Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Soluções de certas congruências quadráticas

Renato dos Santos Resende Fortes

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Martinho da Costa Araújo**

Trabalho financiado pela Capes

Cuiabá - MT

maio de 2017

Soluções de certas congruências quadráticas

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Renato dos Santos Resende Fortes e aprovada pela comissão julgadora.

Cuiabá,26 de maio de 2017

Prof. Dr. Martinho da Costa Araújo
Orientador

Banca examinadora:

Prof. Dr. Martinho da Costa Araújo.
Prof. Dr. José de Arimatéia Fernandes.
Prof. Dr. Aldi Nestor de Souza.

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título **de Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

F738s Fortes, Renato dos Santos Resende.
Soluções de certas congruências quadráticas / Renato dos Santos Resende Fortes. -- 2017
x, 82 f. ; 30 cm.

Orientador: Prof. Dr. Martinho da Costa Araújo.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2017.
Inclui bibliografia.

1. Congruências Quadráticas. 2. Símbolo de Legendre. 3. Resíduos Quadráticos. I. Título.

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

Dissertação de Mestrado defendida em 26 de maio de 2017 e aprovada pela banca examinadora composta pelos Professores Doutores

Prof. Dr. Martinho da Costa Araujo.

Prof. Dr. Aldi Nestor de Souza.

Prof. Dr. José de Arimatéia Fernandes.

Dedico este trabalho à minha mãe Tereza dos Santos de Souza e meu pai Jamil Resende Fortes, meus maiores exemplos de superação e perseverança, que apesar das dificuldades souberam transmitir toda sua sabedoria e apoio em todos os momentos.

Agradecimentos

Agradeço à Deus pela conquista. Aos meus pais, Tereza dos Santos de Souza e Jamil Resende Fortes, pelo apoio durante toda minha vida e pelo esforço para garantir esse momento. A todas as pessoas que contribuíram com o meu crescimento. Ao André Martins Gonçalves e Cristiano Antônio dos Reis, meu muito obrigado pelo suporte e a todos meus amigos pelos momentos de alegria e de descontração. Aos meus colegas de curso e aos meus professores, em especial ao meu orientador Professor Martinho da Costa Araújo, meus agradecimentos pelos momentos de formação. Aos que, apesar de não serem aqui citados, mas que estiveram presentes em minha vida discente, meus agradecimentos.

A aprendizagem se realiza através da conduta ativa do aluno, que aprende mediante o que ele faz e não o que faz o professor.

Ralph W.Tyler.

Resumo

Neste trabalho temos como objetivo determinar as soluções de algumas congruências quadráticas da forma $x^2 \equiv a \pmod{p^k}$, onde p é um primo e k um número natural e da congruência $x^2 \equiv a \pmod{m}$, onde m é um número composto. Apresentaremos o Algoritmo de Tonelli-Shanks para resolver congruências $x^2 \equiv a \pmod{p}$, para p primo impar. Como aplicação determinaremos as soluções inteiras da equação $x^2 - py = a$.

Palavras chave: Congruências Quadráticas; Símbolo de Legendre, Resíduos Quadráticos.

Abstract

In this paper we intend to determine the solutions of some quadratic congruences of the form $x^2 \equiv a \pmod{p^k}$, in which p is a prime and k a natural number and the congruence $x^2 \equiv a \pmod{m}$, in what respect m is a compound number. We will present the Tonelli-Shanks algorithm to solve congruences $x^2 \equiv a \pmod{p}$, for p odd cousin. As the application will determine the entire solutions of the equation $x^2 - py = a$.

Keywords: Quadratic congruences; Legendre's symbol; Quadratic Residue.

Sumário

Introdução

Existe uma enorme dificuldade na resolução de Congruências Quadráticas, pois não há uma fórmula geral para suas soluções, diferentemente do que acontece com Congruências Lineares. Antes de tentarmos achar as soluções de uma Congruência Quadrática, precisamos saber se a mesma é solúvel. Segundo Rocha (2010) "a Lei da Reciprocidade Quadrática lida com a solubilidade de Congruências Quadráticas", ou seja, a Lei da Reciprocidade Quadrática se faz necessário para determinar se a Congruência Quadrática pode, ou não, ser resolvida.

Sendo feito uma pesquisa bibliográfica do assunto em Rosen (2011), Said (1975), Hefez (2013), Santos (2011), Oliveira (2011), Vinogradov e Bernardo (1977) ficou claro, que para resolvermos Congruências Quadráticas, será necessário classificá-las por casos, tendo assim uma melhor compreensão, para entendermos quais serão os métodos empregados para resolvê-las. Antes de irmos à "caça" de suas soluções, devemos introduzir o conceito de Resíduo Quadrático, onde definiremos o Símbolo de Legendre, juntamente com as suas propriedades e também a Lei da Reciprocidade Quadrática, que será de suma importância para determinar se as congruências de grau 2 tem solubilidade, ou seja, se as equações diofantinas consideras como "Ternos Quase Pitagóricos"possuem soluções inteiras. Caso tenha solução a congruência de grau 2, tentaremos viabilizar métodos para encontrar suas soluções.

A utilização das congruências se estende desde a modelagem de simples fenômenos cíclicos ou periódico-discretos, como por exemplo, na contagem das horas, à sua aplicação na criptografia e em ciências da computação, como pode ser observado em (Medeiros, 2015), (Biase e Agustini, 2009) e (Oliveira, 2013), sendo utilizadas ainda em outras áreas, tais como aplicações em acústica, e teoria dos grafos (Rousseau, 2012) . Observa-se ainda que a resolução de Congruências Quadrática passa pela solução de sistemas de Congruências Lineares atráves do Teorema Chinês dos Restos (Rosen, 2011).

Temos por objetivo apresentar uma discussão mais abrangente sobre o estudo de Congruências Quadráticas, do tipo $ax^2 + bx + c \equiv 0 \mod m$, não apenas com $m = p$, p primo, mas

para m composto, com foco na busca de suas soluções.

Este trabalho se dedica a essas discussões, as quais são necessárias à busca das soluções de uma Congruência Quadrática.

Capítulo 1

Um breve histórico sobre o desenvolvimento da Teoria dos Números

A Teoria dos Números é o ramo da matemática responsável pelo estudo das propriedades dos números, principalmente os números inteiros. Um de seus principais focos, o estudo das propriedades dos números primos, já eram estudados por Euclides (325 a. C./265 a.C), Eratóstenes (276 a.C/194 a. C) e Diofanto (cerca de 200 d.C/ a 284 d.C). Grandes matemáticos se destacaram nesse campo, entre eles Fermat (1601/1665), Euler (1707/1783), Legendre (1752/1833) e Gaus (1777/ 1855). Foi em seu livro Disquisiones Aritmeticae, publicado em 1801, que Gaus reuniu os resultados previamente obtidos nesse ramo da matemática acrescentando resultados originais, além de ter introduzido a notação de congruência atualmente utilizada e apresentou uma demonstração da Lei da Reciprocidade Quadrática, de grande importância no estudo das congruências de grau 2.

O debate sobre esse aspecto da teoria dos números pode ser posto numa perspectiva histórica e assinalar o ponto de apoio, de mutação, de readequação e retomadas de alguns posicionamentos de tal debate sobre a Lei de Reciprocidade Quadrática e do momento preciso em que tais bases matemáticas foram assentadas. Trata-se, dessa maneira, de traçar as condições históricas para aquilo que posteriormente na matemática convencionou-se chamar Teoria dos Números.

Diante disso podemos perceber que pessoas já na civilização grega se lançaram ao pensamento matemático, no sentido em que suas indagações, intuições e demais trabalhados produzidos vão constituir algumas bases do pensamento da matemática moderna, nessa perspectiva tomando como experiência da modernidade, aquilo que os historiadores convencionaram cha-

mar de Idade Moderna e que cobre um lapso de tempo que vai do século XV aos fins do século XVIII, em outras palavras o momento em que marca a chegada dos europeus na América e as Revoluções (Inglesa, Francesa e Industrial); marcando notadamente um mundo cada vez mais técnico. O que interessa nesse ponto é justamente o intervalo de tempo, entre os séculos XV e XVIII em que houve duas formas de retomadas histórica do pensamento clássico, da tradição grega, helênica e romana pelo movimento conhecido por Renascimento nos séculos XV e XVI e pelo Iluminismo do século XVIII.

Assim, o percurso histórico que se propõe se pauta em nomes como Euclides (325 a.C/265 a.C) e Eratóstenes (276 a. C/ 194 a.C) que eram, por assim dizer, matemáticos gregos e tinha desenvolvido grandes contribuições nesse campo de pensamento. Já na era cristã outro personagem importante na história da matemática é Diofanto de Alexandria, nascido na cidade egípcia de Alexandria criada em homenagem ao rei macedônio Alexandre, o Grande, no auge de seu poderio militar, mas que no contexto em que nasceu Diofanto, já estava sob domínio dos romanos.

Assim temos o desenvolvimento de uma tradição de matemáticos que tem uma forte ligação com o pensamento clássico do mundo grego e que vão constituir as bases do debate sobre o que futuramente vai se traduzir numa teoria dos números onde nomes como: Euclides, Eratóstenes e Diofanto posteriormente serão retomados pelos renascentistas e pelos iluministas.

Quem eram esses pensadores? O que levaram estes a conceber um pensamento que se pautava em princípios matemáticos? E em que condições faziam isso? Sabe-se que pouquíssimos registros foram deixados e o que podemos aventar sobre tais questões se pautam em resquícios desses registros que até o momento chegaram até nós. Tomemos inicialmente, os nomes de Euclides e Eratóstenes, ambos gregos, mas que tiveram forte ligação com Alexandria, lembrando a força que o império macedônico desfrutava nesse período, ressaltando que o próprio Alexandre, o Grande, tratou de consolidar os aspectos culturais do mundo grego para todas as regiões conquistadas, tal apreço pela cultura grega, se dava principalmente por sua ligação com o pensador grego Aristóteles que havia sido seu preceptor nos tempos de sua juventude. A constituição do império macedônio no século IV a.C. conhecido por helenismo, devido à forte influência da cultura grega, mencionada anteriormente, conheceu o seu auge sob o comando de Alexandre o Grande, cuja grandiosidade, culminará na construção de uma cidade no Egito em sua homenagem, que foi exatamente a cidade de Alexandria e que se tornará o centro cultural do mundo helênico desse período. Dessa maneira mesmo que Atenas tenha conseguido manter

a sua hegemonia no campo do pensamento filosófico, Alexandria tornava-se o grande centro da cultura científica. Assim:

> Os trabalhos de construção da cidade, desejada por Alexandre em memória do seu próprio nome, iniciaram-se em 332 a.C. e prolongaram-se por muito tempo. A posição foi escolhida com intuito infalível: com efeito, encontrando-se junto a foz do Nilo, ela se beneficiava ao mesmo tempo dos resultados do cultivo das férteis terras adjacentes e dos resultados do comércio. A população cresceu rapidamente, agregando-se aos elementos locais aqueles provenientes de toda parte, entre os quais destacam-se sobretudo os Hebreus. Naturalmente, o elemento grego era predominante. Mas foi precisamente nesse contexto cosmopolita que a dimensão cultural propriamente helênica ampliou-se para o sentido helenístico.(REALE e ANTISERI, 2003, p.311)

Como centro cultural do mundo antigo a partir do século IV a.C. temos a criação de instituições de suporte as pesquisas e aos estudos voltados para o pensamento racional como por exemplo, o museu e a biblioteca de Alexandria, atraindo para lá uma série de pesquisadores vindos de várias partes do mundo. Foi assim que:

> Nasceram o Museu (que significa instituição sagrada dedicada as Musas, protetoras das atividades intelectuais) e a "Biblioteca" a ele anexa. O primeiro oferecia todo o instrumental para as pesquisas médicas, biológicas e astronômicas; a segunda oferecia toda a produção literária dos gregos. Sob Ptolomeu II, a Biblioteca encaminhou-se para a imponente cifra de quinhentos mil livros, que pouco a pouco cresceu para setecentos mil, constituindo a mais grandiosa coleção de livros do mundo antigo. (REALE e ANTISERI, 2003, p.312).

Foi diante desse ambiente cultural que se desenvolveu o pensamento matemático de Euclides e de Eratostenes[1] , onde eles puderam ter contato com um amplo material para desenvolver as suas pesquisas, principalmente no campo da geometria que tinha uma certa valorização pela cultura grega, mesmo estando circunscrita aos postulados filosóficos. Temos nesse sentido que:

> Em virtude da disposição própria do pensamento grego, a matemática foi sem dúvida, a ciência que gozou de maior estima, de Pitágoras a Platão. Basta lembrar que, segundo a tradição, Platão mandou inscrever na entrada da Academia a frase "não entre quem não for geômetra".(REALE e ANTISERI, 2003, p.313).

Havia entre a tradição filosófica grega do período clássico, um certo apreço pela geometria, nascida inicialmente da relação com os egípcios no que a desenvolveram de uma forma empírica e prática para as atividades cotidianas, e o primeiro esforço de traduzir essas preocupações em conceitos matemáticos foram realizados pelos filósofos gregos no esforço

[1]Este inclusive foi um dos diretores da biblioteca de Alexandria (REALE e ANTISERI, 2003).

de estabelecer uma forma de explicação da natureza (physis) em contraposição com a tradição mitológica. Assim temos:

> O primeiro grande geômetra grego foi Tales de Mileto, que teria adquirido seus conhecimentos matemáticos com os sacerdotes do Egito, onde se praticava uma geometria prática e empírica, sem cunho científico ou preocupação teórica, limitada a receitas para o cálculo de áreas e volumes. Os gregos transformariam essa incipiente e pragmática Geometria em uma parte da Matemática, baseada na axiomatização e na dedução lógica. A Geometria passaria a ser estudada como Ciência em si, e não somente pelo seu caráter utilitário. Noções, como as de ângulo, ponto, linha, reta e curva, foram criações gregas (Rosa, 2012a, p.144)

Mas o auge da geometria grega alcança maior notoriedade com Euclides, mesmo que tenha existido grandes personagens que contribuíram para o pensamento matemático, foi exatamente com Euclides que se formalizou um paradigma, principalmente na geometria, com a publicação de sua obra *Elementos*:

> Os avanços para uma melhor compreensão e utilização da Geometria se devem, ainda, a extraordinários geômetras, como Demócrito de Abdera, Eudoxo, Eratóstenes e Hipócrates de Quíos. O período áureo da Geometria helênica correspondeu aos trabalhos de Euclides, de Arquimedes e de Apolônio, expoentes da chamada Geometria euclidiana (plana e no espaço), consubstanciada no célebre livro Elementos, que dominaria, de forma absoluta e incontestável, por dois mil anos, a Geometria, até o surgimento da chamada Geometria não euclidiana, descoberta independentemente por Lobatchesvki, Bolyai e Gauss, na segunda metade do século XIX. Alguns historiadores da Matemática apresentam a evolução da Geometria grega por meio de dois grandes sistemas: o pitagórico e o euclidiano. (Rosa, 2012a, p.145)

O nome de Euclides também é importante não por conta do seu domínio no campo da geometria, mas cabe também a ele, o primeiro esforço de sistematização do conhecimento matemático da antiguidade. A esse respeito, Carvalho, estabelece o seguinte posicionamento:

> A sistematização clara e rigorosa de toda a matemática da antiguidade – da geometria à teoria das proporções, passando pela teoria dos números irracionais – deve-se a Euclides. Os Elementos de Euclides são, possivelmente, o livro científico mais reproduzido e mais estudado da história. [...]. Com Euclides, os fundamentos da geometria ainda eram intuitivos (ponto e reta), mas passaram a ser entendidos como objetos geométricos especificados em afirmações não demonstradas, ou seja, axiomas e postulados. (Carvalho, 2012, p.53)

Gostaria agora de tratar de outro nome também importante na história da matemática e que sucedeu Euclides, compartilhando com este o desenvolvimento de suas pesquisas em Alexandria, mas, não somente isso, ele também foi um dos diretores dessa biblioteca, que é exatamente Eratóstenes. O interessante desse matemático, é que ele começou a aplicar o

conhecimento matemático em outros domínios do saber, no caso a geografia. Assim:

> Em 246 a.C. ele foi chamado pelo rei Ptolomeu II à Alexandria como diretor da Biblioteca[...] Era versado em muitos campos do saber, mas não a ponto de impor-se de modo peremptório. Seu mérito histórico foi o de ter aplicado a matemática à geografia e o de ter esboçado o primeiro mapa do mundo seguindo o critério dos meridianos e dos paralelos. (REALE e ANTISERI, 2003, p.320)

Tais conhecimentos matemáticos e o conhecimento teórico lhes permitiu que realizasse cálculos com um nível de complexidade mais elevada ao ponto de aplicar metodologicamente algumas adequações que tornariam possível o cálculo das dimensões do planeta Terra. Dessa maneira:

> Baseando-se em cálculos engenhosos, fundamentados e com correção metodológica, Eratóstenes também conseguiu calcular as dimensões da terra. O resultado por ele obtido foi de 252 mil estádios (aproximadamente 39.960 quilômetros). Na antiguidade, o valor do estádio não era uniforme. Mas, se é verdade que o estádio adotado por Eratóstenes equivalia a 157,5 metros, então a cifra que daí resulta é apenas poucas dezenas de quilômetros inferior à que hoje se calcula. (REALE e ANTISERI, 2003, p.320)

Nesse campo dos cálculos complexos, cujas premissas e axiomas, vinham se constituindo desde o pensamento pitagórico a partir do pensamento dedutivo, Eratóstenes também se lança a outro domínio também muito pesquisado por estes pitagóricos, que trata exatamente da propriedade dos números primos:

> Eratóstenes criou uma técnica para calculá-los (o famoso Crivo de Eratóstenes – numa tabela de 1 a 100, eliminar o número 1 e todos os números pares, exceto o 2, e excluir todos os múltiplos maiores de 3, 5 e 7; os números restantes são primos) e Euclides considerou não haver número finito de números primos. Os pitagóricos identificaram, ainda, os chamados primos gêmeos (3 e 5, 5 e 7, 11 e 13, 17 e 19, etc.) e os primos entre si. Interessaram-se, também, os pitagóricos, pelos ”números pares”(divisíveis por 2) e ímpares (não divisíveis por 2), e pelos igualmente pares, que podem ser divididos em duas partes iguais de pares, como $4, 8, 12, 16, 20, 24$, etc. Trabalharam, também, os números quadrados (resultantes da multiplicação do mesmo número – $9 = 3\times3$, $16 = 4\times4$, $25 = 5\times5$, etc.) e os números cúbicos (resultantes de duas multiplicações do mesmo número – $8 = 2\times2\times2$, $27 = 3\times3\times3$, $64 = 4\times4\times4$, etc.). Os pitagóricos identificavam os números cardinais (1, 2, 3, 4, 5, etc.) e os ordinais (primeiro, segundo, terceiro, etc.)(Rosa, 2012a, p.142)

Tais cálculos dos números primos efetuados por Eratóstenes vai permitir a criação dos números irracionais isso porque até aquele momento:

> Consideravam que todos os números fossem racionais, ou seja, limitados apenas a inteiros e frações. É que todas as linhas deveriam ser constituídas de número inteiro de pontos, e, no entanto, a diagonal de um quadrado e os seus lados não o são. A descoberta, pelos próprios pitagóricos, dos chamados números irracionais ou incomensuráveis, sem relação com a unidade (raízes quadradas de dois, de três, o pi) criou o grave problema da constatação da existência de número que não era inteiro, abalando todo seu sistema filosófico. A solução foi considerar que não se tratava realmente de números, pelo que sua existência foi esquecida, até a publicação do Opus Arithmeticae (1167), de G. Cremona, que o chamou de número irracional.(Rosa, 2012a, p.142-143)

Temos enfim um panorama bem geral do pensamento matemático no mundo antigo que sob uma tradição do mundo grego, cuja preocupação se pauta inicialmente numa tentativa filosófica de pensar o mundo em detrimento do pensamento mitológico, começam por intuir por dedução uma explicação a partir da materialidade prática do cotidiano (preocupação com physis) e em torno disso questões e teorias abstratas começam a surgir sobre a matemática bem como forma de operacionalizar cálculos.

Lembrando, todos esses nomes apresentados até aqui, mostram que mesmo sob o domínio macedônio, os gregos ainda constituíam o centro da atmosfera cultural, mesmo Alexandria fundada no Egito, não quebrará essa proeminência grega, ao contrário se tornará um polo de atração desses gregos, situação esta que começa a entrar em declínio quando um novo povo tenta impor a sua supremacia cultural, no caso, o império romano. Onde:

> O resultado final desse processo perverso foi o declínio paulatino da cultura helênica, até o ponto de ser perseguida pelas autoridades políticas e religiosas daqueles novos tempos. A Biblioteca, parcialmente queimada pelas legiões de Júlio César, foi danificada por diversas invasões e insurreições. Em 269, a Biblioteca foi novamente queimada por ordem de Zenóbia, Rainha de Palmira, quando conquistou o Egito. É evidente que a cultura grega prosseguiria pelos séculos seguintes, ainda que em declínio e em desprestígio, devido, em parte, pelas novas ideias que começavam a prevalecer e a forjar uma nova Sociedade. (Rosa, 2012a, p.119)

É nesse contexto de transição da hegemonia cultural que era representado pela cultura grega para a hegemonia cultural dos romanos e da disseminação das ideias cristãs pelo mundo antigo, que o matemático Diofanto (200 d.C./284 d.C.) nascido em Alexandria e falecido nessa mesma cidade irá desenvolver suas pesquisas. Diante dessa situação, as reflexões sobre o pensamento matemático, as abstrações e as teorizações realizados no mundo antigo sob preeminência do pensamento grego, que eram todas expressas por frases escritas, ou seja, em discurso, passam a ser substituídas por símbolos, construindo uma linguagem própria para o pensamento

matemático:

> O papel de Diofanto na evolução da Matemática foi um dos mais importantes, pois ao inovar com as notações, substituindo as expressões, até então escritas com palavras, por símbolos, permitiu uma abreviação, facilitando o processo de cálculo. Seu Livro de Aritmética é considerado o primeiro na utilização de símbolos para a indicação de incógnitas e potências, e na resolução de equações indeterminadas (ou diofantinas) e determinadas; um total de 130 problemas de natureza variada é examinado na obra. Foi, assim, o criador das chamadas diofantinas, método para a solução de determinadas equações algébricas. (Rosa, 2012a, p.144)

Os autores que trazemos nesse itinerário, até o presente momento, tiveram grande importância para a história da matemática e formularam seus estudos num ambiente propicio a isto, ou seja, uma cidade cosmopolita, que teria sido Alexandria que trouxe as mais eminentes cabeças pensantes do mundo grego para lá: entre eles Euclides, Eratóstenes, Arquimedes,[2] Diofanto entre outros e que aos poucos vão construindo o vocabulário semântico do pensamento matemático e da teoria dos números. Tais autores vão se tornar a base do pensamento matemático moderno, principalmente entre os movimentos culturais do Renascimento e do Iluminismo que colocará toda uma tradição da matemática em retomadas e novas perspectivas. Nesse processo, por exemplo, vai ser importante a invenção da imprensa por Gutemberg no século XV:

> A divulgação de obras em latim para um público acadêmico e universitário continuaria a se expandir durante o Renascimento Científico, em condições bem melhores, de qualidade e preço, que na Idade Média, graças à tipografia, que permitiu a substituição do manuscrito de folhas de pergaminho pelo livro de folhas de papel. Foi, assim, facilitado o acesso às obras tanto da Antiguidade grega (Escola de Pitágoras, Platão, Aristóteles, Apolônio, Euclides, Arquimedes, Diofanto) e da cultura árabe (al-Khwarizmi, al-Battani, al-Tusi) quanto de autores da primeira fase do Renascimento Científico, como Bradwardine (Arithmetica, publicada em 1495), Jordanus Nemorarius (Arithmetica, em 1496 e 1503 e Geometria Speculativa em 1496), Oresme (De Latitudine formarum, em 1482 e 1486) e Sacrobosco (Algorisme e Sphaera, em 1472). Obras de Chuquet, Leonardo de Pisa e Piero Della Francesca, por exemplo, não foram, contudo, publicadas nessa época. Registre-se a importância, para o desenvolvimento da Matemática na Europa, da tradução e publicação, por Frederico Commandino (1509-1575), dos geômetras gregos (Apolônio, Arquimedes, Aristarco, Euclides, Pappus e Ptolomeu, entre outros). (Rosa, 2012a, p.403)

Diante desse contexto histórico, nomes como François Viète (1540/1603) e Simon

[2] A importância deste pensador também é capital para a história da matemática, mas as análises de sua produção exigiriam um espaço maior para discussão e que não caberia aqui nesse trabalho. Também foi amigo de Eratóstenes e cujas cartas foram publicadas com o título: Cartas a Eratóstenes em que apresentava as bases de seu pensamento. Sobre algumas de suas contribuições ver:Rosa (2012a)

Stevin (1548/1620) se notabilizaram por seus estudos no campo do pensamento matemático dedicado a álgebra, retomando em muitos aspectos algumas premissas da matemática praticada pelos gregos que apresentamos até aqui. Assim enquanto Viète publica em 1591:

> *Sua In artem analyticam isagoge* (Introdução à Arte Analítica), na qual são estudadas, separadamente, a logística numerosa (Aritmética) e a Logística especiosa (Álgebra). Para Viète, "a maneira de penetrar na ciência nova é uma arte especial que consiste em não mais exercer a lógica sobre os números, mas uma logística em que as coisas são figuradas por sinais: logística muito mais hábil e mais poderosa". Demonstrou o valor dos símbolos, introduzindo letras para representar quantidades conhecidas (consoantes) e desconhecidas (vogais). Usou símbolos para as quantidades em Álgebra e para as operações realizadas com elas. Em *De aequationum recognitione et emendatione* (publicada postumamente, em 1615) apresentou métodos para resolver equações de segundo, terceiro e quarto graus. Escreveu, ainda, Viète o *De numerosa potestatum resolutione* (1600), no qual apresentou um processo sistemático de aproximações sucessivas de uma raiz de uma equação. (Rosa, 2012a, p.410)

Em 1585 (seis anos antes da publicação de Viéte) Simon Stevin publica:

> Arithmetique de Simon Stevin de Bruges, dividida em duas partes: a primeira, um grande tratado de Aritmética e Álgebra, e a segunda, uma paráfrase dos quatro primeiros livros de Diofanto, e ainda uma coleção de ensaios A Prática da Aritmética e um comentário sobre a teoria das grandezas incomensuráveis, segundo o livro X de Euclides. Em A Prática da Aritmética, conhecida também como A Décima (De Thiende), Stevin trata das frações decimais, sua mais importante contribuição à Matemática. Apesar de terem sido estudadas anteriormente (Regiomontanus, Rudolff, Viète), Stevin foi o primeiro a substituir as frações comuns pelas frações decimais, que rapidamente seriam adotadas; ou seja, deve-se a ele a introdução de sistema decimal de notações fracionárias. Sua notação para a escrita dos números decimais fracionários resultou, posteriormente, no uso da vírgula. Stevin declarou, inclusive, que era uma questão de tempo para que o sistema decimal fosse empregado nas medidas, nas moedas e nos pesos. (Rosa, 2012b, p.410-411)

Tais contribuições desses matemáticos dos séculos XVI e XVII marcam um momento de revigoramento do pensamento matemático, após, esta figurar em segundo plano durante o período medieval. Nesse sentido é digno de nota o posicionamento de (Araújo, 2013) onde: a matemática na Europa teve uma renovação vigorosa após a Idade Média, onde a Teoria dos Números por apresentar uma área particular da matemática de grande desenvolvimento[3].

