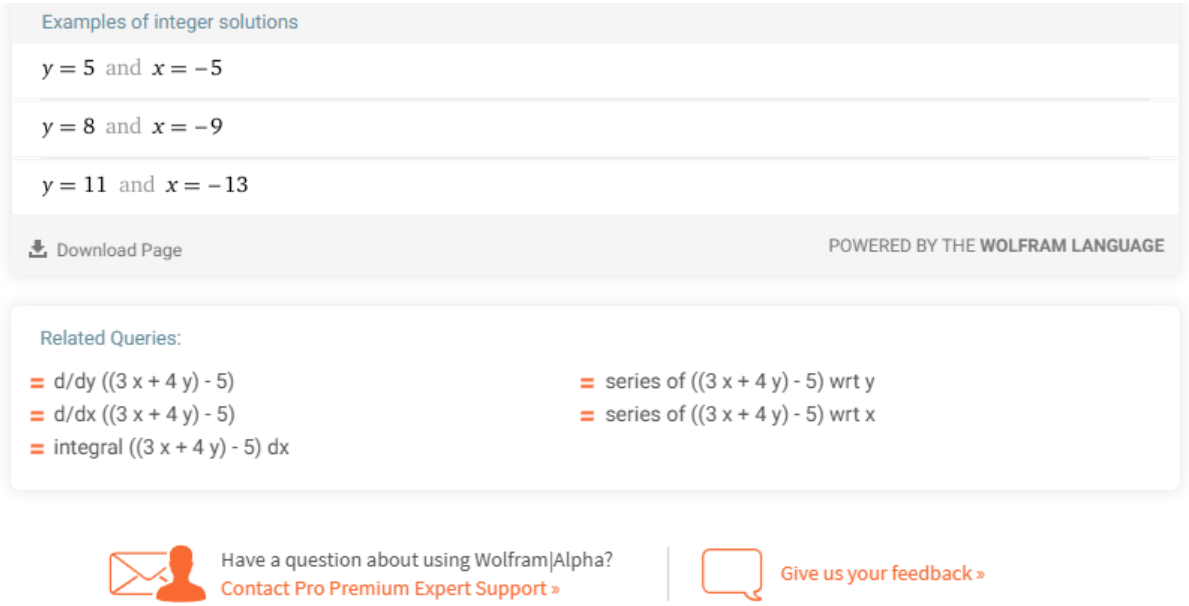


Figura 9 – Parte Dois do Comando Solve em Equações Diofantinas



4 CONCEITOS BÁSICOS DE TEORIA DOS NÚMEROS

A Teoria dos Números é o ramo fascinante da Matemática em que estudamos os números inteiros, na qual nos deparamos com raciocínios elegantes e aplicações surpreendentes. Alguns dos assuntos são nossos conhecidos de longa data, pois trataremos das operações de adição e multiplicação e resoluções de problemas com o uso de equações. Esses conceitos são a base para estudos mais avançados em matemática e têm aplicações em diversas áreas, como criptografia, computação e análise de dados e como sistemas de segurança, como RSA. Poderíamos ainda destacar que nela tratamos dos conceitos como divisibilidade, congruências e suas aplicações.

4.1 DIVISIBILIDADE

Dados dois números inteiros a e b diremos que a divide b, escrevendo $a|b$, quando existir $q \in \mathbb{Z}$ tal que $b = qa$. Neste caso a é divisor ou fator de b ou ainda, que b é um múltiplo de a ou que b é divisível por a. A notação $a \nmid b$ significa a não divide b, ou seja, diremos que não existe q tal que $b = aq$.

Proposição 1 (Propriedades da Divisibilidade)**.** *Quaisquer que sejam os inteiros a, b, c e d, tem-se:*

i) Então $a|a$ e $a|-a$;

ii) Se $a|1$ então $a = 1$ ou $a = -1$;

iii) Se $a|b$ e $c|d$ então $ac|bd$;

iv) Se $a|b$ e $b|c$ então $a|c$;

v) Se $a|b$ e $b|a$ então $a = +b$ ou $a = -b$;

vi) Se $a|b$ com b diferente de zero então, $|a| \leq |b|$;

vii) Se $a|b$ e $a|c$ então para quaisquer q_1, q_2 inteiros temos $a|bq_1 + cq_2$.

Demonstração. Seguem as demonstrações das propriedades:

i) Sabendo que existe as igualdades: $a = a1$ e $-a = -a1 = -1(a1) = a((-1)1) = a(-1)$, então podemos admitir que, $a|a$ e $a|-a$.

ii) Se $a|1$ então existe q inteiro tal que $1 = aq$. Como a, q são inteiros resulta que: $a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$. Por isso, vemos que $a = 1$ ou $a = -1$.

iii) Se $a|b$ e $c|d$ então existem x e y inteiros, tais que: $b = ax$ e $d = cy$. Por isso, $bd = (ax)(cy) = ac(xy)$, ou seja, $ac|bd$.

iv) Se $a|b$ e $b|c$ então existem inteiros x e y tais que: $b = ax$ e $c = by$. E ainda temos que $c = (ax)y = a(xy)$ na qual xy, também é inteiro. Por isso vemos que $a|c$.

v) Se $a|b$ e $b|a$ então existem inteiros, x e y tais que: $b = ax$ e $a = by$ então $a = (ax)y = a(xy)$ na qual xy também é inteiro. Por isso, vemos que $a|a$ e $xy = 1$, ou seja, $x = 1$ e $y = 1$, ou $x = -1$ e $y = -1$. Logo $a = +b$ ou $a = -b$.

vi) Se $a|b$ com b diferente de zero então existe q inteiro tal que $b = aq$. Aplicando o módulo nos dois membros da igualdade: $|b| = |a||q|$. Como b é diferente de zero então q é diferente de zero. Podemos analisar também que $1 \leq |q|$. Multiplicando por módulo de a que é positivo obtemos $|a| \leq |a||q| = |b|$ então $|a| \leq |b|$.

vii) Se $a|b$ e $a|c$ então existem x, y inteiros tais que $b = ax$ e $c = ay$. Multiplicando cada uma das equações acima por q_1 e por q_2, respectivamente. E depois, somando as equações membro a membro teremos: $bq_1 + cq_2 = (ax)q_1 + (ay)q_2 = a(xq_1 + yq_2)$. Então provamos que $a|bq_1 + cq_2$.

□

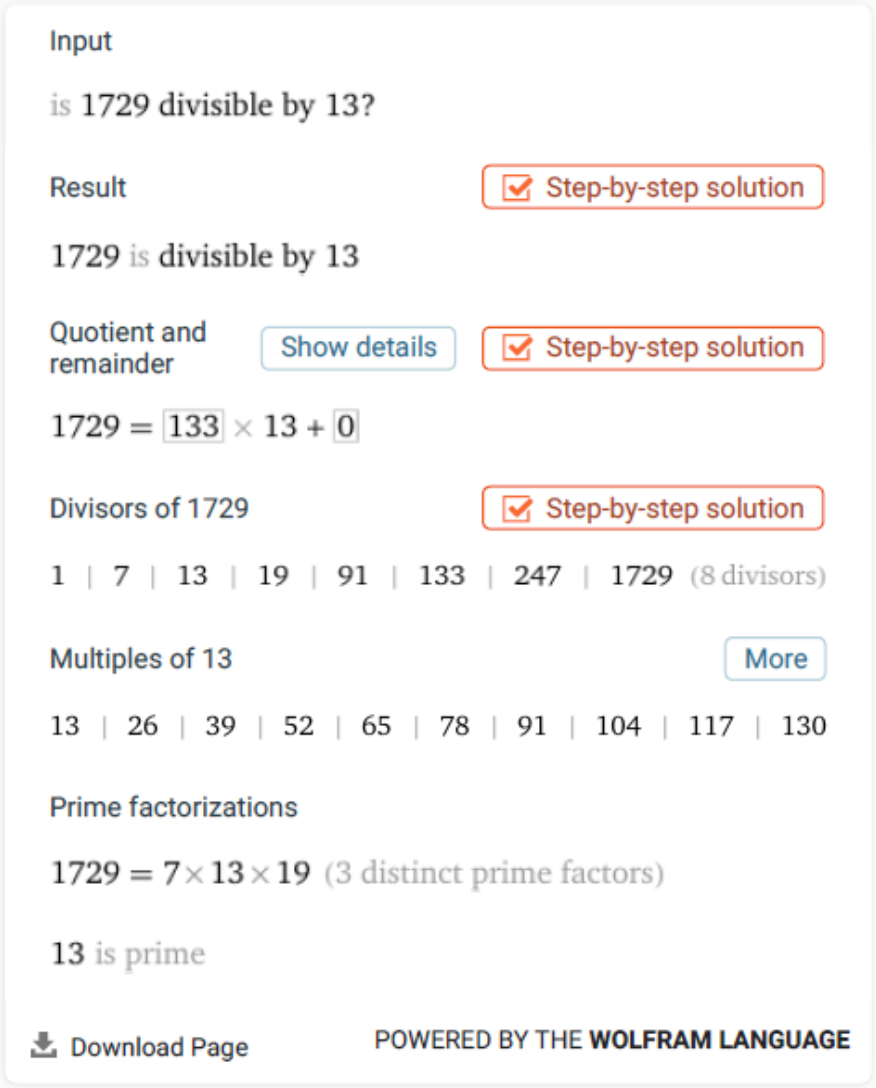
Vamos treinar os comandos do Wolfram Alpha em um exemplo de divisibilidade.

Exemplo 2. Observamos se o número 1729 é divisível por 13. Na barra de comando da tela principal do Wolfram Alpha, escrevemos em inglês *Is 1729 divisible by 13* como abaixo:

Figura 10 – Tela de acesso sobre divisibilidade. Verificação se o 13 é divisor do 1729

Apertando a tecla *Enter* do teclado ou clicando no botão do símbolo de igualdade da barra de comando, temos um relatório sobre essa questão:

Figura 11 – Resultados: Tela de acesso sobre divisibilidade



Observamos que o Wolfram Alpha nos responde que 1729 é divisível por 13 e ainda temos várias análises como: todos os divisores do 1729, a fatoração por primos de 1729, até a afirmação de que o 13 é um número primo.

Exemplo 3. Mostre que $3^{71} - 4$ não é divisível por 3.

Solução:

Na expressão $3^{71} - 4$, escrevemos esse inteiro de outra forma, temos:

$$3^{71} - 3 - 1 =$$

$$3(3^{70} - 1) - 1$$

Sabemos que 3 divide $3(3^{70} - 1)$, mas 3 não divide -1. Por isso, 3 não divide $3^{71} - 4$

Mostraremos agora, com um exemplo, uma utilidade do conceito de divisibilidade.

Exemplo 4. Se $a|b$ e $a|c$ mostre que $a^2|bc$.

Solução:

Se $a|b$ e $a|c$ então existem x e y inteiros tais que:

$$b = ax \quad \text{e} \quad c = ay.$$

Multiplicando as expressões acima membro a membro, temos:

$$bc = ax(ay) = a^2(xy) \quad \text{então} \quad a^2|bc.$$

Exemplo 5. Admitindo que a é um inteiro ímpar, mostre que $24|a\left(a^2-1\right)$.

Solução:

Admitindo que a é ímpar, então sabendo que:

$$a(a^2-1) \;=\; a(a-1)(a+1)$$

Verificamos que: $a-1$ e $a+1$ serão pares e um dos dois múltiplo de 4 e ainda que um deles é múltiplo de 3, pois são três inteiros consecutivos. Mas sabendo que: $24 = 2\cdot 3\cdot 4$, concluímos que $24|a\left(a^2-1\right)$ qualquer que seja o valor de a.

Exemplo 6. Admitindo que a, b sejam ímpares, mostre que $8|a^2-b^2$.

Solução:

Admitindo que a, b sejam ímpares, então existem n, m inteiros, tais que $a = 2n+1$ e $b = 2m+1$. Logo temos que:

$$\begin{aligned} a^2-b^2 &= 4n^2+4n+1-4m^2-4m-1 \\ &= 4\left(n^2-m^2+n-m\right) \\ &= 4\left[\left(n^2-m^2\right)+(n-m)\right]. \end{aligned}$$

Precisamos agora analisar os casos possíveis tomando $c = (n^2-m^2)$ e $d = (n-m)$:

i) Se n, m forem pares, então c, d serão pares, ou seja, da forma $c = 2x$ e $d = 2y$, x,y são inteiros. E ainda,

$$\begin{aligned} a^2 - b^2 &= 4[c+d] \\ &= 4[2x+2y] \\ &= 8[x+y]. \end{aligned}$$

Provamos que $8|a^2 - b^2$.

ii) Se n, m forem ímpares, então $c = n^2 - m^2$, $d = n - m$ serão pares, segue o caso anterior.

iii) Se n for par e m for ímpar, ou vice-versa, c, d serão ambos ímpares, ou seja, $c = 2t+1$ e $d = 2u+1$, para u,t inteiros:

$$\begin{aligned} 4\left[\left(n^2 - m^2\right) + (n-m)\right] &= 4[(2t+1) + (2u+1)] \\ &= 4[(2t+2u+2)] \\ &= 8(t+u+1). \end{aligned}$$

Provamos que $8|a^2 - b^2$.

Exemplo 7. se n é ímpar então $n^2 - 1$ é múltiplo de 8.

Solução:

Se n é ímpar então $n = 2k-1, k \in \mathbb{Z}$.

Por isso:

$$\begin{aligned} n^2 = (2k-1)^2 - 1 &= 4k^2 - 4k + 1 - 1 \\ &= 4k^2 - 4k = 4 \cdot k \cdot (k-1). \end{aligned}$$

Mas por hipótese k é inteiro, logo k ou $k-1$ é par. Por isso $8|4 \cdot k \cdot (k-1)$.

4.1.1 Critérios de Divisibilidade

A ideia é estabelecer regras que permitam determinar se um dado número inteiro, é ou não divisível por um outro número inteiro n, a um custo menor do que efetuar a divisão.

Começamos representando cada número na base 10, da seguinte forma:

$$a = a_r 10^r + a_{r-1} 10^{r-1} + \cdots + a_1 10^1 + a_0 10^0$$

Divisibilidade por 2: Um número inteiro n é divisível por 2 quando o seu último algarismo é par.

Divisibilidade por 3: Um número inteiro n é divisível por 3 se, e somente se, a soma de seus algarismos for um número divisível por 3.

Divisibilidade por 4: Um número inteiro n é divisível por 4 se, e somente se, quando os dois últimos algarismos da direita formam um número que é divisível por 4.

Divisibilidade por 5: Um número inteiro n é divisível por 5 quando o último algarismo for 0 ou 5.

Divisibilidade por 8: Um número inteiro n é divisível por 8 se, e somente se, os três últimos algarismos da direita formam um número divisível por 8.

Divisibilidade por 9: Um número inteiro n é divisível por 9 se, e somente se, a soma de seus algarismos for um número divisível por 9.

As demonstrações destas propriedades e algumas aplicações, podemos encontrar em vários textos como por exemplo: Iniciação a Aritmética (Hefez, 2015) e Aritmética (Hefez, 2014).

4.2 NÚMEROS PRIMOS

Os números primos são números relativamente simples, mas especiais pois desempenham um papel importantíssimo dentro da Teoria dos Números. Por exemplo, na estrutura multiplicativa dos inteiros, eles são suficientes para gerar todos os inteiros.

Definição 8. Dizemos que um número inteiro n maior do que 1 é primo quando n possui somente dois divisores positivos n e 1. Se o número n não é primo, dizemos que o número é composto.

Vamos colocar aqui dois resultados essenciais

Proposição 9. *Todo número par maior do que 2 é composto.*

Demonstração. Seja k um número par e maior do que 2. Então ele é da forma $k = 2x$, sendo que x é inteiro e maior do que 1. Logo, o número k é composto, pois ele possui pelo menos três divisores. □

Proposição 10. *Existem infinitos números primos.*

Demonstração. Vamos supor por absurdo que a quantidade de primos é finita. Seja a o produto de todos os primos. Então o número $a+1$ não é primo, pois ele é maior do que qualquer primo, ou seja, ele é composto. Sem perda de generalidade, podemos dizer que um certo número primo q é divisor de $a+1$. Mas esse primo q também é divisor de a. Então q é divisor de 1. Mas isso é um absurdo. Por isso, supor que existe uma quantidade finita de primos é absurdo. Logo, concluímos que existem infinitos primos. □

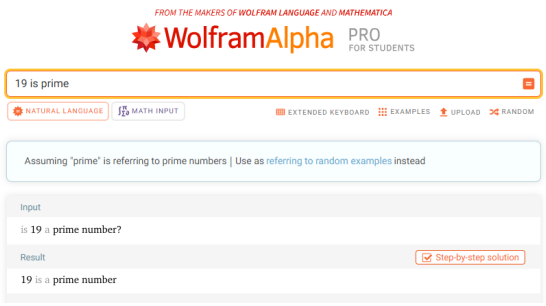
Dentro da teoria dos Números temos muitos resultados importantíssimos. Mas um deles é o Teorema Fundamental da Aritmética, que podemos enunciá-lo assim.

Teorema 4.1 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

A demonstração deste teorema e de suas algumas aplicações, podemos encontrar em vários textos como por exemplo: Aritmética (Hefez, 2014).

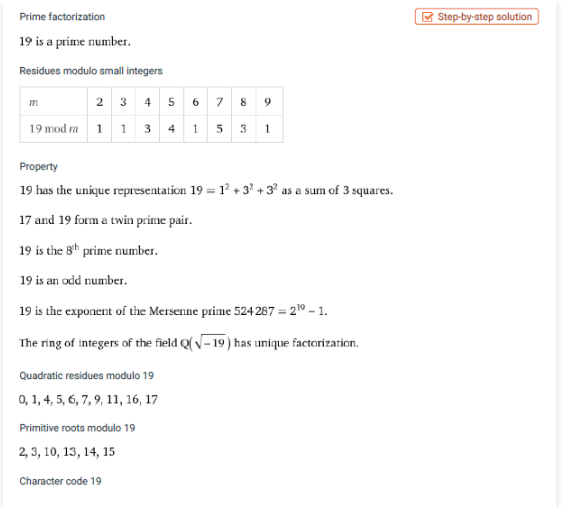
Usando o Wolfram Alpha, podemos verificar se um número é primo e ainda saber quais detalhes sobre ele. Podemos supor a questão: o 19 é primo? Escrevendo em inglês *19 is prime* temos a resposta positiva conforme se segue.

Figura 12 – Verificação se o número 19 é primo



Quando escrevemos apenas o número 19 na barra de comando, o sistema faz um imenso relatório de todas as propriedades do número, por exemplo:

Figura 13 – Algumas propriedades do número



Prime factorization

Step-by-step solution

19 is a prime number.

Residues modulo small integers

m	2	3	4	5	6	7	8	9
$19 \bmod m$	1	1	3	4	1	5	3	1

Property

19 has the unique representation $19 = 1^2 + 3^2 + 3^2$ as a sum of 3 squares.

17 and 19 form a twin prime pair.

19 is the 8^{th} prime number.

19 is an odd number.

19 is the exponent of the Mersenne prime $524\,287 = 2^{19} - 1$.

The ring of integers of the field $\mathbb{Q}(\sqrt{-19})$ has unique factorization.

Quadratic residues modulo 19

0, 1, 4, 5, 6, 7, 9, 11, 16, 17

Primitive roots modulo 19

2, 3, 10, 13, 14, 15

Character code 19

4.3 MÁXIMO DIVISOR COMUM

Dados a e b números inteiros distintos ou não, (a ou b diferente de zero). Um número d é dito um divisor comum de a e de b se $d|a$ e $d|b$, ou seja, existem x e y tais que, $a = xd$ e $b = yd$.

Definição 11. Um número d maior do que 0 é chamado de Máximo Divisor Comum de a e de b quando:

i) d é um divisor comum de a e de b.

ii) d é divisível por todo divisor comum de a e de b

Observação 12. A condição (ii)) acima ainda pode ser enunciada assim: dado c um divisor comum de a e de b, então temos $c|d$. O que está acima dito, Máximo Divisor Comum chamaremos de mdc.

Temos encontrado alunos no ensino fundamental que aprendem mais de um meio de calcular o mdc. Por isso, vamos ilustrar quatro maneiras distintas de calcular o mdc entre dois números. Nos proporciona opções diferentes de cálculos e, com isso, podemos escolher um método que nos deixe mais confortável na resolução.

Exemplo 13. Determine o $mdc(1496, 728)$.

Primeira Solução: Para determinarmos o mdc entre os dois, precisaremos determinar todos os divisores de cada um deles. E isto fazemos por obter todos os seus fatores. Por isso procedemos,

1496	2
748	2
374	2
187	11
17	17
1	

728	2
364	2
182	2
91	7
13	13
1	

Depois de determinar os fatores primos, precisamos de usar os que sejam comuns, assim: $mdc(1496,728) = 2.2.2 = 8$

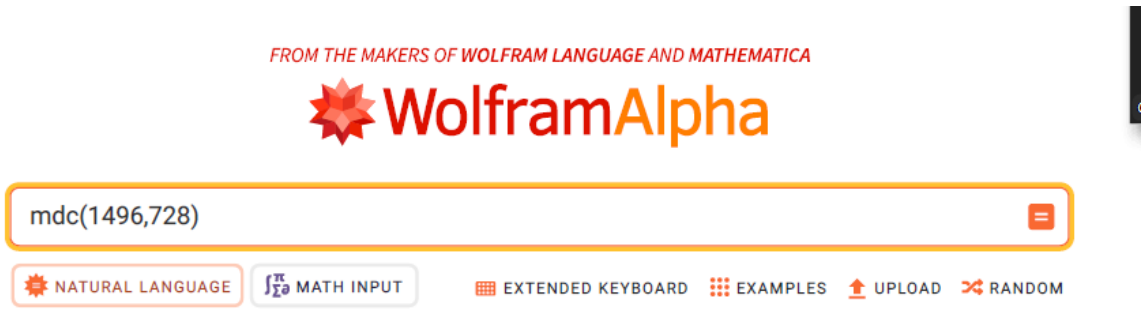
Segunda Solução: Com esta próxima maneira só usamos os que sejam divisores comuns e por isso concluímos que:

1496	728	2
748	364	2
374	182	2
187	91	

Concluímos que $mdc(1496,728) = 2.2.2 = 8$. Outras duas soluções estão mais à frente no tópico sobre o Algoritmo de Euclides.

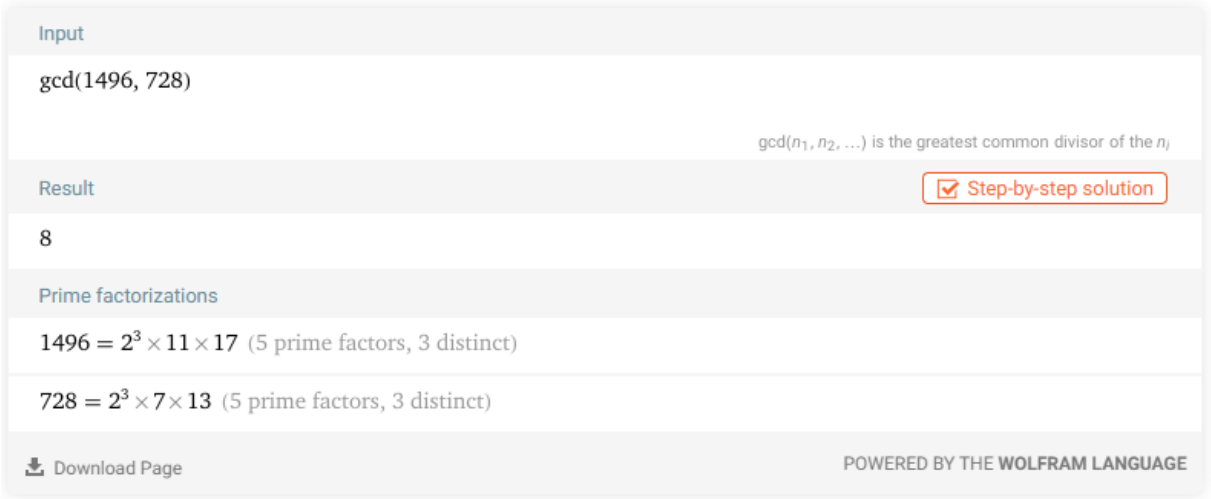
Digitando $mdc(1496,728)$ na barra de comando do Wolfram Alpha:

Figura 14 – $mdc(1496,728)$: barra de comando



Obtemos a resposta que segue:

Figura 15 – $mdc(1496,728)$: resposta



Agora veremos um lema muito usado na Teoria dos Números que utiliza o mdc de dois números e seus respectivos divisores.

Lema 14. *Sejam a e b números naturais não ambos nulos e seja $d = mdc(a,b)$. Considerando $a = xd$ e $b = yd$ então $mdc(x,y) = 1$.*

Demonstração. Se o $mdc(x,y) = d' > 1$ de modo que $x = a'd'$ e $y = b'd'$, obtemos $a = (a'd')d$ e $b = (b'd')d$. Logo $d'd$ seria um fator comum de a e de b. Mas $d'd > d$, concluímos uma contradição, pois o $d'd$ não pode ser divisor comum de a e de b e maior do que o $mdc(a,b)$. □

Agora vamos verificar as soluções de dois exemplos de questões de vestibulares que usam o máximo divisor comum em suas soluções.

Exemplo 15 (Mackenzie-SP)**.** Um painel decorativo retangular, com dimensões 2,31 m e 92,4 cm, foi dividido em um número mínimo de quadrados de lados paralelos aos lados do painel e áreas iguais. Esse número de quadrados é:

$$a)10 \qquad b)8 \qquad c)16 \qquad d)14 \qquad e)12$$

Solução: Podemos converter as medidas 2,31 m e 92,4 cm para uma medida comum, como milímetros e ainda para números naturais. Assim usaremos 2310 mm e 924 mm para repetir a estratégia do exemplo 25.

$mdc(2310,924)$

2310	924	2
1155	462	3
385	154	7
55	22	11
5	2	

$mdc(2310,924) = 462$ mm = 46,2 cm = 0,462 m

$\frac{2,31}{0,462} = 5$ quadrados no comprimento e $\frac{92,4}{46,2} = 2$ quadrados na largura

O total de quadrados será: $5 \times 2 = 10$ quadrados.

Exemplo 16 (UFPE 1ª FASE 2001)**.** Uma escola deverá distribuir um total de 1260 bolas de gude amarelas e 9072 bolas de gude verdes entre alguns de seus alunos. Cada aluno contemplado receberá o mesmo número de bolas amarelas e o mesmo número de bolas verdes. Se a escola possui 300 alunos e o maior número possível de alunos da escola deverá ser contemplado, qual o total de bolas que cada aluno contemplado receberá?

$a)38$ $b)39$ $c)40$ $d)41$ $e)42$

Solução: Se desejamos que o maior número possível de alunos dentre os 300 da escola sejam contemplados, desejamos então determinar o máximo divisor comum de 1260 e 9072, representando o maior divisor das bolas amarelas e das bolas verdes. Assim podemos dizer que teremos essa quantidade de alunos contemplados.

$mdc(1260,9072) = ?$

1260	9072	2
630	4536	2
315	2268	3
105	756	3
35	252	7
5	36	

$mdc(1260,9072) = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7 = 252$ é o número máximo de alunos contemplados.

Cada aluno contemplado receberá: $\frac{1260}{252} = 5$ bolas amarelas e $\frac{9072}{252} = 36$ bolas verdes, ou seja, um total de 41 bolas para cada um dos 252 alunos contemplados.

4.4 DIVISÃO EUCLIDIANA

Nos anos iniciais do Ensino Fundamental aprendemos na Matemática Elementar que, considerando um número D, chamado de dividendo, e um número d, diferente de zero, chamado de divisor, então existe um número q quociente, e existe um número r resto, que satisfazem a igualdade $D = dq + r$. Por exemplo, suponha que uma torta tenha 9 fatias e elas sejam divididas igualmente entre 4 pessoas. Usando a divisão euclidiana, 9 dividido por 4 é 2 com o resto 1. Em outras palavras, cada pessoa recebe 2 fatias de torta, e sobra 1 fatia. Associamos as informações nas letras $D = 9$, $d = 4$, $q = 2$ e $r = 1$, pois $9 = 4.2 + 1$.

Teorema 4.2 (Teorema da Divisão Euclidiana)**.** *Dados dois números naturais D e d, sendo d diferente de zero, sempre existem e são únicos os números naturais q e r tais que* $D = dq + r$ *e* $0 \leq r < d$.

Exemplo abaixo é para ambientar com a expressão da divisão euclidiana.

Exemplo 17. Dados a, b inteiros de modo que $a - b = 184$, $a = bq + r$, $q = 16$ e $r = 4$, quais são os valores de a, b?

Solução:

Se $a - b = 184$, então $a = 184 + b$. Mas temos que $a = bq + r$, por isso $184 + b = bq + r$, e pelas hipóteses:

$$\begin{aligned} 184 + b &= b.16 + 4 \\ 184 - 4 &= 16b - b \\ b &= 12 \end{aligned}$$

Deste modo, obtemos:

$$a = 184 + b = 184 + 12 = 196$$

Neste exemplo observamos que sendo $a = 196$ e $b = 12$ os únicos possíveis valores para q e r são, respectivamente, 16 e 4.

Ilustraremos abaixo algumas divisões euclidianas.

Exemplo 18. Observamos todos os elementos (numerador, divisor, quociente, e resto) nas divisões abaixo:

a) $47 = 3 \cdot 15 + 2$

b) $49 = 20 \cdot 2 + 9$

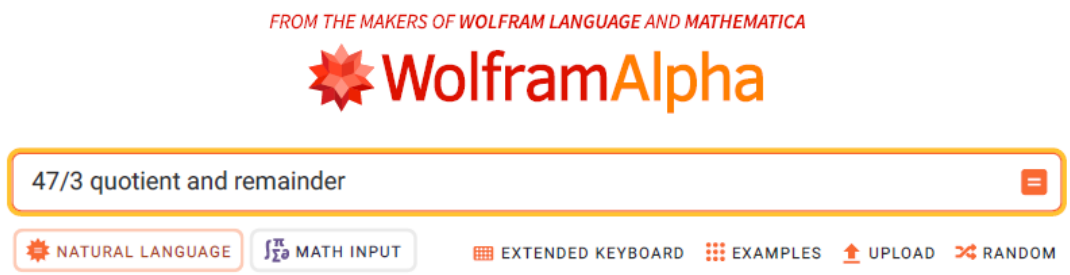
c) $106 = 7 \cdot 15 + 1$

d) $-13 = (-3) \cdot 4 - 1$

e) $-13 = 3 \cdot (-4) - 1$

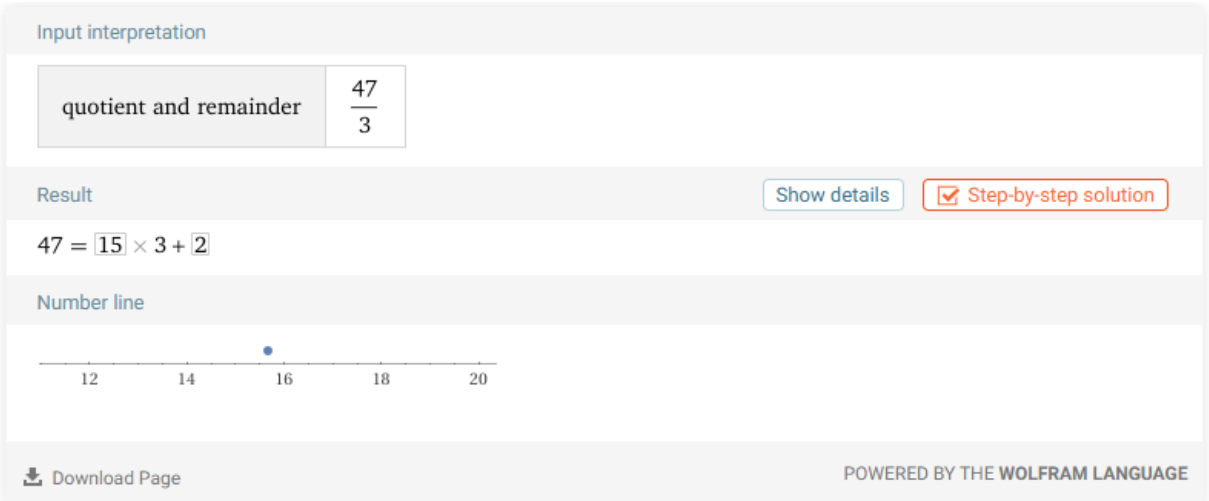
Podemos ilustrar o item *a* acima no Wolfram Alpha da seguinte forma: digitando na barra de comando do Wolfram Alpha, $47/3$ *quocient and remainder*:

Figura 16 – Quociente e resto de 47 por 3: comando



Conseguimos o resultado esperado conforme o item *a* anterior.

Figura 17 – Quociente e resto de 47 por 3: resposta



Exemplo 19. Quantos são os múltiplos de 5 entre 1 e 457?

Primeira solução:

Pela divisão euclidiana, conseguimos $457 = 5 \cdot 91 + 2$. Ou seja, o maior múltiplo de 5 será o $91 \cdot 5$ e o menor o $1 \cdot 5$. Logo, os múltiplos desejados serão: $1 \cdot 5, 2 \cdot 5, 3 \cdot 5, \ldots, 91 \cdot 5$; ou seja, são 91 múltiplos de 5.

Segunda solução:

De 1 a 457, o menor e o maior múltiplo de 5 são, respectivamente, 5 e 455 (pelo critério da divisibilidade por 5). Então, sabendo que temos n quantidade de múltiplos de 5, podemos escrever $455 = 5 + (n-1) \cdot 5$. Logo, desenvolvemos da seguinte forma:

$$\begin{aligned} 455 - 5 &= 5n - 5 \\ 450 + 5 &= 5n \\ 455 &= 5n \end{aligned}$$

Concluindo que temos $n = 91$ múltiplos de 5.

Um exemplo similar, mas com uma peculiaridade que nos inspira cuidados, é o que está em sequência.

Exemplo 20. Quantos múltiplos de 7 existem entre 123 e 2551?

Primeira solução:

Pela divisão euclidiana, temos:

$$2551 = 7 \cdot 364 + 3 \quad \text{e} \quad 123 = 7 \cdot 17 + 4$$

Então os múltiplos de 7 neste intervalo serão: $18 \cdot 7, 19 \cdot 7, 20 \cdot 7, \ldots, 364 \cdot 7$; ou seja, $364 - 17 = 347$ números.

Segunda solução:

De forma análoga, repetiremos o raciocínio acima:

$$2551 = 7 \cdot 364 + 3 \quad \text{e} \quad 123 = 7 \cdot 17 + 4$$

então o menor e o maior múltiplo de 7 serão, respectivamente, $18 \cdot 7 = 126$ e $364 \cdot 7 = 2548$. Considerando n a quantidade de múltiplos de 7 temos:

$$\begin{aligned} 2548 &= 126 + (n-1) \cdot 7 \\ 2422 &= 7n - 7 \\ 2429 &= 7n \end{aligned}$$

Então concluímos que $n = 347$ números.

Exemplo 21. Prove que:

a) se n não é múltiplo de 2 e de 3 então $n^2 - 1$ é múltiplo de 24;

b) para todo $n \in \mathbb{Z}$, 4 não divide $n^2 + 2$.

Solução:

a) Seja n não é divisível por 2 ou por 3. Dividindo n por 6, $n = 6k + r$, r não pode pertencer ao conjunto $\{0,2,3,4\}$. Ou seja, n tem que ser da forma: $6k+1$ ou $6k+5$, para $k \in \mathbb{Z}$. Por isso $n^2 - 1$ será:

   i) $(6k+1)^2 - 1 = 36k^2 + 12k = 12k(3k+1)$.

   Se k é par então, para x inteiro, $12k(3k+1) = 12 \cdot 2x(3k+1) = 24x(3k+1)$, ou seja, $24|n^2 - 1$.

   Se k é ímpar então, para x inteiro, $12k(3k+1) = 12 \cdot (2x+1)[3(2x+1)+1] = 12(2x+1)(6x+4) = 12 \cdot 2(2x+1)(3x+2) = 24(2x+1)(3x+2)$, ou seja, $24|n^2 - 1$.

   ii) $(6k+5)^2 - 1 = 36k^2 + 60k + 24 = 12k(3k+5) + 24$.

   Se k for par $12k = 12 \cdot 2x$ para $x \in \mathbb{Z}$, assim $24x(3k+5) + 24$ é divisível por 24.

   Se k for ímpar, $3k+5$ será par. Por isso, $(6k+5)^2 - 1$ é reescrito da forma $12k(3k+5) + 24 = 12k \cdot 2x + 24$, para $x \in \mathbb{Z}$. Logo $12k(3k+5) + 24$ é divisível por 24.

b) Se n é ímpar, $n = 2k+1$ e $k \in \mathbb{Z}$. Reescrevemos $n^2 + 2$ da forma:

$$(2k+1)^2 + 2 = 4k^2 + 4k + 3 = 4(k^2 + k) + 3$$

Consequentemente temos que $4|4(k^2+k)$ mas $4 \nmid 3$. Logo 4 não divide n^2+2.

Se n é par, $n = 2k$ e $k \in \mathbb{Z}$. Temos a igualdade, $n^2+2 = 2(2k^2+1)$. Mas $2k^2+1$ é ímpar, por isso observamos que $2(2k^2+1)$ não é divisível por 4.

4.5 ALGORITMO DE EUCLIDES

O Algoritmo de Euclides é um método eficiente e antigo para calcular o máximo divisor comum (MDC) entre dois números inteiros. Ele se baseia em divisões sucessivas, em que o resto da divisão anterior se torna o novo divisor, até que o resto seja zero. Criado pelo matemático grego Euclides por volta de 300 a.C., o algoritmo ainda é amplamente utilizado pela sua simplicidade e eficiência com diversas aplicações na matemática e na computação.

Para demonstrar esse algoritmo precisaremos do seguinte lema.

Lema 22. *Dados a, b e c inteiros, se existir* $mdc(a,b-ca)$ *então*

$$mdc(a,b) = mdc(a,b-ca)$$

Demonstração. Seja $d = mdc(a,b-ca)$, então concluímos que, $d|a$ e por isso $d|-ca$. Então $d|b$. Suponha que n seja um divisor comum de a e de b. Logo o n divide o a e o $b-ca$. Como por hipótese $d = mdc(a,b-ca)$, então, n divide d. Deste modo, concluímos que d é o maior divisor comum de a e b. □

Vamos aplicar esse lema no exemplo que segue.

Exemplo 23. Determine o $mdc(10,6)$.

Solução:

$$\begin{aligned} mdc(10,6) &= mdc(10-6,6) = mdc(4,6) \\ &= mdc(4,6-4) = mdc(4,2) = mdc(4-2,2) \\ &= mdc(2,2) = mdc(2-2,2) = mdc(0,2) = 2 \end{aligned}$$

Podemos escrever o Algoritmo de Euclides de forma construtiva da seguinte forma: dados a e b naturais, podemos supor que b seja menor ou igual a a. Se $b = 1$, ou $b = a$, ou b um divisor de a, então teremos que $mdc(a,b) = b$. Supondo que $1 < b < a$ e que b não divida a, podemos escrever: $a = bq_1 + r_1$. O que nos remete a duas possibilidades:

i) se r_1 divide b e pelo Lema 22, $r_1 = mdc(b, r_1) = mdc(a, b)$ e o algoritmo termina.

ii) se r_1 não divide b, podemos efetuar a divisão de b por r_1 e obtemos: $b = r_1 q_2 + r_2$, sendo que $0 < r_2 < r_1$.

O que nos remete a duas novas possibilidades:

i) se r_2 divide r_1 e pelo Lema 22, $r_2 = mdc(r_1, r_2) = mdc(r_1, b) = mdc(a, b)$ e o algoritmo termina.

ii) se r_2 não divide r_1, podemos efetuar a divisão de r_1 por r_2 e obtemos: $r_1 = r_2 q_3 + r_3$, sendo que $0 < r_3 < r_2$.

Prosseguindo com as divisões enquanto for possível obtemos $b > r_1 > r_2 > r_3 > ... > r_n$, e considerando o Princípio da Boa Ordenação, teremos $r_n = mdc(a, b)$.

Podemos montar uma tabela com três linhas e várias colunas de modo que os quocientes ficam na primeira linha. Na segunda linha começamos com o dividendo a esquerda do divisor. Nesta primeira divisão obtemos o primeiro quociente que fica em cima do divisor b e o resto r_1 embaixo do dividendo a exatamente na terceira linha. Este resto r_1 se torna o segundo divisor, a direita do primeiro divisor que agora é o dividendo. Prosseguindo efetuando as divisões, enquanto possível, chegamos no último resto que é igual a zero e o último divisor, na segunda linha que é o máximo divisor comum $mdc(a, b) = r_n$.

	q_1	q_2	q_3	q_4	...	q_n	q_{n+1}
a	b	r_1	r_2	r_3	...	r_{n-1}	r_n
r_1	r_2	r_3	r_4	...	...	0	

As resoluções dos exemplos que se seguem mostram a sua utilidade.

Exemplo 24. Determine o *mdc* entre 372 e 162.

Solução: Usando o Algoritmo de Euclides obtemos:

	2	3	2	1	2
372	162	48	18	12	6
48	18	12	6	0	

$mdc(372,162) = 6$

O procedimento do exemplo (24) acima pode ser escrito assim:

$$\begin{aligned} 6 &= 18 - 12 \cdot 1 \\ 12 &= 48 - 18 \cdot 2 \\ 18 &= 162 - 48 \cdot 3 \\ 48 &= 372 - 162 \cdot 2 \end{aligned}$$

O que podemos substituir linhas e:

$$\begin{aligned} 6 = 18 - 12.1 &= 18 - (48 - 18 \cdot 2) \cdot 1 \\ &= 18 \cdot 3 - 48 \cdot 1 \\ &= (162 - 48 \cdot 3) \cdot 3 - 48 \cdot 1 \\ &= 162 \cdot 3 - 48 \cdot 10 \\ &= 162 \cdot 3 - (372 - 162 \cdot 2) \cdot 10 \\ &= 162 \cdot 23 - 372 \cdot 10 \end{aligned}$$

$mdc(372,162) = 6$.

Exemplo 25. Um pedaço de tecido retangular possui dimensões 105 cm por 65 cm. Eu desejo cortá-lo em pedaços quadrados iguais e de modo que os seus lados tenham o maior tamanho possível. Qual deve ser o tamanho dos lados desses quadrados? Quantos serão esses quadrados?

Solução:

Nesta questão desejamos encontrar um quadrado que possua o maior lado possível. Para isso, a medida desse lado precisa ser um divisor comum de 105 e de 65. Como queremos o maior lado, precisamos calcular o máximo divisor comum. Usando o Algoritmo de Euclides, obtemos:

	1	1	1	1	1	2
105	65	40	25	15	10	5
40	25	15	10	5	0	

$mdc(105,65) = 5$

$\frac{105}{5} = 21$ partes e $\frac{65}{5} = 13$ partes

Cada quadrado possuirá os lados medindo 5 cm. Serão $21 \times 13 = 273$ quadrados.

Agora, temos mais teoria para explicar a continuação do exemplo 13:

Exemplo 26. Terceira Solução: Voltando a atenção ao 13 e utilizando as divisões sucessivas do Algoritmo de Euclides, obtemos:

$$\begin{aligned} 1496 = \ & 728 \cdot 2 + 40 \\ 728 = \ & 40 \cdot 18 + 8 \\ 40 = \ & 8 \cdot 5 + 0 \end{aligned}$$

Quando o resto dá zero acaba o algoritmo. Então o *mdc* é o último resto não nulo, ou seja: $mdc(1496, 728) = 8$

Quarta solução: Pelo método de Euclides

	2	18	5
1496	728	40	8
40	8	0	

$mdc(1496, 728) = 8$

4.6 TEOREMA DE BÉZOUT

Um teorema muito importante que veremos agora é o **Teorema de Bézout** que é um resultado fundamental em teoria dos números. Neste trabalho focaremos a sua utilidade no Algoritmo de Euclides para calcular o MDC de dois números inteiros. O que nos permite determinar se uma equação do tipo $ax + by = c$, tem soluções x e y inteiras, com base nas relações de divisibilidades entre o $mdc(a,b)$ e c.

Teorema 4.3 (Teorema de Bézout)**.** *Dados inteiros a e b, não ambos nulos, existem inteiros x e y tais que* $ax + by = mdc(a,b)$

Demonstração. Consideremos o conjunto de todos os números positivos da forma $as + bt$, em que s e t podem variar ao longo dos inteiros. É óbvio que esse conjunto contém alguns elementos, mesmo que a e b sejam negativos, porque se pusermos $s = a$ e $t = b$ temos que $a^2 + b^2$ é um número positivo e por isso pertence a esse conjunto.

Obviamente $mdc(a,b)$ divide todos os elementos desse conjunto, pela propriedade (vii) da divisibilidade. Seja d o menor dos números $as+bt$. Então, dividindo a por d encontramos q e r, tais que $a = qd + r$. Mas $r < d = as' + bt'$ e $r = a - qd$ é da forma $as+bt$, por isso o resto r tem que ser zero (porque d é o menor elemento do conjunto). Assim sendo $d|a$. Da mesma forma se prova que $d|b$. Se houvesse algum número c maior do que d e tal que, $c|a$ e $c|b$, então $c|d$, o que entra em contradição com $c > d$. Assim d é mesmo $mdc(a,b)$ e portanto $mdc(a,b)$ pode ser escrito como $as' + bt'$. □

Vamos ilustrar algumas aplicações do Teorema de Bézout, e propriedades da Divisibilidade. Aproveitamos também para praticar o software Wolfram Alpha.

Exemplo 27 (Colégio Naval)**.** Qual é o menor valor positivo de k de tal forma que: $2160x + 1680y = k$?

Solução. Para que a equação ter solução o máximo divisor comum de 2160 e 1680 deve dividir o inteiro k. Então calculando o $mdc(2160, 1680)$ obtemos:

2160	2
1080	2
540	2
270	2
135	3
45	3
15	3
5	5
1	

1680	2
840	2
420	2
210	2
105	3
35	5
7	7
1	

$$2160 = 2^4 \cdot 3^3 \cdot 5 \quad \text{e} \quad 1680 = 2^4 \cdot 3 \cdot 5 \cdot 7$$

$$mdc(2160, 1680) = 2^4 \cdot 3 \cdot 5 = 16 \cdot 3 \cdot 5 = 240$$

Mas $2160x + 1680x = 240(9x) + 240(7y) = 240(9x + 7y)$

Pelo Teorema de Bézout, o menor valor positivo de k é $mdc(2160, 1680) = 240$.

Exemplo 28 (PUCMG/07)**.** Um depósito com 3,6m de altura, 4,8m de largura e 7,2m de comprimento foi planejado para armazenar caixas cúbicas, todas de mesmo tamanho, sem que hou-

vesse perda de espaço. Pode-se estimar que o menor número de caixas cúbicas necessárias para encher completamente esse depósito é:

$$a)24 \qquad b)36 \qquad c)48 \qquad d)72 \qquad e)84$$

Solução:

As dimensões da caixa: 3,6 m; 4,8 m e 7,2 m podem ser convertidas para 36 dm, 48 dm e 72 dm, que são medidas com a mesma unidade e com números inteiros, sendo que o foco deste trabalho são as operações com números inteiros.

Para que se tenha o menor número de caixas cúbicas, essas devem ser do maior tamanho possível. O que nos direciona a determinar o máximo divisor comum entre as dimensões do depósito.

O $mdc(36,48,72) =?$. Podemos também verificar quais números primos são múltiplos comuns dos três e:

Tabela 2 – Cálculo do *mdc* com três ou mais números

36	48	72	2
18	24	36	2
9	12	18	3
3	4	6	

$mdc(36,48,72) = 2 \cdot 2 \cdot 3 = 12$ dm = 1,2 m

Então teremos: $\frac{3,6}{1,2} = 3$ caixas na altura, $\frac{4,8}{1,2} = 4$ caixas na largura, $\frac{7,2}{1,2} = 6$ caixas no comprimento, ou seja, $3 \cdot 4 \cdot 6 = 72$ caixas cúbicas de 1,2m de lado.

Nesta sequência de conteúdo, temos três outros resultados que são de muita utilidade dentro da Teoria dos Números.

Corolário 29. *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que* $am + bn = 1$.

Demonstração. Se a e b são primos entre si, então, por definição, $mdc(a,b) = 1$.

Logo, pelo Teorema de Bézout, existem m e n inteiros tais que $am + bn = 1$.

Suponha que existem números inteiros m e n tais que $am + bn = 1$, e seja $d = mdc(a,b)$. Então, por definição de mdc, $d|a$ e $d|b$. Pela propriedade (vii) da divisibilidade, $d|(am + bn)$. O que implica que $d|1$ e $d = 1$. Portanto, $mdc(a,b) = 1$. Logo a e b são primos entre si. □

Tendo analisado a operação divisibilidade e seus critérios veremos agora um resultado de extrema utilidade na teoria dos Números para analisarmos as composições dos números em geral.

Lema 30 (Lema de Gauss)**.** *Se a e b são inteiros tais que* $mdc(a,b) = 1$. *Se* $a|bc$ *então* $a|c$.

Demonstração. Pelo Teorema de Bézout, existem m, n inteiros tais que,

$$am + bn = 1 \tag{1}$$

Multiplicando a equação 1 por c temos que:

$$c(am + bn) = c \qquad \text{e} \qquad cam + nbc = c.$$

Sabemos que $a|am$ e, por hipótese, $a|bc$. Portanto a divide qualquer combinação linear de am e bc. Ou seja a divide $c(am) + n(bc)$ e por isso $a|c$. □

A partir da veracidade do lema de Gauss observamos na sequência um outro resultado também muito importante.

Lema 31 (Lema de Euclides)**.** *Sejam a, b, c inteiros e c é primo. Se* $a|bc$ *então* $a|c$ *ou* $a|b$.

Demonstração. Por hipótese $a|bc$, se $a|c$ está feito. Por outro lado, se o a não divide o c, como c é primo, então $mdc(a,c) = 1$. Pelo Lema de Gauss, então $a|b$. □

Para chegarmos a analisar e utilizar o Teorema Chinês dos Restos, precisaremos de dois outros resultados que trabalham lado a lado e possuem importância fundamental. Apresentarei-os na seção 4.7.

4.7 PEQUENO TEOREMA DE FERMAT E CONGRUÊNCIA

O Pequeno Teorema de Fermat trata-se de um resultado importante na teoria dos números, o resultado tem boas aplicações nas resoluções de problemas matemáticos. Trabalhando junto com a congruência, ele ajuda a resolvermos equações lineares de congruência.

Teorema 4.4 (Pequeno Teorema de Fermat)**.** *Dado um número p primo, tem-se que p divide o número* $a^p - a, \forall\, a \in \mathbb{Z}$.

Desse teorema dito pequeno, mas de grande importância decorre o resultado prioritário que se segue.

Corolário 32. *Sejam p um número primo e a um número natural não divisível por p, então p divide* $a^{p-1}-1$.

Usaremos esses resultados nas soluções de exemplos e que nos ajudarão na próxima seção, em que observaremos formas distintas de resoluções das mesmas questões.

Definição 33 (Congruência)**.** Seja m inteiro maior do que 1. Diremos que dois números $a, b \in \mathbb{Z}$ são congruentes módulo m se a e b possuem o mesmo resto quando divididos por m. Este fato simbolizaremos por: $a \equiv b \pmod{m}$; e lemos assim, a é congruente a b módulo m.

Quando a e b não são congruentes modulo m, escrevemos: $a \not\equiv b \pmod{m}$; e lemos assim, a não é congruente a b módulo m.

Faremos alguns exemplos básicos da definição.

Exemplo 34. a) $15 \equiv 8 \pmod{7}$ pois $15 = 7 \cdot 2 + 1$ e $8 = 7 \cdot 1 + 1$.

b) $32 \equiv 27 \pmod{5}$ pois $32 = 5 \cdot 6 + 2$ e $27 = 5 \cdot 5 + 2$.

c) $31 \not\equiv 29 \pmod{3}$ pois $31 = 3 \cdot 10 + 1$ e $29 = 2 \cdot 9 + 2$.

As congruências são ferramentas fundamentais na Teoria dos Números e podem resolver e simplificar várias operações e problemas. Elas têm uma série de propriedades que facilitam a manipulação e a resolução de equações modulares. Inclusive uma das propriedades envolve o *mmc*. Vamos relembrar:

Definição 35. Um número m maior do que 0 é chamado de Mínimo Múltiplo Comum de a e de b quando:

i) m é um múltiplo comum de a e de b.

ii) m é o menor múltiplo comum de a e de b

Seguem algumas propriedades chaves e em seguida resolveremos algumas aplicações.

Corolário 36. *Dados r número natural e* $a, b, c, d, m, n \in \mathbb{Z}$ *são válidas as seguintes propriedades:*

i) $a \equiv a \pmod{m}$.

ii) *Se* $a \equiv b \pmod{m}$ *então* $b \equiv a \pmod{m}$.

iii) *Se* $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m}$ *então* $a \equiv c \pmod{m}$.

iv) *Se* $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$ *então* $a+c \equiv b+d \pmod{m}$.

v) *Se* $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$ *então* $ac \equiv bd \pmod{m}$.

vi) *Se* $a \equiv b \pmod{m}$ *e* $n|m$ *então* $a \equiv b \pmod{n}$.

vii) $a \equiv b \pmod{m_i}$, $\forall\, i = 1,2,\ldots,r$ *se, e somente, se* $a \equiv b \pmod{mmc(m_1 \ldots m_r)}$.

viii) *Se* $a \equiv b \pmod{m}$ *então* $a^r \equiv b^r \pmod{m}$

As demonstrações destas propriedades e algumas aplicações, podemos encontrar em vários textos como por exemplo: Iniciação a Aritmética (Hefez, 2015) e Aritmética (Hefez, 2014).