Assim o desenvolvimento de uma posterior Teoria dos Números se construiu paulatinamente a partir de vários nomes desde tempos antigos, mas a constituição desta no campo da matemática pura, opera por retomadas ou por exclusões de premissas, de refutações ou de

[3](Araújo, 2013, p.IX)

demonstrações e provas, o que exige um esforço de teorização muito grande. Nesse sentido, de certa forma explica o fato da matemática no período medieval ter adquirido um aspecto secundário, pois a teorização das coisas se dava no domínio da manifestação divina. O campo aberto pelas pesquisas matemáticas entre os séculos XVI e XVIII de nossa era, mostram que um campo de inteligibilidade para o desenvolvimento de uma ciência material e empírica estava se solidificando cada vez mais com a descoberta de outros mundos (o continente americano) e com a constituição de uma burguesia industrial (principalmente com a Revolução Industrial do século XVIII).

> O reconhecimento da importância da Matemática para o desenvolvimento científico e industrial geraria um grande interesse nos meios intelectuais, pela modernização de seu estudo, pela ativa participação da Universidade no processo de renovação e de criatividade, pela ampliação da cooperação internacional, pela fundação de Associações especializadas de pesquisas, e pela divulgação dos estudos e investigações. As Academias perderiam a exclusividade da pesquisa científica em favor das Universidades, e a "profissão de matemático" seria prestigiada nos meios intelectuais. (Rosa, 2012b, p.45)

Isso significa condições favoráveis para o desenvolvimento de cálculos cada vez mais precisos para se aventurar em mundos cada vez mais distantes bem como capitalizar tempo, forças e trabalho para as nascentes sociedades industriais. O fato é que a matemática se tornava cada vez mais complexa e com cálculos cada vez mais minuciosos e rigorosos. Não é o escopo dessa pesquisa aventar todas as contribuições da matemática desse período, mas sim, dos estudos de Congruências Quadráticas, que será apresentado com mais acuidade a seguir. Nesse sentido, gostaria de apresentar alguns nomes importantes sobre esse tema e concluir apresentando as etapas que constituem o nosso estudo. Nesse sentido grandes matemáticos afloraram suas ideias sobre o campo das Congruências Quadráticas entre finais do século XVII e finais do século XVIII culminando na sistematização de tais estudos por Gauss no século XIX. Nesse intervalo de tempo passou nomes importantes entre eles: Fermat (1601/1665), Euler (1707/1783), Legendre (1752/ 1833) e finalmente Gaus (1777/1855).

Fermat (1601/1665) na história da matemática foi pioneiro na formulação das premissas das congruências quadráticas, conforme (Araújo, 2013, p.X.):

> (...) o primeiro matemático a estudar reciprocidade quadrática foi Fermat, que tinha a Matemática como uma atividade de lazer em uma época em que não existiam revistas matemáticas. Fermat tinha um costume curioso de apresentar resultados matemáticos em margens de livros que ele leu e em carta de correspondência com outros matemáticos. Ainda assim, esta forma peculiar de estudar matemática muito contribuiu na direção da demonstração da reciprocidade quadrática. [...] Fermat foi crucial na dedução do caráter quadrático de $-1, \pm 2, \pm 3$, mas foi Euler que prosseguiu com o trabalho de provar as conjecturas de Fermat.

Com Euler (1707/1783) se dá a elaboração das provas das premissas lançadas por Fermat, desenvolvendo com mais rigor as formulações criadas por este último, lembrando que é nesse contexto que se começa a formular a Teoria dos Números. Ainda conforme (Araújo, 2013, p.X.):

> (...) Devido ao grande interesse na Teoria dos Números e por começar a desenvolver os trabalhos de Fermat, tendo contato com Christian Goldbach, Euler percebeu a relação entre a Lei de Reciprocidade Quadrática e os estudos dos diversos binários de certas formas quadráticas.

Percebe-se assim, a constituição de um campo cada vez mais forte no domínio da matemática com a necessidade de provas, de comprovações, de demonstrações da natureza intrínseca e extrínseca dos números com a Teorias dos Números que estava nascendo, a qual Euler e outros matemáticos estavam emersos, retomando inclusive premissas de outros matemáticos. Como se pode ver:

> O objeto de estudo da Teoria dos Números é o sistema de números inteiros (... -3, -2, -1, 0, 1, 2, 3...), assunto de capital importância da Matemática, desde os gregos. Euclides já demonstrara o famoso Teorema Fundamental da Aritmética, segundo o qual, todo número inteiro "n"maior que 1 pode ser representado de modo único como um produto de fatores primos, razão do grande fascínio dos matemáticos pelos números primos. Ao longo da História da Matemática, o assunto mereceu muitos estudos, tendo permanecido o interesse no século XIX, quando o tema teria grande desenvolvimento. (Rosa, 2012b, p.49).

O que se tem dessa maneira, é que as primeiras sistematizações de Fermat, Euler, Legendre e Gauss sobre a Lei de Reciprocidade Quadrática se dá no mesmo contexto da formalização da Teoria dos Números, gestados no mesmo ambiente cultural dos séculos XVIII e XIX.

> Adrien-Marie Legendre (1752-1833), autor de Ensaios sobre os Números (1798, reeditado em 1808, e com apêndices em 1816 e 1825) e de Teoria dos Números (1830), contribuiu, de forma decisiva, para o desenvolvimento do tema, ao examinar sua evolução, ao sistematizar seu exame e ao formular a famosa Lei da Reciprocidade Quadrática, que viria a ser demonstrada por Gauss. (Rosa, 2012b, p.49)

Legendre, por exemplo, publica como foi dito acima dois livros explicitamente marcados pela preocupação de conhecer as propriedades numéricas tanto no Ensaios sobre os Números como também a Teoria dos Números, obras que vão de certa maneira apresentar a problemática sobre a natureza dos números e que será profundamente analisada por outros matemáticos de grande nome, inclusive Gauss.

Em relação à Lei de Reciprocidade Quadrática, uma das grandes contribuições de Legendre foi o de criar uma notação para simbolizar de maneira mais adequada a Lei de Reciprocidade Quadrática na matemática moderna e que inclusive é usada nos dias de hoje, conhecida como símbolo de Legendre.

Por fim gostaríamos de apresentar, algumas contribuições de Gauss para a Lei de Reciprocidade Quadrática e por muitos considerados o maior gênio da matemática, e concluir demarcando as etapas que constituem o presente trabalho.

Gauss se insere num momento de transformação cultural na Europa, marcado ainda pelo paradigma iluminista, que entre outras características se tinham uma posição otimista do mundo por meio do caráter libertador da educação na direção do ideal almejado pelo progresso e pela civilização. Assim passa haver cada vez mais interação entre ensino e pesquisa e o trabalho de Gauss coaduna-se docência e pesquisa:

> C.F. Gauss foi professor da Universidade de Göttingen até sua morte, em 1855. A interação entre ensino e pesquisa foi incrementada depois dessa data, com a vinda de Dirichlet de Berlim. Tal aquisição deu início a uma nova fase para a matemática nessa universidade, com a presença também de Riemann. Os cursos de ambos inauguraram o processo que transformaria essa universidade, no final do século XIX, com a chegada ainda de Klein e Hilbert, em um dos centros matemáticos mais importantes do mundo, ao lado da Universidade de Berlim. (Roque, 2012, p.418)

Temos então um ambiente cultural propício ao desenvolvimento de uma sistemática elaboração de princípios para uma moderna teoria dos números, que vinha sendo constituída desde os matemáticos da Grécia clássica, mas o mais surpreendente é que Gauss tenha se destacado em vários campos do pensamento matemático sendo conhecido como o Príncipe da Matemática.

> O reconhecido gênio matemático do alemão Karl Friedrich Gauss (1777-1855) está presente, praticamente, nos vários domínios da Matemática. Sua extraordinária, diversificada, fecunda, pioneira e extensa contribuição em Matemática pura inclui demonstrações dos teoremas fundamentais da Álgebra e da Aritmética, demonstração da Lei da Reciprocidade Quadrática, formulação da Lei dos Resíduos Quadráticos, Álgebra linear, integração numérica, séries infinitas, equações diferenciais, seções cônicas, funções hipergeométricas, Geometria diferencial, Geometria não euclidiana, Teoria potencial, Análise vetorial, Probabilidades e Estatística (curva de Gauss, distribuição de Gauss). Gênio precoce, Gauss, aos 19 anos (1796), já consignava em seu famoso diário: i) a descoberta do método para a construção, com régua e compasso, de um polígono regular de 17 lados (heptadecágono) e de não ser possível a construção de um de sete lados (heptágono); ii) o desenvolvimento do método dos quadrados mínimos; iii) a descoberta de que todo inteiro positivo é soma de três números triangulares; iv) a descoberta da periodicidade dupla de certas funções elípticas, e, pouco depois, a periodicidade dupla para o caso geral. Em sua tese de doutorado, na Universidade de Helmstädt, deu a primeira demonstração satisfatória, tentada por Newton, Euler, D'Alembert, Laplace e Lagrange, do "Teorema Fundamental da Álgebra"(uma Equação polinomial, com coeficientes complexos e de grau maior que zero, tem pelo menos uma raiz complexa); três demonstrações posteriores seriam apresentadas por Gauss, em 1801, na Disquisitiones Arithmeticae, em 1816 e 1850. (Rosa, 2012b, p.45-46)

Gauss, portanto, apresentou várias contribuições para o desenvolvimento da matemática, que partindo dos pressupostos e conjecturas de toda uma tradição de matemáticos, coube a ele um aprimoramento e refinamento de tais premissas, enfim, não é por acaso que muitos o consideram que a concepção moderna da Teoria dos Números se dá justamente com a publicação de (Gauss et al., 2006):

> (...) tida por muitos como uma das obras-primas da Matemática: **ela prega, por exemplo, a necessidade de rigor meticuloso em Matemática... a Teoria dos Números ultrapassa em muito todos os trabalhos feitos em teoria das funções ou em Geometria até ao menos a metade do século. Ela preside com a Álgebra pura o nascimento das Matemáticas modernas tais como serão concebidas no século XX;** das sete seções do livro, apenas a última não trata da Teoria dos Números. O subsequente desenvolvimento da Teoria, objeto de grande interesse, de intensa pesquisa e de crescente complexidade, teria um desdobramento com repercussões em vários campos da Matemática. [...] Nesse sentido, sua Disquisitiones Arithmeticae é um marco na evolução do assunto. Do total de sete seções, as quatro primeiras são, essencialmente, uma reformulação mais compacta da Teoria dos Números do século XVIII; a quinta versa a respeito da Teoria das Formas Quadráticas binárias; a sexta, de várias aplicações; e a sétima seção trata da resolução da equação ciclotômica geral de grau primos.(Rosa, 2012b, p.49-50)

Todo esse desdobramento histórico sobre a constituição da Teoria dos Números é perti-

nente na medida em que apresenta algumas condições históricas de sua efetivação no campo da matemática. Nesse sentido, a ancoragem de nosso trabalho busca contribuir no campo geral da Teoria dos Números, em particular, no que diz respeito ao estudo das Congruências Quadráticas.

Capítulo 2

Fundamentos Teóricos

Nesse capítulo serão apresentadas noções básicas de divisibilidade, definição de Máximo Divisor Comum, Mínimo Múltiplo Comum e de Equações Diofantinas Lineares. Além da definição de Congruência Linear e suas propriedades, apresentando resultados que possibilitam a determinação de suas soluções, quando existentes e Resíduos Quadráticos e as propriedades do Símbolo de Legendre, assim como a Lei da Reciprocidade Quadrática, que serão necessários ao estudo dos tópicos abordados nesse trabalho.

2.1 Divisibilidade

Daqui em diante escrevemos $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$ para indicar o conjunto dos números inteiros e $\mathbb{N}^* = \{1, 2, 3 \cdots\}$ para indicar o conjunto dos números inteiros positivos

Definição 2.1 *Se a e b são inteiros, dizemos que a divide b, se existe um inteiro positivo c tal que $b = ac$. Neste caso escrevemos $a \mid b$. Se a não divide b escrevemos $a \nmid b$.*

Proposição 2.1 *Se a, b e c são inteiros, $a \mid b$ e $b \mid c$, então $a \mid c$*

Demonstração: Como $a \mid b$ e $b \mid c$ existem inteiros t_1 e t_2 que satisfazem $b = t_1 a$ e $c = t_2 b$. Logo, $c = t_2(t_1 a)$, o que implica na existência de $t = t_1 t_2$ que satisfaz $c = ta$ e assim $a \mid c$.

■

Exemplo 2.1 *Como* $6 \mid 36$ *e* $36 \mid 108$*, então* $6 \mid 108$.

Teorema 2.1 *A divisibilidade tem as seguintes propriedades, para n, a e d inteiros:*

i $n \mid n$

ii *Se* $d \mid n$ *então* $ad \mid an$

iii *Se* $ad \mid an$ *e* $a \neq 0$ *então* $d \mid n$

iv $1 \mid n$

v $n \mid 0$

vi *Se* $d \mid n$ *e* $n \neq 0$ *então* $|d| \leq |n|$

vii *Se* $d \mid n$ *e* $n \mid d$ *então* $|d| = |n|$

viii *Se* $d \mid n$ *e* $d \neq 0$ *então* $\frac{n}{d} \mid n$.

Demonstração:

i Como $n = 1 \cdot n$ segue da definição que $n \mid n$, inclusive para $n = 0$;

ii Se $d \mid n$ então $n = cd$ para algum inteiro c. Logo $an = cad$ implicando que $ad \mid an$;

iii Se $ad \mid an$ então $an = cad$ para algum inteiro c. Como $a \neq 0$, dividindo ambos os lados da igualdade por a, obtém-se $n = cd$ concluindo que $d \mid n$;

iv Como $n = n \cdot 1$ conclui-se que $1 \mid n$;

v Como $0 = 0 \cdot n$ então $n \mid 0$;

vi Como $d \mid n$ e $n \neq 0$ então $n = td$ para t inteiro. Assim, tem-se $|d| \leq |td| = |n|$;

vii Pelo item anterior $|d| \leq |n|$ e $|n| \leq |d|$ implicando que $|d| = |n|$;

viii Se $d \mid n$ então $n = kd$ para algum k inteiro e portanto $\frac{n}{d}$ é inteiro. Como $\left(\frac{n}{d}\right)d = n$ segue por definição que $\frac{n}{d} \mid n$.

■

2.2 Algoritmo da Divisão

Para que seja demonstrado o Algoritmo da Divisão apresentamos o *Teorema de Eudoxius*que será útil na demonstração do algoritmo da divisão. Dados a e b inteiros com $b \neq 0$

então a é múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, para cada par de inteiros a e $b \neq 0$, existe um inteiro q tal que, para $b > 0$,

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

e para $b < 0$,

$$qb \leq a < (q-1)b.$$

Exemplo 2.2 *Se $a = 7$ e $b = 4$, teremos que $q = 1$*

$$1 \times 4 \leq 7 < 2 \times 4.$$

Se $a = 7$ e $b = -4$, teremos $q = -1$

$$(-1) \times (-4) \leq 7 < (-2) \times (-4).$$

Se $a = -7$ e $b = 4$, teremos $q = -2$

$$(-2) \times 4 \leq -7 < (-1) \times 4.$$

Se $a = -7$ e $b = -4$, teremos $q = 2$

$$2 \times (-4) \leq -7 < 1 \times (-4).$$

Teorema 2.2 (Algoritmo da Divisão) *Dados dois inteiros a e b, $b > 0$, existe um único par de inteiros q, r tais que*

$$a = qb + r, \ com \ 0 \leq r < b;$$

q é chamado quociente e r é o resto da divisão de a por b. Quando $r = 0$ dizemos que $b \mid a$.

Demonstração: Pelo teorema de *Teorema de Eudoxius*, como $b > 0$, existe q tal que:

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

O que implica $0 \leq a - qb$ e $a - qb < b$. Assim, definindo $r = a - qb$, garantimos a existência de

q e r. Suponhamos, agora que existe outro para q_1 e r_1 que satisfazem

$$a = q_1 b + r_1 \text{ com } a \leq r_1 < b.$$

Disto, obtém-se $(qb+r)-(q_1b+r_1) = 0$ obtendo $b(q-q_1) = r_1 - r$, o que implica em $b \mid (r_1 - r)$. Mas, $r < b$ e $r_1 < b$. Assim $|r_1 - r| < b$ e como $b \mid (r_1 - r)$, temos $r_1 - r = 0$, o que implica em $r_1 = r$. Logo, $q_1 b = qb$. Assim, $q_1 = q$, já que $b \neq 0$, garantindo assim a unicidade de q e r.

■

2.3 Máximo Divisor Comum

Definição 2.2 *O Máximo Divisor Comum de a e b, denotado por* $(a, b) = d$*, é o maior inteiro que divide a e b simultanemente.*

Teorema 2.3 (Bachet-Bézout) *Sejam* $a, b \in \mathbb{Z}$*. Então existem* $x, y \in \mathbb{Z}$ *com*

$$ax + by = (a, b).$$

Portanto, se $c \in \mathbb{Z}$ *é tal que* $c \mid a$ *e* $c \mid b$*, então* $c \mid (a, b)$*.*

Demonstração: O caso $a = b$ é trivial e tem como solução $x = 1$ e $y = 0$ ou $x = 0$ e $y = 1$. Para os outros casos consideremos o conjunto de todas as combinações lineares $I(a, b) = \{ax + by; x, y \in \mathbb{Z}\}$. Esse conjunto claramente, contém valores positivos, negativos e nulos. Seja $d = ax_0 + by_0$ o menor valor positivo desse conjunto, o qual existe pelo Princípio da Boa ordenação. Dado $m = ax + by \in \mathbb{Z}$, sejam $q, r \in \mathbb{Z}$ o quociente e o resto da divisão euclidiana de m por d de modo que $m = dq + r$ e $0 \leq r < d$. Temos

$$r = m - dq = a(x - qx_0) + b(y - qy_0) \in I(a, b).$$

Mas como $r < d$ e d é o menor elemento positivo de $I(a, b)$, segue que $r = 0$ e portanto $d \mid m$. Como m é um elemento qualquer de $I(a, b)$, concluímos que d divide todos os elementos de $I(a, b)$.

Como $a, b \in I(a, b)$ temos $d \mid a$ e $d \mid b$, logo $d \leq (a, b)$. É possível ainda notar que se $c \mid a$ e $c \mid b$ então $c \mid ax_0 + by_0$ implicando em $c \mid d$. Tomando $c = (a, b)$ temos $(a, b) \mid d$ e como $d \leq (a, b)$, concluímos que $d = (a, b)$.

■

Teorema 2.4 (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.*

Demonstração: Se $n = 2$, o resultado é óbvio, pois 2 é primo. Suponhamos que o resultado seja válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1.n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem primos $p_1, \cdots, p_r$ e $q_1, \cdots, q_s$ tais que $n_1 = p_1...p_r$ e $n_2 = q_1...q_s$. Portanto $n = p_1.\cdots.p_r.q_1.\cdots.q_s$. Vamos provar a unicidade da escrita: se $n = p_1...p_r = q_1...q_s$, sendo p_i e q_j números primos, $i = 1, ...r$, $j = 1, ..., s$, como $p_1 \mid q_1.\cdots.q_s$, segue que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, \cdots, q_s$, podemos supor que seja q_1. Portanto $p_2.\cdots.p_r = q_2.\cdots.q_s$. Como $p_2.\cdots.p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares.

■

Proposição 2.2 *Se* $a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_n^{\alpha_n}$ *e* $b = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n}$, *onde* $p_1, p_2, \cdots, p_n$ *são primos que compõe a e b, então*

$$(a, b) = p_1^{\min\{\alpha_1, e_1\}} p_2^{\min\{\alpha_2, e_2\}} \cdots p_n^{\min\{\alpha_n, e_n\}}$$

Demonstração: Pela definição de Máximo Divisor Comum, nenhum dos fatores p_i pode ter expoente maior que α_i ou e_i. Tomando o menor dos expoentes de p_i, temos não apenas um divisor comum, mas o maior dos divisores comuns de a e b, concluindo a demonstração.

■

2.4 Mínimo Múltiplo Comum

Definição 2.3 *O Mínimo Múltiplo Comum de dois inteiros positivos, a e b, denotado por* $[a, b]$ *é o menor inteiro positivo que é múltiplo simultaneamente de a e de b.*

Proposição 2.3 *Se* $a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_n^{\alpha_n}$ *e* $b = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n}$, *onde* $p_1, p_2, \cdots, p_n$ *são primos*

que compõe a e b, então

$$[a,b] = p_1^{\max\{\alpha_1,e_1\}} p_2^{\max\{\alpha_2,e_2\}} \cdots p_n^{\max\{\alpha_n,e_n\}}$$

Demonstração: Pela definição de Mínimo Múltiplo Comum, nenhum dos fatores p_i pode ter expoente inferior a α_i ou e_i. Tomando o maior dos expoentes de p_i, temos não apenas um múltiplo comum, mas o menor deles, concluindo a demonstração.