Proposição 37. *Dados a, b inteiros e* $a \equiv b \pmod{m}$ *se, e somente se, m divide* $a-b$.

Demonstração. Dividindo a e b por m teremos x, y, r e s tais que:

$$a = mx + r \quad \text{e} \quad b = my + s$$

de modo que, $0 \leq r < m$ e $0 \leq s < m$. Por isso podemos escrever:

$$a - b = mx + r - (my + s) = m(x-y) + (r-s).$$

Sem perda de generalidade podemos supor que $s \leq r$ e por isso: $0 \leq r - s < m$. Por definição de congruência, a e b são congruentes módulo m quando divididos por m têm o mesmo resto $r = s$, se, e somente se, que m divide $a-b$. □

Agora vejamos alguns modos de utilizarmos as propriedades de congruência e esta proposição nas soluções de problemas.

Exemplo 38. Determine os restos das divisões de 2^{24} por:

$$a)5 \qquad b)7 \qquad c)11 \qquad d)17$$

Solução:

Lembramos que o número 5 é primo, esse fato ajuda resolver o item a).

a)

$$2^4 \equiv 1 \pmod 5$$

Usando a propriedade oito das congruências obtemos:

$$(2^4)^6 \equiv (1)^6 \pmod 5$$
$$2^{24} \equiv 1 \pmod 5$$

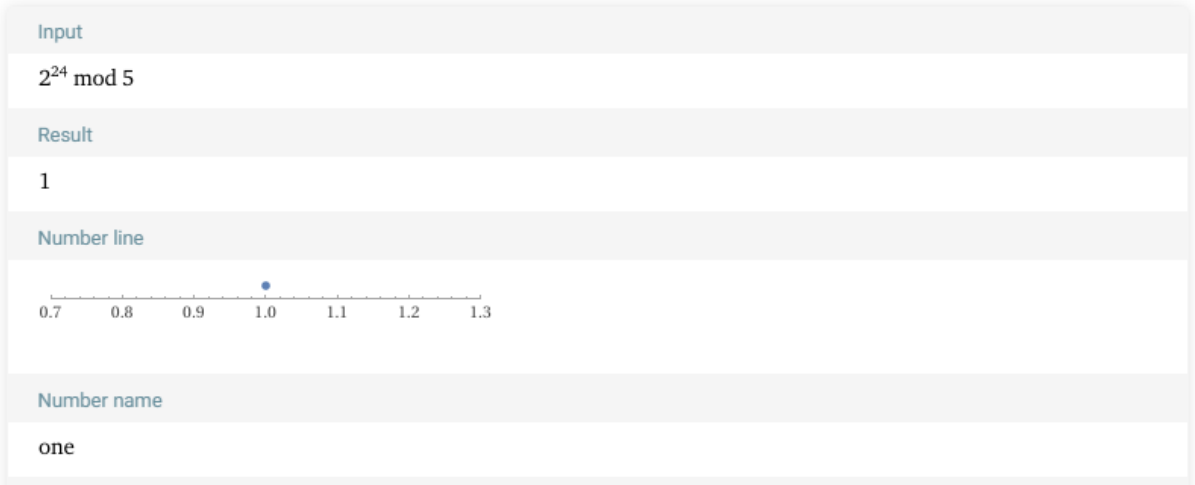
portanto o resto da divisão de 2^{24} por 5 é 1.

Digitando na barra de comando do sistema Wolfram Alpha, $2^{24} \pmod 5$:

Figura 18 – O resto da divisão de 2 elevado a 24 módulo 5: comando

Obtemos como resposta a seguinte tela.

Figura 19 – O resto da divisão de 2 elevado a 24 módulo 5: resposta



As próximas divisões são semelhantes quanto as suas resoluções.

b)

$$\begin{aligned} 2^6 &\equiv 1 \pmod 7 \\ (2^6)^4 &\equiv (1)^4 \pmod 7 \\ 2^{24} &\equiv 1 \pmod 7 \end{aligned}$$

Portanto o resto da divisão de 2^{24} por 7 é 1.

c)

$$\begin{aligned} 2^{10} &\equiv 1 \pmod{11} \\ (2^{10})^2 &\equiv 1^2 \pmod{11} \\ (2^{10})^2 &\equiv 1 \pmod{11} \end{aligned}$$

Usando as propriedades um e cinco das congruências, podemos multiplicar a congruência por um número:

$$\begin{aligned} (2^{10})^2 \times 2^4 &\equiv 1 \times 2^4 \pmod{11} \\ (2^{10})^2 \times 2^4 &\equiv 16 \pmod{11} \end{aligned}$$

mas $16 = 11 \times 1 + 5$

$$(2^{10})^2 \equiv 5 \pmod{11}$$

portanto o resto da divisão de 2^{24} por 11 é 5.

d) Não usaremos o corolário, mas observamos que $2^4+1=16+1$ então:

$$\begin{aligned} 2^4 &\equiv -1 \pmod{17} \\ (2^4)^6 &\equiv (-1)^6 \pmod{17} \\ (2^4)^6 &\equiv 1 \pmod{17} \end{aligned}$$

portanto o resto da divisão de 2^{24} por 17 é igual a 1.

Exemplo 39. Mostre que $42|a^7-a$.

Primeira solução.

Usaremos o Pequeno Teorema de Fermat e propriedades da congruência para mostrar essa divisibilidade. Primeiro fatoramos o 42 da seguinte forma $42=2\cdot 3\cdot 7$. Assim, percebemos a presença de três primos diferentes na fatoração. Analisaremos a congruência em cada primo.

i) pelo Pequeno Teorema de Fermat concluímos que: $a^7 \equiv a \pmod 7$.

ii) começamos com a propriedade reflexiva da congruência, e logo em seguida, o Pequeno Teorema de Fermat:

$$\begin{aligned} a^7 &\equiv (a^3)^2 a \pmod 3 \\ a^3 &\equiv a \pmod 3 \end{aligned}$$

usando a propriedade transitiva, chegamos na congruência desejada:

$$\begin{aligned} a^7 &\equiv (a)^2 a \pmod 3 \\ a^7 &\equiv a^3 \pmod 3 \\ a^7 &\equiv a \pmod 3 \end{aligned}$$

iii) utilizando um raciocínio similar ao do item anterior, obtemos o que desejamos provar.

$$\begin{aligned} a^7 &\equiv (a^2)^3 a \pmod 2 \\ a^2 &\equiv a \pmod 2 \\ a^7 &\equiv a \pmod 2 \end{aligned}$$

Pelas afirmações: (i)) $a^7 \equiv a \pmod 7$; (ii)) $a^7 \equiv a \pmod 3$ e (iii)) $a^7 \equiv a \pmod 2$ podemos verificar pela sétima propriedade de congruências que, $a^7 \equiv a \pmod{7 \times 3 \times 2}$, ou seja, $a^7 \equiv a \pmod{42}$ e por isso, $a^7 - a \equiv 0 \pmod{7 \times 3 \times 2}$, significando $42|a^7 - a$.

Segunda solução.

Faremos a mesma estratégia anterior, isto é, analisando cada fator primo do 42. Pelo Pequeno Teorema de Fermat podemos concluir que: $a^7 \equiv a \pmod 7$.

Fatorando $a^7 - a$ obtemos:

$$\begin{aligned} a^7 - a &= a(a^6 - 1) \\ &= a(a^3 + 1)(a^3 - 1) \\ &= a(a+1)(a^2 - a + 1)(a-1)(a^2 + a + 1) \end{aligned}$$

Os fatores $(a-1)$, a e $(a+1)$ são três números consecutivos. Por isso tanto o 2 como o 3 são fatores do seu produto.

Portanto $a^7 - a$ é divisível por 7, por 3 e por 2, considerando a sétima propriedade das congruências, concluímos que $a^7 - a$ é divisível por 42.

Exemplo 40. Determine o resto da divisão:

a) de 2^{257} por 7.

b) de 3^{23456} por 13.

Solução:

a) Podemos escrever o 257 da forma $257 = 42 \times 6 + 5$.

Então

$$2^{257} = 2^{42 \times 6 + 5} = (2^6)^{42} \times 2^5.$$

Pelo Corolário do Pequeno Teorema de Fermat temos que:

$$\begin{aligned} 2^6 &\equiv 1 \pmod 7 \\ (2^6)^{42} &\equiv 1^{42} \pmod 7 \\ (2^6)^{42} &\equiv 1 \pmod 7 \end{aligned}$$

por isso $(2^6)^{42} \times 2^5 \equiv 1 \times 2^5 \pmod 7$.

Continuamos com a congruência

$$(2^6)^{42} \times 2^5 \equiv 32 \pmod 7,$$

e $32 = 7 \times 4 + 4$, logo o resto da divisão de 2^{257} por 7 é 4.

b) Dividindo 23456 por 12 teremos que:

$$23456 = 12 \times 1954 + 8$$

Sendo N o número congruente ao resto desejado.

$$\begin{aligned} N &\equiv 3^{23456} \pmod{13} \\ N &\equiv (3^{12})^{1954} \times 3^8 \pmod{13} \end{aligned}$$

Vamos analizar cada parte do número $(3^{12})^{1954} \times 3^8$, e usando o Corolário do Pequeno Teorema de Fermat:

$$\begin{aligned} 3^{12} &\equiv 1 \pmod{13}, \\ (3^{12})^{1954} &\equiv 1 \pmod{13} \end{aligned}$$

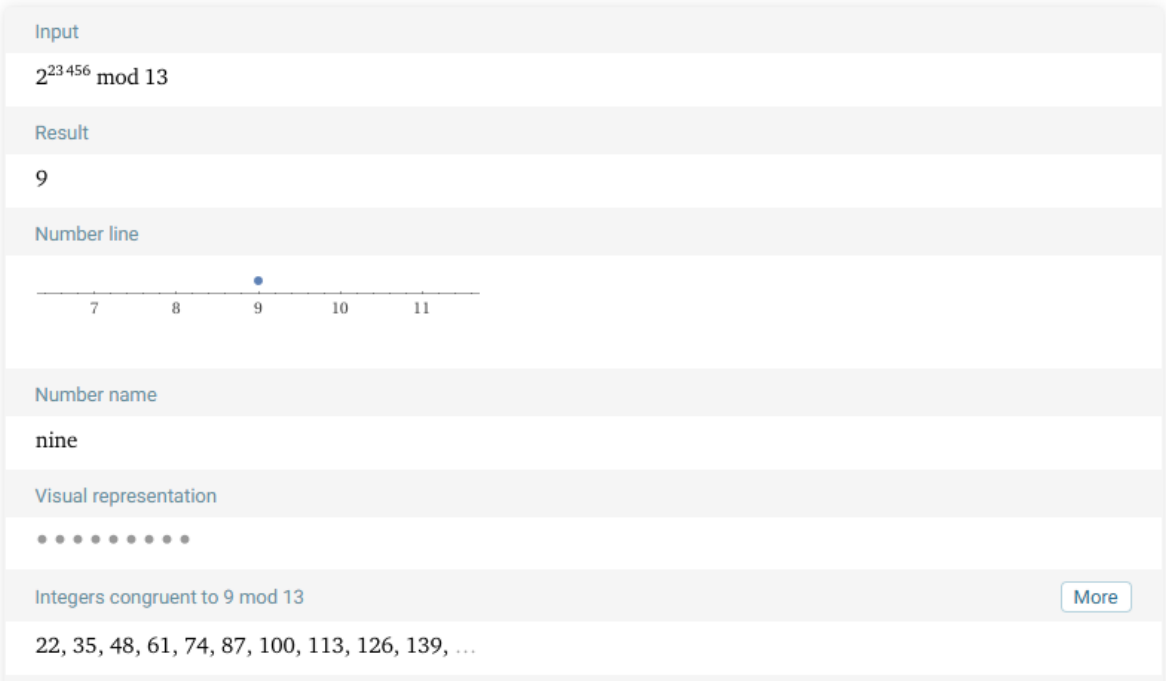
Logo $N \equiv 1 \times 3^8 \pmod{13}$, fazendo essa conta temos que $N \equiv 6561 \pmod{13}$. Dividindo 6561 por 13, obtemos $6561 = 13 \times 504 + 9$. Por isso $N \equiv 9 \pmod{13}$, então o resto da divisão de 3^{23456} por 13 é 9.

Digitando na barra de comando do Wolfram Alpha, 3^23456 $(mod 13)$:

Figura 20 – O resto de uma divisão: comando

Obtemos a seguinte resposta.

Figura 21 – O resto de uma divisão: resposta



Exemplo 41. Prove que $20^{15} - 1$ é divisível por 11.

Solução.

Para que isto aconteça, devemos deixar resto zero na divisão por onze. Sabemos que $mdc(20,11) = 1$ e que o número 20 deixa resto 9 na divisão por 11.

$$\begin{aligned} 20 &\equiv 9 \pmod{11} \\ 20^{15} &\equiv 9^{15} \pmod{11} \\ 20^{15} &\equiv (3^{10})^3 \pmod{11} \end{aligned}$$

Podemos concluir pelo Corolário do Pequeno Teorema de Fermat que: $3^{10} \equiv 1 \pmod{11}$, por isso:

$$\begin{aligned} 20^{15} &\equiv (1)^3 \pmod{11} \\ 20^{15} &\equiv 1 \pmod{11} \end{aligned}$$

Portanto $20^{15} - 1$ é divisível por 11.

Digitando na barra de comando do Wolfram Alpha, 20^15 $(mod 11)$:

Figura 22 – Congruência 20^15 $(mod 11)$: comando

Obtemos a seguinte resposta.

Figura 23 – Congruência 20^15 $(mod 11)$: resposta

O que nos mostra que 20^15 − 1 é múltiplo de 11.

Exemplo 42 (OBM 2008)**.** Mostre que existem infinitos inteiros positivos tais que

$$n|(5^{n-2}-1)$$

Solução.

Aproveitando a infinitude dos números primos e com o uso do Corolário do Pequeno Teorema de Fermat, consideramos $n = 2p$, com p primo, a divisão abaixo é equivalente:

$$\frac{5^{n-2}-1}{n} = \frac{5^{2p-2}-1}{2p} = \frac{(5^{p-1})^2-1}{2p}$$

Analisando essa equivalência por módulo p primo:

$$\begin{aligned} 5^{n-2} &\equiv 5^{2p-2} \pmod{p}, \\ 5^{n-2} &\equiv (5^{p-1})^2 \pmod{p}, \\ 5^{n-2} &\equiv 1 \pmod{p} \end{aligned}$$

concluímos que qualquer primo p divide $5^{n-2}-1$. Agora, tomando p maior do que 2, sabemos que $mdc(2,p) = 1$. Implicando que $mmc(2,p) = 2p = n$, segue que n divide $5^{n-2}-1$, pela propriedade (vii)).

Agora analisaremos uma importante propriedade da aritmética modular que nos ajuda a fazer simplificações mas com uma condição específica.

Lema 43 (Lei do Corte)**.** *Sejam a, b, c e m inteiros com* $m > 1$. *Se* $a \cdot c \equiv b \cdot c \pmod{m}$ *e se* $mdc(c,m) = 1$*, então* $a \equiv b \pmod{m}$.

A demonstração e mais aplicações desse resultado podemos verificar nos Vídeos 44 e 47 do programa PIC da OBMEP com o Prof. Fábio Henrique e no livro Aritmética do autor Abramo Hefez da Coleção PROFMAT.

Exemplo 44. Simplifique a congruência:

$$34 \equiv 4 \pmod{5}$$

Solução.

Podemos simplificar o 34 e o 4 por 2, obtendo respectivamente 17 e 2 nos resultados, pois $mdc(2,5) = 1$. Então, podemos escrever que a $34 \equiv 4 \pmod{5}$ é igual a $17 \equiv 2 \pmod{5}$

Exemplo 45. (OBM(2003)) Seja $n = 9867$. Se você calculasse $n^3 - n^2$, você encontraria um número cujo algarismo das unidades é:

$$a)0 \qquad b)2 \qquad c)4 \qquad d)6 \qquad e)8$$

Solução

Para determinarmos o dígito das unidades de um número, devemos fazer a análise da congruência desse número módulo 10. Então escrevemos:

$$\begin{aligned} 9867 &\equiv 7 \pmod{10}, \\ 9867^2 &\equiv 7^2 \pmod{10}, \end{aligned}$$

e como $7^2 = 49 \equiv 9 \pmod{10}$,

$$9867^2 \equiv 9 \pmod{10} \tag{2}$$

Agora, vamos desenvolver a parte do número ao cubo.

$$\begin{aligned} 9867^2 \cdot 9867 &\equiv 9 \cdot 7 \pmod{10}, \\ 9867^3 &\equiv 63 \pmod{10} \end{aligned}$$

e como $63 \equiv 3 \pmod{10}$

$$9867^3 \equiv 3 \pmod{10} \tag{3}$$

Fazendo a subtração 3 com 2 obtemos:

$$\begin{aligned} 9867^3 - 9867^2 &\equiv 3 - 9 \pmod{10}, \\ 9867^3 - 9867^2 &\equiv -6 \pmod{10} \end{aligned}$$

e como $-6 \equiv 4 \pmod{10}$, concluímos

$$9867^3 - 9867^2 \equiv 4 \ (mod 10)$$

O algarismo das unidades é o 4 e a resposta correta é a letra *c*.

Exemplo 46. (OBMEP(2009)) João mora em Salvador e seus pais em Recife. Para matar a saudade, ele telefona para seus pais a cada três dias. O primeiro telefonema foi feito no domingo, o segundo telefonema na quarta-feira, o terceiro telefonema no sábado, e assim por diante. Em qual dia da semana João telefonou para seus pais pela centésima vez?

Solução:

Listando os dias em que aconteceram as primeiras chamadas, escrevemos:

Primeira chamada: domingo

Segunda chamada: quarta feira

Terceira chamada: sábado

Quarta chamada: terça feira

Quinta chamada: sexta feira

Sexta chamada: segunda feira

Sétima chamada: quinta feira

Oitava chamada: domingo

Nona chamada: quarta feira

Podemos também observar que a cada sete dias a sequência se repete. Por isso em termos de módulo 7 temos:

$$\begin{aligned} 10 &\equiv 3 \pmod 7, \\ 10^2 &\equiv 3^2 \pmod 7, \\ 100 &\equiv 2 \pmod 7 \end{aligned}$$

Assim, o centésimo telefonema será realizado no mesmo dia da semana que o segundo telefonema, isto é, em uma quarta feira.

Exemplo 47. (OBM(2003b)) Considere a sequência oscilante: 1, 2, 3, 4, 5, 4, 3, 2, 1, 2, 3, 4, 5, 4, 3, 2, 1, 2, 3, 4,.... O 2003º termo desta sequência é:

$$a)1 \qquad b)2 \qquad c)3 \qquad d)4 \qquad e)5$$

Solução

Podemos observar que a sequência é infinita e o bloco 1, 2, 3, 4, 5, 4, 3, 2 é formado por 8 termos. Depois começa a repetição do bloco.

Para determinar o termo que está na posição 2003, devemos encontrar o resto da divisão de 2003 por 8, isto é, o número que é congruente a 2003 módulo 8. Podemos analisar que:

$$\begin{aligned} 10 &\equiv 2 \pmod 8, \\ 10^2 &\equiv 2^2 \pmod 8 \end{aligned}$$

Usando a propriedade de multiplicações de congruências,

$$\begin{aligned} 100 \cdot 10 &\equiv 4 \cdot 2 \pmod 8, \\ 1000 \cdot 2 &\equiv 0 \cdot 2 \pmod 8, \\ 2000 &\equiv 0 \pmod 8 \end{aligned}$$

Mas sabemos que $3 \equiv 3 \pmod 8$. Por isso, segue que:

$$\begin{aligned} 2000 + 3 &\equiv 0 + 3 \pmod 8, \\ 2003 &\equiv 3 \pmod 8 \end{aligned}$$

Ou seja, o termo de ordem 2003 da sequência será igual ao terceiro termo, ou ainda o número 3. Portanto a resposta correta é o item *c*.

Exemplo 48. (OBM(2000)) Se os números naturais são colocados em colunas, como se mostra abaixo:

A	B	C	D	E	F	G	H	I
1		2		3		4		5
	9		8		7		6	
10		11		12		13		14
	18		17		16		15	
19		20		21		...		...

Qual coluna aparecerá o número 2000?

a) F *b*) B *c*) C *d*) D *e*) I

Solução

Escrevendo a sequência em ordem numérica crescente de inteiros de 1 a 9, observamos que as letras correspondentes aos números ficarão na seguinte ordem $A, C, E, G, I, H, F, D, B$.

A	C	E	G	I	H	F	D	B
1	2	3	4	5	6	7	8	9

Podemos observar que a sequência se repete a cada 9 termos. Então precisamos determinar a congruência de 2000 módulo 9.

$$\begin{aligned} 10 &\equiv 1 \pmod 9, \\ 10^3 &\equiv 1^3 \pmod 9, \\ 1000 &\equiv 1 \pmod 9 \end{aligned}$$

Multiplicando esta congruência por 2, obtemos

$$\begin{aligned} 2 \cdot 1000 &\equiv 2 \cdot 1 \pmod 9, \\ 2000 &\equiv 2 \pmod 9 \end{aligned}$$

Portanto, o 2000 estará na mesma coluna do número 2 e a resposta correta é o item *c*, ou seja, coluna da letra *C* da tabela.

Exemplo 49. (OBMEP(2005)) Distribuímos os números inteiros positivos em uma tabela com cinco colunas, conforme o seguinte padrão:

A	B	C	D	E
1				
2	3			
4	5	6		
7	8	9	10	
11	12	13	14	15
16				
17	18			
19	20	21		
22	23	24	25	
26	27	28	29	30
31				
32	33			
...				

Continuando a preencher a tabela desta maneira, qual será a coluna ocupada pelo número 2005?

a) coluna A b) coluna B c) coluna C d) coluna D e) coluna E

Solução

Por observar e interpretar a tabela, constatamos que a cada 15 termos a tabela se repete, segundo a sequência que é formada pelas letras: $A,A,B,A,B,C,A,B,C,D,A,B,C,D,E$, nesta ordem.

Para determinarmos a coluna que será ocupada pelo número 2005, deveremos calcular o número que é congruente a 2005 módulo 15. Começamos com dois fatos $10 \equiv 10 \pmod{15}$ e $20 \equiv 5 \pmod{15}$, multiplicamos as duas congruências:

$$200 \equiv 50 \pmod{15},$$
$$200 \equiv 5 \pmod{15}$$

Multiplicando a congruência anterior por 10 e usando o fato que $50 \equiv 5 \pmod{15}$, então:

$$\begin{aligned} 2000 &\equiv 5 \pmod{15}, \\ 2000+5 &\equiv 5+5 \pmod{15}, \\ 2005 &\equiv 10 \pmod{15} \end{aligned}$$

Portanto a coluna ocupada pelo 2005 será a mesma ocupada pelo número 10, isto é, a coluna *D*. Então a resposta correta é o item *d*.

4.8 EQUAÇÕES DIOFANTINAS LINEARES

As equações diofantinas são equações polinomiais nas quais, geralmente se busca somente soluções inteiras. Elas aparecem frequentemente em problemas de teoria dos números.

A palavra diofantina se refere ao matemático helenístico do século III, Diofanto de Alexandria, o qual estudou tais equações e foi um dos primeiros matemáticos a introduzir o uso de símbolos na álgebra. O estudo matemático de problemas diofantinos propostos por Diofanto agora é chamado de análise diofantina.
Consta que na lápide de seu túmulo foi escrito:

> *Aqui jaz Diofanto. Maravilhosa habilidade. Pela arte da álgebra a lápide nos diz sua idade: Deus deu um sexto da vida como infante, um duodécimo mais como jovem, de barba abundante; e ainda uma sétima parte antes do casamento; em cinco anos nasce-lhe o rebento. Lastima! O filho do mestre e sábio do mundo se vai. Morreu quando atingiu metade da idade final do pai. Quatro anos a mais de estudos consolam-no do pesar; para então, deixando a terra, também ele alívio encontrar.*

Daí podemos representar como uma equação algébrica e descobrirmos sua idade:

$$\frac{x}{6}+\frac{x}{12}+\frac{x}{7}+5+\frac{x}{2}+4=x$$

Definição 50. Uma equação é dita diofantina se é uma equação do tipo: $ax+by=c$; na qual a, b e c são inteiros.

Neste texto, analisaremos condições para que as equações tenham soluções inteiras. Em situações mais específicas, tenham soluções naturais.

Teorema 4.5. *Dada a equação diofantina $ax+by=c$, ela tem solução inteira, isto é, existem inteiros x e y satisfazendo a equação se, e somente se, $mdc(a,b)|c$.*

Demonstração. Suponha que $d = mdc(a,b)|c$. Pelo teorema de Bézout, existem u, v inteiros tal que

$$au + bv = d \tag{4}$$

Como o número d divide o c, então $c = dq$, para um certo q inteiro. Multiplicando a equação (4) por q:

$$\begin{aligned} auq + bvq &= dq \\ a(uq) + b(bq) &= dq = c \end{aligned}$$

Considerando $x = uq$ e $y = bq$, achamos uma solução inteira para a equação $ax+by=c$.

Supomos que a equação diofantina tem uma solução inteira. Seja $d = mdc(a,b)$. Consideramos $a = dr$, $b = ds$, e a equação $ax+by=c$:

$$drx + dsy = d(rx+sy) = c.$$

Por isso $d|c$, como queríamos demonstrar. □

Quando as equações diofantinas satisfazem o teorema anterior, elas têm infinitas soluções. Mas essas soluções são dependentes de solução inicial. Isso é mostrado no teorema seguinte, mais ainda nos ajuda a encontrar uma solução específica.

Teorema 4.6. *Suponha que x_0 e y_0 componham a solução inicial da equação diofantina $ax+by=c$ então todas as outras soluções inteiras tem a forma:*

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

sendo que $t \in \mathbb{Z}$ e $d = mdc(a,b)$.

Demonstração. Se x_0 e y_0 é um par ordenado da solução e tomando outro par ordenado x_1 e y_1 solução da equação $ax+by=c$ então:

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

Por isso:

$$\begin{aligned} ax_0 - ax_1 &= by_1 - by_0 \\ a(x_0 - x_1) &= b(y_1 - y_0) \end{aligned}$$

Denotando $d = mdc(a,b)$ então existem $r,s \in \mathbb{Z}$ tais que $a = rd$ e $b = sd$, isto é,

$$r = \frac{a}{d} \qquad \text{e} \qquad s = \frac{b}{d}$$

Substituindo, temos $rd(x_0 - x_1) = sd(y_1 - y_0)$, ou seja,

$$r(x_0 - x_1) = s(y_1 - y_0) \tag{5}$$

Observamos que r divide $s(y_1 - y_0)$. Mas como $mdc(r,s) = 1$ então r divide $(y_1 - y_0)$. Então existe $t \in \mathbb{Z}$ tal que

$$\begin{aligned} y_0 - y_1 &= rt \\ -y_1 &= -y_0 + rt \\ y_1 &= y_0 - rt \end{aligned}$$

Substituindo $y_0 - y_1 = rt$ na equação (5), obtemos que $x_1 - x_0 = st$, e

$$x_1 = x_0 + st.$$

Resumimos no sistema:

$$\begin{cases} x_1 = x_0 + st \\ y_1 = y_0 - rt \end{cases}$$

Pode ser reescrito assim:

$$\begin{cases} x_1 = x_0 + \left(\frac{b}{d}\right) t \\ y_1 = y_0 - \left(\frac{a}{d}\right) t \end{cases}$$

□

Agora vejamos como aplicar este teorema em várias soluções de problemas.

Exemplo 51. Qual é o menor múltiplo positivo de 7 que deixa resto 1 quando divido por 2, 3, 4, 5, 6?

Solução.

Primeiro, procuramos os números x tais que:

$$\begin{aligned} 7x &\equiv 1 \pmod 2, \\ 7x &\equiv 1 \pmod 3, \\ 7x &\equiv 1 \pmod 4, \\ 7x &\equiv 1 \pmod 5 \quad \text{e} \\ 7x &\equiv 1 \pmod 6. \end{aligned}$$

Utilizando a propriedade (vii)), desejamos x tal que $7x \equiv 1 \pmod{60}$, pois $mmc(2,\ldots,6) = 60$. Isso significa que 60 divide $7x-1$. Ou seja, para cada x, existe y tal que $7x-1 = 60y$. Analisando como equação diofantina $7x-60y = 1$, podemos usar o Algoritmo de Euclides para resolver:

	8	1	1	3
60	7	4	3	1
4	3	1	0	

Traduzindo a tabela, temos:

$$\begin{aligned} 60 &= 7\cdot 8+4, \\ 7 &= 4\cdot 1+3 \quad \text{e} \\ 4 &= 3\cdot 1+1 \end{aligned}$$

$$1 = 4-3\cdot 1 = 4-(7-4) = 2\cdot 4-1\cdot 7 = 2(60-7\cdot 8)-1\cdot 7 = 7(-17)-60(-2)$$

Usando o teorema anterior, a solução inicial é $x_0 = -17$ e $y_0 = -2$. Vamos escrever a solução geral $x = -17+60t$ e $y = -2+7t$, com $t \in \mathbb{Z}$ e $mdc(7,-60) = 1$.

O menor valor positivo de x será com $t = 1$, ou seja,

$$x = -17+60\cdot 1 = -17+60 = 43$$

Então o número procurado será o 301 pois:

$$7x = 7\cdot 43 = 301$$

e ainda observamos que:

$$\begin{aligned} 301 &= 2\cdot 150+1 \\ 301 &= 3\cdot 100+1 \\ 301 &= 4\cdot 75+1 \\ 301 &= 5\cdot 60+1 \\ 301 &= 6\cdot 50+1 \end{aligned}$$

Exemplo 52. (Yi Shing aprox. 700 dC) Ache os inteiros que divididos por $2,3,6$ e 12 que deixam restos $1,2,5$ e 5, respectivamente.

Solução.

Com base no enunciado podemos escrever o seguinte sistema de congruência:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 5 \pmod 6 \\ x &\equiv 5 \pmod{12} \end{aligned}$$

Observamos que todas as soluções de $x \equiv 5 \pmod{12}$, são também soluções $x \equiv 5 \pmod 6$ porque 12 é múltiplo de 6. O que reduz o sistema a:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 5 \pmod 6 \end{aligned}$$

Sabendo também que o 6 é múltiplo de 3 e de 2, observando que:

$$\begin{aligned} 5 &= 2\cdot 2+1 \\ 5 &= 3\cdot 1+2 \end{aligned}$$

Concluímos que as duas primeiras congruências são equivalentes a terceira. Sabemos que a terceira é equivalente a quarta. Por isso basta resolver a quarta congruência, $x \equiv 5 \pmod{12}$. A solução geral é $x = 5 + 12t$ para $t \in \mathbb{Z}$. Logo os inteiros são: 17, 29, 41, 53, 65, ...

Exemplo 53. Em determinado jogo estabeleceu-se a regra que as pontuações de cada time só possuem dois valores: 3 ou 5. Lembrando do vergonhoso 7 a 1 que o futebol brasileiro sofreu em 2014, poderíamos dizer que esse jogo poderia ser o futebol?

Solução.

Para que isso seja possível precisamos ter que $5x + 3y = 1$ e $5x' + 3y' = 7$, tais que x, x' e y, y' são números naturais. Vejamos que $mdc(5,3) = 1$ e ainda temos que $1|1$ e $1|7$.

Então as equações

$$5x + 3y = 1 \quad \text{e} \quad 5x' + 3y' = 7$$

possuem soluções inteiras. e pelo Teorema de Bézout, teremos soluções como por exemplo:

$$5(-1) + 3 \cdot 2 = 1 \quad \text{e} \quad 5(-1) + 3 \cdot 4 = 7$$

Concluímos que as soluções gerais são:

i) para $5x + 3y = 1$ é $x = -1 + 3t$ e $y = 2 - 5t$, sendo que $t \in \mathbb{Z}$. Mas para a hipótese do problema x e y devem ser maiores do que zero. Por isso concluímos que, $t > 1/3$ e $t < 2/5$. Podemos verificar que não existe $t \in \mathbb{Z}$ neste intervalo. Logo a equação $5x + 3y = 1$ não possui solução natural. Então concluímos que esse jogo não pode ser o futebol.

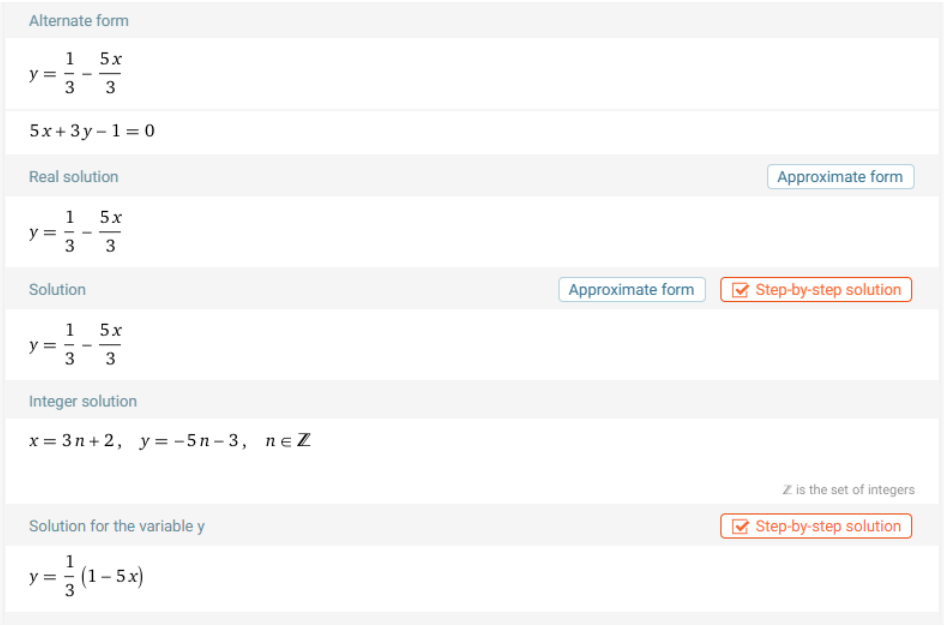
ii) para $5x' + 3y' = 7$ é $x' = -1 + 3t$ e $y' = 4 - 5t$, com $t \in \mathbb{Z}$.

A equação $5x + 3y = 1$ pode ser ilustrada pela representação gráfica do Wolfram Alpha, conforme segue. Para isto, basta digitar $5x + 3y = 1$ na barra de comando.

Figura 24 – Exemplo 53: comando 1

Figura 25 – Exemplo 53: parte um da resposta 1

Figura 26 – Exemplo 53: parte dois da resposta 1



Vejamos agora, similarmente para a equação $5x + 3y = 7$ digitada na barra de comando do Wolfram Alpha.

Figura 27 – Exemplo 53: comando 2

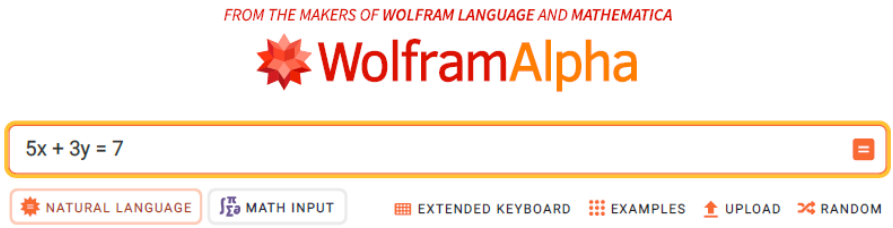


Figura 28 – Exemplo 53: parte um da resposta 2

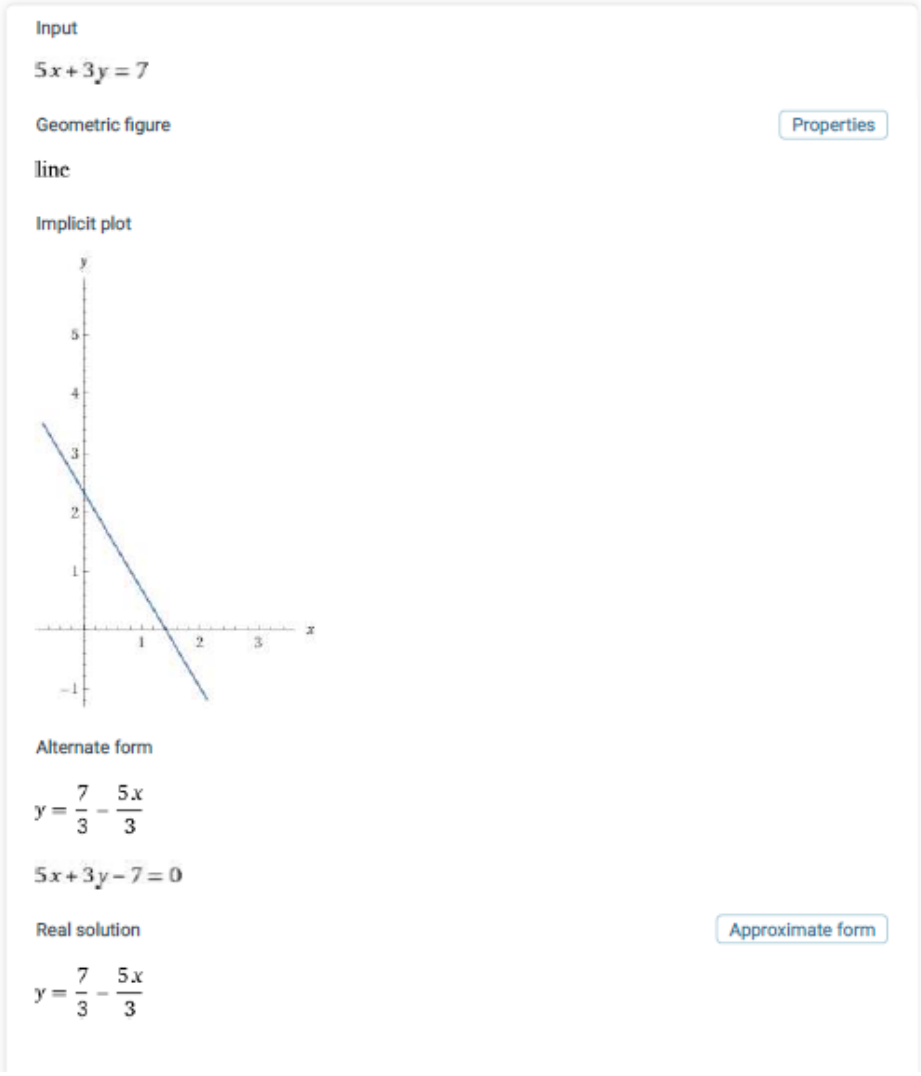
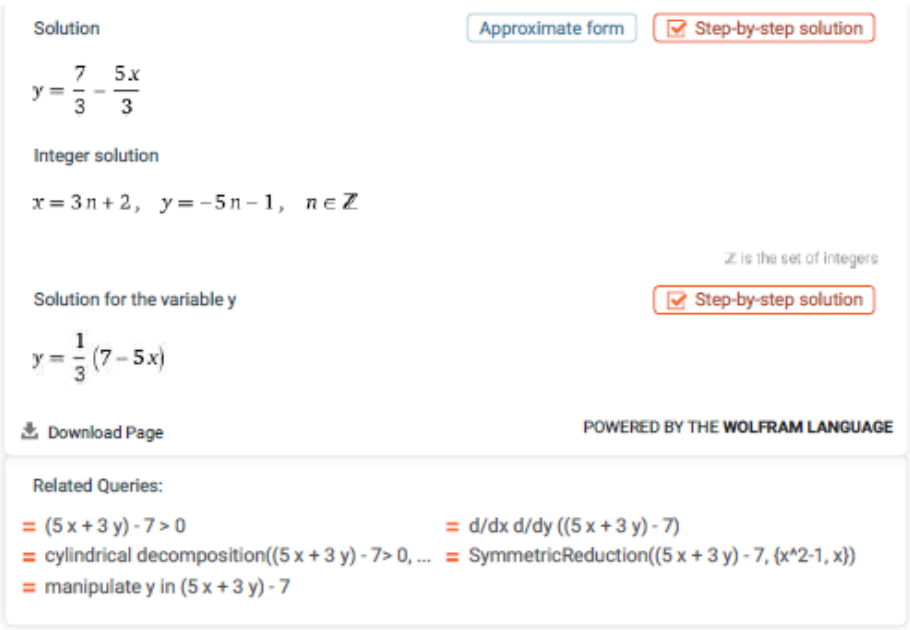


Figura 29 – Exemplo 53: parte dois da resposta 2



Exemplo 54. Considerando a equação diofantina $3x + 5y = 101$.

a) Encontre todas as suas soluções inteiras.

b) Ela possui soluções naturais? Justifique.

Solução.

a) Vamos primeiro verificar a existência de solução calculando o $mdc(5,3)$. Claramente $mdc(5,3) = 1$, e como $1|101$, então concluímos que a equação $3x + 5y = 101$ possui solução inteira. Vamos então encontrar um par x_0 e y_0 que resolva a equação. Pelo Algoritmo da Divisão podemos escrever:

	1	1	2
5	3	2	1
2	1	0	

$$3 = 1 \cdot 2 + 1 \qquad \text{e} \qquad 5 = 1 \cdot 3 + 2 \Longrightarrow 5 - 1 \cdot 3 = 2$$

$$\begin{aligned} 1\cdot 3 &= 1\cdot(5-1\cdot 3)+1 \\ 1\cdot 3 &= 1\cdot 5-1\cdot 3+1 \\ 2\cdot 3-1\cdot 5 &= 1 \end{aligned}$$

Multiplicando a igualdade por 101, obtemos:

$$202\cdot 3-101\cdot 5=101$$

Por isso, o par $x_0=202$ e $y_0=-101$ é uma solução particular e todas as soluções inteiras são do tipo:

$$x=202+5t \text{ e } y=-101-3t, \text{ para } t\in\mathbb{Z}.$$

b) Se a equação $3x+5y=101$ possui soluções naturais, então elas terão que satisfazer $x>0$ e $y>0$. Podemos então analisar que:

$$\begin{aligned} 202+5t &> 0 \\ 5t &> -202 \\ t &> \tfrac{-202}{5} \\ t &> -40,\ldots \end{aligned} \qquad \begin{aligned} -101-3t &> 0 \\ -3t &> 101 \\ t &< \tfrac{-101}{3} \\ t &< -33,\ldots \end{aligned}$$

$$t\in\{-40,-39,-38,-37,-36,-35,-34\}$$

A equação possui soluções naturais se t pertencer ao conjunto acima. Ainda podemos notar que os pares ordenados (x,y) serão: $(2,19),(7,16),(12,13),(17,10),(22,7),(27,4),(32,1)$

Utilizando a barra de comando do Wolfram Alpha para resolver esta equação diofantina:

Figura 30 – Exemplo 54: comando

Obtemos as três seguintes telas como respostas:

Figura 31 – Exemplo 54: parte um da resposta

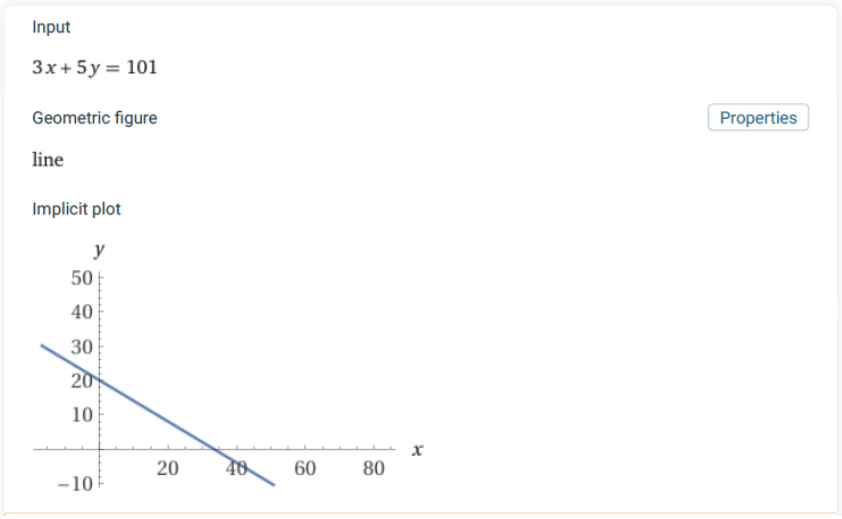


Figura 32 – Exemplo 54: parte dois de resposta

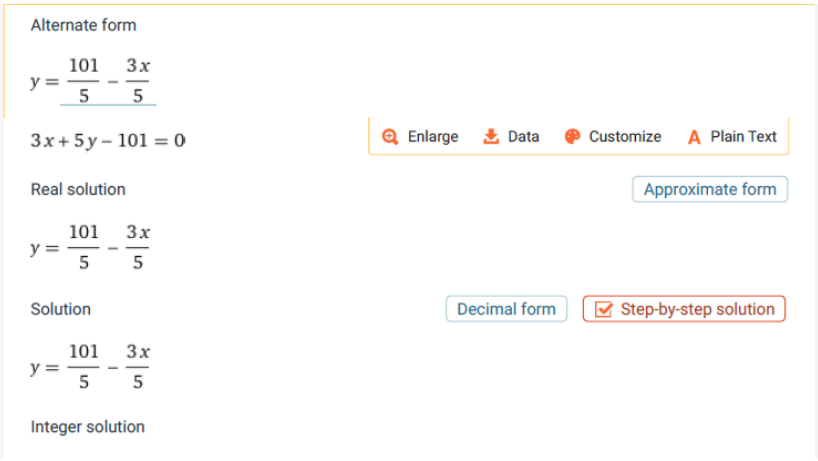
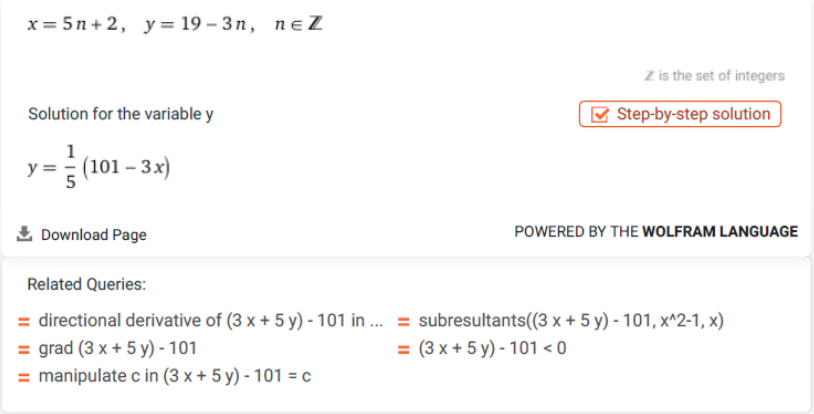


Figura 33 – Exemplo 54: parte três da resposta



Exemplo 55. Encontre todas as medições inteiras de um termômetro tanto em graus Celsius quanto em graus Fahrenheit.

Solução.

As temperaturas de fusão e de solidificação da água nas escalas Celsius e Fahrenheit são $t_{fC} = 100$, $t_{sC} = 0$, $t_{fF} = 212$ e $t_{sF} = 32$, respectivamente.

Considerando C uma temperatura qualquer na escala Celsius e F uma temperatura qualquer na escala Fahrenheit, temos que:

$$(100 - C)/(100 - 0) = (212 - F)/(212 - 32)$$

Resumindo:

$$\frac{C}{100} = \frac{F - 32}{180}$$

Chegando na equação:

$$18C = 10F - 320 \Longleftrightarrow 10F - 18C = 320 \Longrightarrow 5F - 9C = 160$$

Calculando o $mdc(9,5)$ pelo método de Euclides, temos:

	1	1	4
9	5	4	1
4	1	0	

Assim, o $mdc(9,5) = 1$ e sabemos que 1 divide 160 então a equação $5F - 9C = 160$ possui soluções inteiras. Usando o Algoritmo da Divisão:

$$5 = 1 \cdot 4 + 1 \quad \text{e} \quad 9 = 1 \cdot 5 + 4$$
$$1 = 5 - 1 \cdot 4 \quad \text{e} \quad 4 = 9 - 1 \cdot 5$$

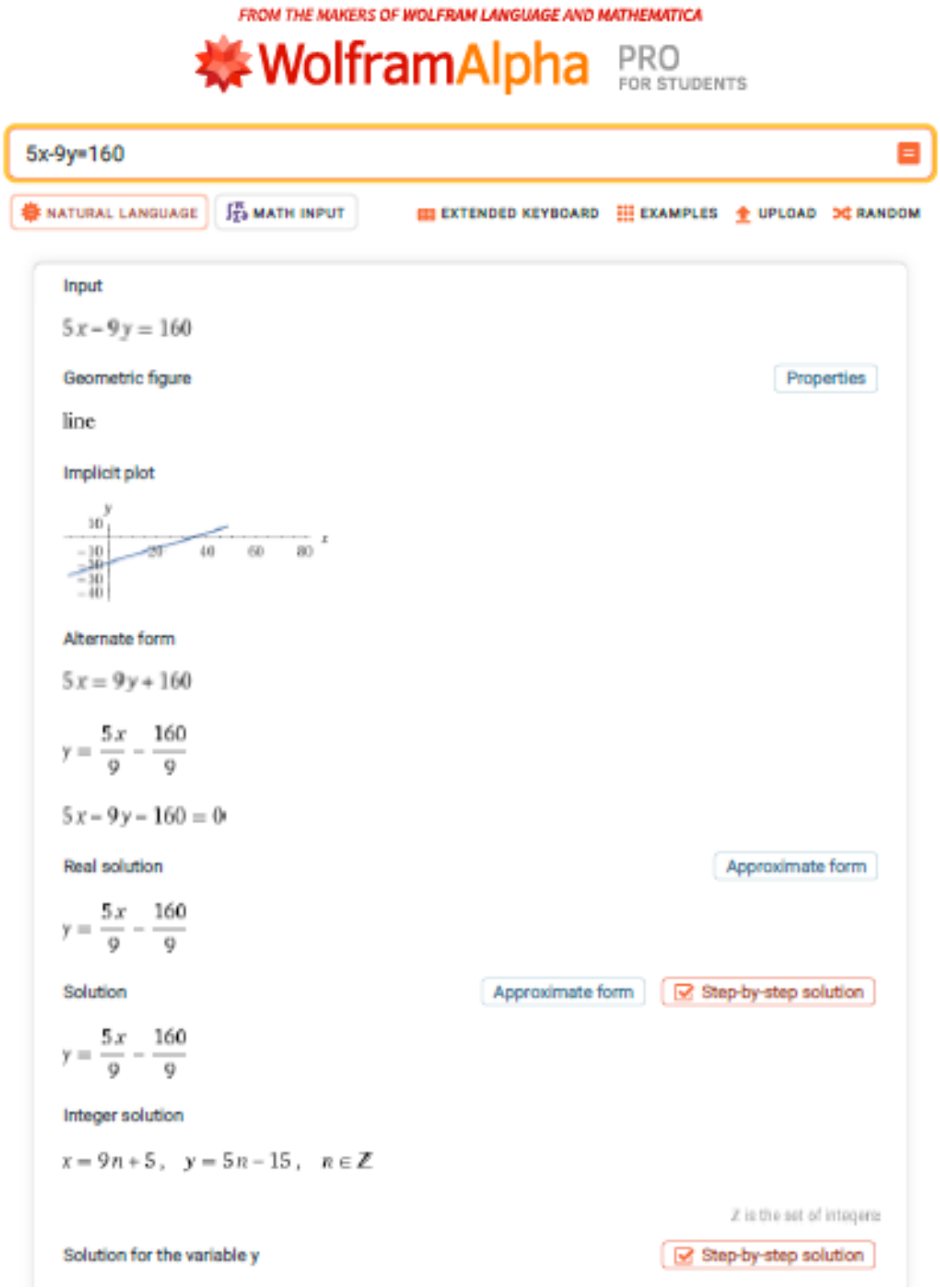
$$\begin{aligned} 1 &= 1 \cdot 5 - 1 \cdot (9 - 1 \cdot 5) \\ 1 &= 1 \cdot 5 - 1 \cdot 9 + 1 \cdot 5 \\ 1 &= 2 \cdot 5 - 1 \cdot 9 \end{aligned}$$

Se $2 \cdot 5 - 1 \cdot 9 = 1$ então $320 \cdot 5 - 160 \cdot 9 = 160$.

Com isso, a solução inicial é $F_0 = 320$ e $C_0 = 160$. E as soluções gerais são $F = 320 - 9t$ e $C = 160 - 5t$, $\forall t \in \mathbb{Z}$, determinando assim todas as soluções inteiras possíveis.