■

2.5 Equações Diofantinas Lineares

Definição 2.4 *Uma equação da forma $ax + by = c$, onde a, b e c são inteiros, é chamada de equação diofantina linear.*

Exemplo 2.3 $5x + 7y = 1$ *e* $6x + 4y = 5$ *são equações diofantinas lineares. A primeira delas possui solução inteira, enquanto a segunda não admite nenhuma solução inteira.*

A seguir é apresentado um teorema que discute a resolubilidade de equações diofantinas lineares, além de caracterizar as suas soluções.

Teorema 2.5 *Sejam a e b inteiros e $d = (a, b)$. A equação $ax + by = c$ possui solução inteira se, e somente se $d \mid c$. Além disso, se (x_0, y_0) é uma solução particular, então todas as soluções são dadas por*

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

em que k é inteiro.

Demonstração: Se $d \nmid c$ a equação $ax + by = c$ não possui solução, pois, como $d \mid a$ e $d \mid b$, deveria dividir c, que é combinação linear de a e b. Para o próximo passo da demonstração utilizaremos o Teorema (2.3), que nos diz que, existem n_0 e m_0 tais que

$$an_0 + bm_0 = d \tag{2.1}$$

Suponha, agora, que $d \mid c$. Então existe um inteiro k tal que $c = kd$. Se multiplicarmos ambos os membros de (2.1) por k obtemos $a(n_0k) + b(m_0k) = kd = c$. Dessa forma, o par (x_0, y_0) com $x_0 = n_0k$ e $y_0 = m_0k$ é uma solução de $ax + by = c$. Para provar a recíproca, basta tomar o para (n_0k, m_0k) como solução.

Tomando o par (x_0, y_0) como uma solução particular, queremos mostrar que os pares da forma

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

são soluções. De fato, temos

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

Mostrando assim, que conhecida a solução particular (x_0, y_0) podemos gerar, a partir dela, infinitas soluções.

Basta-nos mostrar, agora, que todas as soluções podem ser escritas dessa maneira. Suponhamos, então, que (x, y) seja uma solução, isto é, $ax + by = c$.

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

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

o que implica $a(x - x_0) = b(y_0 - y)$. Ao dividirmos os dois membros da última igualdade por d, obtemos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \tag{2.2}$$

Portanto, $\dfrac{b}{d} \mid (x - x_0)$. Então, existe um inteiro k, tal que

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

ou seja,

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

Substituindo este valor de x na equação (2.2) temos

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

mostrando que todas as soluções da equação $ax + by = c$ são da forma

$$x = x_0 + \left(\frac{b}{d}\right)k$$
$$y = y_0 - \left(\frac{a}{d}\right)k.$$

■

Exemplo 2.4 *Tomando a equação diofantina linear* $5x + 7y = 1$. *Podemos utilizar o par* $(10, -7)$ *como solução particular. Como* $(5, 7) = 1$*, todas as soluções são dadas por:*

$$x = 10 + 7k$$
$$y = -7 - 5k,$$

onde $k \in \mathbb{Z}$.

Mais detalhes podem ser vistos em Campos (2013).

2.6 Congruência Linear

2.6.1 Congruência

Definição 2.5 *Sejam* a, b *e* m *números inteiros dizemos que* a *é congruente a* b *módulo* m*,* $m > 0$*, denotado por*

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

se $m \mid (a - b)$. *Caso contrário, diz-se que* a *é incongruente a* b *módulo* m *e denota-se por* $a \not\equiv b \ (mod\ m)$

Exemplo 2.5 *Dessa forma, dizemos que* $37 \equiv 2 \ (mod\ 7)$*, ja que* $7 \mid 37 - 2$ *e* $17 \not\equiv 4 \ (mod\ 7)$*, ja que* $7 \nmid (17 - 4)$

Proposição 2.4 *Se a e b são números inteiros e m um número natural, tem-se $a \equiv b$ (mod m) se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração: Se $a \equiv b \pmod{m}$, então $m \mid (a - b)$. Esse fato implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$.

Reciprocamente, se existir k que satisfaça $a = km + b$, tem-se $km = a - b$, ou seja, $m \mid (a - b)$ o que implica $a \equiv b \pmod{m}$.

■

Proposição 2.5 *Se a, b, c e m são inteiros, tais que $a \equiv b$ (mod m), então*

1 $a + c \equiv b + c$ (*mod* m)

2 $a - c \equiv b - c$ (*mod* m)

3 $ac \equiv bc$ (*mod* m)

Demonstração: Como $a \equiv b \pmod{m}$, tem-se $a - b = km$. Assim, para o item 1, como $a - b = (a + c) - (b + c)$ tem-se $a + c \equiv b + c \pmod{m}$. Analogamente para 2. Para 3 tem-se $(a - b)c = ckm$ implicando em $m \mid (ac - bc)$, e pela definição de congruência, $ac \equiv bc \pmod{m}$.

■

Proposição 2.6 *Se a, b, c, d e m são inteiros, tem-se:*

1 *[(Reflexividade)] $a \equiv a$ (mod m).*

2 *[(Simetria)] Se $a \equiv b$ (mod m), então $b \equiv a$ (mod m).*

3 *[(Transitividade)] Se $a \equiv b$ (mod m) e $b \equiv d$ (mod m) então $a \equiv d$ (mod m).*

Com isso, dizemos que a congruência é uma relação equivalência.

4 *[(Compatibilidade com a soma e diferença)]*

$$\begin{cases} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \pmod{m} \\ a - c \equiv b - d \pmod{m} \end{cases}$$

Em particular, se $a \equiv b$ (mod m), então $ka \equiv kb$ (mod m), para todo $k \in \mathbb{Z}$.

5 *[(Compatibilidade com o produto)]*

$$\begin{cases} a \equiv b \ (mod\ m) \\ c \equiv d \ (mod\ m) \end{cases} \Rightarrow ac \equiv bd \ (mod\ m).$$

Em particular, se $a \equiv b \ (mod\ m)$*, então* $a^k \equiv b^k \ (mod\ m)$*, para todo* $k \in \mathbb{N}$

6 *[(Cancelamento)] Se* $(c, m) = 1$*, então*

$$ac \equiv bc \ (mod\ m) \ \Leftrightarrow \ a \equiv b \ (mod\ m).$$

Demonstração: Para 1 é suficiente observar que $m \mid a - a = 0$.

Em 2, se $m \mid a - b$, então $m \mid -(a - b)$, ou seja, $m \mid b - a$

Em 3, $m \mid a - b$ e $m \mid b - c$, logo $m \mid (a - b) + (b - c)$ e assim $m \mid a - c$.

Para 4, se $m \mid a-b$ e $m \mid c-d$, então $m \mid (a-b)+(c-d)$, implicando em $m \mid (a+c)-(b+d)$. Por outro lado $m \mid (a - b) - (c - d) \Rightarrow m \mid (a - c) - (b - d)$.

Para 5, $m \mid (a - b)c + (c - d)b$ e logo $m \mid ac - cl$.

Para 6, tem-se $m \mid ac - bc$, o que implica que $m \mid (a - b)c$. O fato de $(c, m) = 1$ garante que $m \nmid c$. Logo $m \mid a - b$.

■

Exemplo 2.6 *A congruência* $22 \equiv 2 \ (mod\ 5)$ *é equivalente à* $11 \equiv 1 \ (mod\ 5)$*, já que* $(2, 5) = 1$.

A seguir apresentaremos o caso geral da propriedade do Cancelamento, ou seja, quando $(c, m) = d$ para $d \geq 1$.

Proposição 2.7 *Se* a, b, c *e* m *são inteiros e* $ac \equiv bc \ (mod\ m)$*, então* $a \equiv b \left(mod\ \frac{m}{d}\right)$*, onde* $d = (c, m)$.

Demonstração: $ac \equiv bc \ (\text{mod } m)$ é equivalente a $ac - bc = c(a - b) = km$, para algum $k \in \mathbb{Z}$. Dividindo os dois membros por $d = (c, m)$, se obtém

$$\left(\frac{c}{d}\right)(a - b) = k\left(\frac{m}{d}\right) \Leftrightarrow \left(\frac{m}{d}\right) \mid \left(\frac{c}{d}\right)(a - b).$$

Como $\left(\frac{m}{d}, \frac{c}{d}\right) = \frac{(m, c)}{d} = 1$, significa que $\left(\frac{m}{d}\right) \nmid \left(\frac{c}{d}\right)$. Então $\left(\frac{m}{d}\right) \mid (a - b)$ o que implica $a \equiv b \left(\text{mod } \frac{m}{d}\right)$.

■

Exemplo 2.7 *A congruência* $80 \equiv 10 \pmod{35}$ *pode ser reescrita na forma* $10 \times 8 \equiv 10 \times 1 \pmod{35}$ *e como* $(10, 35) = 5$*, podemos simplificá-la à congruência* $8 \equiv 1 \pmod{7}$.

Definição 2.6 *Se h e r são inteiros, tais que* $h \equiv r \pmod{m}$*, dizemos que r é um resíduo de h módulo m.*

Definição 2.7 *O conjunto de inteiros* $\{r_1, r_2, \cdots, r_s\}$ *é um sistema completo de resíduos módulo m se*

(i) $r_i \not\equiv r_j \pmod{m}$ *para* $i \neq j$

(ii) *para todo inteiro n existe um* r_i*, tal que* $n \equiv r_i \pmod{m}$.

Exemplo 2.8 $\{0, 1, 2, \cdots, m-1\}$ *é um sistema completo de resíduos módulo m. Para verificar esse fato, tomemos os inteiros* $t_0, t_1, \cdots, t_{m-1}$ *com* $t_i = i$*, demonstraremos que eles formam um sistema completo de resíduo módulo m. Pelo Teorema 2.2 sabemos que para cada n, existe um único par de inteiros q e s, tal que* $n = mq + s$*,* $0 \leq s < m$*. Logo* $n \equiv s \pmod{m}$*, sendo s um dos* t_i*. Como* $|t_i - t_j| \leq m - 1$*, temos* $t_i \not\equiv t_j \pmod{m}$ *para* $i \neq j$*. Portanto o conjunto* $\{t_0, t_1, \cdots, t_{m-1}\}$ *é um sistema completo de resíduos módulo m.*

Proposição 2.8 *Se* $a \equiv b \pmod{m_1}$*,* $a \equiv b \pmod{m_2}$*,* $\cdots$*,* $a \equiv b \pmod{m_k}$ *onde* $a, m_1, m_2, \cdots, m_k$ *são inteiros com* m_i *positivos,* $i = 1, 2, \cdots, k$*, então*

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

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

Demonstração: Seja p_n o maior primo que aparece na fatoração de $m_1, m_2, \cdots, m_k$. Cada m_i, $i = 1, 2, \cdots, k$ pode ser expresso como

$$m_i = p_1^{e_{1i}} p_2^{e_{2i}} \cdots p_n^{e_{ni}},$$

sendo que alguns e_{ji} podem ser nulos. Como $m_i \mid (a-b), \forall i = 1, 2, \cdots, k$ temos $p_j^{e_{ji}} \mid (a-b), i = 1, 2, \cdots, k$, $j = 1, 2, \cdots, n$. Logo se tomarmos

$$e_j = \max_{1 \leq i \leq k} \{e_{ji}\}$$

teremos que

$$p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \mid (a - b).$$

Mas,

$$p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} = [m_1, m_2, \cdots, m_k]$$

o que implica $a \equiv b \pmod{[m_1, m_2, \cdots, m_k]}$

■

2.6.2 Congruência Linear

Uma congruência linear na variável x é uma congruência da forma $ax \equiv b \pmod{m}$ onde x é uma incógnita e a, b, m são inteiros e $m > 0$

Se x_0 é uma solução, isto é, $ax_0 \equiv b \pmod{m}$ e $x_1 \equiv x_0 \pmod{m}$ então x_1 também é solução já que $ax_1 \equiv ax_0 \equiv b \pmod{m}$. Dessa forma, se um representante de uma classe de equivalência, definida pela relação de equivalência, é solução, então todo elemento dessa classe é solução.

Exemplo 2.9 *A congruência* $5x \equiv 9 \ (mod 11)$ *tem como solução* $x_0 = 4$. *O fato de* $15 \equiv 4 \ (mod\ 11)$*, garante que* 15 *pertença à mesma classe do* 4*, sendo também, solução da congruência.*

O Teorema a seguir apresenta o critério que garante se uma congruência linear tem solução ou não. Além disso, o Teorema também trata a respeito da quantidade de soluções incongruentes das congruências resolúveis.

Antes de apresentá-lo, porém, é necessário observar que um inteiro x_0 é solução de $ax \equiv b \pmod{m}$ se, e somente se, existe inteiro y tal que $ax_0 = b + my$, ou, reescrevendo $ax_0 - my = b$. Essa relação entre congruências lineares e equações diofantinas lineares será utilizada para demonstrar o Teorema que se segue.

Teorema 2.6 *Sejam* $a, b, m \in \mathbb{Z}$ *tais que* $m > 0$ *e* $(a, m) = d$. *A congruência* $ax \equiv b \ (mod\ m)$ *possui solução se, somente se,* $d \mid b$. *Quando isso ocorre, ela possui exatamente d soluções incongruentes módulo m.*

Demonstração: Do fato de $ax \equiv b \pmod{m}$ possuir solução se, somente se, $ax - my = b$ também possuir, concluímos que, para que essa congruência seja solúvel é condição necessária e suficiente que $d \mid b$.

Quando isso ocorre ela possui infinitas soluções, dadas por

$$(x_k, y_k) = (x_0 - (m/d)k, y_0 - (a/d)k)$$

onde (x_0, y_0) é uma solução particular de $ax - my = b$. Portanto, a congruência $ax \equiv b \pmod{m}$ possui infinitas soluções dadas por

$$x_k = x_0 - \left(\frac{m}{d}\right)k.$$

Estamos interessados em saber o número de soluções incongruentes. Para verificar isso, tomaremos as soluções

$$x_{k_1} = x_0 - \left(\frac{m}{d}\right)k_1 \text{ e } x_{k_2} = x_0 - \left(\frac{m}{d}\right)k_2,$$

para descobrir sob que condições são congruentes. Se x_1 e x_2 são congruêntes módulo m, temos

$$\left(x_0 - \left(\frac{m}{d}\right)k_1\right) \equiv \left(x_0 - \left(\frac{m}{d}\right)k_2\right) \pmod{m}$$

o que implica

$$\left(\frac{m}{d}\right)k_1 \equiv \left(\frac{m}{d}\right)k_2 \pmod{m}.$$

Como $\left(\frac{m}{d}\right)$ temos $(m/d, m) = m/d$. Assim $d = \dfrac{m}{\left(\frac{m}{d}\right)}$, o que implicando que $k_1 \equiv k_2 \pmod{d}$. Concluímos assim, que as soluções incongruentes são obtidas ao tomarmos $k_1 \neq k_2$ e isso ocoree quando k percorre um sitema completo de resíduos módulo d.

■

Exemplo 2.10 *É interessante perceber que a congruência* $8x \equiv 4$ (*mod* 12) *é equivalente a resolver a equação* $8x + 12y = 4$. *Essa congruência tem* 4 *soluções, uma vez que* $(8, 12) = 4$. *Tomando* $x_0 = 2$ *temos*

$$x_k = x_0 - \left(\frac{12}{4}\right)k = x_0 - 3k$$

onde $k = 0, 1, 2, 3$. *Assim temos:*

$$x_0 = 2 - 0 \equiv 2 \ (mod\ 12)$$
$$x_1 = 2 - 3 = -1 \equiv 11 \ (mod\ 12)$$
$$x_2 = 2 - 6 = -4 \equiv 8 \ (mod\ 12)$$
$$x_3 = 2 - 9 = -7 \equiv 5 \ (mod\ 12)$$

Assim, as soluções são dadas por $2, 5, 8$ *e* 11. *Por outro lado, a congruência*

$$4x \equiv 9 \ (mod\ 16)$$

não possui solução, uma vez que $(4, 16) = 4$ *e* $4 \nmid 9$.

O teorema, anterior, além de precisar a quantidade de soluções de uma congruência linear, garante que elas são da forma

$$x_0 - \left(\frac{m}{d}\right)k,$$

onde x_0 é uma solução particular e $0 \leq k < d$. Com os próximos resultados, será possível caracterizar a solução particular e consequntemente definir com mais precisão todas as soluções incongruentes de uma congruência linear.

Definição 2.8 *Dizemos que uma solução* x_0 *de* $ax \equiv b \ (mod\ m)$ *é única módulo* m *quando qualquer outra solução* x_1 *for congruente a* x_0 *módulo* m.

Definição 2.9 *Uma solução* $\overline{a}$ *de* $ax \equiv 1 \ (mod\ m)$ *é chamada de inverso de* a *módulo* m.

Do Teorema 2.6 segue que se $(a, m) = 1$, a possui um único inverso módulo m. Caso $(a, m) \neq 1$, a não possui inverso, uma vez que a congruência $ax \equiv 1 \ (\text{mod}\ m)$ não tem solução, já que $(a, m) \nmid 1$.

Exemplo 2.11 *Como as congruências* $8x \equiv 1 \ (mod 51)$ *e* $8x \equiv 1 \ (mod 63)$*, tem solução dadas, respectivamente, por* 32 *e* 8*, dizemos que* 32 *é o inverso de* 8 *módulo* 51 *e* 8 *é seu próprio inverso módulo* 63. *Esse fato será caracterizado a seguir.*

Proposição 2.9 *Seja* p *um número primo. O inteiro positivo* a *é seu próprio inverso módulo* p *se, e somente se,* $a \equiv 1 \ (mod\ p)$ *ou* $a \equiv -1 \ (mod\ p)$.

Demonstração: Se a é seu próprio inverso $a^2 \equiv 1 \pmod{p}$. Logo $p \mid (a^2 - 1)$, ou seja, $p \mid (a+1)(a-1)$. Como p é primo, $p \mid (a+1)$ ou $p \mid (a-1)$, o que implica em $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$. Facilmente verifica-se que a recíproca é verdadeira.

■

2.6.3 O Teorema Chinês do Resto

Teorema 2.7 (Teorema Chinês do Resto) *Se $(a_i, m_i) = 1$, $(m_i, m_j) = 1$ para $i \neq j$ e a_i, b_i, c_i, m_i inteiros, com $i = 1, \cdots, r$, então o sistema*

$$\begin{cases} a_1 x \equiv c_1 \ (mod\ m_1) \\ a_2 x \equiv c_2 \ (mod\ m_2) \\ a_3 x \equiv c_3 \ (mod\ m_3) \\ \qquad \vdots \\ a_r x \equiv c_r \ (mod\ m_r) \end{cases}$$

possui solução única módulo $m = m_1 m_2 \cdots m_r$.

Demonstração: É importante observar que, como cada uma das equações tem solução o sistema pode ser reescrito da forma

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ x \equiv b_3 \pmod{m_3} \\ \qquad \vdots \\ x \equiv b_r \pmod{m_r} \end{cases}$$

onde os $b_i's$ são as soluções. Consideremos os números $n_i = \dfrac{m}{m_i}$. Dessa forma, $(n_i, m_i) = 1$, já que $(m_i, m_j) = 1$ para $i \neq j$. Logo $n_i x \equiv 1 \pmod{m_i}$ possui solução única que denotaremos por $\overline{n_i}$. Portanto, $n_i \overline{n_i} \equiv 1 \pmod{m_i}$, com $i = 1, 2, \cdots, r$. Assim, temos o número dado por

$$x_0 = b_1 n_1 \overline{n_1} + b_2 n_2 \overline{n_2} + \cdots + b_r n_r \overline{n_r}$$

solução para todas as equações. De fato, quando $i \neq j$, n_j é múltiplo de m_i e portanto $n_j \overline{n_j} \equiv$

0 (mod m_i). Assim temos

$$x_0 = b_1 n_1 \overline{n_1} + b_2 n_2 \overline{n_2} + \cdots + b_i n_i \overline{n_i} + \cdots + b_r n_r \overline{n_r}$$
$$x_0 \equiv b_i n_i \overline{n_i} \,(\text{mod } m_i) \equiv b_i \,(\text{mod } m_i)$$

logo, garantindo que x_0 é solução. Supondo x_1 outra solução, obtemos $x_0 \equiv x_1 \,(\text{mod } m_i)$. Logo $m_i \mid x_0 - x_1$ para todo m_i. Os $m_i's$ são dois a dois primos entre si, dessa forma temos $m \mid x_0 - x_1$. Então $x_0 \equiv x_1 \,(\text{mod } m)$, mostrando, assim, que a solução é única módulo m.

■

Exemplo 2.12 *O sistema de congruências*

$$\begin{cases} x \equiv 1 \,(mod\ 5) \\ x \equiv 2 \,(mod\ 7) \\ x \equiv 3 \,(mod\ 11) \end{cases}$$

Como $(5,7) = (5,11) = (7,11) = 1$ *o sistema tem solução. Logo* $m = 5 \times 7 \times 11 = 385$ *e* $n_1 = 7 \times 11$, $n_2 = 5 \times 11$ *e* $n_3 = 5 \times 7$. *Para determinar os* $\overline{n_i}'s$ *basta resolver*

$$7 \times 11\overline{n_1} \equiv 1 \,(mod\ 5) \Rightarrow 2\overline{n_1} \equiv 1 \,(mod\ 5) \Rightarrow \overline{n_1} = 3$$
$$5 \times 11\overline{n_2} \equiv 1 \,(mod\ 7) \Rightarrow 2\overline{n_2} \equiv 1 \,(mod\ 7) \Rightarrow \overline{n_2} = 6$$
$$5 \times 7\overline{n_3} \equiv 1 \,(mod\ 11) \Rightarrow 2\overline{n_2} \equiv 1 \,(mod\ 11) \Rightarrow \overline{n_3} = 6$$

Como $b_1 = 1$, $b_2 = 2$, $b_3 = 3$ *temos*

$$x_0 = b_1 n_1 \overline{n_1} + b_2 n_2 \overline{n_2} + b_3 n_3 \overline{n_3}$$
$$x_0 = 1 \times 77 \times 3 + 21 \times 55 \times 6 + 31 \times 35 \times 6$$
$$x_0 \equiv 366 \,(mod\ 385).$$

Esse Teorema será de grande importância na busca das soluções de um Congruência Quadrática, apresentada no próximo Capítulo. É necessário, porém, observar que, para que o sistema tenha solução é necessário que cada uma das Congruências seja solúvel.

2.7 Teoremas Fermat e Wilson

Teorema 2.8 (Wilson) *Se p é primo, então* $(p-1)! \equiv -1$ *(mod p).*

Demonstração: Pelo Teorema (2.6) sabemos que a congruência $ix \equiv 1 \pmod{p}$, em que $i \in \{1, 2, \cdots, p-1\}$, possui solução única módulo p. Assim existe $j \in \{1, 2, \cdots, p-1\}$ tal que $ij \equiv 1 \pmod{p}$. De acordo com a Proposição (2.9) sabemos que se $i^2 \equiv 1 \pmod{p}$ então $i \equiv 1 \pmod{p}$ ou $i \equiv -1 \equiv p-1 \pmod{p}$. Assim, ao agruparmos os pares (i, j) tais que $ij \equiv 1 \pmod{p}$ e $i \neq j$ obtemos

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

e portanto

$$1 \cdot 2 \cdots (p-2)(p-1) \equiv p-1 \equiv -1 \pmod{p}.$$

■

Teorema 2.9 *Se n é um inteiro tal que* $(n-1)! \equiv -1$ *(mod n), então n é primo.*

Demonstração: Suponhamos que n não seja primo e $(n-1)! \equiv -1 \pmod{n}$, ou seja, $n \mid ((n-1)!+1)$. Logo existem r e s tal que $n = rs$ tal que $1 < r, s < n$. Dessa forma $r \mid (n-1)!$ e, como r é um divisor de n, $r \mid ((n-1)!+1)$. Logo deve, também, dividir a diferença $(n-1)!+1-(n-1)! = 1$ o que é um absurso já que $r > 1$. Portanto, n deve ser primo.