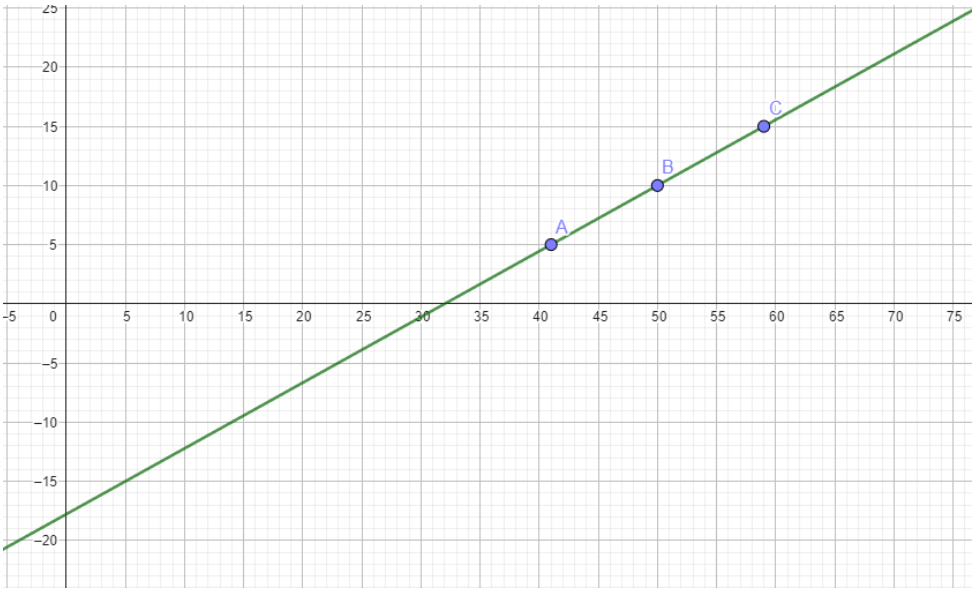
Na barra de comando do Wolfram Alpha se digitarmos $5x - 9y = 160$, tomando x para a escala Fahrenheit e y para a escala Celsius obtemos:

Figura 34 – Exemplo 55: $5x - 9y = 160$: comando e resposta



Podemos observar que as soluções inteiras estarão presentes no gráfico de uma reta no plano cartesiano conforme o que se segue. Os pares ordenados serão : $A = (41,5), B = (50,10), C = (59,15)$ e etc.

Figura 35 – Exemplo 55: $5x - 9y = 160$, ilustração das respostas no Plano Cartesiano



5 TEOREMA CHINÊS DOS RESTOS

O foco deste trabalho é o Teorema Chinês dos Restos e algumas de suas aplicações elementares com aplicações no Wolfran Alfha. Para esse fim, no capítulo anterior, abordamos diversos tópicos na revisão bibliográfica, entre os quais se destacam: o conjunto dos números inteiros e suas propriedades básicas, o máximo divisor comum, as congruências modulares e as equações diofantinas. Além disso, esses conteúdos foram tratados de forma mais aprofundada do que normalmente ocorre no ensino básico. Isso se deve ao fato de que, embora desempenham um papel fundamental na resolução de muitos problemas envolvendo números inteiros, esses temas são frequentemente subutilizados nesse nível de ensino.

Neste capítulo, apresentamos o Teorema Chinês dos Restos, bem como exemplos de suas aplicações. Acreditamos que os conteúdos abordados, da forma como serão apresentados, possam servir como material de apoio tanto para professores em sala de aula quanto para alunos em busca de recursos suplementares para a resolução de problemas — em especial, com vistas à participação em olimpíadas de Matemática.

Teorema 5.1 (Teorema Chinês dos Restos)**.** *Seja o sistema*

$$\begin{aligned} X &\equiv c_1 \pmod{m_1} \\ X &\equiv c_2 \pmod{m_2} \\ &\vdots \\ X &\equiv c_r \pmod{m_r} \end{aligned}$$

Se $mdc(m_i, m_j) = 1$*, para todo par* m_i*,* m_j *com* $i \neq j$ *e* $i, j \in \{1, 2, \ldots, r\}$*, então o sistema anterior possui solução módulo* $M = m_1 \cdot m_2 \ldots, m_r$*.*

Estas soluções são do tipo:

$$X = M_1 y_1 c_1 + \cdots + M_r y_r c_r + tM$$

em que $t \in \mathbb{Z}$*,* $M_i = \dfrac{M}{m_i}$ *e* y_i *é a solução de* $M_i Y \equiv 1 \pmod{m_i}$*, para todo* $i = 1, 2, \ldots, r$*.*

Para consultar a demonstração deste teorema podemos verificar nas obras:

- Aritmética, de Abramo Refez, Coleção PROFMAT
- Números: Uma Introdução à Matemática, Polcino

- Chinês dos Restos: Ensino e Aplicações, de Walace da Silva Glória, Universidade Federal do Amazonas - PROFMAT

Vejamos então, como aplicar este teorema para determinar soluções de diversos problemas. Primeiramente vamos relembrar como resolver uma congruência por inspeção.

Exemplo 56. Para cada item abaixo determine o menor inteiro positivo x que resolve a congruência:

a) $3x \equiv 1 \pmod{11}$

b) $5x \equiv 1 \pmod{29}$

Solução.

a) Considerando $x = 4$ podemos escrever: $3x = 3 \cdot 4 = 12 \equiv 1 \pmod{11}$, por isso $x = 4$ satisfaz a congruência.

b) Similarmente se usarmos $x = 6$ obtemos: $5x = 5 \cdot 6 = 30 \equiv 1 \pmod{29}$, por isso $x = 6$ satisfaz a congruência.

Exemplo 57. Há números que quando divididos por 3 e por 2 deixam restos iguais a 1. Desta classe de números, quantos e quais são os maiores do que 50, menores do que 100 e múltiplos de 7?

1ª Solução. O foco principal deste trabalho é o Teorema Chinês do Resto. Mas desde o início declarei a importância de valorizarmos as individualidades dos alunos. Por isso, neste caso veremos três soluções par a mesma questâo.

Por inspeção, podemos verificar que o 7 satisfaz a primeira condição, ou seja: quando divididos por 3 e por 2 deixam restos iguais a 1. Então a classe $x = 7 + 2 \cdot 3 \cdot t$ para $t \in \mathbb{Z}$ satisfaz a primeira condição.

De acordo com a segunda condição do problema precisamos ter que: $50 < x < 100$

$$\begin{aligned} 50 < \quad & 7 + 6 \cdot t \quad < 100 \\ 50 < 7 + 6t \quad & \text{e} \quad 7 + 6t < 100 \\ 43 < 6t \quad & \text{e} \quad 6t < 93 \end{aligned}$$

Concluindo que $t > 7,1$ e $t < 15,5$. Por isso verificamos que $t \in \{8, 9, 10, 11, 12, 13, 14, 15\}$.

Podemos observar que:

t	8	9	10	11	12	13	14	15
x	55	61	67	73	79	85	91	97

Desta relação encontramos vários valores de x e o único que é múltiplo de 7 é o 91.

2ª Solução. Pela primeira exigência do problema precisaremos determinar um valor para x tal que:

$$x \equiv 1 \pmod 3$$
$$x \equiv 1 \pmod 2$$

Observamos que as duas congruências possuem resto 1, e o $mmc(2,3) = 6$. Podemos reduzir o sistema a uma só congruência:

$$x \equiv 1 \pmod 6$$

Chegando a igualdade: $x = 6t + 1$ para $t \in \mathbb{Z}$. Considerando a segunda exigência do problema, precisamos de um múltiplo x de sete, ou seja:

$$x \equiv 0 \pmod 7$$
$$6t + 1 \equiv 0 \pmod 7$$
$$6t \equiv -1 \pmod 7$$

Sabendo da congruência $6 \equiv -1 \pmod 7$, podemos multiplicar com o raciocínio anterior:

$$6 \cdot 6t \equiv (-1) \cdot (-1) \pmod 7$$
$$36t \equiv 1 \pmod 7$$

Sabendo que $t = 7k + 1$ para $k \in \mathbb{Z}$, chegamos na igualdade: $x = 6(7k+1) + 1 = 42k + 7$. Agora vamos analisar a segunda condição $50 < x < 100$.

$$50 < 42k + 7 < 100$$
$$43 < 42k < 93$$

Concluindo que $k < 2,214...$ e $k > 1,023....$ Por isso teremos que $k = 2$, ou seja, $x = 42 \cdot 2 + 7 = 91$.

3ª Solução. Pela primeira exigência do problema precisaremos determinar um valor para x tal que:

$$x \equiv 1 \pmod 3$$
$$x \equiv 1 \pmod 2$$

Observamos também que o $mdc(2,3) = 1$. Pois isso, podemos aplicar o Teorema Chinês dos Restos e: $M = 2 \cdot 3$, $m_1 = 2$ e $m_2 = 3$. Passamos agora a determinar y_1 e y_2, tais que:

$$2y_1 \equiv 1 \pmod 3$$
$$3y_2 \equiv 1 \pmod 2$$

Por inspeção verificamos que $y_1 = 2$ e $y_2 = 1$. Assim as soluções serão do tipo:

$$x = 2 \cdot 1 \cdot 2 + 3 \cdot 1 \cdot 1 + 6t = 7 + 6t$$

Analisando a segunda exigência do problema obtemos:

$$50 < 7 + 6t < 100$$
$$43 < 6t < 93$$

Concluindo que $t < 15,5...$ e $t > 7,16....$ Por isso verificamos que

$$t \in \{8,9,10,11,12,13,14,15\}.$$

Podemos observar que:

t	8	9	10	11	12	13	14	15
x	55	61	67	73	79	85	91	97

Desta relação encontramos vários valores de x e o único que é múltiplo de 7 é o 91.

Exemplo 58. Determine a solução geral do sistema abaixo, e as soluções positivas x menores do que 100:

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$

1ª Solução

Se considerarmos cada congruência em separado observaremos que

1. Para $x \equiv 1 \pmod 3$ por inspeção vemos que:

   $x \in \{4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, \dots\}$

2. Para $x \equiv 2 \pmod 5$ por inspeção vemos que:

   $x \in \{7, 12, 17, 22, 27, 32, 37, 42, 47, 52, \dots\}$

3. Para $x \equiv 3 \pmod 7$ por inspeção vemos que:

   $x \in \{10, 17, 24, 31, 38, 45, 52, \dots\}$

   E o primeiro x que é comum nas três listas é 52, ou seja, que satisfaz as três equações, ou ainda, resolve o sistema de congruência. Mas há outros que também resolvem o sistema. Desde que eles satisfaçam o Teorema 5.1, ou seja:

   $$x = 52 + (\text{um múltiplo comum de 3, 5, 7})$$
   $$x = 52 + 3 \cdot 5 \cdot 7t = 52 + 105t \text{ para } t \in \mathbb{Z}.$$

   Observamos que este método não é prático. Ele funcionou pois, os números envolvidos são pequenos. Por isso, a solução do Teorema Chinês dos Restos é genérica.

2ª Solução.

Com o intuito de usar o teorema, observamos que $mdc(3,5) = mdc(3,7) = mdc(5,7) = 1$ e considerando: $M = 3 \cdot 5 \cdot 7 = 105$, $M_1 = 5 \cdot 7 = 35$, $M_2 = 3 \cdot 7 = 21$ e $M_3 = 3 \cdot 5 = 15$.

E a solução será do tipo: $x = 35 \cdot c_1 \cdot y_1 + 21 \cdot c_2 \cdot y_2 + 15 \cdot c_3 \cdot y_3 + M \cdot t$ para $t \in \mathbb{Z}$. Falta calcular os números y_i, $i = 1, 2, 3$:

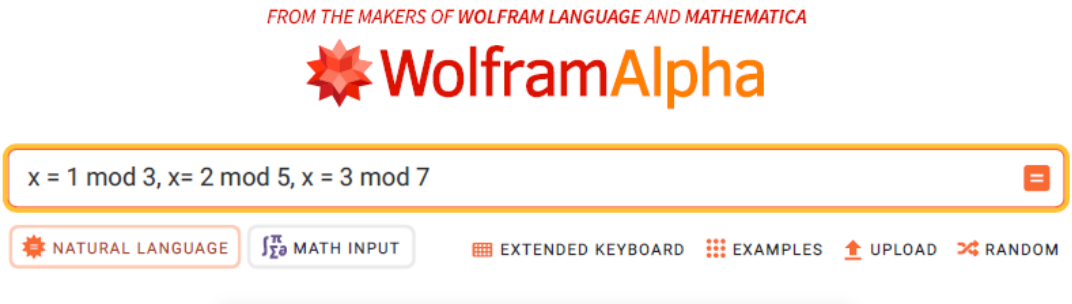
$$35y_1 \equiv 1 \pmod 3, \quad 21y_2 \equiv 1 \pmod 5 \quad \text{e} \quad 15y_3 \equiv 1 \pmod 7$$
$$35 \cdot 2 \equiv 1 \pmod 3, \quad 21 \cdot 1 \equiv 1 \pmod 5 \quad \text{e} \quad 15 \cdot 1 \equiv 1 \pmod 7$$
$$70 \equiv 1 \pmod 3, \quad 21 \equiv 1 \pmod 5 \quad \text{e} \quad 15 \equiv 1 \pmod 7$$

Resulta por inspeção $y_1 = 2$, $y_2 = 1$ e $y_3 = 1$. Pelo Teorema Chinês dos Restos, a solução geral é:

$$x = 35 \cdot 1 \cdot 2 + 21 \cdot 2 \cdot 1 + 15 \cdot 3 \cdot 1 + 105 \cdot t = 157 + 105t$$

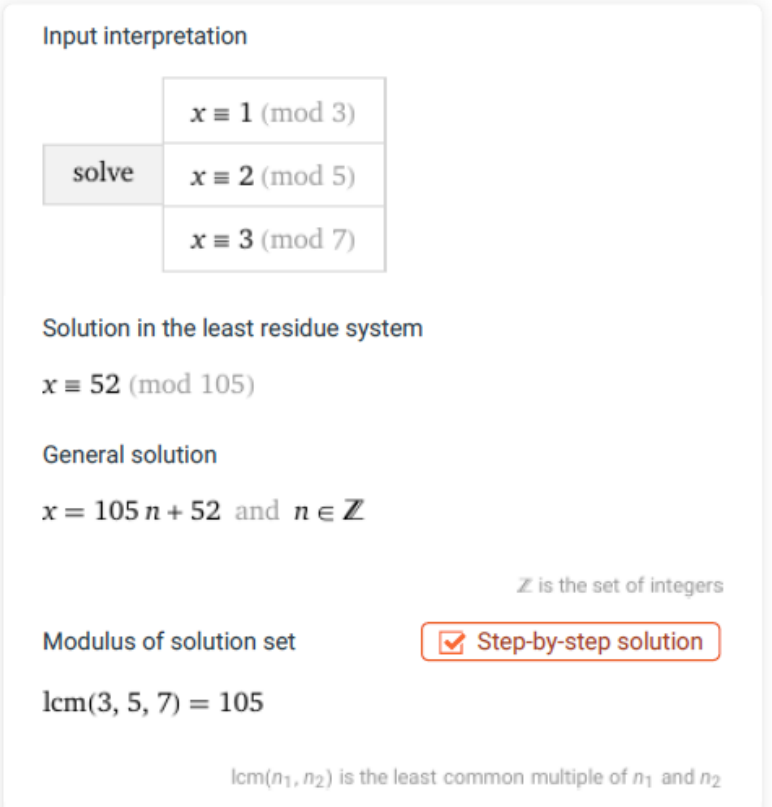
Como as soluções têm que ser menores do que 100, isto acontecerá apenas tomando $t = -1$, ou seja, $x = 157 + 105(-1) = 52$. Agora usando Wolfram Alpha, digitando na barra de comando, $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$:

Figura 36 – Exemplo 58: comando



Obtemos as soluções do sistema conforme segue:

Figura 37 – Exemplo 58: resposta



Exemplo 59. Na Introdução tinha comentado um problema antigo com os seguinte dizeres: “Há certas coisas cujo número é desconhecido. Se contá-los por três, restamos dois; aos cinco, temos três sobrando, e aos setes, sobram dois. Quantas coisas existem?”

Figura 38 – Original do problema de *Sun Tzu Suan Ching*

Solução.

Modernamente para responder a essa pergunta, deve-se resolver o seguinte sistema de congruências:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

E sua solução se aplica aos números naturais x tais que:

$$x = 2 \cdot 35 \cdot y_1 + 3 \cdot 21 \cdot y_2 + 2 \cdot 15 \cdot y_3 + 3 \cdot 5 \cdot 7 \cdot t,\ t \in \mathbb{Z}.$$

Pelo Teorema Chinês dos Restoss, calculamos os números y_i com as congruências abaixo:

$$35 \cdot y_1 \equiv 1 \pmod 3,\ 21 \cdot y_2 \equiv 1 \pmod 5 \text{ e } 15 \cdot y_3 \equiv 1 \pmod 7$$

Por inspeção achamos os valores dos y_i que são: $y_1 = 2, y_2 = 1$ e $y_3 = 1$

Concluímos que:

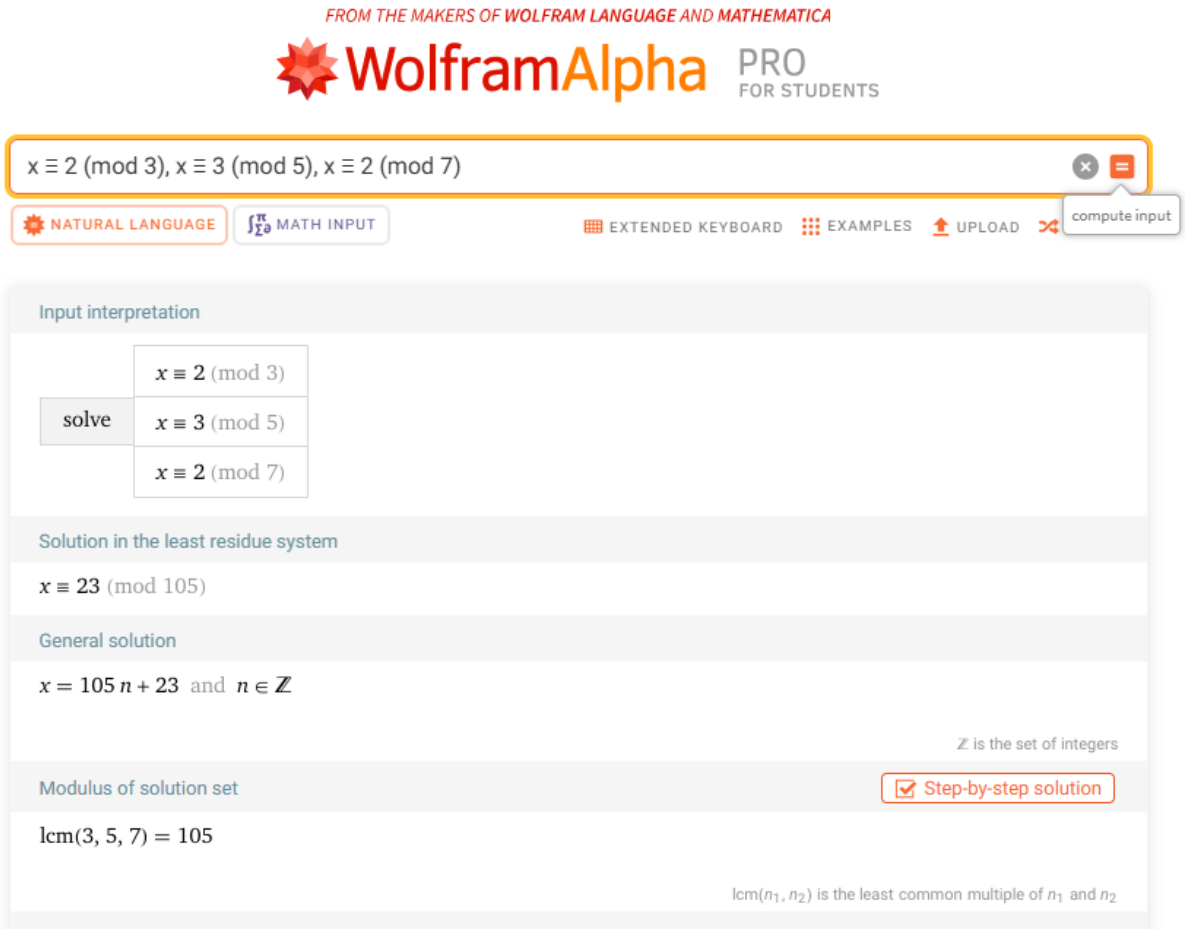
$$\begin{aligned} x &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 5 \cdot 7 + 3 \cdot 5 \cdot \cdot 7 \cdot t \\ x &= 233 + 105t \end{aligned}$$

Logo os menores valores positivos para essas coisas são tais como a tabela que se segue:

t	-2	-1	0
x	23	128	233

Digitando $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$ na barra de comando do Wolfram Alpha, obtemos as soluções do sistema conforme segue.

Figura 39 – Exemplo 59: comando e solução



Exemplo 60. Qual é o menor valor positivo que a variável x pode assumir desde que ele seja solução do sistema:

$$x \equiv 9 \pmod{11}$$
$$x \equiv 10 \pmod{13}$$

Solução: Aplicando o Teorema Chinês dos Restos deveremos determinar x tal que:

$$x = 9 \cdot 13 \cdot y_1 + 10 \cdot 11 \cdot y_2 + 11 \cdot 13t \text{ e } t \in \mathbb{Z}$$

$$13 \cdot y_1 \equiv 1 \pmod{11} \quad \text{e} \quad 11 \cdot y_2 \equiv 1 \pmod{13}$$
$$y_1 = 6 \quad \text{e} \quad y_2 = 6$$

Então concluímos que:

$$\begin{aligned} x &= 9\cdot 13\cdot 6+10\cdot 11\cdot 6+11\cdot 13\cdot t \\ x &= 702+660+143\cdot t \\ x &= 1362+143\cdot t \end{aligned}$$

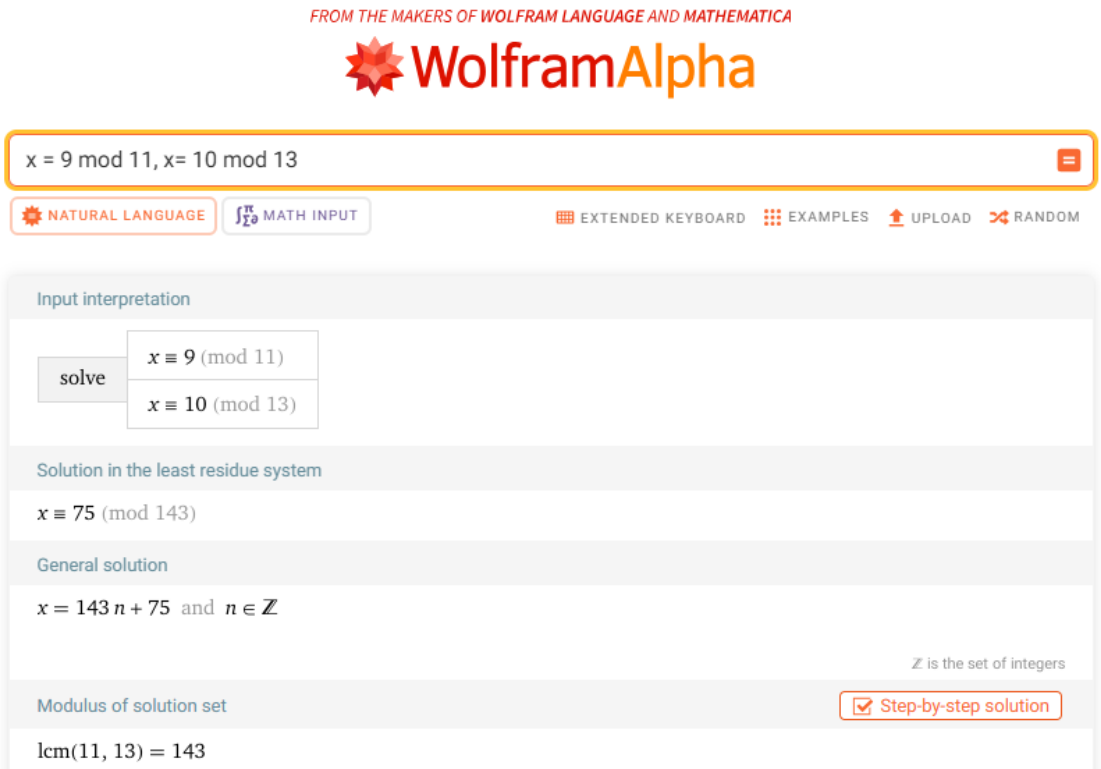
E as soluções gerais são $x = 1362 + 143t$. Precisamos soluções que assumam valores positivos:

t	0	-1	-2	-3	-4	-5	-6	-7	-8	- 9
x	1362	1219	1076	933	790	647	504	361	218	75

O menor valor positivo é $x = 75$.

Digitando $x \equiv 9 \pmod{11}$, $x \equiv 10 \pmod{13}$ na barra de comando do Wolfram Alpha, obtemos as soluções do sistema conforme segue.

Figura 40 – Exemplo 60: comando e solução



Exemplo 61. Existe uma classe de números que se forem divididos por 7 ou 5 deixam restos respectivamente 4 ou 3. Desta classe quais são os que estão entre 100 e 200?

1ª Solução.

Denotando essa classe de números por x, então temos:

$x \equiv 3 \pmod 5$

$x \equiv 4 \pmod 7$

Sabemos que a solução geral é $x = 3 \cdot 7 \cdot y_1 + 4 \cdot 5 \cdot y_2 + 5 \cdot 7 \cdot t$ para $t \in \mathbb{Z}$, em que os números y_1 e y_2 satisfazem

$$7 \cdot y_1 \equiv 1 \pmod 5 \qquad \text{e} \qquad 5 \cdot y_2 \equiv 1 \pmod 7$$
$$y_1 = 3 \quad \text{e} \quad y_2 = 3$$

Concluímos que os valores de x:

$$\begin{aligned} x &= 3 \cdot 7 \cdot 3 + 4 \cdot 5 \cdot 3 + 5 \cdot 7 \cdot t \\ x &= 63 + 60 + 35t \text{ e por isso } x = 123 + 35t \end{aligned}$$

Ou seja, a classe é descrita por $x = 123 + 35t$ para $t \in \mathbb{Z}$.

A questão pede os elementos da classe entre 100 e 200, então teremos que:

t	0	1	2
x	123	158	193

2ª Solução.

Considerando as congruências (i) $x \equiv 3 \pmod 5$ e (ii) $x \equiv 4 \pmod 7$ podemos escrever de (i) que : (iii) $x = 5r + 3$ para $r \in \mathbb{Z}$.

Substituindo este valor na congruência (ii) obtemos:

$$\begin{aligned} 5r + 3 &\equiv 4 \pmod 7 \\ 5r + 3 - 3 &\equiv 4 - 3 \pmod 7 \\ 5r &\equiv 1 \pmod 7 \end{aligned}$$

Verificamos por inspeção que uma solução é $r = 3$. E também podemos escrever $15r \equiv 1 \cdot 3 \pmod 7$ De modo que, temos:

$15 \equiv 1 \pmod 7$ e $r \equiv 3 \pmod 7$.