■

Teorema 2.10 (Pequeno Teorema de Fermat) *Seja p primo. Se $p \nmid a$ então* $a^{p-1} \equiv 1$ *(mod p).*

Demonstração: O conjunto $\{0, 1, \cdots, p-1\}$ forma um sistema completo de resíduo módulo p. Assim, qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0, 1, \cdots, p-1\}$. Consideremos os números $a, 2a, \cdots, (p-1)a$. Como (a, p)=1, nenhum desses números é congruênte a zero módulo p e são todos incongruentes módulo p, já que $aj \equiv ak \pmod{p}$ implica que $j \equiv k \pmod{p}$ e isto só acontece quando $j = k$.

Temos, então, um conjunto de $p-1$ elementos incongruentes módulo p e não divisíveis por p. Logo, cada um deles é congruente um dos elementos do conjunto $\{1, 2, \cdots, p-1\}$. Assim temos

$$a(2a)(3a) \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},$$

ou seja,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

O fato de $((p-1)!, p) = 1$ nos permite cancelar o fator $(p-1)!$ de ambos os lados, obtendo $a^{p-1} \equiv 1 \pmod{p}$.

■

Corolário 2.1 *Se p é primo e a é um inteiro positivo, então $a^p \equiv a \pmod{p}$.*

Demonstração: É necessário analisar dois casos: $p \mid a$ e $p \nmid a$. No primeiro caso obtemos $p \mid a(a^{p-1} - 1)$ o que implica em $a^p \equiv a \pmod{p}$. No segundo caso segue do Teorema anterior que $p \mid (a^{p-1} - 1)$, donde $p \mid a(a^{p-1} - 1)$ implicando em $p \mid (a^p - a)$ e assim $a^p \equiv a \pmod{p}$.

■

2.8 Resíduos Quadráticos

Vamos responder a seguinte questão: se p é um primo ímpar e a um inteiro positivo relativamente primo com p, quando a é um quadrado módulo p?

Definição 2.10 *Seja m um inteiro positivo e a um inteiro positivo com $(a, m) = 1$. Dizemos que a é um resíduo quadrático módulo m, se exite $x \in \mathbb{Z}$ tal que $x^2 \equiv a \pmod{m}$. Caso não exista tal inteiro x, dizemos que a é um resíduo não quadrático módulo m.*

Exemplo 2.13 *Note que*

$$\begin{array}{lll} 1^2 \equiv 1 \pmod{7}, & 2^2 \equiv 4 \pmod{7}, & 3^2 \equiv 2 \pmod{7} \\ 4^2 \equiv 2 \pmod{7}, & 5^2 \equiv 4 \pmod{7}, & 6^2 \equiv 1 \pmod{7}. \end{array}.$$

Logo $1, 2$ e 4 são resíduos quadráticos módulo 7 e $3, 5$ e 6 são resíduos não quadráticos módulo 7. Também escrevemos $\mathbf{RQ_7} = \{1, 2, 4\}$ e $\mathbf{RNQ_7} = \{3, 5, 6\}$.

Exemplo 2.14 *Quais os inteiros são resíduos quadráticos módulo 11? Note que*

$$\begin{array}{lllll} 1^2 \equiv 1 \pmod{11} & 2^2 \equiv 4 \pmod{11} & 3^2 \equiv 9 \pmod{11} & 4^2 \equiv 5 \pmod{11} & 5^2 \equiv 3 \pmod{11} \\ 6^2 \equiv 3 \pmod{11} & 7^2 \equiv 5 \pmod{11} & 8^2 \equiv 9 \pmod{11} & 9^2 \equiv 4 \pmod{11} & 10^2 \equiv 1 \pmod{11} \end{array}.$$

Assim $\mathbf{RQ_{11}} = \{1, 3, 4, 5, 9\}$. Observe que $\mathbf{RNQ_{11}} = \{2, 6, 7, 8, 10\}$.

Agora vamos determinar o número de inteiros que são resíduos quadráticos módulo p primo.

Teorema 2.11 *Se p é um primo ímpar, então existem exatamente $\frac{(p-1)}{2}$ resíduos quadráticos módulo p e $\frac{(p-1)}{2}$ resíduos não quadrático módulo p.*

Demonstração: Para encontrar todas os resíduos quadráticos módulo p entre os inteiros

$$1, 2, 3, 4, \cdots, p-1,$$

calculamos os quadrados módulo p desses $(p-1)$ inteiros

$$1^2, 2^2, 3^2, 4^2, \cdots, (p-1)^2 \pmod{p}.$$

Pela Proposição (3.1) da página 51, $x^2 \equiv a \pmod{p}$ não tem solução ou tem duas soluções incongruêntes módulo p, segue que temos $\frac{(p-1)}{2}$ resíduos quadráticos módulp p entre os inteiros $1, 2, 3, 4, \cdots, p-1$. Os $(p-1) - \frac{(p-1)}{2} = \frac{(p-1)}{2}$ inteiros positivos restantes são resíduos não quadráticos módulo p.

■

Definição 2.11 *Seja p primo ímpar e a um inteiro positivo tal que $p \nmid a$. O Símbolo de Legendre $\left(\frac{a}{p}\right)$ é definido por*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & se \quad a \text{ é um resíduo quadrático módulo } p \\ -1 & se \quad a \text{ é um resíduo não quadrático módulo } p \end{cases}$$

Exemplo 2.15 $\left(\frac{3}{11}\right) = 1$, *pois existe $x \in \mathbb{Z}$ tal que $x^2 \equiv 3 \pmod{11}$, por exemplo $x = 5$ e 6.*

Exemplo 2.16 $\left(\frac{2}{11}\right) = -1$, *pois não existe $x \in \mathbb{Z}$ tal que $x^2 \equiv 2 \pmod{11}$.*

Agora, temos interesse em responder a seguinte questão: Quando um inteiro é um resíduo quadrático módulo p primo?

Primeiro vamos lembrar que:

Observação 2.1 *Sejam $a, b, m \in \mathbb{Z}$ com $m > 0$ e $d = (a, m)$:*

i) *se $d \nmid b$, então a congruência $xa \equiv b \pmod{p}$, não tem solução,*

ii) *se $d \mid b$, então a congruência $xa \equiv b \pmod{p}$, tem exatamente d soluções incongruentes módulo m.*

Teorema 2.12 (Critério de Euler) *Seja p um primo ímpar e a um inteiro positivo tal que $p \nmid a$. Então*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}} \pmod{p}.$$

Demonstração: Suponha que $\left(\frac{a}{p}\right) = 1$, ou seja, a congruência $x^2 \equiv a \pmod{p}$ tem solução, digamos $x = x_0$, logo $x_0^2 \equiv a \pmod{p}$. Pelo Teorema de Fermat $a^{p-1} \equiv 1 \pmod{p}$, assim $a^{\frac{(p-1)}{2}} \equiv (x_0^2)^{\frac{(p-1)}{2}} \equiv (x_0)^{p-1} \equiv 1 \pmod{p}$. Então $a^{\frac{(p-1)}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$. Suponha que $\left(\frac{a}{p}\right) = -1$, ou seja, a congruência $x^2 \equiv a \pmod{p}$ não tem solução. Pelo item ii) da observação anterior, temos para cada k com $1 \leq k \leq p-1$, $(k, p) = 1$ um único inteiro l tal que $k \cdot l \equiv a \pmod{p}$. Como $x^2 \equiv a \pmod{p}$ não tem solução segue que $k \neq l$. Portanto agrupando os inteiros $1, 2, 3, 4, \cdots, p-1$ em $\frac{(p-1)}{2}$ pares (kl) cujo produto $kl \equiv a \pmod{p}$, obtemos

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots \cdot (p-2)(p-1) \equiv a^{\frac{(p-1)}{2}} \pmod{p}$$
$$(p-1)! \equiv a^{\frac{(p-1)}{2}} \pmod{p}.$$

Pelo teorema de Wilson

$$a^{\frac{(p-1)}{2}} \equiv (p-1)! \equiv -1 \pmod{p}$$

então $\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}} \pmod{p}$.

■

Exemplo 2.17 *Para $p = 23$ e $a = 5$, temos $5^{11} \equiv -1 \pmod{23}$. Logo $\left(\frac{5}{23}\right) = -1$, portanto 5 é um* $\mathbf{RNQ_{23}}$.

Algumas Propriedades do Símbolo de Legrendre.

Teorema 2.13 *Seja p primo ímpar e a, b são inteiros não divisíveis por p*

i *se $a \equiv b \pmod{p}$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$*

ii $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

iii $\left(\frac{a^2}{p}\right) = 1$

Demonstração:

i se $a \equiv b \pmod{p}$, então $x^2 \equiv a \pmod{p}$ tem solução se e somente se

$$x^2 \equiv b \pmod{p}$$

tem solução. Portanto $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$.

ii Por hipótese e pelo Critério de Euler $\left(\frac{a}{p}\right) = a^{\frac{(p-1)}{2}} \pmod{p}$, $\left(\frac{b}{p}\right) = b^{\frac{(p-1)}{2}} \pmod{p}$ e $\left(\frac{ab}{p}\right) = (ab)^{\frac{(p-1)}{2}} \pmod{p}$. Então

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{\frac{(p-1)}{2}} b^{\frac{(p-1)}{2}} = (ab)^{\frac{(p-1)}{2}} \equiv \left(\frac{ab}{p}\right)$$

.

iii Como $\left(\frac{a}{p}\right) = \pm 1$, por *ii*) $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^2 = (\pm 1)^2 = 1$.

■

Observação 2.2 *Por ii) do Teorema anterior: Seja p um primo ímpar e a um inteiro positivo tal que* $p \nmid a$. *Vamos escrever* $a = \pm 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, *então*

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}}{p}\right) = \left(\frac{2^{\alpha}}{p}\right)\left(\frac{p_1^{\alpha_1}}{p}\right)\left(\frac{p_2^{\alpha_2}}{p}\right)\cdots\left(\frac{p_k^{\alpha_k}}{p}\right)$$

Exemplo 2.18 $\left(\frac{75}{97}\right) = \left(\frac{3 \cdot 5 \cdot 5}{97}\right) = \left(\frac{3}{97}\right)\left(\frac{5^2}{97}\right)$. *Como* $10^2 \equiv 3 \pmod{97}$ *e* $\left(\frac{5^2}{97}\right) = 1$, *temos* $\left(\frac{75}{97}\right) = (1)(1) = 1$.

O próximo resultado, conhecido como Lema de Gauss, nos dará mais um método para determinar $\left(\frac{a}{p}\right)$, para todo primo ímpar p e todo número natural a, tal que $(a, p) = 1$.

Proposição 2.10 (Lema de Gauss) *Seja p um primo ímpar e a um inteiro não divisível por p. Então*

$$\left(\frac{a}{p}\right) = (-1)^s,$$

onde s é a quantidade de resíduos positivos módulo p dos números

$$a, 2a, 3a, ..., \left(\frac{p-1}{2}\right)a,$$

que são maiores que $\frac{p}{2}$.

Demonstração: Considere os inteiros $a, 2a, 3a, \cdots, \frac{(p-1)}{2}a$. Sejam $u_1, u_2, \cdots, u_s$, os menores resíduos positivos destes inteiros que são maiores do que $\frac{p}{2}$ e $v_1, v_2, \cdots, v_t$, os menores resíduos positivos que são menores do que $\frac{p}{2}$. Como

$$(a, p) = (2a, p) = (3a, p) = \cdots = \left(\frac{(p-1)}{2}a, p\right) = 1,$$

estes menores resíduos são menores do que p, ou seja, estão entre 1 e $p-1$.

Os inteiros

$$p - u_1, p - u_2, \cdots, p - u_s, v_1, v_2, \cdots, v_t \tag{2.3}$$

são exatamente os inteiros $1, 2, 3, 4, \cdots, \frac{(p-1)}{2} \pmod{p}$. De fato, quaisquer dois inteiros de (2.3) não são congruentes módulo p, pois existem exatamente $\frac{(p-1)}{2}$ inteiros em (2.3) e todos são inteiros positivos maiores ou iguais a $\frac{(p-1)}{2}$. Em outras palavras,

$$u_i \not\equiv u_j \pmod{p} \text{ e } v_i \not\equiv v_j \pmod{p}, \forall i \neq j.$$

Caso uma dessas congruências venha ocorrer, teríamos

$$ma \equiv na \pmod{p}$$

onde m e n são inteiros positivos com $1 \leq m \leq \frac{(p-1)}{2}$ e $1 \leq n \leq \frac{(p-1)}{2}$. Como $(a, p) = 1$ teríamos

$$m \equiv n \pmod{p}$$

o que seria impossível, pois $1 \leq m \leq \frac{(p-1)}{2}$ e $1 \leq n \leq \frac{(p-1)}{2}$. Também temos $p - u_i \not\equiv v_j \pmod{p}$. Caso fosse congruente, teríamos

$$p - ma \equiv na \pmod{p}$$

$$-ma \equiv na \pmod{p}.$$

Como $(a, p) = 1$ teríamos $ma \equiv -na \pmod{p}$ o que seria impossível, pois

$$1 \leq m \leq \frac{(p-1)}{2} \text{ e } 1 \leq n \leq \frac{(p-1)}{2}.$$

Portanto

$$p - u_1, p - u_2, \cdots, p - u_s, v_1, v_2, \cdots, v_t$$

são os inteiros $1, 2, 3, \cdots, \frac{(p-1)}{2}$ em alguma ordem. Então

$$\begin{aligned} (p-u_1)(p-u_2)\cdots(p-u_s)\cdot v_1 \cdot v_2 \cdot \cdots \cdot v_t &\equiv \left(\frac{(p-1)}{2}\right)! \pmod{p} \\ (-1)^s(u_1)(u_2)\cdots(u_s).v_1.v_2\cdots v_t &\equiv \left(\frac{(p-1)}{2}\right)! \pmod{p} \end{aligned} \tag{2.4}$$

Como $u_1, u_2, \cdots, u_s, v_1, v_2, \cdots, v_t$ são os menores resíduos positivos de

$$a, 2a, 3a, 4a, \cdots, \frac{(p-1)}{2}a \pmod{p}$$

temos

$$\begin{aligned} u_1 \cdot u_2 \cdot \cdots \cdot u_s \cdot v_1 \cdot v_2 \cdot \cdots \cdot v_t &\equiv a, 2a, 3a, 4a, \cdots, \frac{(p-1)}{2}a \pmod{p} \\ u_1 \cdot u_2 \cdot \cdots \cdot u_s \cdot v_1 \cdot v_2 \cdot \cdots \cdot v_t &\equiv a^{\frac{(p-1)}{2}}.\left(\frac{(p-1)}{2}\right)! \pmod{p}. \end{aligned} \tag{2.5}$$

De (2.4) e (2.5), temos

$$(-1)^s a^{\frac{(p-1)}{2}} \cdot \left(\frac{(p-1)}{2}\right)! \equiv \left(\frac{(p-1)}{2}\right)! \pmod{p}.$$

Como $\left(\left(\frac{(p-1)}{2}\right)!, p\right) = 1$, segue que

$$(-1)^s a^{\frac{(p-1)}{2}} \equiv 1 \pmod{p}$$

multiplicando por $(-1)^s$, obtemos

$$a^{\frac{(p-1)}{2}} \equiv (-1)^s \pmod{p}$$

Pelo Critério de Euler

$$\left(\frac{a}{p}\right) \equiv (-1)^s \pmod{p}$$

■

Exemplo 2.19 *5 é um resíduo quadrático módulo* 11*? Queremos calcular* $\left(\frac{5}{11}\right)$*. Pelo Lema de Gauss, Devemos calcular o número dos menores resíduos positivos dos inteiros*

$$1 \cdot 5, 2 \cdot 5, 3 \cdot 5, 3 \cdot 5, 4 \cdot 5, 5 \cdot 5 \ (mod\ 11) = 5, 10, 4, 9, 3.$$

Logo existem exatamente dois desses números maiores do que $\frac{p}{2} = \frac{11}{2} = 5,5$*, que são* 10 *e* 9*. Portanto* $\left(\frac{5}{11}\right) = (-1)^2 = 1$*, logo 5 é um resíduo quadrático módulo 11.*

2.8.1 Lei da Reciprocidade Quadrática

Segundo Hefez (2006), Gauss demonstrou, em 1796 aos dezoito anos, o belo Teorema da Reciprocidade Quadrática, anteriormente descoberto, sem demonstração completa, por Euler e Legendre. Atualmente existem 2071 demonstrações da Lei da Reciprocidade Quadrática (Mota, 2006).

Teorema 2.14 (Lei da Reciprocidade Quadrática) *Sejam p e q primos ímpares distintos. Então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{q-1}{2}}.$$

Três demonstrações distintas podem ser encontradas em Araújo (2013).

Observação 2.3 *Também podemos escrever* $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$.

Observação 2.4

$$\begin{cases} \dfrac{(p-1)}{2} & \text{é par quando} \quad p \equiv 1 \ (mod\ 4) \\ \dfrac{(p-1)}{2} & \text{é ímpar quando} \quad p \equiv 3 \ (mod\ 4). \end{cases}$$

Segue que

1. $\frac{(p-1)}{2}\frac{(q-1)}{2}$ *é par quando*

$$\begin{cases} p \equiv 1 \ (mod\ 4) \quad e \quad q \equiv 1 \ (mod\ 4) \\ \qquad\qquad\qquad ou \\ p \equiv 1 \ (mod\ 4) \quad e \quad p \equiv 3 \ (mod\ 4). \end{cases}$$

2. $\frac{(p-1)}{2}\frac{(q-1)}{2}$ *é ímpar quando*

$$\begin{cases} p \equiv 3 \ (mod\ 4) \\ \qquad e \\ q \equiv 3 \ (mod\ 4). \end{cases}$$

Portanto

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \begin{array}{l} se\ p \equiv 1 \ (mod\ 4)\ e\ q \equiv 1 \ (mod\ 4) \\ ou\ p \equiv 1 \ (mod\ 4)\ e\ q \equiv 3 \ (mod\ 4) \end{array} \\ -1 & se\ p \equiv 3 \ (mod\ 4)\ e\ q \equiv 3 \ (mod\ 4). \end{cases}$$

Como $\left(\frac{p}{q}\right) = \pm 1$ *e* $\left(\frac{q}{p}\right) = \pm 1$, *escrevemos*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \begin{array}{l} se\ p \equiv 1 \ (mod\ 4)\ e\ q \equiv 1 \ (mod\ 4) \\ ou\ p \equiv 1 \ (mod\ 4)\ e\ q \equiv 3 \ (mod\ 4) \end{array} \\ -\left(\frac{q}{p}\right) & se\ p \equiv 3 \ (mod\ 4)\ e\ q \equiv 3 \ (mod\ 4). \end{cases}$$

Podemos dizer que se p e q são primos ímpares, então $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, *a não ser que* $p \equiv 3 \ (mod\ 4)$ *e* $q \equiv 3 \ (mod\ 4)$ *que neste caso* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Exemplo 2.20 *Calcule* $\left(\frac{713}{1009}\right)$

- $p = 713 = 23 \cdot 31$ *e* $q = 1009$ *é primo.*
- *Pelo Teorema 2.13-ii da página 35:* $\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$.
- *Como* $1009 \equiv 1 \ (mod\ 4)$ *e* $23 \equiv 31 \equiv 1 \ (mod\ 4)$, *pela Observação 2.4:* $\left(\frac{23}{1009}\right) = \left(\frac{1009}{23}\right)$ *e* $\left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right)$.
- *Como* $1009 \equiv 20 \ (mod\ 23)$ *e* $1009 \equiv 17 \ (mod\ 31)$, *pelo Teorema 2.13-i:* $\left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right)$ *e* $\left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right)$.
- *Pelo Teorema 2.13-ii-iii:* $\left(\frac{20}{23}\right) = \left(\frac{4.5}{23}\right) = \left(\frac{2^2}{23}\right)\left(\frac{5}{23}\right) = 1 \cdot \left(\frac{5}{23}\right)$.

- *Como* $5 \equiv 1 \ (mod\ 4)$ *e* $23 \equiv 3 \ (mod\ 4)$*, pela Observação 2.4 e pelo Teorema 2.13-i* $\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right)$
- *Como* $5 \equiv 1 \ (mod\ 4)$ *e* $5 \equiv 2 \ (mod\ 3)$*, pela Observação 2.4 e o Teorema 2.13-i:* $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right)$.
- *Pelo Critério de Euler* $\left(\frac{2}{3}\right) \equiv (-1)^{\frac{3-1}{2}} = 2 \equiv -1 \ (mod\ 3)$. *Assim* $\left(\frac{23}{1009}\right) = -1$.
- *Como* $17 \equiv 1 \ (mod\ 4)$*, pela Observação 2.4:* $\left(\frac{17}{31}\right) = \left(\frac{31}{17}\right)$.
- *Como* $31 \equiv 14 \ (mod\ 17)$*, pelo Teorema 2.13-i:* $\left(\frac{31}{17}\right) = \left(\frac{14}{17}\right)$.
- *Pelo Teorema 2.13-ii:* $\left(\frac{14}{17}\right) = \left(\frac{2 \cdot 7}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right)$ *e pelo Critério de Euler* $\left(\frac{2}{17}\right) \equiv 2^{\frac{17-1}{2}} \equiv 1 \ (mod\ 17)$.
  Logo $\left(\frac{14}{17}\right) = \left(\frac{7}{17}\right)$. *Como* $7 \equiv 3 \ (mod\ 4)$*, pela Observação 2.4:* $\left(\frac{7}{17}\right) = \left(\frac{17}{7}\right)$
- *Como* $17 \equiv 3 \ (mod\ 7)$*, pelo Teorema 2.13-i;* $\left(\frac{3}{7}\right) = \left(\frac{3}{7}\right)$

  Como $7 \equiv 3 \ (mod\ 4)$ *e* $3 \equiv 3 \ (mod\ 4)$*, pela Observação 2.4:* $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right)$

  Como $7 \equiv 1 \ (mod\ 3)$*, pelo Teorema 2.13-i:* $-\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = 1$.

  Assim $\left(\frac{31}{1009}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$.

  Portanto $\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right) = (-1)(-1) = 1$.