Concluímos que $r = 7s + 3$ para $s \in \mathbb{Z}$, e substituindo esta expressão na equação (iii):

$$\begin{aligned} x &= 5 \cdot (7s + 3) + 3 \\ x &= 18 + 35s \end{aligned}$$

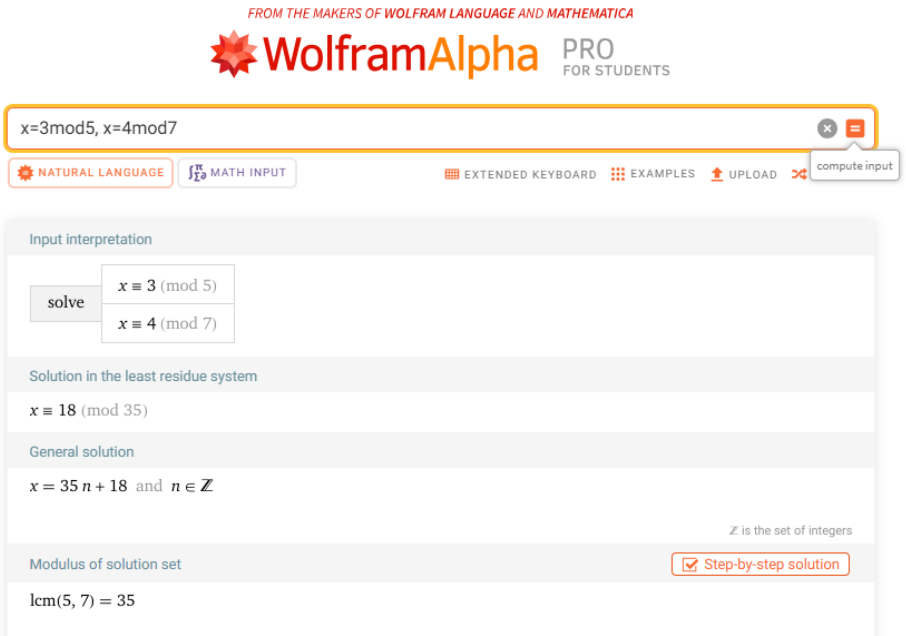
Pelo enunciado temos que determinar o valor de modo que:

$$\begin{aligned} 100 < 18 + 35s < 200 \\ 82 < 35s < 182 \\ 2,342... < s < 5,2 \end{aligned}$$

s	3	4	5
x	123	158	193

Digitando $x \equiv 3 \pmod 5$ e $x \equiv 4 \pmod 7$ na barra de comando do Wolfram Alpha obtemos:

Figura 41 – Exemplo 61: comando e solução



Exemplo 62. Determine a classe de números positivos x que satisfazem o sistema:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 5 \\ x &\equiv 1 \pmod 2 \end{aligned}$$

1ª Solução.

Por verificação observamos que o 7 satisfaz o sistema de congruência, pois:

$$7 = 2 \cdot 3 + 1$$

$$7 = 1 \cdot 5 + 2$$

$$7 = 3 \cdot 2 + 1$$

Somando os múltiplos do $mmc(3,5,2) = 30$ a esta solução particular também teremos soluções, ou seja, $x = 7 + 30 \cdot t$ para $t \in \mathbb{Z}$. Como a restrição do problema se aplica apenas para soluções positivas:

$$7 + 30t > 0$$

$$t > -0,23...$$

$$t = 0, 1, 2, ...$$

2ª Solução.

De acordo com o Teorema Chinês dos Restos, podemos escrever,

$$M = 3 \cdot 5 \cdot 2 = 30,\ M_1 = 5 \cdot 2 = 10,\ M_2 = 3 \cdot 2 = 6 \text{ e } M_3 = 3 \cdot 5 = 15$$

A solução geral fica desta forma.

$$x = 1 \cdot 10 \cdot y_1 + 2 \cdot 6 \cdot y_2 + 1 \cdot 15 \cdot y_3 + 3 \cdot 5 \cdot 2 \cdot t \text{ para } t \in \mathbb{Z}.$$

Para completar calculamos os números y.

$$\begin{array}{rcl} 10 \cdot y_1 & \equiv & 1 \pmod 3, \quad 6 \cdot y_2 \equiv 1 \pmod 5, \quad 15 \cdot y_3 \equiv 1 \pmod 2 \\ y_1 & = & 1 \qquad\qquad y_2 = 1 \qquad\qquad y_3 = 1 \end{array}$$

Para $t \in \mathbb{Z}$, podemos escrever que:

$$\begin{array}{rcl} x & = & 1 \cdot 10 \cdot 1 + 2 \cdot 6 \cdot 1 + 1 \cdot 15 \cdot 1 + 30 \cdot t \\ x & = & 10 + 12 + 15 + 30 \cdot t \\ x & = & 37 + 30 \cdot t \end{array}$$

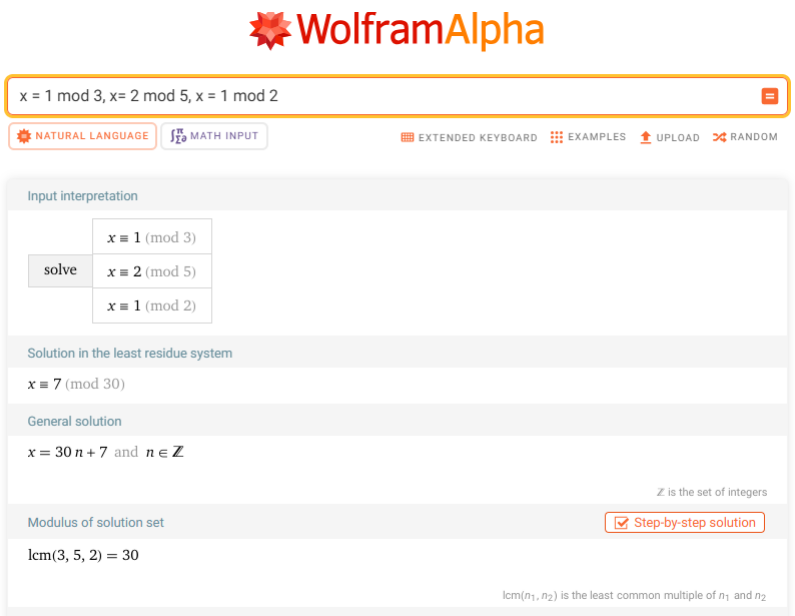
Pelo enunciado devemos determinar o valor de x de modo que,

$$\begin{aligned} 37+30t &> 0 \\ t &> -1,23... \end{aligned}$$

Por isso, t deve ser maior ou igual a -1

Digitando $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 1 \pmod 2$ na barra de comando do Wolfram Alpha, obtemos as soluções do sistema conforme segue.

Figura 42 – Exemplo 62: comando e solução



Exemplo 63. Em uma companhia de soldados, os soldados foram divididos em grupos:

- de 3 em 3 sobram 2
- de 4 em 4 sobram 3
- de 5 em 5 sobram 4
- de 7 em 7 sobram 6

Quantos soldados tem essa companhia se eles são menos de 800?

Solução.

De acordo com os exemplos anteriores e usando x para a quantidade desses sodados então:

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 4, \quad x \equiv 4 \pmod 5 \quad \text{e} \quad x \equiv 6 \pmod 7$$

Pelo Teorema Chinês dos Restos temos a solução geral.

$$x = 2\cdot 4\cdot 5\cdot 7\cdot y_1 + 3\cdot 3\cdot 5\cdot 7\cdot y_2 + 4\cdot 3\cdot 4\cdot 7\cdot y_3 + 6\cdot 3\cdot 4\cdot 5\cdot y_4 + 3\cdot 4\cdot 5\cdot 7\cdot t \quad t \in \mathbb{Z}$$

Precisamos de y_i tais que,

$$140\cdot y_1 \equiv 1 \pmod 3, \quad 105\cdot y_2 \equiv 1 \pmod 4, \quad 84\cdot y_3 \equiv 1 \pmod 5 \quad \text{e} \quad 60\cdot y_4 \equiv 1 \pmod 7$$

Então determinamos que: $y_1 = 2, y_2 = 1, y_3 = 4$ e $y_4 = 2$. Assim sendo a solução geral será da seguinte forma:

$$\begin{aligned} x &= 2\cdot 4\cdot 5\cdot 7\cdot 2 + 3\cdot 3\cdot 5\cdot 7\cdot 1 + 4\cdot 3\cdot 4\cdot 7\cdot 4 + 6\cdot 3\cdot 4\cdot 5\cdot 2 + 3\cdot 4\cdot 5\cdot 7\cdot t \\ x &= 560 + 315 + 1344 + 720 + 420t \\ x &= 2939 + 420t \end{aligned}$$

Pelo enunciado a quantidade de soldados é maior do que 0 e menor do que 800:

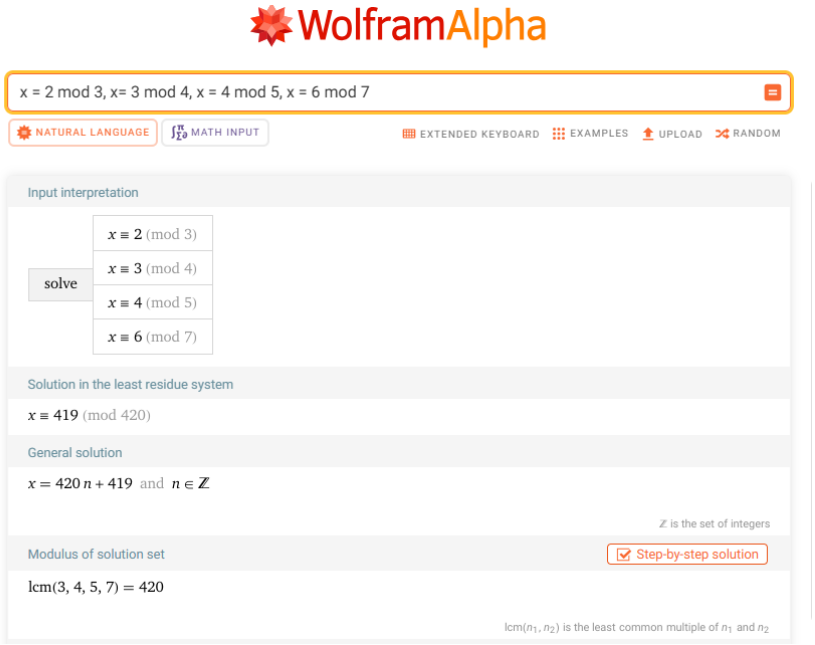
$$\begin{aligned} 0 &< 2939 + 420t < 800 \\ -6,99\cdots &< t < -5,09\ldots \end{aligned}$$

Por isso, obtemos $t = -6$.

$$\begin{aligned} x &= 2939 + 420(-6) \\ x &= 2939 - 2520 \end{aligned}$$

Concluímos então que a companhia tem 419 soldados. Digitando $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$, $x \equiv 4 \pmod 5$ e $x \equiv 6 \pmod 7$ na barra de comando do Wolfram Alpha obtemos a resposta:

Figura 43 – Exemplo 63: comando e solução



Exemplo 64. Determine as soluções particular e geral da congruência $3x \equiv 11 \pmod{2275}$ sabendo que $2275 = 25 \cdot 13 \cdot 7$.

1ª Solução.

Pensando na possibilidade da construção de um sistema para usar o Teorema Chinês dos Restos, observamos que $mdc(7,13) = mdc(7,25) = mdc(13,25) = 1$.

$$3x \equiv 11 \pmod{7}, \quad 3x \equiv 11 \pmod{13} \quad \text{e} \quad 3x \equiv 11 \pmod{25}$$

Precisamos adaptar o sistema para o Teorema, ou seja, determinar os inversos do 3 módulo 7, 13 e 25. Isso significa resolver cada equação modular abaixo:

$$3x \equiv 1 \pmod{7} \quad 3x \equiv 1 \pmod{13} \quad 3x \equiv 1 \pmod{25}$$

Calculamos os inversos $x_1 = 5, x_2 = 9$ e $x_3 = 17$ de cada equação acima, respectivamente. Logo, o sistema fica da seguinte forma:

$$x \equiv 11.5 \pmod{7}, \quad x \equiv 11.9 \pmod{13} \quad \text{e} \quad x \equiv 11.17 \pmod{25}$$
$$x \equiv 55 \pmod{7}, \quad x \equiv 99 \pmod{13} \quad \text{e} \quad x \equiv 187 \pmod{25}$$
$$x \equiv 6 \pmod{7}, \quad x \equiv 8 \pmod{13} \quad \text{e} \quad x \equiv 12 \pmod{25}$$

Começamos calcular os números do teorema, $M = 7 \cdot 13 \cdot 25 = 2275$, $M_1 = 13 \cdot 25 = 325$, $M_2 = 7 \cdot 25 = 175$ e $M_3 = 7 \cdot 13 = 91$. Efetuando as divisões dos $M_i s$ por 7, 13 e 25 obteremos os restos r_1, r_2 e r_3, respectivamente:

$$\begin{array}{rcllll} 325 & = & 7.46+3, & 175 = 13.13+6 & \text{e} & 91 = 25.3+16 \\ r_1 & = & 3 & r_2 = 6 & \text{e} & r_3 = 16 \end{array}$$

Obtemos um novo sistema mais fácil para determinar os y_i:

$$\begin{array}{rcllll} 3x & \equiv & 1 \pmod 7, & 6x \equiv 1 \pmod{13} & \text{e} & 16x \equiv 1 \pmod{25} \\ y_1 & = & 5 & y_2 = -2 & \text{e} & y_3 = 11 \end{array}$$

A solução geral é do tipo,

$$\begin{aligned} x &= M_1 \cdot c_1 \cdot y_1 + M_2 \cdot c_2 \cdot y_2 + M_3 \cdot c_3 \cdot y_3 + 7 \cdot 13 \cdot 25 \cdot t \text{ , para } t \in \mathbb{Z}. \\ x &= 325 \cdot 6 \cdot 5 + 175 \cdot 8 \cdot (-2) + 91 \cdot 12 \cdot 11 + 2275t \\ x &= 18962 + 2275t \end{aligned}$$

O menor valor positivo de x será quando utilizarmos o $t = -8$

$$\begin{aligned} x &= 18962 - 2275 \cdot (-8) \\ x &= 18962 - 18200 \\ x &= 762 \quad \text{(uma solução particular)} \end{aligned}$$

A solução geral é $x = 762 + 2275t$ para qualquer $t \in \mathbb{Z}$.

2ª Solução. Considere a congruência,

$$3x \equiv 11 \pmod{2275}$$

Podemos escrever a seguinte equação diofantina, $3x + 2275y = 11$. Sabendo que 3 e 2275 são primos entre si, implica que esta equação possui solução inteira. Então vamos calcular o inverso de 3 módulo 2275. Dividimos 2275 por 3: $2275 = 3 \cdot 758 + 1$. Por sorte, o resto é 1 e temos o número desejado 758.

Retomando a equação modular, multiplicamos por 758:

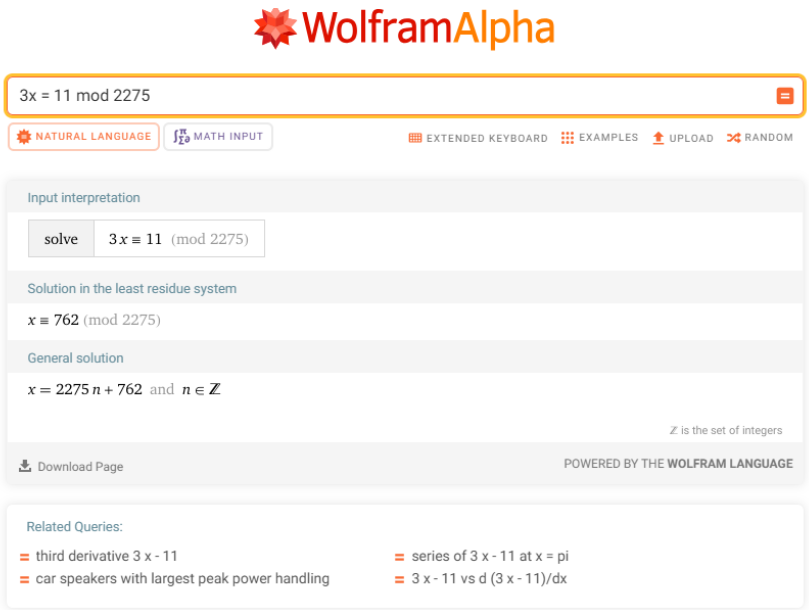
$$\begin{aligned} x &\equiv 758 \cdot 11 \pmod{2275} \\ x &\equiv 8338 \pmod{2275} \\ x &\equiv 762 \pmod{2275} \end{aligned}$$

De acordo com o algoritmo da divisão, as soluções particular e geral são:

$$x = 762 \quad \text{e} \quad x = 762 + 2275t, \text{ para } t \in \mathbb{Z}$$

Digitando $3x \equiv 11 \pmod{2275}$ na barra de comando do Wolfram Alpha obtemos as respostas:

Figura 44 – Exemplo 64: comando e solução



Exemplo 65 (ENQ - 2025 - II)**.** Três satélites artificiais orbitam a Terra e serão recalibrados sempre que passarem simultaneamente pelo meridiano de Greenwich. Seus ciclos orbitais são:
• Satélite A: Completa uma órbita a cada 7 horas e passou por Greenwich às 2 horas do dia 0.
• Satélite B: Completa uma órbita a cada 11 horas e passou por Greenwich às 3 horas do dia 0.
• Satélite C: Completa uma órbita a cada 10 horas e passou por Greenwich às 4 horas do dia 0.
Determine o primeiro instante t (em horas após o dia 0) em que os satélites serão recalibrados.
Solução. De acordo com as hipóteses do problema, os instantes de recalibragem serão dados

pelas soluções do seguinte sistema de congruências:

$$\begin{aligned} x &\equiv 2 \pmod 7 \\ x &\equiv 3 \pmod{11} \\ x &\equiv 4 \pmod{10} \end{aligned}$$

Calculando os máximos divisores comuns dois a dois com os modulares encontramos que, $mdc(7,11) = mdc(7,10) = mdc(11,10) = 1$, por isso usaremos o Teorema Chinês dos Restos. Do sistema acima, observamos que $c_1 = 2, c_2 = 3, c_3 = 4, M = 7 \cdot 11 \cdot 10 = 770, M_1 = 11 \cdot 10 = 110, M_2 = 7 \cdot 10 = 70, M_3 = 7 \cdot 11 = 77$. Precisamos determinar os inversos de 110, 70 e 77 nos seus respectivos módulos, ou seja, os y_{is} tais que

$$\begin{aligned} 110y_1 &\equiv 1 \pmod 7 \\ 70y_2 &\equiv 1 \pmod{11} \\ 77y_3 &\equiv 1 \pmod{10} \end{aligned}$$

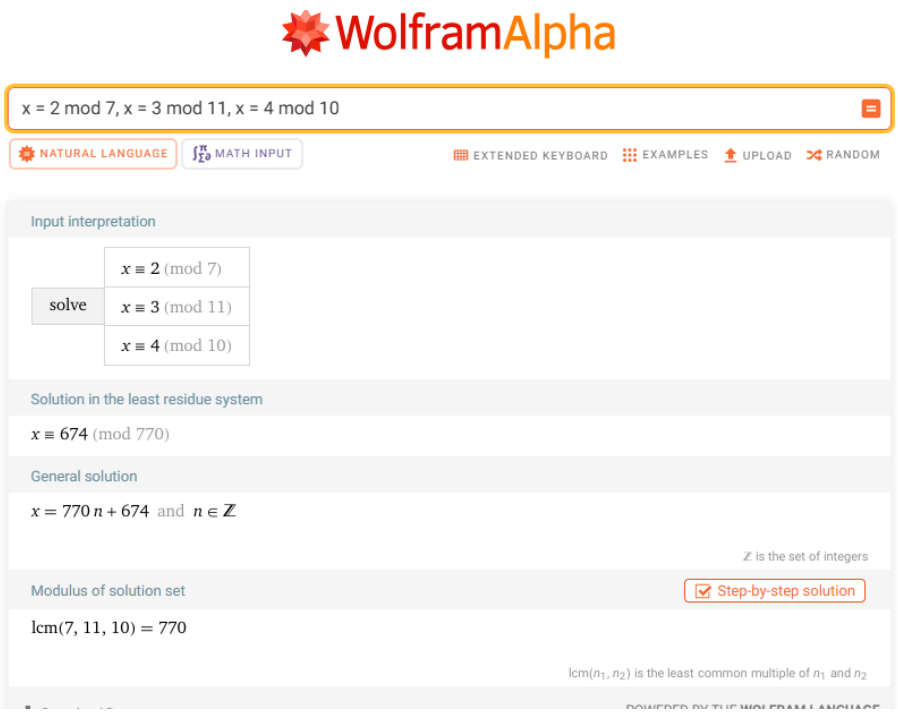
Por inspeção, determinamos que $y_1 = 3$, $y_2 = 3$ e $y_3 = 3$. Concluímos que as soluções do sistema são dadas por:

$$\begin{aligned} x &= 110 \cdot 2 \cdot 3 + 70 \cdot 3 \cdot 3 + 77 \cdot 4 \cdot 3 + 770t \\ x &= 674 + 770t, \text{ para } t \in \mathbb{Z} \end{aligned}$$

Portanto, o primeiro instante em que os três serão recalibrados se dará 674 horas após o dia 0.

Digitando $x \equiv 2 \pmod 7, x \equiv 3 \pmod{11}, x \equiv 4 \pmod{10}$ na barra de comando do Wolfram Alpha obtemos as respostas:

Figura 45 – Exemplo 65: comando e solução



Exemplo 66. A Teoria do Biorritmo é um conceito pseudocientífico que defende que a vida das pessoas é influenciada por três ciclos rítmicos — físico (23 dias), emocional (28 dias) e intelectual (33 dias) — que se iniciam no nascimento, e afetam o desempenho e o comportamento da pessoa. Embora a existência de ritmos biológicos seja reconhecida cientificamente, a teoria do biorritmo não possui base científica para prever o comportamento humano, sendo criticada pela comunidade médica e considerada por muitos como uma forma de pseudociência. Os estados físico, mental e emocional de uma pessoa oscilam periodicamente, a partir do dia do nascimento, em ciclos de 23 dias, 29 dias e 33 dias, respectivamente. Os dias mais positivos dos ciclos físico, mental e emocional são, respectivamente, o sexto, o sétimo e o oitavo de cada ciclo. Nos primeiros dez anos de vida de uma pessoa, quando os três ciclos ocorrem de forma mais positiva simultaneamente?

Solução. Considerando estas hipóteses podemos escrever o sistema de congruência,

$$\begin{aligned} x &\equiv 6 \pmod{23} \\ x &\equiv 7 \pmod{29} \\ x &\equiv 8 \pmod{33} \end{aligned}$$

Primeiro, os máximos divisores comuns $mdc(23,29) = mdc(23,33) = mdc(29,33) = 1$, então podemos usar o Teorema Chinês dos Restos. Pelo Teorema, podemos determinar a solução

geral $x = 957 \cdot 6 \cdot y_1 + 759 \cdot 7 \cdot y_2 + 667 \cdot 8 \cdot y_3 + 23 \cdot 29 \cdot 33 \cdot t$, $t \in \mathbb{Z}$. Determinando os números y_{is},

$$\begin{aligned} 957y_1 &\equiv 1 \pmod{23} \\ 759y_2 &\equiv 1 \pmod{29} \\ 667y_3 &\equiv 1 \pmod{33} \end{aligned}$$

Por inspeção, constatamos que $y_1 = 5, y_2 = 6$ e $y_3 = 19$. Então a solução geral é do tipo $x = 161972 + 22011t$, para $t \in \mathbb{Z}$. De acordo com as hipóteses do problema, desejamos determinar a menor solução positiva. Este fato se dará para $t = -7$, ou seja,

$$x = 161972 + 22011 \cdot (-7) = 7895 \text{ dias.}$$

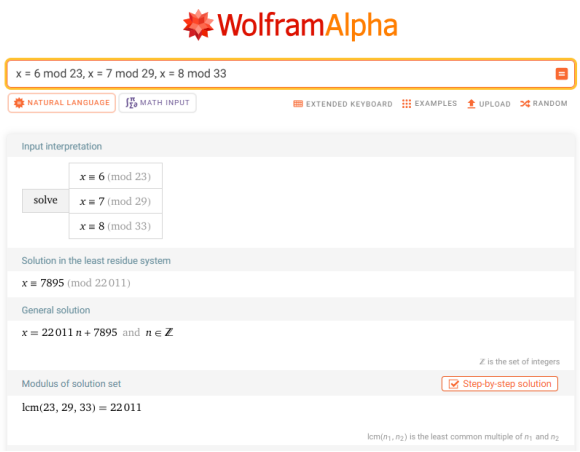
Os anos geralmente tem 365 dias, a menos dos anos bissextos. Por isso, fazendo uma aproximação para anos de 365 dias obtemos:

$$x = 7895 = 21 \cdot 365 + 230 \text{ dias.}$$

Concluímos então, que os três ciclos não ocorre durante os 10 primeiros anos de vida de uma pessoa.

Digitando $x \equiv 6 \pmod{23}, x \equiv 7 \pmod{29}, x \equiv 8 \pmod{33}$ na barra de comando do Wolfram Alpha obtemos as respostas:

Figura 46 – Exemplo 66: comando e solução



6 UMA INTRODUÇÃO DE APLICAÇÕES DA TEORIA DOS NÚMEROS NA CRIPTOGRAFIA

A palavra criptografia origina-se do grego kriptos = oculto ou secreto e de graphéin = escrever, portanto a palavra criptografia significa escrita oculta. O termo se refere ao conjunto de técnicas usadas para codificar uma mensagem e torná-la ininteligível para quem não possua a chave necessária para decifrá-la, ou seja, para quem não deva descobrir a mensagem. Trataremos de algumas aplicações práticas da congruência modular, destacando a criptografia. Nos dias atuais, em que grande parte das informações é trocada pela internet, a criptografia está presente garantindo a segurança no envio e recebimento de dados sigilosos. Informações transmitidas durante compras on-line, por exemplo, utilizam métodos criptográficos para assegurar que dados pessoais sejam acessados apenas por pessoas autorizadas.

Um dos métodos mais antigos e famosos de sistemas criptográficos foi um sistema usado na Roma antiga por Júlio César, denominado Cifra de César. O sistema consiste em substituir cada letra do alfabeto na mensagem original por outra letra do alfabeto, seguindo um padrão bem determinado. Uma das principais vantagens da Cifra de César é que tanto a codificação quanto a decodificação podem ser realizadas de forma simples. No entanto, sua principal desvantagem é o número limitado de possibilidades de substituição — apenas 26 padrões, ou seja, 26 chaves de codificação. O método de Júlio César é a substituição de cada letra na primeira linha pela letra correspondente da segunda linha da tabela a seguir:

Alfabeto	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifra	D	E	F	G	H	I	J	K	L	M	N	O	P
Alfabeto	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifra	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Ilustraremos nos exemplos que se seguem:

Exemplo 67. Texto: CHATGPT. Chave: +3

Solução.

Cifrado: FKDWJSW (Cifra de César)

Exemplo 68. Criptografe a palavra “SEGURANÇA” usando um deslocamento de +3.

Solução.

VHJXUDQFD

Exemplo 69. Uma mensagem foi cifrada com a Cifra de César de modo que puderam ler: "PDNH WUDLQ VWRS". Qual foi a mensagem enviada?

Solução.

Usando deslocamento 3, deslocamos cada letra 3 posições para trás no alfabeto. Fazendo da seguinte forma:

i) PDNH: P→M, D→A, N→K, H→E resultando em MAKE

ii) WUDLQ: W→T, U→R, D→A, L→I, Q→N resultando em TRAIN

iii) VWRS: V→S, W→T, R→O, S→P resultando em STOP

Portanto a mensagem decifrada é: MAKE TRAIN STOP

6.1 TEORIA BÁSICA

Poderíamos então definir Criptografia como conjunto de técnicas usadas para proteger informações, transformando-as em dados legíveis em um formato ilegível (chamado texto cifrado), de modo que apenas pessoas autorizadas possam entender o conteúdo.

1. Conceitos básicos:

   A criptografia se baseia na ideia de cifrar (codificar) e decifrar (desfazer a codificação) mensagens.

   i) Texto plano (ou texto claro): mensagem original, por exemplo, MENSAGEM SECRETA

   ii) Texto cifrado: mensagem transformada por um algoritmo de criptografia, por exemplo, QHQVDJHP VHFUHWD

   iii) Chave: É uma informação secreta usada pelo algoritmo para criptografar e descriptografar os dados, por exemplo, número, senha ou sequência de bits.

2. Tipos de criptografia:

   2.1. Criptografia Simétrica

   A criptografia simétrica, também conhecida como criptografia de chave única, é o tipo de criptografia em que a mesma chave é utilizada tanto para codificar

quanto para decodificar uma mensagem. Dessa forma, o emissor e o receptor devem possuir a mesma chave.

Esse sistema não é considerado seguro, pois, caso uma terceira pessoa descubra a chave de encriptação, ela terá acesso total à mensagem secreta. Além disso, o emissor e o receptor necessitam de um meio seguro para trocar informações sobre a chave, o que representa um desafio adicional.

i. A mesma chave é usada para cifrar e decifrar, por exemplo, AES, DES, RC4;

ii. Vantagem: rápida;

iii. Desvantagem: é difícil compartilhar a chave com segurança.

2.2. Criptografia Assimétrica

A criptografia de chave pública, também conhecida como criptografia assimétrica, consiste em um método que utiliza dois pares de chaves: uma chave pública e uma chave privada, as quais estão matematicamente relacionadas entre si. O emissor da mensagem possui um dos pares de chaves e o receptor, o outro. Para enviar uma mensagem, o emissor utiliza a chave pública do receptor, de modo que apenas este possa decriptar a mensagem, uma vez que somente ele detém a chave privada correspondente.

i. Usa duas chaves diferentes: uma pública (para cifrar) e uma privada (para decifrar), por exemplo, RSA, ECC.

ii. Muito usada em comunicações seguras na internet (como HTTPS).

2.3. Criptografia de Hash: a criptografia de hash é um algoritmo que transforma dados de qualquer tamanho em uma sequência de caracteres de tamanho fixo, única e irreversível. Ela serve para verificar a integridade de arquivos, garantir a segurança de senhas e autenticar documentos, pois qualquer alteração nos dados de entrada resultará em um hash completamente diferente. Ao contrário da criptografia tradicional, o hash não é reversível e seu propósito principal é criar um "resumo"único dos dados, e não a confidencialidade.

i. Não serve para decifrar, pois não há retorno possível;

ii. Transforma o texto em um resumo fixo, por exemplo, SHA-256, MD5;

iii. Muito usada para verificar integridade de dados ou armazenar senhas.

3. Aplicações da Criptografia:

    3.1. Transações bancárias e cartões de crédito;

    3.2. Comunicações seguras (e-mails e mensagens);

    3.3. Armazenamento seguro de senhas;

    3.4. Assinaturas digitais e certificados;

    3.5. Proteção de dados pessoais (LGPD).

Com o avanço da computação, surgiram métodos criptográficos cada vez mais complexos e difíceis de serem quebrados, já que os computadores passaram a executar algoritmos complexos em tempo reduzido. Entretanto, o avanço da criptoanálise também ocorreu de forma acelerada. Apesar da codificação e da decodificação terem se tornado mais rápidas com o apoio da computação, o problema da chave privada ainda persistia. Era necessário um meio seguro para que o emissor e o receptor combinassem previamente uma chave.

Em 1976, uma dupla de pesquisadores apresentou uma solução inovadora para o problema da troca segura de chaves. Esta dupla foi composta por Whitfield Diffie e Martin Hellman, que se destacaram como autores do artigo New Directions in Cryptography. Nesse trabalho, os dois cientistas propuseram a ideia de um sistema de criptografia assimétrica, introduzindo o conceito de utilização de pares de chaves distintas — uma pública e outra privada — para o processo de codificação e decodificação de mensagens. Embora o método ainda não tivesse sido implementado de forma prática à época, o estudo representou um marco fundamental no desenvolvimento da criptografia moderna.

Podemos então formalizar os mais variados códigos de envios de mensagens. O segredo das mensagens é garantido através da manutenção do segredo das chaves. O problema ficou estabelecido principalmente em como os correspondentes trocavam as chaves. Neste exemplo entrou a Criptografia em especial com o uso das noções de congruências.

Exemplo 70. Digamos que José e Pedro querem trocar entre si uma chave secreta usando celular.

Uma solução: O primeiro passo é a definição das chaves públicas e secretas. José e Pedro escolhem as chaves públicas que precisam ser números naturais: $r = 26$ e $s = 197$. A partir daí cada um deles escolhe um número natural que será a chave secreta pessoal: José vai ser $a_j = 5$ e Pedro será $a_p = 3$.

O segundo passo é a adaptação das chaves escolhidas, a etapa do José é calcular o único número $b_j < 197$ tal que:

$$26^{a_j} \equiv b_j \pmod{197}$$

observamos que a equação envolve as chaves públicas e o expoente é a chave secreta do José. A solução b_j é enviada para o Pedro.

$$26^5 = 26^2 \cdot 26^2 \cdot 26 \equiv 85 \cdot 85 \cdot 26 = 187850 \equiv 109 \pmod{197}$$

Determinando assim o $b_j = 109$. Pedro faz algo semelhante:

$$26^3 = 26^2 \cdot 26 \equiv 85 \cdot 26 = 2210 \equiv 43 \pmod{197}$$

Determinando assim o $b_p = 43$ enviado para o José.

O terceiro passo é a chave secreta principal do método. Para isso, a parte do José é calcular:

$$b_p^{a_j} \equiv (r^{a_p})^{a_j} = r^{a_p \cdot a_j} \equiv a \pmod{197}$$

Vejamos que b_p é a chave calculada por Pedro. O cálculo é:

$$43^5 \equiv (26^5)^3 \equiv 109^3 \equiv 148 \pmod{197}$$

Como era de se esperar, Pedro faz a conta:

$$b_j^{a_p} \equiv (r^{a_j})^{a_p} = r^{a_p \cdot a_j} \equiv a \pmod{197}$$

a chave secreta está determinada: $a = 148$.

Mas o sucesso deste método reside no fato de ser difícil descobrir qualquer dos três números a_j, a_p ou a conhecendo apenas os dados públicos r, s, b_j e b_p. Este problema se dá pois, dado um $n \in \mathbb{N}$, é relativamente fácil calcular o resto da divisão de um n^a por um certo m. Mas o oposto é mais difícil, ou seja, dado um y, tal que $y \in \mathbb{N}$, é difícil determinar a, tal que, y é o resto da divisão de n^a por m. Além da fundamentação teórica, este exemplo apresenta que demonstram o processo de encriptação e descriptação de mensagens.

O primeiro método de criptografia assimétrica foi desenvolvido em 1977 por Ronald Rivest, Adi Shamir e Leonard Adleman, pesquisadores do Massachusetts Institute of Techno-

logy (MIT), baseando-se nas ideias de Diffie e Hellman. Rivest e Shamir eram cientistas da computação, enquanto Adleman era matemático. O sistema criado ficou conhecido como RSA, em homenagem ao trio de pesquisadores. O funcionamento do RSA baseia-se na teoria dos números, especialmente nos conceitos de congruência modular e no estudo dos números primos. A criptografia assimétrica permite não apenas a transmissão segura de informações, mas também a autenticação da identidade do remetente. Além do RSA, outros métodos amplamente utilizados incluem Diffie-Hellman, DSA, ElGamal e o algoritmo de curvas elípticas (ECC).

Segundo Rousseau e Saint-Aubin (2015), o método RSA é utilizado para a transmissão de dados sensíveis, como informações de cartões de crédito ou dados bancários. Contudo, em mensagens muito extensas, o algoritmo exige cálculos extremamente longos e complexos, mesmo quando executados por computadores. Dessa forma, quando uma mensagem não necessita de proteção por um longo período, é possível optar por outros métodos de criptografia mais leves.

Entre os sistemas de criptografia empregados para o envio de e-mails, destacam-se o DES (*Data Encryption Standard*, ou seja, Padrão de Encriptação de Dados) e o AES (*Advanced Encryption Standard*, ou seja, Padrão de Encriptação Avançado). Ambos utilizam chaves privadas, o que significa que o emissor e o receptor devem compartilhar a mesma chave de encriptação. Para garantir maior velocidade e segurança, a troca da chave é frequentemente realizada por meio do algoritmo RSA.

A seguir, será apresentado mais detalhadamente o método RSA, com a explicação de seu funcionamento e exemplos de aplicação. Esse método utiliza a teoria das congruências modulares e as propriedades dos números primos. Assim, além da fundamentação teórica, serão apresentados exemplos práticos de encriptação e decriptação de mensagens.

6.2 MÉTODO RSA

O método RSA baseia-se, essencialmente, na escolha de dois números primos p e q, e no cálculo de seu produto $n = p \times q$. A segurança do método está em escolher números primos com muitos dígitos, pois para decodificar a mensagem é necessário fatorar o número n, que terá uma grande quantidade de dígitos. Atualmente, existem programas capazes de gerar números primos de grande magnitude; no entanto, não há algoritmo eficiente que consiga fatorar um número muito grande em um tempo viável. É importante destacar que a base matemática da

criptografia é aprendida ainda no Ensino Básico, e hoje está presente em praticamente todas as atividades realizadas na internet.

Proposição 71. *Considere a,b números naturais. Então temos que*

$$mdc(ma,mb) = m \cdot mdc(a,b)$$

Proposição 72. *Sejam a,b,n números inteiros. Temos que $mdc(n,ab) = 1$ se e somente se $mdc(n,a) = mdc(n,b) = 1$.*

Proposição 73. *Sejam a e n dois inteiros com a menor do que n. Se $mdc(a,n) = 1$, então existe um único $x \in \{1,2,3,...,n-1\}$ tal que, $ax \equiv 1 \pmod{n}$.*

Para analisarmos os últimos resultados junto com exemplos, precisaremos das seguintes definições:

Definição 74. A função ϕ (*lê-se fi*) de Euler, denotada por $\phi(n)$ determina a quantidade de números naturais menores do que n e relativamente primos com n. Define-se $\phi(1) = 1$.

Definição 75. Um sistema completo de resíduos módulo m é todo conjunto de números inteiros cujos restos pela divisão por m, são os números da sequência $1,2,3,...,m-1$, sem repetições e numa ordem qualquer.

Definição 76. Um sistema de resíduos módulo m é u conjunto de números inteiros $r_1, r_2, ..., r_s$ tais que:

i) $mdc(r_1,m) = 1$ qualquer que seja i

ii) r_i não é congruente a r_j se i é diferente de j

iii) Para cada n inteiro tal que, $mdc(n,m) = 1$, existe i tal que, n é congruente a r_i módulo m.

Teorema 6.1 (Teorema de Euler)**.** *Se a é menor do que m e $mdc(a,m) = 1$, então $a^x \equiv 1 \pmod{m}$, sendo que, $x = \phi(m)$*

As proposições, definições e teoremas anteriormente mencionadas possuem suas apresentações, demonstrações e aplicações em obras como: Fundamentos de Aritmética (Domingues, 1991), Aritmética (Hefez, 2014) e Introdução à Teoria dos Números (Santos, 2020)

Com estas definições, proposições, e teoremas podemos pensar em uma situação hipotética específica:

Exemplo 77. Duas amigas muito íntimas, Carla e Marla desejam se comunicar por códigos que garanta a confidencialidade na transmissão de informações. para conseguirem manter confidências decidiram usar o método RSA. Carla desejava enviar a mensagem M = 19 para a sua amiga Marla. Mas por segurança ela não podia simplesmente a remeter. Por isso ela e Marla escolheram um método secreto e seguro de envio de mensagens. o RSA.

Solução

Carla codificou a sua mensagem com o número $M = 19$. Marla que irá receber a mensagem escolheu dois números primos 7 e 13, calculou o número principal $n = 7 \cdot 13 = 91$.

Para enviar a mensagem M para Marla, Carla faz o código utilizando a chave pública de Marla: 91. Para isso Carla efetua o cálculo:

$$C \equiv M^x \pmod{91}$$

A letra x é exatamente um número entre 1 e $\phi(91) = 6 \cdot 12 = 72$. Outro critério para a escolha do x é que $\text{mdc}(x, 72) = 1$. A Carla escolheu $x = 17$ satisfazendo esses dois critérios.

Procede então, com argumentos para determinar o resto da divisão de 19^{17} por 91.

$$\begin{aligned} 19 &\equiv 19 \pmod{91}, \\ 19^2 &\equiv 19^2 \pmod{91} \end{aligned}$$

Sabendo que $19^2 = 361$, usamos a divisão euclidiana $361 = 3 \cdot 91 + 88$, e escrevemos:

$$\begin{aligned} 19^2 &\equiv 88 \pmod{91}, \\ 19^2 \cdot 19^2 &\equiv 88 \cdot 88 \pmod{91}, \\ 19^4 &\equiv 7744 \pmod{91} \end{aligned}$$

Mas dividindo $88^2 = 7744$ por 91 obtemos $7744 = 85 \cdot 91 + 9$. Por isto podemos escrever que:

$$\begin{aligned} 19^4 &\equiv 9 \pmod{91}, \\ 19^{4 \cdot 4} &\equiv 9^4 \pmod{91} \end{aligned}$$

Mas $9^4 = 6561 = 72 \cdot 91 + 9$ e por isso:

$$\begin{aligned} 19^{16} &\equiv 9 \pmod{91}, \\ 19^{16} \cdot 19 &\equiv 9 \cdot 19 \pmod{91}, \\ 19^{17} &\equiv 171 \pmod{91} \end{aligned}$$

Pela divisão euclidiana $171 = 1 \cdot 91 + 80$, escrevemos que:

$$19^{17} \equiv 80 \pmod{91}$$

Determinamos $C = 80$, então Carla envia a mensagem codificada para Marla.

A fim de decodificar a mensagem Marla calcula

$$M \equiv C^d \pmod{91}$$

para um certo d tal que satisfaz $d \cdot x \equiv 1 \pmod{\phi(n)}$. O valor de $\phi(91) = 72$ já foi calculado por Marla, só resta calcular:

$$d \cdot 17 \equiv 1 \pmod{72}$$

Usando o Algoritmo de Euclides obtemos que:

$$\begin{aligned} 72 &= 4 \cdot 17 + 4 \\ 72 - 4 \cdot 17 &= 4 \\ 17 &= 4 \cdot 4 + 1 \end{aligned}$$

Nessa parte, precisamos reunir as informações:

$$\begin{aligned} 1 &= 17 - 4 \cdot (72 - 17 \cdot 4) \\ 1 &= 17 - 4 \cdot 72 + 17 \cdot 16 \\ 1 &= 17 \cdot 17 - 4 \cdot 72 \end{aligned}$$

Chegamos no $d = 17$. Para decodificar a mensagem, Marla faz os cálculos para determinar o resto da divisão de 80^{17} por 91. Para chegar na resposta, precisamos começar com o seguinte

argumento:

$$\begin{aligned} 80 &\equiv 80 \pmod{91}, \\ 80^2 &\equiv 80^2 \pmod{91} \end{aligned}$$

Calculando $80^2 = 6800 = 70 \cdot 91 + 30$, determinamos:

$$\begin{aligned} 80^2 &\equiv 30 \pmod{91}, \\ 6400^3 &\equiv 30^3 \pmod{91}, \\ 6400^6 &\equiv 30^6 \pmod{91} \end{aligned}$$

Fazendo $30^6 = 729000000 = 8010989 \cdot 91 + 1$, chegamos:

$$\begin{aligned} 6400^6 &\equiv 1 \pmod{91}, \\ 6400^{12} &\equiv 1^2 \pmod{91}, \\ 6400^{12} \cdot 80^2 \cdot 80^2 \cdot 80 &\equiv 1 \cdot 30 \cdot 30 \cdot 80 \pmod{91}, \\ 80^{17} &\equiv 72000 \pmod{91} \end{aligned}$$

Verificamos que $72000 = 791 \cdot 91 + 19$, finalmente podemos escrever:

$$80^{17} \equiv 19 \pmod{91}$$

Assim a Marla conseguiu a mensagem da Carla: $M = 19$.

Usamos aqui um exemplo onde foram escolhidos por Marla, dois números primos 7 e 13 que são bem pequenos. Mas podemos programar um computador com este métodos a escolher dois números primos bem grandes. Sendo assim, os cálculos ficam mais trabalhosos e difíceis de determinar os outros números. O valor do número d é calculado pelo computador de Marla que conhece p e q, como também o número $\phi(n)$. Assim, ela decripta a mensagem.

Mas este trabalho tem como público-alvo estudantes do sexto ano do Ensino Fundamental ao terceiro ano do Ensino Médio, bem como professores que atuam nesse segmento da Educação Básica. Busca-se, com isso, proporcionar subsídios teóricos e metodológicos que possibilitem a leitura, o estudo inicial e o aprimoramento do conhecimento, favorecendo a construção de uma fundamentação teórica sólida voltada ao ensino e à aprendizagem da Matemática na Educação Básica.

7 SEQUÊNCIA DIDÁTICA

Agora passarei a considerar uma aplicação dos três fatores primordiais deste trabalho. Vejamos:

Exemplo 78. Uma escola envia informações sigilosas (como senhas de acesso ou notas de alunos) por meio do sistema de criptografia RSA. Um aluno autorizado recebe uma mensagem codificada que, ao passar pelo processo de criptografia, resultou no número 12. Esse número, por si só, não revela o conteúdo da mensagem, pois foi obtido a partir de um método matemático que utiliza conceitos como números primos e congruências. O desafio proposto é justamente o papel do destinatário autorizado: usando a chave correta e o procedimento matemático inverso (descriptografia), ele deve descobrir qual era a mensagem original antes de ser transformada em 12.

Solução:

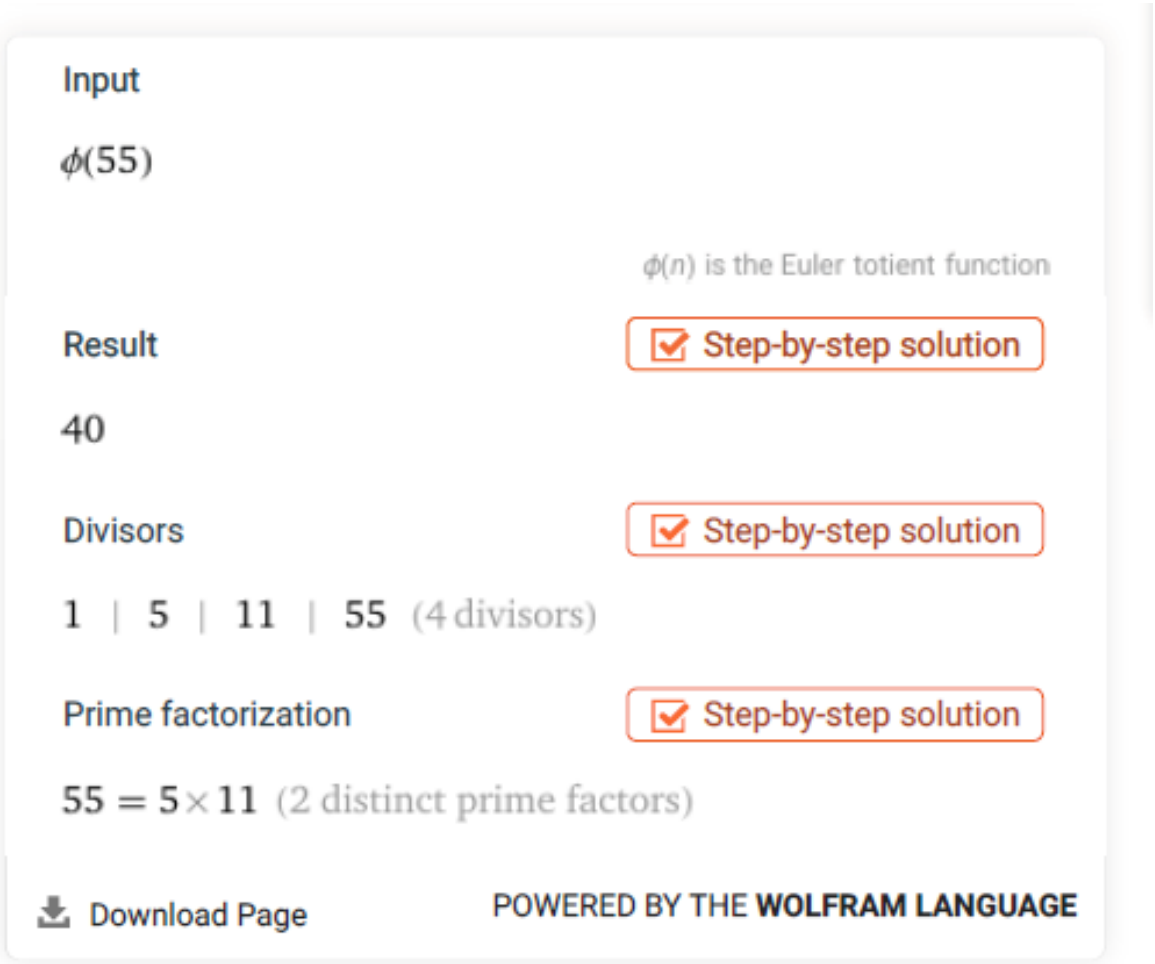
Este problema em vez de ser apenas um exercício abstrato ele representa uma situação real de segurança da informação, algo tão primordial em nossos dias e com ele conseguimos destacar a importância da Matemática na proteção de dados por meio do método RSA.

O método RSA tem como argumento a escolha de dois números primos bem grandes para ser a chave pública, que denotamos por n, que é igual ao produto desses dois primos. Por isso o valor de n acaba sendo também enorme. Este fato dificulta a fatoração de n. Mas como iremos apresentar os cálculos, o uso e a funcionalidade do método, vamos supor que o aluno escolheu dois números primos pequenos para facilitar as contas e informa a escola o número principal n, tal que, considerando p e q dois números primos, tais que, $p = 5$ e $q = 11$ então, $n = p \cdot q = 5 \cdot 11 = 55$.

O aluno ainda calcula: $\phi(55) = (5-1) \cdot (11-1) = 4 \cdot 10 = 40$

Figura 47 – Phi de Euler - barra de comando

Figura 48 – Phi de Euler - resposta



Com este n em mãos então, a escola que deseja codificar a mensagem $M = 23$, escolhe x que satisfaça as seguintes condições:

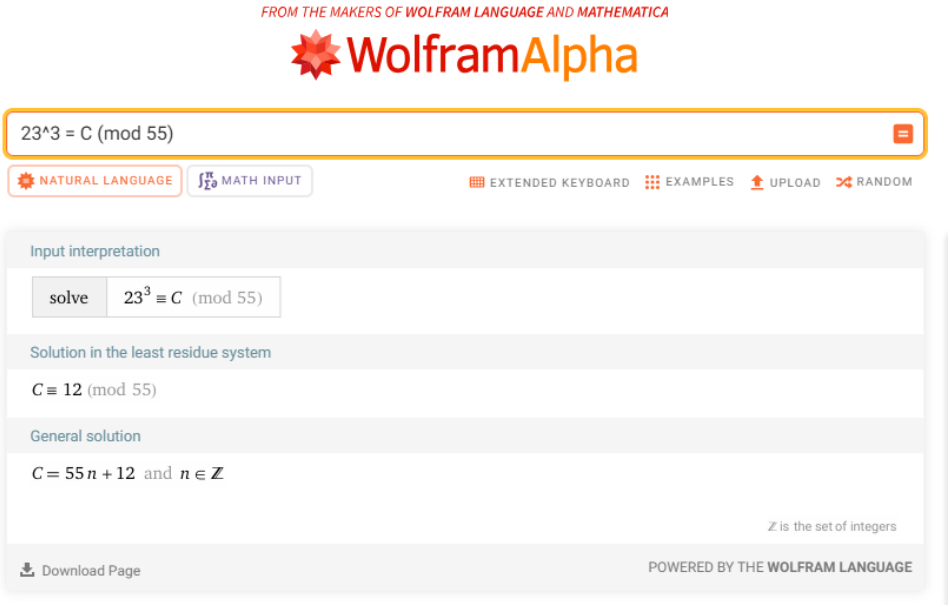
O número x está entre 1 e $\phi(55) = 40$, e ainda $\text{mdc}(x, 40) = 1$, de modo que ele resolva a congruência $C \equiv M^x \pmod{55}$.