Como consequência da Lei da Reciprocidade Quadrática temos que:

Corolário 2.2 *Seja p um número primo ímpar. Tem-se*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, \ se\ p \equiv 1\ ou\ p \equiv 7 \ (mod\ 8) \\ -1, \ se\ p \equiv 3\ ou\ p \equiv 5 \ (mod\ 8) \end{cases}$$

Demonstração: (Vamos usar o Lema de Gauss). Se s é o número dos menores resíduos postivo dos inteiros

$$1.2, 2.2, 3.2, \ldots, \frac{(p-1)}{2}.2$$

que são maiores do que $\frac{p}{2}$, então

$$\left(\frac{2}{p}\right) = (-1)^s .$$

Todos esses inteiros são menores do que p, entre eles precisamos contar os que são maiores do que $\frac{p}{2}$, para encontrar quantos são os menores do que $\frac{p}{2}$, ou seja, para encontrar o nosso s. Note que o inteiro $2j$ para $1 \leq j \leq \frac{(p-1)}{2}$ é menor do que $\frac{p}{2}$ (pois $2\ j \leq \frac{p}{2}$ logo $j \leq \frac{p}{4}$) quando $j \leq \frac{p}{4}$. Então existem inteiros $\left[\frac{p}{4}\right]$ no conjunto

$$\left\{1.2, 2.2, 3.2, \ldots, \frac{(p-1)}{2}.2\right\}$$

que são menores do que $\frac{p}{2}$. Consequentemente existem

$$s = \frac{(p-1)}{2} - \left[\frac{p}{4}\right]$$

maiores do que $\frac{p}{2}$. Portanto pelo lema de Gauss $\left(\frac{2}{p}\right) = (-1)^{\frac{(p-1)}{2} - \left[\frac{p}{4}\right]}$.Afirmamos que

$$s = \frac{(p-1)}{2} - \left[\frac{p}{4}\right] = \frac{\left(p^2-1\right)}{8} \pmod 2 .$$

De fato, Precisamos cosiderar as classes de congrências de p módulo 8, em dois casos:

1^o) Consideremos $\dfrac{\left(p^2-1\right)}{8}$ Se $p \equiv \pm 1 \pmod 8$, então $p = 8k \pm 1$ para $k \in \mathbb{Z}$, logo

$$\frac{\left(p^2-1\right)}{8} = \frac{\left((8k \pm 1)^2 - 1\right)}{8} = \frac{64k^2 \pm 16k + 1 - 1}{8} = \frac{8\left(8k^2 \pm 2k\right)}{8}$$

$$\frac{\left(p^2-1\right)}{8} = \left(8k^2 \pm 2k\right) = 2k\,(4k \pm 1) \equiv 0 \pmod 2 .$$

Se $p \equiv \pm 3 \pmod 8$, então $p \equiv 8k \pm 3$ para $k \in \mathbb{Z}$, logo

$$\frac{\left(p^2-1\right)}{8} = \frac{\left((8k \pm 3)^2 - 1\right)}{8} = \frac{64k^2 \pm 48k + 9 - 1}{8} = \frac{8\left(8k^2 \pm 6k + 1\right)}{8}$$

$$\frac{\left(p^2-1\right)}{8} = \left(8k^2 \pm 6k + 1\right) = 2k\,(4k \pm 3) + 1 \equiv 1 \pmod 2 .$$

2^o) Consideremos $\dfrac{(p-1)}{2} - \left[\dfrac{p}{4}\right]$. Se $p \equiv 1 \pmod 8$, então $p - 1 = 8k$ para $k \in \mathbb{Z}$, logo

$\frac{(p-1)}{2} = 4k$, $\frac{p}{4} = 2k + \frac{1}{4}$ e

$$\frac{(p-1)}{2} - \left[\frac{p}{4}\right] = 4k - \left[2k + \frac{1}{4}\right] = 4k - 2k = 2k \equiv 0 \,(\text{mod } 2)\,.$$

Se $p \equiv 3 \,(\text{mod } 8)$, então $p - 3 = 8k$ para $k \in \mathbb{Z}$, logo $\frac{(p-1)}{2} = 4k + 1$, $\frac{p}{4} = 2k + \frac{3}{4}$ e

$$\frac{(p-1)}{2} - \left[\frac{p}{4}\right] = 4k + 1 - \left[2k + \frac{3}{4}\right] = 4k + 1 - 2k = 2k + 1 \equiv 1 \,(\text{mod } 2)\,.$$

Se $p \equiv 5 \,(\text{mod } 8)$, então $p - 5 = 8k$ para $k \in \mathbb{Z}$, logo $\frac{(p-1)}{2} = 4k + 2$, $\frac{p}{4} = 2k + 1 + \frac{1}{4}$ e

$$\frac{(p-1)}{2} - \left[\frac{p}{4}\right] = 4k + 2 - \left[2k + 1 + \frac{1}{4}\right] = 4k + 2 - (2k + 1) = 2k + 1 \equiv 1 \,(\text{mod } 2)\,.$$

Se $p \equiv 7 \,(\text{mod } 8)$, então $p - 7 = 8k$ para $k \in \mathbb{Z}$, logo $\frac{(p-1)}{2} = 4k + 3$, $\frac{p}{4} = 2k + 3 + \frac{1}{4}$ e

$$\frac{(p-1)}{2} - \left[\frac{p}{4}\right] = 4k + 3 - \left[2k + \frac{7}{4}\right] = 4k + 2 - (2k) = 2k + 2 \equiv 0 \,(\text{mod } 2)\,.$$

Fazendo a comparação das classes de congurências módulo 2 de $\frac{(p-1)}{2} - \left[\frac{p}{4}\right]$ e $\frac{\left(p^2-1\right)}{8}$ com as quatro possíveis classes de congurências do primo p módulo 8, temos

$$\frac{(p-1)}{2} - \left[\frac{p}{4}\right] \equiv \frac{\left(p^2-1\right)}{8} \,(\text{mod } 2)$$

Portanto para todo primo p

$$\left(\frac{2}{p}\right) = (-1)^{\frac{\left(p^2-1\right)}{8}}\,.$$

Em outras palavras

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ se } p \equiv \pm 1 \,(\text{mod } 8) \\ -1 \text{ se } p \equiv \pm 3 \,(\text{mod } 8) \end{cases}\,.$$

Portanto

$$\left(\frac{2}{p}\right) = (-1)^{\frac{\left(p^2-1\right)}{8}} = \begin{cases} 1 \text{ se } p \equiv \pm 1 \,(\text{mod } 8) \\ -1 \text{ se } p \equiv \pm 3 \,(\text{mod } 8) \end{cases}\,.$$

■

Corolário 2.3 *Se p um número primo maior do que* 3. *Então*

$$\left(\frac{3}{p}\right) = \begin{cases} 1, \text{ se } p \equiv 1 \text{ ou } p \equiv 11 \ (mod\ 12) \\ -1, \text{ se } p \equiv 5 \text{ ou } p \equiv 7 \ (mod\ 12). \end{cases}$$

Demonstração: Pela Lei de Reciprocídade Quadrática.

i)

$$\begin{cases} \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \text{ se } p \equiv 1 \pmod 4 \\ \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) \text{ se } p \equiv 3 \pmod 4. \end{cases}$$

Temos $\left(\frac{p}{3}\right) = 1$ se $p \equiv 1 \pmod 3$ e $\left(\frac{p}{3}\right) = -1$ se $p \equiv 2 \pmod 3$. Analizando os casos:

ii) $\left(\frac{3}{p}\right) = 1$ se $p \equiv 1 \pmod 4$ e $p \equiv 1 \pmod 3$, ou se $p \equiv 3 \pmod 4$ e $p \equiv 2 \pmod 3$, ou seja, quando $p \equiv \pm 1 \pmod{12}$.

iii) $\left(\frac{3}{p}\right) = -1$, se $p \equiv 1 \pmod 4$ e $p \equiv 2 \pmod 3$, ou se $p \equiv 3 \pmod 4$ e $p \equiv 1 \pmod 3$, que implica que $p \equiv \pm 5 \pmod{12}$

■

Corolário 2.4 *Se p um número primo maior do que* 5. *Então*

$$\left(\frac{5}{p}\right) = \begin{cases} 1, & \text{se } p \equiv i \ (mod\ 20), i = 1, 3, 7, 9 \\ -1, & \text{se } p \equiv i \ (mod\ 20), i = 11, 13, 17, 19. \end{cases}$$

Demonstração: Pela Lei de Reciprocídade Quadrática.

i)

$$\begin{cases} \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) \text{ se } p \equiv 1 \pmod 4 \text{ ou } p \equiv 3 \pmod 4 \\ \left(\frac{5}{p}\right) = -\left(\frac{p}{5}\right) \text{ não existe, pois } 5 \not\equiv 3 \pmod 4. \end{cases}$$

Temos $\left(\frac{p}{5}\right) = 1$ se $p \equiv 1 \pmod 5$ ou $p \equiv 4 \pmod 5$ e $\left(\frac{p}{5}\right) = -1$ se $p \equiv 2 \pmod 5$ ou $p \equiv 3 \pmod 5$. Analizando os casos:

ii) $\left(\frac{5}{p}\right) = 1$ se $p \equiv 1 \pmod 4$ e $p \equiv 1 \pmod 5$ ou se $p \equiv 1 \pmod 4$ e $p \equiv 4 \pmod 5$ ou se $p \equiv 3 \pmod 4$ e $p \equiv 1 \pmod 5$ ou se $p \equiv 3 \pmod 4$ e $p \equiv 4 \pmod 5$, ou seja, quando $p \equiv \pm 1 \pmod{12}$ ou $p \equiv \pm 11 \pmod{20}$.

iii) $\left(\frac{5}{p}\right) = -1$, se $p \equiv 1 \pmod 4$ e $p \equiv 2 \pmod 5$ ou se $p \equiv 1 \pmod 4$ e $p \equiv 3 \pmod 5$ ou se $p \equiv 3 \pmod 4$ e $p \equiv 2 \pmod 5$ ou se $p \equiv 3 \pmod 4$ e $p \equiv 3 \pmod 5$), implica que $p \equiv \pm 3 \pmod{20}$ ou $p \equiv \pm 7 \pmod{20}$

■

Capítulo 3

Congruência Quadrática

Uma congruência quadrática é uma equação do tipo

$$ax^2 + bx + c \equiv 0 \pmod{n} \tag{3.1}$$

em que x é incógnita, a, b, c são inteiros e n é um número inteiro maior que 1 que não divide a. As Congruências Quadráticas, ao contrário das Congruências Lineares, não possuem uma regra geral de resolução, sendo assim, se faz necessário um estudo mais detalhado das resoluções. Esse capítulo terá como objetivo determinar se uma congruência quadrática é solúvel ou não, além disso, discutir e elencar métodos e ferramentas para determinar as soluções de (3.1).

3.1 Estudo das Congruências Quadráticas

Para analisar as soluções de uma congruência quadrática, tomemos 3. Suponhamos que existe um número primo p que divide a e n. Analisaremos, agora, os seguintes casos:

i) $p|b$ e $p|c$: A congruência pode ser simplificada da seguinte maneira

$$\frac{a}{p}x^2 + \frac{b}{p}x + \frac{c}{p} \equiv 0 \left(\mod \frac{n}{p}\right)$$

.

ii) $p \nmid b$ e $p \mid c$: Neste caso as soluções da congruência são da forma $x = py$, onde $y \in \mathbb{Z}$, pois $ax^2 + bx + c = kn$ e como $p \mid a$, $p \mid n$ e $p \mid c$, temos que $p \mid bx$, já que $bx = kn - ax^2 - c$.

Como $p \nmid b$, segue que $p \mid x$. Ao substituirmos x na congruência obtemos

$$a(py)^2 + bpy + c \equiv 0 \pmod{n}$$

que pode ser simplificada da seguinte maneira

$$apy^2 + by + \frac{c}{p} \equiv 0 \left(\mod \frac{n}{p}\right).$$

iii) $p \mid b$ e $p \nmid c$: Nesse caso, a congruência não possui solução, uma vez que $\frac{c}{p}$ não é um número inteiro. Pois a congruência $ax^2 + bx + c \equiv 0 \pmod{n}$ equivale a $ax^2 + bx + c = nt$, para algum $t \in \mathbb{Z}$, e por sua vez $nt - ax^2 - bx = c$, mas por hipótese p divide a, b e n o que implica que p divide $nt - ax^2 - bx$ logo p divide c, o que é uma contradição.

iv) $p \nmid b$ e $p \nmid c$: Se x é uma solução da congruência, então $p \mid (bx + c)$, ou seja, $bx + c \equiv 0 \pmod{p}$, o que implica em $x \equiv -c\overline{b} \pmod{p}$, em que $\overline{b}$ é o inverso multiplicativo de b módulo p. Assim, existe t tal que $x = tp - cd$, onde $d \equiv \overline{b} \pmod{p}$. Substituindo $x = tp - cd$ na congruência obtemos

$$a(tp - cd)^2 + b(tp - cd) + c \equiv 0 \pmod{n}$$

logo,

$$a(tp - cd)^2 + btp + (c - bcd) \equiv 0 \pmod{n}$$

o que implica em

$$ap^2t^2 + (bp - 2acdp)t + ac^2d^2 + (c - bcd) \equiv 0 \pmod{n}.$$

Temos ac^2d^2 divisível por p, pois, por hipótese a é divisível por p, e ainda, p^2, $(bp - 2acdp)$ são múltiplos de p; desse modo $c - bcd \equiv 0 \pmod{p}$, ou seja, $p \mid (c - bcd)$. Assim, podemos dividir a congruência por p, obtendo uma congruência módulo $\frac{n}{p}$.

Dessa forma, concluímos que se existe um primo p que divide n e a, a congruência não terá solução, caso ela se enquadre no caso *iii*), caso contrário, será equivalente a uma congruência do tipo

$$a'x^2 + b'x + c' \equiv 0 \left(\mod \frac{n}{p}\right),$$

onde $a'p = a$. Caso haja algum outro primo que divide a' e $\frac{n}{p}$ repete-se o processo. Apresentaremos a seguir alguns exemplos .

Exemplo 3.1 *a) A congruência* $28x^2 + 42x + 10 \equiv 0 \ (mod\ 70)$ *tem o fator primo* 2 *comum a todos os termos. Simplificando a congruência pelo caso i), obtemos*

$$14x^2 + 21x + 5 \equiv 0 \ (mod\ 35).$$

É possível perceber que a congruência não possui solução usando o caso iii), uma vez que 7 é um divisor de 14*, de* 21 *e de* 35*, mas não divide* 5*.*

b) Agora na congruência $5x^2 + 4x + 10 \equiv 0 \ (mod\ 45)$*, é possível observar que 5 é um fator comum aos coeficientes* 5 *e* 10*, mas* $5 \nmid 4$*. Logo nos deparamos com o caso ii). Portanto as soluções devem ser da forma* $x = 5y$*. Reescrevendo a congruência, temos*

$$5(5y)^2 + 4(5y) + 10 \equiv 0 \ (mod\ 45)$$

que por sua vez pode ser simplificada em

$$25y^2 + 4y + 2 \equiv 0 \ (mod\ 9)$$

que não pode ser ser mais reduzida por esse processo.

c) Na congruência $6x^2 + 5x + 2 \equiv 0 \ (mod\ 105)$*, observamos que* $3 \mid 6$*,* $3 \nmid 5$ *e* $3 \nmid 2$*, nos remetendo ao caso iv). Logo, se x é uma solução da congruência, então* $3 \mid (5x + 2)$*, ou seja,* $5x + 2 \equiv 0 \ (mod\ 3)$*, implica que* $x \equiv 2 \ (mod\ 3)$*. Assim existe um t tal que* $x = 3t + 2$*. Substituindo* $x = 3t + 2$ *na congruência obtemos*

$$6(3t + 2)^2 + 5(3t + 2) + 2 \equiv 0 \ (mod\ 105)$$

$$54t^2 + 87t + 36 \equiv 0 \ (mod\ 105),$$

que por sua vez pode ser simplificada para

$$18t^2 + 29t + 12 \equiv 0 \ (mod\ 35)$$

que também não pode ser mais reduzida por esse processo.

Dessa forma, é possível concluir que a resolução de congruências quadráticas se reduz à resolução de

$$ax^2 + bx + c \equiv 0 \pmod{n}$$

em que $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$ e $(a, n) = 1$.

Analisando agora, a decomposição em fatores primos de n. Sendo $n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ e $(a, n) = 1$, a congruência $ax^2 + bx + c \equiv 0 \pmod{n}$ é equivalente ao sistema.

$$\begin{cases} ax^2 + bx + c \equiv 0 \pmod{2^{\alpha}} \\ ax^2 + bx + c \equiv 0 \pmod{p_1^{\alpha_1}} \\ ax^2 + bx + c \equiv 0 \pmod{p_2^{\alpha_2}} \\ \vdots \\ ax^2 + bx + c \equiv 0 \pmod{p_r^{\alpha_r}} \end{cases}$$

Pelo Teorema Chinês do Resto, concluímos que o número de soluções da congruência $ax^2 + bx + c \equiv 0(\mod n)$ é igual ao produto do número de soluções de cada congruência do sistema (caso exista). Dessa forma, o estudo da congruência módulo n se reduz ao estudo de

$$ax^2 + bx + c \equiv 0 \pmod{p^k}$$

onde $a, b, c \in \mathbb{Z}$, p é primo, $k \in \mathbb{N}$ e $p \nmid a$.

3.1.1 Primeiro caso: p primo ímpar

Consideremos a equação

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{3.2}$$

onde p é primo, os coeficientes $a, b, c \in \mathbb{N}$ e $(a, p) = 1$.

Observação 3.1 *:Para $p = 2$, a congruência (3.2) é equivalente a uma Congruência Linear da forma $(a + b)x + c \equiv 0$ (mod 2), pois $x^2 \equiv x$ (mod 2). Daqui por diante consideraremos p um primo ímpar.*

Sendo p primo ímpar, tal que $(a, p) = 1$, a congruência

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

ao ser multiplicada por $4a$, (observando que $(4a, p) = 1$), é equivalente

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$$

que, por sua vez, completando quadrado é equivalente a

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p},$$

como $2a$ e p são primos relativos podemos tomar $y = 2ax + b$ e $\triangle = b^2 - 4ac$, obtendo

$$y^2 \equiv \Delta \pmod{p} \tag{3.3}$$

Portanto o estudo das soluções das congruências quadráticas (3.2) se reduzem ao estudo das soluções da congruência (3.3). Finalmente, para cada solução y_0 de (3.3) temos que resolver a congruência linear $2ax + b \equiv y_0 \pmod{p}$, para determinar as soluções da congruência (3.2).

O próximo resultado fornece critérios para que uma congruência quadrática módulo p primo do tipo (3.2) possua solução ou não.

Teorema 3.1 *Seja p primo, $p \geq 3$ e $a, b, c \in \mathbb{Z}$, $p \nmid a$. A congruência*

$$ax^2 + bx + c \equiv 0 \ (mod\ p)$$

possui duas soluções incongruentes módulo p se $\left(\frac{\Delta}{p}\right) = 1$, uma se $\left(\frac{\Delta}{p}\right) = 0$ e não possui solução se $\left(\frac{\Delta}{p}\right) = -1$.

A Demonstração deste Teorema pode ser encontrada em Oliveira (2011).

Deste modo temos uma caracterização de solubilidade das congruências quadráticas. Apresentaremos a seguir um critério para constatar se $x^2 \equiv -1 (\text{mod } p)$ é solúvel ou não.

Teorema 3.2 *$x^2 \equiv -1 (mod\ p)$ tem solução se e somente se $p = 4k + 1$ para algum inteiro k*

Demonstração: $\Rightarrow$) Seja a um inteiro tal que

$$a^2 \equiv -1 \pmod{p}.$$

Então pelo Teorema de Fermat,

$$a^{p-1} \equiv 1 \equiv \left(a^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

resulta que $\dfrac{p-1}{2}$ é par e consequentemente p é da forma $4k+1$.

$\Leftarrow$) Teremos que aplicar o Teorema de Wilson: $(p-1)! \equiv -1 \pmod{p}$.

$$1 \cdot 2 \cdot 3 \cdots (p-3)(p-2)(p-1) = 1 \cdot (p-1) \cdot 2 \cdot (p-2) \cdots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right).$$

Como $p - a \equiv -a \pmod{p}$, temos

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-3)(p-2)(p-1) \equiv & 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \left(\frac{p-1}{2}\right)\left(-\frac{p-1}{2}\right) \\ \equiv & (-1^2)(-2^2) \cdots \left(-\left(\frac{p-1}{2}\right)^2\right) \\ \equiv & (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \pmod{p} \end{aligned}$$

Como p é da forma $4k+1$, segue que $\dfrac{p-1}{2}$ é par e como $(p-1)! \equiv -1 \pmod{p}$, obtemos

$$\left(\frac{p-1}{2}!\right)^2 \equiv -1 \pmod{p}.$$

■

Exemplo 3.2 *Determine se a equação diofantina* $x^2 - 17y = 5$ *possui soluções naturais.*
Temos que $x^2 - 17y = 5$ *equivalente a* $x^2 \equiv 5$ (*mod* 17)*. Basta verificar se* 5 *é ou não um resíduo quadrático módulo* 17*, caso seja, se a equação diofantina possui solução. Para esta verificação, será usado o Lema de Gauss. Temos* $a = 5$, $p = 17$, $\dfrac{p}{2} = 7,5$ *e* $\dfrac{p-1}{2} = 8$.
Calculando $1.5, 2.5, 3.5, 4.5, 5.5, 6.5, 6.5, 7.5, 8.5$ (*mod* 17) *temos os seguintes resultados.*

$$\begin{aligned} 1.5 &\equiv 5 \mod 17 & 5.5 &\equiv 8 \mod 17 \\ 2.5 &\equiv 10 \mod 17 & 6.5 &\equiv 13 \mod 17 \\ 3.5 &\equiv 15 \mod 17 & 7.5 &\equiv 1 \mod 17 \\ 4.5 &\equiv 3 \mod 17 & 8.5 &\equiv 6 \mod 17. \end{aligned}$$

Nos quais apenas três deles são maiores que $7,5$. *Logo* $s = 3$ *e* $\left(\frac{5}{17}\right) = (-1)^3 = -1$. *Concluindo assim que a equação diofantina* $x^2 - 17y = 5$ *não possuí soluções naturais.*

Exemplo 3.3 *Analisaremos, agora, a congruência* $8x^2 + 5x + 1 \equiv 0$ (*mod* 23).
Observe que $p = 23$ *é um primo ímpar,* $(8, 23) = 1$ *e* $(32, 23) = 1$ *Multiplicando a equação por* 4*a, ou seja, por* 32 *obtemos*

$$256x^2 + 160x + 32 \equiv 0 \ (mod\ 23)$$

Completando quadrado temos a seguinte congruência

$$(16x + 5)^2 \equiv 16 \ (mod\ 23).$$

Tomando $y = 16x + 5$ *e* $\triangle = 16$*, iremos resolver a seguinte congruência.*

$$y^2 \equiv 16 \mod 23$$

É fácil observar que $(\pm 4)^2 \equiv 16$ (*mod* 23) *e que* $y = \pm 4$ (*mod* 23). *Resolver a congruência* $8x^2 + 5x + 1 \equiv 0 \mod 23$ *é o mesmo que resolver as congruências* $16x + 5 \equiv 4 \ (\mod 23)$ *e* $16x + 5 \equiv -4 \ (\mod 23)$*, obtendo as seguintes soluções,* $x \equiv 10$ (*mod*23) *ou* $x \equiv 21$ (*mod*23).

Podemos resolver a congruência quadrática do Exemplo (3.3) usando o conceito de inverso multiplicativo módulo p. O exemplo a seguir será usado um método alternativo, do proposto inicialmente, para resolução da congruência quadrática apresentada no Exemplo (3.3).

Exemplo 3.4 *Resolveremos, agora, a congruência* $8x^2 + 5x + 1 \equiv 0$ (*mod* 23)*, usando o inverso multiplicativo do coeficiente a módulo p, ou seja, estamos interessados em saber quem é o inverso multiplicativo de* 8 *módulo* 23*. Para isto devemos resolver a equação Diofantina*

$$8t - 23z = 1$$

ou construindo tábua de multiplicação completa para o corpo de inteiros módulo 23*. Fazendo um dos dois processos, descobre-se que o inverso multiplicativo de* 8 *módulo* 23 *é o* 3*. Multiplicando a congruência* $8x^2 + 5x + 1 \equiv 0$ (*mod* 23) *por 3 obtemos,*

$$x^2 + 15x + 3 \equiv 0 \ (mod\ 23)$$

Observe que o coeficiente do termo x é ímpar, ao completarmos quadrado, desta maneira, teremos

$$\left(x + \frac{15}{2}\right)^2 \equiv \frac{219}{3} \ (mod\ 23)$$

onde $\frac{15}{2}$ *e* $\frac{219}{3} \in \mathbb{Q}$*. Assim, podemos adicionar ou subtrair módulo* 23*, desta maneira teremos o coeficiente do termo x par e uma classe de equivalência módulo* 23*, para obter a congruência*

$$x^2 + 38x + 3 \equiv 0 \ (mod\ 23).$$

Procedemos, então a completar o quadrado da seguinte forma.

$$x^2 + 38x + 361 \equiv 361 - 3 \ (mod\ 23)$$

$$(x + 19)^2 \equiv 358 \ (mod\ 23)$$

$$(x + 19)^2 \equiv 13 \ (mod\ 23)$$

Tomando $y = x + 19$*, devemos resolver a congruência* $y^2 \equiv 13 \ (mod\ 23)$*. Para encontrar as soluções para y, continuamos adicionando o módulo* $p = 23$ *até obtermos um quadrado perfeito. Isso significa, encontrar um inteiro y tal que* $y = \pm\sqrt{23t + 13}$*, com* $t \in \mathbb{N}$*. Atribuindo valores para t, vemos que quando* $t = 1$ *implica que* $y = \pm 6$*. Agora, podemos encontrar a solução da congruência quadrática original, resolvendo as congruências* $x + 19 \equiv 6 \mod 23$ *e* $x + 19 \equiv -6 \ (mod\ 23)$*, que resulta as mesmas soluções do Exemplo (3.3) da página 52.*

Observação 3.2 *Uma progressão aritmética de razão p primo, gera quadrados perfeitos, se somente se, o seu primeiro termo for um Resíduo Quadrático módulo p.*

O próximo exemplo será uma congruência quadrática que não possuí solução.

Exemplo 3.5 *Seja a congruência* $5x^2 + 2x + 1 \equiv 0 \ (mod\ 11)$*.*
Observe que $p = 11$ *é um primo ímpar,* $(5, 11) = 1$ *e* $(20, 11) = 1$ *Multiplicando por* 4*a a congruência, obtemos*

$$(10x + 2)^2 \equiv 6 \ (mod\ 11)$$

tomando $y = 10x + 2$ *e* $\Delta = 6$ *temos* $y^2 \equiv \Delta \ (mod\ 11)$*, mas a congruência não possui solução, uma vez que* 6 *é um resíduo não quadrático módulo 11, ou seja, o Símbolo de Lagendre* $\left(\frac{\Delta}{11}\right) = -1$*.*

A seguir veremos uma congruência quadrática que possuí uma solução.

Exemplo 3.6 *Seja a congruência* $4x^2 + 5x + 3 \equiv 0$ (*mod* 23)
Como $23 \nmid 4$, *multiplicando por* $4a = 4.4 = 16$ *a congruência, teremos* $y = 2ax + b$ *e* $\Delta = b^2 - 4ac$, *obtendo uma congruência equivalente à* $y^2 \equiv \Delta$ (*mod p*), *daí segue que,*

$$y^2 = (8x + 5)^2 \equiv \Delta = 25 - 48 = -23 \equiv 0 \ (mod\ 23).$$

Temos $8x + 5 \equiv 0$ (*mod* 23), *o que implica que a solução da congruência quadrática original é dada somente por* $x \equiv 8$ (*mod* 23).

Proposição 3.1 *Se p é um primo ímpar e* $p \nmid \Delta$, *então a congruência* $y^2 \equiv \Delta$ (*mod p*) *não tem solução ou têm exatamente duas soluções incongruentes modulo p.*

Demonstração: Pelo Teorema (3.1) da página 50 a congruência não terá solução se $\left(\frac{\Delta}{p}\right) = -1$. Suponha que a congruência tenha uma solução, digamos $y = z$, isto é, $z^2 \equiv \Delta \pmod{p}$. Claramente $y = -z$ também é uma solução, desde que $(-z^2) = z^2 \equiv \Delta \pmod{p}$. Também $z \not\equiv -z \pmod{p}$, porque se $z \equiv -z \pmod{p}$, isto implicaria que $2z \equiv 0 \pmod{p}$, que é um absurdo, uma vez que p é ímpar e não divide z, já que $z^2 \equiv \triangle \pmod{p}$ e $p \nmid \Delta$.
Basta mostrar que as duas soluções (quando existem) são as únicas. Suponha que $y = z$, $y = w$ são duas soluções desta congruência quadrática, consequentemente $z^2 \equiv y^2 \equiv \Delta \pmod{p}$, então $z^2 - y^2 = z^2 - w^2 \equiv a - a \equiv 0 \pmod{p}$. Isto significa que $p \mid z + w$ ou $p \mid z - w$, que implica que $z \equiv -w \pmod{p}$ ou $z \equiv w \pmod{p}$. De qualquer jeito, ficamos apenas com duas soluções distintas, $y \equiv \pmod{p}$ e $y \equiv -z \pmod{p}$.

■

Observação 3.3 *Quando a congruência (3.3) da página 50 tem uma solução, significa que o número* Δ *é múltiplo de p. Quando a congruência (3.3) tem duas soluções, diz-se que o número* Δ *um resíduo quadrático módulo p. Caso contrário, se a congruência (3.3) não tem soluções, o número* Δ *é dito um resíduo não quadrático módulo p.*

3.1.2 Segundo Caso: $p = 2^k$

Dividiremos em dois sub-casos, o primeiro quando b é par e o segundo quando b é ímpar:

i) Sendo $p = 2$, com $2 \nmid a$ e b par, temos que a congruência

$$ax^2 + bx+ \equiv 0 \pmod{2^k}$$

ao ser multiplicada por a, fica

$$a^2x^2 + abx + ac \equiv 0 \pmod{2^k}$$

uma vez que $(a, 2) = 1$, e completando quadrados obtemos

$$\left(ax^2 + \frac{b}{2}\right)^2 \equiv \left(\frac{b^2}{2} - ac\right) \pmod{2^k}.$$

Caso análogo ao mostrado anteiormente para p primo.

ii) Se b é impar, c deve ser par, uma vez que a é impar. Caso contrário a congruência não tem solução. Ao tomarmos a congruência

$$ax^2 + bx + c \equiv 0 \pmod{2^k}$$

e multiplicá-la por $4a$, obtemos

$$4a^2 + 4abx + 4ac \equiv 0 \pmod{2^{k+2}}$$

que, por sua vez, pode ser reescrita completando quadrados na forma

$$(2ax + b)^2 + 4ac - b^2 \equiv 0 \pmod{2^{k+2}}$$

implicando em

$$(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{2^{k+2}}.$$

Exemplo 3.7 *Analisaremos um exemplo que tem o coeficiente b da congruência quadrática par.*
Dado a congruência $3x^2 + 4x + 5 \equiv 0$ (*mod* 16) *temos* $2 \nmid 3$ *e* 4 *é par, logo ao multiplicarmos por* 3 *a congruência, fica*

$$9x^2 + 12x + 15 \equiv 0 \ (mod\ 2^4),$$

completando quadrado, obtemos

$$(3x + 2)^2 \equiv 4 - 15 \equiv 5 \ (mod\ 16).$$

Exemplo 3.8 *Analisaremos agora uma congruência quadrática que tem o coeficiente b da congruência ímpar.*
Seja a congruência $3x^2 + 5x + 1 \equiv 0$ (*mod* 8)*. Observe que* $8 \nmid 3$*,* 5 *é ímpar e* 1 *também é ímpar. Logo a congruência proposta não possui solução, uma vez que, se* x_1 *fosse uma solução par, o mesmo não satisfaria a congruência, já que* $3x_1^2 + 5x_1 + 1$ *teria paridade respectivamente* **par + par +ímpar = ímpar** *que é incongruente módulo* 8*. De maneira análoga se* x_2 *fosse uma solução ímpar, também a expressão* $3x_2^2 + 5x_2 + 1$ *teria paridade ímpar. Portanto a congruência* $3x^2 + 5x + 1 \equiv 0$ (*mod* 8) *não possui solução.*

Assim, concluímos que a congruência $ax^2 + bx + c \equiv 0 \pmod{2^k}$ tem o estudo de suas soluções reduzido ao estudo de uma congruência da forma $x^2 \equiv d \pmod{2^s}$.

3.1.3 Congruências $x^2 \equiv a$ (mod p^k)

Tomemos a congruência

$$x^2 \equiv a \pmod{p^k},$$

em que $a, k \in \mathbb{Z}$. Podemos considerar que $p \nmid a$ pois, se $p|a$ então $p|x^2$ e consequentemente $p|x$. Assim se a congruência tiver solução será da forma $x = py$ para algum $y \in \mathbb{Z}$. Substituindo a solução na congruência obtemos $p^2y^2 \equiv pb \pmod{p^k}$, que ao ser simplificada é reduzida à

$$py^2 \equiv b \pmod{p^{k-1}}.$$

Devemos ter $k > 1$ pois, caso contrário, a congruência teria como única solução, $x \equiv 0 \pmod{p^k}$. Se $p|b$, o processo é repetido até que seja obtido uma congruência

$$x^2 \equiv a' \pmod{p^r},$$

em que $p \nmid a'$, observando que se $r = 1$ e $\left(\frac{a'}{p}\right) = 1$ a congruência não admite solução.
Desta forma o estudo das soluções de Congruência Quadráticas pode ser realizado considerando uma congruência do tipo $x^2 \equiv a \pmod{p^k}$ em que p é primo e $p \nmid a$.

Exemplo 3.9 *Analisaremos uma congruência em que* $r = 1$.
Seja a congruência $x^2 \equiv 18\ (mod\ 27)$. *Temos* $27 = 3^3$ *e* $3 \mid 18$. *Assim se a congruência tiver solução, será da forma* $x = 3y$ *para algum* $y \in \mathbb{Z}$. *Substituindo na congruência obtemos*

$$3^2y^2 \equiv 3.6\ (mod\ 3^3)$$

que ao ser simplificada é reduzida à

$$y^2 \equiv 2\ (mod\ 3^1)$$

Fácil perceber que $r = 1$ *e* $3 \nmid 2$ *e, por sua vez,* 2 *é um resíduo não quadrático módulo* 3. *Concluindo assim que a congruência* $3^2y^2 \equiv 3.6\ (mod\ 3^3)$ *não admite solução.*

A finalidade nas próximas seções é determinar métodos para encontrar as soluções das congruências quadráticas. Veremos, ainda, que para determinar as soluções de $x^2 \equiv a\ (\text{mod}\ p^k)$ é necessário resolver a congruência $x^2 \equiv a\ (\text{mod}\ p)$.

3.2 Estudo das soluções da Congruência Quadrática p primo ímpar

O intuito desta seção é mostrar como resolver congruências da forma $x^2 \equiv a\ (\text{mod}\ p)$ sem recorrer a método de tentativas, como mostrado no exemplo a seguir.

Exemplo 3.10 *Resolva* $x^2 \equiv 5\ (mod\ 61)$.
De acordo com o Critério de Euler, a equação $x^2 \equiv 5(mod\ 61)$ *tem soluções desde que* $5^{30} \equiv 1\ (mod\ 61)$*, de fato,*

$$5^3 \equiv 125 \equiv 3\ (mod\ 61)$$

$$\left(5^3\right)^{10} \equiv 3^{10}\ (mod\ 61)$$

Mas temos que $3^5 \equiv 243 \equiv -1\ (mod\ 61)$*, portanto*

$$5^{30} \equiv \left(3^5\right)^2 \equiv (-1)^2 \equiv 1\ (mod\ 61).$$

Isso mostra que 5 *é Resíduo quadrático módulo* 61. *Agora para encontrarmos as soluções, continuamos adicionando o módulo* $p = 61$ *até obtermos um quadrado perfeito, assim como no*

Exemplo 3.4.

$$x^2 \equiv 5 \equiv 5 + 61 \equiv 5 + 2(61) \equiv \cdots \equiv 5 + 20(61) = 1225 = 35^2 \ (mod\ 61)$$

Então temos $x^2 \equiv 35^2$ (*mod* 61)*, que dá* $x = 35$ *ou* $x = -35$*. As soluções são* $x \equiv -35 \equiv 26$(*mod* 61) *e* $x \equiv 35$ (*mod* 61)*.*

3.2.1 Primos ímpares congruentes a 3 módulo 4

Teorema 3.3 *Dado p primo ímpar da forma* $p \equiv 3$ (*mod* 4) *e a um resíduo quadrático módulo p. Então,* $x' \equiv \pm a^{\frac{p+1}{4}}$ (*mod p*) *é solução da congruência* $x^2 \equiv a$ (*mod p*)*.*

Demonstração: Ao substituir x' na congruência $x^2 \equiv a \pmod{p}$, obtemos
$(x')^2 \equiv \left(a^{\frac{p+1}{4}}\right)^2 \pmod{p}$, ou seja,
$(x')^2 \equiv a^{\frac{p+1}{2}} \pmod{p}$.
Pelo Critério de Euler temos $(x')^2 \equiv a \cdot \left(\frac{a}{p}\right) \pmod{p}$. Como a é um Resíduo Quadrático módulo p, implica que $\left(\frac{a}{p}\right) = 1$. Logo, $(x')^2 \equiv a.1 \equiv a \pmod{p}$.

■

Veremos no próximo exemplo a aplicação do Teorema (3.3).

Exemplo 3.11 *Resolva a equação* $x^2 + 25x + 24 \equiv 0$ (*mod* 31)*.*

É equivalente a resolver $y^2 \equiv \Delta$ (*mod p*)*, onde* $\Delta = b^2 - 4ac$ *e* $y = 2ax + b$*.* $y^2 \equiv 25^2 - 4 \cdot 24 \equiv 529 \equiv 2$ (*mod* 31)*, pelo Teorema (3.1) da página 50 temos que a equação possui solução, visto que* $\left(\frac{2}{31}\right) = 1$*, além disso,* $31 = 4 \cdot 8 + 3$*, aplicando o Teorema, temos que as soluções são da forma* $y \equiv \pm 2^{\frac{31+1}{4}}$ (*mod* 31)*. Temos*

$$2^5 \equiv 1 \ (mod\ 31)$$

$$2^3 \equiv 8 \ (mod\ 31)$$

$$2^8 = 2^5.2^3 \equiv 1.8 = 8 \ (mod\ 31).$$

Logo, $y^2 \equiv 2$ (*mod* 31)*, tem como soluçao* $y = \pm 8$ (*mod* 31)*.*

- *Para* $2x + 25 \equiv 8$ (*mod* 31) *a solução é* $x \equiv 19$ (*mod* 31)
- *Para* $2x + 25 \equiv -8$ (*mod* 31) *a solução é* $x \equiv 12$ (*mod* 31)*.*

3.2.2 Primos ímpares congruentes a 5 módulo 8

Teorema 3.4 *Se a é um Resíduo Quadrático módulo p e $p \equiv 5 \pmod 8$ em que $s = a^{\frac{p+3}{8}}$. Então a congruência $x^2 \equiv a \pmod p$ terá como solução $\pm s$ ou $2^{\frac{(p-1)}{4}} \cdot s$.*

Demonstração: Como $p \equiv 5 \pmod 8$, pelo Corolário (2.2), temos $\left(\frac{2}{p}\right) = -1$. Pelo Critério de Euler, temos $2^{\frac{(p-1)}{2}} = -1 \pmod p$. Assim, a congruência

$$s^4 = \left(a^{\frac{(p+3)}{8}}\right)^4 = a^{\frac{(p+3)}{2}} = a^{\frac{(p-1)}{2}} a^2 \equiv a^2 \pmod p$$

implica em $s^2 \equiv \pm a \pmod p$ se $s^2 \equiv -a \pmod p$, consequentemente $2^{\frac{(p-1)}{4}} \cdot s$ será solução para $x^2 \equiv a \pmod p$.

■

Exemplo 3.12 *Resolva a equação $11x^2 + 15x + 5 \equiv 0 \pmod{61}$*

Essa congruência é equivalente a resolver $y^2 \equiv \Delta \pmod p$, onde $\Delta = b^2 - 4ac$ e $y = 2ax + b$. Segue que $y^2 \equiv 15^2 - 4 \cdot 11 \cdot 5 \equiv 5 \pmod{61}$. Usando a Lei de Reciprocidade Quadrática temos $\left(\frac{5}{61}\right) = (-1)^{\frac{5-1}{2}\frac{61-1}{2}} \left(\frac{61}{5}\right)$, mas $\left(\frac{61}{5}\right) = \left(\frac{1}{5}\right) = 1$, isso implica que $\left(\frac{5}{61}\right) = 1$, pelo Teorema (3.1) da página 50 a equação possui solução. É possível verificar que $61 \equiv 5 \pmod 8$, logo aplicando o Teorema (3.4) da página 59, $s = 5^{\frac{61+3}{8}} = 5^8 = 390625 \equiv 42 \pmod{61}$, que não é solução da congruência, uma vez que $(42)^2 \equiv 56 \equiv -5 \pmod{61}$. Logo a solução será dada por $2^{\frac{61-1}{4}} s = 2^{15} \cdot 42$.

Temos

$$2^6 = 64 \equiv 3 \pmod{61}$$

$$2^3 \equiv 8 \pmod{61}$$

$$2^{15} = 2^6.2^6.2^3 \equiv 3.3.8 = 72 \equiv 11 \pmod{61}$$

Logo a solução de $y^2 \equiv 5 \pmod{61}$ será $y \equiv 11 \cdot 42 \equiv \pm 35 \pmod{61}$.

- *Para $22x + 15 \equiv 35 \pmod{31}$ a solução é $x \equiv 12 \pmod{61}$.*
- *Para $22x + 15 \equiv -35 \pmod{31}$ a solução é $x \equiv 49 \pmod{61}$.*

Portanto as soluções de $11x^2 + 15x + 5 \equiv 0 \pmod{61}$ são dadas por $x \equiv 12, 49 \pmod{61}$.

3.2.3 Algoritmo Tonelli-Shanks

O algoritmo Tonelli-Shanks é usado para resolver congruências da forma

$$x^2 \equiv a \pmod{p},$$

onde a é um resíduo quadrático (mod p) e p é um primo ímpar.

O algoritmo de Tonelli-Shanks não pode ser usado para módulos compostos. Encontrar raízes quadradas módulo números compostos é um problema computacional equivalente à fatoração inteira.

Uma versão equivalente, mas ligeiramente mais redundante deste algoritmo foi desenvolvida por Alberto Tonelli em 1891. A versã que será apresentada, foi desenvolvida independentemente por Daniel Shanks em 1973, que explicou:

"Meu atraso na aprendizagem destas referências históricas foi porque eu tinha emprestado o Volume 1 da História de Dickson a um amigo e ele nunca mais me devolveu o livro", Shanks (1972).

O objetivo de exibir este algoritmo é resolver a equação $x^2 \equiv a \pmod{p}$ onde p é um primo ímpar satisfazendo $p \equiv 1 \pmod 4$ e a é um resíduo quadrático modulo p, isto é o Símbolo de Legendre $\left(\frac{a}{p}\right) = 1$.

Processo do Algoritmo

1. Fatorar o inteiro par $p-1$, obtendo $p - 1 = 2^s.Q$. Onde Q é ímpar
2. Achar um inteiro positivo y tal que $\left(\frac{y}{p}\right) = -1$.
3. Calcular os seguintes valores.
   - $R \equiv a^{\frac{Q+1}{2}} \pmod{p}$
   - $c \equiv y^Q \pmod{p}$
   - $t \equiv a^Q \pmod{p}$
   - $E = S$
4. Processamento das soluções **(Laço ou Loop)**

A Se $t \equiv 1 \pmod{p}$, então o algoritmo pará e as duas soluções da congruência são R e $p - R$. Se $t \not\equiv 1 \pmod{p}$, então execute as duas etapas a seguir

B Encontre o mínimo i tal que $0 < i < E$ e que $t^{2^i} \equiv 1 \pmod{p}$.

C Calcular $b \equiv c^{2^{E-i-1}} \mod p$ e substituir as quantidades R, c, t e E da seguinte maneira

i $R \equiv Rb \pmod{p}$

ii $c \equiv b^2 \pmod{p}$

iii $t \equiv b^2 t \pmod{p}$

iv $E = i$

Voltando para a Etapa **A**.

O valor inicial de $R \equiv a^{\frac{Q+1}{2}} \pmod{p}$ é uma estimativa inicial da solução para a congruência. O restante do algoritmo é refinar repetidamente esta estimativa para alcançar uma solução. Observe que o passo 4-B é para determinar a ordem do número t. Cada vez que um novo valor de t é calculado, a ordem do novo t é menor que a ordem do t anterior. O objetivo é alcançar um t de ordem 1, o que significa que o número t em si seria congruente a 1 módulo p, à altura em que a estimativa R se torna uma solução. A demonstração do algoritmo pode ser vista em Dan Ma (2015).

Exemplo 3.13 *Use o algortimo de Tonelli-Shanks para resolver* $x^2 \equiv 67$ (*mod* 193).

O número 193 *é primo e o valor do Símbolo de Legendre é* $\left(\frac{67}{193}\right) = 1$, $\left(\frac{67}{193}\right)\left(\frac{193}{67}\right) = (-1)^{\frac{67-1}{2}\frac{193-1}{2}}$, $\left(\frac{67}{193}\right) = 1\left(\frac{67}{193}\right) = \left(\frac{59}{67}\right)$.

Mas $\left(\frac{59}{67}\right) = (-1)^{\frac{67-1}{2}\frac{57-1}{2}}\left(\frac{67}{59}\right) = (-1)\left(\frac{8}{59}\right) = (-1)\left(\frac{2^2}{59}\right)\left(\frac{2}{59}\right) = (-1)\cdot 1\cdot(-1)$. *Logo* $\left(\frac{67}{193}\right) = 1$. *Portanto a congruência possuí solução.*

A seguir mostraremos as etapas.

Etapa 1 $p - 1 = 192 = 2^6 \cdot 3$*;* $S = 6$ *e* $Q = 3$

Etapa 2 *Pelo Corolário (2.4) da página 44,* $y = 5$ *é um Resíduo não Quadrático módulo* 193.

Etapa 3 *Calcular os seguintes valores. Todos os cáculos são módulo* $p = 193$

- $R \equiv a^{\frac{Q+1}{2}} = 67^{\frac{3+1}{2}} = 67^2 \equiv 50$
- $c \equiv y^Q = 5^3 \equiv 125$
- $t \equiv a^Q = 67^3 \equiv 69$
- $E = S = 6$.

Observe que t não é congruente a 1 *módulo 193. Por isso, precisamos executar o Loop*

Loop Iteração 1

Achamos o menor natural i, $0 < i < E$*, tal que* $t^{2^i} \equiv 1$*. Dado* $b \equiv c^{2^{E-i-1}}$*, substituímos os valores,*$R, c, t,$ *e E como segue:*

- $i = 5$*, o menor inteiro i,* $0, i, E$*, tal que* $t^{2^i} \equiv 1$*,*

$$\begin{aligned} 69^2 &\equiv 129 \ (mod\ 193) \\ \left(69^2\right)^2 &\equiv 129^2 \equiv 43 \ (mod\ 193) \\ \left(69^4\right)^2 &\equiv 43^2 \equiv 112 \ (mod\ 193) \\ \left(69^8\right)^2 &\equiv 112^2 \equiv 192 \ (mod\ 193) \\ \left(69^{16}\right)^2 &\equiv 192^2 \equiv 1 \ (mod\ 193). \end{aligned}$$

- $b \equiv c^{2^{E-i-1}} = 125^{2^{6-5-1}} \equiv 125.$
- $R_1 \equiv Rb = 50 \cdot 125 \equiv 74.$
- $c_1 \equiv b^2 = 125^2 \equiv 185.$
- $t_1 \equiv c_1.t = 185 \cdot 69 \equiv 27 \ (mod\ 193).$
- $E_1 = 5.$

Observamos que t_1*, também, não é congruente a* 1 *módulo* 193*, Novamente faremos o Loop.*

Iteração 2

- $i = 4$*, o menor i,* $0 < i < E_1$*, tal que* $t_1^{2^i} \equiv 1$*;*

$$\begin{aligned} 27^2 &\equiv 150 \ (textmod\ 193) \qquad \left(27^2\right)^2 \equiv 150^2 \equiv 112 \ (mod\ 193) \\ \left(27^4\right)^2 &\equiv 112^2 \equiv 192 \ (mod\ 193) \qquad \left(27^8\right)^2 \equiv (-1)^2 \equiv 1 \ (mod\ 193) \end{aligned}$$

- $b \equiv c_1^{2^{E_1-i-1}} = 185^{2^{5-4-1}} \equiv 185$
- $R_2 \equiv R_1 b = 74 \cdot 185 \equiv 180$
- $c_2 \equiv b^2 = 185^2 \equiv 64$
- $t_2 \equiv c_2.t_1 = 64 \cdot 27 \equiv 184 \ (mod\ 193)$

- $E_2 = 4$

Observamos que t_2, também, não é congruente a 1 *módulo* 193*, Novamente faremos o Loop.*

Iteração 3

- $i = 3$*, o menor i,* $0 < i < E_2$*, tal que* $t_2^{2^i} \equiv 1$*;*

$$184^2 \equiv 81 \ (mod\ 193)$$
$$\left(184^4\right)^2 \equiv 81^2 \equiv 192 \ (mod\ 193)$$
$$\left(184^8\right)^2 \equiv (-1)^2 \equiv 1 \ (mod\ 193$$

- $b \equiv c_2^{2^{E_2-i-1}} = 64^{2^{4-3-1}} \equiv 64$
- $R_3 \equiv R_3 b = 180 \cdot 64 \equiv 133$
- $c_3 \equiv b^2 = 64^2 \equiv 43$
- $t_3 \equiv c_3.t_2 = 43 \cdot 184 \equiv 192 \equiv -1 \ (mod\ 193)$
- $E_3 = 3$

Observamos que t_3, também, não é congruente a 1 *módulo* 193*. Novamente faremos o Loop.*

Iteração 4

- $i = 1$*, o menor i,* $0 < i < E_3$*, tal que* $t_3^{2^i} \equiv 1$*;*

$$(-1)^2 \equiv 1 \ (mod\ p)$$

- $b \equiv c_3^{2^{E_3-i-1}} = 43^{2^{3-1-1}} \equiv 43^2 \equiv 112$
- $R_4 \equiv R_3 b = 133 \cdot 112 \equiv 35$
- $c_4 \equiv b^2 = 112^2 \equiv -1$
- $t_4 \equiv c_4.t_3 = 43 \cdot (-1)(-1) \equiv 1 \ (mod\ 193)$
- $E_4 = 1$

Agora encontramos $t_4 \equiv 1$ (*mod* 193)*, Portanto as soluções da congruência dada são* $x \equiv R_4 \equiv 35$ (*mod* 193) *e* $x \equiv p - R_4 \equiv 193 - 35 = 158$ (*mod* 193)*.*

3.3 Soluções das Congruências Quadráticas $x^2 \equiv a \pmod{p^n}$

O propósito desta seção é averiguar em que condição a congruência $x^2 \equiv a \pmod{p^n}$, quando p é primo ímpar, possui solução e como encontra-las.