Por isso, a escola escolhe $x = 3$. Para determinar o valor do C resolvendo a congruência:

$$C \equiv 23^x \pmod{55}$$

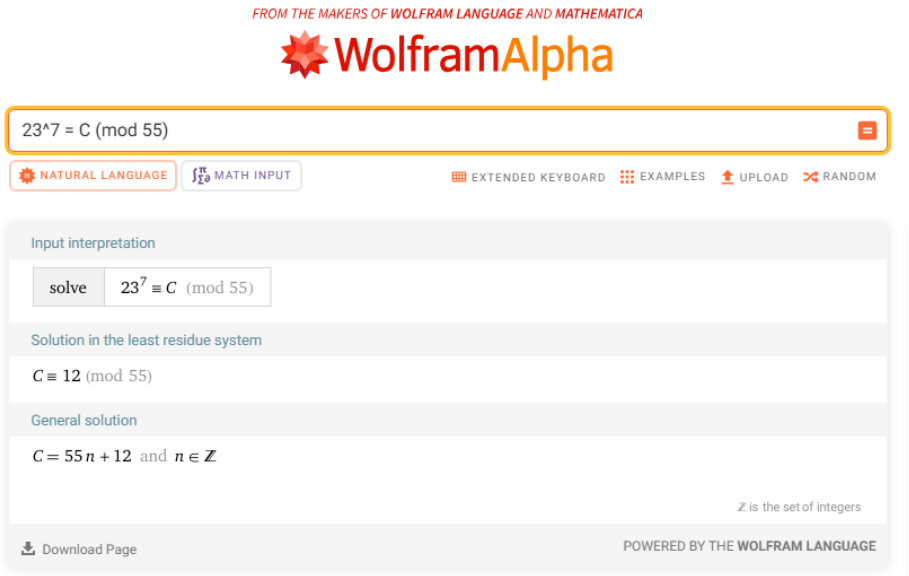
$$C \equiv 23^3 \pmod{55}$$

Figura 49 – Resolução da congruência: $23^3 \equiv C \pmod{55}$



Mas, se a escola escolhesse outro número que satisfaça as condições anteriores também daria $C = 12$, por exemplo, se escolher $x = 7$:

Figura 50 – Resolução da congruência: $23^7 \equiv C \pmod{55}$



A escola envia ao aluno a mensagem criptografada $C = 12$. O aluno começa o processo de descriptografia, isto é, ele precisa resolver a congruência modular:

$$M \equiv C^d \pmod{55}$$

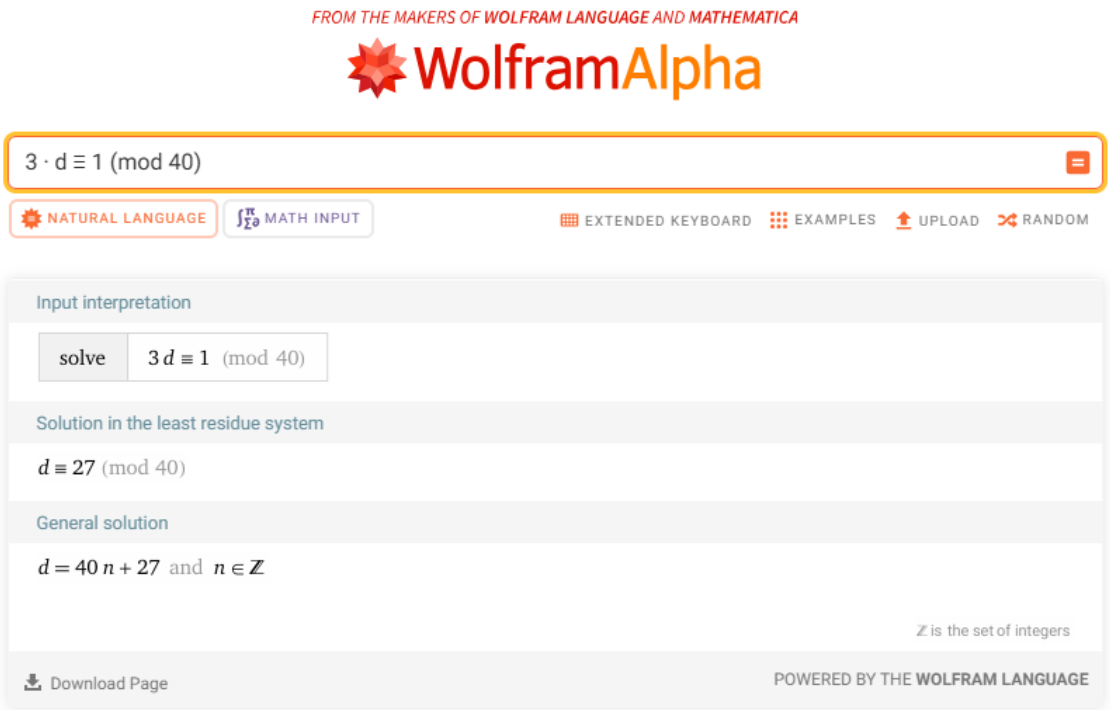
Para isso, o d deve satisfazer:

$$x \cdot d \equiv 1 \pmod{40} \qquad 3 \cdot d \equiv 1 \pmod{40}$$

Mas como o d depende do $\phi(55) = 40$ e este depende de p e q, que em modo geral são escolhidos entre os primos bem grandes. Consequentemente o valor do d também será bem grande. Mas como explicado anteriormente p e q foram escolhidos pequenos para efeito de demonstrações dos cálculos. Por isso, neste exemplo o valor do d não será tão grande.

Digitando na barra de comando do Wolfram Alpha, $3 \cdot d \equiv 1 \pmod{40}$, ele obtém:

Figura 51 – Resolução da congruência: $3 \cdot d \equiv 1 \pmod{40}$



Portanto, o aluno conclui que $d = 27$. Ele deve agora descriptografar a mensagem $C = 12$. Então, é necessário calcular o valor de M, que é a mensagem original tal que,

$$M \equiv C^d \pmod{55}$$

Para valores bem grandes da variável d, este é um processo muito longo, demorado e difícil. Por isso, recorremos ao Teorema Chinês dos Restos desmembrando o d em d_p e d_q, com os quais o aluno faz menos cálculos e resolve a questão. Para isso, ele monta um sistema auxiliar. Explicaremos teoricamente a montagem do sistema auxiliar, em alguns passos:

Passo 1: De acordo com a sétima propriedade das congruências vii), transformamos a equação $M \equiv C^d \pmod{55}$ no seguinte sistema,

$$\begin{cases} M \equiv C^d \pmod{5} \\ M \equiv C^d \pmod{11} \end{cases}$$

Podemos construir o sistema similar da seguinte maneira:

$$\begin{cases} M \equiv C^{d \pmod{4}} \pmod{5} \\ M \equiv C^{d \pmod{10}} \pmod{11} \end{cases}$$

Já com este sistema, trabalharemos com potências no contexto da aritmética modular. Essa teoria permite a substituição de potências com expoentes elevados por potências equivalentes com expoentes menores, preservando o mesmo resto na divisão modular. Tal procedimento é especialmente vantajoso, pois evita a realização de cálculos envolvendo potências muito grandes e simplifica significativamente a resolução dos problemas propostos. Sem modificar o resultado, conseguimos formalizar a descriptogafia com o uso do Teorema Chinês dos Restos.

Passo 2: Usaremos o Corolário do Pequeno Teorema de Fermat 4.7 para calcular congruência com valores menores e admitindo que p não divide C, se não, a mensagem seria nula, por isso escrevemos:

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

Analogamente, a equação funciona para o primo q: $C^{q-1} \equiv 1 \pmod{q}$

Passo 3: Para mostrar que $C^d \equiv C^{d \pmod{p-1}} \pmod{p}$, precisamos do algoritmo da divisão:

$$d = q(p-1) + d_p, \quad \text{onde } 0 \leq d_p < p-1$$

Elevando C a d, usando o passo anterior, algebricamente entendemos que:

$$C^d \equiv (1)^q \cdot C^{d_p} \equiv C^{d_p} \pmod{p}$$

Analogamente, repetimos o processo para o primo q e chamamos o resto da divisão de d_q.

Concluindo que

$$\begin{cases} M \equiv C^{d_p} \pmod 5 \\ M \equiv C^{d_q} \pmod{11} \end{cases}$$

Passo 4: O sistema auxiliar é

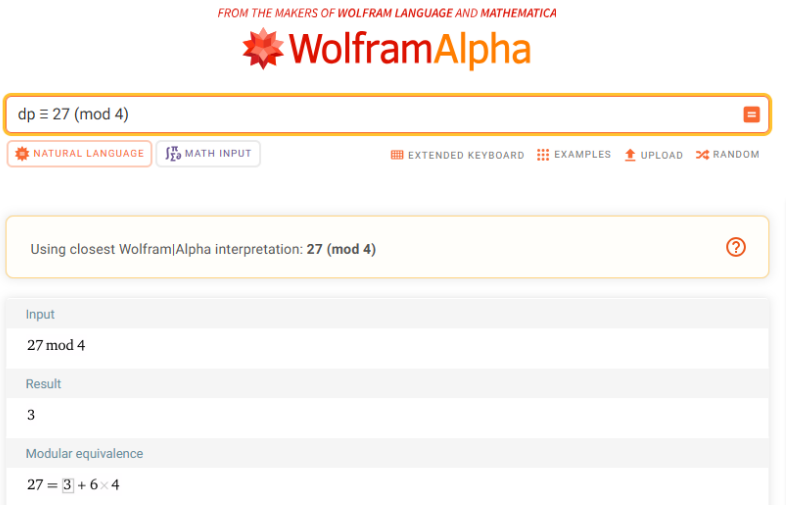
$$\begin{cases} M \equiv C^{d_p} \pmod 5 \\ M \equiv C^{d_q} \pmod{11} \end{cases}$$

Pelo passo 3 sabemos que é equivalente ao sistema inicial.

$$\begin{cases} M \equiv C^{d} \pmod 5 \\ M \equiv C^{d} \pmod{11} \end{cases}$$

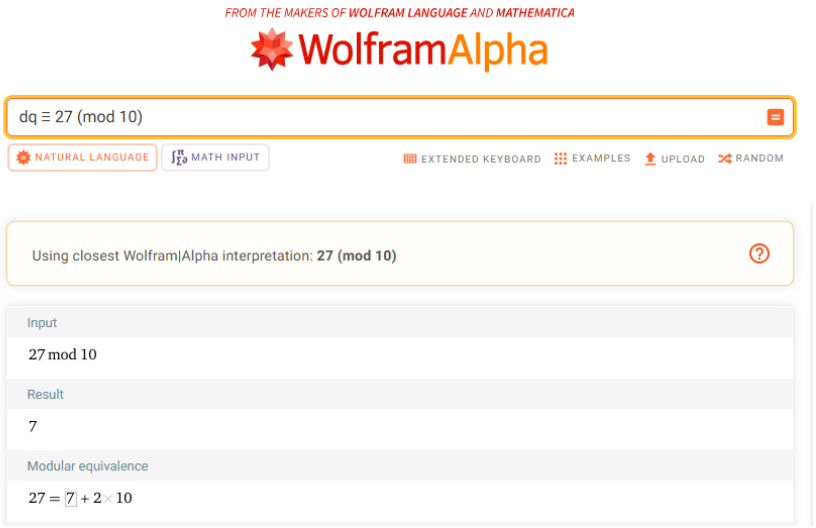
Vamos aplicar essa demonstração usando o Wolfram Alpha. Primeiro, iremos calcular os expoentes d_p e d_q. Digitando na barra de comando $d_p \equiv 27 \pmod 4$, o aluno obtém a resposta que $d_p = 3$

Figura 52 – dp Barra de Comando e Resposta



Agora, digitando na barra de comando do Wolfram Alpha $d_q \equiv 27 \pmod{10}$:

Figura 53 – dq na barra de comando e resposta



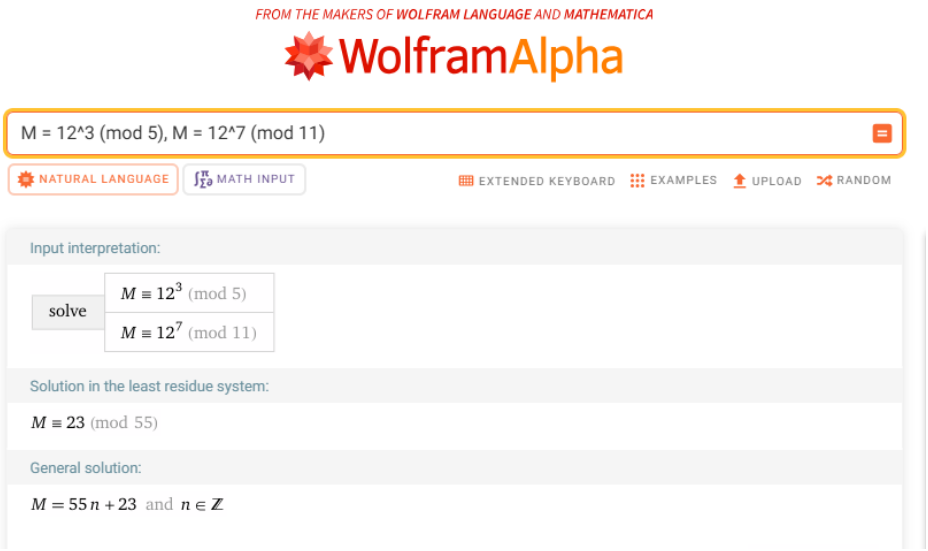
Obtemos a resposta que $d_q = 7$. Agora ele monta o seguinte sistema auxiliar de congruência,

$$\begin{cases} M \equiv C^3 \pmod 5 \\ M \equiv C^7 \pmod{11} \end{cases}$$

Vamos digitar na barra de comando do Wolfram Alpha

$$M = 12^3 \pmod 5, M = 12^7 \pmod{11}$$

Figura 54 – Barra de comando: Sistema de Congruência



Concluímos então que a mensagem original é 23.

Este problema em vez de ser apenas um exercício abstrato ele representa uma situação real de segurança da informação, algo tão primordial em nossos dias e com ele conseguiremos destacar a importância da Congruência e do Teorema Chinês dos Restos dentro da Teoria dos Números na proteção de dados pessoais.

Observamos aqui que a Congruência Modular é uma ferramenta excelente usando conceitos básicos da Teoria dos Números, permite estabelecer propriedades como o Teorema Chinês dos Restos, e utilização dos restos das divisões entre números inteiros. Conseguimos assim visualizar a sua aplicabilidade por meio da criptografia e em especial o Método RSA. Apresentamos os conceitos clássicos da teoria de congruência modular e algumas de suas propriedades. Ademais, ilustramos alguns cenários de aplicações as resoluções de problemas. A metodologia deste projeto fundamenta-se na motivação de professores e alunos engajados no Ciclo Dois do Ensino Fundamental e Ensino Médio, Por isso é bom relembrarmos que:

1. Contextualização Relevante: A escolha de trabalhar com criptografia RSA traz significado prático ao conteúdo matemático abstrato. O exemplo da escola enviando informações sigilosas conecta-se com a realidade digital dos estudantes, tornando o aprendizado mais motivador.

2. Integração de Ferramentas Tecnológicas: O uso sistemático do Wolfram Alpha como recurso de validação e apoio é bem estruturado. As capturas de tela ilustram claramente como os alunos podem verificar seus cálculos, promovendo autonomia e confiança.

3. Progressão Conceitual: A sequência dos conteúdos demonstra como conceitos aparentemente desconexos (números primos, congruências, Teorema Chinês dos Restos) convergem para uma aplicação prática sofisticada.

4. Precisamos então alinhar com a BNCC pois: A explicitação das habilidades da BNCC: (EM13MAT101, EM13MAT102, EM13MAT301, EM13MAT405) fortalece a proposta e facilita sua implementação por outros professores pois elas podem serem resumidas em:

• EM13MAT101: Interpretar e resolver problemas que envolvam números inteiros, divisibilidade e relações algébricas, utilizando diferentes estratégias e representações.

• EM13MAT102: Investigar propriedades numéricas e algébricas, estabelecendo conjecturas, generalizações e validações por meio de exemplos e contraexemplos.

• EM13MAT301: Resolver e elaborar problemas que envolvam congruência modular, explorando regularidades e padrões numéricos.

• EM13MAT405: Utilizar tecnologias digitais para investigar, modelar, simular e validar resultados matemáticos, analisando criticamente as soluções obtidas.

Como analisamos acima, podemos então introduzir: “Uma certa mensagem 12 foi criptografada pelo método RSA e enviada para o seu destinatário.”; e propor os seguntie passos:

- Motivação e Contextualização

• Problematização inicial: Discussão sobre segurança digital e necessidade de criptografia.

• Apresentação do desafio: “Como descriptografar a mensagem 12”.

• Exploração de conceitos prévios: Revisão de conceitos, números primos, divisibilidade e resto da divisão.

- Congruências e Função de Euler.

• Introdução às congruências: Definição, exemplos, propriedades básicas.

• Função ϕ de Euler: Conceito, cálculo, prática com Wolfram Alpha.

• Atividade prática: Exercícios de fixação com aplicação no Wolfram Alpha.

- Teorema Chinês dos Restos e Aplicação no RSA

• Apresentação do TCR: Enunciado e estratégia de resolução.

• Resolução do desafio: Descriptografia da mensagem passo a passo.

• Síntese e reflexão: Importância da matemática na segurança digital.

O exemplo é extremamente denso para estudantes do 6º ano 9º. Mas alguns alunos diferenciados dessas séries e que fazem cursos específicos como o PIC - OBMEP, poderão tirar muito proveito do artigo. Quando pensamos em relação a alunos do Ensino Médio, a complexidade deste texto é adequada. Este texto em especial deverá ajudar aos alunos em curso de formações continuadas extracurriculares em seu contínuo aprendizado da Teoria dos Números.

Ao avaliar da aprendizagem

• A observação da participação durante as atividades.

• A verificação dos cálculos intermediários.

• A análise dos registros no roteiro do estudante.

Com a aplicação de uma Avaliação Somativa conseguiremos:

• Problema desafio: Descriptografar uma nova mensagem usando RSA simplificado.

• Questões conceituais: Explicar por que o TCR funciona, importância dos números primos no RSA.

• Aplicação prática: Criar um sistema simples de criptografia.

Possíveis critérios de análise da aprendizagem pode-se fazer através da:

- Compreensão dos conceitos fundamentais (30%).

- Execução correta dos procedimentos (40%).

- Uso adequado do Wolfram Alpha (15%).

- Capacidade de explicar o raciocínio (15%).

Reserve tempo para os alunos refletirem sobre:

• “Qual foi a parte mais difícil? Por quê?”

• “Onde você pode usar esse conhecimento?”

• “O que você aprendeu sobre segurança digital?"

A Sequência Didática pode ser descrita com o seguinte roteiros de aulas:

Roteiro de Aulas:

1. Alinhamento com a BNCC: atentar pontos da BNCC durante as atividades as habilidades e competências relacionados com por exemplo:

- EM13MAT101: Interpretar situações-problema envolvendo números e suas operações.

- EM13MAT102: Utilizar propriedades dos números e operações.

- EM13MAT301: Resolver problemas com linguagem matemática e argumentação lógica.

- EM13MAT405: Utilizar tecnologias digitais na resolução de problemas matemáticos.

As habilidades deverão serem desenvolvidas ao longo das aulas por meio da resolução de problemas, uso de tecnologia e aplicação prática da matemática na criptografia.

2. Objetivo Geral

Compreender conceitos da Teoria dos Números aplicados à criptografia RSA.

Objetivos Específicos

- Revisar números primos, divisibilidade e resto da divisão

- Compreender congruências modulares - Estudar a função ϕ de Euler - Aplicar o Teorema Chinês do Resto

- Resolver um problema de descriptografia

- Utilizar o Wolfram Alpha como ferramenta de confirmação de resultados

3. Preparação do Professor

- Estudar previamente o uso do Wolfram Alpha

- Resolver completamente o problema proposto

- Antecipar dúvidas comuns (ex: interpretação de congruências)

4. Desenvolvimento de conceitos básicos em 10 aulas de 50 minutos cada.

Etapa 1: Introdução de conceitos e revisão de outros conceitos

Aula 1 – Problematização - Discussão: segurança digital e criptografia - Pergunta norteadora: “Como proteger informações na internet?”

Aula 2 – Apresentação do desafio - Proposta: “Como descriptografar a mensagem 12?”

- Debate: por que isso é difícil?

Aula 3 – Revisão de conceitos prévios

- Definição de Números Primos e determinação de uma sequência dos menores primos positivos.

Aula 4 – Revisão de conceitos prévios

- Divisibilidade: análise de critérios de divisibilidades

- Resto da divisão

- Exercícios contextualizados

Etapa 2 – Congruências Modulares

Aula 5 – Congruências:

- Definição e resoluções de exercícios exemplos

- Apresentação de Propriedades Básicas Fundamentais

- Exercícios

Aula 6 – Prática com tecnologia

- Uso do Wolfram Alpha para resolver os exercícios da Aula 4 e 5.

Etapa 3 – O Teorema Chinês do Resto e Aplicação no método RSA:

Aula 7 – Teorema Chinês do Resto

- Enunciado

- Estratégias de resoluções

- Resoluções com o Wolfram Alpha

Aula 8 – Função ϕ de Euler

- Conceito e utilização

- Cálculos e identificação de resultados

- Aplicações com tecnologia Wolfram Alpha

Aula 9 – Resolução do desafio proposto de início:

- Descriptografia passo a passo

- Uso do Wolfram Alpha

Aula 10 – Síntese e reflexão:

- Uma análise dos alunos sobre

- Importância da matemática na segurança digital

- Aplicações reais do RSA - Discussão final

A sequência didática apresenta núcleo conceitual sólido, contextualização significativa e integração tecnológica adequada. A articulação entre Teoria dos Números e criptografia, por meio do sistema RSA, demonstra ao estudante que a matemática transcende o ambiente escolar, constituindo elemento fundamental da segurança digital contemporânea. Além de desenvolver competências algébricas, a proposta estimula argumentação matemática, investigação e pensamento crítico, consolidando a aprendizagem significativa.

Então, dividindo a turma em dois grupos, de modo que um grupo faça a Criptografia e o outro a Descriptografia, pode-se utilizar 3 horas/aulas de 50 minutos cada, para os alunos resolverem a sua parte do problema e a cada cálculo que os alunos fizerem da função de Euler, resolução de congruência e sistema de congruência, mostrar a resolução no Wolfram Alpha como garantia que o método funciona graças à Aritmética Modular e que ainda o Teorema Chinês dos Restos minimiza os processos, ou seja, fazemos cálculos menores.

A aplicação dos conceitos de divisibilidade, potenciação modular, números primos, congruência e sistemas de congruências ocorre de forma integrada especialmente na resolução de problemas da Teoria dos Números e da criptografia. A divisibilidade permite analisar relações entre inteiros e identificar fatores comuns, sendo fundamental para reconhecer números primos, que são aqueles divisíveis apenas por 1 e por eles mesmos e que desempenham papel central em métodos criptográficos. A congruência estabelece uma relação entre números que deixam o mesmo resto na divisão por um módulo, possibilitando simplificar cálculos envolvendo inteiros grandes. A potenciação modular, por sua vez, utiliza propriedades das congruências para calcular potências elevadas de maneira eficiente, reduzindo resultados ao resto da divisão por um módulo. Já os sistemas de congruências permitem determinar um número que satisfaça simultaneamente várias condições modulares, sendo resolvidos, por exemplo, pelo Teorema Chinês dos Restos, o que torna possível acelerar cálculos e garantir segurança e eficiência em aplicações matemáticas e computacionais.

8 CONSIDERAÇÕES FINAIS

Uma célebre frase atribuída a Nikolai Lobachevsky (1792–1856) afirma que: “Não há ramo da matemática, por mais abstrato que seja, que um dia não possa ser aplicado a fenômenos do mundo real.” Essa citação expressa a convicção do matemático russo de que a matemática, mesmo em seus níveis mais teóricos, possui potencial para aplicações práticas em diferentes contextos.

O significado da frase revela a crença de Lobachevsky de que, embora a matemática possa parecer puramente abstrata, ela mantém uma relação intrínseca com o mundo físico e, em algum momento, encontrará formas de descrever, representar e modelar a realidade.

O impacto dessa visão é notável, pois evidencia sua filosofia matemática, que valorizava a conexão entre a abstração teórica e a aplicabilidade prática. Essa perspectiva antecipou um princípio fundamental da matemática e da física modernas: a utilidade universal das ideias matemáticas na compreensão e explicação dos fenômenos do mundo real.

Neste texto desenvolvemos vários assuntos como por exemplo a Álgebra que em suma é teórica, mas que pudemos visualizar de várias formas a sua aplicabilidade.

Podemos concluir em três pontos:

i) Introdução

   O presente projeto tem como propósito o desenvolvimento de atividades voltadas ao treinamento para olimpíadas de matemática, bem como a oferta de oficinas destinadas a alunos interessados em aprofundar seus conhecimentos além do conteúdo regularmente abordado em sala de aula. A iniciativa visa estimular o raciocínio lógico, o pensamento crítico e o interesse pela Matemática, contribuindo para a formação de estudantes mais autônomos e preparados para desafios acadêmicos e competitivos.

ii) Justificativa

   A proposta surgiu a partir da necessidade de incentivar os estudantes a aprimorarem seu desempenho em olimpíadas de Matemática e, consequentemente, enfrentarem Provas, Vestibulares e as etapas do Exame Nacional do Ensino Médio (ENEM) com maior segurança e tranquilidade.

   Observa-se que o conteúdo referente às congruências modulares, por exemplo, não integra o currículo do Ensino Básico, apesar de sua base teórica ser introduzida ainda no Ensino Fundamental. O domínio desse conhecimento representa uma ferramenta de

grande utilidade na resolução de problemas matemáticos, permitindo abordagens mais rápidas, seguras e eficientes.

Além disso, a resolução de exercícios utilizando congruências modulares possibilita ao aluno empregar estratégias diversas para alcançar o resultado esperado, o que se torna um diferencial importante em olimpíadas como a Canguru, OBMEP e OBM, nas quais o fator tempo é decisivo. Assim, acredita-se que o ensino desse conteúdo pode contribuir significativamente para o desempenho dos participantes.

iii) Objetivos

3.1 Objetivo Geral: Promover o estudo e a aplicação das Congruências Modulares e do Teorema Chinês dos Restos como ferramenta de apoio à resolução de problemas matemáticos, com foco na preparação para olimpíadas e avaliações externas. Utilizando um método computacional para justificar as soluções.

3.2 Objetivos Específicos:

Incentivar o interesse dos alunos pela Matemática por meio de oficinas e treinamentos específicos;

Explorar o uso das congruências modulares na resolução de problemas práticos e teóricos;

Desenvolver o raciocínio lógico e a autonomia intelectual dos estudantes;

Preparar os participantes para competições e avaliações, aprimorando suas estratégias de resolução e gestão do tempo durante as provas. A partir daí é esperado que eles consigam desenvolver um maior raciocínio lógico nas provas do ENEM, concursos e etc, bem como em todas as etapas de suas atividades.

REFERÊNCIAS

CARRAHER, T. N.; CARRAHER, D. W.; SCHLIEMANN, A. L. D. **Na vida dez, na escola zero**. São Paulo: Cortez, 1988.

DOMINGUES, H. H. **Fundamentos de Aritmética**. São Paulo: Atual, 1991.

HEFEZ, A. **Aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2014. (Coleção PROFMAT).

HEFEZ, A. **Iniciação à Aritmética**. Rio de Janeiro: IMPA/OBMEP, 2015.

SANTOS, J. P. d. O. **Introdução à Teoria dos Números**. 3. ed. Rio de Janeiro: IMPA, 2020.