3.3.1 Solubilidade e construção das soluções de $x^2 \equiv a \pmod{p^n}$

Teorema 3.5 *Se p é um primo ímpar e $(a, p) = 1$, então $x^2 \equiv a \pmod{p^n}$ tem exatamente duas soluções se a é um resíduo quadrático de p, e nenhuma solução se a é um resíduo não quadrático de p.*

Demonstração: Suponha que $x^2 \equiv a \pmod{p^n}$ pode ser resolvido, $\forall n \in \mathbb{N}$ então $x^2 \equiv a \pmod{p}$ também é solucionável, logo $\left(\frac{a}{p}\right) = 1$. Inversamente, deixe $\left(\frac{a}{p}\right) = 1$; Isto é, suponha que $x^2 \equiv a \pmod{p}$ é solúvel. Vamos agora provar por indução que $x^2 \equiv a \pmod{p^n}$ é solúvel para cada inteiro positivo n. Claramente é verdade quando $n = 1$. Então suponha que é verdade para um inteiro arbitrário $k \geq 1 : x^2 \equiv a \pmod{p^k}$ é solúvel. Vamos mostrar que $x^2 \equiv a \pmod{p^{k+1}}$ também é solucionável, construindo assim uma solução.
Seja α uma solução de $x^2 \equiv a \pmod{p^k}$, então $\alpha^2 \equiv a \pmod{p^k}$, isto é, $\alpha^2 = a + ip^k$ para algum inteiro i. Agora geramos uma solução da forma $a + jp^k$ da congruência $\alpha^2 \equiv a \pmod{p^{k+1}}$. Então

$$\begin{aligned}(\alpha + jp^k)^2 &= \alpha^2 + 2\alpha jp^k + j^2p^{2k} \\ &\equiv \alpha^2 + 2\alpha jp^k \pmod{p^{k+1}}, \qquad \text{desde que } 2k > k+1 \\ &\equiv (a + ip^k) + 2\alpha jp^k \pmod{p^{k+1}} \\ &\equiv a + (i + 2\alpha j)p^k \pmod{p^{k+1}}.\end{aligned}$$

Agora escolha j tal que $i + 2\alpha j \equiv 0 \pmod{p}$. Tal j existe, já que desde que $(2\alpha, p) = 1$. Com tal j, $(\alpha + jp^k)^2 \equiv a \pmod{p^{k+1}}$. Assim $\pm(\alpha + jp^k)$ é uma solução de $x^2 \equiv a \pmod{p^{k+1}}$.
Portanto concluímos, por indução, que $x^2 \equiv a \pmod{p^n}$ é solúvel para cada inteiro positivo n.

■

Outra Demonstração do Teorema 3.5 pode ser dada da seguinte maneira.

Demonstração: Tomemos $f(x) = x^2 - a$, temos que $f'(x) = 2x$ e se $x = x_1 \pmod{p}$ é uma solução de $x^2 \equiv a \pmod{p}$, então como $(a, p) = 1$, $(x_1, p) = 1$ e como p é ímpar $(2x_1, p) = 1$. Portanto, $f'(x)$ não é divisível por p. Do fato de $x = x_1 \pmod{p}$ concluímos que

$x = x_1 + pt_1$, onde $t_1 \in \mathbb{Z}$. Utilizando a Expansão em série de Taylor, podemos escrever $f(x)$ da seguinte maneira:

$$f(x) = \frac{f(x_1)(x - x_1)^0}{0!} + \frac{f'(x_1)(x - x_1)}{1!},$$

o que implica, ao colocarmos $x = x_1 + pt_1$ em $f(x) \equiv 0 \pmod{p^2}$, em

$$f(x) = f(x_1) + f'(x_1)(x_1 + pt_1 - x_1) = f(x_1) + pt_1 f'(x_1) \equiv 0 \pmod{p^2}.$$

Simplificando a congruência por p, obtemos

$$\frac{f(x_1)}{p} + t_1 f'(x_1) \equiv 0 \pmod{p}.$$

Como $p \mid f(x_1)$ e $p \nmid f'(x_1)$, então $p \mid t_1$. Assim, temos uma solução,

$$t_1 \equiv t_1' \pmod{p} \Rightarrow t_1 = t_1' + pt_2.$$

Temos, agora, que $x = x_1 + pt_1' + p^2 t_2 = x_2 + p^2 t_2$. Utilizando esse valor de x em $f(x) \equiv 0 \pmod{p^3}$ temos

$$f(x_2) + p^2 t_2 f'(x_2) \equiv 0 \pmod{p^3},$$

que por sua vez implica em

$$\frac{f(x_2)}{p^2} + t_2 f'(x_2) \equiv 0 \pmod{p^3}.$$

Como $x_2 \equiv x_1 \pmod{p}$ e $f'(x_2) \equiv f'(x_1) \pmod{p}$, então $p \nmid f'(x_2)$. Logo, a última congruência tem uma solução:

$$t_2 \equiv t_2' \pmod{p} \Rightarrow t_2 = t_2' + pt_3.$$

Assim,

$$x = x_2 + p^2 t_2' + p^3 t^3 = x_3 + p^3 t_3.$$

Continuando esse raciocínio encontramos, a partir da solução de $x^2 \equiv a \pmod{p}$, a solução de $x^2 \equiv a \pmod{p^k}$. Assim com a condição que $f'(x_1)$ não seja divisível por p toda solução $x \equiv x_1 \pmod{p}$ de $f(x) \equiv 0 \pmod{p}$ proporciona uma solução de $f(x) \equiv 0 \pmod{p^k}$ dada por:

$$x = x_k + p^k t_k$$

$$x \equiv x_k \pmod{p^k}.$$

■

Constatando, assim, que o caso $p = 2$ é diferente, e o método de resolubilidade é dada na Secção (3.4).

Observação 3.4 *Este resulta refere-se a solubilidade e construção das soluções das congruência quadráticas módulo p^k com p primo ímpar. Se $x^2 \equiv a \pmod{p}$ é solúvel, então $x^2 \equiv a \pmod{p^n}$ também é solúvel. E suas soluções podem ser usadas, passo a passo, para gera as soluções de $x^2 \equiv a \pmod{p^k}$.*

Exemplo 3.14 *Encontre a solução de $x^2 \equiv 23 \pmod{7^3}$.*
Primeiramente constataremos se a congruência $x^2 \equiv 23 \equiv 2 \pmod{7}$ é soluvel. Como $\left(\frac{2}{7}\right) = 1$, a congruência $x^2 \equiv 23 \pmod{7}$ é solúvel e é fácil verificar que as soluções são $x \equiv 3, 4 \pmod{7}$.

Tomando uma das soluções de $x^2 \equiv 23 \pmod{7}$, construímos as soluções de $x^2 \equiv 23 \pmod{7^2}$. Elegendo o 3 como solução de $x^2 \equiv 23 \pmod{7}$, implica que $3^2 = 23 + 7i$ para algum inteiro i, a saber $i = -2$. Então $3^2 = 23 + (-2) \cdot 7$. Seguindo os passos da demonstração do Teorema (3.5), segue que, $\alpha = 3 + 7j$ é uma solução de $x^2 \equiv 23 \pmod{7^2}$. Imediatamente $\alpha^2 \equiv 23 \pmod{7^2}$,

$$\begin{aligned}(3 + 7j)^2 &= 9 + 42j + 49j^2 \\ &\equiv 9 + 42j \pmod{7^2} \\ &\equiv [23 + (-2) \cdot 7] + 42j \pmod{7^2} \\ &\equiv 23 + 7(2 - 6j) \pmod{7^2}.\end{aligned}$$

Segue que $\alpha_1^2 \equiv 23 + 7(2 - 6j) \equiv 23 \pmod{7^2}$, simplificando a congruência, obtemos $-2 + 6j \equiv 0 \pmod{7}$, resolvendo, concluímos que $j \equiv 5 \pmod{7}$. Uma vez estabelecido o valor de j encontramos o valor de α. Assim, concluímos que $\alpha_1 = 3 + 7j \equiv 3 + 7 \cdot 5 \equiv 38 \pmod{7^2}$, ou seja, ± 38 é uma solução de $x^2 \equiv 23 \pmod{7^2}$.

Usaremos agora 38 para gerar uma solução de $x^2 \equiv 23 \pmod{7^3}$. Como $38^2 \equiv 23 \pmod{7^2}$, é o mesmo que $38^2 = 23 + k \cdot 7^2$, para algum k inteiro, a saber $k = 29$, Então $38^2 = 23 + 29 \cdot 7^2$. De maneira análoga para encontrarmos as soluções de $x^2 \equiv 23 \pmod{7^3}$,

temos $\alpha_2 = 38 + 7^2 \cdot l$ *uma solução de* $x^2 \equiv 23\ (mod\ 7^3)$.

$$\begin{aligned}(38 + 7^2 l)^2 &= 38^2 + 76.7^2.l + 7^4 l \\ &\equiv 38^2 + 76.7^2.l\ (mod\ 7^3) \\ &\equiv (23 + 29.7^2) + 76.7^2\ (mod\ 7^3) \\ &\equiv 23 + 7^2(29 + 76.l)\ (mod\ 7^3).\end{aligned}$$

Com esse processo basta encontrar l tal que $29 + 76l \equiv 0\ (mod\ 7)$ *para encontrarmos o valor de* α_2. *Ao resolver* $29 + 76l \equiv 0\ (mod\ 7)$, *encontramos* $l = 1$. *Então* $\alpha_2 = 38 + 7^2 \cdot 1 \equiv 87\ (mod\ 7^3)$, *logo* ± 87 *é uma solução da congruência* $x^2 \equiv 23\ (mod\ 7^3)$. *Para a outra solução* $x \equiv 4\ (mod\ 7)$, *fazemos* $a = 23$ *e* $p = 7$

1º *Tome* α *e* k *(expoente do módulo* 7*),* $\alpha = 4$ *e* $k = 1$

2º *Tome* $\alpha^2 = a + ip^k$ *e resolva para i,* $\alpha^2 = 23 + 7i$, *obtemos* $i = -1$

3º *Resolva* $i + 2\alpha\jmath \equiv 0\ (mod\ p)$ *para j, então*

$$-1 + 2 \cdot 4j \equiv 0\ (mod\ 7)$$

encontrando $j \equiv 1\ (mod\ 7)$

4º *A solução de* $x^2 \equiv a\ (mod\ p)$

$\alpha + jp = 4 + 1.7 = 11$ *é uma solução de* $(x^2 \equiv 23\ (mod\ 7^2)$

5º *Utilize* α *e k:* $\alpha = 11$ *e* $k = 2$

Repita os passos $2 - 4$ *para encontrar para encontrar uma solução de* $x^2 \equiv a\ (mod\ 7^3)$.

6º *Expressar* α^2 *na forma* $a + ip^2$, $\alpha^2 = a + ip^2$, *obtemos* $121 = 23 + i.7^2$; $i = 2$

7º *Resolver a congruência Linear*

$$i + 2\alpha j \equiv 0\ (mod\ p)\ para\ j.$$

$$2 + 2 \cdot 11j \equiv 0\ (mod\ 7);\ \ j = 5$$

8º *Gerar as soluções de* $x^2 \equiv a\ (mod\ p^3)$

$\alpha + jp^2 = 11 + 5 \cdot 7^2 = 256$ *é uma solução de* $x^2 \equiv 23 \ (mod\ 7^3)$.

Portanto as soluções do Exemplo proposto são: $x \equiv 87, 256 \ (mod\ 7^3)$.

Exemplo 3.15 *Resolva a congruência* $x^2 \equiv 3 \ (mod\ 121)$.

Como {0,1,2,3,4,5,6,7,8,9,10} é um Sistema Completo de Resíduo módulo 11 *e* 5 *e* 6 *satistfazem a congruência* $x^2 \equiv 3 \ (mod\ 11)$ *podemos escrever que* $x = 5 + 11t$ *e* $x = 6 + 11t$. *Se atribuirmos valores a t, as soluções naturais menores que* 121 *que satisfazem o módulo* 11 *são,* $16, 17, 27, 28, 38, 39, 49, 50, 60, 61, 71, 72, 82, 83, 93, 94, 104, 105, 115$, *e* 116, *dos quais duas satisfazem o módulo* 121. *Testando todas elas,* $x \equiv 27 \ (mod\ 121)$ *e* $x \equiv 94 \ (mod\ 121)$ *são as soluções buscadas.*

A abordagem acima aumenta a dificuldade à medida que aumenta a base do expoente, dado o número de operações realizadas. Para evitar essa situação o próximo exemplo será resolvido de acordo com a segunda demonstração do Teorema (3.5) da página 62.

Exemplo 3.16 *Resolva a congruência* $x^2 \equiv 3 \ (mod\ 121)$

Para verificar se $x^2 \equiv 3 \ (mod\ 121)$ *é soluvel, devemos constatar se* 3 *é um resíduo quadrático módulo* 11, *de fato é. Usando a Fórmula de Taylor de tal forma que toda solução* $x \equiv x_1 \ (mod\ p)$ *da congruência* $f(x) \equiv 0 \ (mod\ p)$ *e com a condição da derivada* $f'(x_1)$ *não ser dividida por p, proporciona uma solução da congruência* $f(x) \equiv 0 \ (mod\ p^n)$ *da forma* $x = x_n + p^n t_n$. *Deste modo* $x^2 \equiv 3 \ (mod\ 121)$ *equivale a* $x^2 - 3 \equiv 0 \ (mod\ 121)$. *Calculando de* $x^2 \equiv 3 \ (mod\ 11)$, *temos como solução* $x_1 = 5 + 11t_1$ *e* $x_1' = 6 + 11t_1'$. *Tomando* $f(x) = x^2 - 3$, *para*

$$f(5) = 22 \text{ e } f(6) = 33$$

e para a derivada de $f'(x) = 2x$, *os valores são*

$$f'(5) = 10 \text{ e } f'(6) = 12$$

onde, nem 10 *e nem* 12 *são divisiveis por 121. Resolvendo*

$$f(5) + 11t_1 f'(5) \equiv 0 \ (mod\ 121)$$

que é equivalente a

$$22 + 11t_1 \cdot 10 \equiv 0 \ (mod\ 121)$$

resulta em

$$2 + 10t_1 \equiv 0 \ (mod\ 11)$$

se dividirmos tudo por 11 *e fazendo as operações,* $t_1 \equiv 2$ *que é equivalente a* $t_1 = 2 + 11t$. *Substituindo em* x_1

$$x_1 = 5 + 11(2 + 11t) = 27 + 121t.$$

Resolvemos, agora, $f(6) + 11t_1' f'(6) \equiv 0 \ (mod\ 121)$ *equivalente a* $33 + 11t_1' \cdot 33 \equiv 0 \ (mod\ 121)$. *Dividindo por* 11 *e fazendo operações,* $t_1' \equiv 8 \ (mod\ 11)$ *que representamos como* $t_1' = 8 + 11t$. *Subsitituindo*

$$x_1' = 6 + 11(8 + 11t) = 94 + 121t$$

Portanto as soluções de $x^2 \equiv 3 \ (mod\ 121)$ *são* $x \equiv 27, 94 \ (mod\ 121)$.

Exemplo 3.17 *Resolva a equação* $4x^2 + 13x + 15 \equiv 0 \ (mod\ 19^2)$.

A equação $4x^2 + 13x + 15 \equiv 0 \ (mod\ 19^2)$ *terá solução se somente se*

$$4x^2 + 13x + 15 \equiv 0 \ (mod\ 19)$$

Para $4x^2 + 13x + 15 \equiv 0 \ (mod\ 19)$ *as soluções são*

$$x_1 = 2 + 19t \text{ e } x_2 = 9 + 19t$$

Os valores para estas raízes, para a equação e sua derivada são

$$f(x) = 4x^2 + 13x + 15 \begin{cases} f(2) = 57 \\ f(9) = 456 \end{cases} \quad e \quad f'(x) = 8x + 13 \begin{cases} f'(2) = 29 \\ f'(9) = 85 \end{cases}$$

Aplicando estes valores a equação $f(x) + f'(x) \cdot p \cdot t_1 \equiv 0 \ (mod\ p^n)$, *resulta:*

$$57 + 29 \cdot 19t \equiv 0 \ (mod\ 19^2)$$

que dividindo por 19 *nos fornece* $3 + 29t \equiv 0 \ (mod\ 19)$. *Calculando* $t \equiv 13 \ (mod\ 19)$ *resulta em* x_1

$$x_1 = 3 + 19(13 + 17t) = 249 + 19^2 t.$$

Agora para x_2

$$456 + 85 \cdot 19t \equiv 0 \ (mod\ 19^2)$$

que dividindo por 19, resulta em $24 + 85t \equiv 0 \ (mod\ 19)$. *Calculando,* $t \equiv 10 \ (mod\ 19)$ *que implica que* x_2*:*

$$x_2 = 9 + 19(10 + 19t) = 199 + 19^2 t.$$

Portanto as soluções da equação proposta, são:

$$x \equiv 199, 249 \ (mod\ 19^2).$$

Proposição 3.2 *Se* a *é um Resíduo Quadrático módulo* p *então as soluções da congruência* $x^2 \equiv a \ (mod\ p^k)$ *em que* $(a, p) = 1$ *são* $x \equiv \pm P\overline{Q}$*, onde*

$$P = \frac{(z + \sqrt{a})^k + (z - \sqrt{a})^k}{2},\ Q = \frac{(z + \sqrt{a})^k - (z - \sqrt{a})^k}{2\sqrt{a}}$$

e $z^2 \equiv a \ (mod\ p)$ *e* $\overline{Q}$ *o inverso de* Q *módulo* p^k.

Demonstração: Mostraremos que P e Q são inteiros.

$$(z + \sqrt{a})^k = \sum_{p=0}^{k} \binom{k}{p} z^{k-p} \cdot a^{\frac{p}{2}} = \binom{k}{0} z^k + \binom{k}{1} z^{k-1} \cdot a^{\frac{1}{2}} + \binom{k}{2} z^{k-2} \cdot a^{\frac{2}{2}} + \binom{k}{3} z^{k-3} \cdot a^{\frac{3}{2}} + \cdots + \binom{k}{k} z^{k-k} \cdot a^{\frac{k}{2}}$$

$$(z - \sqrt{a})^k = \sum_{i=0}^{k} \binom{k}{p} z^{k-i} \cdot a^{\frac{i}{2}} \cdot (-1)^i = \binom{k}{0} z^k - \binom{k}{1} z^{k-1} \cdot a^{\frac{1}{2}} + \binom{k}{2} z^{k-2} \cdot a^{\frac{2}{2}} - \binom{k}{3} z^{k-3} \cdot a^{\frac{3}{2}} + \cdots + \binom{k}{k} z^{k-k} \cdot a^{\frac{k}{2}} \cdot (-1)^i$$

$$-(z - \sqrt{a})^k = \sum_{i=0}^{k} \binom{k}{p} z^{k-i} \cdot a^{\frac{i}{2}} \cdot (-1)^{i+1} = -\binom{k}{0} z^k + \binom{k}{1} z^{k-1} \cdot a^{\frac{1}{2}} - \binom{k}{2} z^{k-2} \cdot a^{\frac{2}{2}} + \binom{k}{3} z^{k-3} \cdot a^{\frac{3}{2}} - \cdots + \binom{k}{k} z^{k-k} \cdot a^{\frac{k}{2}} \cdot (-1)^{i+1}$$

Dai, se k é ímpar, temos

$$\frac{(z + \sqrt{a})^k + (z - \sqrt{a})^k}{2} = \binom{k}{0} z^k + \binom{k}{2} z^{k-2} \cdot a^{\frac{2}{2}} + \binom{k}{4} z^{k-4} \cdot a^{\frac{4}{2}} + \binom{k}{6} z^{k-6} \cdot a^{\frac{6}{2}} + \cdots + \binom{k}{k-1} z^{k-1} \cdot a^{\frac{k-1}{2}}$$

$$P = \frac{(z + \sqrt{a})^k + (z - \sqrt{a})^k}{2} = \sum_{c=0}^{\frac{k-1}{2}} \binom{k}{2c} z^{k-2c} \cdot a^c$$

Como $\sum_{c=0}^{\frac{k-1}{2}} \binom{k}{2c} z^{k-2c} \cdot a^c$ é inteiro, temos que $P = \frac{(z + \sqrt{a})^k + (z - \sqrt{a})^k}{2}$ é inteiro, para todo k

ímpar pertencente aos naturais. Agora, se k é par, temos

$$P = \binom{k}{0}z^k + \binom{k}{2}z^{k-2}\cdot a^{\frac{2}{2}} + \binom{k}{4}z^{k-4}\cdot a^{\frac{4}{2}} + \binom{k}{6}z^{k-6}\cdot a^{\frac{6}{2}} + \cdots + \binom{k}{k}z^{k-k}\cdot a^{\frac{k}{2}} = \sum_{d=0}^{\frac{k}{2}}\binom{k}{2d}z^{k-2d}\cdot a^d$$

Como $\sum_{c=0}^{\frac{k}{2}}\binom{k}{2d}z^{k-2d}\cdot a^d$ é inteiro, temos que $P = \dfrac{(z+\sqrt{a})^k + (z-\sqrt{a})^k}{2}$ é inteiro, para todo $k \in \mathbb{N}$.

Tomando, agora, $Q = \dfrac{(z+\sqrt{a})^k - (z-\sqrt{a})^k}{2\sqrt{a}}$, se k é ímpar temos

$$Q = \binom{k}{1}z^{k-1} + \binom{k}{3}z^{k-3}\cdot a^1 + \binom{k}{5}z^{k-5}\cdot a^2 + \binom{k}{7}z^{k-7}\cdot a^3 + \cdots + \binom{k}{k}a^{\frac{k-1}{2}} = \sum_{j=0}^{\frac{k-1}{2}}\binom{k}{2j}z^{k-(2j+1)}\cdot a^j.$$

Como $\sum_{j=0}^{\frac{k-1}{2}}\binom{k}{2j}z^{k-(2j+1)}\cdot a^j$ é inteiro, temos que $Q = \dfrac{(z+\sqrt{a})^k - (z-\sqrt{a})^k}{2\sqrt{a}}$ é inteiro, para todo k ímpar pertecente aos naturais.

Agora se k é par, temos

$$Q = \binom{k}{1}z^{k-1} + \binom{k}{3}z^{k-3}\cdot a^1 + \binom{k}{5}z^{k-5}\cdot a^2 + \binom{k}{7}z^{k-7}\cdot a^3 + \cdots + \binom{k}{k-1}a^{\frac{k}{2}} = \sum_{i=0}^{\frac{k}{2}}\binom{k}{2i}z^{k-(2i+1)}\cdot a^i.$$

Como $\sum_{i=0}^{\frac{k}{2}}\binom{k}{2i}z^{k-(2i+1)}\cdot a^i$ é inteiro. Assim $Q = \dfrac{(z+\sqrt{a})^k - (z-\sqrt{a})^k}{2\sqrt{a}}$ é inteiro, para todo $k \in \mathbb{N}$.

Ao substituirmos a por z^2 em Q obtemos

$$Q = \frac{(z+\sqrt{a})^k - (z-\sqrt{a})^k}{2\sqrt{a}} \equiv \frac{(z+\sqrt{z^2})^k - (z-\sqrt{z^2})^k}{2\sqrt{z^2}} \equiv \frac{(2z)^k}{2z} \pmod{p}$$

o que implica em

$$Q \equiv 2^{k-1}z^{k-1} \pmod{p}$$

Por hipótese a é um resíduo quadrático módulo p, com isso $(a, p) = 1$, implicando que $(Q, p) = 1$. Dessa forma, $\overline{Q}$ pode ser determinado através da congruência $Q\overline{Q} \equiv 1 \pmod{p^k}$. Tomando

$$P^2 - aQ^2 = \left(\frac{(z+\sqrt{a})^k + (z-\sqrt{a})^k}{2}\right)^2 - a\left(\frac{(z+\sqrt{a})^k - (z-\sqrt{a})^k}{2}\right)^2$$

que é igual a

$$\frac{4(z+\sqrt{a})^k(z-\sqrt{a})^k}{4} = ((z+\sqrt{a})(z-\sqrt{a}))^k \equiv (z^2-a)^k \equiv 0 \pmod{p^k}$$

implica em

$$P^2 - aQ^2 \equiv 0 \pmod{p^k}$$

Assim,

$$P^2 \equiv aQ^2 \pmod{p^k} \Rightarrow (P\overline{Q})^2 \equiv a \pmod{p^k}$$

demonstrando o resultado.

■

Exemplo 3.18 *Para exemplificar esse algoritmo tomaremos a congruência do Exemplo (3.14) da página 66. Onde vimos que* $z^2 \equiv 23$ (*mod* 7) *admite duas soluções dadas por* $z^2 \equiv \pm 3$ (*mod* 7)*. Calcularemos os valores de P e Q para* $z_1 = 3$ *e* $z_2 = 4$*:*

$$P_1 = \frac{(3+\sqrt{23})^3 + (3-\sqrt{23})^3}{2} = \frac{468}{2} = 234$$

Analogamente para z_2*, obtemos* $P_2 = 340$ *e*

$$Q_1 = \frac{(3+\sqrt{23})^3 - (3-\sqrt{23})^3}{2\sqrt{23}} = \frac{100\sqrt{23}}{2\sqrt{23}} = 50.$$

De maneira análoga, para z_2*, obtemos* $Q_2 = 71$.
Recordando que $\overline{Q_1}$ *e* $\overline{Q_2}$ *são os inversos multiplicativos de* 7^3*, respectivamente, iguais a* 295 *e* 29*. Dessa forma, temos:*

$$x_1 \equiv 234 \times 295 \equiv \pm 87 \text{ (}mod\text{ } 343\text{)}$$

$$x_2 \equiv 340 \times 29 \equiv \pm 256 \text{ (}mod\text{ } 343\text{).}$$

Basta-nos agora, constatar que as soluções x_1 *e* x_2 *são iguais, uma vez que* $\pm 87 \equiv \pm 256$ (*mod* 343)

3.4 Soluções da Congruência $x^2 \equiv a \pmod{2^k}$

Consideremos a congruência

$$x^2 \equiv a \,(\mathrm{mod} 2^k). \tag{3.4}$$

De acordo com a segunda demonstração do Teorema (3.5) da página 63, o fato de $f'(x_1) = 2x_1$, impossibilita a aplicação do mesmo, uma vez que $(f'(x_1), 2) \neq 1$. Se x_0 é uma solução da congruência (3.4), o fato de $(a, 2) = 1$ implica em $(x_0, 2) = 1$ e ao reescrevê-la na forma

$$(x^2 - 1) + 1 \equiv a \,(\mathrm{mod}\ 2^k),$$

observa-se que:

- Se $k = 1$, a congruência (3.4) tem solução somente se $a \equiv 1 \mod 2$, isso ocorre quando $x \equiv 1 \,(\mathrm{mod}\ 2)$.
- Se $k = 2$, a congruência (3.4) admite solução se $a \equiv 1 \,(\mathrm{mod}\ 4)$, ou seja, quando $x \equiv \pm 1 \,(\mathrm{mod}\ 4)$.
- Se $k = 3$, a congruência (3.4) é solúvel se $a \equiv 1 \mod 8$. Dessa forma, a congruência (3.4) apresenta 4 soluções dadas por $x \equiv \pm 1 \,(\mathrm{mod}\ 8)$ ou $x \equiv \pm 3 \,(\mathrm{mod}\ 8)$.
- Para $k > 3$, a congruência (3.4) tem 4 soluções e assim como no caso anterior, para que haja solução, é necessário que $a \equiv 1 (\mathrm{mod}\ 8)$.

O Teorema a seguir caracteriza as soluções da congruência $x^2 \equiv a \,(\mathrm{mod}\ 2^k)$.

Teorema 3.6 *Se $k \geq 3$ e $a \in \mathbb{Z}$, tal que $a \equiv 1$ (mod 8), a congruência $x^2 \equiv a$ (mod 2^k) admite 4 soluções, e se x_k é uma solução, então as soluções dessa congruência são dadas por*

$$x_k, -x_k, x_k + 2^{k-1} \, e \, -x_k - 2^{k-1} \mod 2^k$$

Demonstração: O resultado já foi mostrado para $k = 3$. Para verificar sua validade para $k > 3$ tomaremos $x = \pm(1 + 4t_3)$, tal que $t_3 \in \mathbb{Z}$. É importante observar que x pode representar qualquer número ímpar. Veremos, para quais valores de x a congruência $x^2 \equiv$

a (mod 16) é satisfeita. Assim, temos

$$(1 + 4t_3)^2 \equiv a \text{ (mod 16)},$$

que implica em

$$1 + 8t_3 + 16t_3^2 \equiv 1 + 8t_3 \equiv a \text{ (mod 16)} \Rightarrow t_3 \equiv \frac{a-1}{8} \text{(mod 2)}.$$

Dessa forma, podemos escrever $t_3 = t_3' + 2t_4$ e consequentemente $x = \pm(1+4t_3'+8t_4) = \pm(x_4+8t_4)$. Testaremos, agora, quais desses números satifazem a congruência $x^2 \equiv a$ (mod 32). Assim,

$$(x_4 + 8t_4) \equiv a \text{ (mod 32)}$$

e seguindo o raciocínio análogo obtemos $t_4 = t_4' + 2t_5$. Portanto, $x = \pm(x_5 + 16t_5)$. Continuando esse processo, conclui-se que para $k \geq 3$ a congruência $x^2 \equiv a$ (mod 2^k) é satisfeita quando $x = \pm(x_k + 2^{k-1}t_k)$. Dessa forma, como t_k pode assumir os valores 0 ou 1, as 4 soluções dessa congruência são dadas por

$$x_k, -x_k, x_k + 2^{k-1}, -x_k - 2^{k-1}.$$

■

Exemplo 3.19 *Verificaremos se o Exemplo* (3.7) *da página* 53 *possui solução. Vimos que* $3x^2 + 4x + 5 \equiv a$ (*mod* 16) *é equivalente a resolvermos* $y^2 \equiv 5$ (*mod* 16)*, em que* $y = 3x + 2$*, que por sua vez, não possui solução, visto que* $5 \not\equiv 1$ (*mod* 8)*.*

Exemplo 3.20 *Analisaremos a congruência* $x^2 \equiv 41$ (*mod* 64)*. Ela admite quatro soluções, uma vez que* $41 \equiv 1$ (*mod* 8)*. Escrevendo x na forma* $x = \pm(1 + 4t_3)$ *temos*

$$(1 + 4t_3)^2 \equiv 41 \text{ (}mod\text{ 16)}$$

que implica

$$1 + 16t_3^2 + 8t_3 \equiv 41 \text{ (}mod\text{ 16)}.$$

Assim,

$$8t_3 \equiv 40 \text{ (}mod\text{ 16)} \Rightarrow t_3 \equiv 1 \text{ (}mod\text{ 2)}.$$

Logo, $t_3 = 1 + 2t_4$. *Então* $x = \pm[1 + 4(1 + 2t_4)] = \pm(5 + 8t_4)$. *Assim temos*

$$(5 + 8t_4)^2 \equiv 41 \ (mod\ 32)$$
$$25 + 64t_4^2 + 80t_4 \equiv 41 \ (mod\ 32).$$

Assim $t_4 = 2t_5$ *e* $x = \pm(5 + 16t^5)$. *Temos, finalmente, que a congruência pode ser escrita na forma*

$$(5 + 16t_5)^2 \equiv 41 \ (mod\ 64)$$

implicando em

$$25 + 256t_5^2 + 160t_5 \equiv 41 \ (mod\ 64).$$

Dessa forma

$$160t_5 \equiv 16 \ (mod\ 64) \ \Rightarrow \ t_5 \equiv 1 \ (mod\ 2).$$

Com esses resultados concluímos que $2t_5 = 1 + 2t_6$ *e logo* $x = \pm(13 + 32t_6)$. *Como* t_6 *pode assumir os valores* 0 *ou* 1, *as quatro soluções são dadas por* $x \equiv \pm 13, \pm 45 \ (mod\ 64)$.

Sabemos, agora, verificar a existência de soluções de congruências da forma $x^2 \equiv a \pmod{p^k}$ e conhecemos métodos para a sua resolução, consoante a p ser ímpar ou não. Na próxima Seção trataremos a respeito das soluções de $x^2 \equiv a \pmod{m}$, em que m é um número composto.

3.5 Soluções da Congruência $x^2 \equiv a \pmod{m}$

Considerando a congruência

$$x^2 \equiv a \pmod{m}, \tag{3.5}$$

em que $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ e $(a, m) = 1$. Como visto no início desse Capítulo, a solução da congruência quadrática (3.5) passa pela solução do sistema,

$$\begin{cases} x^2 \equiv a \pmod{2^{\alpha}} \\ x^2 \equiv a \pmod{p_1^{\alpha_1}} \\ x^2 \equiv a \pmod{p_2^{\alpha_2}} \\ \qquad \vdots \\ x^2 \equiv a \pmod{p_r^{\alpha_r}}. \end{cases} \tag{3.6}$$

De acordo com o Teorema (3.4) da página 56 e Teorema (3.5) da página 61, é possível resolver o sistema (3.6), quando as seguintes condições são satisfeitas:

- $a \equiv 1 \pmod 2$, se $\alpha = 1$
- $a \equiv 1 \pmod 4$, se $\alpha = 2$.
- $a \equiv 1 \pmod 8$, se $\alpha \geq 3$.
- $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = \cdots \left(\frac{a}{p_r}\right) = 1$.

Se essas condições são satisfeitas, as soluções da congruência quadrática (3.5), serão dadas pelas soluções dos sistemas da forma:

$$\begin{cases} x \equiv x_0 \pmod{2^{\alpha}} \\ x \equiv x_1 \pmod{p_1^{\alpha_1}} \\ x \equiv x_2 \pmod{p_2^{\alpha_2}} \\ \qquad \vdots \\ x \equiv x_r \pmod{p_r^{\alpha_r}}, \end{cases} \tag{3.7}$$

onde x_0 são as soluções da congruência $x^2 \equiv a \pmod{2^{\alpha}}$, x_1 são as soluções da congruência $x^2 \equiv a \pmod{p_1^{\alpha_1}}$,$\cdots$, x_r são as soluções da congruência $x^2 \equiv a \pmod{p_r^{\alpha_r}}$.

- Se $\alpha = 0$, $x^2 \equiv a \pmod{2^{\alpha}}$ então todo os valores de x são soluções congruentes;
- Se $\alpha = 1$, $x^2 \equiv a \pmod{2^{)}}$, então temos uma única solução;
- Se $\alpha = 2$, $x^2 \equiv a \pmod 4$, então temos duas soluções;
- Se $\alpha \geq 3$, $x^2 \equiv a \pmod{2^{\alpha}}$, então temos quatro soluções.

Pelo Teorema (3.5) da página 61, as congruências $x^2 \equiv a \pmod{p_i^{\alpha_i}}$ com $i = 1, 2, \cdots, r$ terão duas soluções cada uma. Usando o Teorema Chinês do Resto para resolver o sistema (3.7), a quantidade de soluções da congruência quadrática (3.5) será:

- 2^r soluções, se $\alpha = 0$ ou $\alpha = 1$,
- 2^{r+1} soluções, se $\alpha = 2$,
- 2^{r+2} soluções, se $\alpha \geq 3$.

Exemplo 3.21 *Suponha que desejamos resolver a seguinte congruência quadrática*

$$x^2 \equiv 9 \ (mod\ 308). \tag{3.8}$$

Temos $308 = 2^2 \cdot 7 \cdot 8$*, então resolver a congruência (3.8) é equivalente a resolver o sistema*

$$\begin{cases} x^2 \equiv 9 \ (mod\ 2^2) \\ x^2 \equiv 9 \ (mod\ 7) \\ x^2 \equiv 9 \ (mod\ 11) \end{cases} \tag{3.9}$$

Verificaremos se cada uma das congruências quadráticas do sistema (3.9) tem solução. Como $9 \equiv 1 \ (mod\ 4)$ *e* $\left(\frac{9}{7}\right) = \left(\frac{9}{11}\right) = 1$*, então a congruência (3.8) é solúvel. Resolvendo cada uma das congruências do sistema (3.8), encontramos, respectivamente, as seguintes soluções, dadas por* $x_0 \equiv \pm 1 \ (mod\ 4)$, $x_1 \equiv \pm 3 \ (mod\ 308)$ *e* $x_2 \equiv \pm 3 \ (mod\ 11)$*. As soluções da congruência (3.8) será dada pelas soluções dos sistemas de congruências lineares:*

$$\begin{cases} x \equiv x_0 \ (mod\ 2^2) \\ x \equiv x_1 \ (mod\ 7) \\ x \equiv x_2 \ (mod\ 11), \end{cases}$$

onde a quantidade de soluções da congruência (3.8) será $2^3 = 8$*. Para encontrarmos as oitos soluções da congruência (3.8), devemos encontrar as soluções dos seguintes sistemas lineares*

$$\begin{cases} x \equiv 1 \ (mod\ 2^2) \\ x \equiv 3 \ (mod\ 7) \\ x \equiv 3 \ (mod\ 11) \end{cases} \quad \begin{cases} x \equiv 1 \ (mod\ 2^2) \\ x \equiv 3 \ (mod\ 7) \\ x \equiv -3 \ (mod\ 11) \end{cases} \quad \begin{cases} x \equiv 1 \ (mod\ 2^2) \\ x \equiv -3 \ (mod\ 7) \\ x \equiv 3 \ (mod\ 11) \end{cases} \quad \begin{cases} x \equiv 1 \ (mod\ 2^2) \\ x \equiv -3 \ (mod\ 7) \\ x \equiv -3 \ (mod\ 11) \end{cases}$$

$$\begin{cases} x \equiv -1 \ (mod\ 2^2) \\ x \equiv 3 \ (mod\ 7) \\ x \equiv 3 \ (mod\ 11) \end{cases} \begin{cases} x \equiv -1 \ (mod\ 2^2) \\ x \equiv 3 \ (mod\ 7) \\ x \equiv -3 \ (mod\ 11) \end{cases} \begin{cases} x \equiv -1 \ (mod\ 2^2) \\ x \equiv -3 \ (mod\ 7) \\ x \equiv 3 \ (mod\ 11) \end{cases} \begin{cases} x \equiv -1 \ (mod\ 2^2) \\ x \equiv -3 \ (mod\ 7) \\ x \equiv -3 \ (mod\ 11) \end{cases}$$

Para resolvermos os sistemas lineares usaremos o Teorema Chinês do Resto. Como $(4, 7) = (7, 11) = (4, 11) = 1$*, as soluções dos sistemas lineares serão dados por* $X = x_0 n_0 \overline{n_0} + x_1 n_1 \overline{n_1} + x_2 n_2 \overline{n_2}$ $(mod\ 308)$*, onde* $n_i = \dfrac{m}{m_i}$*, tal que* $m = 308, m_0 = 4, m_1 = 7$ *e* $m_2 = 11$ *e* $\overline{n_i}$ *é solução de* $n_i x \equiv 1 \ (mod\ m_i)$ *com* $i = 0, 1, 2$*.*

Resolvendo, por exemplo, o sistema linear:

$$\begin{cases} x \equiv 1 \ (mod\ 2^2) \\ x \equiv 3 \ (mod\ 7) \\ x \equiv 3 \ (mod\ 11), \end{cases} \tag{3.10}$$

segue que n_i *e* $\overline{n_i}$ *com* $i = 0, 1, 2$*, é* $n_0 = 77, n_1 = 44, n_2 = 28$ *e*

$77x \equiv 1 \ (mod\ 4)$	$44x \equiv 1 \ (mod\ 7)$	$28x \equiv 1 \ (mod\ 11)$
$\overline{n_0} \equiv 1 \ (mod\ 4)$	$\overline{n_1} \equiv 4 \ (mod\ 7)$	$\overline{n_2} \equiv 2 \ (mod\ 11)$

Portanto a solução do sistema (3.10) será dada por

$$X \equiv 77 \cdot 1 \cdot 1 + 44 \cdot 3 \cdot 4 + 28 \cdot 3 \cdot 2 = 773 \equiv 157 \ (mod\ 308)$$

Resolvendo os outros sistemas de maneira análoga ao sistema (3.10), as oito soluções da congruência (3.8), são $x \equiv 3 \ (mod\ 308)$*,* $x \equiv 25 \ (mod\ 308)$*,* $x \equiv 129 \ (mod\ 308)$*,* $x \equiv 151 \ (mod\ 308)$*,* $x \equiv 157 \ (mod\ 308)$*,* $x \equiv 179 \ (mod\ 308)$*,* $x \equiv 283 \ (mod\ 308)$ *e* $x \equiv 305 \ (mod\ 308)$*.*

3.6 Aplicação

É de suma importância o estudo de pontos racionais sobre curva plana, por exemplo, são empregadas em criptografia e fatoração de números inteiros. O principal problema envolvendo as curvas algébricas consiste em encontrar pontos com coordenadas racionais que satisfaçam a sua equação. Encontrada suas coordenadas, podemos obter a estrutura de grupo destas curvas.

Quando a parábola $x^2 - 7y = -2$ possui coordenadas inteiras?

Transformaremos a equação da parábola dada na forma de congruência, ou seja, $x^2 - 7y = -2$

é equivalente a $x^2 \equiv 2 \pmod 7$. A congruência terá solução inteira se $\left(\frac{2}{7}\right) = 1$, de fato, $3^2 \equiv 2 \mod 7$.

As coordenadas inteiras da parábola serão da forma

$$\begin{cases} x = 3 + 7t \\ y = 1 + 6t + 7t^2 \end{cases} \quad ou \quad \begin{cases} x = 4 + 7t \\ y = 2 + 8x + 7t^2 \end{cases}$$

3.6.1 Como achar as soluções inteiras de $x^2 - py = a$

Se a é um Resíduo Quadrático módulo p e x_0 é uma solução particular de $x^2 \equiv a \mod p$, então

$$x = \pm x_0 \pm p \cdot t \text{ é solução}$$

Sejam x_0 e x_1 soluções incongruentes módulo p temos:

$$\begin{cases} x_0^2 \equiv a \pmod p \\ x_1 \equiv a \pmod p \end{cases} \Rightarrow \quad x_1^2 - x_0^2 \equiv 0 \mod p \Rightarrow \quad (x_1 - x_0) \cdot (x_1 + x_0) \equiv 0 \pmod p$$

$$x_1 \equiv x_0 \qquad \text{ou} \qquad x_1 \equiv -x_0 \Rightarrow x_1 = x_0 + pt \qquad \text{ou} \qquad x_1 = -x_0 + pt$$

Subsitituindo temos: $x^2 \equiv a \pmod p \Rightarrow \quad x^2 = a + py$, daí

$$a + py = (x_0 + pt)^2$$

$$a + py = x_0^2 + 2x_0pt + p^2t^2$$

$$y = \frac{x_0^2 - a}{p} + 2x_0t + pt^2.$$

Referências Bibliográficas

Araújo, L. R. (2013). Congruências quadráticas, reciprocidade e aplicações em sala de aula. Dissertação de Mestrado, PROFMAT–UFPB, João Pessoa/PB.

Biase, A. e Agustini, E. (2009). Criptografias elgamal, rabin e algumas técnicas de ciframento. *FAMAT*, 13:35–64.

Campos, G. D. M. (2013). Equações diofantinas lineares. Dissertação de Mestrado, PROFMAT– UFMT, Cuiabá/MT.

Carvalho, J. F. d. (2012). Evolução do pensamento matemático, das origens aos nossos dias. *Ciência e Cultura*, 64(2):52–55.

Dan Ma (2015). Solving quadratic congruences with odd prime moduli. Disponível em `https://exploringnumbertheory.wordpress.com/2015/12/09/solving-quadratic-congruences-with-odd-prime-moduli/` Acesso em: 1/nov/2016.

Gauss, C. F., Brüning, J., e Schappacher, N. (2006). *Disquisitiones arithmeticae*. Olms-Weidmann.

Hefez, A. (2006). *Elementos da Aritmética*. SBM., Rio de Janeiro.

Hefez, A. (2013). *Aritmética*. SBM, Rio de Janeiro.

Medeiros, J. M. G. d. (2015). Congruências quadráticas, reciprocidade e aplicações em sala de aula. Dissertação de Mestrado, PROFMAT–UFPB, João Pessoa/PB.

Mota, M. L. (2006). LEI DA RECIPROCIDADE QUADRÁTICA. Disponível em `http://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/LRQ_MM.pdf/` Acesso em: 02/dez/2016.

Oliveira, F. (2011). Introdução à Teoria de Números. Disponível em http://arquivoescolar.org/bitstream/arquivo-e/42/1/tnumeros.pdf/ Acesso em: 29/nov/2016.

Oliveira, M. C. (2013). Aritmética: criptografia e outras aplicações de congruências. Dissertação de Mestrado, PROFMAT– UFMS, Campo Grande/MS.

REALE, G. e ANTISERI, D. (2003). História da filosofia: filosofia pagã antiga, v. 1 tradução: Ivo storniolo. *São Paulo: Paulus*.

Rocha, L. (2010). A lei de reciprocidade quadrática. Disponível em https://www.academia.edu/6736840/A_Lei_da_Reciprocidade_Quadratica/ Acesso em: 20/dez/2016.

Roque, T. (2012). *História da matemática*. Zahar.

Rosa, C. A. P. (2012a). Da antiguidade ao renascimento científico. In *História da Ciência*, volume I, página 469. Fund. Alexandre Gusmão, Brasília, 2ª ed. edição.

Rosa, C. A. P. (2012b). O pensamento científico e a ciência no século XIX. In *História da Ciência*, volume II, página 375. Fund. Alexandre Gusmão, Brasília, 2ª ed. edição.

Rosen, K. H. (2011). *Elementary number theory*. Pearson Education, Boston.

Rousseau, S. (2012). Quadratic and cubic reciprocity. Dissertação de Mestrado, Eastern Washington University, Cheney/ Washington.

Said, S. (1975). Introdução à teoria dos números. *Coloquio Brasileiro de Matematica, IMPA*, 10.

Santos, J. P. O. (2011). *A intrudução a Teoria dos Números*. SBM, Rio de Janeiro.

Shanks, D. (1972). Five number-theoretic algorithms. In *Proceedings of the second Manitoba conference on numerical mathematics*, volume 51, página 70.

Vinogradov, I. e Bernardo, E. B. (1977). *Fundamentos de la teoría de los números*. Mir.

Apêndice

A.1 Polinômio de Taylor

Os polinômios são funções fáceis de serem manipulados. É natural, portanto, buscar aproximar funções mais complicadas por funções polinomiais. A Fórmula de Taylor nos fornece uma regra para determinar o polinômio de grau n que melhor se aproxima de uma dada função em uma vizinhança de um ponto p no seu domínio. De uma forma geral, se a função dada $f(x)$ for derivável até ordem n, procuramos um polinômio p de grau n satisfazendo

$$p^{(k)}(x_0) = f^{(k)}(x_0), \qquad k = 0, 1, 2, \cdots, n,$$

tal polinômio terá a seguinte forma

$$p_n(x) = f(x_0) + f'(x_0)(x - x_0) + \left(\frac{f''(x_0)}{2}\right)(x - x_0)^2 + \cdots + \left(\frac{f^{(n)}(x_0)}{n!}\right)(x - x_0)^n$$

o qual é chamado de polinômio de Taylor de ordem n de $f(x)$ numa vizinhança de x_0.

Definimos o polinômio de Taylor de ordem 1 de $f(x)$ numa vizinhança de p por

$$p_1(x) = f(x_0) + f'(x_0)(x - x_0)$$

e p_1 é a função linear que melhor aproxima localmente $f(x)$ numa vizinhança de x_0.